JOURNAL OF GLOBAL ACCOUNTING
9 (1) April, 2023.
ISSN: 1118 – 6828
https://journals.unizik.edu.ng/joga

COMPUTERIZED FORENSIC INVESTIGATION TECHNIQUE AND FRAUD DETECTION IN THE PUBLIC SECTOR: PERCEPTION OF PROFESSIONAL ACCOUNTANTS IN ANAMBRA STATE

Paper Type: *Original Research Paper.*
Correspondence: *bc.ofoje@unizik.edu.ng*

Key words: *Computerized Forensic investigation, Forensic Accounting, Fraud Detection, Fraud Litigation.*

CITATION: Ofoje, B.C. & Aggreh, M. (2023). Computerized Forensic Investigation Technique and Fraud Detection in the Public Sector: Perception of Professional Accountants in Anambra State, *Journal of Global Accounting*, 9(1), 407 – 447.

Available:https://journals.unizik.edu.ng/joga

Bibbian C. Ofoje[1] Meshack Aggreh[2]
[1]Postgraduate Research Student [2]Lecturer, Department of Accountancy, Nnamdi Azikiwe University, Awka, Nigeria
1 Email: bc.ofoje@unizik.edu.ng
2 Email: aggrehmeshack@gmail.com

ABSTRACT:

The study examines the relationship between computerized forensic investigation and fraud detection in Nigeria. The three specific objectives of the study were to: determine the perception on forensic accounting practice regarding fraud detection in the Nigerian Public sector; determine the relationship between fraud litigation practice and fraud detection in the Nigerian Public sector; evaluate the perception of accountants on whether computerized forensic accounting techniques aid in fraud detection in the Nigerian Public sector. Descriptive survey research design was adopted for the study. Purposive sampling approach was applied in selecting a sample of two hundred and forty-two (242) professional accountants from a population of 612 professional accountants affiliated to ICAN and ANAN and are practicing in Anambra State. Primary data were collected through the means of a structured questionnaire. The inferential analysis in the present study was done by means of Ordinal Regression Model at 5% significance level. The results showed that: forensic accounting practice significantly and positively relates to fraud detection in the Nigerian public sector (β = 0.4339, p-value = 0.011); there is no significant relationship between fraud litigation practice and fraud detection in the Nigerian Public sector (β = -0.0302, p-value = 0.822); computerized forensic accounting techniques significantly aids in fraud detection in the Nigerian Public sector (β = 0.3089, p-value = 0.010). The study recommended that organizations in the Nigerian public sector should consider utilizing computerized techniques, such as data analytics and artificial intelligence, to support their fraud detection efforts. These techniques can automate and streamline the process of fraud detection, making it faster and more accurate..

1. INTRODUCTION

As a result of recent highly publicized financial scandals, reported increase in occupational fraud and heightened concern over money laundering to support terrorism and racketeering, legislative mandates and public expectations have heightened the necessity to further define the auditor's and accountant's responsibility for detecting fraud within organizations. Successful fraud or forensic accounting analysis and findings reported by practicing professionals show the difference between whether perpetrators avoid detection of their illegal activities or they are brought to justice. In most cases, success is directly and primarily dependent upon the knowledge skills and abilities of the professionals performing the work. Consequently, the demand for entry-level professionals with formal education in fraud and forensic accounting has grown. Academic institutions and stakeholder organizations that provide education in this field are faced with a number of questions regarding the nature, extent, and format of a worthwhile computerized forensic investigation.

The history of forensic accounting can be traced back, as far as 1817, in *Meyer v. Sefton*, a case in Canada that allowed an 'expert witness' to testify in court. Forensic accounting as a profession continued to grow during the latter half of the century, as the Generally Accepted Accounting Practice and tax laws became widespread and mandatory (Oyedokun, 2013). It was observed however, by the Association of Certified Fraud Examiners (2018) that the challenges posed by fraud are significant and it further stated that the annual, global losses caused by occupational fraud exceed several billion US Dollars. The Association of Certified Fraud Examiners (2019) further opined that apart from asset misappropriation, other form of occupational fraud exist namely corruption and financial statement fraud. The cases of Enron and WorldCom which rocked the corporate world have brought the field of forensic investigation and forensic audit into the limelight. Forensic auditing and forensic investigation is seen as summarizing all other investigation related areas in unearthing fraudulent practices. One of the best forensic strategies that can be used in resolving the assertion of fraudulent activities is Forensic Audit and Forensic Investigation. Red flags of financial crime can be detected at first instance in a variety of ways such as by accident, by whistle-blowing, by auditors, by data mining, by controls and testing, or by the organization's top management requesting an inspection on the basis of mere suspicion. Karwai (2004) (as cited in Amake & Ikhatua, 2015) opined that, increase wave of fraud is causing a lot of havoc in the Nigeria federal ministries. This is because fraud has penetrated into every aspect of country's federal ministries and parastatals. Okunbor and Obaretin (2010) reported that the spates of corporate failure have placed greater responsibilities and functions on accountant to

equip themselves with skills to identify and act upon indicators of poor corporate governance, mismanagement, frauds, money laundering and wrong doing".

Forensics refers to the scientific methods used to solve a crime (www.pinow.com). Forensic investigation is the gathering and analysis of all crime-related physical evidence in order to come to a conclusion about a suspect. Forensic accounting includes the use of accounting auditing, and investigative skills to assist in legal matters (www.pinow.com). It consists of two major components. Litigations services that recognized the role of an accountant as an expert consultant, and investigative service that uses a forensic accountant's skills and may require possible court room testimony (Okoye & Gbegi, 2013). Forensic accounting could be used to reverse the leakages that cause corporate failures. This can be attributed to the fact that proactive forensic accounting practice seeks out errors, operational vagaries and deviant transactions before they crystallize into fraud (Ozkul & Pamukc, 2012). With the rise of digital technology, computerized approach to work processes and operations, there came about the need of performing forensic audit via the computer based technology, which therefore will be in a form acceptable in the court of law in event of any court proceeding thereafter.

Lutkevich (2021) defined computerized forensics as the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The terms digital forensics and cyber forensics are often used as synonyms for computer forensics. The objectives of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it. According to Tjeng and Nopianti (2020), one of the causes of the problematic detection of fraud is due to the continued development of forensic accounting and the absence of experts who can identify and disclose the presence of a fraud such that handling it becomes difficult. Accounting graduates who work as accountants or auditors ought to understand forensic accounting and investigation. Therefore, this branch of accounting is paramount, requires skills, improvement and actions that will ameliorate the current trend of problems, especially those related to fraud issues in the digital environment and outside the digital environment that often occurs as an indication of corruption in the system. Computer forensics requires a well-balanced combination of technical skills, legal acumen, ethical conduct and current computer software.

Recent corporate accounting scandals have led to increase legal and regulatory requirement for improved corporate governance. These requirements address internal controls for detecting and deterring fraud and encourage financial statements auditors to be more aggressive in searching for fraud. In turn, this has resulted in increased demand for entry-level practitioners and professionals who have greater fraud awareness, as well as competence, knowledge and computer skills related to fraud and forensic accountant. On a more basic level, traditional accounting graduates entering the profession as corporate accountants and internal or external auditors are expected to have a greater understanding of fraud and forensic accounting skills and techniques. In addition there is a disparity between the old accountants and the new accountants where the former seems not to have a proper understanding of computerized forensic accounting techniques. There is a growing demand for professional Accountants in forensic and litigation advisory services. The position of the court in Nigeria is of the belief that fraud being an allegation of a criminal nature; hence the standard of proof is proof beyond reasonable doubt. Therefore, when such accountants and auditors obtain evidences during fraud investigations, in most cases it is difficult to prove the obtained evidences in the court of law. In recent times, cybercrime has increased astronomically. The handling of cybercrime cases is still quite tricky because the technology in Nigeria is still inadequate, and there appear to be high lack of knowledge of digital techniques. The techniques, methods and unique moves used to manipulate and circumvent a system are innumerable and the possibility of detecting all such fraud may just be a mirage. Only a minute number of cases that occur are actually revealed while there are most likely astonishing number cases occurring periodically, which are undisclosed (Tjeng & Nopianti, 2020). These perpetrators are getting much more advanced in perpetrating this mischievous act with all impunity hence, the need for computerized forensic investigation and fraud detection.

Numerous research efforts has been made in assessing the importance of the services of computerized forensic investigations to business organizations especially in improving the quality of litigations and uncovering fraud. Most of these research efforts, among others include: Ojukwu, Ubi, Olugbemi, Olugbemi and Emefiele (2020); Baroto, and Prasetyo (2020); Griffiths and Pretorius (2021); Kearns (2015); Okolo, Iduma and Ani (2018); Veerankutty, Ramayah and Ali (2018); Cook and Clements (2009); Laubscher, Rabe, Olivier, Eloff and Venter (2005); Gardi (2018), which have focused on the fraud and forensic accounting activities in non-government institutions, banks and other financial institutions.

This study has identified this lacuna in forensic accounting research especially in the Public sector for developing economy like Nigeria.

1.1 Objectives of the Study

The aim of this research study is to establish the relationship between computerized forensic investigation and fraud detection in Nigeria while the specific objectives are to:

1. determine the perception on forensic accounting practice regarding fraud detection in the Nigerian Public sector.
2. determine the relationship between fraud litigation practice and fraud detection in the Nigerian Public sector.
3. evaluate the perception of accountants on whether computerized forensic accounting techniques aid in fraud detection in the Nigerian Public sector.

1.2 Hypotheses

The following hypotheses are formulated in Null form:

i. *Ho:* Forensic accounting practice does not significantly relate to fraud detection in the Nigerian public sector.
ii. *Ho*: There no significant relationship between fraud litigation practice and fraud detection in the Nigerian Public sector.
iii. *Ho*: Computerized forensic accounting techniques do not significantly aid fraud detection in the Nigerian Public sector.

2. LITERATURE REVIEW

2.1 Conceptual review

2.1.1 Forensic accounting

Forensic accounting is the specialty area of the accountancy profession which describes engagements that result from actual or anticipated disputes or litigation. Forensic accounting has many definitions as there are many writers in this area of accounting literature. There is thus no single definition adjudged to be the best. By 1980, major academic studies were published on this area of study, (Rassey, 2009), thus, leading to a new profession in the field of accounting and audit. Alhassan (2021) opined that forensic accounting being a contemporary area in accounting has an essential position in protecting the Nigerian public sector against economic and financial irregularities. According to Eze and Okoye (2018), Forensic accounting technique should be encouraged by the National Universities Commission as a field of study by its inclusion in the curriculum at the undergraduate and

post-graduate studies. The professional bodies should as well include forensic accounting in their professional examination. It is concerned with the use of accounting discipline to help determine issues of facts in business litigation (Okunbor & Obaretin, 2010). This profession identified a field composed of accounting, auditing, and investigative skills (Ozkul & Pamukc, 2012).

