Comparative Analysis of Network Forensic Tools and Network Forensics Processes

Fahad M Ghabban
College of Computer Science and Engineering. Information system department. Taibah University. Saudi Arabia. Madina
fghaban@taibahu.edu.sa

Ibrahim M Alfadli
College of Computer Science and Engineering. Information system department. Taibah University. Saudi Arabia. Madina
ialfadli@taibahu.edu.sa

Omair Ameerbakhsh
College of Computer Science and Engineering. Information system department. Taibah University. Saudi Arabia. Madina
oameerbakhsh@taibahu.edu.sa

Amer Nizar AbuAli
College of Computer Science and Engineering. Information system department. Taibah University. Saudi Arabia. Madina
aabuali@taibahu.edu.sa

Arafat Al-Dhaqm
Faculty of Engineering, School of Computing, University Technology Malaysia
Malaysia, Johor
mrarafat1@utm.my

Mahmoud Ahmad Al-Khasawneh
Faculty of Computer & Information Technology
Al-Madinah International University
Shah Alam, Malaysia
mahmoud@outlook.my

Abstract— **Network Forensics (NFs) is a branch of digital forensics which used to detect and capture potential digital crimes over computer networked environments crime. Network Forensic Tools (NFTs) and Network Forensic Processes (NFPs) have abilities to examine networks, collect all normal and abnormal traffic/data, help in network incident analysis, and assist in creating an appropriate incident detection and reaction and also create a forensic hypothesis that can be used in a court of law. Also, it assists in examining the internal incidents and exploitation of assets, attack goals, executes threat evaluation, also by evaluating network performance. According to existing literature, there exist quite a number of NFTs and NTPs that are used for identification, collection, reconstruction, and analysing the chain of incidents that happen on networks. However, they were vary and differ in their roles and functionalities. The main objective of this paper, therefore, is to assess and see the distinction that exist between Network Forensic Tools (NFTs) and Network Forensic Processes (NFPs). Precisely, this paper focuses on comparing among four famous NFTs: Xplico, OmniPeek, NetDetector, and NetIetercept. The outputs of this paper show that the Xplico tool has abilities to identify, collect, reconstruct, and analyse the chain of incidents that happen on networks than other NF tools.**

Keywords— *Digital forensics, Network forensics, Comparative analysis, Xplico, OmniPeek, NetDetector, NetIetercept*

I. INTRODUCTION

Network Forensic Tools (NFTs) are able to collect the whole network stream of traffic, permit customers to analyse the network stream of traffic based on their requirements and find the main elements about the traffic [1], [2]. NFTs are able to be aligned with IDSs and firewalls in order to create the protection of network, also to record all traffic records for rapid examination. NFTs allow corporations of seized, collected, and analysed packets of network traffic, which allows the investigator to obtain traffic forms between different machines. Several NFTs have been offered in the literature which offer consistent data collection and strong analytical abilities. Furthermore, numerous security tools are proposed for network security. However, these tools have been created for collecting and processing evidence, and do not have a forensic purpose [3], [4]. This paper focuses on comparing among five NFTs: Xplico, OmniPeek, NetDetector, and NetIetercept. Then select the best tool based on their capabilities and features.

The structure of this paper arranged as follows: Section 2 presents the digital forensic field. Section 3 reviews the network forensic tools and Section 4 offers the discussion part, and Section 5 concludes the paper.

II. DIGITAL FORENSICS

The digital forensics discipline is used to investigate cybercrimes [5]–[7]. It consists of several branches as shown in Figure 1: Database forensic, mobile forensics, computer forensics, social network forensics, forensic data analysis, IoT forensics [8], drones forensic, and network forensics. The database forensics field is a branch of digital forensics which used to solve database crimes. It received much attention from researchers to address database incidents [9]–[17]. The database forensic field is complex and heterogeneous field due to the variety of database system infrastructures and m multidimensional nature of the database systems [18]–[20]. Therefore, at the time of writing this article, this domain lacks a unified forensic framework to facilitate and organize domain knowledge amongst domain forensic users [21]–[23]. Additionally, the database forensic domain lacks a universal forensic tool which creates many challenges among domain practitioners [24], [25]. Mobile forensics is a significant branch of digital forensics which used to address mobile cybercrimes.

