ZULFAQAR Journal of Defence Science, Engineering & Technology
e-ISSN: 2773-5281
Vol. XX, Issue XX (2024)
DOI: https://doi.org/10.58247/jdset-XXXX-XXXX-XX
Journal homepage: https://zulfaqarjdset.upnm.edu.my

DIGITAL FORENSIC READINESS IN CYBERSECURITY: A REVIEW OF THE LITERATURE AND IDENTIFICATION OF KNOWLEDGE GAPS

Norulzahrah Mohd Zainudin[a], Nor Asiakin Hasbullah[a*], Muslihah Wook[a], Suzaimah Ramli[a], Noor Afiza Mat Razali[a]

[a] Department of Computer Science, Faculty of Defence Science & Technology, National Defence University of Malaysia, Sg. Besi Camp, 57000 Kuala Lumpur, Malaysia

ARTICLE INFO

ARTICLE HISTORY
Received: 00-00-0000
Revised: 00-00-0000
Accepted: 00-00-0000
Published: 00-00-0000

KEYWORDS
Digital forensic
Readiness
Cybersecurity
Forensic investigation
Digital evidence

ABSTRACT

This literature review and gap analysis present an overview of the current state of digital forensic readiness realm over the past five years. The significance of digital forensic readiness (DFR) has grown in importance for organizations to adequately prepare for potential cyber-attacks and effectively respond. The review reveals a lack of standardization in digital forensic readiness practices across different types of organizations and industries, indicating a need for more standardized approaches and guidelines. Another notable gap identified is the limited focus on emerging technologies, necessitating further research to ensure that digital forensic readiness practices keep pace with technological advancements. The review emphasizes the ongoing need for research to address the gaps in current knowledge, enabling organizations to enhance their preparedness to respond to potential cyber-attacks quickly and effectively, as well as ensure the integrity of digital evidence collection and forensic investigations. Additionally, it underscores the critical components of a comprehensive digital forensic readiness program, including incident response, risk management, and threat detection.

1.0 INTRODUCTION

In the current digital era, the importance of cybersecurity cannot be overstated. Organizations must prioritize being well-prepared to safeguard their digital assets, effectively respond to security incidents, and conduct thorough investigations in the face of escalating cyber threats. Digital forensic readiness (DFR) stands as a critical component of cybersecurity, focusing on the organization's ability to swiftly identify, evaluate, and respond to security breaches. It encompasses the establishment of policies, procedures, and tools necessary for detecting and addressing security incidents, as well as the competence to collect and analyse digital evidence for investigative purposes. Developing a tailored digital forensic readiness program is imperative for any organization reliant on digital data, ensuring it meets the specific requirements of the organization.

Sustaining digital forensic readiness requires ongoing monitoring and assessment. Organizations must consistently appraise their digital forensic capabilities, identify areas that require enhancement, and implement appropriate adjustments. This may involve regular testing and simulation of security issues to verify the effectiveness of the incident response plan and other procedures. Furthermore, in the modern digital environment, where cyber threats and attacks are becoming more common and sophisticated, this research is critically important. Organisations and individuals are more susceptible to potential cyber incidents including data breaches, unauthorised access, and cyber-espionage as they continue to use and rely on digital technologies. In this situation, the ability of an organisation to respond quickly and effectively to such situations is greatly enhanced by digital forensic capability. This research aims to provide a comprehensive overview of the present state of digital forensic readiness practices and procedures,

*Corresponding Author | Hasbullah, N. A. | asiakin@upnm.edu.my

therefore contributing to ensuring the development of effective cybersecurity strategies. This is accomplished by performing a thorough analysis of the available literature in this field.

2.0 RESEARCH BACKGOUND

The incorporation of digital forensic readiness is of paramount importance for organizations seeking to enhance their cyber security posture, enabling them to effectively prepare for potential cyber-attacks and promptly respond to them. The significance of digital forensic readiness has been increasingly emphasized by the academic and industry communities over the past decade. As a result, numerous studies and frameworks have emerged with the aim of strengthening digital forensic readiness practices [1].

