NUML International Journal of Engineering and Computing
Issue: 2 Volume: 3
https://numl.edu.pk/journals/nijec
Print ISSN: 2788-9629
E-ISSN: 2791-3465
DOI: 10.52015/nijec.v3i2.85

The Role of Digital Forensics in Cybercrime Investigations

Hassan Shah Khan_1[a*], Syed Muhammad Atif_ 2[b], Abeer Mustufa _ 3[c]

[a]College of Computing and Software Engineering. Ziauddin University, Karachi, Pakistan (hassan.19088@zu.edu.pk)
[b]Department of Computer Science & Information Technology, SSUET, Karachi, Pakistan (syed.muhammad.atif@gmail.com)

[c]College of Computing and Software Engineering. Ziauddin University, Karachi, Pakistan (abeer.19127@zu.edu.pk)

Submitted	Revised	Published
22-May-2025	21-June-2025	23-June-2025

Abstract

The explosion of technology in recent years has revolutionized the face of cybercrime and requires new and innovative approaches to investigating digital crimes. In this research, we present the all-encompassing role of digital forensics in cybercrime investigations with a focus on methodologies, tools, and techniques for computer forensics, mobile forensics, network forensics, and IoT forensics solutions. With the steady growth of digital systems, and the integration of these systems, has come an increase in the importance of accurate and efficient forensic methods. This paper studies the effectiveness of current digital forensic strategies and presented the challenges faced while implementing them, i.e. encryption, anti- forensic measures, and the proliferation of digital forensic evidence. The key findings now include increasing dependence on specialist forensic software, the challenges of legality and jurisdiction, and the urgent necessity of global legislation and standards so that cross-border collaboration may be effective. The paper also looks at AI and ML in automating forensics and increasing the speed and accuracy of gathering evidence. By filling the current methodological gaps and examining the existing real-life cases, this study highlights the need to keep pace with innovation in digital forensics to counteract the ever growing cyber threats adequately.

Keywords: Digital Forensics, Cybercrime Investigation, Forensic Tools and Techniques, Computer and Mobile Forensics, Network and IoT Forensics

1. Introduction

Digital forensics is a field of knowledge involving the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law [1, 2]. It encompasses various categories such as computer forensics, mobile forensics, network forensics, and new areas such as IoT [3, 4]. Digit forensics are an important tool in the effort to close the gap between technical data

* Corresponding Author: Hassan Shah Khan (hassan.19088@zu.edu.pk)

analysis and legal investigation, and offers important contributor to the treatment of digital evidence in a world more and more connected [5, 6].

- In the recent past, cybercrimes (e.g., ransomware attack, data breach, identity theft, and intellectual property theft) have increased drastically, causing tremendous harm to individuals, organizations, and governments [7, 8].
- Digital forensics enables investigators to: Recover and examine vital evidence from compromised systems [9].
- Trace down the attacker by monitoring network traffic and system logs [10, 11].
- Develop policies to reduce and prevent cyber incidents in the future [12]. Back up the court case with admissible evidence [13].

The main purpose of this research is to analyze the importance of digital forensics in response to the increased complexities of cybercrime. By examining the development and status of the digital forensic methods, we intend to provide insights into the tools and methods applied to them in several domains of forensics including computer, mobile, network and Internet of Things (IoT) forensics. Further, this research will attempt to pinpoint the roadblocks and deficiencies that prevent these approaches from being truly effective, specifically in relation to evidence preservation, legal admissibility and cross-jurisdictional cooperation. This has been well explained with reference to methodologies and case studies, the research aims to present practical implications and guidelines to enhance the efficiency, accuracy and reliability in digital forensic investigations [14, 15]. Its accomplishment is paving the way toward the evolution of digital forensics in support of the digital world and its preservation [16, 17].