It received many works to overcome mobile issues [26]–[29]. However, it is suffering from several drawbacks, such as redundant investigation terminologies, processes, concepts, and practices. On the contrary, computer forensics is a branch of Digital Forensics (DF) that used to detect, collect, preserve, and analyse evidence data [30]–[32]. NF on the other hand is a branch of digital forensics which aims to reveal network cybercrimes. Thus, this paper focuses on NFTs.

Fig. 1. Digital forensics fields

III. NETWORK FORENSICS FIELD

Several investigation processes models have been proposed for NF in the literature. However, these models are proposed for specific purposes. For example, [33] proposed a new common process model and analyses several operations for NF as shown in Figure 2. They produced a new framework to solve the research limitations and review the work-in-progress. The proposed framework consists of four investigation processes: multi-sensor data fusion, identification of attack events, attack reconstruction, and incident response. Multi-sensor data fusion confirms that the complete incident/attack data is seized for investigation of the incident/attack. Identification of helpful network actions facilitates data decrease as unnecessary data is deleted. Attack reconstruction and traceback allow the trial of the attacker. Incident response enables improvement and reduces destruction [34], [35].
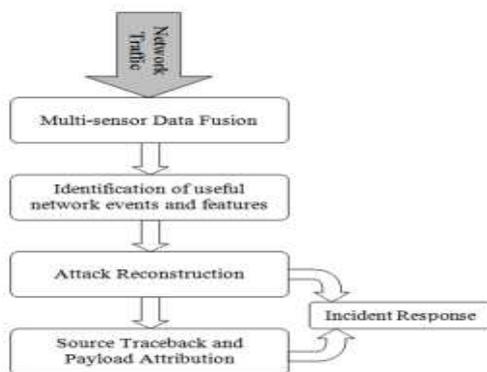
Fig. 2. Common process model for NFs field [33]

A common process framework for NF has been proposed by [36] as shown in Figure 3. It consists of nine investigation processes: preparation, detection, incident response, collection, preservation, examination, analysis, investigation, and presentation. The preparation process is used to prepare a mandatory authorization and screech warrant to avoid any illegal issues. The detection process is used to verify, check, and confirm the suspected attacks. The purpose of the incident response process is to put an action strategy of how to respond to future attacks and recover from the current destruction. The collection process is an important/significant process used to collect data from sensors, where is the preservation process is used to protect the integrity of the collected data. The examination process is used to check and evaluate the authentication or originality of the collected data. The analysis process is used to reconstruct the timeline of the events and reveal the evidence. The investigation process is used to verify the path from a victim network or system via any intermediary systems and communication pathways, back to the point of attack origination. Leveraging human psychosocial attribute, studies in [34], [35], [37], [38] developed human centric network forensic frameworks. Their frameworks and model contain diverse human behavioural component which is capable of distinguishing human at the network level. Extending the human component, studies in [39]–[41] integrated behavioural component as a process for network attribution. Attempt to further finetune the attribution was carried out using digital forensic readiness process, ranging from the cloud [30], [42]–[45] to the intranet traffic [46]. The final process presentation is used to present whole investigation tasks in a human language for legal personal and providing a declaration of several processes used to arrive at the conclusion [47].
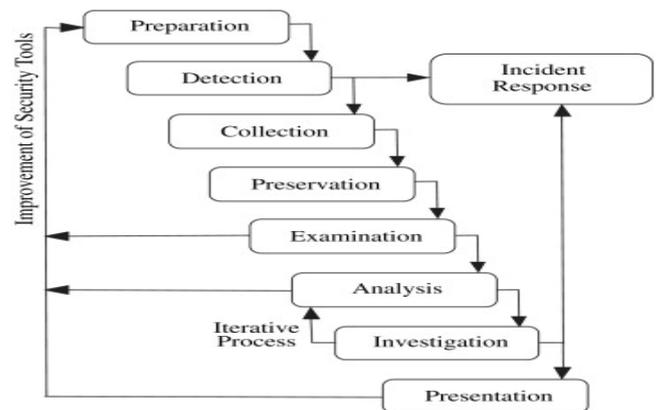
Fig. 3. Generic process model for NFs field [36]