In recent years, the importance of digital forensic readiness has garnered even more attention due to the surge in cybercrime and the growing recognition of the value of digital evidence in legal proceedings. However, many organizations still face challenges in implementing adequate measures for digital forensic readiness, thereby impeding their ability to respond to cyber-attacks in an effective manner [1]. These challenges include resource constraints, lack of awareness or training, and difficulties in keeping pace with rapidly evolving technology [2]. Furthermore, digital forensic readiness practices can vary significantly across different types of organizations and industries, underscoring the need for standardized approaches and guidelines [3]. To address these challenges, various models and frameworks have been proposed to assess and enhance digital forensic readiness. Various models and frameworks offer a comprehensive set of guidelines for organizations to manage and mitigate cybersecurity risks, including recommendations for digital forensic readiness [4]. For instance, the Integrated Model for Digital Forensic Readiness provides a framework for cyber security organizations to evaluate their digital forensic readiness and identify areas for improvement [5].

Continual research is essential to remain up to date with emerging technologies and threats, as well as to continuously enhance digital forensic readiness practices. This encompasses research into novel approaches and techniques for digital evidence collection and analysis, as well as investigations into the effectiveness of different models and frameworks for evaluating and enhancing digital forensic readiness [4]. For organisations to successfully respond to possible cyberattacks and data breaches, digital forensic readiness is a crucial aspect of cybersecurity. Although putting into practise digital forensic readiness measures might be difficult, several models and frameworks have been put forth to evaluate and enhance these procedures. To develop the subject and improve organisations' capacity to manage and mitigate cybersecurity threats, ongoing research is required.

2.1 Comprehensive Overview Of Digital Forensic Readiness Models And Frameworks: A Synthesis Of Recent Literature

Table 1 presents a comprehensive overview of the significant contributions made by a carefully selected range of research articles published in reputable journals over the past five years, focusing on the topic of digital forensic readiness in the context of cyber security. The articles included in the table were chosen based on their relevance to the subject matter and their scholarly merit. The table effectively summarizes various approaches and perspectives concerning digital forensic readiness, along with the associated challenges and best practices in implementing effective measures. Each entry in the table includes essential details such as author names, publication year, and a concise summary of the primary findings and key insights derived from the respective articles.

The compilation of these publications in the table offers a comprehensive and up-to-date understanding of the current state of research on digital forensic readiness in the field of cyber security. This valuable resource serves as a reference tool for researchers, practitioners, and policymakers alike who are interested in gaining insights into this critical and continually evolving topic. By examining the table, stakeholders can obtain a comprehensive overview of the various research perspectives, enabling them to identify emerging trends, knowledge gaps, and potential avenues for further investigation and development in the realm of digital forensic readiness. Overall, this table demonstrates the broad range of topics and contributions in the field of digital forensic readiness in various areas. They also highlight the need for ongoing research and development to keep up with rapidly evolving technologies and threats, and to continually improve digital forensic readiness practices.

