APPLICATION OF DIGITAL FORENSICS IN CYBERCRIME INVESTIGATIONS: THEORETICAL FRAMEWORK

Inda Kreso
Faculty of Criminal Justice, Criminology and Security Studies University of Sarajevo, Bosnia and Herzegovina, indakreso@fkn.unsa.ba

Abstract: Crime evolves in accordance with contemporary trends, particularly those associated with technological advancements. As technology progresses, criminal activity likewise adapts, with cybercrime as a prominent illustration of this phenomenon. Given the persistent rise in cybercrime, including hacking, identity theft, and ransomware attacks, our responses must be equally robust and effective. Investigating cybercrime presents significant challenges. Despite advancements in technology, the difficulties surrounding cybercrime investigations continue to evolve. Digital forensics is a valuable tool for investigating cybercrime. The tools used in digital forensics can significantly improve the effectiveness of these investigations. Literature suggests using digital forensics methodology and tools to enhance the identification, collection, and preservation of digital evidence in cybercrime investigations, improving the accuracy and reliability of the investigations. This paper undertakes a literature review as its methodological framework to illustrate that integrating digital forensics in the investigation phase may significantly enhance the effectiveness of cybercrime investigations. The prevalence of cybercrime is a significant issue in modern society. Criminology, as a scientific discipline, must consistently and actively study the phenomenon of cybercrime. Technology is advancing at a rapid pace, making it essential to stay updated with the latest trends to effectively combat cybercriminals. The academic community recognizes digital forensics as a crucial research area. Nonetheless, a gap remains that calls for new studies focusing on the significance of thorough investigations into cybercrime. Existing literature indicates that there is no universally accepted definition of cybercrime. A common approach in defining cybercrime involves identifying the key concepts and terms relevant to cybercrime investigations. To accurately define cybercrime, literature suggests classifying it into five categories: unauthorized access to computer data and systems, unauthorized interception of data confidentiality, interference with data and systems, and computer-related forgery and fraud. Additionally, offenses such as child pornography and violations of copyright rights are considered as cybercrime. These categories collectively encapsulate the various facets of cybercrime. It is crucial to differentiate between pure cybercrime and crime facilitated by cyberspace. This paper will investigate pure cybercrime and apply digital forensics within that context. Pure cybercrime, or cyber-dependent crimes, can only be committed through computers, computer networks, and other information communication technology. This includes spreading viruses and malware, hacking, and launching distributed denial-of-service (DDoS) attacks. It is crucial to emphasize that pure cybercrime is directed against computers and computer networks. On the other hand, cyber-enabled crimes have been increasing in recent years due to the widespread use of computers, computer networks, and other forms of information technology. Unlike pure cybercrime, which solely relies on information technology, cyber-enabled crimes can also occur without using such technology, including traditional fraud and theft. While cyber fraud and theft can be perpetrated in a digital environment, they are not inherently dependent on information technology. Investigating cybercrime is a complex task. A skilled hacker or cybercriminal is the opposite of a cybercrime investigator, which adds to the challenges of cybercrime investigation. Digital forensics refers to the practice of identifying, recovering, and analyzing electronic data in order to unveil and interpret crucial information. Its primary objective is to preserve the integrity of evidence, ensuring it remains in its original condition. This process entails a thorough and systematic investigation, which includes the collection, identification, and validation of digital information to accurately reconstruct previous events. Digital forensics has emerged as an indispensable tool in the investigation of crimes, particularly in relation to cybercrime and therefore it is very important to research application of digital forensics in cybercrime investigations.
Keywords: cybercrime, investigation, digital forensics, digital evidence preservation

