Advanced Research on Information Systems Security

ISSN: 2795-4609 | ISSN: 2795-4560
Print & Online

Digital Forensics on Trending Technologies: A systematic Literature Review

Ricardo S. Santos

COPELABS – Universidade Lusófona, Campo Grande 388, Lisboa, 1700-097, Portugal
Email: p6221@ulusofona.pt

Abstract

Currently enterprises tend to approach Cyber-Security using a prevent/mitigate approach. However, when an attack happens it is of extreme importance to do extensive digital forensic investigation. This investigation will allow to know exactly, where, how and what went wrong. Moreover, digital forensics face difficult challenges such as, the evolution of technology (Cloud Computing, Internet of Things (IoT), *etc.*) and the ingenuity of attackers that always encounter new ideas to achieve their objectives. Thus, this work's main goal is to do a systematic literature review of publicly available and indexed papers on the digital forensics field with special focus on trending technology areas.

Keywords: Digital Forensics; Cyber-Security; Internet of Things; Cloud Computing; Big Data;

Citation: R. S. Santos, "Digital Forensics on trending technologies: A systematic literature review", ARIS2-Journal, vol. 4, no. 2, pp. 04–15, Dec. 2024.

DOI: https://doi.org/10.56394/aris2.v4i2.40

* Corresponding author. Email address: p6221@ulusofona.pt

1. Introduction

The Cyber-Security field is in constant change and is of extreme importance nowadays. With the advances of IoT and mobile telecommunications (5G, 6G and future generations) devices that were seen as mere objects can now be connected to the Internet and communicate between them. For instance, fridges, toasters, ovens, light bulbs or doors. Despite having positive advantages and since these devices are online, they can be a target for an attacker. In a near future, ransomware attacks or Denial-of-Service (DoS) on so called smart devices may become a reality. An example of a large scale IoT attack can be on smart water meters, where an attacker can alter the consumption of water from an entire city. This type of attack can generate huge financial impact on the water supply company. Moreover, since these IoT devices are generally connected to the user's Wireless Fidelity (Wi-Fi) router, in an extreme case the attacker only needs to have access to the victim's access point via a man in the middle attack.

Furthermore, with the current wars occurring around the Globe, Cyber-Security plays an important role in the defense of a country. For instance, imagine an enemy country controlling the power grids, water supplies, and military installations remotely. In a more extreme scenario, the enemy may gain access to a nuclear power plant allowing the shutdown or an explosion in one of the reactors. In addition, in recent years there are known cyber-attacks between countries to steal money or cryptocurrencies sometimes to finance military programs.

Thus, to analyze how cyber-attacks are performed or to know how an attacker managed to get access to a device or enterprise network, it is important to perform digital forensics. Generally, this investigation's main goals are on the one hand, to implement security measures and patch eventual security breaches that will try to prevent future attacks and in the other hand, find the culprits of such attacks and present them to justice.

The main goal of this work is to perform a systematic literature review of recently published papers in the digital forensics field. Thus, the remainder of this work is divided as follows. First, a brief explanation on how a typical digital forensic investigation is performed is presented in Section 2. Afterwards, in Section 3 the research methodology used to select the analyzed papers is shown, followed by the results that are presented and briefly comment in Section 4. Finally, in Section 5 a conclusion about the topic of interest is made.

2. How a typical digital forensic investigation is performed

Whenever there is a Cyber-attack to a company, it is policy to investigate how the attackers were able to perform it and how did they bypass supposedly secure systems. This is done not only to patch eventual security breaches but also to prevent future attacks. This type of investigation is often called digital forensic investigation. The investigation model used depends on the scenario, but usually the most known and used is the Kruse & Heiser model [1]. This model is composed of four steps as shown in Figure 1 and briefly described in the following subsections.

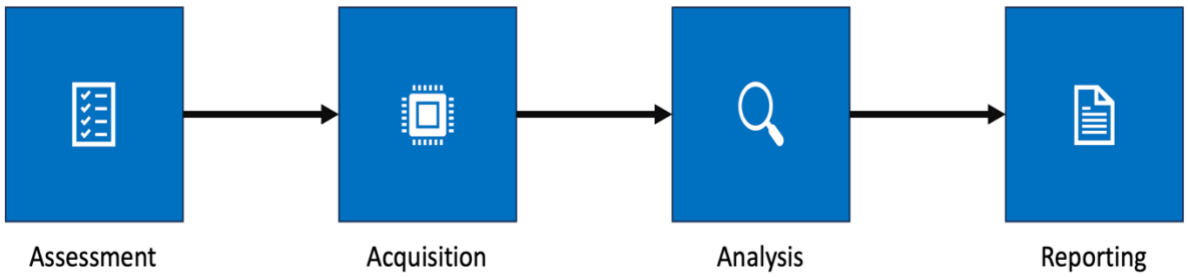

Figure 1: Kruse & Heiser Model.

