DIGITAL FORENSICS IN CYBERCRIME INVESTIGATIONS.

Mark William Hakim Adolfo
Dept. of Computer Science & Applications
Sharda University,
Greater Noida, India
Markwilliamhakim612@gmail.com

MR. Ravi Prakash
Department of Computer Science and Application
Sharda University
Greater Noida. Uttar Pradesh
India,
ravi.chaturvedi1@sharda.ac.in

Abstract
— The rapid proliferation of digital technology has brought with it an unprecedented surge in cybercrime, demanding robust investigative methodologies capable of extracting, preserving, and analyzing digital evidence in legally admissible ways. This paper presents a comprehensive investigation into digital forensics as applied to cybercrime cases, tracing the evolution from early disk-imaging techniques to modern cloud and mobile forensics. We examine the systematic forensic process model comprising identification, preservation, collection, analysis, and presentation phases, while evaluating widely used forensic toolkits including Autopsy, FTK, EnCase, Volatility, Wireshark, and Cellebrite UFED. The paper analyzes empirical cybercrime statistics from 2018 to 2023, documenting the global cost trajectory from $1.5 trillion to over $10.3 trillion, and discusses the implications for investigative practice. Key challenges addressed include encryption barriers, anti-forensics techniques, jurisdictional complexities, massive data volumes, and the evolving cloud computing landscape. Legal and ethical dimensions are explored through the lens of major international frameworks such as the Budapest Convention and domestic legislation, including CFAA, GDPR, and the Indian IT Act. We further discuss emerging trends in artificial intelligence-assisted forensics, blockchain evidence, and IoT forensics. The findings indicate that while digital forensics has matured significantly as a discipline, it must continuously adapt to counter sophisticated threat actors and evolving technologies. Future directions include automated forensic pipelines, standardized international legal procedures, and enhanced privacy-preserving investigation methods.

Keywords— digital forensics; cybercrime investigation; electronic evidence; incident response; forensic tools; chain of custody; anti-forensics; cloud forensics.

Introduction

The digital revolution has fundamentally transformed the nature of criminal activity. As society becomes increasingly reliant upon networked computing infrastructure, malicious actors exploit these dependencies to conduct an ever-expanding range of cybercrimes — from sophisticated ransomware campaigns targeting critical infrastructure to large-scale financial fraud and identity theft operations. The Internet Crime Complaint Center (IC3) reported receiving over 912,000 complaints in 2023, representing a staggering escalation compared to the 467,361 complaints filed in 2019 [1]. The financial toll is equally alarming: global cybercrime costs are projected to reach $10.5 trillion annually by 2025, surpassing the GDP of most developed nations [2].

Digital forensics — defined as the application of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events — has emerged as the cornerstone of cybercrime investigation [3]. Unlike traditional forensic disciplines, digital forensics must contend with the volatile, mutable, and distributed nature of electronic evidence, demanding rigorous methodologies to ensure evidentiary integrity.

This paper provides a comprehensive examination of digital forensics in the context of cybercrime investigations. Section II surveys the historical evolution of the discipline. Section III details the core forensic investigation process model. Section IV presents an empirical analysis of cybercrime trends. Section V evaluates leading forensic tools and technologies. Section VI addresses the major challenges facing practitioners. Section VII examines the legal and ethical framework. Section VIII discusses emerging research frontiers, and Section IX concludes with forward-looking recommendations.

II. BACKGROUND AND EVOLUTION OF DIGITAL FORENSICS

A. Historical Origins

The origins of digital forensics can be traced to the early 1980s, when law enforcement agencies first encountered personal computers in criminal investigations. The FBI's Computer Analysis and Response Team (CART), established in 1984, represents one of the earliest institutionalized efforts to extract and analyze digital evidence [4]. Early practitioners employed rudimentary methods — copying floppy disk contents and manually examining hexadecimal dumps — that bore little resemblance to the systematic methodologies in use today.

The 1990s witnessed a critical maturation phase driven by the proliferation of the World Wide Web, the emergence of networked environments, and several high-profile cases that underscored the importance of electronic evidence. The prosecution of Kevin Mitnick in 1995 — at the time considered the most wanted computer criminal in the United States — highlighted the capacity of digital evidence to prove sophisticated cybercrimes that left no physical traces [5]. This era also saw the development of the first purpose-built forensic tools, including Safe Back (1990), which enabled exact bit-stream copies of hard disks for forensic analysis.