*Corresponding Author | Hasbullah, N. A. | asiakin@upnm.edu.my

Table 1. A comprehensive overview of DFR journal and proceeding articles

Topic	References
Focuses on Expert Reviews of a Cloud Forensic Readiness Framework Designed for Organizations.	[6]
Discusses the Application of Blockchain as a Distributed Ledger for Modern Digital Forensics, Focusing on the Chain-Of-Custody.	[7] [1]
Explores the Implications of Healthcare Data Breaches for Digital Forensic Readiness and Incident Response.	[8]
Proposes the Development of a Capability Maturity Model for Digital Forensic Readiness.	[9]
Discusses Digital Forensic Readiness for Financial Networks, Addressing the Specific Requirements and Challenges in this Sector.	[10]
Examines Digital Forensic Readiness in Wireless Medical Systems	[11]
Presents a Digital Forensic Readiness Approach for Evidence Preservation in Software-Defined Networks.	[12]
Discusses Actionable Threat Intelligence for Enhancing Digital Forensics Readiness and Proactive Incident Response.	[13]
Examines Forensic Readiness Within the Maritime Sector	[1]
Introduces a Natural Human Language Framework for Digital Forensic Readiness in the Public Cloud.	[14]
Presents CFRF, a Dependable Cloud Forensic Readiness Framework Designed to Enhance Forensic Preparedness in Cloud Computing Environments.	[15]
Presents a Roadmap for Verifying Forensic Readiness in Software Development Processes.	[16]
Presents an Architectural Design for A Cloud Forensic Readiness As-A-Service (CFRAAS) Model	[17]
Discusses The Modelling of Cloud Forensics Readiness using a Meta-Analysis	[18]
Explores the Potential use of Keystroke Logging from the Cloud as Digital Evidence for Proactive Forensic Readiness Purposes.	[19]
Advocates for a Dynamic Approach to Digital Forensic Readiness in SDN Platforms	[20]
Proposes a Digital Forensic Readiness Framework Specifically for Smart Homes, Addressing the Unique Challenges and Requirements.	[21]
Provides a Roadmap for Acquiring Digital Evidence in IoT Digital Forensics in Edge Computing Environments.	[22]
Provides a Comprehensive Survey of Challenges, Approaches, and Open Issues in IoT Forensics.	[23]
Proposes a Next-Generation Digital Forensic Readiness BYOD Framework to Enhance Preparedness for Bring Your Own Device Environments.	[24]
Discusses Indicators for Assessing the Maturity and Readiness of Digital Forensic Investigations in the Era of Industrial Revolution 4.0.	[25]
Presents a Cybercrime Semantic Trigger Process for Digital Forensic Readiness	[3]
Addresses The Implementation Challenges and Issues Associated with Digital Forensic Readiness in Software-Defined Networks.	[2]
Introduces Foreplan, a Planning Tool to Support Digital Forensics Readiness on the Internet of Vehicles (IoT) Environment.	[26]
Discusses the Development of a Digital Forensic Readiness Intelligence Crime Repository to Aid in Forensic Investigations.	[27]
Explores Digital Forensic Readiness in Operational Cloud Environments using ISO/IEC 27043 Guidelines on Security Monitoring.	[28]
Analyses the Digital Forensic Readiness Index (DIFRI) and its Application in Cybercrime Response Using Statistical Methods.	[29]
Presents an Exploratory Study on Readiness Frameworks in IoT Forensics	[30]

*Corresponding Author | Hasbullah, N. A. | asiakin@upnm.edu.my

Topic	References
Introduces a Ready-IoT Model, a Novel Forensic Readiness Approach for the Internet of Things (IoT) Environment.	[31]
Proposes a Risk Assessment Model for Digital Forensic Readiness in IoT, Aiding in The Acquisition of Digital Evidence.	[32]
Proposes a Novel Forensic Readiness Framework Applicable to the Drone Forensics Field, Addressing Unique Challenges and Requirements.	[33]
Presents an Extended Digital Forensic Readiness and Maturity Model	[34]
Reviews Research Trends, Challenges, And Emerging Topics in Digital Forensics, Providing an Overview of the Field.	[4]
Proposes a Smart Digital Forensic Readiness Model Specifically Designed for Shadow IoT Devices to Improve Incident Response Capabilities.	[35]
A Retraction Note Related to a Novel Technique for Privacy-Preserving Digital Forensic Readiness in Healthcare Data Stored in the Cloud.	[36]
Provides a Systematic Analysis of The Readiness of Blockchain Integration in IoT Forensics	[37]
Conducts a Cost-Benefit Analysis of Digital Forensic Readiness in Information Systems to Evaluate Its Advantages and Challenges.	[38]
Presents a Case Study on the Digital Forensic Readiness of Major Cloud Platforms	[39]
Presents a Digital Forensic Readiness Information System	[40]
Proposes a Secure Storage Model to Enhance Digital Forensic Readiness in Organizations.	[41]
Explores the Requirements and Challenges Associated with Digital Forensic Readiness in Industrial Automation and Control Systems.	[42]
Presents an Integrated Model for Digital Forensic Readiness Applicable to Cyber Security Personnels.	[5]
Develops a Novel Digital Forensics Readiness Framework for Wireless Medical Networks Using Specialized Logging Techniques.	[43]

2.2 Key Topics And Trends In Digital Forensic Readiness

The final table as in Table 2 presented in this study offers a comprehensive breakdown of the identified themes and findings, as outlined in the initial mapping table. The organisation of this table is based on topic categorisation, accompanied by references to specific articles that delve into each theme. The primary objective of this tabular representation is to enhance the comprehension of the multifaceted dimensions of digital forensic readiness in various areas. It underscores the diverse array of challenges and issues faced by organizations during the implementation of digital forensic readiness measures. Additionally, it showcases the recommended best practices and frameworks proposed to tackle these challenges effectively.

