Computer and Telecommunication Engineering 2024, 2(4), 3070.
https://doi.org/10.54517/cte3070

Review

IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem

Nishchal Soni

School of Bioengineering and Biosciences, Lovely Professional University, Punjab 144001, India; nishchalresearch@gmail.com

CITATION

Soni N. IoT forensics: Challenges, methodologies, and future directions in securing the Internet of Things ecosystem. Computer and Telecommunication Engineering. 2024; 2(4): 3070. https://doi.org/10.54517/cte3070

ARTICLE INFO

Received: 14 November 2024
Accepted: 20 December 2024
Available online: 29 December 2024

Abstract: The rapid growth of the Internet of Things (IoT) has significantly impacted digital forensics, introducing both new opportunities and challenges. IoT forensics, a specialized field within digital forensics, focuses on the acquisition, analysis, and interpretation of data from diverse IoT devices such as smart home systems, wearables, and industrial platforms. This review examines the current state of IoT forensics, highlighting challenges such as device diversity, data volatility, encryption, and the need for real-time analysis. It also evaluates existing forensic methodologies and tools, assessing their effectiveness and limitations in addressing these challenges. Furthermore, the paper identifies critical research gaps and proposes future directions, including the development of standardized forensic frameworks and greater collaboration between IoT manufacturers and forensic experts. The aim is to advance IoT forensic practices to keep pace with rapidly evolving IoT technologies, thereby enhancing the investigation and prosecution of cybercrimes.

Keywords: IoT forensics; cloud computing; digital forensics; Internet of Things

1. Introduction

The Internet of Things (IoT) is a transformative technological advancement that connects an ever-growing number of devices—ranging from household items like smart thermostats and refrigerators to critical industrial machinery and infrastructure systems. This interconnected ecosystem fosters unparalleled convenience, automation, and operational efficiency across various sectors, including healthcare, manufacturing, transportation, and smart cities. However, as IoT devices proliferate and become increasingly sophisticated, they introduce a series of complex challenges, particularly in the domain of digital forensics. Unlike traditional digital forensics, which focuses primarily on computer systems and mobile devices, IoT forensics involves investigating a vast and diverse range of interconnected devices, each possessing unique attributes, communication protocols, and data formats [1–3].

IoT devices generate a massive volume of data, which is both a boon and a burden for forensic investigators. On one hand, the large and diverse data sets provide rich sources of potential evidence, but on the other, they introduce substantial challenges in terms of data acquisition, analysis, and preservation. The data generated by IoT devices is often dispersed across multiple physical and virtual locations, transmitted through various communication protocols, and stored in a wide range of formats. This diversity complicates the process of data collection and analysis, making it difficult to ensure evidence integrity and continuity [4,5]. The dynamic and real-time nature of IoT data further exacerbates these challenges, as investigators must contend with continuously evolving data sources that can change rapidly during an investigation.

A core challenge in IoT forensics is the heterogeneous nature of the devices and systems involved. Unlike traditional digital environments that rely on standardized protocols and data formats, IoT devices are produced by a wide array of manufacturers, each employing proprietary technologies and communication standards. This fragmentation necessitates the development of specialized forensic tools and methodologies capable of handling the diverse range of IoT devices and networks [6,7]. Moreover, the decentralized architecture of many IoT ecosystems means that data is often fragmented and dispersed across different devices, cloud services, and edge computing nodes, making it difficult to piece together a cohesive and complete forensic picture. Ensuring data integrity and continuity in these fragmented environments is essential for maintaining the reliability and admissibility of evidence [8,9].

In addition, IoT devices often implement advanced encryption and security mechanisms to protect the privacy and security of user data. While these security measures are critical for safeguarding sensitive information, they also present significant barriers for forensic investigators who must decrypt and analyze the data to gather relevant evidence [10]. The use of proprietary encryption schemes, coupled with the absence of standardized forensic procedures, compounds the difficulty of accessing and interpreting IoT data. This challenge is particularly pronounced in devices that employ custom encryption or security protocols that may not be well-supported by existing forensic tools.

