A Detection and Investigation Model for the Capture and Analysis of Network Crimes

Iman S. Alansari
Computer Science Department, College of Computer Science and Engineering, Taibah University, Saudi Arabia
iansari@taibahu.edu.sa (corresponding author)

Received: 24 August 2023 | Revised: 7 September 2023 | Accepted: 12 September 2023

 DOI: https://doi.org/10.48084/etasr.6316

ABSTRACT

Investigation in the field of network forensics involves examining network traffic to identify, capture, preserve, reconstruct, analyze, and document network crimes. Although there are different perspectives on the practical and technical aspects of network forensics, there is still a lack of fundamental guidelines. This paper proposes a new detection and investigation model for capturing and analyzing network crimes, using design science research. The proposed model involves six processes: identification, verification, gathering, preservation, examination, analysis, and documentation. Each process is associated with several activities that provide the investigation team with a clear picture of exactly what needs to be performed. In addition, the proposed model has a unique activity, namely reporting. As a result, this model represents a comprehensive approach to network forensics investigations. It is designed to work in conjunction with established forensic techniques to ensure that forensic evidence from the network is collected and analyzed efficiently and effectively following accepted forensic procedures. The proposed model was compared with existing models in terms of completeness, showing that it is complete and can be adapted to any type of network and legal framework.

Keywords-network forensics; digital forensics; design science research

I. INTRODUCTION

In today's world, information is one of the most valuable assets. Several factors are contributing to what is being called the fourth industrial revolution, such as the digitalization of the production process, connections through social networks, and the use of software as a service. All these elements are important for companies to increase their outreach, productivity, and efficiency [1-2]. During the last decades, there have been many emerging areas and technologies with the potential to propel the development of efficient problem-solving approaches. These areas include the Internet of Things, Cyber-Physical Systems, Artificial Intelligence (AI), Big Data, and Cloud Computing [3-9]. These technologies have created many network assets vital to the proper functioning of the products of the new industrial revolution. These assets can be vulnerable to cyberattacks and, since these attacks take advantage of anonymity, there is a sense of impunity on the internet for them [10]. Several years ago, the Brazilian government introduced a law to mitigate these criminal activities and make it possible to charge offending agents involved in these crimes and, consequently, ensure the security of sensitive information in the country.

Information security principles are incorporated into the requirements and planning process [11-14]. To monitor a network, techniques and technologies such as Intrusion Detection Systems (IDS) are often used to ensure that it is protected [15-16]. The security infrastructure of companies is frequently tested based on these principles [17]. Crackers take advantage of vulnerabilities in internet-based services, applications, or communication networks to cause damage to those services, applications, or communications, causing outages, or even destroying or stealing data. For example, Denial of Service (DoS) and Distributed Denial of Service (DDoS) are two attacks increasingly launched [18-21], but affected users or service providers do not have any information about them because there is no investment in monitoring them.

Monitoring a network to keep it secure generates a large amount of information, but perpetrators of malicious activities are rarely prosecuted for their actions [22]. This may be because there are not enough practical mechanisms (e.g. laws, methodologies, and/or technologies) to help criminal prosecution. The perpetrators have a sense of impunity because there are loopholes in the law that do not classify those acts as crimes. Malicious activities are increasingly reported, including the leakage of personal data through security holes in victims' computers [23]. In 2012, Law 12.737, also known as the Criminal Code for Computer Crimes in Brazil, allowed certain activities in the digital environment to be characterized as crimes.

There is no doubt that Internet-based security systems can detect malicious activities; however, it is important to note that records are usually lost in the huge amount of data generated by these tools [24-25]. Generally, network security experts are designated to clarify these malicious activities. They must

explain through evidence the following items: the author, the cyberattack technique used, the host on which the incident occurred, the author's intentions or motivation, and any damage resulting from the attack. A network expert may not be able to determine whether certain malicious activity on the network is a crime [26]. Therefore, communication between the investigator and the forensic analysis expert during the investigation process is necessary so that the evidence, represented by the IDS data, can be analyzed to uncover the crime. Another problem is that due to the dynamicity and large volume of network traffic, some data that can be evidence of malicious activities might be deleted or lost [27].

This study aimed to develop a comprehensive detection and investigation model using design science research to capture and analyze network crimes committed in a network environment. The model consists of six steps: identification, verification, gathering, preserving, examining, and analyzing and documenting. Each process involves several activities through which the investigation team can create a clear picture of the tasks that need to be completed.

II. RELATED WORKS

According to [28], network forensics is a branch of digital forensics that deals with investigating a network in real-time, on the fly, or post-mortem. To ensure the evidential value and integrity of the collected data, it is necessary to identify, extract, interpret, reconstruct, analyze, and document network-related events in a way that ensures the verification of their evidential value. The data collected from these networks can be used as evidence to corroborate or verify the hypotheses and assertions made by individuals and groups regarding the networking event. In other words, network forensics is primarily concerned with identifying and extracting critical network-based indicators to investigate network-based attacks. These can be used in conjunction with network security postures and network readiness processes to enhance the probative evidential weight of possible network artifacts, all of which are used to enhance network security posture [29-31].