For researchers and practitioners interested in gaining a comprehensive understanding of the various facets of digital forensic readiness and the pivotal factors influencing its implementation and efficacy, this table serves as a valuable point of reference. Furthermore, it facilitates the identification of research gaps and informs future investigations on digital forensic readiness in such areas. Here is a more detailed explanation of each topic and the references that are associated with it. Importance of digital forensic readiness: The importance of digital forensic readiness is a key focus in addressing cyber-attacks promptly and effectively. Daubner et al. [16] highlights the necessity for organizations to prepare for potential cyber-attacks and respond swiftly. Challenges to implementing digital forensic readiness: Implementing digital forensic readiness poses several challenges for organizations. These challenges, as discussed in several articles encompass resource constraints, limited awareness or training, and difficulties in keeping pace with rapidly evolving technology [1-2, 4, 13, 23, 25, 38, 42].

*Corresponding Author | Hasbullah, N. A. | asiakin@upnm.edu.my

Table 2. The main topics and references of the articles

Topic	References
Importance of Digital Forensic Readiness	[16]
Challenges to Implementing Digital Forensic Readiness	[1-2, 4, 13, 23, 25, 38, 42]
Models and Frameworks for Assessing and Improving Digital Forensic Readiness	[5, 9, 24, 30-31, 34-35, 41, 43]
Incident Response Planning, Evidence Preservation and Digital Forensic Readiness	[3, 7, 17, ,40]
Digital Forensic Readiness in the Network Environment	[2, 12, 20, 33]
Digital Forensic Readiness in the Healthcare Industry	[8, 11, 36, 43]
Digital Forensic Readiness for the Banking and Finance Industry	[10]
Digital Forensic Readiness in Cloud Computing Environments	[6, 14-15, 17-19, 28, 36, 39]
Digital Forensic Readiness in IoT and Emerging Technologies	[21-22, 26, 30-33, 35, 37]
Evaluating the Effectiveness of Digital Forensic Readiness Measures	[29, 38]

Models and frameworks for assessing and improving digital forensic readiness: Models and frameworks have been developed to assess and enhance digital forensic readiness. The significance of standardized approaches and guidelines in this regard is underscored in various articles [5, 9, 24, 30-31, 34-35, 41, 43]. Incident response planning, evidence preservation and digital forensic readiness: Incident response planning and evidence preservation are crucial for organizations to effectively handle and mitigate cybersecurity incidents [3, 7, 27, 40]. Digital forensic readiness in the network environment: Digital forensic readiness in the network environment involves proactive measures taken by organizations to prepare for potential cyber incidents. It is to ensure effective incident response, evidence preservation, cybersecurity enhancement, compliance, and accountability in a network environment. Numerous authors have extensively examined the significance of digital forensic readiness within the network environment [2, 12, 20, 33]. Digital forensic readiness in the healthcare industry: The context of digital forensic readiness extends to specific industries such as healthcare service. Some articles examine into the distinctive challenges and considerations associated with digital forensic readiness in the industry [8, 11, 36, 43].

Digital forensic readiness for the banking and finance industry: Digital forensic readiness holds significant importance in the banking and finance industry to ensure the overall stability of the financial ecosystem. Kwon et al. [10] addresses this topic, highlighting the issues and considerations that are associated with digital forensic readiness in this industry. Digital forensic readiness in cloud computing environments. This topic explores the conception and significance of digital forensic readiness within cloud computing platforms. Several researchers have studied digital forensic readiness in the cloud environment thoroughly [6, 14, 15, 17-19, 28, 36, 39].

Digital forensic readiness in IoT and emerging technologies: The emergence of new technologies presents challenges in the field of digital forensic readiness. Many authors have highlighted the importance of staying updated with IoT and emerging technologies and comprehending the associated challenges to effectively address digital forensic readiness [21-22, 26, 30-33, 35, 37]. Evaluating the effectiveness of digital forensic readiness measures: Evaluating the effectiveness of digital forensic readiness measures is a crucial area of inquiry for organizations. Nasiroh and Romahon [29] and Mouhtaropoulos [38] stress the ongoing need for evaluation and improvement of digital forensic readiness practices. Overall, this table concisely synthesizes the literature on digital forensic readiness in cybersecurity. It underscores the significance of organizational readiness for cyber-attacks, while addressing challenges, best practices, and the importance of continuous research and development in response to evolving technologies and threats.