A network forensic model for SYN attack has been proposed by [48] to offer effective preservation as shown in Figure 4. It consists of three investigation processes: collection and preservation module, analysis module, and preservation module. The collection and preservation process are used to seize whole network events from the network interface for

79

forensic analysis. The analysis module is used to analyse the whole collected data started in the host system. The purpose of the presentation module is to reveal the analysis module production if allowing port scanning attack [49], [50].
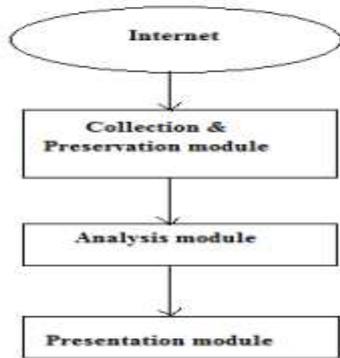

Fig. 4. Architecture model for NFs field [48]

A common model for could network forensics has been proposed by [51][7]. It consists of five investigation processes as illustrated in Figure 5: reporting, analysis, aggregation, separation, and data collection.
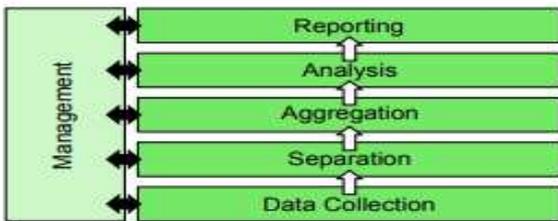

Fig. 5. Cloud forensics process model [52]

A common process for botnet forensics is presented by [52]. The specific limitation of the research which is existing in implementation is recognized and offered as challenges [45][53]. This model consists of nine investigation processes as displays in Figure 6: Preparation of security tools, Reorganizations of bots, incident response, collection, retention, inspection, analysis, investigation, and results.
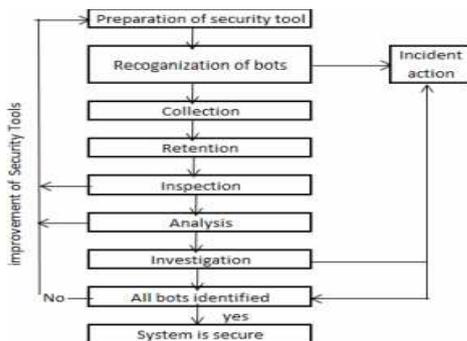

Fig. 6. Botnet process model [52]

A collection process model has been introduced by [54]. It consists of one collection process. The main purpose of this model is to collect evidence that can categorize the highly

precise potential evidence [41]. Several process models have been proposed for the NFs field, however, it suffers from redundant investigation processes. For, example [33] consists of four (4) processes, [36] entails nine(9) investigation processes, [48] comprises of three investigation processes, [51] includes five (5) investigation processes, [52] involves nine (9) investigation processes, and finally [54] has one investigation process. Therefore, the NFs field needs a high abstract model (metamodel) to combine and unify whole existing process models [55].

IV. NETWORK FORENSIC TOOLS

NFTs have been proposed for NF in the literature as shown in Figure 2. However, these tools are proposed for specific purposes.
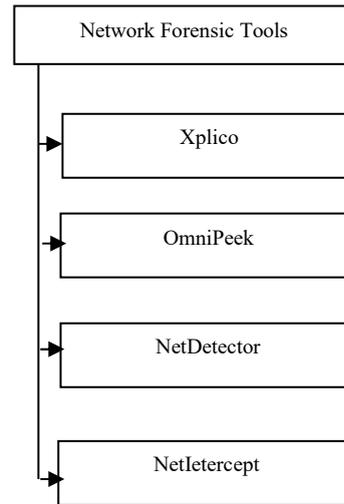

Fig. 7. Network forensics tools

For example, Xplico is an open-source network forensic analysis tool that is used to reconstructing audio, video, images, pdf, and several other text files from a network capture [53], [56], [57] It developed for the Linux platform. It has several capabilities:

- Collect application data.\
- Collect information from database/files using SQLite or MYSQL

Analysis capabilities: Support online and offline analysis of packet capture.