Despite the many successful developments introduced to the field (the evidence collection tools and techniques being a notable instance), some issues remain unresolved. Researchers frequently face reasons for the frequent obsolescence of technology, jurisdictional complexities (ranging from mono to multi-centric systems), and increasing complexity of encrypted environments. Recent research has highlighted cooperation among all players including governments, law enforcement, and the private sector as the way to successfully tackle such barriers [18].

***R**esearch Questions*

The following research questions guide the study:

1. How has the digital forensics evolved with the challenges associated with contemporary cybercrimes?
2. What are the best practice tools and methodologies being applied?
3. What challenges the investigators do face in maintaining the integrity of digital evidence?
4. How can it possible to standardize and enhance best practices of digital forensic worldwide?

2. Literature Review

*2.1 **E**volution of Digital Forensics*

Personal Computers become widely used and paved the way for cybercrimes and digital forensics started developing in the 1980s, A digital forensics emerged a response to tremendous growth of personal computer use during the 1980s in all area of daily life from home to work [19]. Early methods concentrated on collecting data by hand from closed systems of various sizes. In the 1990s the dawn of the forensic software such as EnCase and FTK (Forensic Toolkit)-allowed a more consistent method of data retrieval and analysis [20]. The 2000s represented further advances when NIST's own guidelines encouraging more contemporary methodology to digital evidence collection and preservation came into being [7]. Major Milestone in depth is explained in Table 1 [21, 22, 23].

Table 1: Major Milestones

Year	Milestone	Significance
1995	Introduction of EnCase and FTK	Enabled comprehensive imaging and analysis of hard drives
2002	Establishment of NIST forensic guidelines	Standardized forensic practices across jurisdictions
2010	Expansion to mobile and cloud forensics	Broadened forensic scope beyond traditional computers
2020s	Focus on IoT and emerging technologies	Adapted to modern threats involving smart devices

1. Legacy forensic methods have been left behind due to the rapid development of cybercrime tactics [24].
2. Challenges include: Encryption and Obfuscation: Advanced encryption methods prevent access to the data. Scale: Big data is time-consuming to process, especially when spread across multiple storage systems [24].
3. APT (Advanced Persistent Threat): These take longer to investigate, as they are stealthy, focused assaults [24].

Global cybercrime investigations encounter jurisdictional conflicts, differing privacy laws, and ethical dilemmas, such as: Maintaining the integrity of evidence while respecting user privacy [25]. Adhering to chain-of-custody protocols to ensure admissibility in court. Digital forensics employs an array of software and hardware tools to address the challenges of modern investigations [26]. Common Categories of Digital Forensic Tools and Their Functions is explained in Table 2 [17, 27, 28].

Table 2: Common Categories of Digital Forensic Tools and Their Functions

Tool Category	Example Tools	Primary Function
Forensic Imaging Tools	FTK Imager, EnCase	Capture and preserve disk images
File Recovery Tools	Recuva, R-Studio	Recover deleted or corrupted files
Network Traffic Analyzers	Wireshark, NetWitness	Analyze and monitor network communications

Limited advancements in forensic methodologies for IoT devices and email [29]. Persistent issues with cross-border evidence sharing and analysis. Lack of standardized protocols for cloud forensic investigations [30].

3. Methodology

*3.1 **R**esearch Design Qualitative Approach*

This study applies qualitative methods to provide a comprehensive analysis:

- Qualitative Analysis: Focuses on the examination of case studies to illustrate the practical application of tools and techniques. *Data Sources and Collection Methods*

Data was collected from:

1. Academic Publications**:** Peer-reviewed journals and conference proceedings.
2. Industry Reports**:** Insights from forensic tool developers and practitioners.
3. Case Studies**:** Detailed analysis of five high-profile cybercrime investigations.

*3.2 **C**omparative Analysis of Tools*

The study conducted a comparative analysis of five widely used forensic tools based on their domain, strengths, limitations, and use cases. Comparative Analysis of Tools explained in table 3.