2.1. Assessment

The assessment is the first step when performing a digital forensic investigation. In this step, the scope and venue of the investigation are defined. The identification of the stakeholders, sources of evidence, the tools and qualified personnel needed are also established. The collection of the legal documentation necessary to enter and search for evidence in a company or in private property of a suspect is also obtained. Without this documentation, eventual evidence collected can be posed as inadmissible in court, since in most countries a grant from a judge is needed for the majority of investigations.

2.2. Acquisition

The acquisition is the phase where hardware is seized for later examination. During this stage extra care is needed so that the system state is not altered. The integrity of the evidence must be preserved at all costs. As a rule of thumb, the investigators should never work on the originals and should create images and backups. Moreover, integrity checks should also be used to prove that no evidence was altered since its collection.

2.3. Analysis

As the name implies, this is the stage where the seized hardware is analyzed in an attempt to discover potential evidence. Attackers often use anti-forensics tactics such as, hidden partitions or encryption to hide files. Deleted files are also a common tactic to hide evidence, but this does not always work since in some scenarios they can be recovered. Steganography is also widely used to hide messages in multimedia files. The evidence found must then be interpreted to hopefully reconstruct the crime scene.

2.4. Reporting

Reporting is the last stage of a digital forensic investigation, and it consists in the production of a document to present to court and/or company. This document usually contains every task that was performed during the investigation, the list of equipment seized, first response documentation, user manuals, logs, timelines, *etc*. This step is critical since without a robust documentation, the court can declare the evidence inadmissible. Moreover, the produced documentation should allow other investigators to reproduce the findings.

3. Research Methodology

Given the large database of papers in this area, a method to select admissible papers to be presented in this work had to be used. To do so, the Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) Model [2] was chosen. The PRISMA model allows the reduction of the search query and allows the selection of adequate papers to the research in question. This model's first task is to select a set of keywords that are going to be used to search a database of papers. In this work, the searches were performed in IEEE Xplore [3] since its one of the most know and reputable sources for research papers available online. The set of keywords used can be seen in Table 1.

Table 1: Keywords used to search potential papers.

Keyword	Operator
Digital Forensics	AND
Challenges	OR
Cloud Computing	OR
Internet of Things	OR
Social Media	OR
Automotive	OR
Big Data	OR

To make the search more relevant, a search filter was applied so that only papers publish in 2018 or afterwards were returned. Using the settings in Table 1 and the search filter a total of 112 papers were returned.

3.1 Screening and Eligibility

From the returned papers, an analysis was performed to determine the eligible ones to be analyzed in the following section. This process was performed by the three steps visible in Figure 2. From the performed analysis a total of 20 papers were selected.

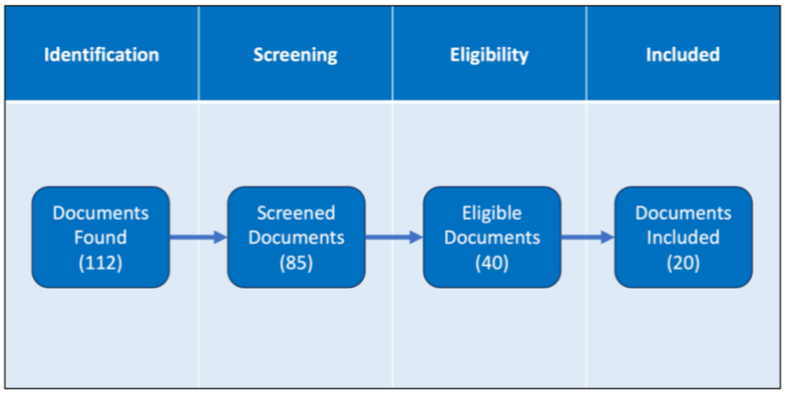

Figure 2 - Selection process based on the PRISMA model.

4. Results

In this section, the papers selected using the PRISMA model are analyzed. To provide a better organization of this section, the papers were divided into categories that are represented by the following subsections.