- Analyze live stream of traffic
- Support many protocols ARP, PPP, VLAN, IPV4, IPV6,
-      SNOOP, TCP, IRC, HYYP, SMTP, FTP, SIP, HTTP,   DNS, and UDP.
- Presentation and Reporting: Presented results in a

human-readable manner and producing data in colorful tables.
- Platform: Linux

- Tool supporting: it supports most of the digital forensic fields

The second NF tool is OmniPeek which is used to analyse collected packets [58], [59]. It was developed by WildPackets Inc. This tool has two major roles of network troubleshooting and procedure examination. It has many capabilities:

- Support email analysis sflow and netflow statistics
- Platform: Linux and Windows.
- GUI: easy to use (fast examining, drill-down, and correcting performing jams through a variety of network)
- Collect data from any network topology.
- Support many borders and links to an unrestricted amount of TimeLine.

The third NF tool is NetDetector which is one of the most famous NF tools [60]. This tool has been developed for security purposes [61]. It is used for the discovery of malicious activities in the network. It has many features:

- IDS tool
- Analysing how the attack did happen and by whom, when the attack did happen, what the proper actions can be carried to fix the attack.
- Analysing security protocols of the network.

The fourth NF tool is NetIetercept which is used to collect and analyse network traffics for real-time catching [60]. It has many features:

- It works with UDP and TCP protocols.
- Advanced examination skills
- GUI that permits investigators to select proper features, and create complete reports, invisible to network users.

Throughout this survey, it is very clear that the NF field has several forensic tools which differ in their roles and capabilities [62]. For example, the Xplico tool has many capabilities to collect. Analyse, and present network activities, however, it is specific for Linux OS, whereas OmniPeek tool is supported by two platforms (Linux and Windows), however, it is not a pure forensics tool [63]. It is used for network troubleshooting and procedure examination. Although, NetDetector is the most NF tool, however, it is developed for security purposes. It does not have the capabilities to analyse and present evidence. Therefore, the best NF tool amongst these four tools is Xplico which has several capabilities to identify, collect, examine, analyse, and present network crimes [64].

V. DISCUSSION

The process of understanding the effectiveness and reliability of a network forensic tools is often hinged on the underlying model on which specific tool was developed. Whilst NetIetercept and NetDetector could provide a veritable tool for potential evidence acquisition: a phase of the network forensic models, they are largely limited to that phase of forensics. This, therefore, limits the potential effectiveness of the tools. Therefore, a phase specific tool would always be limited to the actual phase it is designed to address. Xplico, on the other hand, has the potential to span multiple phases of the network forensic model. Whilst the use is not limited to network forensic analysis, it has the potential to evolve towards a one-stop-shop to network forensics. This is similar to tools such as Autopsy, which offers open-source forensic capability. Furthermore, the logic of cross platform gives an added functionality for all forensic investigators. Going forward, therefore, network forensic researchers and practitioners can leverage the functionalities provided by this open-source tools for effective forensic investigation.

VI. CONCLUSION

Several NFTs have been offered for the network forensic field to identify, capture, collect, analyse, and document network incidents. These tools are varying in their roles and functionalities. Thus, this paper, conducted a comparative analysis amongst four famous NFTs to select the best forensic tool. The outcome of this paper shows that the Xplico tool is the best which covers whole forensic tasks (identification, collection, examination, analysis, and presentation). The future work of this paper is to review more NFTs and conduct real scenario/case studies to evaluate the capabilities of the Xplico tool.

REFERENCES

[1] I. R. Adeyemi, S. Abd Razak, and N. A. N. Azhan, "A review of current research in network forensic analysis," Int. J. Digit. Crime Forensics, vol. 5, no. 1, pp. 1–26, 2013.

[2] I. Adeyemi, S. Razak, and N. Azhan, "Identifying critical features for network forensics investigation perspectives," Int. J. Comput. Sci. Inf. Secur., vol. 10, no. Issue 9, p. 108, 2012.