Table 3: Comparative Analysis of Tools

Tool	Domain	Strength	Limitation	Use Case
EnCase	Computer Forensics	Comprehensive file system analysis	High cost	Corporate data breach investigations
Cellebrite	Mobile Forensics	Effective mobile data recovery	Limited to certain devices	Criminal case investigations
Wireshark	Network Forensics	Real-time traffic monitoring	Requires expertise	Intrusion detection in networks
Magnet AXIOM	Cloud Forensics	Specialized for cloud data recovery	Jurisdictional limitations	Cloud-based financial fraud cases
IoT Inspector	IoT Forensics	Analysis of smart device vulnerabilities	Limited to certain devices	Smart home breach investigations

*3.3 **C**ase Studies*

Case studies provided insights into the practical application of these tools:

1. Corporate Data Breach**:** EnCase was used for hard drive imaging and file recovery.
2. Mobile Fraud Investigation**:** Cellebrite effectively retrieved deleted communications.
3. Network Intrusion**:** Wireshark identified malicious network traffic patterns

4. Digital Forensics Categories

*4.1 **C**omputer Forensics*

4.1.1 Computer Systems Under Scrutiny & Hard drive and file systems analysis

This includes interpreting data from computers in order to find evidence. Some of the most widely used methods include disk underpinning and metadata analysis. It facilitates in the tracking of user activities, deleted data recovery, and unauthorized access detection. They are now in legal frameworks which help to maintain the integrity and admissibility of evidence in court. EnCase and FTK software enable investigators to restore deleted or damaged files and inspect file systems for signs of disruption. They can uncover hidden partitions, fragmented files, and corrupt or altered files. Such an analysis is important to better understand: what the system did, was used for, or had happened before, during, and after an outage.

*4.2 **M**obile Forensics*

4.2.1 Forensic Extraction of Data from Mobile Devices & Challenges in Forensics on a Mobile Platform

Mobile-forensics specialists recover data from smartphones, tablets, and other hand-held gadgets. Categories of data are SMS logs, Call logs, and App logs. Methods like logical, physical, file system extraction are utilized, depending on the device type and state. Specialized software, like Cellebrite and Oxygen Forensic Suite are used to extract and decrypt data. Active OS and encryption technologies pose challenges for forensic recovery and analysis. Device diversity and vendor specific software also challenge traditional forensic methods. On the other hand, remote-wiping and cloud synchronization can result in only partial or no evidence at all during the investigation.

4.3 Network Forensics

4.3.1 Network Traffic Monitoring and Analysis

Network forensics is about recording and analyzing each data packet in order to catch an intruder or unwanted activities. It allows for the detection of malware, suspicious communication patterns and data stealing. Packet inspection tools such as Wireshark, tcpdump and intrusion detection (IDS) are widely used. The main actions performed are log analysis, packet trace, and attack vector identification. Analysts combine data from firewalls, routers, and SIEM systems to piece together timelines of the attacks. This assists in identifying the origin, modus operandi and effect of the intrusion towards incident response and prevention.

4.3 IoT Forensics

4.4.1 IoT Devices Investigated & Issue of Privacy and Security

IoT forensics encompasses the investigation of smart things like wearables, home automation systems and industrial IoT configurations. These devices may contain logs, sensor data, and communication logs that can be used as evidences. Researchers must also cope with a wide range of hardware, proprietary protocols, and small storage sizes in the corresponding analysis. Millions of IoT devices are gathering huge amount of sensitive personal data, which could lead to privacy concerns and demand a specialized forensics methods. This data being accessed without proper authorization can result in surveillance, identity theft, and even manipulation of device order. Forensic methods are required to maintain the soundness of the data and respect to the privacy laws and ethical values. The categories of digital forensics are illustrated graphically in Figure 1

