European Journal of Accounting, Auditing and Finance Research
Vol.11, No. 9, pp.85-100, 2023
Print ISSN: 2053-4086(Print),
Online ISSN: 2053-4094(Online)
Website: https://www.eajournals.org/
Publication of the European Centre for Research Training and Development-UK

Digital Forensics in the Era of Cybercrime: Emerging Trends and Challenges for Forensic Accountants in Nigeria

[1]Micah, Ezekiel Elton Mike, Ph.D; [2] Saidu, Ibrahim Halidu, Ph.D ; [3]Ibitomi, Taiwo, Ph.D.; & [1]Sanusi, Bello Sambo

[1]Airforce Institute of Technology, Kaduna, Kaduna State, Nigeria
Department of Accounting
[2]ANAN University, Kwal, Jos, Plateau State, Nigeria
Department of Financial Reporting.
[3]Achievers University, Owo, Ondo State, Nigeria
Department of Business Administration

doi: https://doi.org/10.37745/ejaafr.2013/vol11n985100 Published August 26 2023

Citation: Micah, E.E.M., Saidu, I.H., Ibitomi T. and Sanusi, B.S. (2023) 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

ABSTRACT*:* *This study examined the impact of technology on digital forensics and the challenges faced by forensic accountants in the era of cybercrime. The study highlights the four dimensions in which technology has an impact on digital forensics: technical, legal, organizational, and educational. The paper also discusses how emerging technologies such as artificial intelligence and machine learning can be used in digital forensics, along with the challenges they present. Cloud computing is also examined, and the challenges it poses for forensic accountants who need to access and analyze financial data stored or processed in the cloud are discussed. The research used a qualitative research design and incorporated the chain of custody theory in digital forensics. The findings of this study suggest that forensic accountants need to update their knowledge and skills in digital forensics to keep up with the latest trends and technologies in cybercrime in Nigeria. It is recommended that forensic accountants adopt a multidisciplinary approach that integrates accounting principles with digital forensics methods and tools. Additionally, following best practices and guidelines for digital evidence collection, preservation, analysis, and presentation is crucial to ensure the integrity, reliability, and admissibility of digital evidence in court.*

KEYWORDS*:* digital forensics, cybercrime, forensic accountants

INTRODUCTION

Cybercrime is a global phenomenon that poses serious threats to individuals, businesses, governments and society at large. According to the International Telecommunication Union (ITU),

cybercrime is "any crime that involves a computer and a network" (ITU, 2023: 1). Cybercrime can take various forms, such as hacking, phishing, identity theft, ransom ware, cyber espionage, cyber terrorism and cyber warfare. Cybercrime can cause significant financial losses, reputational damage, operational disruption, legal liability and national security risks.

The rapid development of information and communication technologies (ICTs) has enabled cybercriminals to exploit the vulnerabilities of digital systems and networks, as well as the human factors that influence their use and security. Cybercriminals can operate across borders, jurisdictions and sectors, making it difficult to detect, prevent and prosecute their activities. Moreover, cybercrime is constantly evolving and adapting to new technologies, regulations and countermeasures.

In this context, digital forensics plays a vital role in combating cybercrime by providing the methods and tools to collect, preserve, analyze and present digital evidence from various sources, such as computers, mobile devices, cloud services, social media platforms and Internet of Things (IoT) devices. Digital forensics can help identify the perpetrators, motives, methods and impacts of cybercrime, as well as support the investigation, prosecution and adjudication of cybercrime cases.
However, digital forensics also faces many challenges and limitations in the era of cybercrime. Some of these challenges include the increasing volume and complexity of digital data, the diversity and dynamism of digital devices and platforms, the encryption and obfuscation of digital evidence, the legal and ethical issues of digital evidence collection and handling, the shortage of qualified and skilled digital forensic practitioners and the lack of standardization and harmonization of digital forensic procedures and practices.

One of the domains that is particularly affected by cybercrime and require digital forensics is forensic accounting. Forensic accounting is "the application of accounting principles, theories and discipline to facts or hypotheses at issue in a legal dispute" (American Institute of Certified Public Accountants [AICPA) (AICPA, 2023a). Forensic accounting can help detect, investigate and prevent fraud, corruption and other economic crimes that involve financial transactions, records and statements. Forensic accounting can also assist in calculating economic damages, valuing businesses or assets, resolving disputes or litigations and providing expert testimony or opinions.
However, forensic accounting also faces many challenges and opportunities in the era of cybercrime. Some of these challenges include the increasing sophistication and diversity of cyber fraud schemes, such as phishing, advance fee fraud, credit card fraud, payroll fraud, invoice fraud and cryptocurrency fraud (Oyedokun et al., 2023). These schemes can target individuals, businesses or governments and can cause significant financial losses and reputational damage. Moreover, forensic accountants have to deal with the challenges of digital forensics, such as accessing, analyzing and presenting digital evidence from various sources and formats, complying with legal and ethical standards and staying updated with the latest technologies and trends.