1. INTRODUCTION

Utilizing digital forensics methods and tools has become a common approach in investigating crimes. This is particularly crucial in cybercrime investigations. Digital forensics tools are highly effective, enabling easier, more efficient, and secure identification, collection, and preservation of digital evidence that is essential in cybercrime investigations. Using digital forensics in cybercrime investigations ensures accuracy and reliability (Adedayo M. Balogun & Tranos Zuva, 2018; Arshad et al., 2018; Ayotunde, 2022; Brown, 2015; Chen & Dong, 2023; Da-Yu Kao et al., 2018; Ding, 2025; Eboibi, 2020). The most crucial component in digital investigation is digital evidence,

and all digital forensics tools are utilized to collect, preserve, or analyze this evidence. Digital evidence refers to data obtained from digital devices, such as computers, smartphones, servers, storage media, or network systems, that is used in legal investigations to prove criminal activities (Batista et al., 2023; Billard, 2018; Bonomi et al., 2020; Da-Yu Kao et al., 2018; Jain & Sonowal, 2025; Patil et al., 2021; Wu et al., 2019; Yunianto et al., 2019).The primary focus of a digital investigation is to maintain the integrity of digital evidence in its original state, ensuring that it remains untampered during the collection and subsequent investigation processes. It is essential to ensure that digital forensics techniques effectively identify, collect, and preserve digital evidence in cybercrime investigations, thereby enhancing the overall accuracy and reliability of these investigations. Investigating cybercrime is challenging and requires personnel with a unique set of skills. When conducted correctly, a cybercrime investigation is the most effective tool against cybercrime. Investigating cybercrime presents unique challenges and complexities. Unlike other crime investigations, it often requires specialized software for collecting, storing, and analyzing digital evidence. Methods, concepts, and tools of digital forensics in cybercrime investigations significantly enhance the preservation of digital evidence for court proceedings. Digital forensics plays a crucial role in enhancing the overall effectiveness of investigations, fostering positive outcomes while ensuring that the processes are both credible and trustworthy. By employing sophisticated techniques and methodologies, it provides a thorough examination of digital evidence, which significantly contributes to the integrity of the investigative process (Alotaibi et al., 2023; Bhat et al., 2021; Dubey et al., 2023; Ekuma & Fon, n.d.; Gorda & Chechulin, 2023; Horan & Saiedian, 2021; Nouh et al., 2019; J. J. Oerlemans, 2017; J.-J. Oerlemans & Galič, n.d.; Sikos, 2021). The most crucial aspect of any crime investigation is evidence. In the case of cybercrime investigations, this evidence exists in digital form. Therefore, one of the most important steps in the investigative process is to preserve the data evidence that has been identified and collected from electronic devices (Arshad et al., 2018; Kreso, 2025). One of the primary challenges in digital forensics is the collection and extraction of digital evidence necessary for investigations. This digital evidence is vital for identifying the criminals who commit cybercrimes. Literature indicates that digital forensics techniques facilitate the secure identification, collection, and preservation of digital evidence during the investigation phase. Authors argue that proper evidence collection techniques used in digital forensics guarantee better preservation of the digital evidence in the investigation phase (Alotaibi et al., 2023; Du et al., n.d.; Hamid Lone & Naaz Mir, 2017; Horsman, 2019; Lone & Mir, 2019; Maratsi et al., 2022; Mohammed et al., 2019; Page et al., 2019; Scholarworks & Beardall, 2023; van Beek et al., 2020). The literature indicates that disk imaging aids cybercrime investigators in creating forensic copies (disk images) to prevent data loss or modification. Disk imaging is a key technique for ensuring the preservation of digital data during the identification and collection phase of the investigation process. Using disk images instead of working directly on the original data ensures that the original data remains unaltered and intact. Typically, digital forensics experts or investigators utilize specialized tools to analyze the disk image, while keeping the original data untouched and in read-only mode (Choi et al., 2021; Dubey et al., 2023; Garfinkel, 2010; Gopalan et al., 2019; Sunde & Dror, 2019; Vincze, 2016). The data on disk images is also secured using a cryptographic hash function, providing an additional layer of protection during the investigation phase. Using these digital forensics practice, investigators can verify that the disk image accurately replicates the original storage device. Digital evidence must be preserved not only during the investigation phase but throughout the entire process, from the investigation to its presentation in court. Hence, the digital evidence must be reliable and trustworthy. Research indicates that the chain-of-custody rule is the most effective method used in digital forensics to preserve evidence. According to the author (Brown, 2015), the chain-of-custody process ensures digital evidence is unaltered and untampered. The chain-of-custody rule ensures that any evidence presented is in the same condition as when it was collected (Brown, 2015; Dimitriadis et al., 2020). The chain of custody in digital forensics refers to the documented and continuous process of handling digital evidence to preserve its integrity and admissibility in court (Tsai, 2021). Chain of custody is not a new concept in investigations, but it is essential for verifying the authenticity of evidence. The traditional chain of custody is paper-based and tracks the chronological order of evidence custody. Individuals and organizations involved in investigations are documented, ensuring transparent information is always available about who had access to the evidence. In the digital forensics, the process of maintaining the chain of custody has been digitalized, making it easier to manage. The literature highlights the potential benefits of utilizing blockchain technology due to its unique architectural features, which provide a secure and transparent method for ensuring the chain of custody. This technology creates an immutable and timestamped record of all transactions, making it easier to track the provenance of assets and verify their authenticity. By employing decentralized protocols, blockchain can enhance accountability and reduce the risk of data tampering, thereby improving trust among stakeholders (Akter et al., 2020; AlKhanafseh & Surakhi, 2024; Almutairi & Moulahi, 2023; Atlam et al., 2024; Billard, 2018; Efanov & Roschin, 2018; Ekuma & Fon, n.d.; Sathyaprakasan et al., 2021; Shatakshi Johri, 2024; Tsai, 2021; Tyagi et al., 2024). Literature indicates that the chain of custody concept enhances the