4.1. Digital Forensics in Cloud Computing

The usage of Cloud Computing is in constant grow and is becoming indispensable for some enterprises. With the growth of this technology, new challenges for digital forensics arise. As one may know, cloud computing relies mainly in Virtualization and offers three main services:

1) Infrastructure as a Service (IaaS)
2) Platform as a Service (PaaS)
3) Software as a Service (SaaS)

To further understand the differences between the three services, one should have in mind the following items:

- Applications
- Data
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

In the case of IaaS, the cloud user manages the applications, data, runtime, middleware and operating system. While in PaaS, the user only manages the applications and runtime. In SaaS, the user only utilizes the service. It does not manage anything. Now that one has some knowledge about the available services in Cloud Computing, an analysis on the challenges of Digital Forensics in this type of scenario is made below.

Due to the use of virtualization and contrary to local premises, the data is no longer in one place, for instance in a hard drive. This is one of the challenges that digital forensics face in Cloud Computing. Since the data in spread across multiple places and sometimes even spread across different servers, data analysis and reconstruction becomes a non-trivial task [4]. Furthermore, when a user decides to free the resources that it is occupying the data is immediately deleted resulting in a harder detection of attacks and evidence collection.

In recent years, new methodologies to circumvent these problems have been proposed. For instance, in [5] the authors proposed a framework for analyzing cloud logs and extract meaningful information. This information can help the investigators carrying the operation. In their framework, the authors proposed some useful features such

as, the extraction of Uniform Resource Locator (URL) hits and Internet Protocol (IP) addresses from the logs. Another approach was used in [6], where a mechanism to detect malicious behavior on the cloud was proposed. This mechanism performs a memory analysis on potential malicious virtual machines. In [7], a secure logging scheme was proposed to encrypt cloud logs. The system not only protects sensible user information that may be present in logs but is also capable of detecting Distributed Denial of Server (DDoS) attacks.

Despite the advances in this area, digital forensics in Cloud Computing will be an active research area for the next few years due to the complex nature and constant evolution of such environment.

4.2. Digital Forensics in IoT

The usage of IoT has been growing in recent years due to their low implementation price and rapid deployment model. The general idea of IoT is to interconnect devices creating a Wireless Sensor Network (WSN) to share data. For instance, temperature values collected from a sensor with the aim to detect forest fires. Moreover, the application scope of IoT has been increasing in recent years. Areas such as, education, agriculture, transport and medical are experimenting with IoT devices. It is expected that this scope will only increase in coming years. These applications and the types of devices used imply new challenges in the digital forensics area. Since these devices are generally optimized for low power consumption and computing power, the security field is sometimes forgotten. Thus, IoT is becoming a honey pot for attackers. To attack such devices, there are four main areas that an attacker can explore [8]:

- Hardware
- Software
- Data
- Protocol

In the hardware case, an attacker can insert a malicious node in the network or interfere in the radio frequency of the devices. Moreover, since these devices are usually placed in remote areas an attacker can simply discover where it is and change its characteristics without no one noticing. The software attack consists in tampering with the operating system, firmware, or a web application (if present). In this case, such attacks can be performed using phishing, malware, trojans, DDoS or breaches in the system. The data attack can happen as a leak of valuable data, such as sensor values or location information. Since IoT devices generate great amounts of data, this type of attacks can have severe consequences. Finally, the protocol attack consists in tampering the protocol used by the IoT devices to communicate between them.

Due to the complex nature and heterogeneity of IoT hardware and architecture, when attack happens it may be difficult to perform a forensic analysis. On the one hand, since the devices can be placed anywhere, it may be difficult to obtain a search warrant or discover where the devices are placed. Moreover, the IoT devices can be connect to more than one network, making gathering evidence a challenge. Furthermore, due to the simple nature of these devices the memory capacity is limited. Thus, data can be easily overridden if it is not backed up to another device, meaning that data collection can be a non-trivial task. On the other hand, since the data generated

by these devices can be stored in multiple locations in the cloud it can be difficult for an attacker to delete traces of their actions.

To address these challenges clever approaches have been proposed recently such as in [9], where the authors proposed a framework for IoT data acquisition and analysis. This framework resorts to a mobile and desktop application developed by the authors to collect artifacts and reconstruct a timeline of events. In [10], the author proposed a proactive model that resorts to evidence classification to evaluate cybercrime digital evidence. The authors in [11], presented a novel way to preserve evidence in IoT scenarios using Blockchain instead of traditional hashes. This method promises to improve the integrity and authenticity of collected evidence. In [12], an approach using artificial intelligence (AI) to detect intrusions in IoT devices was presented. This approach utilizes a lightweight deep neural network to classify network traffic and detect an attack. In [13], the authors proposed a digital chain of custody to IoT applied in healthcare facilities that complies with the ISO/IEC 27050:2021 standard. Finally, in [14], a framework for a forensic analysis in a Raspberry Pi was developed. The process starts by identifying evidence, followed by the acquisition. To preserve the data, the authors rely on the usage of blockchain.