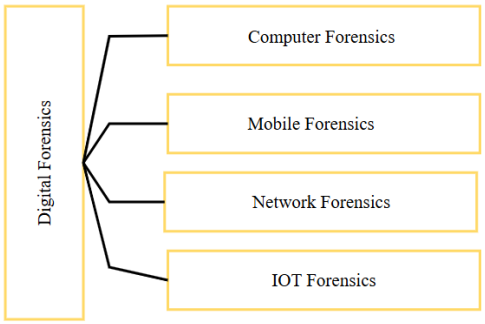

Figure 1: Categories of Digital Forensics

5. Digital Forensics Stages

5.1 Identification

Identification is an indispensable step in every DFI process. This stage is about identifying and identifying digital devices, systems and storage that are possibly sources of relevant evidence. These could be computers, phones, servers, the cloud, network gear or external drives. The detectives start by surveying the crime scene, the real-world crime scene as well as the virtual crime scene, to figure out where evidence might be. For instance, in a cybersecurity incident, analysts might investigate server log files, firewall access logs, and router settings to find the device or address that is the source of an attack. It is important to speed up right sources of evidence at the beginning of an investigation because you do not want to lose hard information or cross-contaminating the evidence.

*5.2 **C**ollection*

After identification, comes the gathering of digital evidences. The purpose of this phase is to collect information in a forensically sound manner and in its original state with its integrity maintained. This requires the use of specialized hardware and software tools to guarantee that no tampering with the evidence occurred during acquisition. For example, write blockers are used in order not to undesirably write on storage media when extracting data. Investigating officers also produce forensic images - complete bit by bit copies of the original storage medium thus enabling source data to be examined without having to use source systems again. This is recorded in detail including times, tools, and personnel to ensure a valid chain of custody for legal purposes.

*5.3 **P**reservation*

Preservation ensures that once digital evidence is collected, it remains intact, unaltered, and available for future analysis or legal use. This involves storing the data in secure, tamper-proof containers such as encrypted drives or forensic vaults with restricted access. Regular integrity checks are performed using cryptographic hash functions like SHA-256 or MD5 to verify that the data has not been altered. Comparing the original hash values with new ones during analysis confirms the authenticity of the evidence. Backups are also maintained in controlled environments to prevent accidental loss. Effective preservation is essential for ensuring the reliability of forensic investigations, especially in long-term or multi-agency cases.

*5.4 **E**xamination*

The examination will perform a methodical analysis of digital information to find evidence that either supports or refutes an investigative theory. This is accomplished using computer forensics tools to sift through and make sense of relevant data in large sets of data. Usual methods include text searching, by which you find documents, emails or files around a specific topic or person. Particular timeline analysis is also used for timeline reconstruction, like login events, file changes or unauthorized activities. This allows investigators to see what occurred, when and who all was involved. Thorough investigation is extremely important for strong and legally solid case preparation.

*5.5 **A**nalysis*

The analysis is based on the examination stage and identifies relations between the data from various sources and draws coherent conclusions. This stage can entail associating user activities, system logs, application usage, and network traffic information. For example, they could correlate email time stamps with firewall log data to determine the location and timing of a phishing attack. Pattern matching, outlier detection, and behavior analysis are also critical here. The objective of this article is to reveal the correlation of the digital evidence at the scene of crime, and to give a clear introduction of the crime case. This phase needs to remain secure as it transforms raw data into usable final intelligence for legal or internal means.

*5.6 **R**eporting*

Reporting is the last part of the process whereby all unearthed evidences are documented in an organized and understandable manner. The report must start with an Executive Summary addressing the most important findings and conclusions, avoiding the use of technical terms and for the readers on policy level. They are then continued with a Detailed Evidence Description comprising databases, logs, known files, screenshots, metadata, and forensic images that form the basis for the findings. The report needs to be transparent, fact-based and court-admissible, according to law and regulations. Further, Figure 2 in this paper presents a visual representation of the key steps involved in the digital forensics process

