Proceedings of the 3rd International Conference on Software Engineering and Machine Learning
DOI: 10.54254/2755-2721/151/2025.22847

Application of Digital Forensics in Cybercrime Investigations

Yitai Huang

Changchun University of Technology, Changchun, China
hyt811626@gamil.com

Abstract: As cybercrime continues to pose significant threats to individuals, businesses, and national security, digital forensics has become an important tool for investigating cybercrime. This article explores the application of digital forensics technology, with a focus on disk forensics, memory forensics, and network forensics. It provides an overview of common forensic techniques, including key forensic methods, their advantages, limitations, and real-world applications. This study emphasizes the latest advancements in forensic tools and technologies, including AI-driven automation and machine learning-based anomaly detection, highlighting their role in recovering digital evidence, identifying cybercrime activities, and supporting legal proceedings. However, despite these advancements, challenges such as encrypted data, anti-forensic techniques, and increasingly complex network threats were also discussed. These findings emphasize the necessity of standardized forensic protocols, the integration of AI-driven automation, and improved forensic methods to enhance investigation efficiency and ensure the integrity and reliability of digital evidence in the legal environment.

Keywords: Digital Forensics, Cybercrime Investigation, Disk Forensics, Memory Forensics, Network Forensics

1. Introduction

With the rapid development of information technology, cybercrime has become a major global challenge, posing threats to individuals, businesses, and national security. In this context, digital forensics has become an essential tool for identifying, analyzing, and mitigating cyber threats [1]. The global digital forensics market is projected to grow from USD 9.9 billion in 2023 to USD 18.2 billion by 2028 [2], reflecting the growing demand for advanced forensic solutions in combating cybercrime.

Currently, digital forensics is primarily used in law enforcement and criminal investigations, but its applications have expanded to corporate security, intellectual property protection, and fraud detection. In cybercrime investigations, digital forensics involves the collection, preservation, and analysis of electronic evidence to reconstruct criminal activities and support legal proceedings. Digital forensics encompasses various specialized techniques, including disk forensics [3], memory forensics [4],network forensics [5]and so on. These techniques rely on different types of forensic tools and methodologies to extract and analyze data from compromised systems. The approach used in digital forensics varies depending on the nature of the crime and the digital environment involved, by leveraging advanced forensic methods, investigators can trace cybercriminals, recover lost data, and ensure the integrity of digital evidence in court proceedings.

DOI: 10.54254/2755-2721/151/2025.22847

Accurately detecting digital evidence in cybercrime investigations is crucial for assessing the scope of criminal activity and developing effective response measures because researching digital forensics can help develop standardized protocols to ensure evidence integrity and compliance with legal frameworks while integrating AI and automation into digital forensics, investigators can improve efficiency, reduce investigation time, and enhance accuracy. Moreover, researching advanced forensic methods can aid in early threat detection, rapid response, and crime prevention, ultimately enhancing public safety and national security.

The aim of this study is to analyze the latest research on the application of digital forensics in cybercrime investigations, as there is a growing need for efficient, reliable, and legally sound methodologies to collect, analyze, and preserve digital evidence. Given the increasing complexity of cybercrimes and the evolving tactics used by cybercriminals, it is essential to develop faster, more automated, and accessible forensic techniques that can be effectively utilized by investigators, law enforcement agencies, and cybersecurity professionals. This research seeks to enhance the understanding of modern digital forensic approaches, improve forensic capabilities, and support the development of standardized procedures to strengthen cybercrime investigations and legal proceedings.

This review explores recent advancements in the development and application of digital forensics in cybercrime investigations, focusing on techniques used to analyze disk, memory, and network. A brief overview of digital forensic methods is provided, discussing their advantages and limitations. Subsequently, different forensic techniques are examined, including their working principles and improvements over time. Next, recent research from the past decade on digital forensic applications in cybercrime investigations is reviewed. The studies are analyzed in detail, emphasizing forensic tools, types of cybercrimes investigated, and key analytical parameters relevant to modern digital forensic practices.

2. Disk analysis-based forensic techniques

With the increasing reliance on digital storage devices, disk analysis-based forensic techniques have become crucial in digital investigations. These technologies are used to discover deleted files, analyze metadata, recover lost information, and reconstruct user activities. This paragraph outlines the key methods, applications, and challenges of disk analysis-based forensic techniques.

