We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

185,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



Chapter

Digital Forensics in Cyber Security—Recent Trends, Threats, and Opportunities

Mohammed I. Alghamdi

IntechOpen

Abstract

The rapid technological advancement has led the entire world to shift towards digital domain. However, this transition has also result in the emergence of cybercrimes and security breach incidents that threatens the privacy and security of the users. Therefore, this chapter aimed at examining the use of digital forensics in countering cybercrimes, which has been a critical breakthrough in cybersecurity. The chapter has analyzed the most recent trends in digital forensics, which include cloud forensics, social media forensics, and IoT forensics. These technologies are helping the cybersecurity professionals to use the digital traces left by the data storage and processing to keep data safe, while identifying the cybercriminals. However, the research has also observed specific threats to digital forensics, which include technical, operational and personnel-related challenges. The high complexity of these systems, large volume of data, chain of custody, the integrity of personnel, and the validity and accuracy of digital forensics are major threats to its large-scale use. Nevertheless, the chapter has also observed the use of USB forensics, intrusion detection and artificial intelligence as major opportunities for digital forensics that can make the processes easier, efficient, and safe.

Keywords: digital forensics, data security, cybercrime, data theft, security attack

IntechOpen

1. Introduction

The introduction of Web 2.0 technologies and the significant development in the digital hemisphere has notably changed the paradigm of the entire world. Nowadays, people are increasingly engaged in web-based interactions, contribute to open projects, and share their Chapter online. However, the anonymity and ease with which all of these can be executed raise distress about trust and verifiability [1]. In particular, the evolution of digital technologies has resulted in the emergence of new ways of conducting computer crimes. Besides, the availability of networks, along with highly optimized data transfer, has raised security concerns. Malicious methodologies, tools, and software are implemented and designed every day to pose a threat to public and private networks while simultaneously exploiting data storage, for extracting useful information [2]. To counter this emerging threat, digital forensics has gained major attention in resolving cybersecurity threats. As discussed by [3], digital forensics is the science of presenting, documenting, analyzing, preserving, and identifying information and evidence from electronic and digital

devices while safeguarding the privacy of users. Furthermore, it also makes use of scientific techniques to recreate and explain the sequence of the events. By evaluating, reviewing, and recording these sequences, digital forensics aims at presenting such illegal artifacts as evidence in the court of law.

The modern world is undoubtedly driven by social networks and the evolution in digital technologies have further evolved cyber-crimes that significantly contributed in the development of new techniques, tools, and attacks that enable attackers to penetrate even in the well-controlled environment [4]. With that said, security experts, academics, and law enforcement agencies use digital forensics to tackle the increasing number of cyber anomalies. Such experts deploy scientific methods, such as identification, validation, interpretation, and documentation on digital devices like RAM, phones, memory cards, floppy disks, and flash drives to collect digital evidence. However, with the advancement in digital forensics techniques, hackers are equally exploiting anti-forensics technology to either produce delay or completely erase digital evidence [5]. Moreover, albeit the digital forensics framework is designed to ensure users privacy, the availability of ubiquitous internet access, the internet of things (IoT), and cloud computing has inspired new cybercrime waves. Furthermore, digital forensics is expected to face unique and new challenges because cyber threats and malware are being equipped with highly sophisticated and powerful anti-forensics techniques. Thus, it is important to investigate those challenges while simultaneously discovering recent digital forensics trends. In this account, the present study is dedicated to analyzing threats, opportunities, and recent trends of digital forensics in cybersecurity.

2. Recent digital forensic trends

2.1 Cloud forensics

Cloud forensics has recently immense much attention by forensics experts due to the fact that cloud computing offers massive resource pool, cost-effective solution, dynamicity, and wide access for storage. Hybrid, private, and public models of cloud computing exists, in addition to multiple services, such as security as service, database as service, integration as service, and software as service [5]. Furthermore, most companies and organizations transfer their products and services across the cloud every day due to multiple benefits, including high scalability, reduced cost of IT infrastructure, business continuity, and access to automatic updates. As a result, cloud computing has been widely accepted in multiple governments and private companies. Likewise, Communication Service Providers have established data centers across the globe in various jurisdictions that provide cloud services for ensuring value-effectiveness and service availability [4]. However, the rise in the number of cybercrimes and security in the cloud environment are the major hurdles for organizations to transfer their systems to this platform. Moreover, since forensics investigation in a cloud computing environment is complex, security analysts see cloud computing as a potential area of concern. Therefore, cloud forensics has gained major attention by forensics investigators to resolve cloud computing issues. Cloud forensics can be described as the potential application of digital forensics in a cloud-based environment [6]. This field utilizes scientific principles, proven methods, and technological practices to process events in cloud environment via reporting, examination, preservation, collection, and identification of digital data, so that events can be reconstructed.