As network-related threats have become more sophisticated, it is necessary to further delineate this subdomain to combat these threats. Cyber forensics is classified as another subdomain, as many network-based attacks can also be described as cyberattacks. Many cyberattacks or cybercrimes are carried out maliciously on a regular basis around the world. There is some evidence that network forensics can deter some complex cyber incidents with the ability to provide intelligence. This field of study includes several models that can be applied to the investigation of processes. For example, in [32], a spread network logging model was presented that could perform cyber forensics over the Internet. In [33], a network forensics model was developed based on distributed techniques. Such techniques can greatly simplify the collection of forensic evidence, providing a central platform for storing it and allowing the easy integration of well-known attribution methods as part of the collection process. In [34], a model capable of collecting and storing leaked digital evidence was developed, using an immune agent designed to capture and store such digital evidence. Data agents were distributed throughout the organization, and the forensic center provided the forensic analysis. In [35], a model was proposed to extract the most important characteristics from currently used digital forensic process models. This was a concept-based model that incorporated some of the most important characteristics of current digital forensic process models into a generic model applicable to network forensic investigation. Infrastructure-as-a-Service (IaaS) is a cloud computing platform that delivers infrastructure as a service, including network forensics [36]. A framework for forensics-as-a-service can be envisioned in a cloud infrastructure as a set of automated cloud management services. As a result, subjects will be able to remotely control the forensic process at the cloud provider using an authorized environment that they can access remotely. Data acquisition and analysis can be done directly by cloud service providers if they choose to.

In [37], a reference model of a distributed cooperative network forensics system was proposed, which could accelerate the investigation process and enhance the capacity for emergency response. A major objective of the proposed model was to link misbehavior activities/traffic with adaptive location filter guidelines, based on which the recommended location filters are discarded in advance or in real-time. This was achieved by evaluating the complete supportive database, determining the possible misbehavior, and restating the misbehavior to perform a forensic investigation. The network forensics model was developed based on scattered methods, providing an automated approach to collect forensic evidence and store it effectively, supporting the informal combination of recognized approaches and producing attack attribution displays. In [38], a theoretical and official information model was proposed for forensic investigations on online community networks. This model was composed of an event-based knowledge model that offers theoretic ideas that can help develop and explain the actions related to the event and support the building and explaining of the associated events. A semantically rich image of the concept was provided to the users through the application of the proposed ontology. In [39], the particle deep framework was presented, which was based on optimization and deep learning using Particle Swarm Optimization (PSO) to choose hyperparameters for the Deep Neural Network (DNN).

Several network forensic models, frameworks, and processes have been proposed to investigate network crimes, but most of them are governed by a system of general records, where analytical data and interactions between police and insurance companies are distributed between various units. An advantage would be the possibility for forensic specialists to easily access all related data as part of the examination and, at the same time, ensure their integrity using digital signatures. However, as shown in Table I, most of the network forensics models and frameworks focus on collecting data rather than examining the whole forensic investigation process. A major drawback of these frameworks is that some of the information provided to the participants could be shared, introducing additional difficulties in confidentiality. A further problem with existing frameworks is that they focus primarily on the stages related to protection and information gathering. Additionally, network forensics is known to have several drawbacks, such as the difficulty in analyzing data due to the variety of data

sources, the level of granularity of data, the integrity of data, their use as legal evidence, and privacy issues. These drawbacks can be grouped into three general categories: technical, legal, and resource-related. These results indicate that there is a need for a comprehensive framework/model to combine all redundant and overlapped concepts, processes, tasks, and activities to make it more effective.

TABLE I. NETWORK FORENSICS MODELS

Year	Network forensics models	Forensic procedures based on NIST standards				Type of the model	
		Protecting	Gathering	Analyzing	Reporting	Practical	Theoretical
2004	[40]	✗	✗	✗	✗	✗	✓
2005	[41]	✗	✗	✗	✗	✗	✓
2007	[42]	✓	✓	✓	✓	✗	✗
2007	[43]	✗	✓	✗	✗	✗	✓
2010	[44]	✗	✗	✓	✓	✓	✗
2010	[45]	✓	✓	✓	✓	✗	✓
2010	[35]	✓	✓	✓	✓	✗	✓
2012	[46]	✓	✓	✗	✗	✓	✓
2012	[47]	✓	✓	✓	✓	✓	✓
2012	[48]	✓	✓	✗	✗	✓	✓
2012	[49]	✗	✗	✓	✗	✓	✗
2013	[50]	✗	✓	✓	✗	✓	✗
2013	[51]	✗	✗	✓	✗	✓	✗
2013	[52]	✓	✓	✓	✓	✗	✓
2013	[53]	✗	✓	✓	✗	✗	✓
2013	[54]	✓	✓	✓	✓	✗	✓
2014	[55]	✗	✓	✗	✗	✗	✗
2016	[56]	✗	✓	✓	✗	✗	✗
2018	[57]	✓	✓	✓	✓	✗	✓
2019	[58]	✓	✓	✓	✓	✓	✓
2019	[59]	✗	✓	✓	✗	✗	✓
2019	[60]	✓	✓	✗	✗	✓	✗
2019	[61]	✗	✗	✓	✗	✓	✗
2020	[62]	✗	✓	✗	✗	✓	✗
2020	[63]	✗	✓	✓	✗	✓	✗
2021	[64]	✗	✓	✓	✓	✗	✓
2022	[65]	✓	✓	✗	✗	✗	✓
2023	[66]	✗	✓	✓	✓	✗	✓