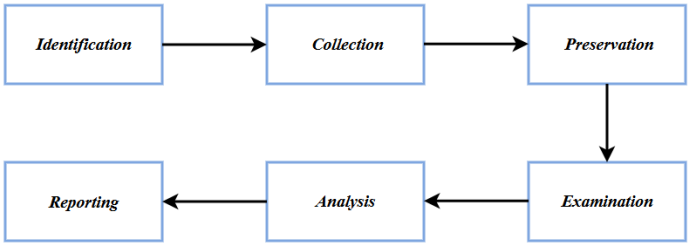

Figure 2: Stages of Digital Forensics

6 Tools Used in Digital Forensics

6.1 Software Tools

6.1.1 Forensic Imaging Tools

Such tools generate a sector-by-sector replica of a digital device as evidence. Popular tools include: FTK Imager: Takes forensic images and does verification. X-Ways Forensics: Comes with quick imaging and deep analysis. Guymager: A Linux-based open-source solution too, which prides itself on being 'fast and reliable'.

6.1.2 Software for file recovery and analysis

Software utilities developed to restore and analysis of deleted or hidden files: Recuva: Great for retrieving lost files on Windows. Autopsy: Free and open source with advanced analysis capabilities. Magnet AXIOM : Collects and examines data from computer, mobile, and cloud sources.

6.2 Hardware Tools

6.2.1 Write Blockers

These devices prevent any modifications to storage media during analysis. Key Write Blockers explained in Table 4.

Table 4: Key Write Blockers

Device	Purpose	Advantages	Limitations	Example Use Case
Tableau T35u	Blocks USB-based modifications	Supports high-speed USB drives	Limited support for legacy devices	Corporate investigations
Wiebetech Forensic UltraDock	Prevents tampering on SATA devices	Easy to use and portable	High cost	Criminal evidence preservation

6.2.2 Data Acquisition Devices

These are specialized devices for duplicating and preserving storage data. Disk Jockey PRO**:** Captures and clones hard drives efficiently. DeepSpar Disk Imager**:** Ideal for recovering data from failing drives.

*6.3 **E**merging Tools*

6.3.1 AI-Driven Forensic Tools & Cloud-Based Forensic Solutions

Tools like Axiom Cyber and Nuix use AI to analyze large datasets and identify patterns. Emerging features include anomaly detection and automated classification. Magnet AXIOM Cloud and AWS Forensics**:** Manage its definitions to collect and analyze the data in cloud multi-tenant environments. Key Tools in Digital Forensics in depth explained in Table 5.

Table 5: Key Tools in Digital Forensics

Category	Tool	Key Function	Strengths	Limitations
Forensic Imaging	FTK Imager	Creates disk images	High integrity	High resource demand
File Recovery	Recuva	Recovers deleted files	Simple to use	Limited enterprise support
Network Analysis	Wireshark	Captures and analyzes packets	Real-time visibility	Steep learning curve
Mobile Forensics	Cellebrite UFED	Extracts data from mobile devices	Supports locked devices	High cost
Cloud Forensics	Magnet AXIOM Cloud	Recovers cloud-stored data	Cross-platform capability	Jurisdictional challenges

7 Techniques in Digital Forensics

*7.1 **E**vidence Collection and Preservation*

7.1.1 Chain of Custody & Ensuring Data Integrity

A documented process to ensure evidence integrity from collection to court presentation. Essential steps include logging the date, time, and individuals handling the evidence. Use of hashing algorithms such as MD5 or SHA-256 to verify that evidence has not been tampered with. Tools like HashMyFiles are commonly used.

*7.2 **D**ata Recovery and Analysis*

7.2.1 Deleted File Recovery & Network Traffic Analysis

Specialized tools recover files deleted intentionally or accidentally. Tools: Recuva for consumer-level recovery. R-Studio for professional investigations. Capturing and analyzing network packets to trace unauthorized access or malware activities. Tools: Wireshark**:** Visualizes packet-level data. NetWitness Investigator**:** Identifies unusual traffic patterns.