B. Formalization and Standardization

The 2000s brought increasing formalization as academic institutions, professional organizations, and government bodies worked to establish standardized frameworks. The Scientific Working Group on Digital Evidence (SWGDE) published guidelines that provided a foundation for evidence handling practices, while the National Institute of Standards and Technology (NIST) established the Computer Forensic Tool Testing (CFTT) program to validate forensic software [6]. The publication of ISO/IEC 27037:2012 — Guidelines for Identification, Collection, Acquisition and Preservation of Digital Evidence — marked a significant milestone in international standardization.

Simultaneously, academic programs in digital forensics proliferated. Institutions including Purdue University, University College Dublin, and Edith Cowan University developed dedicated curricula, establishing digital forensics as a recognized scientific discipline rather than a practitioner craft. Professional certifications, including the Certified Forensic Computer Examiner (CFCE) and Certified Computer Examiner (CCE), provided credentials that courts could recognize when evaluating expert testimony.

C. The Cloud and Mobile Era

The second decade of the twenty-first century introduced two transformative challenges: cloud computing and mobile devices. By 2020, over 50% of enterprise workloads resided in cloud environments, creating significant complications for evidence acquisition [7]. Traditional forensic approaches premised on physical access to storage media became inadequate when evidence might reside on servers distributed across multiple jurisdictions, controlled by third-party service providers operating under different legal frameworks. Simultaneously, the ubiquity of smartphones — devices containing comprehensive records of communications, location data, financial transactions, and social interactions — made mobile forensics a critical subspecialty.

III. THE DIGITAL FORENSICS INVESTIGATION PROCESS MODEL

A systematic investigation process is fundamental to ensuring that digital evidence is admissible in legal proceedings. The widely adopted five-phase model — Identification, Preservation, Collection, Analysis, and Presentation — provides a structured framework that guides practitioners from initial incident response through court testimony [8].

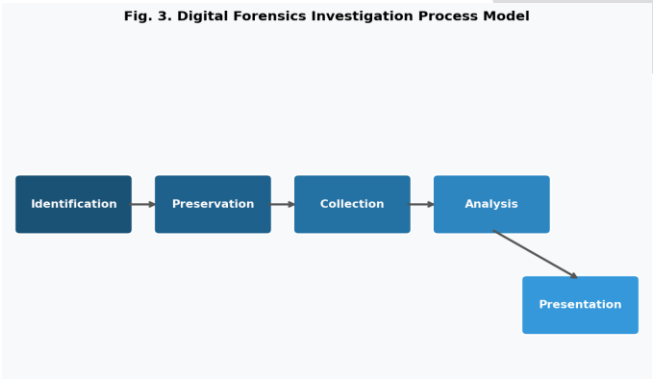


Fig. 3. Digital Forensics Investigation Process Model

A. Identification

The identification phase involves recognizing the existence of an incident, determining its scope, and identifying potential sources of digital evidence. Investigators must answer fundamental questions: What systems were involved? What data is potentially relevant? Where might evidence reside? This phase requires collaboration between technical teams, legal counsel, and organizational stakeholders. Sources may include workstations, servers, mobile devices, network logs, cloud services, IoT devices, and third-party systems [9]. Proper documentation of the digital crime scene begins here, as any action taken — even observation — can potentially alter digital evidence.

B. Preservation

Preservation is arguably the most legally critical phase of the investigation. The central objective is to prevent alteration, contamination, or destruction of digital evidence. This encompasses both physical preservation (protecting hardware from damage, electromagnetic interference, or unauthorized access) and logical preservation (preventing software-level changes to data). Write-blockers — hardware or software mechanisms that prevent write commands from reaching storage media during imaging — are essential tools in this phase. The chain of custody documentation, which records every individual who accesses evidence, every transfer of custody, and every examination performed, must be established and meticulously maintained from this point forward [10].