III. METHODOLOGY

This study used the Design Science Research (DSR) method to develop a detection and forensic investigation network model. Figure 1 shows the three main steps used in this study, adopted from [67-68].

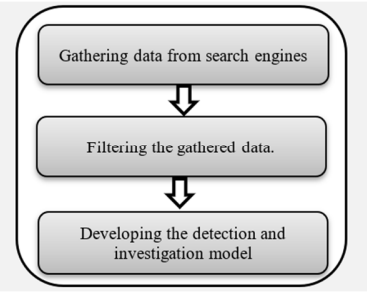

Fig. 1. Development methodology.

Five common search engines were used: Scopus, Web of Science, IEEE Xplore, Springer Link, and Google Scholar. The search used three keywords, "Network forensic," "Network investigation," and "Network crimes," for a period from 2000 to 2023. The search in the above-mentioned search engines resulted in 23555 articles. The documents considered in this study were limited to research articles, technical articles, book chapters, books, and theses. Table II displays the search results.

TABLE II. OVERVIEW OF THE ARTICLES PUBLISHED ON NETWORK FORENSICS

Search Engine	Results
IEEE Xplore	1399
Scopus	355
Web of Science	290
Springer	899
Google Scholar	1700
Total	4643

A metamodeling approach was used to develop the detection and investigation model for network forensics. A metamodeling approach can be described as a nonlinear iterative process used to construct a high-level model that organizes and structures diverse domains at a higher level of abstraction [15, 70]. In the first step, relevant network forensic

models were identified and selected using the coverage criteria adapted from [71]. Then, by analyzing the semantic similarities between these models [72], the concepts and processes that were common to each model were extracted. As a result of combining and harmonizing the extracted processes and concepts into common abstract terms based on naming, similar meanings, and common activities [73], the extracts were combined and harmonized. As shown in Figure 2, six processes were proposed: identification, verification, gathering, preservation, examination, and analysis and documentation.

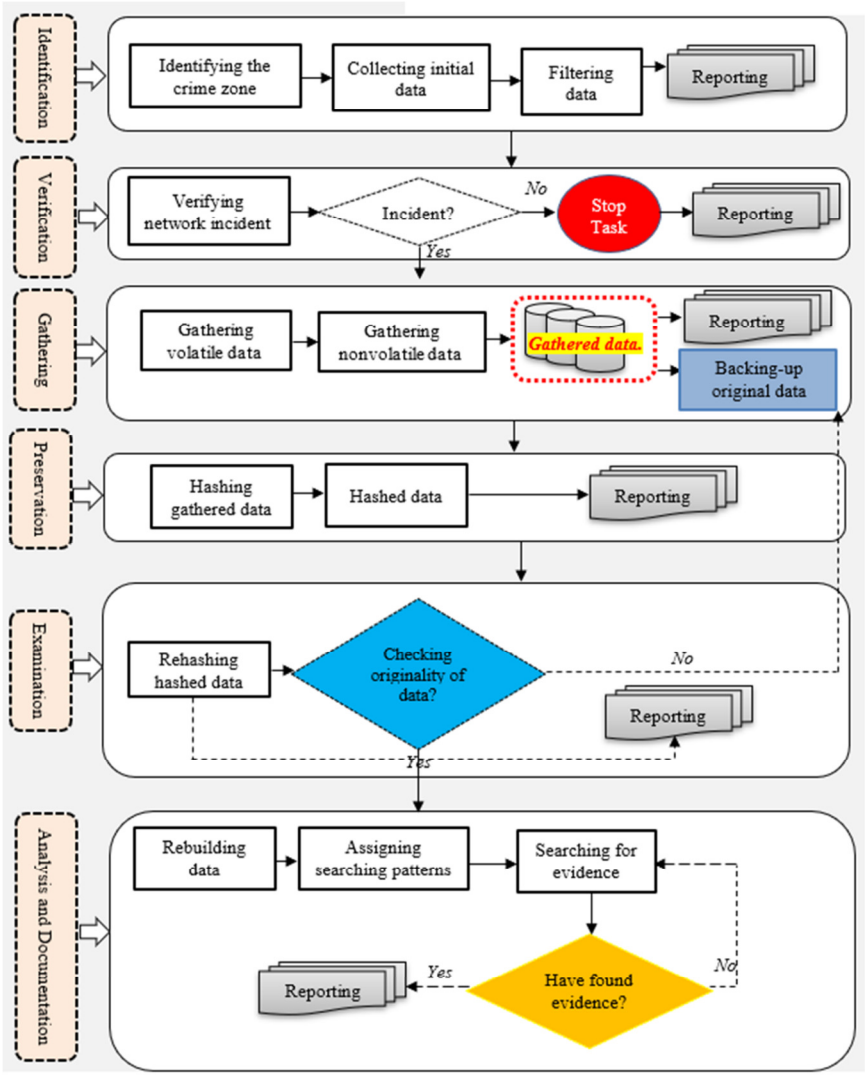

Figure 2. Proposed detection and investigation model for capturing and analyzing network crimes.

