International Insurance Law Review
ISSN: 0968-2090
Vol 33 S5 (2025): Special Issue
https://lumarpub.com/iilr

Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges

[1*]Dr. C Murugamani, [2]Bhuvan Unhelkar, [3]Dr. Siva Shankar S
[1*]Professor, Department of Computer Science and Engineering, GRT Institute of Engineering and Technology, Tiruttani, INDIA
[2]Professor, Muma College of Business University of South Florida 8350 N. Tamiami Trail Sarasota, Florida. USA.
[3]Professor & Head, IPR Department of Computer Science and Engineering, KG Reddy College of Engineering and Technology, RR district, Telangana, INDIA
Email: [1*]murugamanija@gmail.com; [2]bunhelkar@usf.edu; [3]drsivashankars@gmail.com
ORCID: [1*]https://orcid.org/0009-0004-5361-6164
*Corresponding Author: Dr. C Murugamani

Abstract
The rapid proliferation of digital technologies has transformed the nature, scale, and complexity of cybercrime, making digital forensics a cornerstone of modern cybercrime investigations. Digital forensics involves the systematic identification, preservation, analysis, and presentation of digital evidence to support legal proceedings. However, investigators face significant legal and technical challenges that can undermine the effectiveness and admissibility of such evidence. This paper critically examines the dual dimensions of these challenges. On the legal front, issues such as jurisdictional conflicts, cross-border data access, privacy and data protection regulations, chain of custody, and the admissibility of electronic evidence pose persistent obstacles, particularly in cases involving cloud computing and transnational cybercrimes. From a technical perspective, the study highlights difficulties arising from encryption, anonymization technologies, anti-forensic techniques, massive data volumes, heterogeneous devices, and the rapid evolution of cyber tools and platforms. The paper further explores the gap between technological advancements and existing legal frameworks, emphasizing the need for harmonized laws, standardized forensic procedures, and continuous capacity building for investigators and judicial authorities. By synthesizing current practices, case law trends, and emerging technologies, this research underscores the necessity of an integrated legal-technical approach to digital forensics. The findings aim to contribute to policy development, forensic readiness, and the strengthening of cybercrime investigation mechanisms in an increasingly digitalized society.
Keywords: Digital Forensics, Cybercrime Investigation, Electronic Evidence, Legal Challenges, Technical Challenges

1. Introduction

The blistering development of digital technologies has changed the basic patterns of committing and investigating cybercrime, and the digital forensics has become one of the most important parts of the contemporary crime investigation. Digital forensics refers to the process of identification, collection, analysis, and presentation of digital evidence obtained out of the computing systems, networks, and digital devices. Nevertheless, the growing sophistication of the

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

cyber space has brought some doubts about the uniformity, dependability, and legal validity of forensic approaches among jurisdictions (Horsman, 2020). With the increasing scale and sophistication of the incidents of cybercrime, investigators must manage a wide range of types of digital evidence and provide methodological rigor and evidentiary integrity. The lack of standardized forensic methodology across all systems is also a problem that complicates this issue, especially when it comes to heterogeneous systems and technologies that develop rapidly (Horsman, 2021).

Ensuring the integrity and admissibility of evidence during a legal process is one of the most important elements of digital forensic investigation, which is facilitated by the need to maintain a sound chain of custody to guarantee evidence integrity. Any failure on the part of evidence handling may render the validity of forensic results deceptive and render the result of the judicial system feeble. In order to mitigate these problems, decentralized and highly resistant evidence management methods have been suggested, including blockchain-based chain of custody systems (Alruwaili, 2021). The independently verifiable electronic custody ledgers investigated in further research have facilitated transparency and traceability in the forensic lifecycle. The methods are designed to reduce the conflict of the integrity of evidence and create confidence between court personnel and crime investigators (Burri et al., 2020). With such improvements, it is difficult to put into practice in practice since the integration is complex and scalability is also an issue not to mention the legal uncertainty about the acceptability of new technologies in the courtrooms.

The heterogeneity of digital environments has made the field of forensic investigations very broad. Mobile devices are a significant source of digital evidence, but bring about a special set of problems of data volatility, encryption, and proprietary operating systems. The recent developments in the area of mobile device forensics demonstrate that evidence retrieval and validation become more challenging because of the introduction of more effective security controls and privacy safeguards (Barmpatsalou et al., 2018). Other issues occur during the analysis of location-based evidence based on mobile devices where their contextual interpretation and methodological transparency is necessary to prevent falsification of forensic evidence (Casey et al., 2020). The mobile forensics field keeps providing evidence of research gaps based on the reliability of tools, the completeness of data, and the skills of the investigator (Chernyshev et al., 2017).

