Intersection of Electronic Security and Digital Forensics: Data Protecting Techniques and Uncovering Data Clues

Norman Nelufule(✉), Boitumelo Nkwe, Daniel Shadung, Kele Masemola, Tanita Singano, Japhtalina Mokoena, Zamo Ngubane, and Ntombizodwa Thwala

Defence and Security Cluster, Council for Scientific and Industrial Research (CSIR), Information and Cybersecurity Centre (ICSC), Brummeria, Pretoria 0184, Republic of South Africa
nnelufule@csir.co.za

Abstract. With the current era of technology, protecting data and infrastructure has become more of a concern as sensitive information is being stored on Digital platforms. The various new technologies being developed make it harder to secure electronic data as malicious actors keep utilizing the latest tips and tools to perform attacks. These latest technologies also display gaps within digital forensics as there are not a lot of tools that can assist in the investigation of cyber incidents and properly preserve digital evidence after an incident has been detected. For example, as more individuals and organizations migrate their data and infrastructure to cloud platforms, new skills and forensic tools are required to extract evidence from the cloud. This study presents various electronic security measures and case studies of security breaches where the use of Digital Forensics assisted with the investigation and the subsequent results assisted the organization affected or educated other institutions to be aware of techniques used by malicious actors. Keeping abreast with the latest tools and techniques will ensure that effective security measures are implemented to prevent security breaches. The continuous adaptation in technologies will assist in ensuring that investigators are able to perform forensically sound.

Keywords: Digital Forensics · Digital Evidence · Data Protection · Electronic Security

1 Introduction

The Fourth Industrial Revolution (4IR) represents the current era of technological advances, that is characterized by the convergence of digital, physical, and biological technologies in producing, accessing, and managing big data. The evolution of industrial revolution technologies has a long history as depicted in Fig. 1. As we increasingly rely on the electronic systems to create and store sensitive information, data protection tools and systems becomes an integral part of safeguarding individuals' privacy, ensuring business continuity, maintaining national security, and fostering trust in the digital

A. Sere et al. (Eds.): AFRICOMM 2023, LNICST 587, pp. 351–367, 2025.
https://doi.org/10.1007/978-3-031-81570-6_23

world. At the intersection of electronic security and digital forensics, the 4IR has both advantages and disadvantages. The 4IR brings cutting-edge technologies like artificial intelligence (AI), machine learning (ML), and big data analytics, which can be exploited to develop more sophisticated and proactive cybersecurity solutions. These solutions can be deployed to detect patterns, detect anomalies, and predict the potential digital security breaches, thereby bolstering electronic security measures [1–3]. With advancements in digital forensics tools and techniques, organizations can investigate and analyze cyber incidents more efficiently. Digital forensics can also help in locating the source of a security breach, aiding in developing appropriate response strategies and mitigating future security risks.

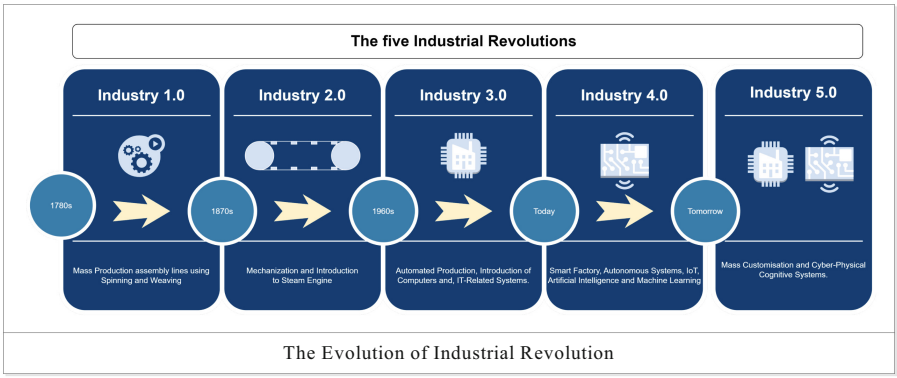

Fig. 1. The Illustration of the Evolution of Industrial Revolution.

Despite bringing advantages, the 4IR also enhances the capabilities of cyber attackers to develop more tools for security breaches. Cybercriminals can exploit advanced technologies to launch more sophisticated attacks, making it challenging to detect and respond to threats effectively [1, 4–11]. As the 4IR empowers defenders with tools and technologies, it also enhances the capabilities of cybercriminals. In [12], it was discussed that cybercriminals can exploit advanced technologies to launch more sophisticated and targeted attacks, making it challenging to detect and respond to threats effectively. [13] mentioned that cybercrimes suspects are also escaping traceability due to the anti-forensic tools that helps them to avoid detection.

