FORSEC: Forensic and Security Journal
Vol. 1, No. 1
ISSN: xxxx-xxxx
DOI: xxxx.forsec

Cloud and IoT Forensics for Strengthening Cybercrime Investigation: Acquisition Challenges and Analytical Frameworks

Malika Dienta Prakasiwi
Universitas Mercu Buana Yogyakarta, Yogyakarta, Indonesia

Article Info

Article history:

Received 09 02, 2025
Revised 09 05, 2025
Accepted 09 04, 2025

Keywords:

Blockchain;
Cloud Forensics;
Cybercrime Investigation;
Digital Evidence;
IoT Forensics.

ABSTRACT

With the rapid adoption of cloud services and Internet of Things (IoT) devices, digital forensics faces new challenges in acquiring and analyzing evidence stored across distributed and heterogeneous environments. This research presents a comparative study of forensic acquisition methods for cloud and IoT platforms, emphasizing both their potential and limitations in cybercrime investigations. Using case simulations involving Amazon Web Services (AWS), Google Cloud, and IoT-enabled smart home devices, the study evaluates logical, API-based, and memory dump acquisition strategies. Results indicate that API-driven cloud acquisition offers efficiency but faces jurisdictional restrictions, while IoT forensic acquisition remains hindered by proprietary protocols and volatile data. The paper also highlights the integration of artificial intelligence (AI) for anomaly detection, blockchain for evidence integrity, and semantic correlation frameworks to reconstruct multi-source timelines. Findings confirm that cloud and IoT forensics require hybrid technical and legal approaches to ensure evidence admissibility and investigative effectiveness.

Corresponding Author:

Malika Dienta Prakasiwi,
Fakultas Teknologi Informasi,
Universitas Mercu Buana Yogyakarta, Yogyakarta, Indonesia,
Email: 221210003@student.mercubuana-yogya.ac.id.

1 INTRODUCTION

The rapid digitization of society has led to widespread reliance on cloud services and Internet of Things (IoT) devices for communication, commerce, and critical infrastructure. Over 60% of organizations globally now rely on cloud storage for daily operations, according to IDC (2023) [1]. At the same time, the proliferation of IoT devices has accelerated, with more than 15 billion units deployed worldwide by 2024 [2]. This surge in adoption, while beneficial, significantly expands the attack surface available to cybercriminals.

Cloud services have been increasingly exploited for hosting phishing campaigns and distributing malware, making them attractive platforms for malicious actors [3]. Similarly, IoT devices such as smart cameras, wearable health trackers, and industrial sensors have been misused for botnet attacks and unauthorized surveillance [4]. Investigating such cases presents unique challenges, as forensic practitioners must deal with distributed environments, ephemeral data, and proprietary protocols that vary across vendors [5]. Legal admissibility further complicates the process since evidence stored across jurisdictions often requires Mutual Legal Assistance Treaties (MLATs**)** to access, which can slow investigations considerably [6]. Additionally, anti-forensic strategies, such as encrypted synchronization, firmware manipulation, and volatile memory wiping, increase the risk of critical evidence being lost during investigations [7]. These barriers demand adaptive forensic frameworks that combine technical, legal, and organizational readiness.

Against this backdrop, the core problem addressed in this research lies in the increasing difficulty of acquiring and analyzing digital evidence in cloud and IoT ecosystems. Unlike traditional computer forensics, where evidence is relatively stable and stored locally, cloud and IoT evidence is volatile, encrypted, and geographically distributed, often across multiple jurisdictions. As a result, reliance on a single acquisition method, such as logical extraction, frequently leads to incomplete or inconclusive findings. This problem is further compounded by legal and procedural limitations, as investigators must comply with both national legislation and international standards to ensure evidentiary admissibility.