3.0 RESEARCH GAPS

The studies indicate a lack of standardization in the practices of digital forensic readiness across different organizations and industries. This gap underscores the need for the development of more standardized approaches and guidelines to ensure that organizations are adequately prepared for potential cyber-attacks. For instance, whereas some organisations could have established rules and norms for the collection and storage of digital evidence, others might not. This inconsistency can make it difficult for forensic analysts and investigators to work together or communicate evidence across organisations, as well as

*Corresponding Author | Hasbullah, N. A. | asiakin@upnm.edu.my

discrepancies in the admissibility and dependability of digital evidence in legal proceedings. To maintain consistency and dependability in digital forensic ready practises, it is essential to establish standardised procedures and guidelines in this area.

The current state of research in the field of digital forensic readiness reveals a limited focus on emerging technologies. While some studies concentrate on established technologies like the Internet of Things (IoT), cloud computing and mobile devices, there is a pressing need for further investigations that specifically target emerging technologies such as autonomous vehicles, drones, collaborative robots (cobots), warehouse automation, blockchain, and artificial intelligence. This gap in research hinders the development of effective digital forensic readiness practices that can effectively adapt to the rapid advancements in technology. To address this issue, it is essential for researchers to explore into the implications, challenges, and potential solutions pertaining to these emerging technologies. By doing so, they can make valuable contributions to the improvement of digital forensic practices and ensure their continued relevance in the face of evolving technological landscapes.

Despite some studies recognising the significance of human variables, such as awareness and training, there is little focus on them in the field of digital forensic readiness. To fully understand how human variables contribute to the efficacy of digital forensic readiness practices, more research is necessary. This knowledge gap highlights the need for more research on the human aspects that affect the readiness of digital forensics. By examining this topic, researchers can advance the knowledge of how human factors affect the efficacy of digital forensic readiness practices, resulting in more thorough and reliable methods in this area.

4.0 CONCLUSIONS

This literature study and gap analysis, which recognises the increasing importance of digital forensic preparation for organisations in preparing for cyberthreats and effectively defending against them, shed light on the present state of cybersecurity readiness. The analysis highlights the lack of standardisation in digital forensic readiness practises, demonstrating the obvious necessity for consistent methods and regulations across various organisations and industries. Another noticeable gap was the insufficient attention paid to upcoming technologies, which stresses the need for more study to make sure that digital forensic readiness keeps pace with technological changes. The review also emphasises how crucial it is for continuously conducting research to fill these knowledge gaps so that organisations can improve their readiness to respond quickly and effectively to potential cyberattacks while preserving the integrity of digital evidence gathering and forensic investigations. It also highlights important elements of an extensive program for digital forensic preparation, including threat detection, risk management, and incident response. Overall, this evaluation is an invaluable tool for researchers, professionals, and organisations looking to strengthen their cybersecurity and digital forensic capability.

5.0 CONFLICT OF INTEREST

The authors declare no conflicts of interest.

6.0 AUTHORS CONTRIBUTION

Mohd Zainudin, N. (Conceptualisation; Methodology; Validation; Formal analysis; Data curation; Formal analysis; Investigation; Resources; Software; Visualisation; Writing - original draft)
Hasbullah, N. A. (Conceptualisation; Methodology; Validation; Writing - review & editing; Supervision)
Wook, M. (Conceptualisation; Methodology; Validation; Formal analysis; Writing - review & editing; Supervision)
Ramli, S. (Conceptualisation; Methodology; Validation; Writing - review & editing; Supervision)
Mat Razali, N. A. (Methodology; Validation; Project administration)

7.0 ACKNOWLEDGEMENTS

The authors fully acknowledge Ministry of Higher Education (MOHE) and National Defence University of Malaysia (NDUM) which makes this important research viable and effective.

*Corresponding Author | Hasbullah, N. A. | asiakin@upnm.edu.my

REFERENCES

[1] Tam, K., & Jones, K. (2019, June). Forensic readiness within the maritime sector. In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA) (pp. 1-4). IEEE.

[2] Karie, N. M., & Valli, C. (2021). Digital Forensic Readiness Implementation in SDN: Issues and Challenges. arXiv preprint arXiv:2107.13759.

[3] Baror, S. O., Venter, H. S., & Ikuesan, R. A. (2021, December). A Digital Forensic Readiness Cybercrime Semantic Trigger Process. In International Conference on e-Infrastructure and e-Services for Developing Casino, F., Dasaklis, T. K., Spathoulas, G. P., Anagnostopoulos, M., Ghosal, A., Borocz, I., ... & Patsakis, C. (2022). Research trends, challenges, and emerging topics in digital forensics: A review of reviews. IEEE Access, 10, 25464-25493.