On the other hand, forensic accountants also have many opportunities to leverage digital forensics to enhance their capabilities and performance in the era of cybercrime. Some of these opportunities include using digital forensic tools and techniques to identify, collect, preserve and analyze digital evidence from various sources and platforms, such as emails, websites, social media, mobile devices, cloud services and blockchain (PwC, 2023). These tools and techniques can help forensic accountants uncover hidden or deleted data, trace digital footprints, reconstruct events or transactions, verify or falsify claims or allegations and generate reports or visualizations. Moreover, forensic accountants can use digital forensics to collaborate with other professionals, such as law enforcement agencies, regulators, auditors, lawyers and judges, to share information, coordinate actions and provide support or advice.

Therefore, this research aims to explore the emerging trends and challenges of digital forensics in the era of cybercrime and their implications for forensic accountants. The research questions were:

i. What are the current and future trends of cybercrime and how do they affect forensic accounting?
ii. What are the current and future challenges of digital forensics and how do they affect forensic accounting?
iii. How can forensic accountants use digital forensics to enhance their capabilities and performance in the era of cybercrime?

The scope of the study was Nigeria, the reason was that the use of technology among accountants is still at a very low rates mostly in forensic accounting. Therefore, there is need for such study in Nigeria to enable forensic accountants to understand the use of technology in carrying out their daily activities in checking out for fraud in various organization.

LITERATURE REVIEW

Digital Forensics

There is no universally accepted definition of digital forensics. However, digital forensics is the process of identifying, preserving, analyzing, and presenting digital evidence in a legally acceptable manner (Casey & Backhouse 2006). Also, digital forensics is the application of scientific methods to collect, examine, interpret, and report on digital data that can provide information about past or present events that are relevant to a legal or investigative matter (Carrier & Spafford 2006). Digital forensics is a vital component of cybersecurity that helps to combat and prevent cybercrime. Digital forensics professionals use various methods and tools to collect, examine, interpret, and report on digital evidence that can provide crucial information about cyber incidents and actors.

The scope of digital forensics covers various aspects of digital data acquisition and analysis. Some of these aspects are:

i. Digital data acquisition: This involves the extraction of digital data from various sources, such as devices, networks, cloud services, or online platforms. The data acquisition process must follow certain standards and procedures to ensure the integrity, authenticity, and admissibility of the evidence.
ii. Digital data examination: This involves the inspection of digital data using various tools and techniques to identify relevant information, such as files, metadata, logs, timestamps, hashes, or encryption keys. The examination process must be conducted in a forensically sound manner to avoid altering or damaging the evidence.
iii. Digital data interpretation: This involves the analysis of digital data using various methods and frameworks to infer meaning, significance, and context from the evidence. The interpretation process must be based on logical reasoning and scientific principles to support valid conclusions.
iv. Digital data reporting: This involves the presentation of digital data using various formats and media to communicate the findings, opinions, and recommendations based on the evidence. The reporting process must be clear, concise, and accurate to convey the relevant information to the intended audience.

The scope of digital forensics also covers various sub-disciplines that focus on specific types or sources of digital evidence. Some of the sub-disciplines such as computer forensics which focuses on the analysis of digital data stored or processed on computers or laptops; mobile device forensics which focuses on the analysis of digital data stored or processed on mobile devices such as smartphones or tablets; network forensics: This focuses on the analysis of digital data transmitted or received over networks such as LANs or WANs; cloud forensics: This focuses on the analysis of digital data stored or processed on cloud services such as Google Drive or Dropbox; social media forensics which focuses on the analysis of digital data generated or shared on social media platforms such as Facebook or Twitter. Others include malware forensics, memory forensics; database forensics; and multimedia forensics, among others.

The scope of digital forensics is constantly evolving and expanding as new technologies and challenges emerge in the digital world. Therefore, digital forensics professionals need to keep up with the latest developments and trends in their field and update their skills and knowledge accordingly.

Importance of Digital Forensics in the Era of Cybercrime

Cybercrime is a growing threat that affects individuals, businesses, governments, and society as a whole. Cybercrime refers to any illegal activity that involves the use of computers, networks, or digital devices to commit or facilitate crimes. Some examples of cybercrime are hacking, identity theft, phishing, ransomware, cyber stalking, online fraud, cyberterrorism, and cyberwarfare. According to the FBI, cybercrime cost the U.S. economy $4.2 billion in 2020 alone (FBI, 2021).