preservation of digital evidence in cybercrime investigations and improves the overall accuracy and reliability of these investigations.

2. MATERIALS AND METHODS

This paper employed a literature review methodology to address two research questions. To ensure all the necessary documentation was collected, a thorough search through multiple online databases was conducted. The searched online databases are: CORE, Digital Forensic Research Workshop (DFRWS), Google Scholar, ResearchGate, and SSRN (Social Science Research Network). The systematic literature review was performed in three phases.

- Phase one or the planning phase involved: identifying the need for a systematic literature review on a specific topic, defining the research questions, and creating a systematic literature review protocol.
- Phase two or process of conducting a literature review consisted of: selecting academic papers, extracting data, and synthesizing that data.
- Phase three of the systematic literature review involved answering the research questions using the finding of the systematic literature review.

The papers and studies gathered during the collection process directly address the defined research questions and adhere to the established selection criteria. When collecting primary studies, it is essential to categorize them based on their relevance. To achieve this, we must establish specific criteria known as inclusion and exclusion criteria. The inclusion criteria outlined in this paper are as follows:

- Studies that present and examine cybercrime investigations.
- Studies that explore the use of digital forensics concepts and tools in cybercrime investigations.
- Studies that investigate effective methods for protecting digital evidence during cybercrime investigations.
- Studies that assess how digital forensics enhances the outcomes of computer crime investigations.

All studies and papers that met the specified criteria were included in the subsequent analysis. Those studies that did not meet these criteria were classified as irrelevant. During the paper collection phase, a total of 110 papers were initially gathered through keyword searches: cybercrime, investigation, digital forensics tools, digital forensics in investigation, cybercrime investigation techniques, digital evidence, preservation of digital evidence. After the initial step of collecting the works, the next phase involved analyzing them based on their titles. At this stage, 42 papers were excluded because they did not fully align with the research field. In the next phase, the remaining 68 studies were analyzed based on their abstracts. It was concluded that 56 of these papers met the inclusion criteria. Therefore, 56 papers were included in the subsequent analysis. These studies fully satisfied the inclusion criteria and addressed the research questions. In total 56 academic papers were collected and later analyzed.

Research questions in this paper are:

RQ1: The practical application of digital forensics techniques significantly enhances the identification, collection, and preservation of digital evidence in cybercrime investigations.

