



International Journal for
Electronic Crime Investigation

ISSN: 2522-3429 (Print)
ISSN: 2616-6003 (Online)

DOI: <https://doi.org/10.54692/ijeci.2026.1001/273>

Research Article

Vol. 10 issue 1 Jan-Jul 2025

Emerging Trends in Mobile and Cloud Digital Forensics: A Survey

Syeda Shan-e-Zahra¹, Irshad Ahmed Sumra², Jasia Javed³, Sidra Khan⁴

^{1,2,3,4}School of Systems and Technology, University of Management and Technology, Lahore, 54000, Pakistan

Corresponding Author: s2025108003@umt.edu.pk

Received: June 25, 2026, **Accepted:** June 29, 2026; **Published:** June 30, 2026

ABSTRACT

From its beginnings in computer disc analysis, digital forensics has greatly expanded to include a variety of fields, such as mobile, cloud, network, database, and multimedia forensics. The article provides a comprehensive review of the latest digital forensic methods with emphasis on mobile and cloud forensics. We reach the conclusion that cloud forensics is still at an early stage of development and its tools suffer from basic problems of abstraction, volatility, and scalability, whereas the tools for mobile forensics, such as CAINE and EnCase, are relatively mature and reliable. As a result of the new containerized environment enabled by Docker and Kubernetes, there is now a 'race to acquisition' problem as the temporary evidence is being lost and deleted automatically. The findings from our investigation throw light on key areas where explainable automated analysis, Forensic-as-a-Service frameworks, and cross-cloud evidence correlation still have a long way to go. Through product, performance and functional indicators we conduct comparison of forensic tools and propose future avenues of forensic research, which include proactive forensic readiness programmers and zero-trust forensic frameworks.

Keywords: Digital forensics, mobile forensics, cloud forensics, forensic tools, container forensics, evidence acquisition, cybercrime investigation

1. INTRODUCTION

To collect, analyses, store, and present digital data for investigative purposes, digital forensics uses scientific concepts. Digital forensics is concerned with digital evidence such as computers, cellphones, servers, networks and cloud-related systems, whereas the physical forensics is about DNA, bloodstains and other

physical evidence. The area has developed from the idea of computer disc analysis into a multitude of specialized fields with their own tools and methods [1]. The increased use of mobile devices and cloud computing has drastically changed the investigative scene. Mobile devices have high volume potentially acceptable data, and currently, 75% of the world's population uses mobile devices as the main platform for computing [1]. In addition to

bringing new forensic issues and unparalleled scalability, cloud computing has revolutionized organizational infrastructure. The methods developed for the actual hardware access context will no longer apply in these contexts [2].

Distributed storage, virtualized infrastructure, multi-tenancy, and remote access via provider-controlled interfaces are all features of cloud environments. These characteristics make it very challenging to collect, preserve, and validate evidence [3]. In highly dynamic environments (e.g. containerized applications using Docker, Kubernetes), workloads and artefacts related to that workload may only temporarily exist in the system before being automatically erased or overwritten [4].

The proliferation of cloud-native applications and connectivity devices, Internet of Things (IoT) devices and systems, edge computing, and Artificial Intelligence (AI) enabled infrastructure, is making these digital forensic investigations more challenging. Most modern incidents these days take place on more than one device, ranging from the platforms and virtual machines used, through mobile devices, to cloud services. Forensic investigators need integrated investigation frameworks that can correlate heterogeneous evidence while preserving the integrity, privacy and admissibility of the data. This changing picture underscores the need for ongoing advances in the techniques and methods of forensic practice and encourages a comparative discussion in this survey. Moreover, this paper makes a contribution by exploring existing tools in the forensic field, documenting the existing research gaps, and discussing emerging technologies which will influence the future of digital forensic investigation.