To respond to this problem, the research is designed with several objectives. The technical objective is to evaluate multiple acquisition techniques—API-based, logical snapshotting, and network capture for cloud environments, as well as firmware dumping, memory extraction, and log collection for IoT devices—in terms of their recovery rates, acquisition times, and evidence coverage. Analytically, the study seeks to reconstruct user activity and malicious behavior by correlating diverse evidence sources, including cloud storage metadata, access logs, and IoT device telemetry. Practically, the research aims to identify recurring challenges from real-world case studies such as credential theft, IoT botnet attacks, and cross-border evidence handling, and to propose adaptive solutions involving hybrid acquisition strategies, AI-assisted forensic triage, and blockchain-based chain-of-custody mechanisms. Strategically, the research aspires to propose a forensic readiness model that can be applied in developing countries such as Indonesia, where gaps in technical infrastructure and legal harmonization still exist.

The significance of this research is multifold. Theoretically, it enriches digital forensic studies by comparing acquisition methods across heterogeneous environments and by combining experimental results with case-based analysis. Practically, it provides actionable insights for investigators and law enforcement agencies on how to maximize evidence recovery while maintaining procedural compliance. Legally, it emphasizes the importance of chain-of-custody safeguards to strengthen the admissibility of digital evidence in court. At the policy level, it underlines the urgency of implementing forensic readiness strategies through investment in laboratories, human resources, and international collaboration. Beyond its academic and institutional contributions, the research also benefits society at large by reducing cybercrime risks, safeguarding digital assets, and reinforcing public trust in digital services.