Each process consists of several activities. The identification process is used to identify and respond to a network crime that has occurred. Using it, the crime zone would be identified and the initial data on the crime would be collected and filtered to use them in the verification process. At this stage, the first report is being prepared. The second part is the verification process, which is used to verify and confirm whether the network incident is real or not. When an actual network crime occurs on a network, the investigation will move to the gathering process, otherwise, it will be stopped. The investigation team will prepare a report on this process. Gathering is the third process, where volatile and nonvolatile data are collected from the identified sources. A backup of the gathered data is stored on an external hard disk to ensure data integrity and future use. Again, a report is prepared on the activities of this process. The preservation process ensures that the integrity of the collected data is protected. Hashing is used to protect data integrity. Again, the investigation team prepares a report on the activities during this step.

The fifth process involves examination of the data to determine their authenticity. The acquired data will be rehashed to ensure their authenticity since they have already been hashed in the preservation process. If the original data have been modified, the investigation process will proceed to the gathering process to take a copy of the original data; otherwise, the investigation process will progress to the final process, after

preparing a detailed report on this step. The final process is the analysis and documentation. Data must be reconstructed in the procedure of looking for evidence. The data collected at this stage need to be rebuilt first, and the investigation team needs to consider search patterns, such as email, credit card, location, and mobile numbers. The search for evidence is a repetitive process where data are searched for evidence over and over again. At the end of the investigation process, the investigators will prepare a detailed report on the entire process.

IV. RESULTS AND DISCUSSION

This section discusses the proposed model and compares it with other existing studies. This study proposed a model to detect, investigate, and analyze network crimes. In summary, the process consists of six main components: identification, verification, gathering, preservation, examination, and analysis and documentation. One of the main advantages of the proposed model is that it can function independently. The investigation team receives a clear view and a single report for each process, which is an innovative feature in this domain.

TABLE III. COMPARISON OF THE PROPOSED AND EXISTING NETWORK FORENSICS MODELS

Year	Network forensics models	Forensic processes based on NIST standards				Proposed model coverage
		Protecting	Gathering	Analyzing	Reporting	
2004	[40]	✗	✗	✗	✗	✓
2005	[41]	✗	✗	✗	✗	✓
2007	[42]	✓	✓	✓	✓	✓
2007	[43]	✗	✓	✗	✗	✓
2010	[44]	✗	✗	✓	✓	✓
2010	[45]	✓	✓	✓	✓	✓
2010	[35]	✓	✓	✓	✓	✓
2012	[46]	✓	✓	✗	✗	✓
2012	[47]	✓	✓	✓	✓	✓
2012	[48]	✓	✓	✗	✗	✓
2012	[49]	✗	✗	✓	✗	✓
2013	[50]	✗	✓	✓	✗	✓
2013	[51]	✗	✗	✓	✗	✓
2013	[52]	✓	✓	✓	✓	✓
2013	[53]	✗	✓	✓	✗	✓
2013	[54]	✓	✓	✓	✓	✓
2014	[55]	✗	✓	✗	✗	✓
2016	[56]	✗	✓	✓	✗	✓
2018	[57]	✓	✓	✓	✓	✓
2019	[58]	✓	✓	✓	✓	✓
2019	[59]	✗	✓	✓	✗	✓
2019	[60]	✓	✓	✗	✗	✓
2019	[61]	✗	✗	✓	✗	✓
2020	[62]	✗	✓	✗	✗	✓
2020	[63]	✗	✓	✓	✗	✓
2021	[64]	✗	✓	✓	✓	✓
2022	[65]	✓	✓	✗	✗	✓
2023	[66]	✗	✓	✓	✓	✓

The forensic processes in existing models are generally based on the NIST standard. There are four main investigation processes in network forensics: preservation, acquisition, analysis, and reporting. The proposed model not only covers these processes but also adds two more, i.e. identification and verification. Table III compares the proposed and existing network forensic investigation models.