RQ2: The adoption of standardized digital forensic methodologies improves the accuracy and reliability of cybercrime investigations, leading to higher conviction rates.

The main findings of the conducted literature review are detailed in the Results section of this paper.

3. RESULTS

Following a comprehensive literature review of academic research, two research questions can be definitively answered.

- The practical application of digital forensics techniques significantly enhances the identification, collection, and preservation of digital evidence in cybercrime investigations:
- Incorporating the principles of digital forensics into cybercrime investigations significantly improves the identification, collection, and preservation of digital evidence. Key concepts of digital forensics, such as creating a forensic disk image or a secure copy of the original digital data, utilizing cryptographic hash functions, and maintaining a chain of custody, ensure that digital evidence remains protected and untampered throughout the investigation process and up to its presentation in court.
- The adoption of standardized digital forensic methodologies improves the accuracy and reliability of cybercrime investigations, leading to higher conviction rates:
- The literature suggests that using standardized digital forensic methodologies enhances the accuracy and reliability of cybercrime investigations. Unlike other types of crime investigations, cybercrime cases involve handling digital data, which can be easily altered or destroyed. This highlights the critical importance of accuracy and reliability in cybercrime investigations. Digital forensics helps ensure that these investigations are conducted in a secure and dependable manner.

4. DISCUSSIONS

Yet another concept utilized in digital forensics to preserve the integrity and ensure the inalterability of digital evidence is the application of cryptographic hashing functions. For instance, when a disk image is created, a hash function generates a unique hash value, producing a distinct digital fingerprint of the original data. Another example is using hashing in the chain of custody. Hash values are generated and documented when data is entered into the chain of custody. These hash values serve to verify that the digital evidence has not been altered during its transfer among various participants in the investigation process, including forensic examiners, law enforcement, and the court (Chavhan et al., n.d.; Goni et al., 2020; Mahrous et al., 2021; Tyagi et al., 2024). The primary role of cryptographic hash functions in the chain of custody is to identify unauthorized access to digital evidence. By utilizing a hash function, it is ensured that digital evidence cannot be accessed or altered without detection. Because of these features, cryptographic hash functions serve as ideal tools for preserving the authenticity of digital evidence and enhancing the quality of investigations (Aswathnarayanan & Karthik, 2024; Gorda & Chechulin, 2023; Horan & Saiedian, 2021; Jain & Sonowal, 2025; Sviatun et al., 2021). Digital forensics is designed to effectively address cybercrime. The most effective way to combat cybercrime is by utilizing cyber tools. Literature indicates that digital forensics tools can be highly beneficial for investigating cybercriminals, as they are based on the same principles that cybercriminals use to carry out their activities.

5. CONCLUSIONS

In conclusion, digital forensics is essential in cybercrime investigations because it ensures the proper identification, collection, and preservation of digital evidence. As cybercrime evolves with technological advancements, law enforcement and forensic experts must adapt to new and emerging threats. The literature review highlights that digital forensics methodologies greatly improve the effectiveness and reliability of cybercrime investigations. The findings indicate that digital forensics tools equip investigators with the necessary means to securely extract and preserve digital evidence. The accuracy and integrity of digital evidence are crucial in legal proceedings, making digital forensics an essential component of modern investigations. This research emphasizes that digital forensics techniques, such as disk imaging and cryptographic hashing, protect evidence from tampering or unauthorized access. Disk imaging allows investigators to work with a replica of the original data while preserving the integrity of the evidence. Cryptographic hash functions act as a verification mechanism to detect any alterations made to the digital evidence. Furthermore, the chain-of-custody process is fundamental for maintaining the authenticity and admissibility of digital evidence in court. Forensic investigators create a transparent and accountable framework by carefully documenting every step of the evidence-handling process. Recently, blockchain technology has emerged as a promising solution to further strengthen the chain of custody, thereby reducing the risk of evidence tampering. Research suggests that standardizing digital forensic methodologies can improve investigative outcomes and increase conviction rates. A well-defined forensic process ensures consistency, accuracy, and reliability in cybercrime investigations. By adopting standardized procedures, errors can be minimized, and the credibility of digital evidence can be enhanced. Investing in research and development in digital forensics is crucial to staying ahead of cybercriminals. Policymakers must also establish robust legal frameworks to regulate the handling and admissibility of digital evidence. The study confirms that digital forensics plays a vital role in ensuring justice in cybercrime cases. By utilizing forensic tools and methodologies, investigators can uncover critical evidence that strengthens legal proceedings. The credibility of cybercrime investigations relies on the reliability and accuracy of digital evidence. Additionally, future studies should look into the ethical considerations surrounding digital forensics, including privacy issues and data protection regulations.