Digital forensics is a branch of forensic science that deals with the collection, preservation, analysis, and presentation of digital evidence. Digital evidence is any information stored or transmitted in binary form that may be relevant to a legal case. Digital evidence can be found on various devices, such as computers, smartphones, tablets, cameras, flash drives, cloud servers, and networks. Digital forensics can help to identify the source, origin, content, and context of digital data, as well as reconstruct the events and actions that occurred on a digital device or network.
Digital forensics is important in cybersecurity because it helps to:

i. Collect, process, preserve, and analyze evidence that can be found on computers, smartphones, or networks.
ii. Trace the cyber attack path and scrutinize every move the attacker made on your network.
iii. Identify network vulnerabilities and then develop ways to mitigate them.
iv. Provide a report of any data that was copied or removed from the network.
v. Collect, analyze, and preserve digital data, which is often the only source of evidence available in many investigations related to cybercrime, terrorism, and corporate fraud (National University, 2021).
vi. Digital forensics plays a key role in investigating cybercrime, preventing data breaches, providing evidence in legal cases, protecting intellectual property, and recovering lost data (Sikich, 2023). In this paper, we will discuss the definitions and scope of digital forensics in more detail.

Forensic accountants are professionals who apply their accounting knowledge and skills to assist in legal matters, such as fraud detection and prevention, dispute resolution, litigation support and expert testimony. Forensic accountants can work in various sectors, such as public accounting firms, law enforcement agencies, government agencies, corporations, non-governmental organizations and academia.

Forensic accountants are involved in investigating and analyzing financial evidence. They are also involved in developing computerized applications that help analyze and present financial evidence. Forensic accountants adjust their methods and goals for each case. They may use both paper- and computer-based investigation techniques (Accounting.com, 2023).

Forensic accountants perform a variety of tasks during their investigations. They collect data as they research funds, assets, and similar financial information. Forensic accountants also know accounting practices and may testify in court. Responsibilities include (Accounting.com, 2023):

i. Examining financial records and statements to identify irregularities or discrepancies
ii. Tracing the sources and destinations of funds or assets
iii. Calculating the damages or losses caused by fraud or other misconduct
iv. Preparing reports or exhibits that summarize the findings and conclusions

v. Communicating with clients, lawyers, auditors, regulators or other stakeholders
vi. Testifying as an expert witness in court or arbitration proceedings.

Forensic accountants can play a significant role in digital forensics investigations, especially when the cases involve cyber fraud or other financial crimes that leave digital traces. Forensic accountants can use digital forensics tools and techniques to access, analyze and present digital evidence from various sources and platforms, such as emails, websites, social media, mobile devices, cloud services and blockchain (PwC, 2023).

Forensic accountants can use digital forensics to uncover hidden or deleted data, trace digital footprints, reconstruct events or transactions, verify or falsify claims or allegations and generate reports or visualizations. Forensic accountants can also use digital forensics to collaborate with other professionals, such as law enforcement agencies, regulators, auditors, lawyers and judges, to share information, coordinate actions and provide support or advice.

However, forensic accountants also face many challenges and limitations in using digital forensics in their investigations. Some of these challenges include (Kaur *et al.,* 2023):

i. The increasing volume and complexity of digital data
ii. The diversity and dynamism of digital devices and platforms
iii. The encryption and obfuscation of digital evidence
iv. The legal and ethical issues of digital evidence collection and handling
v. The shortage of qualified and skilled digital forensic practitioners
vi. The lack of standardization and harmonization of digital forensic procedures and practices

Therefore, forensic accountants need to enhance their knowledge and skills in digital forensics to cope with the emerging trends and challenges of cybercrime. Forensic accountants need to keep abreast of the latest technologies and trends in cybercrime and digital forensics. Forensic accountants need to adopt a multidisciplinary approach that integrates accounting principles, theories and discipline with digital forensics methods and tools. Forensic accountants need to follow the best practices and guidelines for digital evidence collection, preservation, analysis and presentation. Forensic accountants need to collaborate and communicate effectively with other professionals involved in digital forensics investigations. Forensic accountants need to maintain their professional integrity, objectivity and independence in conducting digital forensics investigations.

Theoretical Framework

This research is anchored on the chain of custody theory in digital forensics. The chain of custody theory is a concept that is essential in digital forensics. The chain of custody in digital forensics is also known as the paper trail forensic link or chronological documentation of the evidence. Chain

of custody indicates the collection, sequence of control, transfer and analysis of digital evidence related to cybercrime (GeeksforGeeks, 2023a).