V. CONCLUSION

Network forensics investigations consist of the examination of network traffic to identify, capture, preserve, reconstruct, analyze, and document crimes that have taken place on a network. Several perspectives have been proposed on the practical and technical aspects of network forensics. On the other hand, there is a lack of clear fundamental guidelines and perspectives on the subject. This study proposed a new detection and investigation model for capturing and analyzing network crimes to fill this gap, using the design science research method. The proposed model involves six processes: identification, verification, collection, preservation, examination, and analysis and documentation. Each of these processes includes several activities. Using this model, the investigation team would have a clear picture of what must be done to carry out the investigation. The proposed model includes a distinct activity that is not included in previous studies, namely, reporting. Consequently, this model represents a comprehensive approach to network forensics investigations. With the implementation of this model, investigators will be able to gather and analyze network forensic evidence following the established procedures efficiently and effectively and, at the same time, ensure that network forensic evidence is obtained and analyzed by accepted forensic procedures. The proposed model not only is adaptable to any type of network or legal framework but could also be applied to any type of service.

REFERENCES

[1] A. Al-Dhaqm, S. A. Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A Review of Mobile Forensic Investigation Process Models," *IEEE Access*, vol. 8, pp. 173359–173375, 2020, https://doi.org/10.1109/ACCESS.2020.3014615.

[2] F. M. Ghabban, I. M. Alfadli, O. Ameerbakhsh, A. N. AbuAli, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Comparative Analysis of Network Forensic Tools and Network Forensics Processes," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Cameron Highlands, Malaysia, Jun. 2021, pp. 78–83, https://doi.org/10.1109/ICSCEE50312.2021.9498226.

[3] V. R. Kebande, R. A. Ikuesan, N. M. Karie, S. Alawadi, K.-K. R. Choo, and A. Al-Dhaqm, "Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments," *Forensic Science International: Reports*, vol. 2, Dec. 2020, Art. no. 100122, https://doi.org/10.1016/j.fsir.2020.100122.

[4] S. Abd Razak, N. H. Mohd Nazari, and A. Al-Dhaqm, "Data Anonymization Using Pseudonym System to Preserve Data Privacy," *IEEE Access*, vol. 8, pp. 43256–43264, 2020, https://doi.org/10.1109/ACCESS.2020.2977117.

[5] I. U. Onwuegbuzie, S. A. Razak, I. F. Isnin, T. S. J. Darwish, and A. Al-dhaqm, "Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach," *PLOS ONE*, vol. 15, no. 8, 2020, Art. no. e0237154, https://doi.org/10.1371/journal.pone.0237154.

[6] W. A. H. Altowayti *et al.*, "The Role of Conventional Methods and Artificial Intelligence in the Wastewater Treatment: A Comprehensive

Review," *Processes*, vol. 10, no. 9, 2022, https://doi.org/10.3390/pr10091832.

[7] K. N. Qureshi *et al.*, "A Blockchain-Based Efficient, Secure and Anonymous Conditional Privacy-Preserving and Authentication Scheme for the Internet of Vehicles," *Applied Sciences*, vol. 12, no. 1, 2022, https://doi.org/10.3390/app12010476.

[8] M. Rasool, N. A. Ismail, A. Al-Dhaqm, W. M. S. Yafooz, and A. Alsaeedi, "A Novel Approach for Classifying Brain Tumours Combining a SqueezeNet Model with SVM and Fine-Tuning," *Electronics*, vol. 12, no. 1, 2023, https://doi.org/10.3390/electronics12010149.

[9] M. Q. Mohammed *et al.*, "Review of Learning-Based Robotic Manipulation in Cluttered Environments," *Sensors*, vol. 22, no. 20, 2022, https://doi.org/10.3390/s22207938.

[10] A. Ali *et al.*, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Applied Sciences*, vol. 12, no. 19, 2022, https://doi.org/10.3390/app12199637.

[11] W. M. S. Yafooz, A. Al-Dhaqm, and A. Alsaeedi, "Detecting Kids Cyberbullying Using Transfer Learning Approach: Transformer Fine-Tuning Models," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 255–267.

[12] A. Al-Dhaqm, R. A. Ikuesan, V. R. Kebande, S. Razak, and F. M. Ghabban, "Research Challenges and Opportunities in Drone Forensics Models," *Electronics*, vol. 10, no. 13, 2021, https://doi.org/10.3390/electronics10131519.

[13] A. Al-dhaqm *et al.*, "Database Forensic Investigation Process Models: A Review," *IEEE Access*, vol. 8, pp. 48477–48490, 2020, https://doi.org/10.1109/ACCESS.2020.2976885.

[14] A. A. Alghamdi, "Computerised Information Security Using Texture Based Fuzzy Cryptosystem," *Engineering, Technology & Applied Science Research*, vol. 8, no. 6, pp. 3598–3602, Dec. 2018, https://doi.org/10.48084/etasr.2353.

[15] A. Al-Dhaqm, S. Abd Razak, S. H. Othman, A. Nagdi, and A. Ali, "A Generic Database Forensic Investigation Process Model," *Jurnal Teknologi*, vol. 78, no. 6–11, Jun. 2016, https://doi.org/10.11113/jt.v78.9190.

[16] M. A. Saleh, S. H. Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Common investigation process model for Internet of Things forensics," in *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, 2021, pp. 84–89.