Given these challenges, there is an urgent need for the development of standardized forensic methodologies and tools tailored to the specific requirements of IoT investigations. Traditional forensic tools and practices, which were designed with desktop and mobile systems in mind, often lack the capabilities necessary to handle the complexities of IoT data [11,12]. To address this gap, this paper provides a comprehensive review of the current state of IoT forensics, discussing the challenges, methodologies, and tools in use today. Through a critical examination of existing research, this paper aims to highlight key gaps in the field and propose actionable solutions for enhancing forensic readiness in the IoT ecosystem. Ultimately, this paper seeks to contribute to the development of more effective and standardized forensic practices, supporting the successful investigation and prosecution of cybercrimes within the rapidly evolving world of IoT.

2. Challenges in IoT forensics

The expanding Internet of Things (IoT) ecosystem introduces several unique and complex challenges for forensic investigators. These challenges stem from the diversity of IoT devices, the vast volume of data they generate, and the various security measures employed. As IoT technology continues to evolve, addressing these challenges becomes increasingly crucial for effective digital forensic investigations. Below, we elaborate on the key challenges in IoT forensics, integrating examples and technical specifics where relevant.

2.1. Device diversity and heterogeneity

The IoT landscape is characterized by a wide variety of devices, each with its own specific functionality, architecture, and communication protocols. This diversity complicates forensic investigations, as each device may require different methods for data acquisition and analysis [13]. IoT devices range from simple sensors and smart home appliances to complex industrial machinery and medical equipment, often utilizing proprietary technologies and non-standardized communication protocols.

- Case study: In a forensic investigation involving a smart thermostat (e.g., Nest), the device's data might be stored in a proprietary format, using non-standardized communication protocols like Zigbee or proprietary cloud storage services. This requires specialized forensic tools like X1 Social Discovery for cloud-based data retrieval, or FTK Imager for extracting data directly from the device. Without standardized methods for handling such data, investigators must develop bespoke strategies for each IoT device type.
- Technical specifics: A smart camera, such as a Ring doorbell, might employ proprietary video formats and encrypt its data before transmission. Forensic investigators might need to use Wireshark for packet sniffing and capture the encrypted data packets. If the encryption is robust (e.g., AES), investigators may need to obtain decryption keys from the manufacturer or exploit vulnerabilities in the device's firmware to access the data [7].

The absence of universal forensic standards for IoT devices means that forensic practitioners often encounter inconsistent data formats and storage mechanisms, making it challenging to apply uniform procedures for data extraction, preservation, and analysis [6]. For example, data from a medical IoT device (e.g., a pacemaker) could be stored in highly specialized formats, requiring a deep understanding of the device's architecture to conduct an investigation effectively.

2.2. Data volume and complexity

The volume of data generated by IoT devices is vast and constantly growing, posing significant challenges for forensic investigators. IoT systems produce massive quantities of data, often in real-time, and this data can be distributed across multiple devices, networks, and cloud platforms [4].

- Case study: Consider an industrial IoT (IIoT) system used in a manufacturing plant, where hundreds of sensors monitor machine performance and environmental conditions. The system generates terabytes of time-series data daily, including sensor readings, maintenance logs, and device status reports. Traditional forensic tools struggle to process and analyze such large data volumes. In such cases, investigators may turn to Splunk for its ability to handle large volumes of log and sensor data, parse it efficiently, and visualize potential security breaches or anomalies.
- Technical specifics: The data may also vary in terms of format—sensor data might be in CSV or JSON format, while video surveillance data might be stored in proprietary binary formats. Forensic investigators may need tools like Autopsy to perform data carving or EnCase to recover fragmented or corrupted files from these devices. Moreover, IoT data often includes metadata like

timestamps, device IDs, and sensor types, which must be interpreted to establish a timeline of events. To handle this complexity, investigators need advanced techniques for correlating data across devices and systems [10].

The sheer quantity of data generated by IoT devices can overwhelm traditional forensic tools, necessitating the use of advanced processing techniques and scalable tools that can manage and analyze large datasets. For instance, PRTG Network Monitor can help track real-time network traffic, pinpointing unusual patterns indicative of potential security breaches across IoT devices [8].

2.3. Data volatility and ephemeral nature

IoT devices often store data temporarily or in volatile memory, which means that critical evidence can be lost if not captured quickly. This volatile nature of IoT data presents a major challenge for forensic investigators [9].

