International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
Volume 1 Issue 1 July – September 2024
Website: https://ijarmt.com

# Importance and Advantages of Digital Forensics for Law Enforcement and Corporations

Gourav Kumar Sharma
GST Practioner
Infinity Services (Co-Founder)
An Accounts Outsourcing Firm, Indore (M.P)
Email: gourav.sharma008989@gmail.com

**Abstract**

Digital forensic science is a critical component of today's police work as well as business protection from cybercrime because of its ability to investigate, assess, and even reconstruct information existing in electronic gadgets. Cybercrime and digital frauds are on rise and in this digital world Digital forensics gives the required tools and techniques to fight these crimes effectively. In particularly, for all police departments digital forensic investigation is essential in solving cyber criminal activities including hacking, identity theft and fraud. It helps in finding evidences that may be useful in prosecuting criminals to book their evil deeds and face the law. Another factor has to do with the ease with which one can chase the footprints left behind by the offenders, regenerate lost records and appraise the content of electronic messages in developing solid legal defenses. Organizations gain from the digital forensics in the sense that they secure their organizations from unauthorized intrusions as well as ensure they have mechanisms for dealing with such incidences. Thus, digital forensics can quickly detect breaches, estimate the losses caused by data leaks, unauthorized use of Intellectual Property, and acts of insiders, as well as set corrective actions. It also saves money apart from preserving corporate image and the trust that customers have in organizations. Digital forensics can also be applied in helping to address regulatory requirements enabling the management of digital evidence in a way, which meets specific legal standards. Especially for industries the quality of data, its confidentiality and integrity have a significant relevance such as financial, healthcare and telecommunications industries.

## Introduction

Digital, computer and cyber forensics in essence, involves the search, extraction and analysis of electronic information; this is a critical process for both law enforcement as well as corporate

bodies in the modern world. With the growth of innovation in each facet of people's life, more and more cybercrimes, data compromises, and digital fraud have arisen, which demands a more sophisticated approach in their identification and combating. For law enforcement, digital forensics offers the approach for examining computer-based crimes that occur in computers, cellular phones and other networks. It enables the investigators to get back the accidentally deleted files, track the users' activity trails, and study the e-mail communications, all of which are vital in solving the computer crimes including cyber stalking, cyber frauds, terrorism, and organized crimes. Digital evidence presentation proves useful in court as it helps in getting convictions as well as deliver justice.


Corporations in particular use digital forensics to protect their company's digital resources and therefore uphold security. In circumstances such as data leakage, theft of intellectual property or threats from insiders, digital forensics helps the quick detection and investigation of the incident, which is fundamental in the management and avoidance of further harm. In addition, it helps in compliance with the legal requirements in dealing with the electronic evidence, which is paramount in industries that deal with sensitive information that should meet certain legal requirements to be released to the public. digital forensics is a crucial area that supplements the work of police and enriches the protection of companies against cyber threats and thus is the synthesis of current security approaches.

**Importance of Digital Forensics**

Digital forensics is considered highly relevant in the modern world with its increased focus on technology since it is a foundation of both police and business protection activities. Correspondingly with the growth of cyber threats and digital hazards, digital forensics gains the importance of its mission. This may involve investigating and solving computer-related crime such as cyber criminality, economic crime, identity theft, terrorism and other related crime as well by analyzing digital evidence that is on computers, mobile equipment and networks among others. It is even more forgotten when it comes to constructing robust and tenacious legal arguments when prosecuting or defending a case, or when guaranteeing that justice is delivered. Digital forensics is an important tool for legal entities task, since it contributed to the effective protection of information; it allows to quickly identify and analyze the information security threats that may affect the company and its clients, and avoid the possible negative consequences of such breaches in the form of loss of reputation and trust from customers. Furthermore, digital forensics helps in meeting legal requirements as it involves dealing and preserving of the digital evidence in a way that is legal, this is important so as to avoid getting into trouble with the law. Furthermore, digital forensics helps in establishing strong measures of enhancing the cybersecurity in organizing institutions, since it offers important information in relation to potential threats and contributes to the right strategies in putting into practice the enhanced means of security. This is why digital forensics shall remain crucial in the detailing of any organization or individual's security plan as more digital threats continue to be developed.