In addition to the conventional computing systems, new forensic challenges have been introduced by cloud computing environments and Internet of Things (IoT) environments. Cloud evidence is frequently located in distributed systems, which brings up the issues of jurisdiction, data ownership, and control. Critical analysis of cloud forensic investigations reveals that there are still unresolved problems with the data acquisition, evidence preservation, and legal compliance (Alshabibi et al., 2024). On the same note, IoT systems produce vast amounts of heterogeneous data with minimal forensic preparedness, which hinders the process of correlation and interpretation of evidence. The insecurity and forensic issues with the IoT systems indicate the necessity of specific investigational models that can address limited devices and decentralized information streams (Conti et al., 2018).

Advanced methods of digital forensics have been adopted because of the ever growing complexity of cybercrime. The live forensic methodology has been tested regarding the ransomware mitigation system and has shown potential advantages as well as the risks associated with its implementation in terms of system integrity and contamination of evidence (Davies et al., 2020).

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

To overcome the challenge of investigative complexity, the structured framework has been offered to systematically and reproducibly review and investigate cyberattacks (Dimitriadis et al., 2020). Simultaneously, the development of artificial intelligence and machine learning methods is increasingly applied to forensic operations to improve the detection, classification, and decision-making procedures (Dunsin et al., 2024). Nevertheless, such techniques would raise questions concerning transparency, explainability, as well as, legal defendability, especially when automated outputs are used as evidence.

Anti-forensic methods that are used by cybercriminals to break through detection and interrupt forensic analysis are gaining popularity. Studies regarding anti-forensics emphasize the smart game of forensic players and opponents, exposing shortcomings of current investigation methods (Hasanabadi et al., 2020). Encryption also makes extraction of evidence more difficult particularly within mobile settings where there are secure data storing mechanisms which limit access to crucial artifacts. Recent advances in forensic data extraction of encrypted devices focus on finding a tradeoff between the requirements of an investigation and the legal and ethical limitations (Fukami et al., 2021). The increasing use of open-source forensic tools has led to a question of their admissibility and reliability in court. There are still concerns regarding validation, reproducibility, and expert interpretation in cases where these tools are applied to court cases (Ismail and Akram Zainol Ariffin, 2025).

This research aims to understand the technical and legal issues of digital forensics in the investigation of cybercrime using a structured network based evidence. This study would investigate the nature of attacks, the time variations, network variables, and vulnerability attribution and evaluate the purpose of these variables to forensic credibility and admissibility in the court of law. By being able to solve these issues, the study aims at influencing better forensic practice and decision-making in regards to computer-related crimes.

2. Methodology

2.1 Dataset Description

The present research has utilized the UNSW-NB15 Ground Truth (GT) dataset as the main one to study. The dataset includes 174,347 network traffic logs in CSV format and each record contains a network communication event connected to malicious activity. The data set contains twelve attributes that capture both temporal and network and attack specifics and thus provide an organized view of network forensic data (Moustafa and Slay, 2016). The major features found in the data set are the start and end time, source and destination IP address and ports, communication protocol, attack category and subcategory, attack name, and the references to known vulnerabilities in form of CVE identifiers. These features are evidence of processed network logs that are typically reviewed when investigating cybercrime, and are very similar to the kind of evidence that forensic investigators have access to once the traffic has been captured and analyzed in the first step.

2.2 Data Pre-processing

Preprocessing of the data was performed before the analysis so that the data quality and consistency of analysis would be maintained. Placeholder attributes that were not informative were determined and deleted to avoid possible analytical bias. The time values, that is, the start time and last time fields were initially stored as Unix epoch and converted to human readable

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

date time formats to enable easier temporal and chronological analysis. Records that had incomplete or missing values in key fields like protocol or network addresses were scrutinised closely and eliminated where required in order to preserve the integrity of the analysis. Attributes that were categorical (such as the types of attacks, subtypes and communications protocols) were coded consistently to allow them to be subjected to statistical analyses, and still maintain a semantic meaning.

2.3 Forensic Feature Selection

The feature selection was also informed by the goals of a digital forensic inquiry and emphasized features that had direct evidentiary importance. Temporal indicators that included the start and end time were chosen to aid the reconstruction of attack timelines and correlation of events. To achieve the goal of communication patterns and attacker behavior analysis, network indicators, including source and destination IP addresses, ports, and protocol types, were selected. Attack attribution indicators such as attack category, subcategory, and descriptive attack names were added to allow making the classification and contextual understanding of the malicious activities possible. Also, the vulnerability reference in the form of CVE identifiers were chosen, which will facilitate legal traceability and enhance the connection between the observed attacks and the known software vulnerabilities.