*7.3 **A**dvanced Techniques*

7.3.1 Mobile Forensics & IoT & Cloud Forensics

Focuses on extracting data from smartphones, tablets, and wearable devices. Techniques include rooting/jailbreaking to bypass security measures. Tools: Cellebrite UFED**:** Extracts data from locked devices. MSAB XRY**:** Supports a wide range of mobile platforms. IoT Forensics**:** Involves collecting data from smart devices, such as wearables and home automation systems. Cloud Forensics**:** Focuses on data stored in distributed cloud servers. Challenges: Data volatility in IoT and cloud environments. Jurisdictional conflicts in multi-tenant cloud systems

8 Case Studies

*8.1 **H**igh-Profile Cybercrime Investigations*

Case Study 1: The Sony Pictures Hack (2014) [21]

Overview**:** A politically motivated cyberattack against Sony Pictures Entertainment, attributed to a state-sponsored group. Tools and Techniques Applied**:** Network Forensics**:** Captured and analyzed network traffic logs using tools like Wireshark. Malware Analysis**:** Reverse-engineered the malware used in the attack. Lessons Learned**:** Importance of proactive threat monitoring. Need for robust incident response protocols.

Case Study 2: Colonial Pipeline Ransomware Attack (2021) [24]

Overview**:** A ransomware attack disrupted fuel supplies across the U.S. Tools and Techniques Applied**:** Memory Forensics**:** Investigated live systems using Volatility. Cryptocurrency Tracking: Traced ransom payments using blockchain analytics tools. Lessons Learned**:** Importance of securing operational technology (OT) systems. Need for backup and disaster recovery plans.

Case Study 3: The Cambridge Analytical Data Scandal (2018) [23]

Overview**:** Unlawful data harvesting from millions of Facebook profiles for political advertising. Tools and Techniques Applied**:** Cloud Forensics**:** Analyzed Facebook's API logs to trace data access. Privacy Audits**:** Reviewed compliance with GDPR and other privacy regulations. Lessons Learned**:** The need for stricter data access controls. Enhancing user awareness about data privacy.

Case Study 4: Marriott International Data Breach (2018) [22,25,26]

Overview**:** Breach of 500 million customer records over four years. Tools and Techniques Applied**:** Database Forensics**:** Used SQL tools to trace unauthorized queries. User Behavior Analytics: Identified anomalous user actions. Lessons Learned**:** Early detection through behavior monitoring is vital. Encrypting sensitive data reduces exposure.

*8.3 **C**omparative Analysis of Case Studies*

Comparative Analysis of Case Studies explained in table 6 *[24,25,26]*.

Table 6: Comparative Analysis of Case Studies

Case Study	Successes	Limitations
Sony Pictures Hack	Identified attackers through forensic analysis	Lack of preventive measures
Colonial Pipeline Attack	Successfully traced ransom payments	Limited OT system security
Cambridge Analytica Scandal	Exposed data misuse practices	Delayed response to public outcry
Marriott Data Breach	Comprehensive database analysis	Insufficient encryption of customer data

9 Challenges and Limitations

9.1 Technical Challenges

Data Volumes**:** Managing and analyzing large-scale digital evidence. Encryption and Obfuscation: Dealing with encrypted communication and obfuscated malware. Emerging Technologies**:** Forensics for IoT, cloud, and blockchain systems is still evolving.

9.2 Legal and Jurisdictional Issues & Ethical Dilemmas in Digital Forensics

Cross-Border Investigations: Conflicting international laws and jurisdictional disputes. Admissibility of Evidence: Ensuring digital evidence meets legal standards for court. Privacy Concerns: Balancing thorough investigations with individual privacy rights. Bias in AI Tools: Ethical concerns regarding potential biases in AI-driven forensic tools.