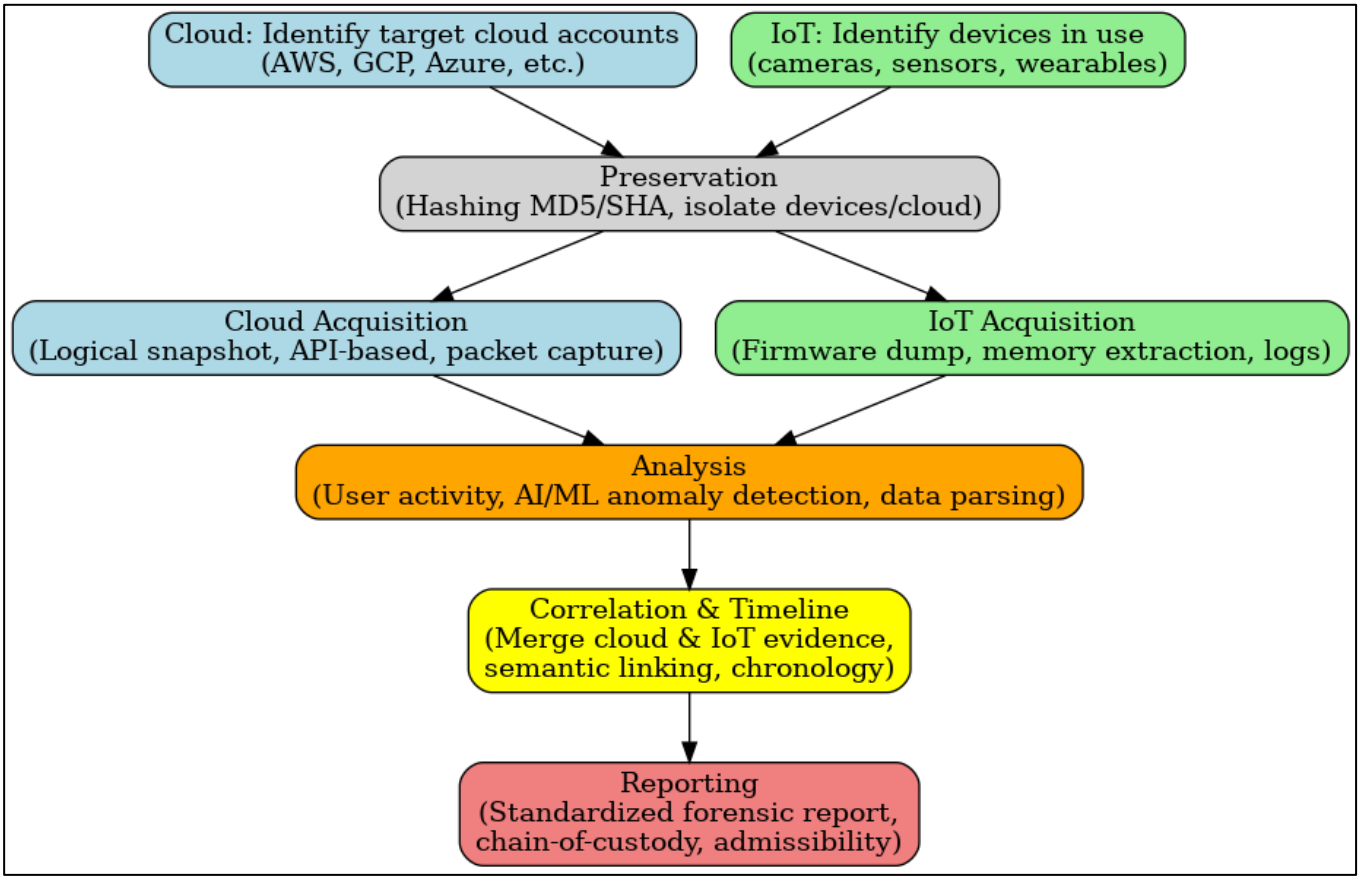

Figure 1. Workflow of Cloud and IoT Forensics

Figure 1 illustrates the workflow of cloud and IoT forensics, which follows the general structure of a forensic investigation but is adapted to address the unique challenges of distributed and heterogeneous environments. The process begins with evidence identification, where investigators determine the relevant cloud accounts (such as AWS, Google Cloud, or Microsoft Azure) and IoT devices (such as cameras, sensors, or wearables) that may contain potential evidence. Once identified, the next step is evidence preservation, which involves securing the devices or accounts and applying cryptographic hashing (MD5, SHA-1, SHA-256) to record their original state. For IoT devices, this may require isolating the device from the network to prevent further tampering, while for cloud evidence, credentials must be secured to ensure data cannot be altered remotely. The third stage, acquisition, involves extracting data using different methods. In cloud environments, investigators may use logical snapshots, API-based acquisition, or network packet captures, while in IoT contexts, methods include firmware dumping, volatile memory extraction, and device log collection. Each of these acquisition strategies has its own trade-offs in terms of completeness, speed, and reliability. Following acquisition, the analysis phase reconstructs user activity and attack behavior. This may involve correlating communication logs, cloud storage access, IoT telemetry, and application metadata. Increasingly, artificial intelligence and machine learning tools are used to automate anomaly detection and highlight patterns that may otherwise go unnoticed. The fifth stage is correlation and timeline reconstruction, where evidence from both cloud and IoT sources is integrated into a single chronological sequence. This step is crucial for establishing the cause-and-effect relationships between different events, such as a suspicious login on a cloud platform followed by an IoT device compromise.

Finally, the reporting phase generates standardized forensic reports in formats such as UFDR (Cellebrite), AXIOM case files, or CSV/HTML exports. Reports include verification details like hash values and chain-of-custody documentation to ensure admissibility in court. This final step ensures that the evidence is not only technically valid but also legally defensible.

In summary, Figure 1 highlights that cloud and IoT forensic workflows must integrate multiple acquisition and analysis techniques, converge evidence into coherent timelines, and maintain strict compliance with legal standards to ensure that findings can be trusted in judicial contexts.

2 RESEARCH METHOD

In conducting this study, a structured forensic methodology was followed, encompassing the phases of collection, preservation, acquisition, analysis, and reporting. During the acquisition stage, several specialized forensic tools were employed, each chosen for its particular strengths in handling cloud and IoT data.

One of the main tools was X-Ways Forensics, which is particularly effective for analyzing cloud disk images and virtual machine snapshots. This tool was utilized to examine cloud storage artifacts and system-level data captured from virtualized environments. In parallel, FTK Imager was applied to capture volatile memory from IoT devices. This capability is critical because IoT devices often operate with very limited local storage, making memory dumps one of the few reliable sources of evidence before data is overwritten.

For cloud-based acquisitions, Magnet AXIOM Cloud was employed to interact directly with service provider APIs, including Amazon Web Services (AWS) and Google Cloud. This tool enabled structured extraction of user files, logs, and metadata, while also supporting cloud authentication workflows to ensure that evidence was collected in a legally defensible manner. In the IoT domain, network analysis tools such as Wireshark and IoT Inspector were integrated to capture traffic between devices and their cloud services. These tools provided valuable insights into command-and-control communication, firmware updates, and anomalous traffic patterns that could indicate compromise.

