**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**
**IMPACT FACTOR: 7.056**

***IJCSMC, Vol. 13, Issue. 8, August 2024, pg.99 – 106***

# Digital Forensic Accounting: An Overview

**Fatima Ismail AL-Hadi[1]; Nagi Ali Al-Shaibany[2]**

[1]IT Department, Faculty of Computer and Information Technology, Sana'a University, Yemen
[2]IT Department, Faculty of Computer and Information Technology, Sana'a University, Yemen
[1] fatima2017@su.edu.ye; [2] Shabiany@su.edu.ye

**DOI: https://doi.org/10.47760/ijcsmc.2024.v13i08.011**

***Abstract— Forensic analysis has become crucial for detecting financial crimes such as fraud, extortion, money laundering, and tax evasion in a rapidly evolving world. This type of analysis is also essential for promoting economic development and enhancing public trust in governments. As fraud strategies advance alongside rapid digital innovations, traditional forensic accounting relies on manual data examination and is increasingly inadequate for addressing sophisticated criminal fraud. The rise in cybercrime underscores digital forensics' need to conduct effective investigations. This study provides an overview of digital forensic accounting, emphasizing the need for forensic accountants to acquire digital forensic skills to conduct thorough investigations. It reviews previous research highlighting the importance of integrating digital technologies into forensic accounting, stressing that this convergence is crucial for enhancing the detection of financial crimes and cyber fraud. Furthermore, the study outlines the basic concepts of both traditional forensic accounting and digital forensics and presents some digital forensic accounting tools that can be utilized in forensic accounting and computer forensics.***

***Keywords— Forensic Science, Forensic accounting, Digital forensics, Digital forensic accounting, Cyber fraud***

## I. INTRODUCTION

Forensic science (FS) utilizes scientific knowledge and techniques to uncover evidence in criminal investigations. The evidence obtained through this process is characterized by high confidence and reliability, rendering it highly trustworthy with a significant probative value that deems it admissible in court. Moreover, it also offers a moderate degree of utility, proving advantageous for research purposes [1]. FS plays a crucial role in understanding patterns of criminal behavior and furnishing proof to bolster inquiries into illegal activities. Through assembling remnants found at the scenes of crimes, forensic experts assume the role of investigators in deciphering unlawful actions. Consequently, this process enables them to derive valuable perspectives that have the potential to enhance protective measures and, in the final analysis, ensure the safety of our societies [2].

*© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden* 

The study in [3] explored the efficacy of forensic methodologies in detecting corruption, focusing on using tools like digital forensics, forensic auditing, and forensic accounting to uncover undisclosed assets, expose financial discrepancies, and gather evidence for legal proceedings. The study delved into corruption cases in the Khomas Region of Namibia to identify and scrutinize common tactics of deceitful individuals and entities. Forensic science plays a crucial role in investigations due to its ability to generate objective and highly precise evidence. This attribute significantly enhances the technological advancement of the procedure[4].

Advanced anti-corruption mechanisms are deemed necessary in emerging nations, as indicated by the Corruption Perception Index (CPI) [5]. Forensic accountants should embrace digital forensic investigation processes in cases involving cyber fraud [6].

Forensic accounting is a combination of accounting, auditing, criminology, and law. The investigation is considered unbiased and serves the interests of company owners and stakeholders. Forensic accounting is a practice that combines traditional accounting with legal frameworks to detect fraud and enhance prosecution efforts.Forensic accounting can help prevent financial crime by identifying and tracking potential fraud instances [7].

Digital Forensics (DF) is a field of forensic science that investigates and interprets digital data. DF is a field of forensic science that investigates and interprets digital data. Digital forensics involves analyzing, validating, and interpreting digital evidence associated with a crime. The proliferation of internet-connected gadgets has led to greater security vulnerabilities for digital media. The internet hosts a variety of attacks, malware, and malicious activities. Crimes can occur due to security flaws and vulnerabilities. Therefore, DF is necessary to promote transparency and prevent crimes [8].

The motivation of this study is to show the critical importance of digital forensic accounting as technology for combating fraud in developing countries that need this technology, particularly since traditional forensic accounting methods alone are insufficient.