2.4 Analytical Approach

The objectives of the digital forensic investigation influenced feature selection and were limited to attributes with direct evidentiary value. Temporal indicators that included the start and end time were chosen to aid the reconstruction of attack timelines and correlation of events. To achieve the goal of communication patterns and attacker behavior analysis, network indicators, including source and destination IP addresses, ports, and protocol types, were selected. Attack attribution indicators such as attack category, subcategory, and descriptive attack names were added to allow making the classification and contextual understanding of the malicious activities possible. Also, the vulnerability reference in the form of CVE identifiers were chosen, which will facilitate legal traceability and enhance the connection between the observed attacks and the known software vulnerabilities.

2.5 Technical Challenges Assessment

A further analysis of the dataset was conducted to determine technical issues of network-based digital forensic investigations. Lack of data about the payload of the packets prevents in-depth inspection of the content and only analysis of metadata evidence. Attribution dependency on network level properties creates confusion in attributing attacks, especially when several kinds of attacks have similar communication properties. The fact that the features overlap between the categories of attacks and the use of labeled evidence instead of raw traffic data makes the issue of proper forensicc interpretation even more difficult. These constraints are based on the real-life problems of forensic practitioners since investigators may be forced to make conclusions based on unfinished or pre-processed evidence due to time and financial constraints.

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

2.6 Legal and Evidentiary Considerations

Legally, the dataset allows one to analyze the admissibility and reliability of network logs as digital evidence. The organized format of the information reflects the way digital evidence is normally presented in legal cases, which makes it possible to evaluate its value as evidence. Although CVE references improve traceability and facilitate assigning a vulnerability to an established list, usage of processed logs instead of unprocessed traffic brings up the issue of evidence completeness and integrity. The findings add to the difficulties in proving intent and cause when using network metadata alone and emphasize that establishing high standards of legal admissibility of digital evidence is difficult in the absence of the chain-of-custody information on a comprehensive basis.

2.7 Ethical Considerations

UNSW-NB15 Ground Truth data is anonymized publicly available data that does not have any personally identifiable information. All evaluations that were undertaken in this work were carried out with the sole purpose of academic research. The research ethics were upheld throughout the research and the dataset was used responsibly and in accordance with the acceptable research ethics code of conduct.

3.Results

3.1 Dataset Overview

It analysed 174, 347 network traffic records obtained out of the UNSW-NB15 Ground Truth dataset. The records are processed network communications events that are related to malicious activity seen in controlled experimental conditions. The data sample has represented a wide diversity of cybercrime tendencies to the various types of attacks, temporal, and vulnerability sources, which offers a true foundation of network-based digital forensic study. Table 1 above has already outlined the dataset attributes and their respective forensic relevance. Such contextual details define the scope of evidence of the data and facilitate the interpretation of the findings given in this section.

Table 1. Dataset Attribute Description

Attribute	Description	Forensic Relevance
Start time	Unix timestamp indicating when the attack activity began	Enables forensic timeline reconstruction and temporal correlation of attack events
Last time	Unix timestamp indicating when the attack activity ended	Supports determination of attack duration and persistence
Attack category	High-level classification of the cyberattack (e.g., Exploits, DoS, Reconnaissance)	Facilitates attack type identification and high-level forensic categorization
Attack subcategory	Detailed classification specifying the attack technique	Assists in fine-grained forensic analysis and attack attribution
Protocol	Network protocol used during the attack (e.g., TCP, UDP)	Essential for protocol-specific forensic investigation and traffic interpretation
Source IP	IP address of the attack origin	Used for attacker tracing, correlation, and source analysis

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

Source Port	Network port used by the source system	Supports traffic pattern analysis and behavioral profiling
Destination IP	Target system IP address	Helps identify victim systems and attack targets
Destination Port	Targeted service port on the destination system	Indicates attacker focus on specific services and potential vulnerabilities
Attack Name	Descriptive name of the attack or exploit	Facilitates understanding of attack behavior and forensic reporting
Attack Reference	Reference to known vulnerabilities (e.g., CVE identifiers)	Enhances legal traceability and strengthens evidentiary credibility
Placeholder column (.)	Non-informative placeholder field present in the original dataset	No forensic relevance; excluded during preprocessing

3.2 Distribution of Attack Categories

The distribution of categories of attack should be known to assess the representativeness and analytical constraints of the data. The prevalence of attacks themselves has a direct impact on the performance of the forensic detection, prioritization of investigations, as well as the validity of analytical decisions. The frequency of categories of attacks used in the data is depicted in Figure 1, which gives a pictorial summary of the proportion of each type of attack. The figure clearly shows that there is a very strong imbalance between attack categories with the large dominating category being the exploit-based attacks, the next category is fuzzers, denial-of-service attacks, and reconnaissance activities.