The rapid pace of technological advances in the 4IR requires continuous training and upskilling for security professionals and digital forensic investigators [12, 13]. Maintaining expertise in emerging technologies can be resource-intensive for the organizations. Training and awareness are key components so that users of technology can understand the pros and cons of those technologies. Such training and awareness sessions should incorporate the legal aspects of cybersecurity, data breaches, cybercrimes, cyberlaws, and digital forensics to enhance knowledge and capability on how to legally deal with cyber incidents. This is important as electronic security and digital forensic can intersect during cyber incidents investigations and some cases may end up in court to litigate suspect. In [14], it was discussed that the intersection of electronic security and digital

forensics can raise complex legal and ethical questions, such as data ownership, chain of custody, and the use of artificial intelligence in decision making processes during digital forensics investigations. These are the main components that specialist should understand and master, since digital evidence acquired without following these crucial steps can be dismissed in a court law. This work aims to outline some of the advantages that are offered by enabling electronic security for the purpose of protecting data, detecting data clues, and enhancing the identification and extraction of digital evidence. This paper also aims to explore by means of systematic review, various electronic security measures and case studies of security breaches where the use of Digital Forensics assisted with the investigations. These concepts will cover the intersection of electronic security tools and digital forensic investigations. The remainder of this work is presented as follows: Sect. 2 presents the background of digital forensic, Sect. 3 presents the methodology adopted in this work, Sect. 4 presents the analysis and findings, and Sect. 5 presents the conclusion.

2 Background

In the 1940s, no one thought that computers can fall victims of cyber-attacks due to the size and complexity of the first working digital computing device tested in 1943 [15]. This computer was also referred to as monster machine, and access to this monster machine was limited and there was no network to connect two computers to each other. The notion of a computer virus was established way back in 1949 when John von Neumann realized that written computer program has a potential to reproduce themselves [15]. In the 1970s, the history of computer security was established during a research project that was gaining access to the internet and developing remote computer network access [15]. Around 1979, a 16-year-old Kevin Mitnick got arrested for hacking crimes that he has been committing for years [15]. In the year 1987, Andreas Luning and Kai Figge contributed to the first computer antivirus, leading to the birth of cybersecurity tools and electronic security [15]. Around 1996, after the world experienced the internet, many viruses began to surface with more sophisticated methods including polymorphism creating a new challenge for cybersecurity companies. Early 2000s after emailing and social media was established, cyber threats began to multiply [15].

Digital forensic emerged during the 1980s after the personal computers were introduced and they stated gaining popularity in the 1990s after the FBI hosted the first International Law Enforcement Conference on Computer Evidence in the United States [16]. Since the advent of 4IR, digital forensic has become a necessity and many countries do not have skills and expertise to combat the high rate of crimes as analyzed in [16–18] This historical background of cybercrimes and digital forensics can also be summarized as shown in Table 1.

2.1 Digital Forensic Techniques

Digital forensics procedure is described as the use of computing resources and the juristic investigative approaches to preserve, collect, and examine digitally acquired evidence [19]. This process demands that appropriate legal procedures are followed to ensure that

Table 1. Table of timelines in cybercrimes

Year of Event	Description of Event
1978	First cybercrime in Florida involving the unauthorized and erasure of data from a computing system. During these period cybercrimes were resolved according to the existing laws in the absence of federal laws of cybercrimes
1983–1984	Canada passed the legislation to deal with cybercrimes, the US also passed the Federal Computer Fraud and Abuse Act
1990–1992	UK passed the British Computer Misuse Act. First paper on cybercrime by Collier and Spaul
2002–2005	Best practices for computer forensic paper awarded to the Scientific Working group on Digital Evidence. ISO 1725 was published for the competence of testing and calibration laboratories
2005 and beyond	Various cybercrimes related regulations were discussed and adopted

there is legal search authority, chain of custody, use of validated digital forensic tools, repeatability, reporting, and potentially expert testimony in a court of law. The process is carried out by a digital forensic expert who is trained in the field and certified to use the required tools to produce credible digital evidence admissible in a court. According to the National Institute of Standards and Technology (NIST), the digital forensic investigation framework can be summarized graphically as in Fig. 2 [20]. In this figure, the process starts at evidence collection phase, then proceeds to examination phase which include, choice, the identification, and correlation subphases, from examination phase it proceeds to analysis phase which includes the construction and analysis of acquired evidence, the analysis phase is followed by the generated report. This process can also be repeated to ensure admissibility of digital evidence in court.