To reinforce the integrity of evidence handling, a blockchain-based prototype ledger was also tested as part of the chain-of-custody process. Every stage of evidence handling—from initial acquisition to final reporting—was logged into this distributed ledger, ensuring transparency and immutability. Compared to conventional chain-of-custody documentation, this approach offered an additional safeguard against tampering or disputes in legal proceedings.

The evaluation process adopted in this research was comparative in nature. For cloud environments, three acquisition strategies were assessed: logical snapshotting, API-based extraction, and network packet capture. Each of these methods was tested against variables such as recovery percentage, acquisition speed, and completeness of data. Similarly, for IoT devices, three approaches were compared: firmware dumping, live memory extraction, and log acquisition. The aim was to determine not only the technical effectiveness of each method but also its practical feasibility in real-world investigative contexts.

The comparative results revealed clear trade-offs. API-based cloud acquisition provided the highest recovery rates but was heavily dependent on vendor cooperation and legal authorization. Logical snapshots were faster but often missed encrypted or hidden files. Network captures, while less effective in recovery, were still valuable for detecting anomalies in encrypted traffic flows. For IoT devices, memory extraction achieved the highest completeness of recovery, though it was extremely time-sensitive and required immediate action before power loss or data overwrite occurred. Firmware dumping allowed for more comprehensive access to system-level data but risked rendering the device inoperable, while log acquisition was simple but prone to manipulation and incompleteness.

By presenting these tools and comparative strategies in a single methodological framework, this study highlights that no single tool or method is sufficient. Instead, a hybrid approach that combines multiple acquisition methods, reinforced with modern verification mechanisms, provides the most reliable pathway for investigating cloud and IoT-based cybercrimes.

Table 1. Summary of Tools Used in Cloud and IoT Forensics

Tool / Approach	Primary Function	Strengths	Limitations
X-Ways Forensics	Cloud disk image and VM snapshot analysis	Lightweight, efficient at parsing file systems and disk structures	Limited cloud API integration; requires prior acquisition of disk images
FTK Imager	Memory capture from IoT devices	Reliable volatile memory acquisition; widely recognized in court	Volatility of data; requires immediate action before data is overwritten
Magnet AXIOM Cloud	Cloud API-based acquisition (AWS, GCP, etc.)	High recovery rate; structured logs and metadata; strong reporting tools	Dependent on vendor cooperation and authentication tokens
Wireshark / IoT Inspector	Network traffic monitoring for IoT	Effective in detecting anomalies, malware communication, and C2 channels	Limited against encrypted traffic; requires continuous monitoring
Blockchain Prototype Ledger	Chain-of-custody verification	Immutable and transparent records of evidence handling	Prototype stage; not yet widely adopted in legal frameworks

Table 2. Comparative Evaluation of Acquisition Methods

Environment	Acquisition Method	Avg. Recovery (%)	Avg. Time	Strengths	Limitations
Cloud	Logical Snapshot	~78	12 min/GB	Fast and simple; good for preliminary investigation	Limited scope; may miss encrypted/hidden data
	API-based Acquisition	~89	15 min/GB	Highest recovery; structured access via provider APIs	Jurisdictional/legal dependency; requires provider support
	Network Packet Capture	~65	20 min/GB	Useful for anomaly detection and monitoring live traffic	Incomplete; heavily affected by encryption
IoT	Firmware Dumping	~82	45 min/device	Comprehensive low-level access	Risk of device bricking; requires hardware expertise
	Live Memory Extraction	~90	60 min/device	Best recovery of volatile data	Highly time-sensitive; needs immediate access
	Log Acquisition	~70	20 min/device	Easy and fast to perform	Logs can be incomplete, manipulated, or erased

3 RESULTS AND ANALYSIS

The first part of the results focuses on the evaluation of different cloud acquisition techniques. Cloud forensics presents unique challenges because data is stored in distributed infrastructures and is often protected by strong encryption and vendor-specific protocols. To assess the efficiency of different strategies, this study compared **logical snapshotting, API-based acquisition, and network packet capture**. The results are summarized in Table 1, which highlights the recovery percentages, average acquisition times, and the challenges inherent in each approach.Table 1 compares recovery percentages.