The America Institute of Certified Public Accountants (AICPA) defines forensic accounting as services that involve the application of specialized knowledge and investigative skills possessed by Certified Public Accountant utilizes the practitioner's specialized accounting, auditing, economic, tax, and other skills (AICPA 2010). Forensic accounting is the integration of accounting, auditing and investigative skills (Zysman, 2004). "Forensic" entails "suitable for use in a court of law," and it is to that standard and potential outcome that forensic accountants generally have to work (Crumbley, Heitger & Smith, 2007). Singleton and Singleton (2010) stated that forensic accounting is the comprehensive view of fraud investigation and includes preventing frauds and analyzing antifraud control which involves the gathering of nonfinancial information. Forensic accountants are trained to look beyond the numbers and deal with the business realities of situations. Analysis, interpretation, summarization and the presentation of complex financial business related issues are prominent features of the profession. He made further report that the activities of forensic accountants involve: investigating and analyzing financial evidence; developing computerized applications to assist in the analysis and presentation of financial evidence; communicating their findings in the form of reports, exhibits and collections of documents; and assisting in legal proceedings, including testifying in courts, as an expert witness and preparing visual aids to support trial evidence (Bhasin, 2007). According to Kasum (2009) and Crumbley, Heitger and Smith (2007), forensic accounting can also be viewed as investigative accounting or fraud audit, a discipline that combines forensic science and accounting. Crumbley et al, further opined that forensic science refers to the application of laws of nature to the laws of man. Extending this, he asserted that a forensic scientist is one who examines and interprets evidence and facts in legal cases and also offers expert opinions regarding their findings in the court of law. Also Zysman (2004) viewed forensic accounting as a synthesis of accounting, auditing and investigative skills. Coenen (2005) asserts that forensic accounting uses accounting concepts and techniques in solving legal problems. The Association of Certified Fraud Examiners(2010), defines forensic accounting as the use of skills in potential or real civil or criminal dispute, including generally accepted accounting and auditing principles in

establishing loss of profit, income, property or damage, estimations of internal controls, fraud and others that involve inclusion of accounting expertise into the legal system.

From these definitions, it is worthy to state that forensic accounting involves the application of financial accounting concepts, auditing techniques and investigative procedures in solving legal problems. It is also imperative to note that the responsibility of preventing and detecting fraud in financial statements lies not only in the hands of management of an enterprise, but also other control institutions and mechanisms. Adequate system of internal control, efficient internal auditing procedures and periodic audit committee are the key elements for prevention and detection of frauds that are created through property misuse as well as those that use financial statements as instruments of frauds. However, external auditing and forensic accounting perform retrospective control of financial data with the aim of detecting omissions, frauds and securing the reliability and credibility of the financial statements.

2.1.2 Fraud investigation

A fraud investigation tries to determine whether fraud has taken place and tries to detect evidence of fraud which has occurred. Fraud is considered to involve misrepresentation with intent to deceive. In most cases, fraud investigations are investigations of white collar crime, which involves surveillance and careful consideration of complicated financial records (Oyedokun, 2015). In the views of Singleton & Singleton (2010) forensic accounting comprehensively entails fraud investigation, prevention of fraud and analyzing antifraud controls in addition to gathering non-financial information. Yormark (2004) stated that the forensic examination team should be carefully chosen. A decision should be made to outsource for more experienced staff members or staff members demonstrating skills in investigative techniques if needed. The author also stated that with the initiation of the whistleblower protection provisions of Sarbanes-Oxley, employees will be more likely to speak about irregularities they observed which might result in additional fraud investigations. Most fraud investigations begin with a meeting between the investigator and the client. The person launching the investigation explains to their investigators why they suspect fraud has taken place and hand over any evidence they have to the investigator. A good fraud investigator will use this initial information to find more evidence and more facts. A fraud investigator may use surveillance, audit trails, asset searches, background checks, employee investigations, business investigations, and other types of methods to get to the bottom of a case. According to Association of Certified Fraud Examiners, Manual (2019), in an organization, fraud examination is carried out for various objectives as follows: identifying

improper conduct, identifying the persons responsible, stopping fraud, sending a message that fraud will not be tolerated, determine the extent of potential losses, facilitate the recovery, prevent future losses, mitigate other consequences, and strengthen internal control. The role of fraud examiner in an investigation is mostly divided into four activities: obtaining evidence, reporting, testifying, and assisting in fraud detection and prevention.

2.1.2.1 Obtaining evidence

The value of a fraud examination stands on the credibility of the evidence obtained. Evidence of fraud generally takes the form of documents or statements by witnesses; therefore, fraud examiners must know how to obtain documentary evidence and witness statements legally and adequately (ACFE, 2019).

2.1.2.2 Reporting

Once the evidence has been obtained and analyzed, and findings have been drawn from it, the fraud examiner must report the results to the designated individuals (e.g., management, the board, or the audit committee). A fraud examination report is a narration of the fraud examiner's specific activities, findings, and, if appropriate, recommendations (ACFE, 2019).

2.1.2.3 Testifying

Often, fraud examiners are called upon to provide testimony and report their findings at a deposition, trial, or other legal proceedings. When providing testimony, fraud examiners must be truthful. They should also communicate clearly and succinctly (ACFE, 2019).

2.1.2.4 Assisting in Fraud Detection and Prevention

Fraud Examiners are not responsible for preventing fraud; such responsibilities belong to management or other appropriate authority. Nevertheless, fraud examiners are expected to actively pursue and recommend appropriate policies and procedures to prevent fraud (ACFE, 2019). Since most of the fraudulent cases use evidence consisting of accounting data and specifically accounting data retrieved from an AIS system of some sort, these investigators must be well trained in the AIS documentation processes as well as being experienced with the identification and understanding of the effect of inadequate internal controls of AIS systems. In addition, forensic accountants do not need to not only be able to understand AIS data, but they must also be able to articulate and explain sometimes highly technical and complex evidence to the court in simple enough terms to be understood (Bressler, 2012). An investigator might utilize digital forensics tools to recover and investigate material discovered

in a digital device to support the investigation (Baroto & Prasetyo 2020). Eiya and Otalor (2013), described forensic investigation as the utilization of specialized investigative skills in carrying out an inquiry conducted in such a manner that the outcome will have application to a court of law. A forensic investigation may be grounded in accounting, medicine, engineering or some other discipline.

2.1.3 Investigation skills

Investigation is the search and examination of the particulars of an event to determine the unique, hidden, or complex facts surrounding the event. Investigation is a vital part of forensic accounting and auditing process but only applied when the event or transaction is obscured.

It could be referred to as a detailed verification and clarification of doubt about a transaction or event (Oyedokun, 2015). Such audits where investigative skills are required is known investigative audit. For an investigative audit to be effectively performed, the forensic accountant must have adequate investigative skills to enable him carry out proper investigations. He must therefore use some approaches, procedures or techniques commonly used in an investigation or investigation of a crime. Such investigative skills should be encouraged and imbibed in the academic curriculum of the training accountants/auditor.

Tjeng and Nopianti (2020) observed that, the investigation is not necessarily directly carried out because the indications found are generally still very premature so that it requires a little deepening in order to obtain evidence that is strong enough to be carried out investigation investigations. However, Meuldijk (2017) opined that, the overall outline of the investigative audit process, from beginning to end, is broken down as follows:

2.1.3.1 Preliminary Information Review

The examiner carries out: gathering additional information, compiling facts and process events, determining and calculating tentative financial losses, determining tentative irregularities, and preparing initial hypotheses (Meuldijk, 2017).

2.1.3.2 Planning Investigation Examination

At the planning stage, the initial hypothesis testing, identification of evidence, determining the place or source of evidence, analyzing the relationship of evidence with related parties, and preparing an investigation program (Meuldijk, 2017).

2.1.3.3 Implementation

At the implementation stage: a collection of evidence, physical testing, confirmation, observation, analysis and testing of documents, interviews, refinement of hypotheses and review of working papers (Meuldijk, 2017).

2.1.3.4 Reporting

The contents of the report of the investigation audit include elements against the law, facts and processes of the incident, the impact of financial losses due to irregularities/acts against the law, causes of unlawful actions, parties involved in irregularities/actions against the law that occur, and forms of cooperation between the parties involved in irregularities/actions against the law (Meuldijk, 2017).

2.1.3.5 Follow Up

At this follow-up stage: the process has been submitted from the audit team to the leadership of the organization and formally subsequently submitted to law enforcement. Submitting a report on the results of an investigative audit is expected to have entered the investigation stage. Regarding testimonies in the proceedings in court, an investigative audit team can be appointed by the organization to provide expert information if needed (Meuldijk, 2017).

2.1.4 Computerized Forensics

Computer forensics remains the investigators best tools in the detection and implementation of white-collar investigations. While the forensic accounting profession continues to grow, most accounting students do not have exposure to a class in computer forensics. To be effective, it is essential that forensic accountants be knowledgeable of and able to apply basic computer forensic skills (Kearns, 2015). The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information (Chigozie-Okwum, Michael & Ugboaja, 2017). Digital forensics begins with the collection of information in a way that maintains its completeness and integrity. Investigators then analyze the data or system to determine if it was swapped or changed, how it was changed and who made the changes. The use of computer forensics is not always tied to a crime. The forensic process is also used as part of data recovery processes to gather data from a crashed server, failed drive, reformatted operating system (OS) or other situation where a system has unexpectedly stopped working (Lutkevich, 2021). Banarescu (2015) stated that, in the last few years, we have been witnessing a massive increase in the quantity of data (text, pictures, audio, video

etc.), both at global and economic level entities. This process is amplified by the entry of any entity mentioned above into the virtual environment. Data comes from everywhere, from numerous and diverse sources like contracts, customer interactions, call centers, social media, phones, emails, faxes, and others. The trend is to use these data for the interest of the entity (conceiving strategies, opportunities identification, goodwill development, preventing and detecting fraud etc.). The use of data analysis processes and the software dedicated to these operations provide extensive and in-depth analysis of the phenomena and processes of the informal economy, fraud and corruption, as the information and communication technology becomes a sine qua non instrument of registered (formal) economy. Although on the analytical market, there is a wide spectrum of specialized tools capable to support and enhance the antifraud activity, unfortunately, the survey results indicate that managers are not taking advantage of them.