[3] V. R. Kebande, N. M. Karie, and H. S. Venter, "A generic Digital Forensic Readiness model for BYOD using honeypot technology," in 2016 IST-Africa Week Conference, 2016, pp. 1–12.

[4] V. R. Kebande, S. O. Baror, R. M. Parizi, K.-K. R. Choo, and H. S. Venter, "Mapping digital forensic application requirement specification to an international standard," Forensic Sci. Int. Reports, vol. 2, p. 100137, 2020.

[5] S. O. Baror, H. S. Venter, and R. Adeyemi, "A natural human language framework for digital forensic readiness in the public cloud," Aust. J. Forensic Sci., vol. 0, no. 0, pp. 1–26, 2020, doi: 10.1080/00450618.2020.1789742.

[6] S. O. Baror, R. A. Ikuesan, and H. S. Venter, "A defined digital forensic criteria for cybercrime reporting," Proc. 15th Int. Conf. Cyber Warf. Secur. ICCWS 2020, no. ii, pp. 617–626, 2020, doi: 10.34190/ICCWS.20.056.

[7] N. M. Karie and V. R. Kebande, "Building ontologies for digital forensic terminologies," Int. J. Cyber-Security Digit. Forensics, vol. 5, no. 2, pp. 75–83, 2016.

[8] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," 2016, doi: 10.1109/FiCloud.2016.57.

[9] A. Al-Dhaqm, S. A. Razak, S. H. Othman, A. Nagdi, and A. Ali, "A generic database forensic investigation process model," J. Teknol., vol. 78, no. 6–11, 2016, doi: 10.11113/jt.v78.9190.

[10] A. Ali, A. Al-Dhaqm, and S. A. Razak, "Detecting Threats in Network Security by Analyzing Network Packets using Wireshark," 2014.

[11] M. Bakhtiari and A. M. R. Al-dhaqm, "Mechanisms to Prevent lose Data."

[12] 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), 2014, pp. 322–327.

[13] S. Abd Razak, N. H. M. Nazari, and A. Al-Dhaqm, "Data Anonymization Using Pseudonym System to Preserve Data Privacy," IEEE Access, vol. 8, pp. 43256–43264, 2020.

[14] 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 Sci. Int. Reports, vol. 2, p. 100122, 2020.

[15] A. Al-Dhaqm et al., "CDBFIP: Common database forensic investigation processes for Internet of Things," IEEE Access, vol. 5, pp. 24401–24416, 2017.

[16] 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, doi: 10.1371/journal.pone.0170793.

[17] A. Al-Dhaqm et al., "Categorization and organization of database forensic investigation processes," IEEE Access, vol. 8, pp. 112846–112858, 2020.

[18] A. Aldhaqm, S. Abd Razak, S. H. Othman, A. Ali, and A. Ngadi, "Conceptual investigation process model for managing database forensic investigation knowledge," Res. J. Appl. Sci. Eng. Technol., vol. 12, no. 4, pp. 386–394, 2016.

[19] M. Ngadi, R. Al-Dhaqm, and A. Mohammed, "Detection and prevention of malicious activities on RDBMS relational database management systems," Int. J. Sci. Eng. Res., vol. 3, no. 9, pp. 1–10, 2012.

[20] A. Al-Dhaqm, S. Razak, and S. H. Othman, "Model derivation system to manage database forensic investigation domain knowledge," in 2018 IEEE Conference on Application, Information and Network Security (AINS), 2018, pp. 75–80.

[21] 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, doi: 10.1109/ACCESS.2020.3008696.

[22] A. Al-Dhaqm et al., "Database forensic investigation process models: A review," IEEE Access, vol. 8, pp. 48477–48490, 2020.

[23] A. Aldhaqm, S. Abd Razak, and S. H. Othman, "Common Investigation Process Model for Database Forensic Investiga-tion Discipline," in the 1st ICRIL-International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia, 2015, pp. 297–300.

[24] I. U. Onwuegbuzie, S. Abd Razak, I. Fauzi 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, p. e0237154, 2020.