Table 3. Cloud Acquisition Comparison

Method	Recovery (%)	Avg. Time (GB/min)	Challenges
Logical Snapshot	78	12	Limited scope, vendor lock-in
API-based Acquisition	89	15	Jurisdiction, authentication issues
Network Capture	65	20	Encrypted traffic, incomplete logs

As shown in Table 3, logical snapshotting achieved a recovery rate of 78% with an average acquisition time of 12 minutes per gigabyte. This method proved efficient for preliminary investigations where quick access to data was required. However, its limitations included a restricted scope of recovery and dependency on vendor-specific features, meaning that important hidden or encrypted files often remained inaccessible.

API-based acquisition outperformed the other methods with a recovery rate of 89% and an average time of 15 minutes per gigabyte. This strategy allowed for structured data extraction directly through cloud service provider interfaces, including user files, metadata, and access logs. While highly effective, this method also presented significant challenges, particularly with respect to jurisdictional issues and authentication dependencies. Investigators were often required to obtain legal authorization and credentials, which could delay or even restrict access to critical evidence.

In contrast, network packet capture achieved the lowest recovery rate at 65% and was the slowest, requiring 20 minutes per gigabyte. Despite these drawbacks, packet capture remained valuable for detecting anomalies in traffic flows, such as attempts to exfiltrate data or evidence of malware communication. However, its utility was limited in cases where traffic was encrypted, leading to incomplete evidence collection.

Taken together, the results in Table 3 demonstrate a clear trade-off: while API-based acquisition offers the most comprehensive recovery, it is highly dependent on external cooperation and legal frameworks; logical snapshots are fast but limited in scope; and network captures provide supplementary insights into live traffic but cannot be relied upon as a primary evidence source. These findings confirm that no single method is sufficient, and that a hybrid acquisition approach is often required in cloud forensic investigations.

The second part of the results focuses on forensic acquisition methods for IoT devices. Unlike cloud environments, IoT platforms introduce additional complexity due to hardware diversity, proprietary firmware, and volatile data that can disappear

once devices are powered off. To evaluate their effectiveness, this study compared firmware dumping, memory extraction, and log acquisition. The outcomes are presented in Table 4, which details recovery percentages, acquisition times, and key challenges encountered during experiments.

Table 4. IoT Acquisition Comparison

Method	Recovery (%)	Avg. Time (min/device)	Challenges
Firmware Dumping	82	45	Requires device access, risky
Memory Extraction	90	60	Volatile, requires immediate action
Log Acquisition	70	20	Incomplete, tamperable

As illustrated in Table 2, firmware dumping achieved an average recovery rate of 82% with a duration of approximately 45 minutes per device. This method was able to provide comprehensive low-level access to device data, including system binaries and configuration files. However, the process carried significant risks because improper handling could corrupt the firmware or render the device permanently inoperable [11].

Memory extraction demonstrated the highest recovery performance at 90%, although it required around 60 minutes per device. This approach was particularly effective for capturing volatile data, such as encryption keys, session tokens, and real-time application states. Its primary limitation was its sensitivity to time, since evidence could easily be lost if the device was powered down or left running for too long [12].

By contrast, log acquisition had the lowest recovery rate at 70%, although it was the fastest method, requiring only 20 minutes per device. Log files were easy to obtain and provided useful records of user actions or system events. Nevertheless, logs were highly vulnerable to manipulation or deletion by attackers, which significantly reduced their reliability as standalone forensic evidence [13].

Overall, Table 2 highlights that IoT forensics faces a persistent trade-off between completeness and practicality. Firmware dumping and memory extraction can yield deep and valuable insights but demand specialized skills and controlled environments. Log acquisition, while quick and accessible, cannot be solely relied upon for comprehensive investigations. These findings suggest that a hybrid IoT forensic strategy—combining volatile memory capture with firmware analysis and log inspection—offers the most reliable pathway for investigators when handling IoT-related cybercrime [11]–[13].