## II. RELATED WORK

The author stated in [9] that cybersecurity measures aim to protect financial information and mitigate the risk of fraudulent activities. Forensic accountants are tasked with examining fraud cases related to cybersecurity breaches and deficiencies in internal controls. The study in [10] explored how forensic accounting adapted to digital advancements. Recent research indicated that financial fraud was becoming more sophisticated with technology. Forensic accountants had to employ new tools to address the growing threat. Research in [6] illustrated the connection between digital forensic accounting and decreased cyber fraud in Nigeria. Accountants using these methods were better at identifying phishing scams, advance fee fraud, and credit card fraud. The study recommended enhanced training for accountants and government adoption of these procedures to provide more evidence for court cases. The study in [3] examined the potential of forensic tools in combating corruption in Namibia's Khomas Region. Financial records and electronic data were analyzed to uncover hidden corruption and gather evidence for prosecution. This approach aimed to prevent future corruption and restore trust in the administration. The study recommended enhancing the forensic skills of law enforcement and financial institutions for more efficient investigations. In [11], the research focused on how forensic accounting enhanced financial reporting and increased user trust. The study highlighted that forensic accounting practices could improve the reliability of financial reports and bolster confidence among stakeholders. The study in [12] demonstrated that digital forensics could be an effective tool in fraud auditing. It provided a real-world example of warehouse theft to show how fraud auditing, which focuses on anomalies and patterns, differed from financial auditing. The study emphasized the importance of coordination between fraud auditors and digital investigators in detecting financial crimes in the digital age. The study in [13] highlighted the evolution of forensic accounting techniques in the digital age as financial crimes grew more complex. It pointed out the necessity of integrating cutting-edge technologies and digital methods into modern forensic accounting practices. The study explored both traditional and advanced techniques, underscoring the need for forensic accountants to stay updated to combat fraud effectively. In [7], the research investigated the use of forensic accounting and improved management controls to combat cyber fraud in banks. The goal was to enhance efficiency and reputation by minimizing losses. A model was created to demonstrate the synergy of these tactics, which was validated through testing. The proposal was for banks to employ both forensic accounting and improved internal controls to effectively combat cybercrime.

## III. DIGITAL FORENSIC

The expertise of computer forensics allows accountants to make informed decisions about what measures to take and how to proceed with an inquiry without tainting the evidence [14]**.** Computer forensics, also known as digital forensics, encompasses various domains, including network, server, computer, internet, social media, memory, online gaming, data/disk, and VR forensics [15].

There are essential skills that a forensic accountant must acquire to perform their duties effectively one of these skills is computer forensics [16]. Digital Forensics (DF) identifies cybercrime patterns using established

*© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden* 

methodologies for investigating digital crimes by extracting Potential Digital Evidence (PDE) to present in court. Principles in DF involve extracting digital evidence without tampering, conducting examinations and analyses in a repeatable manner, and maintaining accountability [17]. Digital forensics is the study of recovering and examining evidence from digital devices, particularly in cases involving computer-related crimes [18].

The typical DF process includes three phases: acquisition, analysis, and presentation. Digital evidence is gathered during the acquisition process, analyzed later, and finally presented [8].

**Acquisition**: During this step, digital evidence is collected from various electronic devices such as hard drives, USB drives, and cameras. To prevent the original evidence from being altered, a copy (image) of the device's data is created [8].

**Analysis:** After gathering data, it is inspected and analyzed. This includes identifying potential criminal evidence, such as documents, photographs, videos, logs, and so on. The investigator evaluates and analyses these artifacts to gain a better understanding [8].

**Presentation**: Finally, the investigator compiles a report that summarizes their findings. This report describes the procedures followed during the inquiry, the evidence gathered, its interpretation, and the overall outcome. This report is commonly used in court for legal proceedings [8].

### A. Digital Forensic Services

The utilization of computer and network technologies in business accounting has grown due to the expansion of electronic accounting. Consequently, techniques for finding, protecting, examining, and presenting digital evidence in investigations and court cases have been developed. Forensic accountants have devised methods for locating, safeguarding, examining, and presenting digital evidence in investigations and legal proceedings [19].

Digital forensics involves various processes such as collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence from digital sources using scientifically proven techniques [20]. This procedure aims to reconstruct unlawful incidents or prevent unauthorized acts that may disrupt scheduled operations.