The chain of custody theory is based on the principle that digital evidence must be preserved and protected from any alteration, tampering or loss during the investigation process. The chain of custody theory ensures that the digital evidence is reliable, authentic and admissible in court. The chain of custody theory also helps to establish the identity and credibility of the digital forensic practitioners who handled the evidence (GeeksforGeeks, 2023a).

The chain of custody theory consists of four main elements: identification, collection, preservation and documentation. Identification involves locating and recognizing potential digital evidence from various sources and platforms. The collection involves acquiring and extracting digital evidence using appropriate tools and techniques. Preservation involves securing and storing digital evidence in a safe and controlled environment. Documentation involves recording and reporting all the details and actions related to the digital evidence, such as date, time, location, description, hash value, signature, etc. (EC-Council, 2023).

The chain of custody theory originated from the legal concept of chain of custody in physical evidence. The chain of custody in physical evidence refers to the chronological documentation of the custody, control, transfer and disposition of physical evidence related to a crime (Legal Information Institute, 2023). The chain of custody in physical evidence was developed to ensure the integrity and admissibility of physical evidence in court. The chain of custody theory in digital forensics was developed by adapting the concept of chain of custody in physical evidence to the context of digital evidence. The chain of custody theory in digital forensics was proposed by various researchers and practitioners in the field of digital forensics and cybercrime, such as Casey (2004), Carrier (2005), Reith et al. (2002), Rogers (2006) and lots more.

The central arguments of the chain of custody theory in digital forensics are:

i. Digital evidence is volatile, fragile and dynamic, which makes it vulnerable to alteration, tampering or loss during the investigation process.
ii. Digital evidence must be preserved and protected from any modification or damage during the investigation process to maintain its integrity and admissibility in court.
iii. Digital evidence must be documented and reported in a clear, accurate and complete manner during the investigation process to establish its authenticity and credibility in court.
iv. Digital forensic practitioners must follow the best practices and standards for collecting, preserving and documenting digital evidence during the investigation process to ensure their professionalism and competence.

The weaknesses of the chain of custody theory in digital forensics are:

i. Digital evidence is complex and diverse, which makes it difficult to identify, collect and preserve all relevant digital evidence from various sources and platforms.

ii. Digital evidence is subject to legal and ethical issues, such as privacy, consent, jurisdiction, etc., which may limit or restrict the access or use of digital evidence during the investigation process.
iii. Digital forensic practitioners face various challenges and limitations, such as a lack of resources, skills, training, tools, etc., which may affect their ability to collect, preserve and document digital evidence during the investigation process.
iv. Digital forensic procedures and practices are not standardized or harmonized across different sectors, regions or countries, which may create inconsistency or discrepancy in collecting, preserving and documenting digital evidence during the investigation process.

The chain of custody theory in digital forensics applies to this study because it provides a framework for analyzing the emerging trends and challenges of digital forensics in the era of cybercrime and their implications for forensic accountants. The chain of custody theory can help to identify and evaluate the current and future sources and platforms of digital evidence related to cybercrime and forensic accounting, assess and compare the current and future tools and techniques for collecting, preserving and documenting digital evidence related to cybercrime and forensic accounting, examine and critique the current and future legal and ethical issues of digital evidence collection and handling related to cybercrime and forensic accounting, explore and suggest the current and future best practices and standards for digital evidence collection, preservation and documentation related to cybercrime and forensic accounting, investigate and explain the current and future roles and responsibilities of forensic accountants in using digital forensics to enhance their capabilities and performance in the era of cybercrime, among others.

METHODOLOGY

This study adopts a qualitative research design to explore the emerging trends and challenges of digital forensics in the era of cybercrime and their implications for forensic accountants. Qualitative research is suitable for this study because it allows the researcher to understand subjective experiences, beliefs and concepts, gain in-depth knowledge of a specific context or culture, explore under-researched problems and generate new ideas (Scribbr, 2023).

The data collection method used in this study is secondary data analysis. Secondary data analysis is when previously gathered data are reanalyzed to find answers to research questions that differ from the questions asked in the original research (Hinds *et al.*, 1997). Secondary data analysis has several advantages, such as saving time and resources, increasing the sample size and diversity, enhancing the validity and reliability of the findings, and facilitating the comparison and synthesis of different studies (University of Wolverhampton, 2023). The secondary data used in this study are derived from various sources, such as academic journals, books, reports, websites and media articles. The secondary data are selected based on the following criteria: relevance, credibility, timeliness, and accessibility

The data analysis method used in this study is content analysis. Content analysis is a research method used to identify patterns in recorded communication. Content analysis can be both quantitative (focused on counting and measuring) and qualitative (focused on interpreting and understanding) (, 2023). In this study, qualitative content analysis is used to make inferences by analyzing the meaning and semantic relationship of words and concepts in the secondary data. According to Scribbr (2023), the content analysis process involves defining the unit of analysis, developing a coding scheme, applying the coding scheme, and analyzing the results:

RESULTS AND DISCUSSION

This section presents the research findings based on secondary data analysis and content analysis. The research findings are organized into three themes: advancements in technology and their impact on digital forensics, the use of artificial intelligence and machine learning in digital forensics, and cloud computing and its challenges for forensic accountants.