[25] A. Al-Dhaqm, S. Razak, R. A. Ikuesan, V. R Kebande, and S. Hajar Othman, "Face Validation of Database Forensic Investigation Metamodel," Infrastructures, vol. 6, no. 2, p. 13, 2021.

[26] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Towards adapting metamodeling approach for the mobile forensics investigation domain," in International Conference on Innovation in Science and Technology (lICIST), 2015, p. 5.

[27] A. Al-Dhaqm, S. Abd 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.

[28] A. Ali, S. Abd Razak, S. H. Othman, and A. Mohammed, "Extraction of common concepts for the mobile forensics domain," in International Conference of Reliable Information and Communication Technology, 2017, pp. 141–154.

[29] R. A. Ikuesan, S. O. Ganiyu, M. U. Majigi, Y. D. Opaluwa, and H. S. Venter, "Practical Approach to Urban Crime Prevention in Developing Nations," in ACM International Conference Proceeding Series, 2020, pp. 1–8, doi: 10.1145/3386723.3387867.

[30] V. Kebande, H. S. Ntsamo, and H. S. Venter, "Towards a prototype for achieving digital forensic readiness in the cloud using a distributed NMB solution," in European Conference on Cyber Warfare and Security, 2016, p. 369.

[31] N. M. Karie, V. R. Kebande, and H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," Forensic Sci. Int. Synerg., vol. 1, pp. 61–67, 2019.

[32] A. Al-dhaqm, M. Bakhtiari, E. Alobaidi, and A. Saleh, "Studding and Analyzing Wireless Networks Access points."

[33] E. S. Pilli, R. C. Joshi, and R. Niyogi, "A framework for network forensic analysis," in International Conference on Advances in Information and Communication Technologies, 2010, pp. 142–147.

[34] I. R. Adeyemi, S. Abd Razak, M. Salleh, and H. S. Venter, "Leveraging human thinking style for user attribution in digital forensic process," 2017.

[35] A. R. Ikuesan, S. Abd Razak, H. S. Venter, and M. Salleh, "Polychronicity tendency-based online behavioral signature," Int. J. Mach. Learn. Cybern., vol. 10, no. 8, pp. 2103–2118, 2019.

[36] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," Digit. Investig., vol. 7, no. 1–2, pp. 14–27, 2010.

[37] I. R. Adeyemi, S. A. Razak, H. S. Venter, and M. Salleh, "High-level online user attribution model based on human Polychronic-Monochronic tendency," in 2017 IEEE International Conference on Big Data and Smart Computing, BigComp 2017, 2017, pp. 445–450, doi: 10.1109/BIGCOMP.2017.7881753.

[38] I. R. Adeyemi, S. A. Razak, and M. Salleh, "Individual difference for HCI systems: Examining the probability of thinking style signature in online interaction," in Proceedings - 2016 4th International Conference on User Science and Engineering, i-USEr 2016, 2017, pp. 51–56, doi: 10.1109/IUSER.2016.7857933.

[39] V. R. Kebande and N. M. Karie, "A Framework for Integrating Multimodal Biometrics with Digital Forensics," vol. 4, no. November 2015, pp. 498–507, 2016, doi: 10.17781/P001929.

[40] A. R. Ikuesan, M. Salleh, H. S. Venter, S. A. Razak, and S. M. Furnell, "A heuristics for http traffic identification in measuring user dissimilarity," Human-Intelligent Syst. Integr., vol. 2, pp. 17–28, 2020.

[41] A. R. Ikuesan and H. S. Venter, "Digital forensic readiness framework based on behavioral-biometrics for user attribution," in 2017 IEEE Conference on Application, Information and Network Security (AINS), 2017, pp. 54–59.

[42] V. R. Kebande and H. S. Venter, "A Cloud Forensic Readiness Model Using a Botnet as a Service," in The International Conference on Digital Security and Forensics (DigitalSec2014), 2014, pp. 23–32, doi: 10.13140/2.1.4880.2249.

[43] V. R. Kebande and H. S. Venter, "Adding event reconstruction to a Cloud Forensic Readiness model," in 2015 Information Security for South Africa (ISSA), 2015, pp. 1–9.