DOI: http://dx.doi.org/10.5772/intechopen.94452

The default characteristics of cloud computing, which includes a high degree of virtualization, data duplication, jurisdiction, and multi-tenancy add various complexity layers in cloud forensics. Besides, the procedures involved in cloud forensics depends on the deployment and service model of cloud computing [7]. For PaaS and SaaS, there is very limited control over the network or process monitoring. In contrast, IaaS not only offers a higher degree of control (DOC), but it also supports friendly forensic mechanism (See **Figure 1**). Despite the complexity involved in cloud forensics, it is undeniable that the evolution of cloud computing has raised privacy and security concerns. This has significantly increased the interest of digital forensics officers in the cloud forensics as it emphasizes on authentication, authorization, and accounting (AAA) protocol while simultaneously reconstructing, investigating, and analyzing a cloud attack event so that cloud system can be quickly recovered from it [8]. This is highly effective and stark in contrast with traditional forensics techniques that utilizes log files to isolate the system in the hope of extracting useful information. Still, it blurs the view of the event. Cloud forensics can be categorized into three categories: Legal, Organizational, and Technical [9]. The legal dimension takes care of the development of agreements and regulations to ascertain that digital forensics methods do not breach regulations and laws. On the contrary, the organizational dimension encompasses organizational factors of the digital forensics [10]. Finally, the technical dimension covers the procedures and tools that are essential to execute forensic investigation in a cloud computing domain. Thus, it can be established that cloud forensics is one of the most prominent trends in the digital forensic domain. It is because, it enables forensics investigators to take full advantage of cloud computing characteristics, such as distributed forensic processing, computing power, reporting, and scalability.

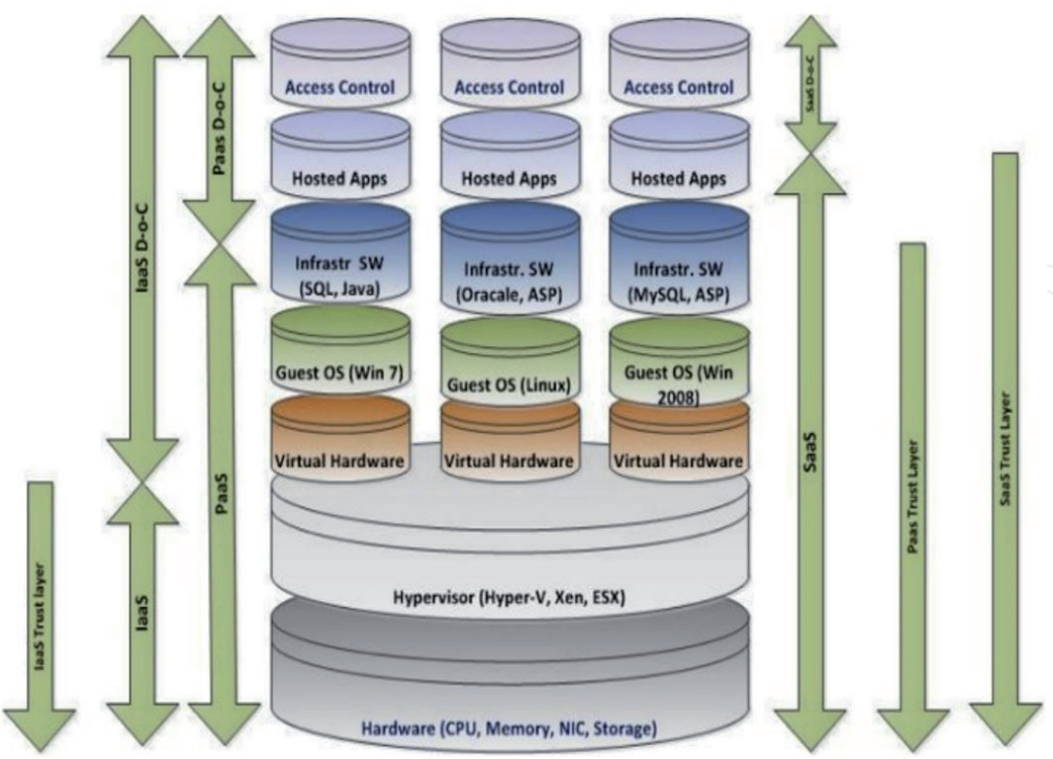


Figure 1.
Trust layer, degree of control, cloud model [6].

2.2 Social media forensics

The advancement in Industry 4.0 and Web 2.0 technologies has significantly increased the acceptance of social media platforms and it has become a primary source of socialization. Users actively share their information, create accounts, and get engage in social forms through these sites. As a result, hackers are exposed to various opportunities to exploit user's account [5]. In addition, different social media applications like LinkedIn, Instagram, Facebook, and Twitter have been exposed to multiple cyber threats and malware. Attacks on social media platforms can take place outside the system/network or within the network. Outside systems attack usually include DDoS, or DoS, while attacks within the network include retrieving cookies data [4]. Besides, it is established that the database of these social media applications is most vulnerable to such attacks. Considering this situation, digital investigators have shifted their interest towards social media forensics. Social media forensics assist experts in carrying out a criminal investigation, where social media posts serve as excellent evidence to investigators (See **Figure 2**). Likewise, social media platforms are a perfect source of information regarding potential offenders, suspects, and witnesses, and it is considered supreme for profiling [11]. In addition, by combining social media with digital forensics, investigators can gain access to a modern and diverse subset of sources of data, including demographic location, photographs, contact lists, geo-location, and text messages. This network data, combined with the metadata, has the potential to assist digital forensics investigations. Furthermore, the metadata can also be used to authenticate online social networking facts. Thus, it can be contended that social media forensics is a rising trend in the digital forensics' domain due to its ability to efficiently providing adequate digital evidence.