Forensic accountants specialize in computer forensics and e-discovery due to the increasing reliance on digital systems. The digital forensic procedure involves four primary objectives: finding, protecting, recovering, and presenting evidence. Digital evidence needs to be organized, displayed transparently, summarized clearly, and explained effectively [21]**.**

## IV. Forensic Accounting

Forensic accounting represents a nascent occupation that has experienced rapid expansion since its inception. Presently, there is a significant need for professionals in this field, and the trend shows continued growth[22]. Traditional forensic accounting involves manually examining financial data, conducting interviews, and analyzing financial statements to detect abnormalities and signs of fraud [23]. Key challenges in forensic accounting and fraud investigation include the proliferation of big data and digital technology, the complexity of financial transactions, and the increasing sophistication of criminals [12]. Forensic accountants utilize distinct methodologies and models to conduct inquiries that offer dependable information (assurance), validation of financial documents (attestation), and specialized guidance (advising) within legal proceedings[24]. One such model is the Beneish Model, a tool used by forensic accountants to combat accounting fraud. Developed by Massoud Beneish, this method allows a comprehensive examination of a company's financial health by analyzing accounts from both the income statement and the balance sheet [25]. Each non-financial listed company's eight indicators are fed into the Beneish regression model, which produces a Manipulation Score. Businesses that have an M-score higher than the -2.22 benchmark ought to be suspected of manipulating earnings [26].

The Beneish Model and its 8 indicators are listed below [25, 26]:

1. Days Sales in Receivables Indicator (DSRI).
2. Gross Margin Indicator (GMI):
3. Asset Quality Indicator (AQI).
4. Sales Growth Indicator (SGI).
5. Depreciation Indicator (DEPI).
6. Sales General and Administrative Expenses Indicator (SGAI).
7. Leverage Indicator (LVGI).
8. Total Accruals to Total Assets (TATA).

The Beneish Model (M-Score) formula is as follows [25, 26]:

Beneish Model = M- Score = -4,840 + (0.920 × DSRI) + (0.528 × GMI) + (0,404 × AQI) + (0,892 × SGI) + (0,115 × DEPI) + (-0,172 × SGAI) + (4,679 × TATA) + (-0,327 × LEVI).

The Beneish Model (M-Score) formula is as follows [21, 22]:

Beneish Model = M- Score = -4,840 + (0.920 × DSRI) + (0.528 × GMI) + (0,404 × AQI) + (0,892 × SGI) + (0,115 × DEPI) + (-0,172 × SGAI) + (4,679 × TATA) + (-0,327 × LEVI)

Forensic accounting practices are classified into three main areas [27]:

*© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden* 

A. Investigative Auditing: The evidence acquired by investigative auditors is an essential component of the investigation process. Effective and precise examination of the information by investigative auditors significantly increases the likelihood of successful outcomes.
B. Litigation Support: The contributions of forensic accountants are critical to the accuracy of court decisions.
C. Criminal Investigation: Police forces in many industrialized countries rely on forensic accounting tools to conduct effective criminal investigations into accounting fraud.

### A. Forensic Accounting Challenges

In the era of cybercrime, forensic accounting faces numerous challenges. One major challenge is the growing variety and complexity of cybercrimes, including phishing, advance fee fraud, credit card fraud, payroll fraud, invoice fraud, and cryptocurrency fraud [28].

Another significant obstacle is the absence of a suitable framework for detecting and addressing fraud using forensic accounting techniques [29]. This lack of standardized approaches hampers the effectiveness of forensic accounting in uncovering fraudulent activities.

Additionally, implementing forensic accounting practices can be hindered by several factors, including resource shortages, a lack of specialized expertise, and inadequate managerial support. Overcoming these challenges is crucial for enhancing the role of forensic accounting in fraud prevention and detection from a management perspective[29].