10 Conclusion

This paper exposes the importance of digital forensics in fighting against cybercrime. This paper covers the techniques, tools and methods used in digital investigations and highlights some of the problems with them - and the forensic process - from a practitioner's perspective. New technologies, including AI and blockchain pose both challenges and opportunities. As a result, future work must develop effective forensic frameworks for these technologies. Organizations should invest in advanced forensic tools and training. Governments and industry stakeholders must collaborate to establish unified standards and frameworks. Researchers should explore innovative solutions to address ethical and jurisdictional challenges.

11 Future Directions

11.1 Emerging Trends in Digital Forensics

Role of AI and Machine Learning

- AI-based software such as Magnet AXIOM uses machine learning techniques to automatically classify evidence and detect anomalies.
- Predictive analytics can predict future vectors of attack from historical data.

Blockchain-Paired Integration

- Blockchain can ensure the integrity of evidence by maintaining tamper-proof logs.
- Smart contracts could automate evidence collection and chain-of-custody documentation.

10.2 Recommendations for Improving Digital Forensics

Development of Unified Standards & Enhancing Cross-Border Collaboration

- International protocols to regulate digital forensics procedures and evidence management.
- Establishing intergovernmental agreements to facilitate data sharing and joint investigations.
- Creating centralized repositories for global threat intelligence.

Acknowledgment

I am grateful to my supervisor, Dr. Syed Muhammad Atif, Assistant Professor, Computer Science Department, for his help and continued support during the scope of this research work.

Disclosure Statement

This review article is for educational and academic purpose only. The author states that there is no funding or any conflict of interest related to this work.

Author Contributions

Hassan Shah Khan (1st author): Led the design and structure of the manuscript, conducted the primary research, performed the comparative analysis of forensic tools, and wrote the main sections of the paper including the literature review and methodology.
Dr. Syed Muhammad Atif (2nd author): Supervised the research work, guided the formation of the research methodology, and reviewed the manuscript for academic quality and coherence.
Abeer Mustufa (3rd author): Supported data collection, curated references, and assisted in formatting tables and figures throughout the manuscript.

References:

[1] Digital forensics – Wikipedia. https://en.wikipedia.org/wiki/Digital_forensics

[2] "Digital Forensics", EC-Council, 2022. Available: https://www.eccouncil.org/cybersecurity-exchange/computer-forensics/what-is-digital-forensics/#phase-viii---documentation-and%20reporting. [Accessed: 01- Jan- 2022]

[3] https://www.techtarget.com/searchsecurity/definition/computer-forensics

[4] Ghazinour, K., Vakharia, D. M., Kannaji, K. C., & Satyakumar, R. (2017, September). A study on digital forensic tools. 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI). https://doi.org/10.1109/ICPCSI.2017.8392304

[5] Jean-Paul A. Yaacoub, 2021. Digital Forensics vs. Anti-Digital Forensics: Techniques, Limitations, and Recommendations. https://arxiv.org/abs/2103.17028

[6] Yee Ching Tok, Chundong Wang, 2020. STITCHER: Correlating Digital Forensic Evidence on Internet-of-Things Devices. https://doi.org/10.48550/arXiv.2003.07242

[7] Barbara Guttman, John M. Butler, Kelly Sauerwein, November 2022. Digital Investigation Techniques: A NIST Scientific Foundation Review. Digital Investigation Techniques: A NIST Scientific Foundation Review. https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8354.pdf

[8] The Hacking of Sony Pictures: A Columbia University Case Study, 2022. https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf

[9] Ravindu Denuwan, July 2023. Marriott International Data Breach. https://www.researchgate.net/publication/372524901_Marriott_International_Data_Breach

[10] https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal

[11] Jack Beerman, 2023. A Review of Colonial Pipeline Ransomware Attack https://ieeexplore.ieee.org/document/10181159