[5] Zainudin, N. M., Hasbullah, N. A., Wook, M., Ramli, S., & Razali, N. A. M. (2022). Digital forensic readiness for cyber security practitioners: an integrated model. Journal of Positive School Psychology, 6(3), 8423-8433.

[6] Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts reviews of a cloud forensic readiness framework for organizations. Journal of Cloud Computing, 8, 1-14.

[7] Al-Khateeb, H., Epiphaniou, G., & Daly, H. (2019). Blockchain for modern digital forensics: The chain-of-custody as a distributed ledger. Blockchain and Clinical Trial: Securing Patient Data, 149-168.

[8] Chernyshev, M., Zeadally, S., & Baig, Z. (2019). Healthcare data breaches: Implications for digital forensic readiness. Journal of medical systems, 43, 1-12.

[9] Englbrecht, L., Meier, S., & Pernul, G. (2020). Towards a capability maturity model for digital forensic readiness. Wireless Networks, 26, 4895-4907.

[10] Kwon, S., Jeong, J., & Shon, T. (2019, January). Digital forensic readiness for financial network. In 2019 International conference on platform technology and service (PlatCon) (pp. 1-4). IEEE.

[11] Kyaw, A., Cusack, B., & Lutui, R. (2019, November). Digital forensic readiness in wireless medical systems. In 2019 29th International Telecommunication Networks and Applications Conference (ITNAC) (pp. 1-6). IEEE.

[12] Munkhondya, H., Ikuesan, A., & Venter, H. (2019, February). Digital forensic readiness approach for potential evidence preservation in software-defined networks. In ICCWS 2019 14th International Conference on Cyber Warfare and Security: ICCWS (Vol. 268).

[13] Serketzis, N., Katos, V., Ilioudis, C., Baltatzis, D., & Pangalos, G. J. (2019). Actionable threat intelligence for digital forensics readiness. Information & Computer Security, 27(2), 273-291.

[14] Baror, S. O., Venter, H. S., & Adeyemi, R. (2021). A natural human language framework for digital forensic readiness in the public cloud. Australian Journal of Forensic Sciences, 53(5), 566-591.

[15] Bhatia, S., & Malhotra, J. (2020). CFRF: cloud forensic readiness framework–A dependable framework for forensic readiness in cloud computing environment. In Innovative Data Communication Technologies and Application: ICIDCA 2019 (pp. 765-775). Springer International Publishing.

[16] Daubner, L., Macak, M., Buhnova, B., & Pitner, T. (2020, March). Verification of forensic readiness in software development: A roadmap. In Proceedings of the 35th Annual ACM Symposium on Applied Computing (pp. 1658-1661).

[17] Kebande, V. R., & Venter, H. S. (2019). CFRaaS: Architectural design of a Cloud Forensic Readiness as-a-Service Model using NMB solution as a forensic agent. African Journal of Science, Technology, Innovation and Development, 11(6), 749-769.

[18] Kristyan, S. A., & Juhana, T. (2020, October). Modeling Cloud Forensics Readiness using MetaAnalysis Approach. In 2020 International Conference on Information Technology Systems and Innovation (ICITSI) (pp. 364-369). IEEE.

[19] Makura, S. M., Venter, H. S., Ikuesan, R. A., Kebande, V. R., & Karie, N. M. (2020, February). Proactive forensics: Keystroke logging from the cloud as potential digital evidence for forensic readiness purposes. In 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) (pp. 200-205). IEEE.

[20] Akinbi, A. O. (2023). Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. Wiley Interdisciplinary Reviews: Forensic Science, 5(6), e1496.

[21] Philomin, S., Singh, A., Ikuesan, A., & Venter, H. (2020, March). Digital forensic readiness framework for smart homes. In International conference on cyber warfare and security (pp. 627-XVIII). Academic Conferences International Limited.

[22] Shalaginov, A., Iqbal, A., & Olegård, J. (2020). Iot digital forensics readiness in the edge: A roadmap for acquiring digital evidences from intelligent smart applications. In Edge Computing–EDGE 2020: 4th International Conference, Held as Part of the Services Conference Federation, SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings 4 (pp. 1-17). Springer International Publishing.