The advent of social media apps on a mass of platforms has enabled these networking domains to leave digital forensic trace or artifacts that can be of a valuable asset in an investigation. For instance, research like [12] discovered that the chat logs could be extracted from social media applications like Facebook and a huge amount of digital forensic artifacts, such as pictures, location data, friends, posts,

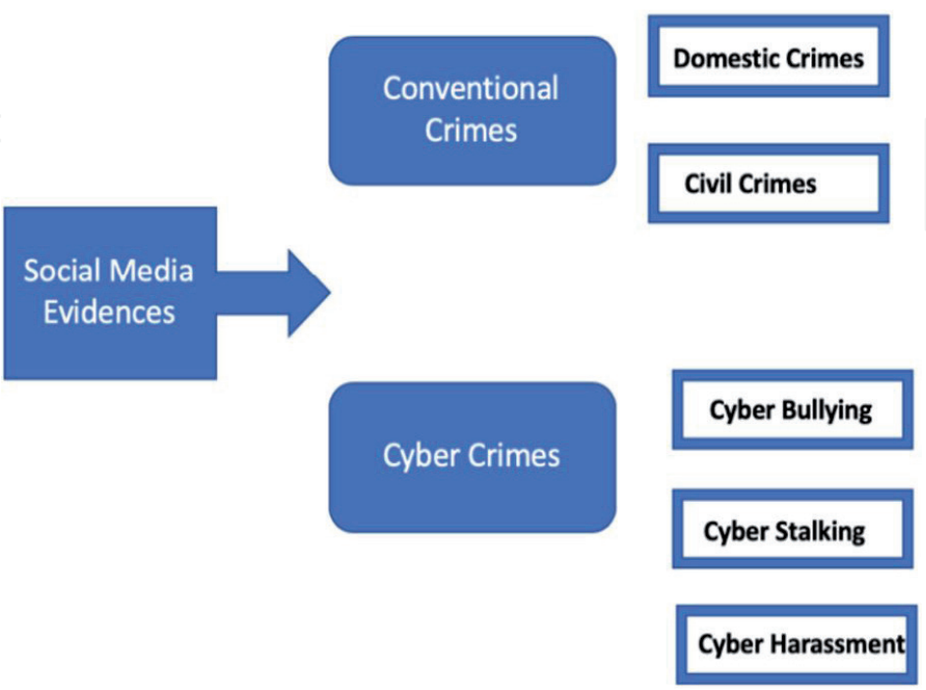


Figure 2.
Use of social media forensics in criminal investigation [4].

passwords, and usernames are left behind as potential evidence. These artifacts are essential evidence, which makes social media forensics as one of the most prominent digital forensic trends. Studies like [13] forensically examined social media applications, including MySpace, Twitter, and Facebook on Androids, iPhones, and Blackberries. The study proclaimed that they were successful in extracting digital forensic artifacts like comments posted, timestamps, passwords, URLs, pictures, and user data in text format. This indicates that social media forensics is not only a powerful tool to trace digital evidence spread across social media, but it also highly efficient in analyzing, authenticating, and acquiring digital evidence. In addition, social media forensics provide three dimensions of functionalities, namely reverse search integration, tempering localization analysis, and metadata visualization and extraction [14]. The first take advantage of Google Image Search is that it provides results in a web browser tab. Secondly, it incorporates six different tampering localization maps that are generated through forensic algorithms, which is further aimed at acquiring different tempering traces on social media. Thirdly, it fully supports metadata listing and displays any potential embedded thumbnails. With the help of these functionalities, forensic experts can further examine the information to extract useful evidence. This has made social media forensics a rising trend in the digital forensic domain.

2.3 IoT forensics

IoT is the latest paradigm that has notably changed the way mobile communication works. Conceptually, IoT can be defined as the interconnectivity of electronic devices that combines situational knowledge and sensing powers to execute tasks, intelligently [15]. Major IoT devices include smartphones, tablets, laptops, personal computers (PCs), and other various embedded portable devices. The continuous growth in the area of IoT has enabled users to share their data across different platforms. Besides, IoT systems can communicate with each other either via internet application programming interface or directly. In addition to this, they can also be controlled through computing devices, like cloud servers. The networking capabilities and smartness of IoT systems provide significant benefits for both business and domestic applications [16]. However, despite its tremendous advantages, IoT systems are subjected to several security threats and attacks, such as mass monitoring, destruction of IoT networks, Denial of Service (DoS), and ransomware. Therefore, digital forensic experts have developed a keen interest in IoT forensics to carry out the digital investigation. The rise of IoT forensics trend is due to the fact that IoT systems present multiple complex and unique challenges in the digital forensics field [4]. Moreover, IoT-based applications contain a huge number of resources and distinct devices that generates a tremendous amount of data, which is known as Big IoT data. This data, combined with digital forensics tools and techniques, provide investigators with an opportunity to trace cybercrimes that further help them in preventing cyber-attacks.