**Need of the Study**

There is a necessity of the systematic research on digital forensics in law enforcement and corporations because of the modern society's use of digital technologies and the corresponding increase of cybercriminal activities and security breaches. While the use of internet and digital devices increases year by year our amounts and varieties of digital evidence rise dramatically making a lot of problems for police and companies. To police, digital forensics cannot be overemphasized as it is a tool that enhances the investigation and prosecution of various types of crimes such as cybercrimes, money fraud, identity theft, and child exploitation all of which are prevalent in the society. Conventional investigation methodologies cannot effectively handle digital investigations as they require highly specialized method, techniques and tools for collection, acquisition, and analysis of digital evidence. Developing these capabilities

guarantees the police's ability to respond to increased and changing types of the cyber threat, as well as to preserve safety. In corporate business, or enterprise environment, the forensics or the process of taking and analysis of digital images is as vital as in the criminal justice system, especially to shield organizations' interests and ensuring business continuity. Hackings, for instances data theft and ransomware are dangerous since they have severe financial and reputational impacts. It is possible to state that spending money on the acquisition of the advanced tools of digital forensics make it possible to respond to security breaches, contain secondary effects, and meet the obligatory norms of the modern law in terms of the data protection. However, it is also necessary to stress the importance of digital forensics for law enforcement and corporate representatives in general and to provide an understanding of best practices, new technologies and opportunities to develop effective forensic solutions to address existing and emerging problems in the digital environment.

**Type of Digital Forensics**

Digital forensics encompasses several specialized branches, each focusing on different types of digital evidence and technological environments. Here are the primary types of digital forensics:

1. Computer Forensics
    - Focuses on extracting and analyzing data from computers, including desktops and laptops.
    - Involves recovering deleted files, examining file systems, and analyzing user activity and system logs.
2. Network Forensics
    - Deals with monitoring and analyzing network traffic to detect and investigate cyber incidents.
    - Involves capturing and examining data packets, tracking intrusions, and identifying malicious activities.
3. Mobile Device Forensics
    - Specializes in recovering and analyzing data from mobile devices such as smartphones and tablets.
    - Involves extracting information like call logs, text messages, emails, GPS data, and app usage.

4. Database Forensics
    - Focuses on investigating databases and their associated data.
    - Involves examining database logs, transactions, and schema to uncover unauthorized access or data manipulation.
5. Email Forensics
    - Specializes in the recovery and analysis of email communications.
    - Involves examining email headers, content, attachments, and metadata to trace the origin and authenticity of emails.
6. Malware Forensics
    - Focuses on identifying, analyzing, and understanding malicious software.
    - Involves reverse engineering malware to determine its functionality, origin, and potential impact.
7. Cloud Forensics
    - Deals with investigating data stored in cloud environments.
    - Involves retrieving and analyzing data from cloud services, understanding the virtualized environments, and ensuring data integrity and chain of custody.
8. Memory Forensics
    - Focuses on analyzing volatile memory (RAM) from computers and other devices.
    - Involves capturing and examining memory dumps to uncover running processes, open network connections, and other in-memory artifacts.
9. IoT Forensics
    - Specializes in investigating Internet of Things (IoT) devices.
    - Involves extracting data from smart devices, sensors, and wearables to understand their interactions and potential security breaches.
10. Audio and Video Forensics
    - Deals with the analysis of audio and video recordings.
    - Involves enhancing, authenticating, and analyzing multimedia files to determine their origin and detect any tampering.
11. Drone Forensics
    - Focuses on investigating unmanned aerial vehicles (UAVs) and their associated data.

- Involves extracting flight logs, GPS data, and other relevant information from drones.

Each type of digital forensics requires specialized tools and expertise to effectively analyze and interpret digital evidence. As technology continues to evolve, new branches of digital forensics are likely to emerge, addressing the growing diversity and complexity of digital environments.

**Literature review**

**Malik, A. W., et al (2024).** Cloud digital forensics can be understood as forensic science that targets specifically cloud environments and their specific difficulties. While engaging in the cloud forensics, the experts have to deal not only with tools and techniques typical to the processes of digital forensics, but also with such peculiarities as cloud architecture, data distribution, and problems related to multi-tenancy. The challenges include; Data : which is likely to be changed or wiped clean within minutes across borders. However, due to distribution of data in cloud environments, it is challenging to determine the geographical location of the data hence leading to legal issues and jurisdictions. These effective cloud forensic investigations involve interacting appropriately with cloud service providers to get proper access to logs and data at the same time protecting the privacy of the individuals as dictated by law and regulations. This field also requires strict measures of data collection and management to ensure a clean custody of the data. The implication that arises from this paper, as cloud computing persists to grow, is the need for forensic professionals to seek out new ideas, skills, and approaches as the increase in diffusion of computer resources' complexities challenges the identification of simple pathways of tracking digitized elements in an environment that is becoming increasingly decentralized and often less transparent.