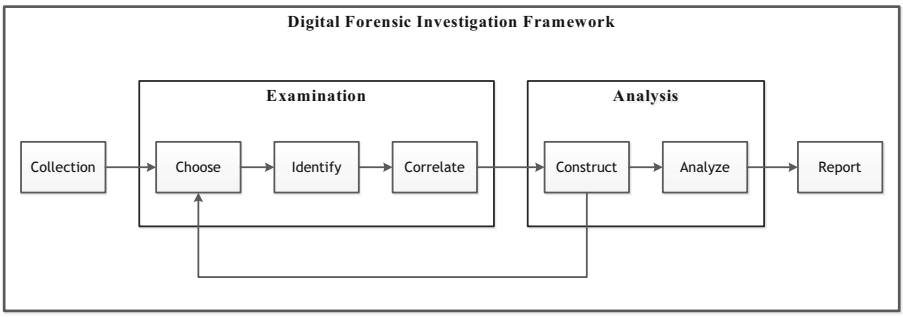

Fig. 2. An overview of Digital Forensic Investigation Process

The warrant of search in digital forensic investigation is a crucial step. In [17], the authors of the "Search and Seizure of Digital Evidence by Forensic Investigators in South Africa" looked at the digital forensics landscape from a South African perspective and identified that there are no set standards or procedures followed by cyber security

professionals. However, there are several international Digital forensics and international standards that digital forensics professionals can follow to ensure that their evidence is handled in a manner that can be admissible in court [17]. Some of the standards that were identified in the research paper are summarized in Table 2.

Table 2. Table of Summary of Digital Forensic Standards followed in South Africa

Standard	Description
Principles of the Association of Chief of Police Officers (ACPO)	In 1997, The ACPO drafted the "Good Practice Guide for Computer-Based Electronic Evidence". This guide outlines four principles for collecting and managing digital evidence • 1st Principle: Investigators should not alter data that may be used in court • 2nd Principle allows investigators to access original data only in exceptional situations and if they are competent to do so • 3rd Principle requires investigators to record all processes applied to digital evidence • 4th Principle requires investigators to follow all legal principles during the analysis of digital evidence
ISO 27037: Security Techniques	Guidelines for identification, collection, acquisition, and preservation of evidence. Digital forensic investigators should do the following: • Minimize the handling of original evidence • All actions taken should be documented • Any changes to the data should be accounted for • Local laws and regulations of evidence should be followed • Investigators should not take actions beyond their level of competence
The ISO/IEC DIS 27037	Standard specifies that all processes in digital forensic investigations should be auditable, repeatable, reproducible, and justifiable. This process has the following goals: • All processes and results should be able to be evaluated by independent forensic investigators • The same results should be obtained when the same procedures and methods are used • Digital forensic investigators should be able to validate all actions and methods used. All the recommended phases should be by investigators which are identification, collection, acquisition, and preservation of evidence • The ISO/IEC DIS 27037 The guidelines and procedures for incident investigations are outlined in the ISO/IEC 27043 Standard on Information Technology. Follows the principle of the Daubert test that states that test outlines factors to ensure the integrity of evidence, including that theories and techniques used by experts should have been tested, subjected to peer review, and enjoy widespread acceptance

The standards summarized in Table 2, guides the sequence of events that should be adhered to during digital evidence collection in cybercrime investigations.

2.2 The Role of Digital Forensic Investigation in Uncovering Clues

Digital forensics plays a critical role in investigating cyber incidents and uncovering clues to identify perpetrators [21–24]. This process entails collecting, preserving, and analyzing digital evidence that will help digital forensics experts to understand the nature and scope of cyberattacks, support legal actions against cybercriminals, and help organizations strengthen their cybersecurity defenses [13, 24–26]. Digital forensics is becoming a broad concept, with various types of forensic investigations involved. These types include but are not limited to mobile, computer, server, networks, emails, database, cloud, etc. some of the most well-known types of digital forensic are depicted in Fig. 3. It is important for someone who intends to be a certified digital forensic examiner to master at least all the types listed below as these are the most useful types of forensics used to uncover digital clues during a cyber incident investigation.

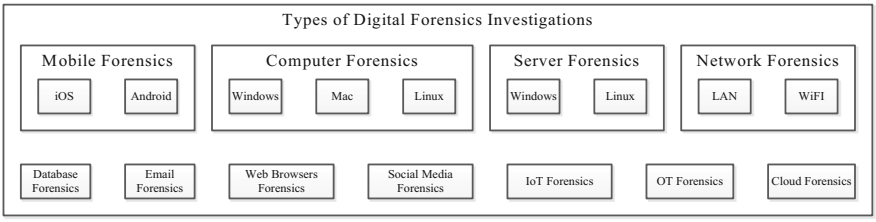

Fig. 3. An overview of the main types of Digital Forensics

Evidence Collection and Preservation

Digital forensic investigations require swift collection and preservation of digital evidence from affected systems and networks to ensure that it remains unaltered and credible. This process involves forensic imaging of storage media, capturing network traffic and maintaining the chain of custody to ensure the admissibility of evidence in legal proceedings [27–33].

Chain of custody is described as the method of tracking, managing, and preserving the timeline and chronological order of how digital evidence is handled by forensics experts during an investigation [34]. The purpose of this process is to ensure that the integrity of the evidence in question is not tampered with by a person who is not authorized to handle any case or incident-related evidence. The evidence must be preserved to ensure its admissibility in a court of law. When there is insufficient documentation in the chain of custody report, the evidence runs the risk of being deemed inadmissible in a court of law.