4 CASE STUDIES AND CHALLENGES

The first case study addresses cloud credential theft, where attackers exploited Google Cloud storage services to host phishing kits that harvested user credentials. In this scenario, logical snapshotting was performed and successfully captured part of the directory structure, but it missed several hidden and encrypted payloads. By contrast, API-based acquisition proved far more effective, enabling the extraction of entire folder hierarchies along with metadata that recorded file creation, modification, and access times. These additional details were essential for establishing when the phishing kits were deployed and by whom they were accessed. Nonetheless, the process also highlighted major challenges. API-based acquisition required proper authentication and authorization tokens, which investigators could only obtain through formal cooperation with the service provider. Furthermore, jurisdictional constraints meant that some of the evidence remained beyond immediate reach, emphasizing the legal complexities of cloud forensics.

The second case study examines an IoT botnet attack, specifically a Mirai variant that compromised a network of smart cameras. These devices were used to launch large-scale Distributed Denial of Service (DDoS) attacks. In this case, log acquisition revealed limited information about device activity, but many crucial records had already been deleted or tampered with by the malware. Firmware dumping offered a broader perspective by exposing configuration files and embedded binaries, but the most revealing results came from memory extraction. By capturing volatile memory from the infected cameras, investigators were able to identify botnet binaries, active processes, and command-and-control (C2) communication attempts. Despite these successes, IoT forensic analysis encountered several difficulties. Memory extraction was highly time-sensitive, requiring immediate access before the devices were rebooted or powered off, while firmware dumping carried the risk of permanently damaging the hardware. The case illustrates the volatile and fragile nature of IoT evidence and the technical expertise required to preserve it.

The third case study involves cross-border cloud evidence in a financial fraud investigation. The fraudulent transactions were traced back to an Amazon Web Services (AWS) S3 bucket, but the data was physically stored in a foreign jurisdiction.

Logical snapshotting allowed investigators to access some metadata, but the bulk of evidence—transaction logs and user files—was only accessible through cooperation with the hosting provider. This reliance on international collaboration created significant delays, as access was contingent upon Mutual Legal Assistance Treaty (MLAT) requests. Although API-based acquisition eventually yielded the required data, the process underscored the legal and procedural barriers inherent in cloud forensics. In addition to technical acquisition challenges, investigators were also required to ensure strict adherence to chain-of-custody protocols to maintain evidentiary integrity across borders.

Collectively, these three case studies demonstrate that both cloud and IoT forensics face persistent barriers, including encryption, volatility, and jurisdictional fragmentation. They also reinforce the necessity of adopting a hybrid investigative approach, in which multiple acquisition techniques are deployed simultaneously to balance efficiency, completeness, and legal defensibility.

4.1 Synthesis of Case Studies: Common Challenges and Solutions

The case studies presented above demonstrate several recurring challenges that are central to both cloud and IoT forensic investigations. In the first case study of cloud credential theft, one of the most prominent issues was the reliance on service providers for access through API-based acquisition, which created dependencies that could delay or restrict evidence retrieval [2]. Moreover, jurisdictional fragmentation meant that investigators often faced barriers when evidence was stored outside national borders, requiring lengthy legal procedures before access could be granted [6].

In the second case study concerning the IoT botnet attack, volatility of data emerged as the greatest obstacle. Volatile memory, which contained the most critical artifacts such as botnet binaries and command-and-control communication details, was easily lost when devices were rebooted or disconnected [12]. In addition, firmware dumping, while comprehensive, carried the risk of corrupting the device, which could compromise both the evidence and the functionality of the hardware [11]. Another recurring challenge was the manipulation or deletion of IoT logs, which reduced the reliability of these artifacts as standalone evidence [13].

The third case study on cross-border cloud evidence revealed the persistent legal and procedural challenges inherent in forensic investigations involving multinational providers. Even when investigators identified the location of evidence, international legal frameworks such as Mutual Legal Assistance Treaties (MLATs) often caused significant delays, reducing the timeliness of forensic response [8]. This dependency on external jurisdictions directly impacts the integrity of the investigation, particularly when evidence may be modified or deleted before access is granted [5].