### B. Forensic Accounting In The Fight Against Crime

Forensic accounting, a relatively new and rapidly growing field, is gaining increasing prominence, especially in emerging economies. A significant challenge in this domain is the shortage of skilled accountants with the technical expertise and competencies necessary for forensic work [30]. This field is crucial for identifying and addressing deceptive practices both within and outside organizations, particularly when third-party actions suggest potential fraud [31]. Forensic accounting integrates investigative, auditing, and accounting skills [32]. Also known as investigative accounting, it represents a synthesis of forensic science and accounting disciplines. This field merges accounting, auditing, and investigative techniques to tackle disputes and legal issues stemming from fraudulent activities. The term "forensic" underscores the field's relevance to judicial proceedings, highlighting the focus of forensic accountants on resolving unresolved matters using established evidence-based principles [29]. A study detailed in [33] examined the role of forensic accounting in mitigating economic crimes in Ukraine. The research found that Ukraine is rapidly adopting forensic expertise to combat fraud, with positive effects on the national economy. The study recommends that Eastern European countries looking to develop effective strategies against economic crime should consider adopting Ukraine's approach to forensic accounting. In the UK, forensic accounting is overseen by certified professionals and is experiencing growing acceptance [34] the expansion of forensic accounting firms and the inclusion of relevant principles in national educational programs have contributed to its increasing prevalence. While advanced countries have developed various frameworks for forensic accounting, there is no universally accepted model due to the unique nature of fraud risks and mitigation strategies in different organizations. The most recent developments in establishing a durable digital framework for forensic accounting are summarized in Table 1 [29].

**TABLE I**
**PROGRESS IN ESTABLISHING A DURABLE DIGITAL FRAMEWORK FOR FORENSIC ACCOUNTING [29]**

| Author | Contribution | Framework phases |
|---|---|---|
| Pilli *et al.* (2010) | A generic framework for network forensics | Preparation, authentication, detection, incidence response, data collection, preservation, protection, examination, analysis, investigation, fact presentation and review |
| Agarwal *et al.* (2011) | Systematic digital forensic investigation model | Preparation, scene capturing, survey, documentation, communication, evidence collection, preservation, examination, analysis, result presentation and review |
| Amshire and Meshram (2012) | Development of a digital forensic model | Planning, scene capturing, examination, analysis, result presentation, review and reporting |
| Prayudi *et al.* (2015) | Digital forensic business model | Digital investigation, evidence handling, object identification and environment recognition |
| Jain and Kalbande (2015) | Digital forensic framework | Planning, authentication, evidence gathering, cybercrime classification, reporting and future update |
| Talib and Alomary (2015) | Comprehensive ontology based-investigation for digital forensics cybercrime | Preparation, investigation, scene capturing and presentation |
| Jadhap and Agarwal (2016) | Digital forensics investigation model for social networking site | Checking, analysis, scanning, communication and reporting |

**Source:** Yang and Wu (2017)

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden 

## V. DIGITAL FORENSIC ACCOUNTING

**Cyber fraud**, also known as internet or online fraud, represents a type of economic cybercrime where the internet is used to obscure or present misleading information with the intent of deceiving individuals into financial loss, asset loss, or other forms of harm[35]. The increasing use of digital media for data storage has been accompanied by a rise in computer crimes and cyber fraud, exacerbating the challenges faced by security and law enforcement agencies globally [36]. The failure of governments to enforce pre-emptive measures has been identified as a major factor contributing to the persistence of cybercrime [37]. To address these offenses, it is crucial for governmental entities to engage in ongoing surveillance [38]. The importance of digital evidence is growing in both criminal and civil cases, as its utilization now encompasses a wide range of criminal activities, including cybercrime [39]. Research in digital forensics and cybercrime has focused on advancing digital forensic techniques due to the increasing role of digital evidence in corruption cases [3]. Key research areas include data recovery, attribution, and evidence retention, particularly in the context of cyber-related corruption [3]. The Systematic Digital Forensic Investigation Model (SDFIM) consists of eleven phases designed to uncover instances of cybercrime and cyber fraud [8]. Forensic accountants, with their expertise in investigative skills, analytical skills, auditing, accounting, and the preservation of digital forensic evidence, are well-positioned to be valuable resources in mitigating cyber fraud [9]. Forensic accounting has been recognized for its significant role in examining fraudulent activities [40]. The exponential increase in instances of financial fraud and white-collar forensics forefront of attention [41]. Digital forensic accounting methods utilize technology to analyze large datasets, identify patterns, and enhance the detection of fraudulent behaviour. Techniques such as computer-assisted auditing, data mining, and advanced analytics are commonly employed [10]. Forensic accounting requires procedures such as evidence collection, analysis, and documentation[11].