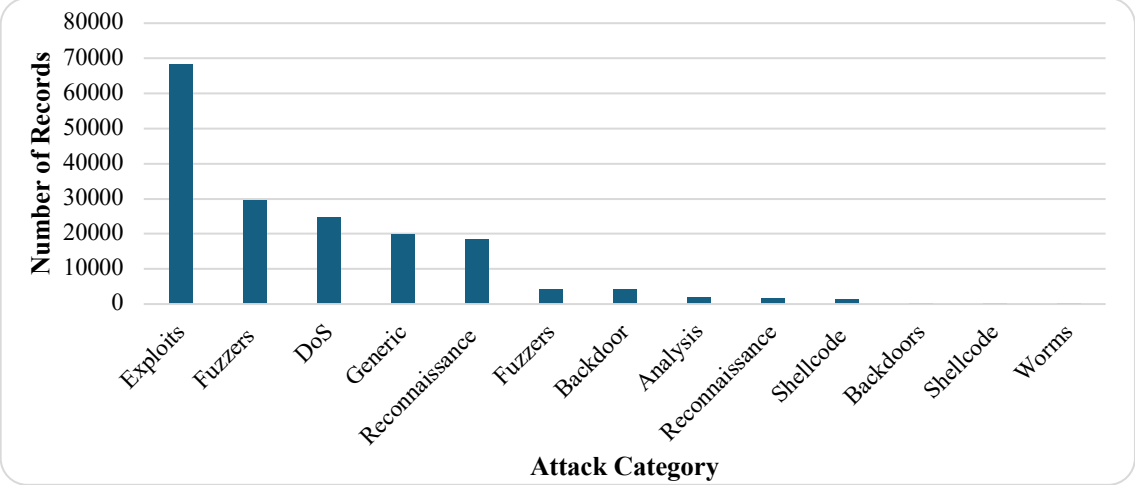

Figure 1: Distribution of Attack Categories

Although Figure 1 is a visual representation of the prevalence of attacks, there is need to quantify them numerically to enable accurate forensic interpretation. Table 2 thus summarizes the exact number of records and percentage contribution of each category of attack, but adds to the visual findings.

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

Table 2: Attack Category Statistics

Attack Category	Number of Records	Percentage (%)
Exploits	68,217	39.13
Fuzzers	29,503	16.92
DoS	24,582	14.10
Generic	19,860	11.39
Reconnaissance	18,392	10.55
Fuzzers (variant)	4,135	2.37
Backdoor	4,097	2.35
Analysis	1,881	1.08
Reconnaissance (variant)	1,744	1.00
Shellcode	1,288	0.74
Backdoors (variant)	256	0.15
Shellcode (variant)	223	0.13
Worms	169	0.10

The overall results of the interpretation of Figure 1 and Table 2 indicate that more sophisticated types of attacks like shellcode and worms are much less common than the activities of exploitation and reconnaissance. This imbalance poses a technical problem to digital forensic investigations because analytical methods that have been trained mostly on majority types of attacks might fail to perform so well with rare attacks that have high effects. These distorted distributions have implications on the generalizability of forensic models and the strategies used in an investigation.

3.3 Temporal Distribution of Cyber Attacks

Time of attacks on computers is a key aspect in reconstruction of the timeline during a forensic investigation and event correlation. It is also interesting to analyze the time the attacks are launched and the time distributions of the clusters of attacks to understand the behavior of attackers and the difficulty of the investigation. Figure 2 shows the temporal distribution of cyber attacks according to the start time of the attack. This number demonstrates the distribution of attack incidents during observation and identifies those periods during which malicious activity is concentrated.

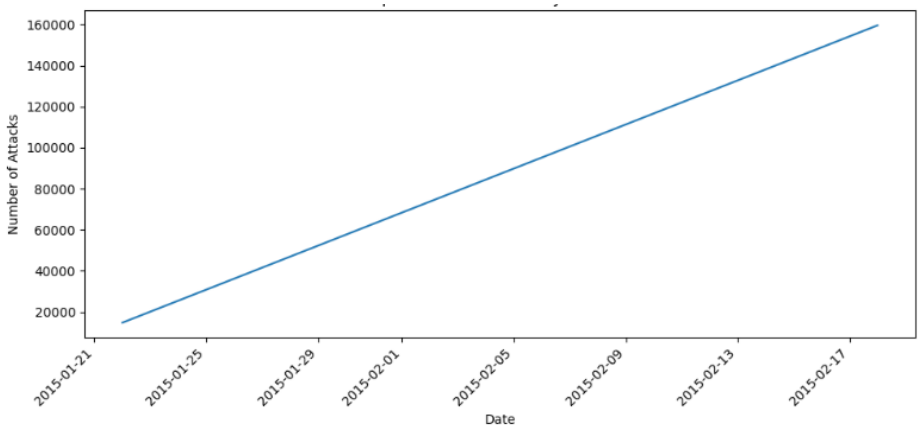

Figure 2: Temporal Distribution of Cyber Attacks

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

The figure 2 shows that there are several attacks that occur in close time windows and many of them are close to one another. This type of temporal concentration implies coordinated or repeated attack events and poses a problem to forensic analysts who need to isolate individual attack events. Interrupted attacks also make it complicated to reconstruct the timeline, especially when an environment has a long term malicious activity.