REFERENCES

Adedayo M. Balogun, & Tranos Zuva. (2018). Criminal Profiling in Digital Forensics: Assumptions, Challenges and Probable Solution.

Akter, O., Akther, A., Uddin, M. A., & Manowarul Islam, M. (2020). Cloud Forensics: Challenges and Blockchain Based Solutions. International Journal of Wireless and Microwave Technologies, 10(5), 1–12. https://doi.org/10.5815/ijwmt.2020.05.01

AlKhanafseh, M., & Surakhi, O. (2024). Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography. Electronics, 13(18), 3729. https://doi.org/10.3390/electronics13183729

Almutairi, W., & Moulahi, T. (2023). Joining Federated Learning to Blockchain for Digital Forensics in IoT. Computers, 12(8). https://doi.org/10.3390/computers12080157

Alotaibi, F., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2023). A Conceptual Digital Forensic Investigation Model Applicable to the Drone Forensics Field. Engineering, Technology and Applied Science Research, 13(5), 11608–11615. https://doi.org/10.48084/etasr.6195

Arshad, H., Jantan, A. Bin, & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. Journal of Information Processing Systems, 14(2), 346–376. https://doi.org/10.3745/JIPS.03.0095

Aswathnarayanan, K., & Karthik, M. A. (2024). "Enhancing Cybercrime Investigation Capabilities: A Comprehensive Analysis of the Tamil Nadu Police Department's Cyber Cell and Operational Procedures." In Madhya Pradesh Journal of Social Sciences A biannually Journal of M. P. Institute of Social Science Research (Vol. 29, Issue 5). https://www.researchgate.net/publication/384145246

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. In Electronics (Switzerland) (Vol. 13, Issue 17). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13173568

Ayotunde, J. (2022). The Effectiveness of Cybercrime Investigations and Prosecution in Nigeria. https://www.researchgate.net/publication/388658641

Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M., & Miranda, F. P. de. (2023). Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. In Journal of Risk and Financial Management (Vol. 16, Issue 8). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/jrfm16080360

Bhat, W. A., AlZahrani, A., & Wani, M. A. (2021). Can computer forensic tools be trusted in digital investigations? Science and Justice, 61(2), 198–203. https://doi.org/10.1016/j.scijus.2020.10.002

Billard, D. (2018). Weighted forensics evidence using blockchain. ACM International Conference Proceeding Series, Part F137704, 57–61. https://doi.org/10.1145/3219788.3219792

Bonomi, S., Casini, M., & Ciccotelli, C. (2020). B-CoC: A blockchain-based chain of custody for evidences management in digital forensics. OpenAccess Series in Informatics, 71. https://doi.org/10.4230/OASIcs.Tokenomics.2019.12

Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55–119. https://doi.org/10.5281/zenodo.22387

Chavhan, M. S., Nirkhi, M., Tech Scholar, M., & Professor, A. (n.d.). Visualization Techniques for Digital forensics: A Survey. In International Journal of Advanced Computer Research.

Chen, C., & Dong, B. (2023). Digital forensics analysis based on cybercrime and the study of the rule of law in space governance. Open Computer Science, 13(1). https://doi.org/10.1515/comp-2022-0266

Choi, H., Lee, S., & Jeong, D. (2021). Forensic Recovery of SQL Server Database: Practical Approach. IEEE Access, 9, 14564–14575. https://doi.org/10.1109/ACCESS.2021.3052505

Da-Yu Kao, Fuching Tsai, Yi-Ting Chao, & Chia-Yang Huang. (2018). Digital Evidence Analytics Applied in Cybercrime Investigations.