The rest of this paper is structured according to: Section 2 introduces the taxonomy of the seven prominent areas of digital forensics and their distinguishing features. Section 3 covers in detail the analysis of mobile forensic tools, extraction methods and comparative performance analysis. Section 4 covers cloud forensic methodologies, complexity of the service models, and the issues of containerized environments. Section 5 summarizes the main results and identifies some key research needs for future. Section 6 wraps the paper with a summary of implications to forensic practitioners and researchers.

2. TYPES OF DIGITAL FORENSICS

There are seven key areas of digital forensics, each having unique tools, methods, and difficulties [1].

2.1. Database Forensics

Database forensics focuses on backups, logs, and transactions while examining physically stored databases. Limited database logging, decreased cutting viability, and encrypted databases that hinder investigations are some of the main challenges [5]. Programs such as Digital Detective Blade may be able to recover deleted database logs [6].

2.2. Network Forensics

To find intrusions and assaults, network forensics monitors and analyses network traffic. Time synchronization issues, a lack of compatibility for the SCADA protocol, and trouble capturing fast network packets are some of the challenges [7]. Zeek, Xplico, Snort, and Wireshark are notable tools [8]

2.3. Disk and Computer Forensics

Retrieving artefacts from hard discs, SSDs, and USB devices is the most traditional forensic method [9]. Data extraction is increasingly using machine learning techniques [10]. FTK Imager, The Sleuth Kit, SANS SIFT, CAINE, and DEFT are examples of common tools [11].

2.4. Multimedia Forensics

In order to confirm integrity and pinpoint source devices, multimedia forensics analyses audio, video, pictures, and documents [12]. Because of worries about deepfakes and GAN-generated content, this subject has received a lot of academic interest in the last ten years [13]. Amped Five, VIP 2.0, Foremost, and Scalpel are some of the tools [14].

2.5. Mobile Forensics

Drones, GPS units, tablets, and smartphones are the main focus of mobile forensics [15]. Multiple operating systems, the lack of unifying frameworks, hardware encryption, and physical acquisition methods that could cause device damage are challenges [16].

2.6. Cloud Forensics

Digital forensic techniques are used to cloud computing settings, such as IaaS, PaaS, and SaaS models, in cloud forensics [17]. The absence of Forensic-as-a-Service architecture, service-level agreements that hinder data collection, jurisdictional issues, and the scarcity of tools are among the difficulties [18]. Although digital forensic domains are traditionally studied independently, real-world cybercrime investigations often require evidence collection from multiple forensic domains simultaneously. For example, a ransomware attack may involve compromised mobile devices, cloud storage, network communications, databases, and endpoint systems. As a result, integrated forensic concepts capable of supporting the capability to correlate evidence from diverse environments

are gaining in importance. These multi-disciplinary efforts add to the accuracy of investigations, analyze data in a timely manner, and increase the reliability of the forensic findings that can be used in a legally admissible capacity in a distributed infrastructure.

3. MOBILE FORENSICS: TOOLS AND TECHNIQUES

Mobile forensics is part of digital investigation because mobile devices are the devices of choice for many people around the world when it comes to computation. Mobile devices are also the devices used by 75% of the world's population for accessing the internet, and for this reason, these devices contain vast quantities of potentially relevant evidence, which can be leveraged for both criminal and civil investigations [19]. There are five different options for extraction in the field that are all appropriate to any particular device situation and investigative circumstance. Manual extraction is the easiest method in which investigators inspect and use the user interface of the device to document what they observe by using screenshots and photos. In order to retrieve active files, contacts, call logs, and messages, logical extraction uses software tools to connect to the device via common interfaces like USB, Bluetooth, or WiFi. Another more advanced method of extraction is JTAG extraction, which is a hardware-based extraction that utilizes special equipment that allows for direct access to the processor of the device without operating system intervention. In certain scenarios where the flash memory chip must be fully recovered, chip-off is a major risk of irreversible damage to the device. A recent development is "micro read" which allows for the highest potential data recovery capacities by reading data directly from the flash memory cells via electron microscopes

[11].