C. Collection and Acquisition

Collection involves the actual capture of digital evidence in a forensically sound manner. The standard approach for persistent storage media is forensic imaging — creating a bit-for-bit copy of the entire storage device that captures not only active files but also deleted files, slack space, unallocated space, and file system metadata. Industry-standard tools such as dd (Linux), FTK Imager, and Guymager produce forensic images in formats including E01 (Expert Witness Format), AFF (Advanced Forensic Format), and raw DD format. Cryptographic hash values (MD5, SHA-1, SHA-256) calculated before and after imaging verify that the copy is an exact duplicate of the original [11]. For volatile evidence — data in RAM that would be lost upon system shutdown — memory acquisition must be prioritized and performed before any other action.

D. Analysis

The analysis phase transforms raw acquired data into meaningful evidence through systematic examination. Investigators employ a range of techniques depending on the nature of the investigation: file system analysis to recover deleted files and examine directory structures; timeline analysis to reconstruct the sequence of events; keyword searching to locate relevant content; metadata analysis to identify document authorship and modification history; network traffic analysis to trace communications; and log analysis to document system and user activities [12]. This phase demands both technical proficiency and investigative intuition, as relevant evidence is often obscured by anti-forensics techniques or buried within terabytes of irrelevant data.

E. Presentation and Reporting

The final phase involves communicating findings in a manner accessible to non-technical audiences, including judges, juries, and legal counsel. The forensic report must be comprehensive, accurate, and written in plain language without sacrificing technical precision. It must document the methodology employed, tools used (including version numbers and validation test results), every step taken during the investigation, and the specific evidence found. Expert witnesses presenting digital evidence must be prepared to explain complex technical concepts and withstand rigorous cross-examination regarding methodology, chain of custody, and the reliability of tools used [13].

IV. EMPIRICAL ANALYSIS OF CYBERCRIME TRENDS

Understanding the quantitative dimensions of cybercrime is essential for contextualizing the role and importance of digital forensics. The following analysis synthesizes data from multiple authoritative sources, including the FBI IC3 Annual Reports, Cybersecurity Ventures, and IBM's Cost of a Data Breach Reports spanning 2019 to 2023.

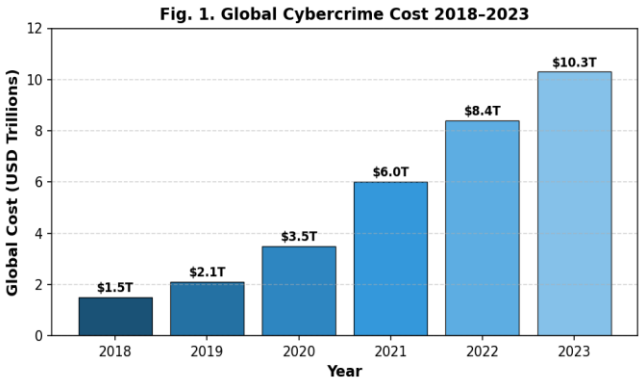


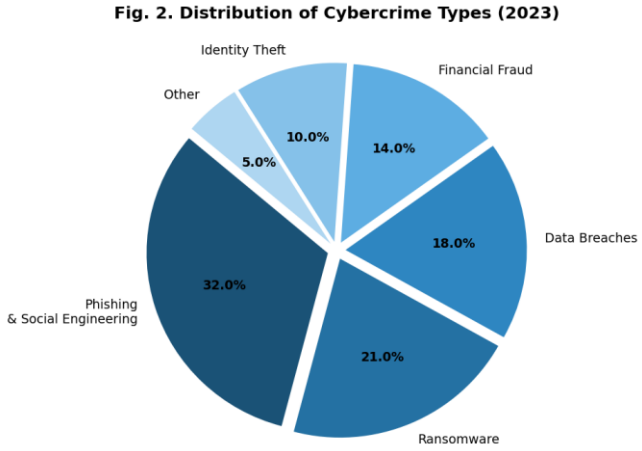
Fig. 1. Global Cybercrime Cost 2018–2023 (Source: Cybersecurity Ventures, FBI IC3)

TABLE I

Global Cybercrime Statistics 2019–2023

Source: FBI IC3 Annual Reports [1]; Cybersecurity Ventures [2]; IBM Cost of a Data Breach Report [14]

As illustrated in Table I and Fig. 1, cybercrime costs have exhibited an alarming upward trajectory, increasing by approximately 587% from 2018 to 2023. This exponential growth reflects both the increasing sophistication of threat actors and the expanding attack surface created by digital transformation initiatives accelerated by the COVID-19 pandemic. Phishing and social engineering attacks represent the most prevalent category, accounting for approximately 32% of all reported incidents, followed by ransomware (21%) and data breaches (18%)



.