**Holt, T. J., et al (2023).** Computer or cybercrime refers to offenses that are committed using information technology or with the help of computers and other electronic devices, and is a relatively recent phenomenon given the ever growing technology requirements of human society. With the advancement in technology systems and networks are also at risk from hackers and other malicious users in new ways. Cyber offences include embezzlement and identity theft, hacking and cyber spying, affecting individuals, organizations and states. This is because crimes in the cyber space have escalated and there is need to find solutions and Digital forensics is such solution. Electronically records are defined as the processes of obtaining and analysing information stored in electronic gadgets with an intention of utilising the collected information from the gadgets in court cases. This field integrates natural legal, technical, as

well as procedural approaches with regard to the enforcement as well as the evaluation of digital evidence. Forensic specialists take all the necessary measures to ensure the data's authenticity and include anything from emails and web history to fragmented files and their metadata. The process not only enable one to learn the details regarding a particular cybercrime but also enable one to trace the offenders hence a worthy factor in the implementation of cyber security measures.

**Lawton, D., et al (2014).** Investigation in the context of digital forensic is an important process by which all information that can be relevant to a case is searched, retrieved and analyzed. This takes place when an incident is reported or when an employer or an employee feels that an incident has occurred and the process involves a systematic and sensitive collection of data from computers, smart phones and other communication devices, servers and cloud storage. The goal is simply to populate the map to know what data is out there and where they are located. The evidence gathering methodology of the discovery phase demands the following features; first; evidence must be gathered efficiently; second; evidence must be gathered effectively with a view of ensuring that despite being gathered and processed; evidence cannot be fed to the court in any distorted form. This refers to employing of tools and methodologies that produces duplicity of data in accurately termed as forensic images leaving the source unaltered. Cyber-security uses logic in analyzing the plethora of the data, and sorting conduits patterns, aberrations and appearances that a human eye will not capture directly. The nature of discovery is complex in digital forensics because of the various data types and the ever changing technological landscape that; there is need to constantly update the tools and techniques used in the process. Moreover, as a legal process, discovery has some legal gaps such as privacy laws and regulations that impact on the discovery process. Gaining knowledge about the how and when of a cyber event goes a long way in the solving of cases, and the drawing up of strategies for avoiding such scares in the future.

**Arshad, H., et al (2018).** Digital forensics is relevant in criminal investigation and yet it struggles with the scientific approval of digital evidence. In the context of technological development digital technologies change rather quickly and with them challenges in terms of reliability and scientific approaches used in digital forensics. Another problem area is that there are no sufficient rules and guidelines that are followed in different jurisdictions to leave no doubts as to how digital evidence should be collected and dealt with. It can have a negative bearing on the accuracy of forensic findings which, should be reproducible and free from doubt, are key requirements in scientific admissibility. Another issue is the actual validation of such

kinds of instruments as forensic software. These tools must be thoroughly validated with respect to the various scenarios and other potential use conditions and the functionality of the data, they, in fact, analyze cannot be changed. Mainly, proprietary software does not allow for verification since there is a lack of information disclosed to the public. In addition, due to the constantly evolving technology, in which installation of patches or new technologies may alter the landscape within a few days, the construction of long-lasting and foolproof forensic methods is challenging.

**Krishnan, S., &Shashidhar, N. (2021).** Concepts of digital forensics and eDiscovery is critical in legal settings with the rise of the use of digital data in litigation and compliance investigations. Digital forensics can be described as a methodical and systematic approach of conducting a thorough analysis to retrieve data from devices in order to attain the evidence in its most pristine state, on the other hand, eDiscovery can be described as the process that entails searching for, locating and projecting the electronically stored information (ESI) in response to a lawful demand. Both of these disciplines complement each other thus improving the accuracy and efficiency of the legal discovery process. Digital evidence presented in a court of law has to undergo a legal scrutiny, for this reason, forensic specialists use specific methodologies to make the evidence meet the required standards.