2.1. Disk analysis techniques

Disk forensic techniques involve various methods for acquiring, processing, and analyzing data stored on digital media. The most common techniques include: Disk imaging involves creating an exact copy of a storage device to preserve the original evidence. Tools such as FTK Imager and EnCase are widely used to acquire forensic images without modifying the original data [6].

Another important technique is data carving, which is used to recover fragmented or deleted files without relying on file system metadata. Techniques such as header-footer analysis and content-based reconstruction allow forensic analysts to extract hidden or lost files [7].

In addition to data acquisition and recovery, log analysis provides valuable forensic evidence. Investigators analyze event logs, security logs, and application logs to track unauthorized access, system modifications, and malware activities [8].

2.2. Advanced application of disk analysis-based forensic techniques

Law enforcement agencies utilize these methods to recover evidence related to cybercrimes, fraud, and illegal activities. Similarly, organizations conduct forensic investigations to detect data breaches, insider threats, and policy violations. Security teams employ disk forensics to analyze and mitigate

DOI: 10.54254/2755-2721/151/2025.22847

cyberattacks, malware infections, and unauthorized access. These applications highlight the importance of disk analysis in maintaining cybersecurity and supporting forensic investigations.

2.3. Challenges and limitations of disk forensic techniques

With the increasing adoption of cloud storage, traditional disk forensic techniques face significant challenges. Dykstra and Sherman examined forensic challenges in cloud storage environments, highlighting difficulties in acquiring, preserving, and verifying evidence due to multi-tenant storage and remote access issues [9].

In addition to cloud-related issues, digital forensic investigations must contend with evolving anti-forensic techniques. An article in Communications of the ACM discusses live forensic analysis risks, including anti-forensic techniques that attackers use to obscure evidence, requiring investigators to adapt their methodologies [10].

Disk forensics also has inherent limitations. Modern SSDs use garbage collection and TRIM commands, which can permanently erase deleted data, limiting forensic data recovery [11]. Furthermore, the increasing size of storage devices requires more time and computational resources for full disk analysis, posing practical challenges in forensic investigations [12].

3. Memory analysis-based forensic techniques

Cybercrime investigations have become increasingly complex as cybercriminals employ advanced techniques to evade detection. Traditional forensic methods that focus on disk analysis often fail to capture volatile evidence, which disappears when a system is powered off. Memory analysis has emerged as a crucial technique in retrieving real-time forensic data, helping investigators uncover malware, hidden processes, encryption keys, network connections, and user activity that may not be available through other forensic approaches. This paragraph provides an overview of common memory analysis methods, applications, and examines their strengths and limitations.

3.1. Memory analysis techniques

3.1.1. Detection of memory-related vulnerabilities

Memory-related vulnerabilities, such as buffer overflows and use-after-free errors, pose significant threats to software security. Traditional detection methods often underutilize flow information, leading to high false-positive rates. To address this, a flow-sensitive graph neural network (FS-GNN) based approach, MVD, has been proposed to detect such vulnerabilities. FS-GNN jointly embeds unstructured information and structured information to capture implicit vulnerability patterns. Evaluations on a dataset containing 4,353 real-world memory-related vulnerabilities demonstrated that MVD achieves better detection accuracy compared to state-of-the-art deep learning-based and static analysis-based approaches [13].

3.1.2. Static analysis for program characterization

Profiling application characteristics dynamically is time-consuming, while static analysis methods, though faster, can be less accurate. An LLVM-based probabilistic static analysis method has been introduced to predict different program characteristics and estimate the reuse distance profile by analyzing the LLVM IR file in constant time, regardless of program input size. This approach accurately predicts application characteristics compared to other LLVM-based dynamic code analysis tools [14].

DOI: 10.54254/2755-2721/151/2025.22847

3.2. Application of memory analysis-based forensic techniques in cybercrime investigations

Cybercriminals increasingly deploy fileless malware that resides entirely in memory, making it undetectable by traditional antivirus software. Memory forensics enables investigators to detect and extract malicious codes directly from system RAM. Memory analysis plays a key role in detecting credential dumping attacks, where cybercriminals extract passwords, authentication tokens, and encryption keys from a compromised system. Cybercriminals exploit banking systems by manipulating transactions using in-memory exploits. Memory forensics helps investigators track fraudulent activities that may not leave traces on disk. Cybercriminals leverage Tor networks and cryptocurrencies for illicit activities such as money laundering and drug trafficking. Memory analysis enables investigators to recover dark web browsing history, cryptocurrency wallets, and encrypted communications.