Figure1: Mobile Forensic Process [24]

The systematic process in the mobile forensics investigation is designed to ensure the integrity of the evidence throughout the process. It begins with the collection and conservation of the artifact, ensuring that the artifact is properly secured and protected from any potential contamination. The next step involves digital evidence extraction and picture backups, when the forensic software makes exact copies of the device's storage for analysis. Once recovered, the data is painstakingly scrutinized, analyzed and verified by the use of specialized forensic procedures to ensure the data is both authentic and admissible according to the law. This approach to the use of meticulous methodology is in place throughout the entire chain of custody of digital evidence from mobile devices throughout enactment of judicial proceedings, ensuring that the evidence is preserved and carries evidentiary weight.

A total of 19 commercial and open-source forensic tools were compared in depth for the

Kali Linux, Windows and Ubuntu platforms and the results revealed noticeable differences in capacity and performance. The measures evaluated products included file system support, reporting format, platform support, and kinds of license. Processing time, memory usage and CPU utilization were analyzed as performance metrics. Functional metrics supported forensic domains and looked at timeline analysis capabilities. Among the CAINE reviewed tools, CAINE and EnCase proved to be the most reliable and accurate, followed by SIFT Workstation and Belkasoft Evidence Center. However, the study also revealed that none of the tools has reached complete reliability and universal applicability across all the forensic realms. This result highlights the fact that in order to conduct comprehensive and successful investigations, investigators usually need to use a variety of tools [1].

The use of AI and machine learning has revolutionized mobile forensics, with instant

artifact classification and automatic malware detection, improved application behavior analysis, and timeline reconstruction. Forensic processing of large volumes of smartphone data is enhanced by the use of AI assisted forensics processing tools, which help to reduce manual efforts and improve accuracy of evidence identification during processing. On the other hand, the benefits of AI-driven forensics come with some challenges related to explainability, transparency, algorithmic bias, and the legal acceptance of AI-produced forensic outcomes. Future mobile forensic studies should thus concentrate on the development of intelligent forensic systems that are explainable, trustworthy and meet both technical and judicial requirements.

4. CLOUD FORENSICS: TOOLS AND TECHNIQUES

While cloud forensics provides digital forensic investigation on the cloud computing environment, the problems associated with it are different from the traditional forensic aspects [2]. The difficulty level of cloud forensics investigations can differ widely depending on the service model. For Infrastructure-as-a-Service configurations, some access to the virtual machines and storage volumes may still exist. However, PaaS and SaaS systems obscure the view, and only a limited amount of information is provided in logs and application data, with provider-generated information being the primary source [19]. Unlike the traditional investigation where examiners may physically pick up hard drives, take forensic photos, and perform controlled laboratory analysis, the cloud systems are distributed storage, virtualized infrastructure, and having remote access through provider controlled interfaces [20].

Cloud Computing architecture consists of three main layers. The service customer side gives access to the user via front end interfaces. The network layer is linked with cloud apps and cloud software infrastructure. The “provider” side includes management systems, service APIs, and back-end hardware facilities. The provider infrastructure is comprised of the core operating system, cloud-specific infrastructure, and underlying IT infrastructure, providing scalable cloud services and maintaining identity and access management systems and a strong back-end support. Recent progress in the storage of workload and other storage artefacts is only possible in highly dynamic settings with the help of the Docker and Kubernetes container platforms [4]. Therefore, a “race to acquisition” exists in which the pertinent evidence must be collected prior to its automatic removal or replacement. Log-based artefacts are the most common types of evidence, especially in SaaS systems, according to systematic mapping studies. IaaS is largely related to disc and snapshot artefacts. As ephemeral and container artefacts become ever more common in PaaS, forensic methods are not quite ready for the dynamic infrastructures. A drawback of automated systems is their lack of transparency; they often work as closed systems that yield results with no apparent lines of reasoning. Legal admissibility in forensic situations is seriously challenged by this. There are still few cloud forensic tools available. IaaS environment is supported by DFF and FROST, IaaS, PaaS, and SaaS by Network Miner and Omnippeek [21]. With the rise of container orchestration platforms like Kubernetes, there are added forensic challenges to the existing cloud infrastructure. Valuable forensic artefacts slip away within seconds and are often lost due to the high dynamism and destruction of containers during task completion. Therefore, investigators need to assume that they must rely on a continuous monitoring, running logging, and

immutable storage snapshots and automated mechanisms that maintain evidence to ensure they remain forensic-ready. The combination of cloud native security monitoring and forensic

acquisition methods therefore will soon be a requirement for investigations conducted in the cloud [36].