Cyber Incident Analysis
Digital forensics experts examine the preserved evidence to construct the sequence of events leading up to and during the cyber incident. They conduct network forensics to retrieve network logs from firewalls and packet tracers and use them to trace and analyze packets. Database logs are also used to view all database transactions that took place. From the Wireless forensics, wireless traffic can be collected and analyzed to retrieve any anomalies on the traffic. Data can be captured through continuous monitoring, during an attack or from captured log data. On the Memory forensics, a lot of information can be gathered from temporary storage such as usernames and passwords.

From the Email forensics, email headers can be used to investigate the email origin, server hopes and its destination, and Malware forensics can also be conducted and analyzed to determine its origin and impact.

This analysis of digital evidence can uncover digital clues, indicators and patterns that may link the attack to specific threat actors. Further analysis may often involve collaboration with intelligence agencies and international partners such as Interpol and other agencies to pursue criminals outside the national jurisdiction area.

Legal Support
Digital forensics findings often serve as critical evidence in legal proceedings. Investigators are expected to present their findings in a clear, reliable, and concise manner that can be understood by legal professionals and the courts to institute criminal prosecution of alleged cybercriminals [14, 22, 35]. This process will also undergo severe cross-examination by the defense council.

Incident Response Improvement
Understanding how the incident occurred and the techniques used by attackers can guide organizations in strengthening their security posture to prevent similar incidents in the future by studying past incidents, security professionals can identify trends, emerging threats, and vulnerabilities to better prepare for future attacks.

Data Recovery
In some cases, cyber incidents may result in data loss or data manipulation. Digital forensics can assist in recovering lost or altered data, which is especially important in cases involving ransomware attacks or data breaches. In a ransomware attack, the attacker encrypts the data and renders it unusable and demand ransom in bitcoin before they decrypt the data, however digital forensic tools can recover the encryptions that can be used to decrypt the data.

3 Methodology

This work adopts a systematic review approach based on cybersecurity incidents related to the South African landscape and beyond as guided by [36–41]. The detail of the proposed approach includes framing, literature searches and assessment. The research materials and literatures data were collected from IEEE Explore, Web of Science and Scopus indexing databases. In addition to these materials, reports and cases were also

used to assess some of the digital forensic technologies adopted and used in some of the successful cases in South Africa. The impact of the exposure of vulnerable systems such as financial institutions and metropolitans were discussed. The role of digital forensics in pursuing and arresting perpetrators has been explained and presented in a tabular form.

3.1 Scoping

The scope of focus on this article includes literature related to electronic security technologies, electronic evidence, digital forensic investigations, and any other combination of electronic security and digital forensics.

3.2 Framing

The rapid advancements in technology have created security gaps that cybercriminals can exploit to launch sophisticated attacks. This has created a need for cybersecurity and digital forensic specialists to constantly update their security and investigation tools to keep up with the attacks. This study uses systematic review to highlight some of the security measures that have been effective in preventing cyberattacks. Furthermore, real-world cases where digital forensics was instrumental in successfully bringing perpetrators to book are presented.

3.3 Literature Search and Assessment

This study used IEEE Explore, Web of Science and Scopus indexing databases to collect data. The search strings used were: "electronic security measures" OR "electronic security tools" OR "data breaches in South Africa". The first step was to filter out irrelevant papers by looking at the keywords from the paper titles. Paper abstracts were then read to identify relevant papers and discard irrelevant ones. Once all the irrelevant papers were filtered out, full text reading of the remaining papers was done.

4 Discussion, Analysis and Findings

4.1 Electronic Security Measures

There are various electronic security measures that are employed to protect data and information systems from unauthorized access, data breaches, and cyberattacks. These measures aim to ensure that there is data confidentiality, data integrity, and data availability regularly. Some of the essential electronic security measures used to safeguard data and information systems are summarized in Table 3.

In 2016, Standard Bank faced a cyber-attack in which cybercriminals attempted to steal funds by targeting the bank's internal systems. However, due to the bank's robust electronic security measures in place, including multi-factor authentication, anomaly detection, and real-time security monitoring and incidence response, the attackers' attempts were thwarted. The security measures in place helped identify and block suspicious transactions, preventing cybercriminals from gaining unauthorized access to customer accounts and sensitive data [20].

In 2018, First National Bank (FNB), also faced a phishing attack where cybercriminals attempted to deceive customers into disclosing their login credentials and personal information. FNB's strong electronic security measures, including email filtering, spam detection, and user awareness, helped the bank to detect and block the phishing emails before they reached a significant number of customers. This proactive approach prevented potential data breaches and protected customers from falling victim to the scam [20].