Fig. 2. Distribution of Cybercrime Types (2023)

The distribution of cybercrime types, illustrated in Fig. 2, underscores the diversification of cybercriminal tactics. Ransomware has emerged as a particularly severe threat, with several incidents — including the Colonial Pipeline attack (2021) and the Kaseya VSA breach (2021) — demonstrating the potential for widespread societal disruption [15]. From a forensic perspective, each cybercrime category presents distinct investigative challenges and requires specialized techniques for evidence recovery.

V. DIGITAL FORENSIC TOOLS AND TECHNOLOGIES

The effectiveness of a digital forensics investigation is substantially dependent upon the tools employed. A comprehensive toolkit must span multiple domains: disk forensics, memory forensics, network forensics, and mobile device forensics. The following subsections evaluate the most widely deployed tools across each domain.

A. Disk and File System Forensics Tools

Autopsy, developed by Basis Technology, is the most widely adopted open-source forensic platform globally. Built upon The Sleuth Kit (TSK) library, Autopsy provides a graphical interface for disk image analysis, deleted file recovery, keyword searching, and hash analysis. Its modular plugin architecture enables extensibility, and the platform supports analysis of FAT, NTFS, Ext2/3/4, HFS+, and other common file systems [16]. FTK (Forensic Toolkit) by Exterro offers comparable functionality in a commercial package notable for its indexed search capabilities and robust database backend, which provides significant performance advantages when processing large evidence sets. EnCase by OpenText has long been the enterprise standard, particularly valued for its scripting language (EnScript) that enables automation of complex forensic tasks.

B. Memory Forensics

Volatile memory (RAM) analysis has become indispensable as malicious actors increasingly employ fileless malware techniques that leave minimal traces on disk. Volatility Framework, an open-source memory forensics platform, supports analysis of memory dumps from Windows, Linux, macOS, and Android systems. Its plugin architecture provides capabilities including process listing, network connection enumeration, registry hive extraction, and malware detection through techniques such as comparing process memory against disk images [17]. Rekall Framework, while now superseded by Volatility 3, contributed significantly to advancing memory forensics methodology.

C. Network Forensics

Network forensics involves the capture, recording, and analysis of network packets for investigative purposes. Wireshark, the industry-standard open-source packet analyzer, enables deep inspection of network traffic across hundreds of protocols and is indispensable for reconstructing network-based attacks. Network Miner provides a complementary approach by extracting files, credentials, and session data from packet captures. In enterprise environments, Security Information and Event Management (SIEM) platforms, including Splunk and IBM QRadar, aggregate and correlate log data from multiple sources, providing investigative teams with a unified view of network activity during an incident.

D. Mobile Device Forensics

Mobile devices have become the primary focus of many investigations due to the extraordinary breadth of data they contain: communications, location history, financial transactions, photographs, and application data. Cellebrite UFED (Universal Forensic Extraction Device) is the law enforcement standard for mobile acquisition, supporting physical, logical, and file system extraction across thousands of device models. MSAB XRY provides comparable capabilities with particular strength in handling encrypted devices. Oxygen Forensic Detective excels at parsing application data from both iOS and Android platforms, including data from messaging applications, social media, and cloud-synchronized content [18].

TABLE II

Comparative Analysis of Digital Forensic Tools

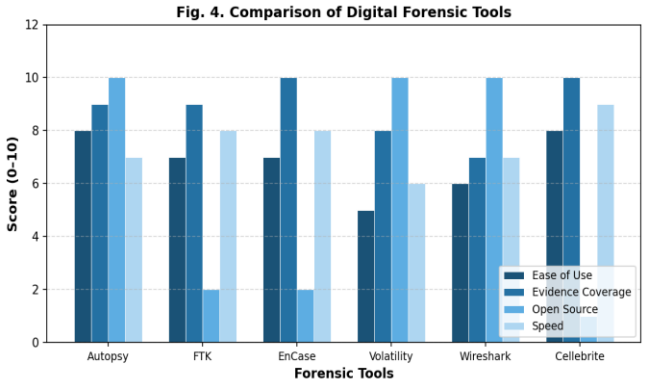


Fig. 4. Comparison of Digital Forensic Tools Across Key Parameters

As illustrated in Table II and Fig. 4, no single tool satisfies all investigative requirements. Commercial solutions such as EnCase and Cellebrite UFED offer superior evidence coverage and vendor support, but at a high cost. Open-source tools, including Autopsy, Volatility, and Wireshark, provide accessibility and community-driven development but may require greater technical expertise. Effective forensic practice typically involves combining multiple tools to achieve comprehensive evidence coverage while cross-validating findings.