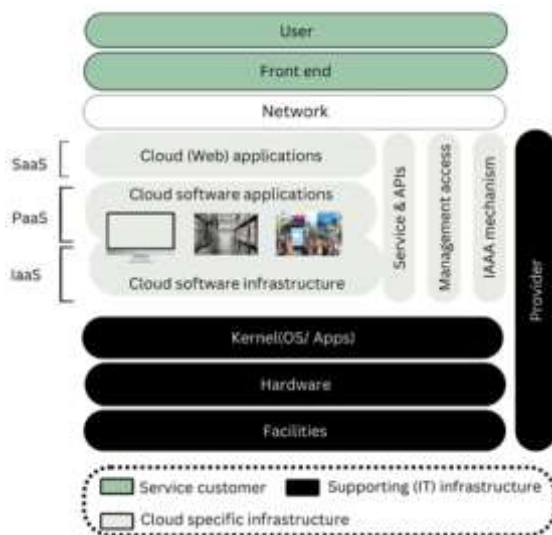


Figure2: cloud forensic process [25]

5. FUTURE RESEARCH DIRECTIONS AND KEY FINDINGS

5.1. Key Findings

This survey shows that mobile forensics seems to be at a relatively mature point compared to cloud forensics. Methodological methods that have been established and common forensic tools like CAINE and EnCase are reliable tools for evidence collection and analysis. Despite the above, mobile forensic investigations are still plagued by various limitations such as hardware encryption, fragmentation of operating systems, anti-forensic techniques and lack of standardized investigation frameworks [1]. Cloud forensics, on the other hand, is a relatively new research field because the cloud environment is dynamic and distributed in nature. The virtualization, multi-tenancy, abstraction of services and the

growing popularity of containerized infrastructures make evidence acquisition more complex. Current forensic tools offer only limited support for cloud environments especially when the access to system resources is limited and the investigated object is Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS) [2], [20]. Moreover, the comparative analysis shows that there is no single tool to support all of the digital forensic domains. Rather, investigators will need to use a variety of forensic tools in conjunction with each other based on the nature of the cyber incident. The results also show growing interest in the use of AI in forensic investigations, but with challenges regarding explain ability, transparency and legal admissibility that still need to be addressed [23].

5.2. Research Limitations Identified in Existing Studies

The comparative analysis identifies some of the limitations that are found in all the studies reviewed. Current research is mostly conducted in particular domains of forensics, and not in a multi domain forensic approach. The immaturation of cloud forensic solutions is hindered by challenges that include virtualization, multi-tenancy, jurisdictional and access problems to cloud infrastructures. Likewise, the majority of AI-assisted forensic methods lack interpretability, which diminishes the potential for the use of automatically derived

information in court. In addition, there are several studies that do not have experimental validation and/or real-world examples of their use in actual forensic investigations, which limits their ability to be seen as practically useful in operational investigations. Moreover, existing methodologies for container forensics, cross-cloud evidence correlation and forensic readiness are still not fully developed, suggesting ample opportunities for further research in the area [20] - [23].