[17] F. M. Alotaibi, A. Al-Dhaqm, W. M. S. Yafooz, and Y. D. Al-Otaibi, "A Novel Administration Model for Managing and Organising the Heterogeneous Information Security Policy Field," *Applied Sciences*, vol. 13, no. 17, 2023, https://doi.org/10.3390/app13179703.

[18] A. A. Zubair *et al.*, "A Cloud Computing-Based Modified Symbiotic Organisms Search Algorithm (AI) for Optimal Task Scheduling," *Sensors*, vol. 22, no. 4, 2022, https://doi.org/10.3390/s22041674.

[19] A. E. Yahya, A. Gharbi, W. M. S. Yafooz, and A. Al-Dhaqm, "A Novel Hybrid Deep Learning Model for Detecting and Classifying Non-Functional Requirements of Mobile Apps Issues," *Electronics*, vol. 12, no. 5, 2023, https://doi.org/10.3390/electronics12051258.

[20] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a New Model to Secure IoT-based Smart Home Mobile Agents using Blockchain Technology," *Engineering, Technology & Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, Apr. 2020, https://doi.org/10.48084/etasr.3394.

[21] V. H. Le, N. Q. Luc, T. T. Dao, and Q. T. Do, "Building an Application that reads Secure Information Stored on the Chip of the Citizen Identity Card in Vietnam," *Engineering, Technology & Applied Science Research*, vol. 13, no. 1, pp. 10100–10107, Feb. 2023, https://doi.org/10.48084/etasr.5531.

[22] I. U. Onwuegbuzie, S. A. Razak, I. F. Isnin, A. Al-dhaqm, and N. B. Anuar, "Prioritized Shortest Path Computation Mechanism (PSPCM) for wireless sensor networks," *PLOS ONE*, vol. 17, no. 3, 2022, Art. no. e0264683, https://doi.org/10.1371/journal.pone.0264683.

[23] M. Salem, S. H. Othman, A. Al-Dhaqm, and A. Ali, "Development of Metamodel for Information Security Risk Management," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 243–253.

[24] A. Al-Dhaqm *et al.*, "CDBFIP: Common Database Forensic Investigation Processes for Internet of Things," *IEEE Access*, vol. 5, pp. 24401–24416, 2017, https://doi.org/10.1109/ACCESS.2017.2762693.

[25] A. Al-Dhaqm *et al.*, "Categorization and Organization of Database Forensic Investigation Processes," *IEEE Access*, vol. 8, pp. 112846–112858, 2020, https://doi.org/10.1109/ACCESS.2020.3000747.

[26] A. Al-dhaqm, "Detecting Threats in Network Security by Analyzing Network Packets using Wireshark," presented at the International Conference of Recent Trends in Information and Communication Technologies, Chandigarh , India, Dec. 2014.

[27] M. Qadeer, C. G. Hussain, and C. M. Hussain, "Computer Forensics and Personal Digital Assistants," in *Modern Forensic Tools and Devices*, John Wiley & Sons, Ltd, 2023, pp. 1–22.

[28] I. R. Adeyemi, S. A. Razak, and N. A. N. Azhan, "A Review of Current Research in Network Forensic Analysis," *International Journal of Digital Crime and Forensics (IJDCF)*, vol. 5, no. 1, pp. 1–26, Jan. 2013, https://doi.org/10.4018/jdcf.2013010101.

[29] I. R. Adeyemi, S. A. Razak, and N. A. N. Azhan, "Identifying critical features for network forensics investigation perspectives." arXiv, Oct. 05, 2012, https://doi.org/10.48550/arXiv.1210.1645.

[30] M. Lagrasse, A. Singh, H. Munkhondya, A. Ikuesan, and H. Venter, "Digital forensic readiness framework for software-defined networks using a trigger-based collection mechanism," in *ICCWS 2020 15th International Conference on Cyber Warfare and Security*, Norfolk, VA, USA, Mar. 2020.

[31] H. Munkhondya, A. R. Ikuesan, and H. S. Venter, "A Case for a Dynamic Approach to Digital Forensic Readiness in an SDN Platform," presented at the International Conference on Cyber Warfare and Security, Reading, UK, 2020.

[32] G. SinghChhabra and P. Singh, "Distributed Network Forensics Framework: A Systematic Review," *International Journal of Computer Applications*, vol. 119, no. 19, pp. 31–35, Jun. 2015, https://doi.org/10.5120/21178-4201.

[33] Y. Tang and T. E. Daniels, "A Simple Framework for Distributed Forensics," presented at the Second International Workshop on Security in Distributed Computing Systems (SDCS) (ICDCSW'05), Jun. 2005, pp. 163–169, https://doi.org/10.1109/ICDCSW.2005.24.

[34] T. Hong, Z. Tao, J. Qi, and Z. Jianbo, "A Distributed Framework for Forensics Based on the Content of Network Transmission," presented at the Instrumentation, Measurement, Computer, Communication and Control, International Conference on, Oct. 2011, pp. 852–855, https://doi.org/10.1109/IMCCC.2011.215.