Accountants use various investigation techniques to examine accounting schemes and frauds perpetrated through digital means [42]. Research conducted in [43] proposed employing a digital forensic framework to identify typical phases of forensic execution, integrating traditional forensic methodology with a digital context to effectively reduce fraud instances. Additionally, research in [44] suggested using an advanced data acquisition model in digital forensic accounting, which focuses on data acquisition, management, and the digital aspects of social spaces commonly used for fraud. Authors in [45] identified three key components of a digital forensic accounting framework: preparation, in-depth investigation, and presentation of findings for fraud detection and prosecution, as illustrated in **Fig.1**.


**Fig.1 Proposed Framework for Digital Forensic Accounting [45]**

### A. DIGITAL FORENSIC ACCOUNTING TOOLS

Specialized software for forensic accounting is available for use in investigations, assisting in the collection of evidence and maintaining data integrity. In the context of investigating illegal activities, digital forensic accounting aids in data recovery and evidence preservation. A list of notable accounting and digital forensic tools is provided in Table 2.

**TABLE II**
**DIGITAL FORENSIC ACCOUNTING TOOLS**

| Sr.No | Tool Name | Utilization | Latest Version | Aspects |
|---|---|---|---|---|
| **1** | Forensic tool kit (FTK) [46-48] | Forensic Accounting and Computer Forensic | 8 | Collects and stores data across networks, supports acquisition from 3,500 mobile devices, detects missing data and malicious activity, and tracks data movements and modifications. |
| **2** | Encase [47-49] | Forensic Accounting and Computer Forensic | 8.7 | Comprehensive Data Handling: Collects data from diverse sources (network, cloud, mobile), generates |

© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden 

| | | | | |
|---|---|---|---|---|
| | | | | detailed reports, utilizes metadata, keywords, and hashes, supports memory acquisition, disk imaging, live device data acquisition via USB, data carving, password recovery, and remote data collection and processing. |
| **3** | ProDiscover [47, 48] | Forensic Accounting and Computer Forensic | 8.2 | Inspects and captures data, performs advanced searches, responds to threats rapidly, includes installable SMART AGENT, malware detection, uses Perl scripts, and generates automatic evidence reports. |
| **4** | Autopsy [49, 50] | Computer Forensic | 4.21 | collaborative work by allowing multiple examiners to handle large cases simultaneously enables text extraction and searches for specific terms and regular expression patterns, extracts artifacts from web browsers, is easy to install on Windows, and supports internal and external hard drives as well as smartphones. |
| **5** | Computer Assisted Audit Tool (CAAT) [51, 52] | Forensic Accounting | Various Versions | Auditing entire datasets to identify red flags, utilizing familiar commands, reducing the learning curve, assisting in report creation, offering flexibility in data export formats, and preserving data integrity by preventing editing and automating test runs. |

## VI. RECOMMENDATIONS

This article underscores the significance of digital forensic accounting in combating financial crime and cyber fraud in the digital age. Several recommendations are proposed to enhance its effectiveness:

Enhance Skills Through Training: Improving the skills of workers by implementing specialized digital forensics training programs for accountants is crucial. Additionally, boosting communication between these professionals and digital investigators will lead to more thorough investigations.

Integrate Digital Forensics in Law Enforcement: Law enforcement and regulatory organizations should incorporate digital forensics into their investigative processes. Investing in advanced tools and providing comprehensive personnel training are essential steps in this integration.

Raise Public Awareness: Public awareness campaigns should be conducted to educate individuals and businesses about internet fraud. These campaigns can encourage the reporting of suspected crimes and promote proactive measures to enhance cybersecurity.

Promote Ongoing Research and Development: Continued research and development are vital for keeping up with advancements in digital forensic technology. Encouraging collaboration between academics and industry professionals will help in developing advanced approaches and best practices in digital forensic accounting.

Implementing these recommendations will contribute to building a stronger system for addressing financial crime in the digital era.