Table1: Research Limitations and Identified Research Gaps in Digital Forensics

Research Area	Identified Limitation	Research Gap
Mobile Forensics	Device diversity, hardware encryption, and OS fragmentation complicate investigations.	Need for standardized cross-platform forensic frameworks.
Cloud Forensics	Limited investigator access due to virtualization and multi-tenancy.	Develop efficient cloud-native forensic acquisition techniques.
Container Forensics	Ephemeral containers result in rapid loss of forensic artifacts.	Automated runtime evidence collection and preservation mechanisms are required.
Forensic Tools	No single tool supports all forensic domains or investigation scenarios.	Design unified and interoperable multi-domain forensic platforms.
Artificial Intelligence	AI-based forensic models lack transparency and explain ability.	Develop Explainable AI (XAI) for legally admissible forensic investigations.
Evidence Correlation	Existing studies mainly focus on single-platform investigations.	Support cross-cloud and multi-source evidence correlation.
Validation	Many proposed frameworks lack real-world experimental validation.	Conduct large-scale empirical evaluations using realistic cyberattack datasets.
Forensic Readiness	Most approaches are reactive rather than proactive.	Develop Forensic-as-a-Service (FaaS) and proactive forensic readiness frameworks.

5.3. Future Research Directions

Further studies are needed on the design of intelligent and integrated forensic scenarios to assist in a multi-digit world. Forensic tools should evolve to include Explainable Artificial Intelligence (XAI), to enhance transparency and

to increase the legal admissibility of computer-generated forensic evidence. Also, the introduction of Forensic-as-a-Service (FaaS) architectures can have a significant impact on the collection of evidence in cloud computing platforms, plus lesser complexity in the investigation process [20]. Another critical

research area is the progress towards forensic preparedness for cloud-native architectures, which includes continuous monitoring of the evidence, automatic preservation of artifacts and runtime logs of containers. New technologies like blockchain can enhance chain-of-custody controls, and federated learning can support

groups to share forensic intelligence without sharing data at the center. Moreover, future forensic solutions should enable cross-cloud evidence correlation, Zero Trust Digital Forensics, scalable multi-domains investigation frameworks for the growing complexity of cyber threats [21], [25].

Table 2: Comparative Analysis of Digital Forensic Methods, Working Models, and Limitations

Author Name	Proposed Method	Working of Model	Limitations
Joseph & Viswanathan (2026)	- Survey of 19 commercial and open-source forensic tools. - Evaluates tools using product, performance, and functional metrics.	- Uses mean and weighted mean scoring. - Compares tools across multiple forensic domains and platforms.	- No tool supports all forensic domains. - Limited cloud forensic tools. - Timeline visualization requires improvement.
Arias et al. (2024)	- Systematic review of anti-forensic techniques. - Classifies methods used to evade forensic investigations.	- Identifies secure deletion, obfuscation, and forgery techniques. - Examines evolution of anti-forensic methods.	- Limited practical implementation guidance. - Few countermeasure strategies proposed. - Advanced anti-forensic detection remains challenging.
Nisioti et al. (2023)	- Review of 49 studies on digital forensic tool selection. - Focuses on attack reconstruction and workload optimization.	- Evaluates existing forensic frameworks. - Identifies gaps in decision support and tool selection.	- No comprehensive multi-domain ranking. - Limited real-world validation. - Decision support requires improvement.
Gupta et al. (2022)	- Reviews passive image forensic techniques. - Examines machine and deep learning approaches.	- Detects copy-move, splicing, and image retouching. - Evaluates feature extraction and classification methods.	- Sensitive to adversarial attacks. - Limited performance on complex forgeries. - Dataset bias affects generalization.
Yang et al. (2022)	- AI-based framework for network forensics. - Uses machine learning for traffic analysis.	- Detects anomalies and network intrusions. - Performs intelligent packet analysis.	- Packet loss in high-speed networks. - Scalability challenges.