[44] V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," Aust. J. Forensic Sci., vol. 50, no. 5, pp. 552–591, 2018.

[45] V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," Aust. J. Forensic Sci., vol. 50, no. 5, 2018, doi: 10.1080/00450618.2016.1267797.

[46] S. M. Makura, H. S. Venter, R. A. Ikuesan, V. R. Kebande, and N. M. Karie, "Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes," 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, pp. 200–205, 2020, doi: 10.1109/ICIoT48696.2020.9089494.

[47] D. Ellison, H. Venter, and A. Ikuesan, "An Improved Ontology for Knowledge Management in Security and Digital Forensics," in European Conference on Cyber Warfare and Security, 2017, pp. 725--733.

[48] D. Avasthi, "Network Forensic Analysis with Efficient Preservation for SYN Attack," Int. J. Comput. Appl., vol. 46, no. 24, pp. 17–22, 2012.

[49] D. Ellison, R. A. Ikuesan, and H. S. Venter, "Ontology for Reactive Techniques in Digital Forensics," 2019 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2019, pp. 83–88, 2019, doi: 10.1109/AINS47559.2019.8968696.

[50] N. M. Karie, V. R. Kebande, H. S. Venter, and K.-K. R. Choo, "On the importance of standardising the process of generating digital forensic reports," Forensic Sci. Int. Reports, vol. 1, p. 100008, 2019.

[51] T. Gebhardt and H. P. Reiser, "Network forensics for cloud computing," in IFIP International Conference on Distributed Applications and Interoperable Systems, 2013, pp. 29–42.

82

[52] M. Thapliyal, A. Bijalwan, N. Garg, and E. S. Pilli, "A generic process model for botnet forensic analysis," in Proceedings of the Conference on Advances in Communication and Control Systems-2013, 2013, pp. 98–102.

[53] V. R. Kebande, N. M. Karie, and H. S. Venter, "Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures," in 2017 1st International Conference on Next Generation Computing Applications (NextComp), 2017, pp. 54–60.

[54] 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. Snort. Retrieved December, 2013, vol. 21, p. 2016.

[55] V. R. Kebande and H. S. Venter, "Adding event reconstruction to a Cloud Forensic Readiness model," 2015, doi: 10.1109/ISSA.2015.7335050.

[56] A. R. Ikuesan and H. S. Venter, "Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet?," Digit. Investig., vol. 30, pp. 73–89, 2019.

[57] A. Tekeoglu and A. S. Tosun, "Investigating security and privacy of a cloud-based wireless IP camera: NetCam," in 2015 24th International Conference on Computer Communication and Networks (ICCCN), 2015, pp. 1–6.

[58] M. Wazid, A. Katal, R. H. Goudar, and S. Rao, "Hacktivism trends, digital forensic tools and challenges: A survey," in 2013 IEEE Conference on Information & Communication Technologies, 2013, pp. 138–144.

[59] I. R. Adeyemi, S. Abd Razak, and M. Salleh, "A psychographic framework for online user identification," in 2014 International Symposium on Biometrics and Security Technologies (ISBAST), 2014, pp. 198–203.

[60] R. Misra and R. Dhir, "Design of Network Forensic System Based on Honeynet," Int. J. Innov. Eng. Technol.

[61] S. Omeleze and H. S. Venter, "Digital forensic application requirements specification process," Aust. J. Forensic Sci., vol. 51, no. 4, pp. 371–394, 2019.

[62] H. Munkhondya, A. Ikuesan, and H. Venter, "Digital forensic readiness approach for potential evidence preservation in software-defined networks," in 14th International Conference on Cyber Warfare and Security, ICCWS 2019, 2019, pp. 268–276.

[63] S. Pretorius, A. R. Ikuesan, and H. S. Venter, "Attributing users based on web browser history," in 2017 IEEE Conference on Application, Information and Network Security (AINS), 2017, pp. 69–74.

[64] H. Munkhondya, A. R. Ikuesan, and H. S. Venter, "A Case for a Dynamic Approach to Digital Forensic Readiness in an SDN Platform," in International Conference on Cyber Warfare and Security, 2020, pp. 584–XVIII.