VI. CHALLENGES IN DIGITAL FORENSICS INVESTIGATIONS

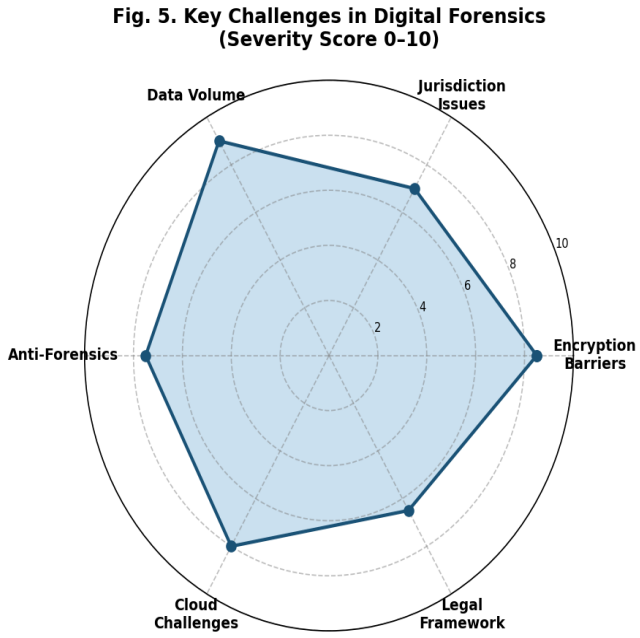


Fig. 5. Key Challenges in Digital Forensics (Severity Score 0–10)

A. Encryption and Cryptographic Barriers

*Full-disk encryption, implemented by default on modern smartphones and increasingly on personal computers (BitLocker on Windows, File Vault on macOS, dm-crypt on Linux), represents one of the most significant barriers to evidence acquisition. Without the encryption key or user passphrase**, encrypted evidence** is computationally intractable — brute-force attacks against modern AES-256 encryption are not feasible with current technology [19]. End-to-end encrypted messaging applications, including Signal and WhatsApp present additional challenges: even with physical access to a device, communication content may be inaccessible. The debate over government mandated encryption backdoors remains deeply contentious, with security researchers arguing that any backdoor is fundamentally incompatible with robust encryption.*

B. Anti-Forensics Techniques

Anti-forensics encompasses deliberate actions taken by perpetrators to impede forensic investigation. Common techniques include secure file deletion using tools such as Eraser or BleachBit, steganography (concealing data within innocuous media files), timestamp manipulation to alter file metadata, rootkit deployment to hide malicious processes and files, and log clearing. More sophisticated actors employ living-off-the-land techniques that use legitimate system tools for malicious purposes, leaving minimal distinguishing artifacts. Countering these techniques requires both specialized analytical methods and a thorough understanding of their technical implementation [20].

C. Jurisdictional and Cross-Border Complexity

Cybercrime is inherently transnational — a phishing campaign may be designed in Eastern Europe, operated through servers in Southeast Asia, and victimize individuals in North America. This geographic dispersion creates profound legal challenges: investigators must navigate multiple legal systems, each with distinct evidentiary standards, data protection laws, and extradition frameworks. Mutual Legal Assistance Treaties (MLATs) provide a mechanism for cross-border evidence sharing, but the process is notoriously slow — average MLAT processing times can exceed one year — creating tension with the time-sensitive nature of cybercrime investigations [21]. The Budapest Convention on Cybercrime has facilitated international cooperation among its 68 signatories, but many nations — including Russia and China, which are frequent sources of cybercriminal activity — have not acceded to the treaty.