Advancements in Technology and Their Impact on Digital Forensics

One of the emerging trends in digital forensics is the rapid development and evolution of technology, which creates both opportunities and challenges for digital forensic practitioners. Technology can provide new sources and platforms of digital evidence, such as mobile devices, social media, the Internet of Things (IoT), blockchain, etc. (Solanke & Biasiotti, 2022). Technology can also provide new tools and techniques for collecting, preserving and analyzing digital evidence, such as artificial intelligence, machine learning, cloud computing, etc. (Solanke & Biasiotti, 2022). However, technology can also pose various difficulties and risks for digital forensics, such as increasing volume and complexity of digital data, encryption and obfuscation of digital evidence, legal and ethical issues of digital evidence collection and handling, etc. (Solanke & Biasiotti, 2022).

According to Solanke and Biasiotti (2022), technology has a significant impact on digital forensics in four dimensions: technical, legal, organizational and educational. The technical dimension refers to the technical aspects of digital forensics, such as methods, tools, standards, etc. The legal dimension refers to the legal aspects of digital forensics, such as laws, regulations, policies, etc. The organizational dimension refers to the organizational aspects of digital forensics, such as roles, responsibilities, collaboration, etc. The educational dimension refers to the educational aspects of digital forensics, such as training, certification, accreditation, etc.

The authors argue that technology can affect each dimension positively or negatively. For example, technology can improve the technical dimension by providing new capabilities and functionalities for digital forensics. However, technology can also challenge the technical dimension by introducing new vulnerabilities and threats to digital forensics. Similarly, technology can affect other dimensions in different ways. Therefore, the authors suggest that digital forensic

practitioners should be aware of the impact of technology on digital forensics and adapt accordingly.

Use of Artificial Intelligence and Machine Learning in Digital Forensics

Another emerging trend in digital forensics is the use of artificial intelligence (AI) and machine learning (ML) in digital forensic analysis. AI and ML are branches of computer science that aim to create systems that can perform tasks that normally require human intelligence or learning. AI and ML can be applied to various domains and problems, such as natural language processing, computer vision, speech recognition, etc. (Solanke & Biasiotti, 2022).

AI and ML can also be applied to digital forensics to assist or automate various tasks or processes involved in digital forensic investigation. According to Solanke and Biasiotti (2022), AI and ML can be used in digital forensics for four main purposes: data mining, data analysis, data interpretation and data presentation. Data mining refers to the process of discovering useful and relevant information from large and complex datasets. Data analysis refers to the process of applying statistical or computational methods to examine and understand the data. Data interpretation refers to the process of drawing conclusions and inferences from the data. Data presentation refers to the process of communicating and visualizing the data and the results.

AI and ML can help digital forensic practitioners to perform these tasks more efficiently and effectively, by reducing human errors, biases and limitations, enhancing accuracy, speed and scalability, and providing new insights and perspectives (Solanke & Biasiotti, 2022). However, AI and ML also have some drawbacks and challenges for digital forensics, such as lack of transparency, explainability and accountability, ethical and legal implications, technical complexity and compatibility, etc. (Solanke & Biasiotti, 2022).

Cloud Computing and Its Challenges for Forensic Accountants

A third emerging trend in digital forensics is the increasing use of cloud computing and its challenges for forensic accountants. Cloud computing is a model of delivering computing services over the internet, such as storage, processing, networking, software, etc. (Mell & Grance, 2011). Cloud computing offers various benefits for users and providers, such as cost reduction, flexibility, scalability, reliability, etc. (Mell & Grance, 2011).

However, cloud computing also poses various challenges for digital forensics, especially for forensic accountants who need to access and analyze financial data stored or processed in the cloud. Some of these challenges include (Eide Bailly LLP, 2020):

i. Loss of control: Users of cloud services do not have direct control over their data or the infrastructure that hosts their data. This may limit or prevent their ability to collect or preserve digital evidence from the cloud.

ii. Data fragmentation: Data in the cloud may be distributed across multiple servers, locations or jurisdictions. This may complicate or hinder the identification or acquisition of relevant data for digital forensics.
iii. Data encryption: Data in the cloud may be encrypted by the users or the providers for security purposes. This may obstruct or delay the access or analysis of data for digital forensics.
iv. Data volatility: Data in the cloud may be dynamic or ephemeral, meaning that they may change or disappear over time. This may affect the integrity or availability of data for digital forensics.
v. Legal issues: Data in the cloud may be subject to different laws or regulations depending on where they are stored or processed. This may create conflicts or uncertainties regarding the ownership, privacy or admissibility of data for digital forensics.