3.4 Network Evidence Patterns

Network level indicators (e.g. destination ports) bring useful forensic data on both the targeting behavior by the attacker and service level exposure. The study of these indicators can assist investigators to prioritize evidence and determine risk to critical services. The ports that are most often targeted to are shown in Figure 3 that demonstrates the attention paid by the attackers to commonly exposed network services.

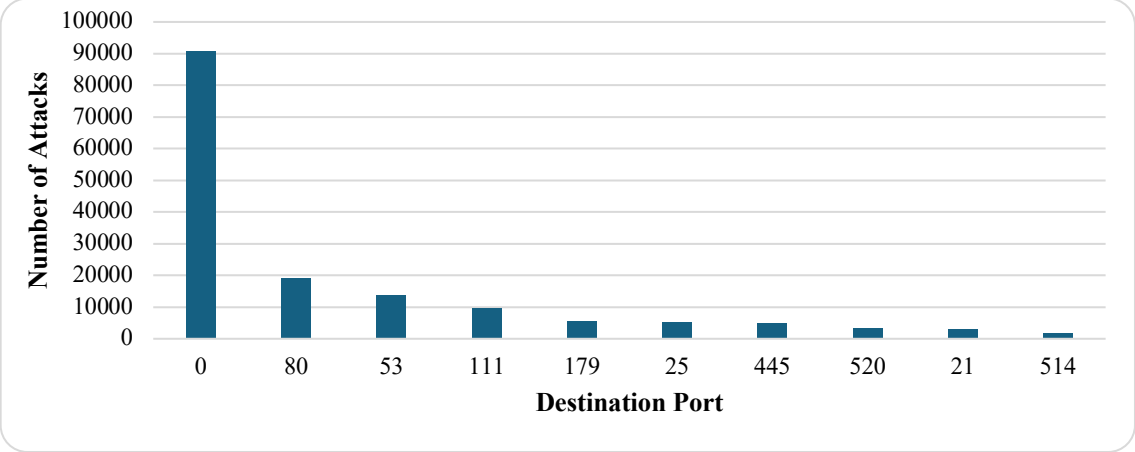

Figure 3: Top Targeted Destination Ports

As illustrated in Figure 3, the data indicates that there is a high concentration of attacks to popular service ports like HTTP, DNS, email and file-sharing services. This trend indicates the preference of the attackers on the services that are extensively deployed and can be accessed externally. Forensically, this concentration facilitates the prioritization of evidence, however, it also complicates the process of attribution as innocent and malicious traffic can have similar network features.

3.5 Attack Attribution and Vulnerability Mapping

Profiling malicious behavior based on known software vulnerabilities is frequently used to successfully attribute the origin of an attack. Vulnerability identifiers like CVE identifiers can be used to increase traceability and increase the evidential value of forensic results. Figure 4 shows the correlation between the number of attacks and the number of vulnerability references, with a comparison of attacks in which there is a specific vulnerability reference to those in which there is no explicit vulnerability reference.