**Hassan, N. A. (2019).** Digital forensics elements include the foundational elements of the discipline together with the process of examination and analysis of the information, either stored in or transferred through, digital devices. This field is very important in ischemia which involves search for evidence from computers, mobile phones, servers, and networks among others. The first step involves acquiring and maintaining the integrity of electronic materials: they cannot be changed from the state they were in at the time they were taken. This is then succeeded by a detailed examination where forensic technologists go through digital replicas of the data in a bid to search for certain information which is very crucial to the case and with out influencing the authenticity of the evidence. These exceptional methods are used when data carving, hashing to check the data integrity and analyzing file attributes.

**Ferrazzano, M., &Raffaella, B. (2021).** Digital forensics is one of the newest and most important specialties in the field of cyber security which demands strict observance of certain guidelines pertaining to the legal use of the materials accumulated by the experts. Guidelines or principles that should be used in the digital forensics are closely associated with a formal process that must be followed, covering such stages as identification, acquisition and examination of the electronic evidence. This entails duplication of all the information contained

in a manner that does not alter the status of the evidence in any way as it will eliminate distortion of data or loss of the same. Due to these reasons, analysts have to ensure that the evidence is traceable and every process that is followed in the investigation is documented for credibility.

**Challenges Faced by Law Enforcement and Corporations**

1. Technical Challenges
    - Encryption and Data Access: Modern encryption techniques make it difficult to access data, requiring sophisticated tools and methods to decrypt and analyze information.
    - Data Volume and Complexity: The sheer volume of digital data and the complexity of different file formats and storage media present significant challenges in data analysis and management.
    - Rapid Technological Advancements: Keeping up with the fast pace of technological changes and emerging cyber threats requires continuous updating of skills, tools, and methodologies.
2. Operational Challenges
    - Resource Constraints: Both law enforcement agencies and corporations often face limitations in terms of budget, manpower, and specialized equipment necessary for conducting comprehensive digital forensic investigations.
    - Skill Gaps: There is a shortage of trained digital forensic experts, which hampers the ability to effectively investigate and respond to cyber incidents.
    - Time Sensitivity: Investigations often need to be conducted swiftly to prevent further damage or data loss, adding pressure on forensic teams to deliver rapid and accurate results.
3. Legal and Ethical Issues
    - Jurisdictional Challenges: Cybercrimes often cross international borders, creating complex jurisdictional issues and requiring cooperation between multiple legal systems and law enforcement agencies.
    - Chain of Custody: Maintaining the integrity and admissibility of digital evidence through proper chain of custody procedures is critical but can be difficult to ensure in practice.

- Privacy Concerns: Balancing the need for thorough investigations with respect for individuals' privacy rights and data protection regulations (e.g., GDPR) presents a significant ethical dilemma.

4. Data Privacy Concerns
    - Regulatory Compliance: Adhering to various data protection regulations and standards while conducting digital forensic investigations can be challenging, especially when handling sensitive personal information.
    - Data Breach Implications: Mismanagement of data during an investigation can lead to further breaches, legal liabilities, and loss of public trust.
5. Coordination and Collaboration
    - Inter-Agency Cooperation: Effective digital forensic investigations often require collaboration between different law enforcement agencies, which can be hampered by bureaucratic hurdles and lack of standardized protocols.
    - Corporate and Law Enforcement Collaboration: Building trust and effective communication channels between corporations and law enforcement is essential but can be difficult due to differing objectives and priorities.
6. Cost and Resource Allocation
    - High Costs of Tools and Training: The advanced tools and continuous training required for effective digital forensics can be prohibitively expensive, especially for smaller organizations and law enforcement agencies with limited budgets.
    - Sustainability: Ensuring that digital forensic capabilities are sustainable over the long term, with ongoing investment in technology and expertise, is a major challenge for both sectors.
7. Evolving Threat Landscape
    - Advanced Persistent Threats (APTs): Cybercriminals and state-sponsored actors employ sophisticated tactics that constantly evolve, making it difficult for forensic teams to stay ahead of new threats.
    - Emerging Technologies: The advent of technologies like the Internet of Things (IoT), blockchain, and cloud computing introduces new challenges for digital forensics, requiring adaptation and innovation in investigative approaches.

Addressing these challenges requires a multi-faceted approach, including investment in technology and training, fostering collaboration between stakeholders, and developing robust legal frameworks to support digital forensic activities.