## VII. CONCLUSIONS

Forensic science plays a crucial role in uncovering evidence for criminal investigations. However, the advent of the digital age has introduced new challenges, notably cybercrime and financial fraud conducted through digital platforms. Traditional forensic accounting methods are increasingly inadequate to address these complex issues. This situation necessitates the integration of digital forensics with forensic accounting, leading to the emergence of digital forensic accounting as a specialized field. By combining expertise in accounting, auditing, and digital forensics, professionals in this field will be equipped to analyze large datasets, identify patterns, and uncover concealed evidence of financial misconduct. Research has demonstrated the effectiveness of digital forensic accounting in mitigating cyber fraud and enhancing financial reporting. As financial crimes become

*© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden* 

more sophisticated, it is essential for forensic accountants to continually develop their skill sets and adopt advanced digital forensic techniques. This ongoing evolution will be critical in addressing and combating the emerging threats posed by increasingly complex financial crimes.

# REFERENCES


**[1].** D. Miano, K. Anangwe, and K. Kiemo, "Disparities in Forensic Science Adoption for Crime Investigation in Kenya: The Role of Police Demographics," *SAGE Open*, vol. 14, no. 1, p. 21582440231225900, 2024.

**[2].** R. Hoffmann, G. E. Meakin, M. Morelato, and C. Roux, "The utility of trace DNA within forensic science for investigative and intelligence purposes," *Wiley Interdisciplinary Reviews: Forensic Science*, p. e1515, 2024.

**[3].** A. Shifiona and B. Lekubu, "Forensics as a Tool in Solving Corruption: A Related Cases in Khomas Region, Namibia," *Southern African Journal of Security*, vol. 1, pp. 26 pages-26 pages, 2023.

**[4].** N. Suleiman and A. Ahmi, "Mitigating corruption using forensic accounting investigation techniques: the watchdog perspectives," *Indian-Pacific Journal of Accounting and Finance*, vol. 2, no. 1, pp. 4-25, 2018.

**[5].** D. Enste and C. Heldman, "Causes and consequences of corruption: An overview of empirical results," 2017.

**[6].** M. A. Awodiran, A. T. Ogundele, U. J. Idem, and O. Emem, "Digital forensic accounting and cyber fraud in Nigeria," in *2023 International Conference On Cyber Management And Engineering (CyMaEn)*, 2023: IEEE, pp. 321-326.

**[7].** O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "The integration of forensic accounting and the management control system as tools for combating cyberfraud," *Academy of Accounting and Financial Studies Journal*, vol. 25, no. 2, pp. 1-14, 2021.

**[8].** H. Dubey, S. Bhatt, and L. Negi, "Digital Forensics Techniques and Trends: A Review," *The International Arab Journal of Information Technology (IAJIT)*, vol. 20, no. 4, pp. 644-654, 2023.

**[9].** J. C. Okechukwu, "Forensic Accountants' Strategies and Cybercrime Mitigation," Northcentral University, 2020.

**[10].** R. E. Daraojimba, O. A. Farayola, F. O. Olatoye, N. Mhlongo, and T. T. Oke, "Forensic accounting in the digital age: a US perspective: scrutinizing methods and challenges in digital financial fraud prevention," *Finance & Accounting Research Journal*, vol. 5, no. 11, pp. 342-360, 2023.

**[11].** A. Desi, R. I. Akintoye, and T. A. Aguguom, "Forensic Accounting, a Veritable Financial Tool for Qualitative Financial Reporting Systems in the 21st Century," *International Journal of Professional Business Review: Int. J. Prof. Bus. Rev.*, vol. 8, no. 6, p. 30, 2023.

**[12].** N. Simeunović, G. Grubor, and N. Ristić, "Forensic accounting in the fraud auditing case," *The European Journal of Applied Economics*, vol. 13, no. 2, pp. 45-56, 2016.

**[13].** O. Odeyemi, C. V. Ibeh, N. Z. Mhlongo, O. F. Asuzu, K. F. Awonuga, and F. O. Olatoye, "FORENSIC ACCOUNTING AND FRAUD DETECTION: A REVIEW OF TECHNIQUES IN THE DIGITAL AGE," *Finance & Accounting Research Journal*, vol. 6, no. 2, pp. 202-214, 2024.

**[14].** G. S. Kearns, "Computer Forensics for Accountants," 2014.

**[15].** B. K. Sharma, M. A. Joseph, B. Jacob, and B. Miranda, "Emerging trends in digital forensic and cyber security overview," *2019 Sixth HCT Information Technology Trends (ITT)*, pp. 309-313, 2019.