Oyedokun (2015) opined that it is not just the content of emails, documents and other files which may be of interest to investigators but also the 'metadata' associated with those files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions. The increase of digital fraud has led many accountants to acquire advance information technology (IT) skills and certifications in order to qualify as IT auditors and forensic accountants (Davis, Schiller & Wheeler, 2007). In the Nigerian judicial system, computer forensics helps ensure the integrity of digital evidence presented in court cases. One of the major approaches adopted by forensic accounting technique in fraud management in Nigeria is the provision of reliable, valid and substantial forensic accounting evidence in fraud prosecution and for litigation services by the Nigerian judicial system. With the application of forensic accounting services and evidence to legal proceedings, litigation services are expected to have been improved so as to ensure effectiveness of the system (Gbegi & Habila, 2007).

As computers and other data-collecting devices are used more frequently in every aspect of life, digital evidence -- and the forensic process used to collect, preserve and investigate it -- has become more important in solving crimes and other legal issues (Lutkevich, 2021). Perhaps the most common example is seizing the computer of a suspect for analysis. In gaining access to or auditing the data on a digital device, computer forensics can also involve white hat (legal) hacking, password and encryption cracking, key logging, digital surveillance, and intrusion detection (Alao & Odum, 2019). It provides an accounting analysis

that is suitable to the court, which will form the basis of discussion, debate and ultimately dispute resolution (Zysman, 2004).

2.1.5 Fraud Detection

Fraud is a legal term that refers to the intentional misrepresentation of the truth in order to manipulate or deceive a company or individual. Fraud is to create a misjudgment or maintain an existing misjudgment to induce somebody to make a contract". It involves enriching oneself intentionally by reducing the value/worth of an asset in secret. Ojukwu, Ubi, Olugbemi, Olugbemi and Emefiele (2020) opined that, defining fraud is as difficult as identifying it. No definite and invariable rule can be laid down as a general proposition in defining fraud as it includes surprise, trick, cunning and unfair ways by which another is cheated. According to Ozkul and Pamukc (2012), when business frauds are analyzed, it is ascertained that three components come together when committing the crime. These are pressure, opportunity, and justification that constitute the fraud triangle. Components of the fraud triangle are similar to the fuel, spark, and oxygen which together cause fire. When the three come together, inevitably fire breaks out. Pressure factors could be gathered into three groups: pressures with financial content, pressures stemming from bad habits and pressures related with job. Opportunity factors are the second component of the fraud triangle.

The AICPA (2016) stated that many financial statement frauds have been perpetrated by intentional override by senior management of what might otherwise appear to be effective internal control. Indeed, with very few exceptions, most of the major fraud cases in the past 50 years that had catastrophic results for the organization were perpetrated by senior members of management circumventing or overriding seemingly sound systems of internal control. To further emphasize on this, Gottschalk (2011), noted that fraud is not a possibility but a probability. He also explains that fraud can be better prevented if decisions are made by a group and not an individual. However, this is not the case if the group has the same interest in mind. Then fraud may not be prevented. Conversely, the group is influenced by the dominant decision maker who ends up deciding everything. Fraud assumes so many different degrees and forms that courts are compelled to context themselves with only few general rules for its discovery and defeat.

2.1.6 Computerized Forensic Investigation and Fraud Detection

Computer forensics is the practice of collecting, analyzing and reporting on digital data in a way that is legally admissible in court of jurisprudence. It can be used in the detection and

prevention of crime and in any dispute where evidence is stored digitally. Computer forensics follows a similar process to other forensic disciplines, and faces similar issues. There are few areas of dispute or crime where computer forensics cannot be applied. The law enforcement agencies have been among the earliest and heaviest users of computer forensics and consequently have often been at the forefront of developments in the field. Computers may constitute a 'scene of a crime', for example with hacking or denial of service attacks or they may hold evidence in the form of audit trail, emails, internet history, documents or other files relevant to crimes such as murder, kidnap, fraud and drug trafficking (Oyedokun, 2015). Computerized forensic investigation entails the use of computer software to aid prevention, deterrence, detection and investigation of fraud and other white-collar crimes. It is a broad concept that covers the use of generalized audit software for data extraction and analysis, the use of spreadsheet, access, database and other specialized software for fraud detection and analysis, as well as the use of the internet and other investigative tools such as public record search, data mining, continuous monitoring and auditing software and link analysis software. The basic concept of "red flags" (fraud risk factors), anomalous relationships, events, conditions, or symptoms that indicate an increased probability of fraud must however not be underestimated in the quests for the use of computerized forensic accounting and investigation.

Computerized forensics is an important tool for solving crimes committed with computers (e.g. phishing and bank fraud), as well as for solving crimes against people where evidence may reside on a computer (e.g. money laundering and child exploitation).Forensic tools have also become a vital tool for Information Assurance because of their ability to reconstruct the evidence left by cyber-attacks. Today, almost every financial fraud incorporates the use of a computer, whether the fraud is falsifying invoices or electronic money laundering (Smith, 2005). According to the Sarbanes-Oxley Act of 2002 and Statement on Auditing Standards No. 99 (SAS 99, 2002), "Consideration of Fraud in a Financial Statement Audit," extended expectations for auditors stating that, "Electronic evidence often requires extraction of the desired data by an auditor with IT knowledge and skills or the use of an IT specialist … it may be necessary for the auditor to employ computer assisted audit techniques … to identify the journal entries and other adjustments to be tested" (AICPA 2012, p. 6). Nelson, Philips and Steuart (2010) define computer forensics as "The process of applying scientific methods to collect and analyze data and information that can be used as evidence." Thus, computer forensics addresses the methods and procedures necessary to investigate possible criminal and non-criminal conduct involving digital data.

From an organizational perspective, investigations should initially proceed with the assumption that the case may be of a criminal nature so that all steps meet the statutory rules for admission of evidence. An understanding of computer forensics allows the accountant to make knowledgeable decisions regarding what steps to take and how to proceed during an investigation and not taint the evidence. Computer forensics is considered by some to be dominated by IT and law-enforcement. Although both play important roles, accountants can also be a vital forensic resource. Accountants, in particularly auditors, are highly familiar with corporate information systems (IS), policies and internal controls, and often possess advanced analytical skills. They possess a broad understanding of the overall systems and databases, access rights, organizational roles and responsibilities which are critical to an effective forensic investigation. They are in a position to recognize the normal routines of organizational agents and to recognize suspicious and unusual activities. IT specialists are primarily concerned with establishing defenses against external attacks and in maintaining and securing the internal environment through authorizations and access rights. Regardless of technical knowledge, organizational agents who inspect digital evidence must be forensically trained or they could taint evidence by opening and inspecting suspect files without first creating a mirror image and following chain-of evidence procedures.

Alao and Odum (2019) stated that in the case of financial statement fraud, entries probably exist as electronic journal entries, login records found in log files, and electronic correspondence between involved individuals. In recent years, auditors find themselves increasingly involved in evidence collection through computer forensics. As it pertains to fraud detection, computer forensics is the process of imaging data for safekeeping and then searching cloned copies for evidence (Gavish, 2007; Dixon, 2005). Perhaps the most common example is seizing the computer of a suspect for analysis. In gaining access to or auditing the data on a digital device, computer forensics can also involve white hat (legal) hacking, password and encryption cracking, key logging, digital surveillance, and intrusion detection (Alao & Odum, 2019). There is even a call for stronger computerized forensic investigation skills in those who perform these audits. This has been collaborated by (Kearns, 2010), who stated that accountants, when properly trained, can provide another forensic asset through a combination of accounting and computer forensics skills that provide a special capability to investigate, analyze and report on suspicious patterns and anomalies and to follow the trail of unauthorized activities.

2.1.7 Computerized/Digital Forensics

Digital Forensics (DF) is roughly forty years old. What we now consider forensic techniques were developed primarily for data recovery. For example, Wood et al. (1987) relate a story about two local data recovery experts working for 70 hours to recover the only copy of a highly fragmented database file inadvertently erased by a careless researcher. By the late 1980s utilities were being widely advertised that could perform a variety of data recovering, including "Unformat, Undelete, Diagnose and Remedy" (Display ad 57, 1987 p.57).These early days were marked by Hardware, software, and application diversity (Garfinkel, 2010), A proliferation of data files formats, many of which were poorly documented. Heavy reliance on time-sharing and centralized computing facilities; rarely was there significant storage in the home of either users or perpetrators that required analysis. In these early days forensics was largely performed by computer professionals who worked with law enforcement on an ad hoc, case-by-case basis. Astronomer Cliff Stoll's foray into network forensics was one of the most celebrated examples of the time (Stoll, 1988, 1990). In all of the above cases, the ability to identify and reconstruct the sequence of events that led to each incident is critical to the success of effective response and recovery measures:

In the first kind of incident, the system administrators of the organization need to determine the identity of the insiders and the underlying causes for the violation. It might even be the case that the insiders had no malicious intentions, but that the original policy had been set ''too tight''. For the second kind of incident, the digital investigators and the prosecution need to reliably attribute the digital crime to a particular suspect. In the third kind of incident, the administrators need to identify the attack vector of the hacker (how did the break-in occur?), to secure their systems against any future attacks that use similar techniques. Fraud occurs because of issues such as, weak internal controls, weak enforcement, and weaknesses in the field of law enforcement, low corporate governance, inadequate accounting standards and others consistent with the level of corruption and weaknesses in the administration of the country.

In Nigeria, cases of fraud that often occur is called cybercrime, or commonly known as white-collar crime. In recent times, cybercrime has increasingly increased. The handling of cybercrime cases is still quite tricky because the technology in Nigeria is quite inadequate, and the lack of knowledge of computerized techniques. Computer hacking was the most popular crime committed using the computer in the 80's. But prior to the passage of the Computer Fraud and Abuse Act of 1984, computer hacking was not even a crime, further

limiting the need to subject systems to forensic analysis. Garfinkel (2010) opined that, today much of the last decade's progress is quickly becoming irrelevant. Digital Forensics is facing a crisis. Hard-won capabilities are in jeopardy of being diminished or even lost as the result of advances and fundamental changes in the computer industry: The growing size of storage devices means that there is frequently insufficient time to create a forensic image of a subject device, or to process all of the data once it is found. The increasing prevalence of embedded flash storage and the proliferation of hardware interfaces mean that storage devices can no longer be readily removed or imaged. The proliferation of operating systems and file formats is dramatically increasing the requirements and complexity of data exploitation tools and the cost of tool development. Whereas cases were previously limited to the analysis of a single device, increasingly cases require the analysis of multiple devices followed by the correlation of the found evidence. Pervasive encryption (Casey & Stellatos, 2008) means that even when data can be recovered, it frequently cannot be processed. Use of the "cloud" for remote processing and storage, and to split a single data structure into elements, means that frequently data or code cannot even be found. Malware that is not written to persistent storage necessitates the need for expensive RAM forensics. Legal challenges increasingly limit the scope of forensic investigations.