Despite the growing benefits of IoT forensics, it cannot be denied that it produces a massive amount of data and acquiring this data significantly increases the workload on data centers [17]. As a result, forensic investigators are forced to face additional analytics, security, and capacity challenges. Furthermore, the preservation and extraction of data from IoT-enabled services and devices present protocol, data formats, and physical interface challenges which further complicate evidence extraction process. However, regardless of several limitations, IoT forensics offers a richer and authentic source of evidence, as compared to conventional computer systems [18]. IoT forensics react to the requirements of users without requiring users' conscious interaction. As a result, the IoT forensics environment provides

contextual evidence that helps digital forensic investigators to analyze physical world events. Thus, IoT forensics is one of the prominent trends of digital forensics domain, not only because of its ability to provide contextual and digital evidence but also due to various challenges faced by this domain.

3. Threats faced by digital forensics

3.1 Technical challenges

The advancement in digital technology has opened doors to various opportunities; however, it has also caused the digital forensics domain to face various challenges. Although different digital forensic experts and researchers have been analyzing and studying numerous known digital forensic issues, there is still a requirement to classify these challenges [19]. In this account, it has been discovered that digital forensic systems are exposed to technical challenges that threaten the integrity of these systems. Technical challenges are those potential threats that can be addressed using existing operations, protocols, and expertise. Understanding that digital forensics demands an optimum combination of ethical conduct and technical skills. Some of the major technical challenges, associated with digital forensics are encryption, a huge volume of data, and incompatibility among diverse forensic tools [20]. The advancement in communication technology has made sophisticated encryption products and services easy and widely accessible. Due to this, encryption algorithms and standards are becoming more complex, which further increases the time and difficulty of conducting cryptanalysis. This technique joins encrypted files together to extract meaningful information. In addition, encryption makes electronic data unreadable, which further enable criminals to camouflage their criminal activities [21]. For a digital forensic officer, this can negatively affect their investigation process. It has been discovered that around 60% of cases - involving some type of encryption - goes unprocessed because it significantly limits the ability of the investigator to extract information from the evidence [22]. Thus, the easy implementation, low cost, and the availability of encryption tools greatly pose a threat to the integrity and credibility of the digital forensics process.

In addition to encryption, huge volumes of data that exist within numerous applications- like enterprise resource planning-also poses a great threat to digital forensic operations. The substantial increase in data volumes significantly reduces the capability of legal systems and forensic investigators to keep up with the digital threats [23]. Likewise, with the introduction of cloud computing, much IT-related hardware, such as network switches, racks, and servers have been replaced with remote-on-demand, virtualized software that are configured according to business needs. Besides, these services and data can be managed and hosted by a third-party or the user from any place. Thus, the data and software have the possibility that it is stored physically across multiple geographic locations [22]. This distributive nature of data substantially lowers the control and visibility of forensic experts over digital forensic artifacts. Similarly, digital forensic tools and techniques commonly differ in cost, complexity, and functionality. Due to this, most of the digital forensic tools contain heterogeneous parts or elements, which increases their incompatibility to work together [20]. Moreover, some forensic tools are not able to handle the ever-increasing storage capacity of target devices. This means that vast targets constitute a major technical challenge to digital forensic operations because they demand more complex analysis techniques. Thus, it is affirmed that different technical challenges pose a great threat to the performance and integrity of digital forensic operations.

3.2 Operational challenges

It is a known fact that digital crimes are intentional in their scope of operation. Due to this, digital forensics is exposed to various operational challenges. Among such challenges, incidence prevention, response, and detection have gained much attention. Traditional IT environments that have on-premises data processing have integrated internal incident management process for ensuring utmost security [20]. This process utilizes intrusion detection systems, log file analysis, and monitoring, in addition to data loss prevention systems that identify and detect data loss, attackers, and intruders. For cloud users, these security incidents can often prove to be challenging. This is because, these security incidents compromise business and personal data and since they are equipped with anti-forensics technology, attackers can steal or destroy potential evidence [24]. Likewise, the lack of standardized procedures and processes in digital forensics alarmingly endangers the evidence extraction and investigation process. It is established that currently, digital forensic models lack standardization that has further increased the complexity of the process. Besides, studies like [22] argue that the lack of universal standards makes it quite tough to assess the competency of forensic experts. The absence of standardized procedures was acceptable when digital forensics was considered a mysterious investigation process that enabled experts to discover hidden pieces of evidence and information that further provided useful insights regarding criminal behaviors. However, with the increase in the development of digital technologies, digital forensic investigation is no longer limited to small computer systems rather a virtualized environment that consists of non-standard interfaces and different storage devices.