**Law**

The legal framework that govern digital forensics in India consists of the Information Technology Act 2000 (IT Act), rules, and regulation derived from the Indian Penal Code (IPC) as well as rules and guidelines under the Indian Evidence Act, 1872. These laws give legal grounds for the examination, acquisition, and the possibility to present the digital evidence in the process. Here's an overview of the key legal provisions and their implications for digital forensics in India:Here's an overview of the key legal provisions and their implications for digital forensics in India:

Information Technology Act, 2000

1. Section 43: This section deals with general cases, unauthorised access, theft and sabotage of computer systems. It provides sanction on unauthorized access to a computer, computer system or a network as well as on unauthorized disclosure of data and tampering with computers.
2. Section 65: This section is concerned with alteration of computer source documents. It provides penalty for whoever, with or without intent to defraud, conceals, destroys or alters any computer source code used for a computer, computer program, computer system, or network.
3. Section 66: This section covers computer-related offenses. It broadly defines hacking, identity theft, and other cybercrimes, prescribing penalties for such activities.
4. Section 66A: Previously addressed the sending of offensive messages through communication services but was struck down by the Supreme Court in 2015 for being unconstitutional.
5. Section 66B to 66E: These sections detail various offenses such as dishonestly receiving stolen computer resources or communication devices (66B), identity theft (66C), cheating by personation using computer resources (66D), and violation of privacy (66E).
6. Section 67: This section deals with publishing or transmitting obscene material in electronic form, prescribing penalties for such actions.
7. Section 69: It gives the government the power to intercept, monitor, or decrypt any information generated, transmitted, received, or stored in any computer resource if it is necessary for the interests of sovereignty, integrity, defense, security of the state, friendly relations with foreign states, or public order.

8. Section 79: Provides immunity to intermediaries (like ISPs) from legal liability for user-generated content if they follow due diligence guidelines and do not actively participate in unlawful acts.

Indian Evidence Act, 1872

1. Section 65A and 65B: These sections concern the electronic records as business evidence. Section 65B deals with provisions of admissibility of electronic records whereby it has provided that electronic records shall only be admissible on the basis of a certificate that will state the contents and manner in which the records have been produced.

Indian Penal Code, 1860

1. Sections 464, 465, 468, and 469: These sections cover offenses related to forgery, including the forgery of electronic records and documents.
2. Section 499 and 500: These sections deal with defamation, which can also apply to defamatory content shared digitally.

**Conclusion**

Digital investigation is an essential component in both law enforcement and corporate security G360. Digital forensics, therefore, holds benefits for law enforcement agencies in probing and or prosecuting numerous forms of electronic crimes such as hacking, fraud and identity theft. In doing so it aids in assisting in the development of good and proper legal cases whereby justice is clearly achieved. The two features of the software of tracing the footprints and recovery of deleted data is extremely useful in handling complicated cybercrimes. In the context of corporations, digital forensics thus assumes the important function to safeguard company data and thus corporate business. In the case of hacking, leaks, piracy and other malicious internal user's activity digital forestry assist in quick detection of threats and security breaches. Besides preventing the daily loss of thousands of dollars, it also contributes to retention of customers as well as adherence to different rules and regulations. In the same way, it aids in the construction of effective cybersecurity measures and preparedness to tackle incidences. Digital forensics is indispensable for law enforcement and corporations; it provides efficient methods to investigate criminal activities, protect against cyber threats and meet the requirements of regulation authorities. With the constant developments witnessed in the area of cyber threat, it is evident that the role of the digital forensics in the enhancement of digital security and soundness will be even more significant in the future.

## Future Work

The practices of the digital forensics for law enforcement and corporations in the future will be useful to address specific areas of work such as adopting more advanced technology, enhancing the tools and techniques utilized in digital forensics, the strengthening of the legal and ethical perspectives related to digital forensic works, and the collaboration and public awareness on digital forensics. AI and ML can improve the speed and efficacy of forensic investigation and blockchain forensics can make the evidence tamper-proof and preserve the chain of the forensic process. Defining modern approaches to create new generation of the tools for the analyzing the using of new technologies, such as IoT devices and cloud computing, the new features for real-time forensic tools is necessary. Forging the goals, norms, and values of digital evidence itself by helping to define international legal standards governing its management and developing extensive codes of ethics for investigators will guarantee the compliance with privacy and data protection. This is why courses that increased the expertise, as well as presented standardisation and certification procedures, have to be implemented. Frameworks and public-private partnerships will also improve inter-agency and cross-sector collaboration and thereby facilitate knowledge exchange as well as shared use of resources. Encouraging academic scholarship and industry-driven advancement will solve existing threats and future c Kathryn Oneto 13 challenges. The appropriate use of big data analytics for the improvement of managing data as well as addressing the problems of data privacy and security is crucial.