Table 3. Table of Summary of Electronic Security Measures

Data Security Measure	Description
Firewalls	The barrier between an organization internal network and external internet that monitors, and controls incoming and outgoing network traffic based on policies
Patch Management	The application of regular software updates and patches for addressing known security vulnerabilities in operating systems, applications, and other related software
Encryption	The conversion of data into a coded format that can only be deciphered with a unique encryption key
Backup and Disaster Recovery	The process of continuous data backups to ensure that data is available in case of data loss due to cyber incidents or hardware failures
Multi-Factor Authentication (MFA)	Demands the user to provides multiple forms of identification before gaining access to a system or data
Physical Security Measures	This is controlled access to data centers and server rooms, video surveillance, and environmental controls. It complements electronic security to protect the physical infrastructure hosting information systems
Security Monitoring and Incidence Response	Deploying of security monitoring tools to allow the organization to detect and respond to security incidents promptly, minimizing the impact of potential data breaches

4.2 Digital Forensics Success Cases in South Africa and Abroad

There are several successful cases wherein perpetrators were found and charged, and some of the money recovered. However, the success rate is very low compared to the high

rise of cybercrimes incident reported annually. South Africa is currently rated number six (6) in the world in terms of cybercrimes incidents (Table 4).

Table 4. Summery of Cases Solved Using Digital Forensics

Digital Forensic Case	Description
Swift Banking System Attacks (2016) [42]	Society for Worldwide Interbank Financial Telecommunication (SWIFT) experienced cyberattacks targeting the messaging system used for international financial transactions. The insights gained from digital forensic analysis helped financial institutions identify and mitigate the risks associated with similar attacks, leading to strengthened security measures within the global financial community
VBS Mutual Bank Heist (2018) [43]	Venda Building Society (VBS) Mutual Bank in South Africa experienced a high-profile cyber heist where cybercriminals siphoned off millions of rands from the bank's systems. The investigation into the incident involved a collaboration between law enforcement agencies and digital forensics experts. The analysis of all the digital evidence, including network logs and communication trails, investigators were able to trace the stolen funds back to specific individuals involved in the heist. Subsequently, several suspects were arrested and prosecuted for their roles in the cyber-attack
Orion Data Leak (2019) [44]	Millions of South Africans' personal information was exposed in a data leak event involving the business Orion in 2019. Working closely with law enforcement and digital forensics teams, the South African Banking Risk Information Centre (SABRIC), a banking sector group dedicated to combating cybercrime, investigated the incident. The cybercriminals responsible for the data leak were found and caught through thorough analysis of digital evidence and collaboration with international partners, which resulted in their successful prosecution

(*continued*)

Table 4. (*continued*)

Digital Forensic Case	Description
Experian Data Breach (2020) [45]	In 2020, Experian, a global credit reporting company with operations in South Africa, experienced a data breach that affected millions of South African citizens. The breach occurred when a suspected fraudster posed as a legitimate client and obtained access to Experian's database. The attacker then stole personal information, including names, identification numbers, and contact details of individuals. Experian promptly disclosed the breach and worked with law enforcement agencies to investigate the incident. This breach underscored the importance of protecting vast databases containing sensitive personal information

4.3 Convergence of Electronic Security and Digital Forensics

The nature of electronic security and digital forensics was outlined in detail in [46], as building a cybersecurity program that comprises of the following levels: *Architecture, Passive defense, active defense, intelligence and offensive.* The purpose of these levels is to ensure that the implemented security controls to prevent low level incidents from occurring in an operational environment. In the case of an incident taking place within an environment, then the organization will have to initiate incident response steps which are defined as an approach that handles and manages the state of the system after it was infiltrated and containing the environment with the hope of recovering it to its pre infiltration state. How Digital forensics can be used within the scope of cybersecurity is investigating crimes and internal policy, violations, reconstructing security incidents, troubleshooting operational problems, and recovering from accidental system damage. The following are goals of Digital Forensics Incident response (DFIR) in the cybersecurity space:

- Swift and effective in responding to security events.
- Investigate incidents with a systematic procedure.
- Minimize damage to the organization including preventing data loss, protecting systems, mitigating business disruption, and reducing compliance risks.
- Recover rapidly and complete from security incidents by Identifying the root cause, eradicating the threat across all organizational systems.
- Facilitate the effective prosecution of attackers by law authorities and provide evidence for legal actions taken by the organization.

4.4 Emerging Threats and the Need to Stay Ahead of Cybercriminals

Emerging threats in the cybersecurity landscape present significant challenges to organizations and individuals alike. Cybercriminals continually evolve their tactics, techniques, and procedures (TTPs) to exploit vulnerabilities and evade traditional security measures.

To effectively combat these threats, continuous innovation and adaptation are essential to stay ahead of cybercriminals. Table 5 summarizes these emerging threats and how they can be tackled.