Therefore, forensic accountants need to be aware of these challenges and adopt appropriate strategies and techniques to overcome them. For example, forensic accountants may need to collaborate with cloud service providers or other stakeholders to obtain access or cooperation for digital forensics. Forensic accountants may also need to use specialized tools or methods to collect, preserve and analyze data from the cloud. Forensic accountants may also need to follow the legal and ethical guidelines and standards for digital forensics in the cloud.

Challenges for Forensic Accountants in Digital Forensics

A final theme that emerged from the research findings is the challenges that forensic accountants face in digital forensics. Forensic accountants are professionals who apply their accounting knowledge and skills to assist in legal matters, such as fraud detection and prevention, dispute resolution, litigation support and expert testimony. Forensic accountants can work in various sectors, such as public accounting firms, law enforcement agencies, government agencies, corporations, non-governmental organizations and academia (Accounting.com, 2020).

However, forensic accountants also face various challenges and limitations in digital forensics, such as:

i. Rapidly evolving cyber threats and their complexity: Cyber threats are constantly changing and becoming more sophisticated and diverse, such as phishing, ransomware, malware, denial-of-service attacks, etc. (ITU, 2018). These threats can target individuals, businesses or governments and can cause significant financial losses and reputational damage. Forensic accountants need to keep abreast of the latest technologies and trends in cybercrime and digital forensics to cope with these threats.
ii. Encryption and anonymization techniques used by cybercriminals: Cybercriminals often use encryption and anonymization techniques to protect their identity and data from being traced or accessed by forensic accountants or other investigators. For example, cybercriminals may use encryption tools to encrypt their data or communications, or they may use anonymization tools such as Tor or VPN to hide their IP address or location

(GeeksforGeeks, 2020). These techniques can make it difficult or impossible for forensic accountants to collect or analyze digital evidence related to cybercrime.

iii. Legal and ethical issues in digital forensics investigations: Digital forensics investigations are subject to various legal and ethical issues that may affect the admissibility or reliability of digital evidence in court. For example, forensic accountants need to comply with the laws and regulations of different jurisdictions that may apply to the digital evidence they collect or analyze, such as privacy laws, data protection laws, intellectual property laws, etc. (Eide Bailly LLP, 2020). Forensic accountants also need to follow the ethical principles and standards of their profession, such as integrity, objectivity, confidentiality, competence, etc. (AICPA, 2017).

Therefore, forensic accountants need to enhance their knowledge and skills in digital forensics to overcome these challenges. Forensic accountants need to adopt a multidisciplinary approach that integrates accounting principles, theories and discipline with digital forensics methods and tools. Forensic accountants need to follow the best practices and guidelines for digital evidence collection, preservation, analysis and presentation. Forensic accountants need to collaborate and communicate effectively with other professionals involved in digital forensics investigations, such as law enforcement agencies, regulators, auditors, lawyers and judges, to share information, coordinate actions and provide support or advice.

Case Studies Analyses

This section presents two case studies and examples of digital forensic investigations, one illustrating a successful investigation and one illustrating a failed investigation.

Successful Digital Forensic Investigation: The BTK Killer

Perhaps the most famous case to be solved through digital forensics is that of the BTK Killer, Dennis Rader, with "BTK" referring to his MO of "bind, torture and kill." Rader enjoyed taunting police during his killing sprees in Wichita, KS. But this also proved to be his fatal flaw. A floppy disk Rader sent to the police revealed his true identity (Rasmussen University, 2019). Rader was a serial killer who murdered 10 people between 1974 and 1991. He sent letters to the media and the police, claiming responsibility for the killings and giving himself the nickname BTK. He also included clues and evidence from the crime scenes, such as photos, drawings and poems. He stopped communicating in 1979, but resumed in 2004, sending more letters and packages to the media and the police (Rasmussen University, 2019).

In one of his letters, Rader asked the police if they could trace a floppy disk. The police replied through a newspaper ad that they could not. Rader then sent a floppy disk to a local TV station, along with a letter and a gold necklace. The police examined the floppy disk and found a deleted Microsoft Word document that contained metadata linking it to Rader's church and his name (Rasmussen University, 2019).