**[16].** W. E. Herbert, I. N. Tsegba, E. E. Ene, and F. Onyilo, "The rise of fraud examination and forensic accounting in Africa: the Nigerian experience," *Archives of Business Research*, vol. 5, no. 4, 2017.

**[17].** N. M. Karie, V. R. Kebande, and H. Venter, "Taxonomy for digital forensic evidence," 2017.

**[18].** B. Prasanthi, "Cyber forensic tools: a review," *International Journal of Engineering Trends and Technology (IJETT)*, vol. 41, no. 5, pp. 266-271, 2016.

**[19].** A. E. Ogunwole and S. A. Jimoh, "Forensic Accounting Services as a Tool for Fraud Mitigation in Selected Kwara State-owned Tertiary Institutions in Nigeria," *NIU Journal of Social Sciences*, vol. 10, no. 1, pp. 57-67, 2024.

**[20].** H. Roselyn Afor, A. S. Akwu-Odo Salihu, F. Eni-Itan Titilayo, and I. Karimu Moses, "Forensic Accounting Techniques And Fraudulent Practices In Nigerian Public Sector," *Journal of Forensic Accounting & Fraud Investigation (JFAFI)*, vol. 6, no. 1, pp. 1-22, 2021.

**[21].** R. Overill and J. Collie, "Deep: Extending the digital forensics process model for criminal investigations," *Athens Journal of Sciences*, vol. 7, no. 4, pp. 225-240, 2020.

**[22].** M. Hitchcock, "The importance and implications of forensic accounting in the financial world," 2018.

**[23].** O. E. Akinbowale, "Information communication technology and forensic accounting in Nigeria," *International Journal of Business and Finance Management Research*, vol. 6, no. 1, pp. 1-7, 2018.

**[24].** T. Ogiriki and E. Appah, "Forensic accounting & auditing techniques on public sector fraud in Nigeria," *International Journal of African and Asian Studies*, vol. 47, no. 1, pp. 10-19, 2018.

**[25].** A. Özcan, "The use of Beneish model in forensic accounting: evidence from Turkey," *Journal of Applied Economics and Business Research*, vol. 8, no. 1, pp. 57-67, 2018.

**[26].** A. H. Elkhaldi, H. H. Flayyih, S. I. Ali, and Y. Mohammed, "The role of the Beneish Model as a tool for forensic accounting in fraud detection in the Tourism Industry," *Ishtar Journal of Economics and Business Studies*, vol. 2, no. 4, pp. 1-12, 2021.

**[27].** N. SULEIMAN, "FORENSIC ACCOUNTING INVESTIGATING TECHNIQUES AND THE PUBLIC SECTOR CORRUPTION IN NIGERIA," 2018.

**[28].** E. E. M. Micah, I. H. Saidu, T. Ibitomi, and B. S. Sanusi, "Digital Forensics in the Era of Cybercrime: Emerging Trends and Challenges for Forensic Accountants in Nigeria," *European Journal of Accounting, Auditing and Finance Research*, vol. 11, no. 9, pp. 85-100, 2023.

**[29].** O. E. Akinbowale, H. E. Klingelhöfer, and M. F. Zerihun, "An innovative approach in combating economic crime using forensic accounting techniques," *Journal of Financial Crime*, vol. 27, no. 4, pp. 1253-1271, 2020.


*© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden* 

**[30].** E. E. Ehioghiren and O. Atu, "Forensic accounting and fraud management: Evidence from Nigeria," *Igbinedion University Journal of Accounting*, vol. 2, no. 8, pp. 245-308, 2016.
**[31].** K. P. Modugu and J. Anyaduba, "Forensic accounting and financial fraud in Nigeria: An empirical approach," *International Journal of Business and Social Science*, vol. 4, no. 7, pp. 281-289, 2013.
**[32].** E. I. Okoye and D. Gbegi, "Forensic accounting: A tool for fraud detection and prevention in the public sector. (A Study of Selected Ministries in Kogi State)," *Okoye, EI & Gbegi, DO (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*, vol. 3, no. 3, pp. 1-19, 2013.
**[33].** K. Serhii, P. Vadym, K. Oleg, M. Oleksandr, and O. Strilets, "Forensic economic examination as a means of investigation and counteraction of economic crimes in East Europe (example of Ukraine)," *J. Legal Ethical & Regul. Isses*, vol. 22, p. 1, 2019.
**[34].** S. Hegazy, A. Sangster, and A. Kotb, "Mapping forensic accounting in the UK," *Journal of International Accounting, auditing, and Taxation*, vol. 28, pp. 43-56, 2017.
**[35].** S. Chen *et al.*, "The Spatiotemporal Pattern and Driving Factors of Cyber Fraud Crime in China," *ISPRS International Journal of Geo-Information*, vol. 10, no. 12, p. 802, 2021. [Online]. Available: https://www.mdpi.com/2220-9964/10/12/802.
**[36].** R. Apau and F. N. Koranteng, "An overview of the digital forensic investigation infrastructure of Ghana," *Forensic Science International: Synergy*, vol. 2, pp. 299-309, 2020.
**[37].** "Mitigating Financial Fraud and Cybercrime: A Systematic Literature Study," *Accounting Studies and Tax Journal (COUNT)*, vol. 1, no. 4, pp. 258-273, 04/26 2024, doi: 10.62207/mnp8nd05.
**[38].** A. R. Javed, W. Ahmed, M. Alazab, Z. Jalil, K. Kifayat, and T. R. Gadekallu, "A comprehensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions," *IEEE Access*, vol. 10, pp. 11065-11089, 2022.
**[39].** H. Guo and J. Hou, "Review of the accreditation of digital forensics in China," *Forensic sciences research*, vol. 3, no. 3, pp. 194-201, 2018.
**[40].** O. Anuolam, T. Onyema, and U. Ekeke, "Forensic accounting and financial crisis in Nigeria," *West African Journal of Industrial and Academic Research*, vol. 17, no. 1, pp. 120-125, 2017.
**[41].** S. M. O. M. I. RATE, I. MOROCCO, R. PROFILE, and M. O. A. D. COUNTRY, "Risk governance & control: Financial markets and institutions," 2014.
**[42].** R. Abdullahi and N. Mansor, "Fraud prevention initiatives in the Nigerian public sector: understanding the relationship of fraud incidences and the elements of fraud triangle theory," *Journal of Financial Crime*, vol. 25, no. 2, pp. 527-544, 2018.
**[43].** M. Reith, C. Carr, and G. Gunsch, "An examination of digital forensic models," *International Journal of Digital Evidence*, vol. 1, no. 3, pp. 1-12, 2002.
**[44].** R. B. Adams, "The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice," 2012.
**[45].** M. Kohn, M. Olivier, and J. Eloff, *Framework for a Digital Forensic Investigation*. 2006, pp. 1-7.
**[46].** N. Simeunović, G. Grubor, and N. Ristić, "Forensic accounting in the fraud auditing case," *The European Journal of Applied Economics*, vol. 13, no. 2, 2016.
**[47].** T. P. Tong, K. Asokan, and I. S. Munjal, "The impact of forensic accounting tools in investigating white-collar crime," in *E3S Web of Conferences*, 2023, vol. 389: EDP Sciences, p. 09034.
**[48].** K. Ghazinour, D. M. Vakharia, K. C. Kannaji, and R. Satyakumar, "A study on digital forensic tools," in *2017 IEEE international conference on power, control, signals and instrumentation engineering (ICPCSI)*, 2017: IEEE, pp. 3136-3142.
**[49].** V. authors, *SUSTAINABLE DEVELOPMENT IN ENGINEERING AND TECHNOLOGY*. ALCOY, 2022.
**[50].** H. Adamu, A. A. Ahmad, A. Hassan, and S. Gambasha, "Web browser forensic tools: Autopsy BHE and net analysis," *Int. J. Res. Innov. Appl. Sci*, vol. 6, no. 5, pp. 103-107, 2021.
**[51].** A. Samagaio and T. A. Diogo, "Effect of computer-assisted audit tools on corporate sustainability," *Sustainability*, vol. 14, no. 2, p. 705, 2022.
**[52].** F. A. Wassie, "Leveraging computer-assisted audit tools for corporate sustainability: Evidence from Ethiopia," *Journal of Infrastructure, Policy and Development*, vol. 8, no. 1, p. 2690, 2023.

*© 2024, IJCSMC All Rights Reserved, ZAIN Publications, Fridhemsgatan 62, 112 46, Stockholm, Sweden* 