Synthesizing across these case studies, four overarching categories of challenges can be identified. The first is encryption and access barriers, which prevent direct acquisition of content from both cloud services and IoT devices [3]. The second is data volatility, as seen in memory extraction for IoT and ephemeral records in cloud environments, where evidence can vanish in seconds without immediate preservation [12]. The third is jurisdictional complexity, since evidence stored abroad requires international cooperation and compliance with foreign laws, leading to delays and partial access [6]. The final challenge is the limitation of single-method acquisitions, because logical, API-based, or log acquisition alone cannot capture the full spectrum of evidence needed for reliable analysis [7].

These findings reinforce the importance of adopting hybrid strategies in digital forensics. Combining logical, API-based, and packet-based methods in cloud investigations can maximize evidence completeness while mitigating encryption barriers [9]. Similarly, integrating firmware dumping, memory extraction, and log analysis in IoT forensics provides complementary strengths, ensuring more resilient evidence collection [11].

5 CONCLUSION

This study has demonstrated that cloud and IoT forensics present both significant opportunities and formidable challenges for digital crime investigation. Through comparative evaluation, the results confirmed that API-based acquisition in cloud environments consistently provides the highest recovery rates, reaching up to 89%, but its effectiveness depends heavily on cooperation from service providers and compliance with jurisdictional requirements. In contrast, logical snapshots, while fast and efficient, often failed to capture hidden or encrypted data, whereas network packet captures were most useful in detecting anomalies in live traffic but produced incomplete results due to pervasive encryption. These findings underline the necessity of tailoring acquisition methods to the investigative context rather than relying on a single strategy.

For IoT devices, the research showed that memory extraction achieved the highest evidence recovery at 90%, making it the most comprehensive method for capturing volatile data such as botnet binaries and active sessions. However, this approach is extremely time-sensitive and risks losing critical evidence if not conducted immediately after device seizure. Firmware dumping, while valuable for accessing low-level system artifacts, carries the inherent danger of damaging devices and potentially altering

evidence, while log acquisition, although quick and accessible, remains the least reliable due to its vulnerability to manipulation and incompleteness. Together, these outcomes emphasize that IoT forensics demands specialized expertise and well-prepared investigative readiness.

The case studies—covering cloud credential theft, IoT botnet attacks, and cross-border cloud evidence—further highlighted the recurring obstacles faced by investigators. These included encryption barriers, which consistently prevented direct access to critical data; data volatility, which caused crucial information to disappear rapidly; jurisdictional fragmentation, which delayed or restricted access to evidence stored abroad; and limitations of single-method acquisitions, which often produced partial or inconclusive results. These findings align with the broader literature, which has similarly emphasized the urgent need for multi-method forensic frameworks that combine technical, legal, and organizational strategies.
From a practical perspective, the study suggests that investigators must adopt hybrid acquisition approaches, integrating multiple techniques such as API-based cloud extraction with network monitoring or combining IoT memory dumps with firmware and log analysis. Such strategies not only maximize evidence recovery but also mitigate the shortcomings of individual methods. Furthermore, the integration of AI-assisted forensic triage can significantly reduce analysis times by automating anomaly detection and prioritizing high-value evidence. Likewise, blockchain-based chain-of-custody systems offer a promising mechanism to strengthen the immutability and credibility of evidence handling, particularly in cases involving multiple jurisdictions.

At the policy level, the research underscores the necessity of forensic readiness, particularly for countries like Indonesia, where technical infrastructure, skilled personnel, and international collaboration mechanisms require significant strengthening. National governments should invest in digital forensic laboratories, enhance investigator training, and establish partnerships with cloud providers and IoT manufacturers to facilitate lawful and timely access to evidence. At the international level, greater harmonization of legal standards and more responsive MLAT procedures are required to overcome cross-border barriers to evidence acquisition.