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

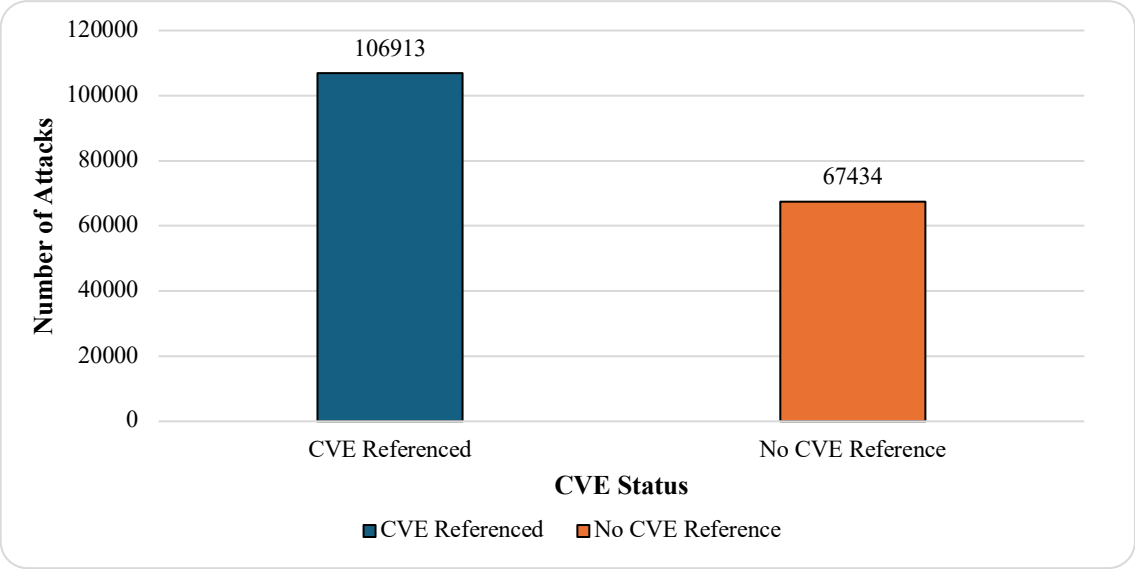

Figure 4: Attack-to-CVE Mapping Frequency

Figure 4 also shows that although a large number of attacks are associated with known vulnerabilities, a significant percentage of them are attributed to CVE without explicit reference to the latter. Besides, various names of attacks can be mapped to the same CVE ID, which creates a degree of ambiguity in the attack classification. These loopholes make it difficult to trace and difficult to provide legal protection because unfinished vulnerability mapping can undermine the credibility of expert opinions and evidence presentations in court.

3.6 Key Findings

All in all, the findings indicate that the attacks were mostly exploit-based, reconnaissance-based, there was a significant temporal concentration of malicious action, focused attacks on common network services, and a partial use of vulnerability reference in attributing the attacks. Collectively, these results point to technical and legal issues in digital forensic investigation of the network, such as the uncertainties of the evidentiary nature, attribution uncertainty, and the concerns about the admissibility and reliability of the processed network logs.

4. Discussion

Digital evidence integrity and provenance is one of the critical issues in cybercrime investigations. Since it is easy to manipulate digital artifacts, investigators have to prove that evidence has not been modified during the forensic lifecycle. Provenance and timestamping systems on blockchains have also been suggested to enhance the evidentiary trust through ensuring that a record of evidence handling processes is immutable (Jaquet-Chiffelle et al., 2020). These types of mechanisms provide greater transparency but bring about operational complexity that could not be easily adopted in a law enforcement setting. Although there is an assurance of tamperproof ledger, compatibility with current forensics, as well as legal frameworks is yet to be achieved. The investigators have to choose between the technical advantages of immutable provenance tracking and the practical facts of scalability, system interoperability, and court admissibility.

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

The digital forensic scene has changed greatly with migration of data and services to cloud infrastructures. Cloud environments present legal issues with regard to jurisdiction, data sovereignty and authority of service providers to manage or dispose of information. Such issues make it hard to obtain evidence and cast doubt on the legality of access and preservation requirements (Karagiannis and Vergidis, 2021). More complexity is given by the distributed nature of the cloud system where evidence can cut across geographical boundaries. The presence of old problems in cloud forensics, including poor visibility, absent standardized acquisition tools, and third-party cooperation, still makes it difficult to achieve reliable investigations (Simou et al., 2016). All these undermine the certainty of forensics and heighten the risk of litigation during a prosecution.

Mobile devices have continued to play a major role in digital evidence but the forensic analysis of these devices has posed recurrent technical issues. The Android devices in particular, are fragmented in terms of hardware, operating systems, and security settings and this makes it difficult to identify and manage evidence. To manage the possible evidence on Android systems properly, organized procedures are needed to make the process complete and forensically sound (Kim and Lee, 2020). The growing access of encryption and secure enclaves on mobile relates to access to critical artifacts even more. These constraints highlight the importance of adaptive forensic methods which are cognizant of the legal limits and at the same time are effective in the investigation.

The Internet of Things has grown the digital forensics to be diverse when compared to the traditional systems. IoTs have high rates of heterogeneous data with little forensic preparedness, and evidence correlation and interpretation are especially difficult. The comparative analysis of IoT forensic models indicates a lack of consistency in scopes, ability to manage data, and the quality of evidence (Mahmood et al., 2024). Limited resources on the device, unstable data storage and proprietary communication protocols further add to these difficulties. With the ongoing presence of IoT adoption, lack of a common standard in forensics is a great threat to technical accuracy as well as legal admissibility.