*Corresponding Author | Hasbullah, N. A. | asiakin@upnm.edu.my

[23] Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., & Markakis, E. K. (2020). A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Communications Surveys & Tutorials, 22(2), 1191-1221.
[24] Ali, M. I., & Kaur, S. (2021). Next-Generation Digital Forensic Readiness BYOD Framework. Security and Communication Networks, 2021(1), 6664426.
[25] Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0. Computers & Security, 105, 102237.
[26] Katsini, C., Raptis, G. E., Alexakos, C., & Serpanos, D. (2021, November). Foreplan: supporting digital forensics readiness planning for Internet of vehicles. In Proceedings of the 25th Pan-Hellenic Conference on Informatics (pp. 369-374).
[27] Kebande, V. R., Karie, N. M., Choo, K. K. R., & Alawadi, S. (2021). Digital forensic readiness intelligence crime repository. Security and Privacy, 4(3), e151.
[28] Makura, S., Venter, H. S., Kebande, V. R., Karie, N. M., Ikuesan, R. A., & Alawadi, S. (2021). Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring. Security and Privacy, 4(3), e149.
[29] Nasiroh, S., & Romahon, R. A. (2021). Analysis Of Digital Forensic Readiness Index (DIFRI) On Cybercrime Response Using Statistical Methods. Perwira Journal of Science & Engineering, 1(1), 34-41.
[30] Zulkipli, N. H. N., & Wills, G. B. (2021). An exploratory study on readiness framework in IoT forensics. Procedia Computer Science, 179, 966-973.
[31] Sadineni, L., Pilli, E. S., & Battula, R. B. (2021, June). Ready-iot: A novel forensic readiness model for internet of things. In 2021 IEEE 7th World Forum on Internet of Things (WF-IoT) (pp. 89-94). IEEE.
[32] Forfot, A. D., & Østby, G. (2021). Digital forensic readiness in iot-a risk assessment model. In Intelligent Technologies and Applications: Third International Conference, INTAP 2020, Grimstad, Norway, September 28–30, 2020, Revised Selected Papers 3 (pp. 53-64). Springer International Publishing.
[33] Alotaibi, F. M., Al-Dhaqm, A., & Al-Otaibi, Y. D. (2022). A novel forensic readiness framework applicable to the drone forensics field. Computational Intelligence and Neuroscience, 2022(1), 8002963.
[34] Taiwo, A., & Claims, I. (2022). An extended digital forensic readiness and maturity model. Forensic Science International: Digital Investigation, 40, 301348.
[35] Fagbola, F. I., & Venter, H. S. (2022). Smart digital forensic readiness model for shadow IoT devices. Applied Sciences, 12(2), 730.
[36] Retraction Note to: A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud.
[37] Khanji, S., Alfandi, O., Ahmad, L., Kakkengal, L., & Al-Kfairy, M. (2022). A systematic analysis on the readiness of Blockchain integration in IoT forensics. Forensic Science International: Digital Investigation, 42, 301472.
[38] Mouhtaropoulos, A. (2022). Digital Forensic Readiness of Information Systems: A cost-benefit variable analysis. Int. J. Cyber Situational Aware., 6(1), 22-46.
[39] Pichan, A., Lazarescu, M., & Soh, S. T. (2022). A case study on major cloud platforms digital forensics readiness-are we there yet?. International Journal of Cloud Computing, 11(3), 268-302.
[40] Rasyid, I. F., & Zagi, L. M. (2022, November). Digital Forensic Readiness Information System For EJBCA Digital Signature Web Server. In 2022 International Conference on Information Technology Systems and Innovation (ICITSI) (pp. 177-182). IEEE.
[41] Singh, A., Ikuesan, R. A., & Venter, H. (2022). Secure storage model for digital forensic readiness. IEEE Access, 10, 19469-19480.
[42] Thron, R., Dirnberger, H., Tjoa, S., & Quirchmayr, G. (2022, January). Requirements and challenges for digital forensic readiness in industrial automation and control systems. In 2022 The 3rd International Conference on Industrial Engineering and Industrial Management (pp. 232-238).
[43] Mpungu, C., George, C., & Mapp, G. (2023, January). Developing a novel digital forensics readiness framework for wireless medical networks using specialised logging. In Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability, London, September 2022 (pp. 203-226). Cham: Springer International Publishing. .

*Corresponding Author | Hasbullah, N. A. | asiakin@upnm.edu.my