			Real-time processing remains difficult.
Docker Inc. (2025)	- Documentation for Docker container platform. - Describes containerization architecture and deployment.	- Supports portable application deployment. - Packages applications with dependencies.	- Does not address forensic evidence acquisition. - Lacks guidance on preserving container artifacts. - No forensic investigation framework.
Y. Yao et al. (2025)	- AI-driven forensic analysis using machine learning. - Automates large-scale cybersecurity investigations.	- Filters and correlates forensic data. - Processes massive cloud log datasets efficiently.	- Poor explainability of AI models. - Limited forensic transparency. - Legal admissibility remains challenging.
S. Almul्ला et al. (2025)	- Comprehensive review of cloud forensic methods. - Summarizes current forensic tools and challenges.	- Reviews cloud forensic techniques. - Identifies major research trends and issues.	- Weak mapping between tools and cloud models. - Limited evaluation of solution maturity. - Research gaps remain.
S. Tyagi et al. (2024)	- Zero Trust digital forensic framework. - Uses cryptographic evidence validation.	- Verifies evidence throughout investigation. - Maintains tamper-resistant chain of custody.	- Limited experimental validation. - Scalability not fully evaluated. - Practical deployment challenges remain.
L. Elie et al. (2024)	- Kubernetes-based container forensic framework. - Investigates runtime events in Azure AKS.	- Collects container metadata and runtime logs. - Detects simulated attacks using Kubernetes artifacts.	- Evaluated only on Azure AKS. - Limited generalizability. - No standardized preservation of transient artifacts.

CONCLUSION

With tested extraction methods and dependable tools like CAINE and EnCase demonstrating excellent accuracy, this evaluation shows that mobile forensics has reached relative maturity.

Nonetheless, issues with hardware encryption, operating system variability, and the lack of unifying frameworks continue to exist. Despite growing popularity of cloud computing, cloud forensics is still relatively new. The industry has basic problems with abstraction,

scalability, and volatility that are not sufficiently addressed by current approaches. There are significant gaps between investigative capabilities and operational realities due to the lack of cloud forensic tools and the rise of containerized systems. Explainable automated analysis, cross-cloud evidence correlation techniques, Forensic-as-a-Service frameworks, and proactive forensic preparedness activities are examples of critical gaps. Investigators need to become experts in a variety of forensic fields as cybercrime grows more sophisticated. Integrated frameworks that provide scale analysis, verifiable integrity measures, and real-time evidence recording while upholding legal requirements must be given top priority in future research.

6. REFERENCES

- [1] P. Joseph and P. Viswanathan, "A comprehensive survey and analysis on multi-domain digital forensic tools, techniques and issues," *Cogent Engineering*, vol. 13, no. 1, p. 2652147, 2026.
- [2] National Institute of Standards and Technology, "NIST cloud computing forensic science challenges," NIST, Tech. Rep. IR 8006, 2020.
- [3] K. Ruan and J. Carthy, "Cloud forensics definitions and critical criteria," *Digital Investigation*, 2011.
- [4] Docker Inc., *Docker Engine Documentation*, 2025. [Online]. Available: <https://www.docker.com/>
- [5] K. E. Pavlou and R. T. Snodgrass, "Forensic analysis of database tampering," *ACM Transactions on Database Systems*, vol. 33, no. 4, pp. 1-47, 2008.
- [6] A. Al-Dhaqm et al., "Development and validation of a database forensic metamodel (DBFM)," *PLoS One*, vol. 12, no. 2, p. e0170793, 2017.
- [7] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digital Investigation*, vol. 7, no. 1-2, pp. 14-27, 2010.
- [8] R. Prasad and V. Rohokale, *Cyber Security: The Lifeline of Information and Communication Technology*. Springer Nature, 2019.
- [9] D. Bem, F. Feld, E. Huebner, and O. Bem, "Computer forensics -- Past, present and future," *Journal of Information Science and Technology*, vol. 5, no. 3, pp. 43-59, 2008.
- [10] L. Ignaczak, G. Goldschmidt, C. A. D. Costa, and R. D. R. Righi, "Text mining in cybersecurity: A systematic literature review," *ACM Computing Surveys*, vol. 54, no. 7, pp. 1-36, 2022.
- [11] L. Sanchez, C. Grajeda, I. Baggili, and C. Hall, "A practitioner survey exploring the value of forensic tools," *Digital Investigation*, vol. 29, pp. S124-S142, 2019.
- [12] W. D. Ferreira, C. B. R. Ferreira, G. da Cruz Júnior, and F. Soares, "A review of digital image forensics," *Computers & Electrical Engineering*, vol. 85, p. 106685, 2020.
- [13] L. Verdoliva, "Media forensics and deepfakes: An overview," *IEEE Journal of Selected Topics in Signal Processing*, vol. 14, no. 5, pp. 910-932, 2020.
- [14] H. Sako, K. Franke, and S. Saitoh, *Computational Forensics*, vol. 6540. Springer, 2011.
- [15] K. Barmapsalou, T. Cruz, E. Monteiro, and P. Simoes, "Current and future trends in mobile device forensics," *ACM Computing Surveys*, vol. 51, no. 3, pp. 1-31, 2019.
- [16] E. Casey, *Digital Evidence and Computer Crime*. Academic Press, 2011.
- [17] S. Khan, A. Gani, A. W. A. Wahab, M.