Additionally, recent advancements in hardware acceleration have enhanced the efficiency of memory forensics. For example, a proposed software tool utilizing CUDA-enabled GPU hardware demonstrated accelerated memory forensics, aiding in the detection of sophisticated malware that employs anti-forensic techniques. This approach underscores the potential of hardware acceleration in enhancing memory analysis capabilities [15].

3.3. Limitations of memory analysis techniques

Some memory analysis tools introduce additional system overhead, affecting application performance. For instance, complex analyses may significantly reduce program execution speed, making them unsuitable for real-time applications. In-depth memory analysis requires developers to have a deep understanding of low-level memory operations. The data analysis process can be complex and time-consuming, impacting development efficiency. Certain memory analysis tools are tailored for specific operating systems or programming languages, limiting their portability. For example, some tools may only be applicable to particular platforms and not others.

4. Network traffic analysis-based forensic techniques

Digital forensics involves the identification, collection, preservation, and analysis of electronic evidence. With the increasing complexity of cybercrimes, network traffic analysis has become an essential tool for forensic investigators. Network Traffic Analysis (NTA) is a crucial technique in digital forensics, aiding in cybercrime investigations, intrusion detection, and evidence collection. By analyzing network packets, logs, and communication patterns, investigators can trace malicious activities, reconstruct cyberattacks, and gather evidence for legal proceedings. This paragraph explores the role of NTA in forensic analysis, highlighting key techniques, related works, challenges, and future directions.

4.1. Network traffic analysis techniques

Network Traffic Analysis (NTA) employs various techniques to enhance the detection and understanding of cyberattacks. Deep Packet Inspection (DPI) involves examining the content of data packets beyond basic header information. This technique enables the identification of applications, services, and potential security threats, playing a crucial role in detecting malicious activities and enforcing network policies [16]. Additionally, Machine learning algorithms, including clustering and classification techniques, have been applied to NTA for anomaly detection and traffic classification. Deep learning models, such as Convolutional Neural Networks and Long Short-Term Memory networks LST, have shown promise in capturing complex patterns in encrypted traffic, enhancing predictive capabilities. For example, scalable Bayesian modeling has been employed for monitoring

DOI: 10.54254/2755-2721/151/2025.22847

and analyzing dynamic network flow data, providing interpretable inferences on traffic flow characteristics [17].

4.2. Advanced applications of network traffic analysis in digital forensics

4.2.1. Big data approaches in network traffic monitoring

A comprehensive survey examined the application of big data techniques in Network Traffic Monitoring and Analysis (NTMA). The study highlighted the challenges posed by the increasing complexity of internet services and traffic volumes, emphasizing the need for scalable NTMA applications. It cataloged previous work adopting big data approaches to manage massive sets of historical data for post-mortem analysis and discussed the integration of machine learning for NTMA [18].

4.2.2. Scalable bayesian modeling for dynamic network flow

Research on scalable Bayesian modeling has focused on monitoring and analyzing dynamic network flow data. This approach allows for real-time, scalable, and interpretable Bayesian inference, facilitating the adaptive characterization and quantification of network dynamics. The methodology has been applied to internet browser traffic flow through site-segments of an international news website, demonstrating its utility in analyzing streaming network count data [17].

4.2.3. Application of network traffic analysis-based forensic techniques

Packet capture tools like Wireshark and tcpdump allow forensic investigators to inspect network communications at a granular level. By analyzing packet headers and payloads, investigators can detect suspicious activity, such as unauthorized access, data exfiltration, or malware communication. Network logs from firewalls, intrusion detection systems (IDS), and SIEM platforms play a vital role in forensic investigations. Correlating logs across different devices helps reconstruct attack timelines and identify compromised systems. Machine learning-based network anomaly detection identifies deviations from normal traffic behavior, which may indicate cyber threats. Behavioral profiling of network entities helps forensic analysts detect stealthy attacks.

4.3. Limitations of network traffic analysis

The widespread adoption of encryption protocols presents significant challenges to NTA. Encrypted traffic renders payload data inaccessible, undermining the effectiveness of traditional inspection methods and necessitating the development of advanced analysis techniques capable of handling encrypted data; Modern networks generate massive amounts of traffic data, making real-time analysis computationally challenging. The sheer volume requires scalable solutions and efficient algorithms to process and analyze data without introducing significant delays; Adversaries employ sophisticated evasion techniques, such as traffic obfuscation, tunneling, and mimicking legitimate traffic patterns, to bypass NTA systems. These strategies complicate the detection of malicious activities, necessitating continuous adaptation of analysis methods.