According to Garfinkel (2010), examiners frequently cannot obtain data in a forensically sound manner or process that data to completion once they obtain it. Evidence, especially exculpatory evidence, may be routinely missed. These problems are most obvious to examiners faced with cell phones and other mobile computing platforms. There are thousands of cell phone models in use around the world, with five major operating systems (Android, Apple, Blackberry, Windows Mobile, and Symbian), more than a dozen "proprietary" systems, and more than 100,000 downloadable applications. There are dozens of "standard" cell-phone connectors and chargers. It is vital for forensics examiners to be able to extract data from cell phones in a principled manner, as mobile phones are a primary tool of criminals and terrorists. But there is no standard way to extract information from cell phones.

The International Standard on Auditing 401 - Auditing in Computer Information Systems Environment- stated that auditing processes for both internal auditors and external auditors have been rapidly changed. Factors that prompted these changes include: the globalization of business; advances in technology; demands for value-added audits; the organizational structure of the client's computerized information systems (CIS) activities; the extent of concentration or distribution of computer processing throughout the organization; particularly

as they may affect segregation of duties; and the availability of data source documents. Some computer files and other evidential matter that may be required by the auditor may exist for only a short period or only in machine-readable form. Accordingly, the auditor should have sufficient knowledge of the CIS to plan, direct, supervise and review the work performed. The auditor should also consider whether specialized CIS skills are needed in an audit. Most importantly, the forensic auditor should have access to a computer, familiarity with an operating system- windows, linux, mac etc.

2.1.8 Forensic Investigation Tools

Al Awadhi, Read, Marrington and Franqueira (2015) opined that forensic tools can take some of the work from the human element but still there is a need to better understand how to allocate and manage person-hours so that investigations can be concluded within reasonable time and reliable findings. According to Laubscher, Rabe, Olivier, Eloff and Venter (2005), it should also not matter who completes the examination of media, which tools are used and which methods employed - the same results should always be obtained. According to Cook and Clements (2009) there are numerous computerized fraud detection tools, some of which were developed specifically for fraud auditing, such as Forensic and Case Management, and many multi-purpose tools that can be utilized in uncovering fraud. We have become concerned about the lack of use of the best tools available to fraud auditors, whether they are external auditors, internal auditors, accounting managers, or forensic specialists.

Forensic tools are intended for use in investigations such that the findings will have application in a court of law, which includes the ability to demonstrate that electronic evidence has not been accidentally altered or intentionally tampered with. Typical capabilities of forensic tools include examining Windows, Unix, and Linux file systems; previewing all files including deleted or hidden files, without altering the data on the disk, including file metadata; creating bit stream copies of disks and packaging the bit stream for transfer to other media, such as CDs or DVDs; aiding in the recovery of deleted, lost, and formatted data from hard drives, diskettes, ZIP discs, USB hard drives, and other removable devices; and using a hash comparison to find known illegal files or identify known good files (Cook & Clements, 2009).

2.1.8.1 Key Logging Tools: Key loggers record every keystroke and mouse action performed by the user of the computer on which these tools are activated. Examples of key logger software are: KeyCapture, Powered Keylogger, Handy Keylogger, Stealth Keylogger and

Perfect Keylogger. The emphasis is on the key logger as primary source for evidence collection and the other tools (CCTV camera and audit logs) as secondary sources (Laubscher et al, 2005).

2.1.8.2 Audit Logs: The general notion of an audit log is appealing for use in an assessment environment. In practice, however, an audit log may be difficult to handle, owing to the volume of data and analysis effort required (Laubscher et al, 2005).To overcome this problem, Laubscher et al (2005), suggest that a backup of the audit log is made and then cleared before the computer-based programming assessment commences. Only transactions within the specific computer based programming assessment time-slot should be recorded for forensic investigation purposes.

The utilization of tools for evidence collection and analysis (crosschecking), i.e., key logger, CCTV camera, audit log and report of logins, facilitates the identification of any party that contravenes assessment regulations. In their study, Cook and Clements (2009) opined that the most commonly used tools are MS Word and MS Excel, MS Access, MSVisio, ACL and Crystal Reports etc. However, in a bid to answer the question of "Which tool is the best?" they observed that, in attempting to generalize an answer, they realized that the answer to the question depends upon the purpose and goals of the audit. Therefore, they recommend computerized tools for each of the three phases and conclude with recommendations that differ based upon the type of fraud auditor.

2.1.9 Forensic Investigation Techniques

Banarescu (2015) observed that successful implementation of an antifraud analytical system highly depends on the manner of retrieving data from a variety of sources, considering that most of them have different formats. It is recommended that the data collected should be interpreted in the same way, using the same techniques and the same methodology, so that creation of data bases to be homogeneous. In the view of Garfinkel (2010) digital forensics research needs to become dramatically more efficient, better coordinated, and better funded if investigators are to retain significant DF capabilities in the coming decade. It is not just the content of emails, documents and other files which may be of interest to investigators but also the 'metadata' associated with those files. A computer forensic examination may reveal when a document first appeared on a computer, when it was last edited, when it was last saved or printed and which user carried out these actions (Oyedokun, 2015).

Although a system of fraud prevention and detection could be expensive, the low degree of response to fraud and the inability to recover losses resulting from internal fraud or abuse could have multiple consequences, difficult to quantify. The actual fraud prevention and detection mechanism combines both human and technical factors (Banarescu, 2015). The lack of standardized abstractions and standardized data formats slows progress by forcing researchers to implement more parts of a system before they can produce initial results. Researchers are forced to spend more time acquiring and preparing data. It is harder to compare research products. And most importantly, the lack of interchange formats limits the ability to create tools that can inter-operate (Garfinkel, 2010). Investigators use a variety of techniques and proprietary forensic applications to examine the copy they have made of a compromised device. They search hidden folders and unallocated disk space for copies of deleted, encrypted or damaged files. Any evidence found on the digital copy is carefully documented in a finding report and verified with the original device in preparation for legal proceedings that involve discovery, depositions or actual litigation (Lutkevich, 2021). Computer forensic investigations use a combination of techniques and expert knowledge. Some common techniques include the following:

2.1.9.1 Cross-drive analysis: This is the forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection (Garfinkel, 2006). Events that raise suspicion are compared with information on other drives to look for similarities and provide context. This is also known as anomaly detection.

2.1.9.2 Live analysis: The examination of computers from within the operating system using custom forensics or existing sys-admin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

2.1.9.3 Deleted files: A common technique used in computer forensics is the recovery of deleted files. Modern forensic software has their own tools for recovering or carving out deleted data, Aaron et al, (2009). Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. This is sometimes known as file carving or data carving. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

2.1.9.4 Stochastic forensics: This method uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft. In the view of Garfinkel (2010) yet another model for forensic processing is to sample and process randomly chosen sections of the drive. This approach has the advantage of potentially being very fast, but has the disadvantage that small pieces of trace data may be missed.

2.1.9.5 Steganography: One of the techniques used to hide data is via steganography; this is the process of hiding data inside of a picture or digital image. Computer forensics professionals can reverse a steganography attempt by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes (Dunbar, 2001). If a cybercriminal hides important information, for example Child pornographic image or other information that a given criminal does not want to have discovered inside an image or other digital file, it may look the same before and after to the untrained eye, but the underlying hash or string of data that represents the image will change.

According to Bressler (2012), perhaps the most successful fraud investigation would be when the forensic accountant's existing skill set is matched with the nature and operation of the fraud examination under investigation. It would be interesting to note that (1) the perceptions of attorneys and judges in the court system as to the importance of forensic investigators' knowledge of AIS; (2) the ability to explain when testifying on fraud cases; (3) whether such testimony might be more convincing with a good background; and (4) understanding of the AIS systems for which the fraud has been perpetuated.

2.1.10 Fraud Litigation Practice

Fraud litigation practice in civil litigation allegations of fraud might be based on a misrepresentation of facts that was either intentional or negligent.

Lawsuits can encompass a number of legal issues and claims from civil litigation to commercial litigation dated claims including, for example: misrepresentation, fraudulent inducement omission and non-disclosure fraudulent concealment. With criminals consistently using technology and other sources to construct new ways of defrauding individuals and companies, professional accountant should have the required skills and a greater knowledge of computer tools and techniques to avoid and detect anomalies

2.2 Theoretical Review

This study is anchored on the fraud diamond theory because, with adequate computerized forensic tools and techniques which involve adequate computer skills, surveillance and careful consideration of complicated financial records, there will be enhanced systemized fraud detection mechanism.

2.2.1 White Collar Crime Theory

This basic theory as upheld in this research work was propounded by Sutherland (1949) as cited in Michael (2004). The term white-collar crime dates back to 1939. Sutherland (1949) as cited in Michael (2004) was the first to coin the term, and hypothesis white-collar criminals, attributed different characteristics and motives than typical street criminals. Sutherland originally presented his theory in an address to the American Sociological Society in attempt to study two field, crime and high society which had no previous empirical correlation. He defined his idea as "crime committed by a person of respectability and high social status in the course of his occupation (Sutherland 1949, cited in Michael 2004). Sutherland noted that in his time, less than two (2) percent of the persons committed to prison in a year belong to the upper class." His goal was to prove a relation between money, social status, and likelihood of going to jail for a white-collar crime, compared to more visible, typical crimes, although, the percentage is a bit higher today.