## References

1. Holt, T. J., Bossler, A. M., &Seigfried-Spellar, K. C. (2022). Cybercrime and digital forensics: An introduction. Routledge.
2. Lawton, D., Stacey, R., & Dodd, G. (2014). eDiscovery in digital forensic investigations. CAST Publication, (32/14).
3. Arshad, H., Jantan, A. B., &Abiodun, O. I. (2018). Digital forensics: review of issues in scientific validation of digital evidence. Journal of Information Processing Systems, 14(2), 346-376.
4. Reyes, A., & Wiles, J. (2011). The best damn cybercrime and digital forensics book period. Syngress.
5. Gourav Kumar Sharma,“Digital Privacy and Constitutional Rights in Administrative Law”,AdvAnces in multidisciplinAryreseArch And innvOAtiOn” icAmri-2023 ON 28-S9TH OCTOBER 2023

6. Krishnan, S., &Shashidhar, N. (2021). Interplay of digital forensics in ediscovery. International Journal of Computer Science and Security (IJCSS), 15(2), 19.
7. Charpentier, H. M. (2013). Computer forensics and law enforcement: The need for inexpensive, reliable, fast and easy to use forensic tools in the field (Doctoral dissertation, Utica College).
8. Hassan, N. A. (2019). Digital forensics basics: A practical guide using Windows OS. Apress.
9. Ferrazzano, M., &Raffaella, B. (2021). Digital forensics: best practices and perspective. COLLEZIONE DI GIUSTIZIA PENALE, 13-48.
10. Jones, A., &Valli, C. (2011). Building a digital forensic laboratory: Establishing and managing a successful facility. Butterworth-Heinemann.
11. Malik, A. W., Bhatti, D. S., Park, T. J., Ishtiaq, H. U., Ryou, J. C., & Kim, K. I. (2024). Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges. Sensors, 24(2), 433.
12. Graves, M. W. (2013). Digital archaeology: the art and science of digital forensics. Pearson Education.
13. Yesilyurt, H. (2011). The response of American police agencies to digital evidence. University of Central Florida.
14. Bayuk, J. (Ed.). (2010). CyberForensics: understanding information security investigations. Springer Science & Business Media.
15. Garrison, C. P. (2010). Digital forensics for network, Internet, and cloud computing: a forensic evidence guide for moving targets and data. Syngress.
16. Manson, D., Carlin, A., Ramos, S., Gyger, A., Kaufman, M., &Treichelt, J. (2007, January). Is the open way a better way? Digital forensics using open source tools. In 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07) (pp. 266b-266b). IEEE.
17. Gourav Kumar Sharma ,"Assessing the Potential Economic Impact of the Digital India Act on India's GDP",International Journal of Research in Economics and Social Sciences(IJRESS) Vol. 13 Issue 09, September- 2023 ISSN: 2249-7382 | Impact Factor: 8.018|
18. Al Fahdi, M. (2016). Automated Digital Forensics and Computer Crime Profiling (Doctoral dissertation, University of Plymouth).

19. Kirschenbaum, M., Ovenden, R., Redwine, G., & Donahue, R. (2010). Digital forensics and born-digital content in cultural heritage collections.
20. Santhy, D. K., &Padmanabhan, D. A. S. (2023). A Review on the Changing Dimensions of Digital Forensics in Criminal Investigations. SVP National Police Academy Journal, Forthcoming.
21. Ijeh, A. C., & Curran, K. (Eds.). (2021). Crime Science and Digital Forensics: A Holistic View. CRC Press.
22. Tsado, L., & Kim, J. S. (2022). Assessing the Practical Cybersecurity Skills Gained through Criminal Justice Academic Programs to Benefit Security Operations Centers (SOCs). Journal of Cybersecurity Education, Research and Practice, 2022(1).
23. Beardall, D. (2023). Unveiling the Digital Shadows: Cybersecurity and the Art of Digital Forensics