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. Array, 5, 100015. https://doi.org/10.1016/j.array.2019.100015

Ding, Z. (2025). The Difficulties and Approaches in Investigate Evidence of New Types Cybercrime. Scientific Journal Of Humanities and Social Sciences, 7, 2025.

Du, X., Le-Khac, N.-A., & Scanlon, M. (n.d.). Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service.

Dubey, H., Bhatt, S., & Negi, L. (2023). Digital Forensics Techniques and Trends: A Review. International Arab Journal of Information Technology, 20(4), 644–654. https://doi.org/10.34028/iajit/20/4/11

Eboibi, F. (2020). A Critical Examination of Cybercrime Investigation Agency under the Nigerian Cybercrimes Act 2015. https://www.researchgate.net/publication/342657697

Efanov, D., & Roschin, P. (2018). The all-pervasiveness of the blockchain technology. Procedia Computer Science, 123, 116–121. https://doi.org/10.1016/j.procs.2018.01.019

Ekuma, N., & Fon, Y. (n.d.). Blockchain Technology for Secure and Transparent Evidence Management in Criminal Investigations

Garfinkel, S. L. (2010). Digital forensics research: The next 10 years. Digital Investigation, 7(SUPPL.). https://doi.org/10.1016/j.diin.2010.05.009

Goni, I., Mishion Gumpy, J., Umar Maigari, T., Muhammad, M., & Saidu, A. (2020). Cybersecurity and Cyber Forensics: Machine Learning Approach. Machine Learning Research, 5(4), 46. https://doi.org/10.11648/j.mlr.20200504.11

Gopalan, S. H., Suba, S. A., Ashmithashree, C., Gayathri, A., & Jebin Andrews, V. (2019). Digital forensics using blockchain. International Journal of Recent Technology and Engineering, 8(2 Special Issue 11), 182–184. https://doi.org/10.35940/ijrte.B1030.0982S1119

Gorda, M. D., & Chechulin, A. A. (2023). Cybercrime investigation model. Informatization and Communication, 3. https://doi.org/10.34219/2078-8320-2023-14-3-92-97

Hamid Lone, A., & Naaz Mir, R. (2017). FORENSIC-CHAIN: ETHEREUM BLOCKCHAIN BASED DIGITAL FORENSICS CHAIN OF CUSTODY. In Scientific and Practical Cyber Security Journal (SPCSJ) (Vol. 1, Issue 2).

Horan, C., & Saiedian, H. (2021). Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. Journal of Cybersecurity and Privacy, 1(4), 580–596. https://doi.org/10.3390/jcp1040029

Horsman, G. (2019). Tool testing and reliability issues in the field of digital forensics. Digital Investigation, 28, 163–175. https://doi.org/10.1016/j.diin.2019.01.009

Jain, R., & Sonowal, B. (2025). Analyzing the Procedure for Investigation in Cybercrime and Admissibility of Electronic Evidence (pp. 265–289). https://doi.org/10.1007/978-3-031-80557-8_12

Kreso, I. (2025). USING BLOCKCHAIN TECHNOLOGY FOR PRESERVING DIGITAL EVIDENCE IN DIGITAL FORENSICS. In KNOWLEDGE-International Journal (Vol. 68, Issue 3).

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44–55. https://doi.org/10.1016/j.diin.2019.01.002

Mahrous, W. A., Farouk, M., & Darwish, S. M. (2021). An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash. IEEE Access, 9, 151327–151336. https://doi.org/10.1109/ACCESS.2021.3126715

Maratsi, M. I., Popov, O., Alexopoulos, C., & Charalabidis, Y. (2022). Ethical and Legal Aspects of Digital Forensics Algorithms: The Case of Digital Evidence Acquisition. ACM International Conference Proceeding Series, 32–40. https://doi.org/10.1145/3560107.3560114

Mohammed, K. H., Mohammed, Y. D., & Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. The International Journal of Cybersecurity Intelligence and Cybercrime, 2(1), 56–63. https://doi.org/10.52306/02010519zjrk2912

Muyambo, E., & Omeleze Baror, S. (n.d.). Systematic Review to Propose a Blockchain-Based Digital Forensic Ready Internet Voting System.

Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019, March 23). Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement. https://doi.org/10.14722/usec.2019.23032

Oerlemans, J. J. (2017). Investigating cybercrime. Meijers-reeks. In J. J.

Oerlemans, J.-J., & Galič, M. (n.d.). Cybercrime investigations.

Page, H., Horsman, G., Sarna, A., & Foster, J. (2019). A review of quality procedures in the UK forensic sciences: What can the field of digital forensics learn? Science and Justice, 59(1), 83–92. https://doi.org/10.1016/j.scijus.2018.09.006

Patil, S., Kadam, S., & Katti, J. (2021). Security enhancement of forensic evidences using blockchain. Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021, 263–268. https://doi.org/10.1109/ICICV50876.2021.9388486

Sathyaprakasan, R., Govindan, P., Alvi, S., Sadath, L., Philip, S., & Singh, N. (2021). An Implementation of Blockchain Technology in Forensic Evidence Management. Proceedings of 2nd IEEE International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2021, 208–212. https://doi.org/10.1109/ICCIKE51210.2021.9410791

Scholarworks, S., & Beardall, D. (2023). Unveiling the Digital Shadows: Cybersecurity and the Art of Digital Forensics.

Shatakshi Johri. (2024). Strengthening Digital Forensics with Blockchain Technology and Algorithms. World Journal of Advanced Research and Reviews, 24(2), 459–467. https://doi.org/10.30574/wjarr.2024.24.2.3317

Sikos, L. F. (2021). AI in digital forensics: Ontology engineering for cybercrime investigations . WIREs Forensic Science, 3(3). https://doi.org/10.1002/wfs2.1394

Sunde, N., & Dror, I. E. (2019). Cognitive and human factors in digital forensics: Problems, challenges, and the way forward. Digital Investigation, 29, 101–108. https://doi.org/10.1016/j.diin.2019.03.011

Sviatun, O. V., Goncharuk, O. V., Chernysh, R., Kuzmenko, O., & Kozych, I. V. (2021). Combating cybercrime: Economic and legal aspects. WSEAS Transactions on Business and Economics, 18, 751–762. https://doi.org/10.37394/23207.2021.18.72

Tsai, F. C. (2021). The application of blockchain of custody in criminal investigation process. Procedia Computer Science, 192, 2779–2788. https://doi.org/10.1016/j.procs.2021.09.048

Tyagi, A. K., Balogun, B. F., & Tiwari, S. (2024). Role of blockchain in digital forensics: A systematic study. In Global Perspectives on the Applications of Computer Vision in Cybersecurity (pp. 197–222). IGI Global. https://doi.org/10.4018/978-1-6684-8127-1.ch008

van Beek, H. M. A., van den Bos, J., Boztas, A., van Eijk, E. J., Schramp, R., & Ugen, M. (2020). Digital forensics as a service: Stepping up the game. In Forensic Science International: Digital Investigation (Vol. 35). Elsevier Ltd. https://doi.org/10.1016/j.fsidi.2020.30102

Vincze, E. A. (2016). Challenges in digital forensics. Police Practice and Research, 17(2), 183–194. https://doi.org/10.1080/15614263.2015.1128163

Wu, Y., Xiang, D., Gao, J. M., & Wu, Y. (2019). Research on investigation and evidence collection of cybercrime Cases. Journal of Physics: Conference Series, 1176(4). https://doi.org/10.1088/1742-6596/1176/4/042064

Yunianto, E., Prayudi, Y., & Sugiantoro, B. (2019). B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management. In International Journal of Computer Applications (Vol. 181, Issue 45).