D. Data Volume and Big Data Challenges

The volume of potential digital evidence in modern investigations has grown exponentially. Enterprise servers may contain petabytes of data; even personal devices routinely hold hundreds of gigabytes. The 2016 San Bernardino investigation reportedly involved extraction and analysis of multiple terabytes of data from a single smartphone [22]. Processing such volumes through traditional sequential analysis is infeasible within investigative timeframes, necessitating automated triage tools and machine learning-assisted analysis to identify relevant subsets of data for detailed examination.

E. Cloud Computing Challenges

Cloud computing has fundamentally altered the digital evidence landscape. Evidence may reside on infrastructure shared with thousands of other customers, potentially in data centers distributed across multiple jurisdictions. Investigators typically cannot access cloud infrastructure directly and must rely on preservation requests and legal process served upon service providers. Response times and scope of production vary significantly across providers, and data may be subject to deletion through automated lifecycle management policies if preservation is not timely requested [23]. Multi-cloud and hybrid environments compound these challenges.

VII. LEGAL AND ETHICAL FRAMEWORK

A. Evidence Admissibility Standards

For digital evidence to be admissible in legal proceedings, it must satisfy established legal standards. In the United States federal courts, the Daubert standard (established in Daubert v. Merrell Dow Pharmaceuticals, 509 U.S. 579, 1993) requires that expert forensic testimony be based on sufficient facts, derived from reliable principles and methods, and applied reliably to the facts of the case. Courts assess whether the methodology has been tested, whether it has been peer-reviewed, whether there is a known error rate, and whether it is generally accepted within the relevant scientific community [24]. The Federal Rules of Evidence, particularly Rules 702 and 901, govern the admissibility of expert testimony and authentication requirements for electronic records.

B. International Legal Frameworks

TABLE III

Key Legal Frameworks Governing Digital Forensics and Cybercrime

As summarized in Table III, the legal landscape governing digital forensics and cybercrime is characterized by fragmentation at the national level and limited international harmonization. The Budapest Convention on Cybercrime (Council of Europe, 2001) remains the most significant international instrument, providing a framework for procedural law applicable to digital investigations and establishing mechanisms for international cooperation [25]. The European Union's General Data Protection Regulation (GDPR) creates complex intersections with forensic investigations: while legitimate law enforcement activities may be exempt from certain GDPR provisions, the regulation significantly affects forensic investigations involving EU citizens' data in civil and private contexts.

C. Chain of Custody and Evidence Integrity

The chain of custody — the chronological documentation of evidence custody, control, transfer, analysis, and disposition — is fundamental to evidence admissibility. Any break in the chain

creates grounds for challenging evidence authenticity. Digital forensics practitioners must meticulously document every action taken: when evidence was collected, by whom, how it was transported, who had access, when it was analyzed, and what actions were taken. Cryptographic hash verification provides a technical mechanism for demonstrating that evidence has not been altered — a match between the hash value computed at acquisition and the hash computed at any subsequent examination constitutes a strong mathematical proof of integrity [26].

D. Privacy and Ethical Considerations

Digital forensic investigations inevitably involve access to deeply personal information. A forensic examination of a mobile device or personal computer may expose intimate communications, medical information, financial records, and information about third parties who are not subjects of the investigation. Forensic practitioners have ethical obligations to limit examination to information relevant to the investigation (proportionality), to handle sensitive information with appropriate discretion, and to avoid disclosure of privileged communications. Professional codes of ethics, including those of the International Association of Computer Investigative Specialists (IACIS) and the High Technology Crime Investigation Association (HTCIA), provide guidance on navigating these obligations [27].

VIII. EMERGING TRENDS AND FUTURE DIRECTIONS

A. Artificial Intelligence and Machine Learning in Forensics

Artificial intelligence and machine learning are increasingly being integrated into digital forensic workflows, addressing the dual challenges of data volume and analytical complexity. Machine learning classifiers can automatically categorize files (e.g., distinguishing CSAM from innocuous images at scale), identify malware families from behavioral patterns, cluster similar documents, and detect anomalous network traffic patterns indicative of compromise. Natural language processing enables semantic analysis of communications beyond simple keyword matching. AI-assisted forensics tools, including Nuix Workstation and Relativity, are already deployed in large-scale investigations [28]. However, the use of AI in forensics raises questions about transparency and explainability — "black box" algorithms may produce results that cannot be adequately explained to a court, potentially undermining admissibility.