In addition to above-discussed threats, digital forensics is also exposed to forensics readiness problem. Forensic readiness can be understood as the capability of computer networks or computer systems to record data and activities in such a way that it can be perceived as authentic and are sufficient enough for forensics purposes [25]. However, the rapid development in cloud computing has forced organizations to dynamically change how they enact, develop, and plan IT strategies. Besides, cloud computing lacks forensic readiness aspect, which further threatens digital forensic operations. Similarly, manual analysis and intervention of physical hard drives is another potential operational challenge that is faced by digital forensics. Albeit, it is simple and straightforward in a single drive, or a single partition, the process becomes much more complicated when RAID configurations are involved [20]. Also, due to the complex nature of digital forensics, manual inspection of hard drive images can potentially risk the digital artifacts. Likewise, it is believed that forensic analysis should be valid, accurate, complete, and reliable. However, balancing between user privacy and retrieving key digital evidence is a major threat to digital forensics. Due to the increase in the storage capacity, often a small portion of the information is used for investigation and a larger amount of information is discarded [26]. This can lead to a breach of the user's privacy, which poses an additional challenge to digital forensic operations. Thus, in light of the evidence, it can be affirmed that operational challenges can notably endanger digital forensic analysis.

3.3 Personnel related challenges

Personnel related challenges endanger the integrity of digital evidence. Among various personnel-related challenges, lack of well-trained forensic staff is the most prominent one [20]. Despite the overwhelming significance of the digital forensics field because of cyber-crimes, the lack of qualified forensic officers threatens the

process of digital forensics. The shortage of well-trained forensic investigators is due to the fierce competition in law enforcement as well as high requirements since digital forensics require technically proficient personnel that are certified and trained to deliver scientifically valid evidence [22]. Likewise, it cannot be denied that digital forensics has gained major importance among forensic practitioners, law enforcement agencies, and computer professionals. Unfortunately, the advancement in this field has encouraged an environment that is threatened by semantic disparities. Another potential personnel-related challenge is a chain of custody. Chain of custody refers to the location log that defines the collection point of the evidence. In digital forensic analysis, it is one of the most crucial issues because it requires physical control of the evidence that is not possible in a digital environment [7]. In addition, due to proprietary technology, procedures, and multi-jurisdictional laws, effectively managing the chain of custody is a major challenge that is faced by digital forensics. Hence, it can be established that personnel-related challenges pose a great challenge to traditional forensic operations.

In addition to the discussed challenges, it is undeniable that digital forensics lack a unified formal representation of standardized procedures and knowledge for analyzing and gathering digital artifacts. This inevitably causes incompatibility and conflict within various digital forensics tools [27]. Errors in the interpretation and analysis of digital artifacts occur when the standardized or formalized procedure for analyzing, preserving, and collecting digital evidence is absent. Likewise, when forensic experts manage a vast amount of data while simultaneously performing forensic investigation, they utilize specialized skills and digital technologies. However, these experts often fail to record their work, which further hampers training and external reviews [22]. Past knowledge and experience should be utilized to further train new digital forensic personnel while fostering knowledge sharing among detective communities. Unfortunately, digital forensic officers either fail to record their work or simply do not follow legal practices that further poses a great threat to digital forensic investigation.

4. Opportunities

4.1 USB forensics

Universal Serial Bus (USB) is a widely used storage device and it is considered very effective for their mobility and capacity. Normally, USB uses USB controller command to ensure security within the USB drive. However, due to its easy accessibility, it is often used in conducting cyber-crimes. The controller command in the USB increases the vulnerabilities when users are undergoing user certification process, which makes it susceptible to cyber-attacks [3]. Fortunately, since USB generates an IP address, it can be used to track USB bypassing attempts. This means that as USB grow in capability and capacity, it has the potential to offer more information in digital forensics analysis. Despite its growing significance in the digital forensics domain, it is undeniable that USB drives pose a great risk to both systems and sensitive data. The easy accessibility, cheap, and small form factor makes USB ideal for theft and destroying potential digital evidence [28]. Malicious software and viruses can be installed in networked or stand-alone computer systems through USB, either inadvertently or deliberately. As a result, potential hackers can completely wipe or cover up their malicious activities. For this reason, USB forensics has become a vital component in computer investigations that allow digital forensic experts to trace USB connection activities in PreFetch, Shortcuts, and Link file folders [29]. Such traces can assist forensic investigators in identifying

various file-related operations, including copying pictures or opening documents. Thus, it is apparent that USB forensics is a rising area of interest for digital forensic analysts and it has the ability to assist them in analyzing and identifying potential digital evidence.