Much of Sutherlands work was, "to separate and define the difference in blue collar street crimes, such as arson, burglary, theft, assault, rape and vandalism which are often blamed on psychological, associational and structural factors" (Adebisi & Gbegi, 2012). Instead, white-collar criminals are opportunists, who over time learn they can take advantage of their circumstances to accumulate financial gain. They are educated, intelligent, affluent, individuals who are qualified enough to get a job which allows them the unmonitored access to often large sum of money. Thus, we could gather that the most economically disadvantaged members of society are not the only ones committing crime. Members of the privileged socioeconomic class are also engaged in criminal behavior. In the view of Gottschalk (2011), if white-collar crime is defined in terms of its two perspectives of off against public for personal or organizational gain, which is committed by non-physical means and by concealment or deception. It is deceitful, it is intentional, it breaches trust, and it involves losses. White-collar criminals are individuals who are wealthy, highly educated, and socially connected, and they are typically employed by and in legitimate organization. They are persons of respectability and high social status who commit crime in the course of their

occupation. It is estimated that a great deal of white-collar crimes is undetected or if detected, it is not reported. Because of the high status of the perpetrators of these crimes, a highly trained and experienced examiner or investigator like the Forensic Auditor is needed to forestall the occurrence of such high profile fraud (Okoye & Obialor, 2020).

2.2.2 Fraud Diamond Theory

Wolf and Hermanson (2004) introduced the fraud diamond model where they presented another view of the factors to fraud. The model adds fourth variable ―capabilities, to the three factor theory of fraud triangle. According to Wolf and Hermanson (2004), Crumbley, Heitger and Smith (2007), perpetrator of fraud must have the necessary traits, abilities, or positional authority to pull off his crime. In other words, the potential perpetrator must have the skills and ability to commit fraud. Nwosu (2015) stated that the diamond theory of fraud explains an individual's capability, personality traits and abilities to contribute a major role in determining whether fraud may occur. However, Nwosu (2015) further observed that while opportunities can open the doorways to fraud, incentive and rationalization will attract people to it, but such an individual must have the capability to recognize the open doorway as an opportunity and should be able to take an undue advantage of the identified loopholes. For example, if someone does not understand how to make journal or ledger entries in the books of accounts, they would not know how to manipulate numbers no matter what the incentive or opportunity is (Rasey, 2009).

Wolfe and Hermanson (2004) in their study stated that a successful fraudster must also lie effectively and consistently. To avoid detection, the fraudster must look at the auditors, investors, and others right in the eye and convincingly tell them lies. Thus, the fraudster should also possess the skill to keep track of the lies, so that the overall story remains consistent. In the fraud case of Phai-Mor, the auditors claimed that Phar-Mor had formed a team of fraudsters made-up of executives and former auditors whose function is to ensure they are working continuously to hide evidence of frauds. Based on deceptive data and inventory, Phar-Mor borrowed millions, basically to finance its unusual rapid growth. In actuality, this cash infusion was made to in necessity to pay off suppliers. Wolf and Hermanson (2004) believed many frauds would not have occurred without the right person with right capabilities implementing the details of the fraud.

2.3 Empirical Review

Okoye and Gbegi (2013) investigated Forensic Accounting: A Tool for Fraud Detection and Prevention in the Public Sector. Their study was conducted with reference to Ministries in Kogi State. The study made use of survey design. The data was obtained from both primary and secondary sources. A total of 370 questionnaires were administered to staff of five (5) selected ministries in the State with 350 copies properly filled and returned. Also personal interviews were conducted with those ministries. The statistical tool used to test hypotheses was Analysis Of Variance (ANOVA). It was discovered from the research that the use of Forensic Accounting will significantly reduce the occurrence of fraud cases in the public sector and the use of Forensic Accountants can help better in detecting and preventing fraud cases in the public sector organizations.

Okoye and Obialor (2020) studied Forensic Investigation and Forensic Audit Methodology: Remedy to Fraudulent Practices in a Computerized Work Environment. The object of the study was 334 accountants' and auditors in 3 Federal ministries in Anambra State. A descriptive survey research design was used for the study while the data analysis techniques adopted for the study consisted of Mean and standard derivation for research questions and Analysis of Variance (ANOVA). The reliability of the instrument was ascertained using Pearson Product Moment Correlation Co-efficient. From the findings of the study, it was revealed that forensic auditors are used for detecting and preventing fraudulent practices in selected federal ministries in Anambra State.

On the study carried out by Tjeng and Nopianti (2020) on The Audit Investigation and Accounting Forensic in Detecting Fraud in Digital Environment. Their study was conducted with reference to Indonesia. The research design used was extant literature. The Researchers conducted a library study by collecting several economic journals and books relating to the problem under study such as the number of fraud cases contained in the digital environment, and then the cases are analyzed in more detail by doing computer forensics. The results of this study indicate that forensic accounting in detecting fraud in the digital environment can be done by computer forensic and investigations that must be done by making copies of the entire log data, making fingerprints from numerical data, making fingerprints from copies, making master list hashes and documenting data that has been done.

Kasum (2009) investigated on The Relevance of Forensic Accounting to Financial Crimes in Private and Public Sectors of Third world Economies: A Study from Nigeria. Primary data in

form of perceptions of accountants, lawyers, economists, bankers, contractors, engineers other related professionals and other knowledgeable individuals in the on Nigeria situation and the subject matter, are the data for this study. The study is a combination of library and empirical; survey is more of an exploratory study. Three hundred number (300) of the questionnaire were distributed and two hundred and sixty (264) were filled and returned as a source of primary data while Z score test of mean was computed for the first three hypotheses and Z score test of proportion was computed for the last hypothesis. From the research, it was found that investigative or forensic accountant has a role to play, generally, but more in the public sector.

Okolo, Iduma and Ani (2018) examined Computer Technique and Fraud Detection in Nigerian Banking Sector. Their study was conducted with reference to 22 Nigeria commercial banks. The objective of this study is to determine the levels at which computer technique of forensic accounting help in frauds detect in Nigerian banking Sector. Survey research design was utilized. The study employed use of primary data. This study was conducted on forensic accountants and they were selected as population. The population of the study is 71 and all was used as sample due to its small nature. The data was generated using questionnaires structured in four point scale and observation. Data analysis techniques that were adopted for this study consisted of frequency, percentages and single factor ANOVA was adopted to measure the variance in the responses. Findings from this work revealed that; the use of Computer technique of Forensic Accounting help in fraud cases detection in the Nigerian banking sector.

Eze and Okoye (2019) studied on how Forensic Accounting and Fraud Detection and Prevention in Imo State Public Sector. The research design used was the descriptive survey. The study adopted structured questionnaire for data collection after validity and reliability test with z-test for the hypothesis testing. The Population of the study comprises of four (4) ministries out of the entire ministries in Imo state and a sample size of about seventy (70) respondents which comprises auditors and accountants and top executives from the four ministries selected. The questionnaire was designed using the five point likert scale and sixty of them were administered to the four ministries while fifty questionnaires were filled and returned. Data analysis was done using the weighted mean and the Z-test statistics. The research findings showed a significant relationship between forensic accounting and fraud detection and prevention in the Public Sector.

Oyedokun (2015) examined Forensic Investigation and Forensic Audit Methodology in a Computerized Work Environment. In the paper, the researcher explored the concept of investigations, forensic investigations, forensic audit investigation methodology, forensic audit and the internal auditor, forensic in computerized work environment, and forensic investigation and audit Reporting using content analysis. The paper recommends that all would be forensic accountants/investigators, fraud/forensic auditors, statutory auditors, and investigative accountants, should be well equipped with forensic accounting techniques in obtaining admissible evidence suitable for litigation purposes.

Okunbor and Obaretin (2010) used a total of 140 statistically sampled respondents of ten companies from five sectors quoted in Nigerian Stock exchange. The research design used was the simple regression model and descriptive statistics for the purpose of data analysis. The result showed that the application of forensic accounting by quoted companies in Nigeria is not effective in curbing fraudulent activities. The general consensus was that it had not been effective as revealed by the frequency scores of those who disagreed.

In the study of Gottschalk (2011), a structured questionnaire of 517 potential respondents only 141 responses were completed and used for the analysis with the help of descriptive statistics. The results reveal that control is the most important means by which fraud is prevented and controlled. However, some respondents believe that influence is more important in terms of ethical guidelines and other measures. Singleton and Singleton (2006) laid weight on forensic accounting and fraud auditing. In the book they wrote, while they emphasized fraud auditing and basic concepts of forensic accounting, in protection from fraud they concentrated on topics such as responsibility of the auditors, red tags and fraud detection, protection from fraud and control, forensic accounting with the dimension of expert testimony.

Pamuke and Ozkul (2012), in their investigation into fraud detection and forensic accounting concluded that forensic accounting will be one of the best careers in the future and urge Companies and government around the world to make material and moral investment for this profession, in order to ensure better world economy free of fraud.

In the study of Baroto and Prasetyo (2020), a design science research methodology was used. The paper elaborated on the investigation of email using a digital forensic framework. The research examines the process of email investigation by extracting the email, indexing the

body of email, and combining digital forensic framework on fraud investigations the result revealed that digital forensics help investigator to analyze an email and maintain the integrity of the entire investigation process.

Madzivire, Nyamwanza, Mushonga, Takachicha, and Mulonda (2020) investigated the effectiveness of forensic audit as a tool for fraud detection and prevention. The study used a total of 20 questionnaires and a mixed approach whereby Quantitative and Qualitative data was gathered from open ended questions and 3 interviews were also conducted. The research design used was the multiple regression method. The research revealed that there is a positive relationship between training, level of education and ability to detect and prevent fraud. It was also found that litigation support service has a huge role to play in the effectiveness of forensic auditing in detecting and preventing fraud.

Griffiths and Pretorius (2021) examined the effect of implementing robotic process automation for auditing and fraud control. The research design was a generic study using a selection process. The research was performed by conducting a literature review that considered 22 articles (through a selection process) on the relevant research themes of robotic process automation, fraud and auditing. The findings suggest that organizations should consider robotic process automation as a means for reducing fraud opportunities in organizations. Robotic process automation may also assist organizations to advance their audit efficiency and effectiveness.

Ojukwu, Ubi, Olugbemi, Olugbemi and Emefiele (2020) examined forensic accounting and fraud detection in Nigerian universities (A study of Cross River University of Technology). The study made use of a desk survey designs. The study adopted desk survey methods in gathering relevant information which were extracted from textbooks, libraries, published and unpublished journals. The population of the study was 250 employees in the university. A structured and validated questionnaire was used to collect data from the sample. Pearson Product Moment Correlation statistical tool was adopted in this study. It was revealed that there was a significant relationship between forensic accounting and financial fraud detection, there was a significant relationship between forensic accounting and financial reporting quality and there was a significant relationship between forensic accounting and internal control.

In their study, Eiya and Otalor (2013) examined forensic accounting as a tool for fighting financial crime in Nigeria. It was observed that in Nigeria, the print and electronic media is replete with news of the charges brought against suspected persons accused of financial crime and charged to court by the anti-graft agencies being dismissed for lack of credible and sufficient evidence. Their paper highlights how forensic accounting can be employed to resolve that challenge It was recommended that the relevant anti-graft agencies should consider engaging the services of forensic accountant to enhance conviction of fraud culprits.