The police then searched Rader's home and seized his computer and other evidence. They also matched his DNA to samples collected from the crime scenes. Rader was arrested in 2005 and confessed to all 10 murders. He pleaded guilty and was sentenced to life imprisonment without parole (Rasmussen University, 2019).This case shows how digital forensics can be used to identify and capture a serial killer who had eluded justice for decades. It also shows how digital evidence can be recovered from deleted or hidden files and how metadata can reveal crucial information about the origin and authorship of digital documents.

Failed Digital Forensic Investigation: The Murder of Connie Dabate

A case that illustrates the challenges and limitations of digital forensics is the murder of Connie Dabate in 2015. According to his arrest warrant, her husband Richard provided an elaborate explanation of the day's events, claiming that he returned home after receiving an alarm alert. Richard went on to claim that, upon entering his house, he was immobilized and tortured by an intruder who then shot Connie dead (The Conversation, 2017).

However, digital evidence from various sources contradicted Richard's story and exposed his lies. For example, data from Connie's Fitbit device showed that she was still alive and moving around the house after Richard claimed she was killed. Data from Richard's phone showed that he had texted his pregnant mistress shortly before Connie's death. Data from their home security system showed that Richard had disabled it before leaving for work that morning (The Conversation, 2017).

The police also found evidence of Richard's financial troubles, marital problems and extramarital affairs. They arrested him in 2017 and charged him with murder, tampering with evidence and making false statements. He pleaded not guilty and is awaiting trial (The Conversation, 2017).

This case shows how digital forensics can be used to uncover inconsistencies and discrepancies in a suspect's alibi or testimony. It also shows how digital evidence can be derived from various devices and platforms that record or store data related to a person's activities or interactions. However, it also shows how digital forensics can face legal and ethical issues, such as privacy rights, consent requirements, and data protection laws, that may limit or restrict the access or use of digital evidence in court.

CONCLUSION AND RECOMMENDATIONS

The findings of the study were organized into three themes: advancements in technology and their impact on digital forensics, the use of artificial intelligence and machine learning in digital forensics, and cloud computing and its challenges for forensic accountants. The research also presented two case studies and examples of digital forensic investigations, one illustrating a successful investigation and one illustrating a failed investigation.

Based on the research findings, the following recommendations are provided:

i. The study recommends that forensic accountants should keep abreast of the latest technologies and trends in cybercrime and digital forensics and update their knowledge and skills accordingly. Forensic accountants should also seek professional development opportunities, such as training, certification or accreditation, in digital forensics.
ii. The study recommends that forensic accountants adopt a multidisciplinary approach that integrates accounting principles, theories and discipline with digital forensics methods and tools. Forensic accountants should also use appropriate tools and techniques for collecting, preserving and analyzing digital evidence from various sources and platforms, such as mobile devices, social media, the internet of things, blockchain and many others.
iii. The study recommends that forensic accountants should follow the best practices and guidelines for digital evidence collection, preservation, analysis and presentation. Forensic accountants should ensure the integrity, reliability and admissibility of digital evidence in court. Forensic accountants should also comply with the laws and regulations of different jurisdictions that may apply to the digital evidence they collect or analyze.
iv. The study recommends that forensic accountants should collaborate and communicate effectively with other professionals involved in digital forensics investigations, such as law enforcement agencies, regulators, auditors, lawyers and judges, to share information, coordinate actions and provide support or advice. Forensic accountants should also establish trust and rapport with their clients and stakeholders.
v. The study recommends that forensic accountants should be aware of the challenges and limitations of digital forensics, such as encryption and anonymization techniques used by cybercriminals, legal and ethical issues in digital forensics investigations, technical complexity and compatibility of digital forensics tools and techniques, etc. Forensic accountants should also be prepared to overcome these challenges and limitations by using specialized tools or methods, seeking expert assistance or advice, or applying alternative strategies or solutions.

Reference

Accounting.com. (2020). Forensic accountant career overview. Retrieved from https://www.accounting.com/careers/forensic-accountant/

Accounting.com. (2020). Forensic accountant career overview. Retrieved from https://www.accounting.com/careers/forensic-accountant/

Accounting.com. (2023). Forensic accountant career overview. Retrieved from https://www.accounting.com/careers/forensic-accountant/

AICPA. (2017). Code of professional conduct. Retrieved from https://www.aicpa.org/research/standards/codeofconduct.html

AICPA. (2017). Code of professional conduct. Retrieved from https://www.aicpa.org/research/standards/codeofconduct.html

Carrier, B. (2005). A hypothesis-based approach to digital forensic investigations. In International Conference on Digital Evidence (pp. 3-15). IEEE.

Carrier, B., & Spafford, E. H. (2006). Getting Physical with the Digital Investigation Process. International Journal of Digital Evidence, 5(2), 1-20.

Casey, E. (2004). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.