The issue of reliability is a central issue in digital forensic practice, especially in cases related to law enforcement. There are still systematic technical and procedural issues with digital forensic investigations, especially when it comes to law enforcement (Vincze, 2016). Empirical evaluations of forensic investigations point at inconsistency in the results of investigations owing to dissimilarities in instruments and expertise, as well as compliance with the procedures (Stoykova et al., 2022). This kind of variation erodes the trust of forensic conclusions and creates doubts in uniformity among cases. The erosion of trust in digital forensic evidence is also compounded by the growing sophistication of the current systems and the use of automated or semi-automated devices. The reliability issues need to be solves through systematic validation of forensic methods and one should be continuously trained as a professional to establish methodological rigor.

Digital forensic investigations have been streamlined and made to be efficient and scalable by the introduction of automation and machine learning methods. There are advanced structures based on the use of predictive analytics that are intended to simplify the process of evidence detection without compromising the privacy (Verma et al., 2019). Although these approaches have a great potential, there are also the risks of transparency, explainability, and bias. It is still unclear that machine learning outputs can be legally accepted as a piece of forensic evidence, especially when

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

the process they are made by is not transparent. To deliver credibility in evidence, investigators should make sure that automated tools are used to supplement and not to substitute expert judgment.

Forensic analysis through the network is very essential in the detection and investigation of cybercrime. Analysis of network intrusion data has also indicated that statistically representative and well-labeled data are essential in the evaluation of network intrusions (Moustafa and Slay, 2016). There is also a tradeoff between forensic granularity and reliance on processed network logs instead of raw traffic because such logs will not provide the contextual information required to make attribution. Moreover, network evidence does not always have clear signs of intent and it is not very easy to demonstrate causality in court. These shortcomings articulate the necessity of careful application of network-based discoveries in courts.

Zero trust digital forensics represents a new paradigm that suggests reevaluating the common beliefs in the trustworthiness of a system. Zero trust solutions can enhance the resilience of forensic services in sophisticated settings because they assume that all elements can be compromised (Neale et al., 2022). Although this is conceptually attractive, there is a need to make significant policy and investment adjustments in investigative infrastructure. Globally, the review of digital evidence practices supports the existence of unequal capacities in forensics and legal standards of practices across jurisdictions (Reedy, 2023). These differences make cross-border investigations more difficult and emphasize that international collaboration and harmonization should take place.

Financial technologies have presented new types of digital evidence that relate to cryptocurrencies, digital payment system, and blockchain-based transactions. Financial cybercrime needs to be investigated with the help of highly specific forensic skills that would be able to comprehend complicated records of transactions and decentralized systems (Nikkel, 2020). These areas further widen the scope of the boundary between technical analysis and interpretation of the law. The results presented in the section reveal that digital forensic investigation requires better standardization, transparency, and more collaboration with other disciplines. To make digital forensics more significant in the investigation of cybercrimes, it is important to mitigate technical constraints, improve the quality of evidence, and harmonize forensic procedures with legal standards. Further work should be done at creating dynamic systems that would reconcile technological advancement with legal strength and accountability.

5. Conclusion

The analysis of structured network-based forensic evidence in this study explored the technical and legal issues related to digital forensics used in investigating cybercrimes. The study investigated the distribution of attacks, their temporal behavior, the patterns of evidence of networks, and attributing vulnerabilities to attacks to evaluate their effects on forensic reliability and admissibility in court. The results indicated that the activities of cybercrime are predominantly represented by attack types- exploit and reconnaissance, highly clustered on a time framework, and are often directed to the network services which have become commonplace. These attributes make it difficult to reconstruct the timeline of the forensic activity, attribute attacks, and interpret evidences. The analysis also indicated the shortcomings of network based forensic datasets such as use of processed logs, lack of payload level evidence and incomplete vulnerability information. These restrictions are a challenge in creating

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

evidentiary completeness, traceability and certainty of the law in judicial procedures. In spite of these limitations, structured network evidence is an important element of a cybercrime investigation with expert interpretation and supporting analysis. On the whole, this study shows that better forensic methodologies should be developed to ensure that the technical rigor is complemented with the law. Improving the evidence provenance, improving the reliability of the dataset, and incorporating the multidisciplinary focus are the keys to the further development of digital forensic practice and its efficiency to cope with the further sophisticated cybercrime-related threats.

References

Alruwaili, F. F. (2021). Custodyblock: A distributed chain of custody evidence framework. *Information*, *12*(2), 88.

Alshabibi, M. M., Bu dookhi, A. K., & Hafizur Rahman, M. M. (2024). Forensic investigation, challenges, and issues of Cloud Data: A systematic literature review. *Computers*, *13*(8), 213.

Barmpatsalou, K., Cruz, T., Monteiro, E., & Simoes, P. (2018). Current and future trends in mobile device forensics: A survey. *ACM Computing Surveys (CSUR)*, *51*(3), 1-31.