Okoye and Ndah (2019), researched on effect of forensic accounting and fraud prevention in manufacturing companies in Nigeria using fifty (50) structured questionnaires to the accounting staff of ten (10) manufacturing companies. The collected data was analyzed using Ordinary Least Square method of multiple regression analyses. From the findings, it was concluded that fraud investigation practices are very important for the prevention of fraud in manufacturing companies. Similarly, fraud litigation practices are an important factor in the prevention of fraud in manufacturing companies.

Adebisi, Okike and Yoko (2016) investigated how forensic accounting has aided the detection and prevention of fraud in Nigeria using the survey research method. Primary data collected was with the aid of questionnaire administered to a sample of 92 professional accountants in the Nigerian public sector analyzed using chi-square. The findings of the study suggest that forensic accounting have a significant role to play in fraud detection and prevention in Nigeria. It was therefore recommended that there should be more forensic accountants' involvement in fraud detection in order to reduce the rate of financial crime in Nigeria.

Olukowade and Balogun (2016) examined the relevance of forensic accounting in the detection and prevention of fraud in Nigeria. The study was a theoretical research. The research found out amongst others that their services will assist audit committee members in carrying out their oversight functions by providing them assurance on internal audit report. Also, laws should be up to date with latest advancement in technology to ensure admissibility of evidence in a law court for successful prosecution of criminal and civil cases. The study recommended that government should ameliorate the cost of hiring the services of forensic accountants and to treat culprits equally without any favoritism.

Veerankutty, Ramayah and Ali (2018) studied the effect of information technology governance on audit technology performance among Malaysian public sector auditors. A

multistage method of data collection was conducted, whereby a total of 1518 questionnaires were emailed and personally administered. Surveys using closed-ended questionnaires were distributed to approximately 309 Malaysia public sector auditors. From their investigation the results show that IT governance mechanisms such as IT strategy and management support significantly influence the audit technology performance. IT governance does play a significant role in assuring the successful utilization of audit technology.

Alao and Odum (2019) investigated fighting fraud in Nigeria banking industry an examination of the impact of forensic auditing. The study was made using survey research design with a sample size of 153 respondents from various categories of staff from ten commercial banks and four audit firms in Nigeria. The primary source data was adopted using questionnaires, personal interviews, and document review. The collected data were analyzed using application of non-parametric statistical test and using Chi-square statistical software, OLS regression analysis. It was found that the forensic auditing departments suffer from multiple challenges, among them being the lack of material resources, technical know-how, interference from management, and unclear recognition of the profession.

Gardi (2018) evaluated the effects of computerized accounting system on auditing process: A case study from Northern Iraq. The study made use of a case study design with sample size of 35 employees at the Zanko bank. Primary data was collected using Questionnaires, personal interviews. The study used correlation coefficient tests and descriptive statistics paired sample T- tests. The result revealed that audit effectiveness has a significant impact on the auditing process and that audit efficiency, significant and other computerized accounting software (CAS) problems do not have significant impacts on the auditing process.

Banarescu (2015) studied on the detecting and preventing fraud with data analytics. The study provides an overview of the way in which technology can be implemented to improve fraud prevention and detection, inside of a public or private economic entity. The study revealed that the processes of data analysis as a tool for preventing and detecting fraud can be used successfully in any field, mainly in those of the database and the data are or may be easily converted into electronic format.

In the study of Bressler (2012) on forensic investigation: the importance of accounting information systems. The study described the role of forensic accountants and why they testify as expert witnesses, transforming financial investigation to forensic investigation and

how forensic accountants transform financial investigation to forensic investigation based on their required forensic accounting qualifications.

Garfinkel (2010) evaluated digital forensics research: the next 10 years. The research design is based on evidence-oriented design. The findings summarizes current forensic research directions and argues that to move forward the community needs to adopt standardized, modular approaches for data representation and forensic processing. The study proposes a plan for achieving that dramatic improvement in research and operational efficiency through the adoption of systematic approaches for representing forensic data and performing forensic computation. It draws on more than 15 years personal experience in computer forensics, an extensive review of the DF research literature, and dozens of discussions with practitioners in government, industry, and the international forensics community.

Nwosu (2015) studied forensic auditing and financial accounting in Nigeria; an assessment. The Survey design was used in the study with a sample size of 143 respondents, consisting of accountants, management staffs, practicing auditors among others was used. Primary data was used in the paper. The data was generated using well-structured likert scale questionnaire. Simple random technique was utilized in selecting the sample size, while the binomial test was employed in the data analysis. The findings of the paper showed that there is significant agreement amongst stakeholders on the effectiveness of forensic auditing in fraud control, financial reporting and internal control quality.

3. MATERIAL AND METHOD

The study utilized descriptive survey research design. Using this design to examine the contribution of computerized forensic investigation towards fraud detection in Nigerian public sector allowed the researcher deploy a sample representative from which primary data was obtained via a survey instrument.

The population of the study comprised all the 612 professional accountants affiliated to the Institute of Chartered Accountants of Nigeria (ICAN) and Association of National Accountants of Nigeria (ANAN) that are practicing in Anambra State (ICAN 257 respondents and ANAN 355 respondents) However, the Purposive sampling technique was deployed to maximise the Taro Yamane (1967) formula for determining the sample size of finite population. Thus, a total of two hundred and forty-two (242) professional Accountants who are mainly Audit and Bursary staff, Internal and External auditors, top management staff,

and forensic auditors in the public sector of Anambra State were sampled. This was to equally ensure that the senior professional accountants and experienced forensic accountants in the public sector of Anambra State participated in the study.

To this end, a 5-point Likert-scale questionnaire was structured and utilised for collation of primary data / responses of the sampled respondents. These were analysed using inferential regression analysis

4. RESULT AND DISCUSSION

4.1 Descriptive Analysis of Data

The responses used in measuring the four variables of the study were averages and their descriptive statistical analyses are shown in Table 1.

Table 1 Descriptive Statistical Analysis of Variables

Variable	Obs	Mean	Std. Dev.	Min	Max
FAP	242	3.5	.7954748	1	5
FLP	242	3.4	.8952645	1	5
CFA	242	3.4	.8859464	1	5
FD	242	3.6	.9233881	1	5

Source: Stata 14.2 Output (2023)

In line with the descriptive analysis presented in Table 1, Forensic Accounting Practices (FAP) averaged 3.5 with a standard deviation of .7954748. This suggests that on average, the respondents' perception was that that FAP helps in detecting fraud. With the same average value of 3.4, the respondents equally opined that Fraud Litigation Practice (FLP) and Computerized Forensic Accounting Techniques (CFA) aid in fraud detection. However, this descriptive analysis is not sufficient to infer that Forensic Accounting Practices, Fraud Litigation Practice and Computerized Forensic Accounting Techniques are significantly related to fraud detection, hence the need for hypothesis testing.

4.2 Test of Hypotheses

The study seeks to provide answers to three research questions by the use of Ordinal Probit Regression technique. The ordinal regression model is used to predict a categorical dependent variable with multiple categories, ordered in a meaningful way. The model estimates the probabilities of a given observation belonging to each category. The result of the Ordinal Probit Regression is provided in Table 4.4.

Table 2 Ordered probit regression

Ordered probit regression Number of obs = 242
LR chi2(3) = 57.21
Prob > chi2 = 0.0000
Log likelihood = -288.75559 Pseudo R2 = 0.0901

FD	Coef.	Std. Err.	z	P>|z|	[95% Conf.	Interval]
FAP	.4338923	.1704714	2.55	0.011	.0997744	.7680101
FLP	-.0302132	.1344984	-0.22	0.822	-.2938252	.2333989
CFA	.308911	.1203446	2.57	0.010	.0730399	.5447821
/cut1	-.3833821	.4207103			-1.207959	.4411949
/cut2	1.057922	.3358761			.399617	1.716227
/cut3	2.361928	.3479154			1.680026	3.043829
/cut4	3.491949	.3710229			2.764758	4.219141

Source: Stata 14.2 Output (2023)

The output in Table 2 is an ordered probit regression, which is used to model an ordinal dependent variable (that is, a variable with a limited number of ordered categories). The number of observations used in the analysis is 242. The LR chi-squared statistic is 57.21, and its associated p-value is 0.0000, which is less than 0.05. This indicates that there is strong evidence to reject the null hypothesis that the model does not fit the data well. The log-likelihood value of the model is -288.75559, and

the pseudo R-squared value is 0.0901, which suggests that the model explains a small but non-trivial proportion of the variation in the dependent variable. The coefficients table shows the estimated coefficients (Coef.), their standard errors (Std. Err.), the associated z-statistics, and the corresponding p-values (P>|z|) for the independent variables "Forensic Accounting Practice" (FAP), "Fraud Litigation Practice" (FLP), and "Computerized Forensic Accounting" (CFA). The confidence intervals for the coefficients are also provided.

To test whether each of the independent variables significantly affects the dependent variable, the researcher used the p-values associated with the z-statistics for each independent variable. A small p-value (typically less than 0.05) indicates that there is strong evidence to reject the null hypothesis that the corresponding independent variable has no effect on the dependent variable.

4.2.1 Hypothesis One

H_o: Forensic accounting practice does not significantly relate to fraud detection in the Nigerian public sector.

The coefficient for Forensic Accounting Practice (FAP) is 0.4339, and its p-value is 0.011 which is less than 0.05. This suggests that there is strong evidence to reject the null hypothesis. Thus, an increase in FAP by a margin significantly increases the chances of fraud detection by 0.4339. The research concluded that Forensic accounting practice significantly and positively related to fraud detection in the Nigeria public sector ($\beta = 0.4339$, p-value = 0.011).

This finding also highlights the importance of forensic accounting in detecting fraud. Forensic accounting is a specialized field that involves the application of accounting and investigative skills to identify and prevent fraud. Forensic accountants use a variety of tools and techniques to analyze financial data and detect fraudulent activities, including analyzing trends and patterns in financial transactions, reviewing internal controls, and conducting interviews with employees. The positive relationship between forensic accounting practice and fraud detection suggested that organizations in the Nigerian public sector that invest in forensic accounting are likely to have

higher levels of fraud detection compared to those that do not. This is because forensic accountants are equipped with the knowledge and skills necessary to identify and prevent fraud, which can improve the efficiency and accuracy of fraud detection efforts. Alhassan (2021); Ojukwu, Ubi, Olugbemi, Olugbemi and Emefiele (2020); Okoye and Obialor (2020); Baroto, and Prasetyo (2020) and Okoye and Gbegi (2013) found similar result.