Table 5. Table of Emerging Threats

Threat Type	Solution
Changing Technology	The technology landscape is continuously evolving with the introduction of new devices, applications, and services. Each new advancement brings its own set of security challenges. To address these evolving threats, cybersecurity professionals must constantly update their knowledge and adapt their strategies to protect against emerging risks
Nation-State Threats	State-sponsored cyberattacks pose significant challenges as they are highly organized, well-funded, and persistent. To counter nation-state threats, continuous innovation is vital to develop advanced threat intelligence, strengthen defense mechanisms, and promote international collaboration
AI threats attacks	Cybercriminals leverage AI to automate attacks, evade detection, and personalize phishing campaigns. Cybersecurity professionals must innovate by incorporating AI into their defense strategies to proactively detect and respond to AI-powered threats
Zero Day Exploits	Zero-day vulnerabilities, unknown to vendors, are lucrative for cybercriminals. They can exploit these vulnerabilities before patches are available and remain hidden

4.5 Challenges and Future Directions

The rapid growth in the development of generative artificial intelligence tools also has a negative impact on the cybersecurity field. Criminals can now create more sophisticated malware that can be very difficult to detect. Social media companies are also upgrading their security features, mobile companies are also not left behind in upgrading the security features. Some of the main challenges and future suggestions are listed in Table 6.

Table 6. Table of Challenges and Future Directions

Digital Forensic Type	Description of Challenges
Cloud Forensic	Security has been upgraded in some of the cloud applications, with multi-factor authentication required to gain access to the cloud data. Digital forensic specialists should explore more tools to uncover the keys to unlock the multi-factor authentication
Sophisticated Cyber threats	Cyber criminals are always ahead of cybersecurity and digital forensic specialists. With the advent of technology, cybercriminals are now able to use Artificial Intelligence tools to develop more sophisticated malware. This means that cyber specialists and digital forensic examiners should always improve their knowledge and tools
Data Privacy and Legal Concerns	Digital forensics involves handling sensitive data which raises privacy concerns and legal challenges related to data protection, and chain of custody [47]. Investigators should navigate through acceptable legal frameworks and ensure that they comply with privacy regulations during their investigation process
Encryption and Anonymization	The growing use of encryption and anonymization techniques by cybercriminals hinders digital forensics investigations. The continuous use of dark web computers makes it difficult for investigators to identify the suspects
Lack of Skilled Personnel	Adequate funding, skilled personnel, and training are essential to ensure effective cybersecurity and digital forensics capabilities
International Collaboration	Cybercrime investigation often transcends national borders, and this requires international collaboration among law enforcement agencies and digital forensics teams. Differing legal jurisdictions, lack of consulate relationships, and challenges in sharing evidence can impede investigations

5 Conclusion

The advantages of utilizing Digital Forensics when handling cyber incidents were stated as there is a correlation with the security of electronic data and digital forensics due to the constant development of technologies in the current era. Various security measures that can be implemented to prevent security breaches, cyberattacks and unauthorized access to certain data were addressed. There is a direct correlation between Digital forensics and incident response and as such collaboration between security professionals and Forensics investigators is necessary to solve incidents that occur in the environment effectively. Securing electronic data and the use of Digital Forensics in investigating and resolving an incident is presented in this paper.

Various case studies were used to display the impact of effective implementation of security measures to prevent breaches and preserve evidence for investigation once an incident has been detected, these case studies helped provide awareness to educate other institutions or individuals about some of the methods used by malicious actors. Challenges with Security and Forensics were presented, and future works included the advancement and adaptation of these techniques and technologies for users and organizations to implement effective controls to secure their data and for investigators in Forensics to develop the skills necessary to preserve, analyze and document electronic evidence obtained. Continued research and understanding of the latest technologies are the only way to stay abreast of what is going on as technology evolves and understanding how to effectively deal with each technology or incident that may occur.

References

1. Renold, A.P.: Survey of evidence collection methods for Internet of Things forensics. In: Proceedings of the 1st IEEE International Conference on Networking and Communications 2023, ICNWC 2023. Institute of Electrical and Electronics Engineers Inc. (2023). https://doi.org/10.1109/ICNWC57852.2023.10127407
2. Castiglione, A., Cattaneo, G., De Maio, G., De Santis, A., Roscigno, G.: A novel methodology to acquire live big data evidence from the cloud. IEEE Trans Big Data **5**(4), 425–438 (2019). https://doi.org/10.1109/TBDATA.2017.2683521
3. Choo, K.-K.R., Esposito, C., Castiglione, A.: Evidence and forensics in the cloud: challenges and future research directions. IEEE Cloud Comput. **4**(3), 1–6 (2017)
4. Li, S., Qin, T., Min, G.: Blockchain-based digital forensics investigation framework in the Internet of Things and social systems. IEEE Trans. Comput. Soc. Syst. **6**(6), 1433–1441 (2019). https://doi.org/10.1109/TCSS.2019.2927431
5. Tiwari, A., Mehrotra, V., Goel, S., Naman, K., Maurya, S., Agarwal, R.: Developing trends and challenges of digital forensics. In: 2021 5th International Conference on Information Systems and Computer Networks, ISCON 2021. Institute of Electrical and Electronics Engineers Inc. (2021). https://doi.org/10.1109/ISCON52037.2021.9702301
6. Silvarajoo, V.R., Yun Lim, S., Daud, P.: Digital evidence case management tool for collaborative digital forensics investigation. In: 2021 3rd International Cyber Resilience Conference, CRC 2021. Institute of Electrical and Electronics Engineers Inc., January 2021. https://doi.org/10.1109/CRC50527.2021.9392497
7. Lee, S., Kim, H., Lee, S., Lim, J.: Digital evidence collection process in integrity and memory information gathering. In: First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE 2005), Taipei, Tawan. IEEE, February, pp. 1–12 (2005)
8. Bennett, D.: The challenges facing computer forensics investigators in obtaining information from mobile devices for use in criminal investigations. Inf. Secur. J. **21**(3), 159–168 (2012). https://doi.org/10.1080/19393555.2011.654317
9. Maheswari, K.U., Shobana, G.: The state of the art tools and techniques for remote digital forensic investigations. In: 2021 3rd International Conference on Signal Processing and Communication, ICPSC 2021, pp. 464–468. Institute of Electrical and Electronics Engineers Inc., May 2021. https://doi.org/10.1109/ICSPC51351.2021.9451718
10. Pourvahab, M., Ekbatanifard, G.: Digital forensics architecture for evidence collection and provenance preservation in IaaS cloud environment using SDN and blockchain technology. IEEE Access **7**, 153349–153364 (2019). https://doi.org/10.1109/ACCESS.2019.2946978