[35] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digital Investigation*, vol. 7, no. 1, pp. 14–27, Oct. 2010, https://doi.org/10.1016/j.diin.2010.02.003.

[36] T. Gebhardt and H. P. Reiser, "Network Forensics for Cloud Computing," in *Distributed Applications and Interoperable Systems*, 2013, pp. 29–42, https://doi.org/10.1007/978-3-642-38541-4_3.

[37] W. Ren, "On A Reference Model of Distributed Cooperative Network, Forensics System.," presented at the The sixth International Conference on Information Integrationand Web-based Applications Services, Jakarta, Indonesia, Sep. 2004.

[38] A. Ali, S. A. Razak, S. H. Othman, A. Mohammed, and F. Saeed, "A metamodel for mobile forensics investigation domain," *PLOS ONE*, vol. 12, no. 4, 2017, Art. no. e0176223, https://doi.org/10.1371/journal.pone.0176223.

[39] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," *IEEE Access*, vol. 8, pp. 145018–145032, 2020.

[40] R. Wei, "A Framework of Distributed Agent-Based Network Forensics System," presented at the Digital Forensic Research Conference, Baltimore, MD, USA, Aug. 2004.

[41] W. Ren and H. Jin, "Distributed agent-based real time network intrusion forensics system architecture design," presented at the 19th International Conference on Advanced Information Networking and Applications (AINA'05), Jan. 2005, vol. 1, pp. 177–182, https://doi.org/10.1109/AINA.2005.164.

[42] D. Wang, T. Li, S. Liu, J. Zhang, and C. Liu, "Dynamical Network Forensics Based on Immune Agent," in *Proceedings of the Third International Conference on Natural Computation*, USA, May 2007, vol. 3, pp. 651–656, https://doi.org/10.1109/ICNC.2007.345.

[43] B. Endicott-Popovsky, D. A. Frincke, and C. A. Taylor, "A Theoretical Framework for Organizational Network Forensic Readiness," *Journal of Computers*, vol. 2, no. 3, pp. 1–11, May 2007, https://doi.org/10.4304/jcp.2.3.1-11.

[44] S. Ngobeni, H. Venter, and I. Burke, "A Forensic Readiness Model for Wireless Networks," in *Advances in Digital Forensics VI*, Hong Kong, China, 2010, pp. 107–117, https://doi.org/10.1007/978-3-642-15506-2_8.

[45] E. S. Pilli, R. C. Joshi, and R. Niyogi, "A Framework for Network Forensic Analysis," in *Information and Communication Technologies*, Kochi, India, 2010, pp. 142–147, https://doi.org/10.1007/978-3-642-15766-0_21.

[46] R. Ammann, "Network Forensic Readiness: a bottom-up approach for IPv6 networks," MSc Thesis, Auckland University of Technology, New Zealand, 2012.

[47] S. Ngobeni, H. S. Venter, and I. Burke, "The modelling of a digital forensic readiness approach for Wireless Local Area Networks," *Journal of Universal Computer Science*, vol. 18, no. 12, pp. 1721–1740, Jun. 2012.

[48] M. Mulazzani, M. Huber, and E. Weippl, "Social Network Forensics: Tapping the Data Pool of Social Networks," 2012.

[49] D. Avasthi, "Network Forensic Analysis with Efficient Preservation for SYN Attack," *International Journal of Computer Applications*, vol. 46, no. 24, pp. 17–22, May 2012.

[50] A. Al-Mahrouqi, S. Abdalla, and T. Kechadi, "Network Forensics Readiness and Security Awareness Framework," presented at the International Conference on Embedded Systems in Telecommunications and Instrumentation (ICESTI 2014), Oct. 2014.

[51] C. Liu, A. Singhal, and D. Wijesekera, "Creating Integrated Evidence Graphs for Network Forensics," in *Advances in Digital Forensics IX*, Orlando, FL, USA, 2013, pp. 227–241, https://doi.org/10.1007/978-3-642-41148-9_16.

[52] M. Thapliyal, A. Bijalwan, N. Garg, and E. S. Pilli, "A Generic Process Model for Botnet Forensic Analysis," presented at the Conference on Advances in Communication and Control Systems (CAC2S 2013), Apr. 2013, pp. 98–102.

[53] E. Saari and A. Jantan, "A framework to increase the accuracy of collected evidences in network forensic by integrating IDS and firewall mechanisms," in *Proceedings of the International Conference on Systems, Control and Informatics*, 2013.

[54] S. Parate, "Application of Network Forensics for Detection of Web Attack using Neural Network," presented at the National Conference on Innovative Paradigms in Engineering & Technology, 2013.

[55] A. R. Amran and A. Saad, "An evidential network forensics analysis model with adversarial capability and layering," in *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, Jan. 2014, pp. 1–9, https://doi.org/10.1109/WCCAIS.2014.6916615.

[56] S. Mittal and R. Singh, "Securing Network Flow Using Network Forensics," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 5, pp. 338–344, May 2016.