Digital evidence is usually stored on a wide range of media devices, usually, the storage devices having removable or internal memory that contains digital artifacts which are usually discovered at a crime scene. These devices often include cellular phones, laptops, portable media players, and digital cameras that use magnetic, electrical, or optical storage media, among which USB flash drives are the most popular ones [22]. Metadata stored in USB flash drives can assist digital forensic experts in identifying detailed information about digital data. This information includes copyright information, geospatial information, or even timestamps that are vital in examining digital forensic evidence. Besides, it is undeniable that USB storage device is considered as the standard for transfer and backup of data files, due to this, potential hackers use USB devices to conduct data theft [30]. Hence, by comprehending the diversity and complexity involved in analyzing USB devices, digital forensic operations can greatly benefit in terms of tracking traces that could lead forensic analysts to potential wrongdoers.

Moreover, in terms of forensics, USB devices contain significant footprints in a various digital environment that are vital in forensic examination [31]. In addition, in USB specification, MSC is considered as a standard for establishing a connection between removable drives. MSC can be defined as a protocol set that takes care of communication between operating systems and USB devices [30]. From a digital forensic standpoint, the MSC protocol gives the digital forensic officer direct access to file systems, clusters, and sectors. Having full control over such file systems, digital forensic experts can easily identify, extract, and thoroughly analyze digital evidence. As a result, USB forensics cannot only reduce the complexity of the digital forensic investigation, but it can also ascertain that the extracted evidence is authentic.

4.2 Intrusion detection

Due to recent development in information systems and rapidly increasing network attacks, intrusion detection systems (IDSs) have become a crucial area of interest in digital forensics field. According to [32], IDS has the capability to detect intrusion attempt that can either render a system unreliable, or unusable, gain access to critical digital evidence, or manipulate information. Such systems are ideal for digital forensic investigators as they reveal suspicious behavior within the network. Likewise, with efficient IDS in place, forensic analysts can easily determine whether the security of the computer system is compromised or the data is being accessed from an unauthorized location [33]. This information is critical in forensic investigations; as forensic experts can use this information to extract useful data which can be presented as potential evidence in the court of law. Besides, if an attacker attempts to sabotage a public or private network, IDS will identify and activate incident response (IR). The digital forensic investigation - combined with IR protocols - would allow investigators to preserve, gather, and identify live data [34]. Further, digital forensic methodologies, combined with IDS, will ascertain that no changes are made to the seized content and evidence. IDS systems can also help in detecting hostile and malicious network activities, specifically by analyzing the acquired packets, blocking attack connections, and by alarming the system administrator for limiting the potential damages. These functionalities are crucial in case of digital forensic investigation, as the attacker would always attempt to erase potential digital evidence.

Albeit digital forensic has made it easy to analyze and detect cyber-crimes, the fact remains that it cannot provide fool-proof security to the network or online storage. In this case, IDS has opened doors to various opportunities for digital forensics, as it not only detects malicious activities, it also monitors traffic data to determine the nature of the attack [35]. Moreover, IDS also possess the ability to warn the system administrator - in case the system has been compromised. Once the event has been detected, the digital forensic process can be conducted for discovering the damage and the extent of the intrusion. Although the primary objective of IDS is to identify potential malicious attempts to prompt evasive measures, with the help of digital forensics, it can be used to extract useful digital evidence for civil, legal, and criminal proceedings [36]. The ultimate goal of IDS is efficiently detecting misuse or unauthorized use of computer networks and systems by both external penetrations and insiders. With digital forensics, investigators can trace criminal, intrusive, or illegal activity back to the criminal while simultaneously obtaining sufficient evidence. Thus, it can be established that IDS provide various opportunities and have the ability to assist in digital forensic investigation. Moreover, IDS systems can ensure that the obtained evidence is safe and it can detect and effectively respond to cybersecurity threats.

4.3 Artificial intelligence

With the rapid rise in the volumes of digital data, digital forensics often struggles to analyze a complex and large amount of information that requires intelligent analysis and computing. For this purpose, artificial intelligence (AI) has become a well-established and crucial domain of latest computer science, which has the ability to tackle sophisticated and computationally large problems in real-time [37]. The complexities and growth in cyber-crime combined with limited resources and time, both human and computational, in addressing cyber-crime significantly limits the capabilities of the digital forensic investigators to apply digital forensic operations and obtain results in a realistic time-frame. This problem can be resolved by combining digital forensic methods, tools, and techniques with AI. The combination of these dynamic domains gives rise to intelligent forensics that can be considered as an interdisciplinary approach that not only uses resources more intelligently and efficiently but also utilizes technological advances to solve digital forensic investigation [38]. Intelligent forensics incorporates a wide range of techniques and tools from social network analysis, computational modeling, and AI for improving the efficiency and overall credibility of digital investigations while simultaneously lowering the time required to extract digital evidence. What makes intelligent forensics unique is its ability to conduct a digital forensic investigation- both before and after the incident. Besides, since intelligent forensics make use of AI technologies like machine learning, it can assist digital forensic investigators in resolving specificity and generality problems by considering cyber-crime patterns.