B. Blockchain and Cryptocurrency Forensics

The widespread adoption of cryptocurrencies for ransomware payments, darknet market transactions, and money laundering has created a specialized forensic subdomain. While often misconceived as providing anonymity, blockchain transactions create an immutable public ledger that, when combined with sophisticated analytical techniques, can often be traced to real-world identities. Companies including Chainalysis, Elliptic, and Cipher Trace have developed platforms specifically for blockchain forensics, enabling investigators to trace fund flows, cluster wallet addresses associated with the same entity, and identify exchange touchpoints where cryptocurrency intersects with the traditional financial system [29].

C. Internet of Things (IoT) Forensics

The proliferation of IoT devices — from smart home assistants and connected appliances to industrial control systems — has created new categories of digital evidence. IoT devices may capture data about their environment (audio, video, sensor readings) that can corroborate or contradict witness accounts. The Amazon Echo device played a pivotal evidentiary role in a 2017 Arkansas murder trial, where investigators sought voice recordings stored in the cloud [30]. IoT forensics faces unique challenges: devices typically have limited storage (evidence may be transmitted to cloud services rather than stored locally), non-standard operating systems and file formats, and limited vendor documentation. The field requires development of specialized acquisition and analysis methodologies.

D. Automated Forensic Pipelines and Triage

The forensic triage paradigm — rapidly processing acquired data through automated analysis to identify high-value evidence before committing investigator resources to full examination — is becoming increasingly important. Purpose-built triage platforms can process a device's accessible data in the field, generating prioritized reports that guide subsequent investigation. This approach significantly reduces time-to-evidence in time-sensitive investigations and enables better allocation of investigator resources across multiple cases [31]. The development of standardized digital forensic ontologies and evidence taxonomies enables interoperability between different triage and analysis platforms

IX. CONCLUSION

This paper has presented a comprehensive examination of digital forensics as applied to cybercrime investigations, spanning the historical evolution of the discipline, the systematic investigation process model, empirical cybercrime trends, forensic tool evaluation, major challenges, the governing legal framework, and emerging research frontiers. Several key conclusions emerge from this analysis.

First, digital forensics has matured significantly from its improvised origins into a structured scientific discipline supported by international standards, validated tools, and established legal frameworks. The development of systematic process models and cryptographic integrity verification mechanisms has substantially strengthened the admissibility and reliability of digital evidence.

Second, the escalating scale and sophistication of cybercrime — illustrated by the 587% increase in global costs from 2018 to 2023 — demands commensurate advancement in forensic capabilities. The discipline must continuously adapt to counter evolving attacker techniques including fileless malware, encrypted communications, and sophisticated anti-forensics tools.

Third, the technical challenges of digital forensics — encryption barriers, massive data volumes, cloud environments, and jurisdictional complexity — can only be adequately addressed through a combination of technological innovation, international legal harmonization, and enhanced cross-border law enforcement cooperation.

Fourth, emerging technologies including artificial intelligence, blockchain analytics, and IoT forensics represent significant opportunities to enhance investigative capabilities, while simultaneously introducing new challenges around explainability, standardization, and legal admissibility.

The authors recommend that future research focus on developing AI-assisted forensic methods that maintain full transparency for legal proceedings, establishing internationally harmonized standards for cloud evidence preservation and production, advancing privacy-preserving forensic techniques that minimize collateral intrusion, and creating specialized frameworks for IoT and emerging technology forensics. As digital technology continues to permeate every dimension of human activity, the importance of rigorous, scientifically grounded digital forensics will only continue to grow.

REFERENCES

[1] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), "Internet Crime Report 2023," FBI, Washington, D.C., USA, 2024.

[2] Cybersecurity Ventures, "Cybercrime to Cost the World 10.5 trillion Annually By 2025," Cybersecurity Ventures, Sausalito, CA, USA, 2020.

[3] S. L. Garfinkel, "Digital forensics research: The next 10 years," Digital Investigation, vol. 7, pp. S64–S73, Aug. 2010, doi: 10.1016/j.diin.2010.05.009.

[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. Waltham, MA, USA: Academic Press, 2011.

[5] T. Shimomura and J. Markoff, Takedown: The Pursuit and Capture of Kevin Mitnick. New York, NY, USA: Hyperion, 1996.

[6] National Institute of Standards and Technology (NIST), "Computer Forensics Tool Testing (CFTT) Program," NIST Special Publication 800-101 Rev. 1, 2014.