The digital forensics in the IoT field has been subject to many studies in recent years but, despite the good advances made in this area there are still some challenges to overcome in the future.

4.3. Digital Forensics in Social Media

The usage of social media has gain rapid adoption in recent years. Due to the large number of users, it has become an area of interest to cybercriminals. Currently, scams carried out through social media are becoming more frequent. For example, using WhatsApp, Telegram or Messenger, criminals can send fraudulent messages to a victim saying that one of their relatives needs money with urgency. Moreover, criminals can take advantage of pictures and videos posted on social media to convince the victims that they are talking with their relatives. Thus, when such scams occur a properly performed digital forensic investigation is needed to prevent future ones.

The digital forensics in social media is also a complex operation. On the one hand, privacy concerns arise from accessing the victims or suspects social media. This can be a problem later in court without a proper warrant. On the other hand, the large volume of data present in social media can also be a challenge for a forensic investigation.

To address these challenges, in recent years several approaches were proposed. One of them is [15], where the authors proposed an evidence acquisition model for social media. This model's first step is to acquire the credentials followed by web crawling to collect data. The data is then analyzed using semantic analysis. The authors in [16], presented a framework that allows forensic investigators to retrieve social media messages from volatile memory. To do so, an Android phone was used to install and interact with Facebook. Afterwards, an image of the internal memory was created. This image was then analyzed using a software where it was possible to discover: 1) Username; 2) Name; 3) Email address; 4) List of Friends; 5) News Feed; 6) User Credentials (Password is a hash); 7) User Activity; 8) IP address. Thus, allowing a forensic investigator to gain substantial knowledge about the suspect/victim. In [17], an approach to perform a forensic investigation on social media and

web app messaging is presented. The authors used real hardware and available forensic tools. More specifically, a Xiaomi Redmi Note 7 and MOBILedit [18] and FINALMOBILE [19]. Then, evidence collection was performed targeting the following apps: 1) WhatsApp; 2) Messenger; 3) Instagram; 4) Telegram. The results shown reveal that, from WhatsApp and Telegram it was possible to extract Images, Videos, Files and Records. While from Messenger and Instagram, nothing was recovered. One of the factors that contributed to this fact can be attributed to a non-Rooted access to the phone. Nevertheless, the recovered files can be decisive for a forensic investigation. Finally, in [20] a framework to retrieve unsent messages from social media apps was presented. This framework is composed of nine steps to perform the acquisition of digital artifacts.

As one can conclude, performing digital forensics in social media is challenging. To worsen this challenge, most users access social media through their smartphones. These devices possess some security measures that make extracting evidence a non-trivial task. Thus, future research in social media forensics can still be of interest in the coming years.

4.4. Digital Forensics in Automotive Systems

Most modern vehicles include some type of infotainment and/or satnav system allowing the user to interact or connect their smartphones to them. Thus, in a digital forensic investigation they can provide some valuable information. However, due to their complex nature the collection of evidence is not straight forward.

In recent years several approaches were proposed to analyze the infotainment and satnav systems. For instance, in [21] the authors proposed an approach to retrieve information from them. To do so, the following tools were utilized: 1) Encase; 2) FTK Imager; 3) FileZilla FTP; 4) Live Forensics. Then, the authors removed an SD Card that was installed in a 2014 Kia Sportage where data related to the satnav was found. Afterwards, the authors tried Universal Serial Bus (USB) and Bluetooth connections without success of retrieving data. A Wireless Fidelity (Wi-Fi) connection was also used, and the authors were able to identify that the infotainment system uses Android and Linux as operating systems. From Linux nothing was extracted, but from Android some media files were successfully extracted. In [22], the authors did some studies on the Event Data Recorder (EDR) present in some modern vehicles. In simple terms, this module is responsible for recording data before, during and after a crash [23]. Thus, this module was utilized to detect if there is evidence of hacking in the data retrieved. In autonomous cars this approach is very interesting because it allows to check if a location spoofing occurred in case of an accident. Nevertheless, in more “traditional” cars the detection of hacking is also useful especially since the number of electronic modules in cars that can suffer attacks has grown significantly.