In addition, by combining digital forensics with AI, forensic experts can effectively apply digital forensic operations both reactively – after cyber-crime has taken place - and proactively – before cyber-crime has occurred. The reactive ability of intelligent forensics can be considered as a part of digital forensic investigation that helps in gaining in-depth insight into the incident, which can further assist the digital forensic officer in examining data sources for potential evidence [38]. For this purpose, intelligent forensics make use of various techniques, including AI and social network analysis. Likewise, intelligent forensics can also be used proactively, where numerous state-of-the-art techniques like machine learning and deep learning predict future threats, specifically by assessing past trends. This can be very valuable for digital forensic investigators, as they will be able to predict what digital

resources have to be preserved for digital evidence. Moreover, with the help of computational intelligence and AI, forensic investigators can employ digital forensic methods more efficiently while ensuring the credibility and reliability of the results [39]. AI also helps in handling large datasets, while collecting digital evidence for forensics [40]. Thus, it can be established that AI has the capability to dynamically transform the way digital forensic works while increasing the accuracy of the results and lowering the time needed to extract useful digital evidence.

5. Conclusion

Digital forensics has gained notable attention due to the increase in cyber-crimes. Albeit the rise in digital technology has benefited various fields, the fact remains that it has presented new ways of conducting cyber-crimes. Besides, malicious software, methodologies, and tools are being designed and implemented every day to pose a threat to public and private networks and simultaneously exploiting data storage, in hope of extracting and exploiting the useful information. These security vulnerabilities and breaches have inspired the developments in digital forensics domain so that digital evidence can be extracted from digital devices and can be used in criminal and civil legal proceedings. For understanding the importance of digital forensics, the present study has thoroughly discussed the recent trends, potential threats, and opportunities of digital forensics in cybersecurity.

Author details

Mohammed I. Alghamdi
Department of Computer Science, Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

*Address all correspondence to: mialmushilah@bu.edu.sa

IntechOpen

© 2021 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. CC BY

References

[1] E. A. Gollub, "Recent trends in digital text forensics and its evaluation," *In International Conference of the Cross-Language Evaluation Forum for European Languages,* pp. 282-302, (2013), September.

[2] A. Aminnezhad and A. Dehghantanha, "A survey on privacy issues in digital forensics," *nternational Journal of Cyber-Security and Digital Forensics (IJCSDF),* vol. 3, no. 4, pp. 183-199, (2014).

[3] F. Dezfouli and A. Dehghantanha, "Digital forensics trends and future," *International Journal of Cyber-Security and Digital Forensics (IJCSDF),* vol. 3, no. 4, pp. 183-199, (2014).

[4] B. K. Sharma, M. A. Joseph, B. Jacob and L. C. B. Miranda, "Emerging trends in Digital Forensic and Cyber security-An Overview," *In 2019 Sixth HCT Information Technology Trends (ITT),* pp. 309-313, (2019), November.

[5] M. Wazid, A. Katal, R. H. Goudar and S. Rao, "Hacktivism trends, digital forensic tools and challenges: A survey.," *n 2013 IEEE Conference on Information & Communication Technologies,* pp. 138-144, (2013), April.

[6] A. Pichan, M. Lazarescu and S. T. Soh, " Cloud forensics: Technical challenges, solutions and comparative analysis.," *Digital investigation,* vol. 13, pp. 38-57, (2015).

[7] S. Zawoad and R. Hasan, "Cloud forensics: a meta-study of challenges, approaches, and open problems," *arXiv preprint arXiv,* p. 1302.6312., (2013).

[8] A. Aminnezhad, A. Dehghantanha, M. T. Abdullah and M. Damshenas, "Cloud forensics issues and opportunities.," *International Journal of Information Processing and Management,* vol. 4, no. 4, p. 76, (2013).

[9] K. Ruan, J. Carthy, T. Kechadi and I. Baggili, "Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results," *Digital Investigation,* vol. 10, no. 1, pp. 34-43, (2013).

[10] K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, "Cloud forensics," *In IFIP International Conference on Digital Forensics. Springer, Berlin, Heidelberg. ,* pp. 35-46, (2011), January.

[11] A. E. A. Rocha, "Authorship attribution for social media forensics.," *IEEE Transactions on Information Forensics and Security,* vol. 12, no. 1, pp. 5-33, (2016).

[12] I. Baggili and F. Breitinger, "Data sources for advancing cyber forensics: what the social world has to offer.," *n 2015 AAAI Spring Symposium Series.,* (2015), March.

[13] N. Al Mutawa, I. Baggili and A. Marrington, "Forensic analysis of social networking applications on mobile devices.," *Digital Investigation,* vol. 9, pp. S24-S33, (2012).

[14] M. Zampoglou, S. Papadopoulos, Y. Kompatsiaris, R. Bouwmeester and J. Spangenberg, "Web and social media image forensics for news professionals.," *In Tenth international AAAI conference on web and social media,* (2016), April.

[15] A. Zanella, N. Bui, A. Castellani, L. Vangelista and M. Zorzi, "Internet of things for smart cities," *IEEE Internet of Things journal,* vol. 1, no. 1, pp. 22-32, (2014).

[16] M. Vangeti, S. K. Yadav and V. Pinnti, "Advantages of Internet of Things (Iot) For Developing Smart Services in Manufacturing Business," *Purakala with ISSN 0971-2143 is an UGC CARE Journal,* vol. 31, no. 25, pp. 62-68, (2020).