11. Hemanth, J., Pelusi, D., Chen, J.I.-Z. (eds.): Intelligent Cyber Physical Systems and Internet of Things. Engineering Cyber-Physical Systems and Critical Infrastructures, vol. 3. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-18497-0
12. Li, K.-C., Gupta, B.B., Agrawal, D.P.: Recent Advances in Security, Privacy, and Trust for Internet of Things (IoT) and Cyber-Physical Systems (CPS), 1st edn. CRC Press, Parkway (2021)
13. Yaacoub, J.P.A., Noura, H.N., Salman, O., Chehab, A.: Advanced digital forensics and anti-digital forensics for IoT systems: techniques, limitations and recommendations. Internet Things **19** (2022). https://doi.org/10.1016/j.iot.2022.100544
14. Van Nguyen, T., Truong, T.V., Lai, C.K.: Legal challenges to combating cybercrime: an approach from Vietnam. Crime Law Soc. Change **77**(3), 231–252 (2022). https://doi.org/10.1007/s10611-021-09986-7
15. Chadd, K.: The history of cybercrime and cybersecurity, 1940–2020. Cybercrimes Mag., 1–5 (2020). https://cybersecurityventures.com/the-history-of-cybercrime-and-cybersecurity-1940-2020/
16. Pieterse, H.: The cyber threat landscape in south africa: a 10-year review. Afr. J. Inf. Commun. **28** (2021). https://doi.org/10.23962/10539/32213
17. Nortjé, J., Myburgh, D.C.: Forensic investigators in South Africa. PER/PELJ **2019** (2019). https://doi.org/10.17159/1727
18. Van Niekerk, B.: An analysis of cyber-incidents in South Africa. Afr. J. Inf. Commun. (AJIC) (20) (2017). https://doi.org/10.23962/10539/23573
19. Avoine, G., Hernandez-Castro, J.: Security of Ubiquitous Computing Systems: Selected Topics. Springer, Cham (2021).https://doi.org/10.1007/978-3-030-10591-4.
20. Dimitriadis, A., Ivezic, N., Kulvatunyou, B., Mavridis, I.: D4I - digital forensics framework for reviewing and investigating cyber attacks. Array **5**, 100015 (2020). https://doi.org/10.1016/j.array.2019.100015
21. Pollitt, M., Caloyannides, M., Novotny, J., Shenoi, S.: Digital forensics: operational, legal and research issues. In: De Capitani di Vimercati, S., Ray, I., Ray, I. (eds.) Data and Applications Security XVII. IFIPIFIP, vol. 142, pp. 393–403. Springer, Boston (2004). https://doi.org/10.1007/1-4020-8070-0_28
22. Nance, K., Ryan, D.J.: Legal aspects of digital forensics: a research agenda. In: Proceedings of the 44th Hawaii International Conference on Systems and Sciences, Kauai, HI, USA. IEEE, February 2011
23. Yaacoub, J.-P.A., Noura, H.N., Salman, O., Chehab, A.: Digital forensics vs. anti-digital forensics: techniques, limitations and recommendations, March 2021. http://arxiv.org/abs/2103.17028
24. Jansen, A.: Digital records forensics: ensuring authenticity and trustworthiness of evidence over time. In: 5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010, pp. 84–88. IEEE Computer Society (2010).https://doi.org/10.1109/SADFE.2010.20.
25. Horsman, G., Lyle, J.R.: Dataset construction challenges for digital forensics. Forensic Sci. Int. Digit. Investig. **38** (2021). https://doi.org/10.1016/j.fsidi.2021.301264
26. Casino, F., et al.: Research trends, challenges, and emerging topics in digital forensics: a review of reviews. IEEE Access **10,** 25464–25493 (2022). https://doi.org/10.1109/ACCESS.2022.3154059
27. Chow, K.P., et al.: Digital evidence search kit. IEEE, Taipei, Taiwan (2005)
28. Dewald, A.: Characteristic evidence, counter evidence and reconstruction problems in forensic computing. In: Proceedings - 9th International Conference on IT Security Incident Management and IT Forensics, IMF 2015, pp. 77–82. Institute of Electrical and Electronics Engineers Inc., August 2015. https://doi.org/10.1109/IMF.2015.15