4.2.2 Hypothesis Two

H_o: There is no significant relationship between fraud litigation practice and fraud detection in the Nigerian Public sector.

The coefficient for Fraud Litigation Practice (FLP) is -0.0302, and its p-value is 0.822, which is greater than 0.05. This suggests that there is not enough evidence to reject the null hypothesis that this independent variable has no effect on the dependent variable. Thus, an increase in FLP by a margin does not significantly affect the chances of fraud detection. The researcher concluded that there was no significant relationship between fraud litigation practice and fraud detection in the Nigerian Public sector (β = -0.0302, p-value = 0.822).

Asmuch as fraud litigation may be important for holding individuals accountable for their actions, it may not be as effective as other approaches such as forensic accounting, in detecting fraud. The forensic evidences obtained are usually not admissible evidence suitable for litigation purposes; in most cases it is difficult to prove the obtained evidences in the court of law without the necessary authorizations. This was in negation to the findings realized by Eze and Okoye (2019); Okoye and Ndah (2019); Olukowade and Balogun (2016).

4.2.3 Hypothesis Three

H_o: Computerized forensic accounting techniques do not significantly aid fraud detection in the Nigerian Public sector.

The coefficient for Computerized Forensic Accounting (CFA) is 0.3089, and its p-value is 0.010, which is also less than 0.05. Hence, there is strong evidence to reject the null hypothesis. Thus, an increase in CFA by a margin significantly increases the

chances of fraud detection by 0.3089. The researcher concluded that Computerized forensic accounting techniques significantly aided in fraud detection in the Nigerian Public sector (β = 0.3089, *p*-value = 0.010).

This finding also highlights the potential benefits of utilizing technology in fraud detection. Computerized techniques, such as data analytics and artificial intelligence, can automate and streamline the process of fraud detection, making it faster and more accurate. By utilizing these techniques, organizations in the Nigerian public sector can improve the efficiency of their fraud detection efforts and increase their chances of identifying and preventing fraud. This finding is in support of the results found by Griffiths and Pretorious (2021); Tjeng and Nopianti (2020); Baroto and Prasetyo (2020); Okolo, Iduma and Ani (2018); Whyte (2018); Adebisi, Okike and Yoko (2016) and Banarescu (2015).

CONCLUSION AND RECOMMENDATIONS

Computerized forensic accounting techniques can significantly aid in the detection of fraud in the Nigerian public sector. These techniques leverage technology to automate and streamline the process of fraud detection. This helps to identify unusual patterns and transactions that may indicate fraudulent activity more efficiently and accurately than manual methods. The use of computerized techniques also helps to reduce the risk of human error, ensuring that fraud detection efforts are consistent and reliable. Additionally, computerized forensic accounting techniques can help to reduce the time and resources required for fraud detection, making it more cost-effective for organizations in the Nigerian public sector. By utilizing computerized forensic accounting techniques, organizations in the sector can enhance their overall fraud detection efforts and improve their ability to prevent fraudulent activities from occurring. Overall, the use of computerized forensic accounting techniques is a key tool in improving fraud detection in the Nigerian public sector.

The findings of the study highlighted the importance of forensic accounting in detecting fraud in the Nigerian public sector. The positive relationship between forensic accounting practice and fraud detection suggests that organizations in the sector that invest in forensic accounting are likely to have higher levels of fraud

detection. The finding that computerized forensic accounting techniques significantly aided in fraud detection highlights the potential benefits of utilizing technology in fraud detection. On the other hand, the limited relationship between fraud litigation practice and fraud detection suggests that the use of fraud litigation as a means of detecting fraud may be limited in the Nigerian public sector.

Based on the findings discussed above, the following recommendations can be made to improve fraud detection in the Nigerian public sector:

1. The Nigeria public sector should invest in the development and implementation of forensic accounting practices. This can be done by hiring qualified forensic accountants, providing training and education on forensic accounting techniques, and implementing systems and procedures to support forensic accounting efforts.
2. Organizations in the Nigerian public sector should consider utilizing computerized techniques, such as data analytics and artificial intelligence, to support their fraud detection efforts. These techniques can automate and streamline the process of fraud detection, making it faster and more accurate.
3. Instead of engaging in fraud litigation, Nigerian public sector should implement strong internal controls to prevent fraud from occurring. This can include implementing policies and procedures to monitor and manage financial transactions, conducting regular audits, and establishing a system for reporting and investigating suspected fraud.

REFERENCES

Abu-Musa, A.A. (2008). Information Technology and Its Implications for Internal Auditing: An Empirical Study on Saudi Organizations, *Managerial Auditing Journal, 23(5)*, 434-466, Retrieved (4/11/2021) from: *https://ideas.repec.org/a/eme/majpps/v23y2008i5p438-466.html*

*A*ssociation of Certified Fraud Examiners (2018). Global Study on Occupational Fraud and Abuse Report to the Nation's *10 (80), Manual*.

Association of Certified Fraud Examiners (2019). Retrieved (4/11/2021) from: *https://www.acfe.com/rttn2016/images/fraud-tree.jpg*

Adebisi, J.F., Okike, B.M. and Yoko, V.E. (2016). The Impact of Forensic Accounting in Fraud Detection and Prevention: Evidence From Nigerian Public Sector, *International Journal of Business Marketing and Management, 1(5)*,34-41, Retrieved (24/10/2021) from: *www.ijbmm.com*

Ademu, I. O. and Imafidon, C. O. (2012). The Influence of Security Threats and Vulnerability on Digital Forensic Investigation, *International Journal of Computer Application, 6 (2)*,1 -6, December, Retrieved (31/10/2021) from: *http://www.rspublication .com/ijca/*

American Institute of Certified Public Accountants (AICPA). Certified in Financial Forensics. Available at: http://fvs.aicpa.org/Memberships/Overview...

Al Awadhi I., Read, J.C., Marrington A. and Franqueira V.N.L. (2015). Factors Influencing Digital Forensic Investigations: Empirical Evaluation of 12 Years of Dubai Police Cases, *Journal of Digital Forensics, Security and Law: 10 (4), Article 1, DOI: https://doi.org/10.15394/jdfsl.2015.1207, Available at: https://commons.erau.edu/jdfsl/vol10/iss4/1*

Alao, B. B. and Odum, A.N. (2019). Fighting Fraud in Nigeria Banking Industry: An Examination of The Impact of Forensic Auditing, *International Journal of Academic Multidisciplinary Research,3 (12),* 22-32, Retrieved (23/10/2021) from: *www.ijeais.org/ijamr*

Albrecht, W.S., Albrecht C., and Albrecht C. (2006). *Fraud Examination & Prevention*. Mason, OH: Thomson Southwestern.

Alhassan, I. (2021). Forensic Accounting and Fraud Detection and Prevention in the Nigerian Public Sector, *International Journal of Empirical Finance and Management Sciences,3(1)*, Retrieved (3/10/2021) from*: https://www.researchgate.net/publication/352374388*

Alhusban, A. A. A., Haloush, H. A., Alshurafat, H., Al-Msiedeen, J. M., Massadeh, A. A. M., and Alhmoud, R. J. (2020). The Regulatory Structure and Governance of Forensic

Accountancy in the Emerging Market: Challenges and Opportunities. *Journal of Governance & Regulation, 9(4),* 149-161, Retrieved (31/10/2021) from: https://doi.org/10.22495/jgrv9i4art13

Banarescu, A. (2015). Detecting and Preventing Fraud with Data Analytics, *Procedia Economics and Finance 32*, 1827 – 1836, Retrieved (30/10/2021) from: https://sciencedirect.com/science/article/pii/S2212567115014859

Baroto, W. A. and Prasetyo, A. H. (2020). Digital Forensic Process in Fraud Investigation: A Case Study on Email Analysis, *International Journal of Scientific Engineering and Science, 4 (9),* 36-40, Retrieved (24/10/2021) from: http://ijses.com/wp-content/uploads/2020/09/16-IJES-V4N9.pdf

Bhasin, M. (2007). Forensic Accounting: A new paradigm for Niche Consulting, *The Chartered Accountant, 1000-1010.*

Bressler, L. (2012). Forensic Investigation: The Importance of Accounting Information Systems, *International Journal of Business, Accounting, and Finance, 5(1),* 67-77, Winter, Retrieved (30/10/2021) from: *www. Sematicscholar.org*

Chigozie-Okwum, C. C., Michael, D. O. and Ugboaja, S.G. (2017). Computer Forensics Investigation, Implications for Improved Cyber Security in Nigeria, *International Journal of Science and Technology,6(1),13,* 59-73, February, Retrieved (4/11/2021) from*: https://www.ajol.info/index.php*

Coenen, T.L. (2005). Forensic Accounting, a new twist on bean counting, Tracy@sequence-inc.com. Retrieved (30/10/2022) from: https://*www.wislawjournal.com*

Cook, G. J. and Clements, L. H. (2009). Computer-based Proactive Fraud Auditing Tools, *Journal of Forensic & Investigative Accounting, 1(2)* 10- 12, Retrieved (23/10/2021) from: https://web.nacva.com/JFIA/Issues/JFIA-2009-2_10

Creswell, J. W. (2012). *Educational Research: Planning, Conducting, and Evaluating Quantitative.* Prentice Hall.

Crumbley D.L., Heitger L.E., and Smith G.S. (2007). *Forensic and Investigative Accounting*, (3rd ed), Chicago: CCH.

Davis, C., Schiller, M. and Wheeler, K. (2007). IT Auditing. New York, NY: McGraw-Hill.

Dixon, P. D. (2005). An overview of computer forensics. IEEE Potentials, 24(5), 710.