- Shiraz, and I. Ahmad, "Network forensics: Review, taxonomy, and open challenges," *Journal of Network and Computer Applications*, vol. 66, pp. 214-235, 2016.
- [18] B. Manral, G. Somani, K.-K. R. Choo, M. Conti, and M. S. Gaur, "A systematic survey on cloud forensics challenges," *ACM Computing Surveys*, vol. 52, no. 6, pp. 1-38, 2019.
- [19] V. Roussev and S. McCulley, "Forensic analysis of cloud-native artifacts," *Digital Investigation*, vol. 16, pp. S104-S113, 2016.
- [20] S. Almulla et al., "A state-of-the-art review of cloud forensics," *Journal of Digital Forensics, Security and Law*, 2025.
- [21] "Cloud Forensic Mapping Study," Systematic mapping study on cloud forensic tools and storage-related investigation techniques, 2020-2025.
- [22] Y. Yang et al., "AI-based solutions for network forensics: Packet analysis and anomaly detection," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2345-2360, 2022.
- [23] A. Nisioti et al., "Digital forensics tool selection, attack reconstruction, and workload optimization: A review of 49 works," *Forensic Science International: Digital Investigation*, vol. 44, p. 301511, 2023.
- [24] BDO, "Navigating the complexities of mobile forensics: Understanding the process in depth," *BDO CyberDigest*, Nov. 27, 2023. [Online].
- [25] M. Asim, A. T. Khan, A. R. Khan, U. I. Minhas, and M. Z. N. Khan, "Cloud digital forensics: Beyond tools, techniques, and challenges," *Sensors*, vol. 24, no. 2, p. 433, Jan. 2024, doi: 10.3390/s24020433.
- [26] M. Hina et al., "Safecard: Deep learning-based semantic analysis for email forensic investigation," *Forensic Science International: Digital Investigation*, vol. 37, p. 301221, 2021.
- [27] J. Choi et al., "Practical approaches for forensic recovery of SQL Server databases," *Digital Investigation*, vol. 36, p. 301112, 2021.
- [28] I. Castillo Camacho and H. Wang, "Deep-learning-based methods for image forensics: A comprehensive review," *IEEE Access*, vol. 9, pp. 133476-133498, 2021.
- [29] A. Javed et al., "Video forensics taxonomy: Deep-fake and forgery detection using machine learning," *Multimedia Tools and Applications*, vol. 80, pp. 30551-30582, 2021.
- [30] E. Nowroozi et al., "Adversarial image forensics: Machine learning techniques for FGSM-based detection," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 6, pp. 2789-2804, 2021.
- [31] S. Gupta et al., "Passive image forensics: A review of detection techniques for doctored images," *ACM Computing Surveys*, vol. 54, no. 6, p. 122, 2022.
- [32] Y. Yang et al., "AI-based solutions for network forensics: Packet analysis and anomaly detection," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2345-2360, 2022.