[12] 2022, https://worldbigroup.com/Event-blogs/breaches-&-IP-theft

[13] https://www.kaspersky.com/resource-center/definitions/data-breach

[14] Noura Hamad, May 2022. Digital Forensics Tools Used in Cybercrime Investigation – Comparative Analysis. https://www.researchgate.net/publication/360463703_Digital_Forensics_Tools_Used_in_Cybercrime_Investigation_-Comparative_Analysis

[15] Cybercrime Investigation Tools and Techniques You Must Know! https://cybertalents.com/blog/cyber-crime-investigation

[16] Bhat, W. A., AlZahrani, A., & Wani, M. A. (2021). Can computer forensic tools be trusted in digital investigations? Science & Justice, 61(2). https://doi.org/10.1016/j.scijus.2020.10.002

[17] Sanders, 2010. Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems. https://repository.root-me.org/R%C3%A9seau/EN%20-%20Practical%20packet%20analysis%20-%20Wireshark.pdf

[18] Mandia, K., Prosise, C., & Pepe, M. (2003). Incident Response & Computer Forensics (2nd ed.). McGraw-Hill. https://cdn.preterhuman.net/texts/law/forensics/Incident%20Response%20and%20Computer%20Forensics%202nd%20ed.%20-%20C.%20Prosise,%20K.%20Mandia%20(2003)%20WW.pdf

[19] Dweikat, M., Eleyan, D., & Eleyan, A. (2021). Digital Forensic Tools Used in Analyzing Cybercrime. Journal of University of Shanghai for Science and Technology, 23(3). https://doi.org/10.51201/Jusst12621

[20] Barik, K., Das, S., Konar, K., Chakrabarti Banik, B., & Banerjee, A. (2021). Exploring user requirements of network forensic tools. Global Transitions Proceedings, 2(2), 350–354. https://doi.org/10.1016/j.gltp.2021.08.043

[21] T. Panhalkar, "E-Mail Forensic tools: Infosavvy Information Security training," Infosavvy Security and IT Management Training, 28-Sep 2020. Available: https://info-savvy.com/e-mail-forensic-tools. [Accessed: 1-Jan-2022].

[22] Prasanthi, B. v. (2016). Cyber Forensic Tools: A Review. International Journal of Engineering Trends and Technology, 41(5). https://doi.org/10.14445/22315381/IJETT-V41P249

[23] Fahad M. Ghabban, Ibrahim Alfadli, August 2021, Comparative Analysis of Network Forensic Tools and Network Forensics Processes. [2108.05579]. https://www.researchgate.net/publication/353862702_Comparative_Analysis_of_Network_Forensic_Tools_and_Network_Forensics_Processes

[24] Mark Reith, 2002. An Examination of Digital Forensic Models. https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf

[25] Sriram Raghavan, 13 November 2012. Digital forensic research: current state of the art. https://link.springer.com/article/10.1007/s40012-012-0008-7

[26] Watson, S., & Dehghantanha, A. (2016). Digital forensics: the missing piece of the Internet of Things promise. Computer Fraud and Security, 2016(6), 5–8. https://doi.org/10.1016/S1361-3723(15)30045-2

[27] Nelson, 2010. Guide to Computer Forensics and Investigations (4th ed.). Cengage Learning. https://www.academia.edu/44012128/Guide_to_Computer_Forensics_and_Investigations_Processing_Digital_Evidence

[28] Ghafarian, A., Mady, A., & Park, K. (2020). An Empirical Analysis of Email Forensics Tools. International Journal of Network Security & Its Applications, 12(3), 39–57. https://doi.org/10.5121/ijnsa.2020.12303

[29] F. S. Ltd, "Email forensics software," Aid4Mail. Available: https://www.aid4mail.com/email-forensics. [Accessed: 02-Jan-2022].

[30] Ruan, K. 2011. Cloud Forensics: An Overview. Advances in Digital Forensics VII, IFIP AICT. https://www.researchgate.net/publication/229021339_Cloud_forensics_An_overview