29. Yadav, D., Mishra, M., Prakash, S.: Mobile forensics challenges and admissibility of electronic evidences in India. In: Proceedings - 5th International Conference on Computational Intelligence and Communication Networks, CICN 2013, pp. 237–242 (2013). https://doi.org/10.1109/CICN.2013.57
30. Zhao, Z.: A framework to analyze reliability of digital evidences in computer systems. In: Proceedings - 2015 6th International Conference on Intelligent Systems Design and Engineering Applications, ISDEA 2015, pp. 21–25. Institute of Electrical and Electronics Engineers Inc., April 2016. https://doi.org/10.1109/ISDEA.2015.15
31. Moussa, A.F.: Electronic evidence and its authenticity in forensic evidence. Egypt. J. Forensic Sci. **11**(1) (2021). https://doi.org/10.1186/s41935-021-00234-6
32. Azemović, J., Mušić, D.: Methods for efficient digital evidence collecting of business processes and users activity in eLearning environments. In: IC4E 2010 - 2010 International Conference on e-Education, e-Business, e-Management and e-Learning, pp. 126–130 (2010). https://doi.org/10.1109/IC4E.2010.92
33. Nikkel, B.J.: Improving evidence acquisition from live network sources. Digit. Investig. **3**(2), 89–96 (2006). https://doi.org/10.1016/j.diin.2006.05.002
34. Alenezi, A., Atlam, H.F., Alsagri, R., Alassafi, M.O., Wills, G.B.: IoT forensics: a state-of-the-art review, challenges and future directions. In: COMPLEXIS 2019 - Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk, pp. 106–115. SciTePress (2019). https://doi.org/10.5220/0007905401060115
35. Khan, A., Wiil, U.K., Memon, N.: Digital forensics and crime investigation: legal issues in prosecution at national level. In: 5th International Workshop on Systematic Approaches to Digital Forensic Engineering, SADFE 2010, pp. 133–140 (2010).https://doi.org/10.1109/SADFE.2010.8
36. Schryen, G.: Writing qualitative is literature reviews—guidelines for synthesis, interpretation, and guidance of research. Commun. Assoc. Inf. Syst. **37**, 286–325 (2015). https://doi.org/10.17705/1cais.03712
37. Kitchenham, B., Pearl Brereton, O., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering - a systematic literature review. Inf. Softw. Technol. **51**(1), 7–15 (2009). https://doi.org/10.1016/j.infsof.2008.09.009
38. Oosterwyk, G., Brown, I., Geeling, S.: A synthesis of literature review guidelines from information systems journals. Kalpa Publ. Comput. **12**, 250–260 (2019)
39. Khan, K.S., Kunz, R., Kleijnen, J., Antes, G.: Five steps to conducting a systematic review. J. R. Soc. Med. **96**, 118–121 (2003). http://www.ncbi.nlm.nih.gov/entrez/query/
40. Siddaway, A.P., Wood, A.M., Hedges, L.V.: How to do a systematic review: a best practice guide for conducting and reporting narrative reviews, meta-analyses, and meta-syntheses. Annu. Rev. Psychol. **70**, 747–770 (2019). https://doi.org/10.1146/annurev-psych-010418
41. Okoli, C.: A guide to conducting a standalone systematic literature review. Commun. Assoc. Inf. Syst. **37**, 1–33 (2015). http://aisel.aisnet.org/cais/vol37/iss1/43
42. Michelle Liu, X.: A risk-based approach to cybersecurity: a case study of financial messaging networks data breaches. Coast. Bus. J. **18**(1) (2021)
43. Motau, T.: The Great Bank Heist Investigator's Report to the Prudential: Venda Building Society (VBS), Johannesburg (2018)
44. Orion, P.: Complainant versus orion pharmaceutical email and website. Code Pract. Rev., 1–4 (2020)

45. Experian ® Data Breach Resolution: Data Breach Industry Forecast 2020, Johannesburg (2020)
46. Salfati, E., Pease, M.: Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT) (2022). https://doi.org/10.6028/NIST.IR.8428
47. Moabalobelo, T., Ngobeni, S., Molema, B., Phantsi, P., Dlamini, M., Nelufule, N.: Towards a privacy compliance assessment toolkit. In: IEEE IST-Africa Conference Proceedings, Pretoria, South Africa, pp. 1–8. IEEE, May 2023