Eiya, O. and Otalor J. I., (2013). Forensic Accounting as a Tool for Fighting Financial Crime in Nigeria, *Research Journal of Finance and Accounting, 4 (6),*Retrieved (24/10/2021) from: www.iiste.org

Eze, E. and Okoye, E.I., (2019). Forensic Accounting and Fraud Detection and Prevention in Imo State Public Sector, *Accounting and Tax Review, 3 (1)*, 12-26, Retrieved (30/10/2021) from: *https://www.atreview.org*

Gardi, B.J.K. (2018). The Effects of Computerized Accounting System on Auditing Process: A Case Study from Northern Iraq, Retrieved (30/10/2021) from: *https://ssrn.com/ abstract=3838327*

Garfinkel S. L. (2006). Forensic feature extraction and cross-drive analysis. In: Proceedings of the 6th annual digital forensic research workshop (DFRWS). Lafayette, Indiana: Elsevier, *http://www.dfrws.org/2006/proceedings/10-Garfinkel.pdf;*

Garfinkel, S.L. (2010). Digital Forensics- The Next 10 years, *Digital investigation 7,(3), S*, 64 - 73, Retrieved (31/10/2021) from: *https://www.researchgate.net*

Gavish, A. (2007). The Hidden Costs of Computer Misconduct. Security

Gbegi, D.O. and Habila, E. (2007). Effect of Forensic Accounting Evidence on Litigation Services in The Nigerian Judicial System, *Nigerian Journal of Management Sciences 6(1)*,104 -113 Retrieved (23/10/2021) from: *https://www.bsum.edu.ng/njms/pdf/vol6No213.pdf*

Gottschalk, P. (2011). Prevention of white collar crime: The role of accounting. *Journal of Forensic and Investigative Accounting*, 3(1), 23-48. Retrieved (30/10/2022) from: *https://biopen.bi.no*

Griffiths, L. and Pretorius, H. W. (2021). Implementing Robotic Process Automation for Auditing and Fraud Control, *A. Gerber and K. Hinkelmann (Eds.): Society5.0, (CCIS 1477)*, 1–11, Retrieved (24/10/2021) from: *https://doi.org/10.1007/978-3-030-86761-4_3*

Iqbal, S. and Alharbi, S.A. (2019). Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics ,Retrieved (29/10/2022) *DOI: http://dx.doi.org/10.5772/intechopen.90233www.intechopen.com*

Justenhoven, P., Sechser, J. and Loitz, D. R. (n.d.). Digitalisation in Finance and Accounting, 1-52, Retrieved (30/10/2021) from: *www.pwc.de*

Kearns, G. S. (2015). Computer Forensic Projects for Accountants, *Journal of Digital Forensics, Security and Law, 10 (3)*,1, Retrieved (24/10/2021) from: *https://commons.erau.edu/jdfsl/vol10/iss3/1*

Kasum, A. S. (2009). The Relevance of Forensic Accounting to Financial Crimes in Private and Public Sectors of Third world Economies: A Study From Nigeria, *Proceedings of the 1st International conference on Government Fraud Ethics and Social responsibility*, 11- 13, June, Retrieved (24/10/2021) from: *https://ssrn.com/abstarct=1384242*

Kothari, C.R. (2004). *Research methodology: Methods and techniques*. New Age International.

Laubscher, R., Rabe, D., Olivier, M., Eloff, J. and Venter, H. (2005). Applying Forensic principles to Computer- Based Assessment, *Advances in digital forensics*, Retrieved (20/10/2021) from: *https://researchgate.net/publication//221352753*

Leedy, P. and Ormrod, J. (2013). *Practical Research, Planning and Design, 10th ed.* Pearson Education.

Lutkevich, B. (2021). Computer Forensics (Cyber Forensics), Retrieved (30/10/2021) from: *https://www.techtarget.com/searchsecutrity/definition/computer-forensics*

Madzivire, E.T., Nyamwanza, L., Mushonga, W., Takachicha, M. T. and Mulonda, D. (2020). An Investigation on the Effectiveness of Forensic Audit as a Tool for Fraud Detection and Prevention, *Journal of Accounting, Business and Finance Research,10 (2),* 49-67, Retrieved (24/10/2021) from: *DOI:10.20448/2002.102.49.67*

Mazumder, M. (2011). Forensic Accounting – An Investigative Approach of Accounting, *SSRN Electronic Journal*, 1-9, June, Retrieved (6/09/2021) from: *https://www.researchgate.net/publication/228320470*

Meuldijk, M. (2017). Impact of digitization on the audit profession, *Audit committee News, 58(3),* 33–35, Retrieved (4/11/2021) from: *https://assets.kpmg.com/content/dam/kpmg/ch/pdf/ac-news-8-impact-digitization-en.pdf*

Nachmias, C. and Nachmias, D. (2007). Research methods in the social sciences. *6th Ed*. London: Arnold Publishers.

Nwosu, M. E. (2015). Forensic Auditing and Financial Accounting in Nigeria; An Assessment; *SSRG International Journal of Economics and Management Studies,2(7),* 5-11, July, Retrieved (31/10/2021) from*: www.internationaljournalssrg.org;*

Ojukwu, S. E., Ubi, J. J., Olugbemi, K. O., Olugbemi, M. D. and Emefiele, C. C. (2020). Forensic Accounting and Fraud Detection in Nigerian Universities (A Study of Cross River University of Technology), *Journal of Accounting and Financial Management, 6(4),* 61 – 72, Retrieved (21/10/2021) from: *www.iiardpub.org*

Okolo, E.U., Iduma, M. C. and Ani, J.I., (2018). Computer Technique and Fraud Detection in Nigerian Banking Sector, Retrieved (24/10/2021) from *https://eprints.gouni.edu.ng/3049/1/computertechnique.pdf*

Okoye, K. R. E. and Obialor, U. G. (2020). Forensic Investigation and Forensic Audit Methodology: Remedy to Fraudulent Practices in a Computerized Work Environment, *International Journal of Educational Benchmark,16 (2)* Retrieved (22/10/202) from: *https://benchmarkjournals.com*

Okoye, E. I. and Ndah, E. N. (2019). Forensic Accounting And Fraud Prevention in Manufacturing Companies in Nigeria, *International Journal of Innovative Finance and Economics Research, 7(1),*107-116, Jan.-Mar., Retrieved (24/10/2021) from: *www.seahipaj.org*

Okoye, E.I. and Gbegi, D.O. (2013). Forensic Accounting: A Tool for Fraud Detection and Prevention in the Public Sector: A Study of Selected Ministries in Kogi State, *International Journal of Academic Research in Business and Social Sciences, 3(3)* 1- 19, March, Retrieved (30/10/2021) from: *https://ssrn/abstract=3162992*

Olasanmo, O. (2013). Computer Aided Audit technique and Fraud detection, *Research Journal of Finance and Accounting*

Olukowade, E. and Balogun, E. (2016). The Relevance of Forensic Accounting in the Detection and Prevention of Fraud in Nigeria, *International Journal of Accounting Research, 2(7),* 67–77. Retrieved (30/10/2021) from: *https://doi.org/10.12816/0017351*

Onyeizugbe, C. U. (2017). *Practical Guide to Research Methodology in Management.* Good Success Press.

Oyedokun, G.E. (2013). An Assessment of the Role of Forensic Accountants in Litigation Support Services (An explanatory approach); Retrieved (25/05/2022) from: *https://ssrn.com/ abstract=2410664*

Oyedokun, G.E. (2015). Forensic Investigation and Forensic Audit Methodology in a Computerized Work Environment, *SSRN Electronic Journal*, January Retrieved (23/10/2021) from: *https://researchgate.net*

Oyedokun, G.E. (2015). Approach to Forensic Accounting and Forensic Audit; Retrieved (30/10/2021) from: *https://ssrn.com/ abstract=2575168*

Oyier, O.E. (2013). The Impact of Forensic Accounting Services on Fraud Detection and Prevention among Commercial Banks in Kenya,

Ozkul, F.U. and Pamukc, A. (2012). *Fraud Detection and Forensic Accounting*, Istanbul, Turkey.

Pallant, J. (2016). SPSS Survival Manual: A Step by Step Guide to Data Analysis using SPSS. *6th ed*. Open University Press/McGraw Hill.

Panneerselvam, R. (2014). *Research methodology*. Prentice Hall of India Learning Pvt. Ltd.

Private Investigator News (2023). Retrieved (31/01/2023) from *https://www.pinow.com/investigations/forensic-investigations*

Rasey, M. (2009). History of forensic accounting. Retrieved (30/10/2022) from:*httsp://www.ehow.com/about_5005763*

SAS 99 (Statement on Audit Standards 99: Consideration of Fraud in a Financial Statement Audit) (2002). Retrieved (25/05/2022) from: *http://www.aicpa.org/Research/Standards/AuditAttest/DownloadableDocuments/AU-00316.pdf*

Saunders, M., Lewis, P. and Thornhill, A. (2012). *Research methods for business students*. Pearson education.

Singleton, T.W. and Singleton, A.J. (2001), *Fraud Auditing and Forensic Accounting, (4th Edition), John Wiley and Sons, Corporate F & A, Publishing*

Stoll, C. (1988). Stalking the wily hacker. Communication of the ACM, 31(5), 484- 500, ISSN: 0001-0782:484e97. Retrieved (31/10/2022) from: https://dl.acm.org/doi/10.1145/42411.42412

Stoll, C. (1989). The cuckoo's egg: tracking a spy through the maze of computer espionage. Random House; 1990.

Tjeng, P. S. and Nopianti, R. (2020). The Audit Investigation and Accounting Forensic in Detecting Fraud in Digital Environment, *International Journal of Accounting and Taxation, 8 (1),* 44-54, June. Retrieved (24/10/2021) from: *https://doi.org/10.15640/ijat.v8n1a6*

Veerankutty, F., Ramayah, T., and Ali, N.A. (2018). Information Technology Governance on Audit Technology Performance among Malaysian Public Sector Auditors, *Social Science, 7,* 124, Retrieved (2/11/2021) from: *www.mdpi.com/journal/socsci*

Whyte, S. T. (2018). Cyber Forensic and Data Collection Challenges in Nigeria, *Global Journal of Computer Science and Technology: G Interdisciplinary,18(3)1,* 35- 38, Retrieved on 6/09/2021 from: https://www.researchgate.net

Wood, C. C., Banks, W.W., Guarro, S. B., Garcia, A. A., Hampel, V. E., and Sartorio, H. P. In: Garcia A. A, editor. *Computer security: a comprehensive controls checklist.* John Wiley & Sons; 1987. pp.123e124).

Yin, R. (2009). Case Study Research: Design and Methods, Essential guide to qualitative methods in organizational research. *Applied Social Research Methods Series, 219*.

Yormark, K. (2004). Making the most of an internal investigation. *Journal of Investment Compliance*, 5, 64-67.

Zysman, A. (2004). Forensic Accounting Demystified: *World Investigators Network Standard Practice for Investigative and Forensic Accounting Engagements, Canadian Institute of Chartered Accountants, (Online),* Retrieved (3/10/2021) from: https://www.forensicaccounting.com