Casey, E., & Backhouse, J. (2006). Introduction to Digital Forensics. In E. Casey (Ed.), Handbook of Computer Crime Investigation: Forensic Tools and Technology (pp. 1-14). Academic Press.

EC-Council. (2023). What is digital forensics | Phases of digital forensics? Retrieved from https://www.eccouncil.org/cybersecurity/what-is-digital-forensics/

Eide Bailly LLP. (2020). The relationship between forensic accounting and cybersecurity. Retrieved from https://www.eidebailly.com/insights/articles/2020/3/the-relationship-between-forensic-accounting-and-cybersecurity

Eide Bailly LLP. (2020). The relationship between forensic accounting and cybersecurity. Retrieved from https://www.eidebailly.com/insights/articles/2020/3/the-relationship-between-forensic-accounting-and-cybersecurity

Eide Bailly LLP. (2020). The relationship between forensic accounting and cybersecurity. Retrieved from https://www.eidebailly.com/insights/articles/2020/3/the-relationship-between-forensic-accounting-and-cybersecurity

FBI. (2021). 2020 Internet Crime Report Released. Retrieved from https://www.fbi.gov/news/pressrel/press-releases/2020-internet-crime-report-released

GeeksforGeeks. (2020). Challenges in digital forensics. Retrieved from https://www.geeksforgeeks.org/challenges-in-digital-forensics/

GeeksforGeeks. (2020). Challenges in digital forensics. Retrieved from https://www.geeksforgeeks.org/challenges-in-digital-forensics/

GeeksforGeeks. (2023a). Chain of custody - Digital forensics. Retrieved from https://www.geeksforgeeks.org/chain-of-custody-digital-forensics/

GeeksforGeeks. (2023b). Cyber forensics. Retrieved from https://www.geeksforgeeks.org/cyber-forensics/

Hinds, P.S., Vogel, R.J.,&Clarke Steffen, .(1997).The possibilities and pitfalls of doing a secondary analysis of a qualitative dataset. QualitativeHealthResearch,7(3),408-424.

LITU. (2018). Understanding cybercrime: Phenomena, challenges and legal response. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime_manual_may2018.pdf

ITU. (2018). Understanding cybercrime: Phenomena, challenges and legal response. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime_manual_may2018.pdf

ITU. (2023). Understanding cybercrime: Phenomena, challenges and legal response. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime_manual_may2023.pdf

Kaur, B., Sood, K., & Grima, S. (2023). A systematic review of forensic accounting and its contribution towards fraud detection and prevention. Journal of Financial Regulation and Compliance, 31(1), 1-23.

Legal Information Institute. (2023). Chain of custody. Retrieved from https://www.law.cornell.edu/wex/chain_of_custody

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

National University. (2021). Why Digital Forensics Is Important in Cybersecurity. Retrieved from https://www.national.edu/2021/07/14/digital-forensics-cybersecurity/

Oyedokun, G. E., Oyedokun, A. O., & Oyelami, O. M. (2023). Digital forensic accounting and cyber fraud in Nigeria. In 2023 International Conference on Cyber Management and Engineering (CyMaEn) (pp. 1-6). IEEE.

PwC. (2023). Forensic services. Retrieved from https://www.pwc.com/ng/en/services/advisory/forensic-services.html

Rasmussen University. (2019). Cracking cases with digital forensics. Retrieved from https://www.rasmussen.edu/degrees/justice-studies/blog/cracking-cases-with-digital-forensics/

Reith, M., Carr, C., & Gunsch, G. (2002). An examination of digital forensic models. International Journal of Digital Evidence, 1(3), 1-12.

Rogers, M. (2006). A new horizon in digital forensics: The rise of cyber forensics analysis. In Proceedings of the 39th Annual Hawaii International Conference on System Sciences (pp. 1-10). IEEE.

Scribbr. (2023a). Content analysis, Guide, methods & examples. Retrievedfromhttps://www.scribbr.com/methodology/content-analysis/

Scribbr. (2023b). What is a research design, Types, guide & examples? Retrieved from https://www.scribbr.com/methodology/research-design/

Solanke, A. A., & Biasiotti, M. A. (2022). Digital forensics AI: Evaluating, standardizing and optimizing digital evidence mining techniques. KI-Künstliche Intelligenz, 36, 143-161. https://doi.org/10.1007/s13218-022-00763-9

The Conversation. (2017). Cyber CSI: The challenges of digital forensics. Retrieved from https://theconversation.com/cyber-csi-the-challenges-of-digital-forensics-37902

The University of Wolverhampton. (2023). Secondary analysis. Retrieved from https://www.wlv.ac.uk/media/wlv/pdf/Secondary-analysis-JRN3815531.pdf