The digital forensics field focused on the automotive industry has been an active research area in recent years. Since self-driving cars are expected to be a reality in a near future, this area is expected to evolve even more due

to the creative ways that hackers will manage to implement. For instance, changing the destination of a self-driving car or even shut down the vehicle remotely.

4.5. Digital Forensics in Big Data

Due to the rapid development of the internet and the increasing number of users, the data generated in upcoming years is expected to be in the order of Zettabytes (ZB). More specifically, according to the IDC in 2025 the data generated around the globe will be 33 ZB [24]. For digital forensics this number is worrying because it means that in a forensic investigation the amount of data that requires analysis will also increase dramatically.

To address this challenge, several approaches have been introduced in recent years. For instance, in [25], a framework targeting digital forensics of Big Data is presented. The authors used artificial intelligence and Big Data technology to analyze and preserve the data. In [26], the authors provided some solutions and tools on how to detect and prevent attacks on Big Data using digital forensics. A framework for large datasets based on a distributed graph analysis is proposed by the authors in [27]. To do so, the first step is to perform some pre-processing to allow the construction of the graphs. Then, a set of algorithms is applied to find valuable information. This information is then analyzed by a digital forensic investigator.

Concluding, one can expect that in the future this research area is going to be increasingly active since the data generated globally is expected to grow. Since cybercriminals are always attacking, it is critical to have relevant frameworks to analyzed large amounts of data.

5. Conclusions

In this paper, a systematic literature review on digital forensics in trending areas was performed. By resorting to the PRISMA methodology and IEEE Xplore, relevant papers in the digital forensics area were found. More specifically, papers that present solutions to digital forensics in Cloud Computing, IoT, Social Media, Automotive and Big Data were analyzed and briefly commented. From the performed analysis in the previous Section, one can conclude that some relevant research has been done in these areas. However, there is still room for future improvements that will benefit and help forensic analysis to be performed more efficiently. Thus, helping combat cybercrime and bring the responsible to justice.

References

[1] W. Kruse and J. Heiser, “Computer Forensics: Incident Response Essentials,” Addison Wesley, Indianapolis, 2002.

[2] PRISMA. "Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA).” Internet: http://www.prisma-statement.org/, 2023 [Nov. 20, 2023].

[3] IEEE. “IEEE Xplore.” Internet: https://ieeexplore.ieee.org/Xplore/home.jsp, 2023 [Nov. 15, 2023].

[4] R. Neware and A. Khan, "Cloud Computing Digital Forensic challenges," 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, 2018, pp. 1090-1092, [Online]. Available: 10.1109/ICECA.2018.8474838.

[5] Z. AlSaed, M. Jazzar, A. Eleyan, T. Bejaoui and S. Popoola, "An Integrated Framework Implementation For Cloud Forensics Investigation Using Logging Tool," 2022 International Conference on Smart Applications, Communications and Networking (SmartNets), Palapye, Botswana, 2022, pp. 01-06, [Online]. Available: 10.1109/SmartNets55823.2022.9994001.

[6] G. Chen, D. Wu, G. Chen, P. Qin, L. Zhang and Q. Liu, "Research on Digital Forensics Framework for Malicious Behavior in Cloud," 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chengdu, China, 2019, pp. 1375-1379, [Online]. Available: 10.1109/IAEAC47372.2019.8997702.

[7] S. N. Joshi and G. R. Chillarge, "Secure Log Scheme for Cloud Forensics," 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, 2020, pp. 188-193, [Online]. Available: 10.1109/I-SMAC49090.2020.9243428.

[8] M. Dave, "Internet of Things Security and Forensics: Concern and Challenges for Inspecting Cyber Attacks," 2022 Second International Conference on Next Generation Intelligent Systems (ICNGIS), Kottayam, India, 2022, pp. 1-6, [Online]. Available: 10.1109/ICNGIS54955.2022.10079829.

[9] H. Chi, T. Aderibigbe and B. C. Granville, "A Framework for IoT Data Acquisition and Forensics Analysis," 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 5142-5146, [Online]. Available: 10.1109/BigData.2018.8622019.

[10] M. Rasmi Al-Mousa, "Generic Proactive IoT Cybercrime Evidence Analysis Model for Digital Forensics," 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 654-659, [Online]. Available: 10.1109/ICIT52682.2021.9491718.

[11] Y. Makadiya, R. Virparia and K. Shah, "," 2023 10th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2023, pp. 490-495, [Online]. Available: https://ieeexplore.ieee.org/document/10112358.