[57] P. Kaur, A. Bijalwan, R. C. Joshi, and A. Awasthi, "Network Forensic Process Model and Framework: An Alternative Scenario," in *Intelligent Communication, Control and Devices*, Singapore, 2018, pp. 493–502, https://doi.org/10.1007/978-981-10-5903-2_50.

[58] S. J. Ngobeni and H. S. Venter, "Design of a wireless forensic readiness model (WFRM)," presented at the Information Security South Africa (ISSA2009) Conference, Johannesburg, South Africa, Jul. 2009.

[59] A. Kyaw, B. Cusack, and R. Lutui, "Digital Forensic Readiness In Wireless Medical Systems," in *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, Auckland, New Zealand, Aug. 2019, https://doi.org/10.1109/ITNAC46935.2019.9078005.

[60] R. Lu and L. Li, "Research on Forensic Model of Online Social Network," in *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, Chengdu, China, Apr. 2019, pp. 116–119, https://doi.org/10.1109/ICCCBDA.2019.8725746.

[61] D. Saputra and The Society of Digital Information and Wireless Communication, "Network Forensics Analysis of Man in the Middle Attack Using Live Forensics Method," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 66–73, 2019, https://doi.org/10.17781/P002558.

[62] H. Arshad, A. Jantan, G. K. Hoon, and I. O. Abiodun, "Formal knowledge model for online social network forensics," *Computers & Security*, vol. 89, Feb. 2020, Art. no. 101675, https://doi.org/10.1016/j.cose.2019.101675.

[63] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, Sep. 2020, https://doi.org/10.1016/j.future.2020.03.042.

[64] R. Nilesh Malvankar and A. Jain, "EnNetForens: An Efficient Proactive Approach For Network Forensic," in *2021 International Conference on Communication, Control and Information Sciences (ICCISc)*, Idukki, India, Jun. 2021, vol. 1, pp. 1–4, https://doi.org/10.1109/ICCISc52257.2021.9484865.

[65] W. Yang, M. N. Johnstone, S. Wang, N. M. Karie, N. M. bin Sahri, and J. J. Kang, "Network Forensics in the Era of Artificial Intelligence," in *Explainable Artificial Intelligence for Cyber Security: Next Generation Artificial Intelligence*, M. Ahmed, S. R. Islam, A. Anwar, N. Moustafa, and A.-S. K. Pathan, Eds. Cham, Switzerland: Springer International Publishing, 2022, pp. 171–190.

[66] A. Wijayanto, I. Riadi, and Y. Prayudi, "TAARA Method for Processing on the Network Forensics in the Event of an ARP Spoofing Attack," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 7, no. 2, pp. 208–217, Mar. 2023, https://doi.org/10.29207/resti.v7i2.4589.

[67] I. U. Onwuegbuzie, S. A. Razak, and A. Al-Dhaqm, "Multi-Sink Load-Balancing Mechanism for Wireless Sensor Networks," in *2021 IEEE International Conference on Computing (ICOCO)*, Kuala Lumpur, Malaysia, Aug. 2021, pp. 140–145, https://doi.org/10.1109/ICOCO53166.2021.9673578.

[68] A. Al-dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a Database Forensic Metamodel (DBFM)," *PLOS ONE*, vol. 12, no. 2, 2017, Art. no. e0170793, https://doi.org/10.1371/journal.pone.0170793.

[69] A. Al-Dhaqm *et al.*, "Digital Forensics Subdomains: The State of the Art and Future Directions," *IEEE Access*, vol. 9, pp. 152476–152502, 2021, https://doi.org/10.1109/ACCESS.2021.3124262.

[70] A. Al-Dhaqm, W. M. S. Yafooz, S. H. Othman, and A. Ali, "Database Forensics Field and Children Crimes," in *Kids Cybersecurity Using Computational Intelligence Techniques*, W. M. S. Yafooz, H. Al-Aqrabi, A. Al-Dhaqm, and A. Emara, Eds. Cham, Switzerland: Springer International Publishing, 2023, pp. 81–92.

[71] A. M. R. Al-Dhaqm, S. H. Othman, S. Abd Razak, and A. Ngadi, "Towards adapting metamodelling technique for database forensics investigation domain," in *2014 International Symposium on Biometrics and Security Technologies (ISBAST)*, Kuala Lumpur, Malaysia, Dec. 2014, pp. 322–327, https://doi.org/10.1109/ISBAST.2014.7013142.

[72] S. R. Selamat, R. Yusof, and S. Sahib, "Mapping Process of Digital Forensic Investigation Framework," *International Journal of Computer Science and Network Security*, vol. 8, no. 10, pp. 163–169, Oct. 2008.

[73] A. Ali, S. A. Razak, S. H. Othman, R. R. Marie, A. Al-Dhaqm, and M. Nasser, "Validating Mobile Forensic Metamodel Using Tracing Method," in *Advances on Intelligent Informatics and Computing*, 2022, pp. 473–482, https://doi.org/10.1007/978-3-030-98741-1_39.