[7] Gartner Inc., "Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019," Gartner Press Release, Sept. 2018.

[8] B. Carrier and E. H. Spafford, "Getting Physical with the Digital Investigation Process," International Journal of Digital Evidence, vol. 2, no. 2, 2003.

[9] M. Pollitt, "An Ad Hoc Review of Digital Forensic Models," in Proc. 2nd Int. Workshop Systematic Approaches to Digital Forensic Engineering, Bellvue, WA, USA, 2007, pp. 43–54.

[10] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," NIST Special Publication 800-86, 2006.

[11] A. Yasinsac et al., "Computer Forensics Education," IEEE Security & Privacy, vol. 1, no. 4, pp. 15–23, Jul.–Aug. 2003, doi: 10.1109/MSECP.2003.1219053.

[12] N. Beebe and J. Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," Digital Investigation, vol. 2, no. 2, pp. 147–167, 2005.

[13] P. Stephenson, "A Comprehensive Approach to Digital Incident Investigation," Information Security Technical Report, vol. 8, no. 2, pp. 42–54, 2003.

[14] IBM Security, "Cost of a Data Breach Report 2023," IBM Corporation, Armonk, NY, USA, 2023.

[15] Cybersecurity and Infrastructure Security Agency (CISA), "Colonial Pipeline Cybersecurity Attack," CISA Alert AA21-131A, 2021.

[16] B. Carrier, "Defining Digital Forensic Examination and Analysis Tools Using Abstraction Layers," International Journal of Digital Evidence, vol. 1, no. 4, 2003.

[17] A. Ligh, A. Case, J. Levy, and A. Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory. Indianapolis, IN, USA: Wiley, 2014.

[18] I. Baggili and F. Breitinger, "Data Sources and Proposed Forensic Analysis Approach for Wearable Devices," in Proc. 10th Int. Conf. Availability, Reliability and Security (ARES), Toulouse, France, 2015.

[19] D. Quick and K.-K. R. Choo, "Impacts of Increasing Volume of Digital Forensic Data: A Survey and Future Research Challenges," Digital Investigation, vol. 11, no. 4, pp. 273–294, 2014.

[20] M. Rogers, "Anti-Forensics," in Handbook of Research on Computational Forensics, Digital Crime and Investigation, C. Li, Ed. Hershey, PA, USA: IGI Global, 2009.

[21] G. Berman and N. Bhuta, "Mutual Legal Assistance: The Solution for Cybercrime?" in Proc. Int. Conf. Cyber Law, 2017.

[22] E. Nakashima and A. Timberg, "FBI paid professional hackers one-time fee to crack San Bernardino iPhone," The Washington Post, Apr. 12, 2016.

[23] D. Quick and K.-K. R. Choo, "Forensic Collection of Cloud Storage Data: Does the Act of Collection Result in Changes to the Data or its Metadata?" Digital Investigation, vol. 10, no. 3, pp. 266–277, 2013.

[24] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

[25] Council of Europe, "Convention on Cybercrime," CETS No. 185, Budapest, Nov. 23, 2001.

[26] P. Turner, "Unification of Digital Evidence from Disparate Sources (Digital Evidence Bags)," Digital Investigation, vol. 2, no. 3, pp. 223–228, 2005.

[27] International Association of Computer Investigative Specialists (IACIS), "IACIS Code of Ethics," IACIS, 2022. [Online]. Available: https://www.iacis.com/about/code-of-ethics

[28] A. Barmpatsalou, D. Damopoulos, G. Kambourakis, and V. Katos, "A Critical Review of 7 Years of Mobile Device Forensics," Digital Investigation, vol. 10, no. 4, pp. 323–349, 2013.

[29] S. Meiklejohn et al., "A Fistful of Bitcoins: Characterizing Payments Among Men with No Names," in Proc. ACM SIGCOMM Conf. Internet Measurement, Barcelona, Spain, 2013.

[30] J. Bates, "Smart Home Device Forensics — Who Else Is Listening?" in Proc. 17th European Conf. Cyber Warfare and Security (ECCWS), Oslo, Norway, 2018.

[31] F. Cohen, "Two Models of Digital Forensic Examination," in Proc. 4th Int. Workshop Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 2009.