In conclusion, cloud and IoT forensics represent an indispensable but evolving field within digital investigations. This study demonstrates that while technical tools and methods can provide deep insights, their effectiveness is constrained by encryption, volatility, and legal limitations. Moving forward, future research should focus on developing standardized forensic frameworks that integrate hybrid acquisition strategies, AI-driven analysis, and blockchain-based verification mechanisms, while also addressing the legal and policy dimensions of cross-border cooperation. Only through such multidisciplinary approaches can forensic investigators effectively respond to the challenges of modern cybercrime and ensure that digital evidence remains both reliable and admissible in court.

ACKNOWLEDGEMENTS

The author wishes to acknowledge the contributions of digital forensic professionals and researchers who shared their expertise and practical perspectives during the development of this study. Their insights into cloud acquisition challenges and IoT forensic methodologies were invaluable in strengthening the comparative analysis presented in this work. The author is also grateful to independent laboratories and open-source communities that provided access to tools, datasets, and reference materials, enabling the testing of multiple acquisition and analysis techniques. Their commitment to advancing forensic science has played a significant role in shaping the outcomes of this research. Lastly, the author extends appreciation to colleagues and peers in the wider digital forensics community whose ongoing discussions, feedback, and encouragement have inspired and supported the completion of this article.

REFERENCES

[1] IDC, “Worldwide Cloud Storage Forecast,” IDC Report, 2023.
[2] A. Jain and R. Gupta, “Cloud-enabled phishing and its forensic investigation,” *Forensic Sci. Int.: Digit. Invest.*, vol. 45, pp. 301–312, 2023.
[3] M. Singh et al., “IoT Botnets: Forensic perspectives,” *IEEE Access*, vol. 12, pp. 11423–11439, 2024.
[4] N. Gruschka, L. L. Iacono, “Challenges in Cloud Forensics,” *ACM Comput. Surveys*, vol. 55, no. 3, pp. 1–36, 2023.
[5] S. Zawoad and R. Hasan, “Trustworthy cloud forensics,” *IEEE Cloud Comput.*, vol. 11, no. 2, pp. 56–64, 2023.
[6] Interpol, “Cloud Evidence and Jurisdictional Barriers,” Interpol Report, 2024.
[7] A. Alenezi and H. Alhassan, “Anti-forensic strategies in IoT,” *Digit. Invest.*, vol. 48, pp. 301–315, 2025.
[8] P. Casey, “Legal admissibility of cloud evidence,” *Int. J. Cyber Criminol.*, vol. 19, no. 1, pp. 67–82, 2024.
[9] Magnet Forensics, “Cloud API-based acquisition,” Technical Whitepaper, 2024.
[10] R. R. Rout et al., “Encrypted traffic analysis in cloud forensics,” *J. Inf. Secur. Appl.*, vol. 81, pp. 103–128, 2024.
[11] K. R. Naik and M. Gupta, “IoT firmware analysis for forensics,” *IEEE Internet Things J.*, vol. 11, no. 6, pp. 10561–

10575, 2024.
[12] L. Al-Bassam, “Volatile memory forensics in IoT,” *Forensic Sci. Int.: Digit. Invest.*, vol. 47, 301–320, 2024.
[13] H. Patel et al., “Comparative study of IoT acquisition methods,” *Procedia Comput. Sci.*, vol. 226, pp. 211–222, 2024.
[14] C. D. Nguyen, “AI-assisted cloud forensic triage,” *IEEE Access*, vol. 12, pp. 88901–88915, 2024.
[15] A. Vasilaras et al., “Artificial Intelligence in Cloud Forensics,” *Forensic Sci. Int.: Digit. Invest.*, vol. 49, 302–311, 2025.
[16] T. Sharma, “Blockchain for chain-of-custody in IoT forensics,” *IEEE Trans. Inf. Forensics Secur.*, vol. 19, pp. 2789–2799, 2024.
[17] Oxygen Forensics, “Cloud and IoT forensic challenges,” Technical Blog, 2025.
[18] Europol, “Cross-border evidence handling,” Europol Policy Paper, 2024.
[19] Amnesty International, “Surveillance in IoT and cloud,” Global Report, 2023.
[20] GSMA, “The Mobile Economy 2024,” GSMA Report, 2024.