Burri, X., Casey, E., Bolle, T., & Jaquet-Chiffelle, D. O. (2020). Chronological independently verifiable electronic chain of custody ledger using blockchain technology. *Forensic Science International: Digital Investigation*, *33*, 300976.

Casey, E., Jaquet-Chiffelle, D. O., Spichiger, H., Ryser, E., & Souvignet, T. (2020). Structuring the evaluation of location-related mobile device evidence. *Forensic Science International: Digital Investigation*, *32*, 300928.

Chernyshev, M., Zeadally, S., Baig, Z., & Woodward, A. (2017). Mobile forensics: advances, challenges, and research opportunities. *IEEE Security & Privacy*, *15*(6), 42-51.

Conti, M., Dehghantanha, A., Franke, K., & Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. *Future Generation Computer Systems*, *78*, 544-546.

Davies, S. R., Macfarlane, R., & Buchanan, W. J. (2020). Evaluation of live forensic techniques in ransomware attack mitigation. *Forensic Science International: Digital Investigation*, *33*, 300979.

Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I-Digital forensics framework for reviewing and investigating cyber attacks. *Array*, *5*, 100015.

Dunsin, D., Ghanem, M. C., Ouazzane, K., & Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, *48*, 301675.

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. *Forensic Science International: Digital Investigation*, *38*, 301169.

Hasanabadi, S. S., Lashkari, A. H., & Ghorbani, A. A. (2020). A survey and research challenges of anti-forensics: Evaluation of game-theoretic models in simulation of forensic agents' behaviour. *Forensic Science International: Digital Investigation*, *35*, 301024.

Horsman, G. (2020). Opinion: Does the field of digital forensics have a consistency problem?. *Forensic Science International: Digital Investigation*, *33*, 300970.

Horsman, G. (2021). Standardizing digital forensic examination procedures: A look at Windows 10 in cases involving images depicting child sexual abuse. *Wiley Interdisciplinary Reviews: Forensic Science*, *3*(6), e1417.

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084

Ismail, I., & Akram Zainol Ariffin, K. (2025). The admissibility of digital evidence from open-source forensic tools: Development of a framework for legal acceptance. *PLoS One*, *20*(9), e0331683.

Jaquet-Chiffelle, D. O., Casey, E., & Bourquenoud, J. (2020). Tamperproof timestamped provenance ledger using blockchain technology. *Forensic Science International: Digital Investigation*, *33*, 300977.

Karagiannis, C., & Vergidis, K. (2021). Digital evidence and cloud forensics: contemporary legal challenges and the power of disposal. *Information*, *12*(5), 181.

Kim, D., & Lee, S. (2020). Study of identifying and managing the potential evidence for effective Android forensics. *Forensic Science International: Digital Investigation*, *33*, 200897.

Mahmood, H., Arshad, M., Ahmed, I., Fatima, S., & ur Rehman, H. (2024). Comparative study of IoT forensic frameworks. *Forensic Science International: Digital Investigation*, *49*, 301748.

Moustafa, N., & Slay, J. (2016). The evaluation of network anomaly detection systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective, 25*(1–3), 18–31.

Neale, C., Kennedy, I., Price, B., Yu, Y., & Nuseibeh, B. (2022). The case for zero trust digital forensics. *Forensic Science International: Digital Investigation*, *40*, 301352.

Nikkel, B. (2020). Fintech forensics: Criminal investigation and digital evidence in financial technologies. *Forensic Science International: Digital Investigation*, *33*, 200908.

Reedy, P. (2023). Interpol review of digital evidence for 2019–2022. *Forensic Science International: Synergy*, *6*, 100313.

Simou, S., Kalloniatis, C., Gritzalis, S., & Mouratidis, H. (2016). A survey on cloud forensics challenges and solutions. *Security and Communication Networks*, *9*(18), 6285-6314.

Stoykova, R., Andersen, S., Franke, K., & Axelsson, S. (2022). Reliability assessment of digital forensic investigations in the Norwegian police. *Forensic Science International: Digital Investigation*, *40*, 301351.

Verma, R., Govindaraj Dr, J., Chhabra, S., & Gupta, G. (2019). Df 2.0: An automated, privacy preserving, and efficient digital forensic framework that leverages machine learning for evidence prediction and privacy evaluation. *Journal of Digital Forensics, Security and Law*, *14*(2), 3.

Vincze, E. A. (2016). Challenges in digital forensics. *Police Practice and Research*, *17*(2), 183-194.

Citation: C. Murugamani; Unhelkar, B. & Shankar S, S. (2025). Digital Forensics in Cybercrime Investigations: Legal and Technical Challenges. *International Insurance Law Review*, 33 (S5), 1072-1084