[17] A. MacDermott, T. Baker and Q. Shi, "Iot forensics: Challenges for the ioa era.," *In 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS),* pp. 1-5, (2018), February.

[18] R. Hegarty, D. J. Lamb and A. Attwood, "Digital Evidence Challenges in the Internet of Things," *In INC,* pp. 163-172, (2014).

[19] M. Al Fahdi, N. L. Clarke and S. M. Furnell, "Challenges to digital forensics: A survey of researchers & practitioners attitudes and opinions.," *In 2013 Information Security for South Africa, IEEE,* pp. 1-8, (2013).

[20] N. M. Karie and H. S. Venter, "Taxonomy of challenges for digital forensics.," *Journal of forensic sciences,* vol. 60, no. 4, pp. 885-893, (2015).

[21] A. M. Balogun and S. Y. Zhu, "Privacy impacts of data encryption on the efficiency of digital forensics technology.," *arXiv preprint arXiv:1312.3183.,* (2013).

[22] E. A. Vincze, "Challenges in digital forensics. Police Practice and Research," vol. 17, no. 2, pp. 183-194, (2016).

[23] S. Raghavan, "Digital forensic research: current state of the art.," *CSI Transactions on ICT,* vol. 1, no. 1, pp. 91-114, (2013).

[24] P. Cichonski, T. Millar, T. Grance and K. Scarfone, "Computer security incident handling guide.," *International Journal of Computer Research,,* vol. 20, no. 4, p. 459, (2013).

[25] Z. Baig, P. Szewczyk, C. Valli, P. Rabadia, P. Hannay, M. Chernyshev, M. Johnstone, P. Kerai, A. Ibrahim, K. Sansurooah and N. Syed, "Future challenges for smart cities: Cyber-security and digital forensics.," *Digital Investigation,* vol. 22, pp. 3-13, (2017).

[26] I. Hong, H. Yu, S. Lee and K. Lee, "A new triage model conforming to the needs of selective search and seizure of electronic evidence.," *Digital Investigation,* vol. 10, no. 2, pp. 175-192, (2013).

[27] N. Rahim, W. A. Wahab, Y. I. Idris and L. M. Kiah, "Digital Forensics: An Overview of the Current Trends.," (2014).

[28] J. Collie, "The windows IconCache. db: A resource for forensic artifacts from USB connectable devices," *Digital investigation,* vol. 9, no. 3-4, pp. 200-210, (2013).

[29] T. Roy and A. Jain, "Windows registry forensics: an imperative step in tracking data theft via USB devices.," *International Journal of Computer Science and Information Technologies,* vol. 3, no. 3, p. International Journal of Computer Science and Information Technologies, (2012).

[30] S. B. Deb and A. Chetry, "USB Device Forensics: Insertion and removal timestamps of USB devices in Windows 8.," *In 2015 International Symposium on Advanced Computing and Communication (ISACC),* pp. 364-371, (2015).

[31] S. Verma, A. Singh, D. Singh and V. Laxmi, "Computer forensics in IT audit and credit card fraud investigation-for USB devices," *In 2014 International Conference on Computing for Sustainable Global Development (INDIACom),* pp. 730-733, (2014).

[32] S. Agrawal and J. Agrawal, "Survey on anomaly detection using data mining techniques.," *Procedia Computer Science,* vol. 60, pp. 708-713, (2015).

[33] M. Ahmed, A. N. Mahmood and J. Hu, "A survey of network anomaly detection techniques.," *Journal of Network and Computer Applications,* vol. 60, pp. 19-31., (2016).

[34] C. P. Grobler, C. P. Louwrens and S. H. von Solms, "A multi-component view of digital forensics.," *In 2010 International Conference on Availability, Reliability and Security, IEEE.,* pp. 647-652, (2012).

[35] P. K. Khobragade and L. G. Malik, "Data generation and analysis for digital forensic application using data mining.," *In 2014 Fourth International Conference on Communication Systems and Network Technologies, IEEE.,* pp. 458-462, (2014).

[36] M. Kumar, M. Hanumanthappa and T. S. Kumar, "Network Intrusion Forensic Analysis Using Intrusion Detection System.," *Int. J. Comp. Tech. Appl,,* vol. 2, no. 3, pp. 612-618, (2011).

[37] F. Mitchell, "The use of Artificial Intelligence in digital forensics: An introduction.," *Digital Evidence & Elec. Signature L. Rev,* (2010).

[38] A. Irons and H. S. Lallie, "Digital forensics to intelligent forensics.," *Future Internet,* vol. 6, no. 3, pp. 584-596, (2014).

[39] A. K. Muda, Y. H. Choo, A. Abraham and S. N. Srihari, "Computational intelligence in digital forensics: forensic investigation and applications.," *Springer International Publishing.,* (2014).

[40] O. M. Adedayo, "Big data and digital forensics.," *In 2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF). IEEE.,* pp. 1-7, (2016).