5. Conclusion and prospect

Despite significant progress in digital forensics, several challenges remain. The increasing use of encryption, anti-forensic techniques, and cloud-based storage complicates evidence acquisition and analysis. Moreover, the growing volume of digital data and the rise of sophisticated cyberattacks demand more efficient, automated, and scalable forensic solutions. Future research should focus on

DOI: 10.54254/2755-2721/151/2025.22847

integrating artificial intelligence and machine learning into forensic analysis to enhance investigation speed and accuracy. Additionally, the development of standardized forensic protocols and international cooperation will be essential to improving cross-border cybercrime investigations.

Looking ahead, emerging technologies such as blockchain, quantum computing, and advanced AI-driven analytics could revolutionize digital forensics. Blockchain can enhance evidence integrity by providing immutable audit trails, while quantum computing could break traditional encryption, presenting both opportunities and challenges for forensic investigators. Furthermore, AI-driven threat detection and automation will play a critical role in proactively identifying cyber threats and reducing investigation time. As cybercriminal tactics continue to evolve, digital forensics must also advance, ensuring that forensic methodologies remain robust, legally admissible, and effective in combating cybercrime.

References

[1] *Årnes, André, ed. Digital forensics. John Wiley & Sons, 2017.*

[2] *Markets and Markets, Digital Forensics Market Size, Global Forecast, Growth Drivers, Opportunities 2028. Available online: Digital Forensics Market Share, Forecast, Trends | Growth Analysis [2030]*

[3] *Pandey, Bishwajeet, et al. "Efficient usage of web forensics, disk forensics and email forensics in successful investigation of cyber crime." International Journal of Information Technology 16.6 (2024): 3815-3824.*

[4] *Prottoy, Rafid Asrar. "Memory Forensics for Analyzing Malicious Activities." (2023).*

[5] *Patil, Rachana Y., and Satish R. Devane. "Network forensic investigation protocol to identify true origin of cyber crime." Journal of King Saud University-Computer and Information Sciences 34.5 (2022): 2031-2044.*

[6] *Carrier, Brian. File system forensic analysis. Addison-Wesley Professional, 2005.*

[7] *Richard III, Golden G., and Vassil Roussev. "Scalpel: a frugal, high performance file carver." DFRWS. 2005.*

[8] *Carvey, Harlan, and Cory Altheide. Digital forensics with open source tools. Elsevier, 2011.*

[9] *Dykstra, Josiah, and Alan T. Sherman. "Understanding issues in cloud forensics: two hypothetical case studies." (2011).*

[10] *Carrier, Brian D. "Risks of live digital forensic analysis." Communications of the ACM 49.2 (2006): 56-61.*

[11] *Jalil Hadi, Hassan, and Sheetal Harris. "SSD Forensic: Evidence Generation And Forensic Research On Solid State Drives Using Trim Analysis." arXiv e-prints (2023): arXiv-2307.*

[12] *Lillis, David, et al. "Current challenges and future research areas for digital forensic investigation." arXiv preprint arXiv:1604.03850 (2016).*

[13] *Cao, Sicong, et al. "MVD: memory-related vulnerability detection based on flow-sensitive graph neural networks." Proceedings of the 44th international conference on software engineering. 2022.*

[14] *Barai, Atanu, et al. "Llvm static analysis for program characterization and memory reuse profile estimation." Proceedings of the International Symposium on Memory Systems. 2023.*

[15] *Korkin, Igor, and Iwan Nesterow. "Acceleration of statistical detection of zero-day malware in the memory dump using CUDA-enabled GPU hardware." arXiv preprint arXiv:1606.04662 (2016).*

[16] *Bremler-Barr, Anat, et al. "Deep packet inspection as a service." Proceedings of the 10th ACM International on Conference on emerging Networking Experiments and Technologies. 2014.*

[17] *Chen, Xi, et al. "Scalable Bayesian modeling, monitoring, and analysis of dynamic network flow data." Journal of the American Statistical Association 113.522 (2018): 519-533.*

[18] *D'Alconzo, Alessandro, et al. "A survey on big data for network traffic monitoring and analysis." IEEE Transactions on Network and Service Management 16.3 (2019): 800-813.*