[12] R. Zhao et al., "A Novel Intrusion Detection Method Based on Lightweight Neural Network for Internet of Things," in IEEE Internet of Things Journal, vol. 9, no. 12, pp. 9960-9972, 15 June15, 2022, [Online]. Available: 10.1109/JIOT.2021.3119055.

[13] L. Donga, R. K. Raj and S. Mishra, "Internet of Healthcare Things (IoHT): Towards a Digital Chain of Custody," 2022 IEEE 10th International Conference on Healthcare Informatics (ICHI), Rochester, MN, USA, 2022, pp. 524-526, [Online]. Available: 10.1109/ICHI54592.2022.00097.

[14] G. Rekha and B. U. Maheswari, "Raspberry Pi Forensic Investigation and Evidence Preservation using Blockchain," 2021 International Conference on Forensics, Analytics, Big Data, Security (FABS), Bengaluru, India, 2021, pp. 1-5, [Online]. Available: 10.1109/FABS52071.2021.9702622.

[15] V. Pawar and D. V. Jose, "Evidence Acquisition in Social Media for Cyber Crime," 2022 Fourth International Conference on Cognitive Computing and Information Processing (CCIP), Bengaluru, India, 2022, pp. 1-6, [Online]. Available: 10.1109/CCIP57447.2022.10058653.

[16] R. D. Thantilage and N. A. Le Khac, "Framework for the Retrieval of Social Media and Instant Messaging Evidence from Volatile Memory," 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Rotorua, New Zealand, 2019, pp. 476-482, [Online]. Available: 10.1109/TrustCom/BigDataSE.2019.00070.

[17] R. F. Abu Hweidi, M. Jazzar, A. Eleyan and T. Bejaoui, "Forensics Investigation on Social Media Apps and Web Apps Messaging in Android Smartphone," 2023 International Conference on Smart Applications, Communications and Networking (SmartNets), Istanbul, Turkiye, 2023, pp. 1-7, [Online]. Available: 10.1109/SmartNets58706.2023.10216267.

[18] MobilEdit. "MobilEdit." Internet: https://www.mobiledit.com, 2023 [Dec. 10, 2023].

[19] FinalMobile. "Finalmobile" Internet: http://fmf.finaldata.com/Download/fmf4.html, 2023 [Dec. 10, 2023].

[20] L. Rosselina, Y. Suryanto, T. Hermawan and F. Alief, "Framework Design for the Retrieval of Instant Messaging in Social Media as Electronic Evidence," 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), Yogyakarta, Indonesia, 2020, pp. 209-215, [Online]. Available: 10.23919/EECSI50503.2020.9251888.

[21] A. Dawabsheh and M. Owda, "In-Vehicles Infotainment System Forensics Case Study," 2023 International Conference on Information Technology (ICIT), Amman, Jordan, 2023, pp. 32-37, [Online]. Available: 10.1109/ICIT58056.2023.10225982.

[22] R. Kurachi, T. Katayama, T. Sasaki, M. Saito and Y. Ajioka, "Evaluation of Automotive Event Data Recorder towards Digital Forensics," 2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring), Helsinki, Finland, 2022, pp. 1-7, [Online]. Available: 10.1109/VTC2022-Spring54318.2022.9860722.

[23] NHTSA. "Event Data Recorder." Internet: https://www.nhtsa.gov/research-data/event-data-recorder, 2023 [Dec. 15, 2023].

[24] Seagate. "The Digitization of the World." Internet: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf, 2023 [Dec. 15, 2023].

[25] J. Song and J. Li, "A Framework for Digital Forensic Investigation of Big Data," 2020 3rd International Conference on Artificial Intelligence and Big Data (ICAIBD), Chengdu, China, 2020, pp. 96-100, [Online]. Available: 10.1109/ICAIBD49809.2020.9137498.

[26] S. Jilani, N. N. Kishore, N. N. Chand, R. D. Varma, G. Raja and P. V. Rao, "Big Data Security: Detect and Prevent the Data from Attacks with Digital Forensic Tools," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 783-787, [Online]. Available: 10.1109/ICSSIT55814.2023.10060947.

[27] S. Ozcan, M. Astekin, N. K. Shashidhar and B. Zhou, "Centrality and Scalability Analysis on Distributed Graph of Large-Scale E-mail Dataset for Digital Forensics," 2020 IEEE International Conference on Big Data (Big Data), Atlanta, GA, USA, 2020, pp. 2318-2327, [Online]. Available: 10.1109/BigData50022.2020.9378152.