- Case study: In an investigation involving a smart home security system, real-time sensor data from motion detectors may be overwritten as new data is generated. If the investigation is delayed, the original data could be lost. To avoid this, forensic investigators might employ tcpdump to capture network traffic in real time or use FTK Imager to create a memory dump from volatile memory. This helps preserve evidence before it is overwritten.
- Technical specifics: For devices that store data temporarily, such as session logs or real-time sensor readings, investigators may need to use Wireshark to capture network traffic before the data is overwritten or deleted. If data is stored in volatile memory (e.g., RAM), specialized tools like Volatility can be used to extract live memory data, which may contain crucial evidence like encryption keys, credentials, or session logs that are otherwise inaccessible [5].

Additionally, some IoT devices are designed with limited data retention capabilities, implementing automatic deletion or overwriting features to ensure minimal data storage. This can be seen in devices like smart thermostats, which often delete historical temperature logs after a set period.

2.4. Security and privacy concerns

Security measures implemented in IoT devices, such as encryption and authentication protocols, can hinder forensic investigations. While these measures are essential for protecting data integrity and user privacy, they present obstacles for forensic experts attempting to access and analyze the data [12].

Case study: In an investigation involving a networked medical device like a pacemaker, encrypted data transmission may occur between the device and a mobile app. To access the data, forensic experts might need to bypass encryption, a process that could involve extracting decryption keys from the device's firmware using specialized tools. One such tool is Cellebrite UFED, which can assist in extracting data from mobile devices that interact with IoT medical equipment, though decryption can be a time-consuming and technically demanding process.

Technical specifics: IoT devices may employ various encryption algorithms like AES or RSA, complicating forensic efforts. Tools like ElcomSoft iOS Forensic Toolkit can help decrypt data from iOS devices associated with IoT systems, but

only if investigators have access to the necessary authentication credentials. This highlights the critical importance of timely access to IoT devices, especially those employing end-to-end encryption for data privacy [13].

Furthermore, privacy concerns associated with IoT devices complicate forensic investigations. Many devices collect sensitive personal data, such as health information from wearable devices or security footage from cameras. Ensuring that investigations comply with privacy regulations (such as GDPR) while preserving evidence is a major challenge for forensic professionals. In cases where personal data is involved, investigators may need to consult legal teams to ensure compliance with privacy laws during the investigation process.

2.5. Emerging IoT-specific threats

As IoT technology evolves, so do the threats and vulnerabilities associated with it. In particular, newer areas such as edge computing vulnerabilities and attacks on IoT-specific communication protocols, including MQTT (Message Queuing Telemetry Transport) and CoAP (Constrained Application Protocol), have become more prevalent. These emerging threats significantly affect forensic readiness and the ability of forensic investigators to acquire and analyze IoT-related evidence.

2.5.1. Edge computing vulnerabilities

Edge computing refers to processing data closer to the source of data generation, such as at IoT devices or local edge nodes, rather than relying on centralized cloud servers. While edge computing can offer advantages in terms of reduced latency and bandwidth efficiency, it introduces several vulnerabilities from a forensic perspective.

- Decentralized data storage: In edge computing environments, data may be stored locally on edge nodes or devices rather than in centralized systems. This decentralized storage complicates the process of data acquisition, as it may be more difficult to identify all potential sources of evidence, especially in cases where edge nodes are distributed across various geographical locations.
    - Evaluation: Tools designed for cloud-based forensics, such as X1 Cloud Collector, may not be equipped to handle decentralized data stored at the edge. These tools would need to adapt to access and acquire data from various local sources, increasing the complexity of the forensic investigation process.
    - Real-World Scenario: In a manufacturing environment where IoT sensors collect data at the edge (e.g., temperature, vibration, and pressure readings), an attack targeting the edge node could erase or manipulate evidence before it is transmitted to the central server. Traditional forensic tools may struggle to retrieve this lost data from local nodes, highlighting the need for edge-computing-aware forensics tools.

2.5.2. Attacks on IoT-specific protocols (MQTT and CoAP)

IoT devices often rely on lightweight communication protocols like MQTT and CoAP to exchange data. These protocols, while efficient, have their own vulnerabilities that can be exploited by attackers, complicating forensic investigations.

- MQTT (Message Queuing Telemetry Transport): MQTT is a popular protocol used for real-time messaging in IoT systems. It is lightweight and designed for low-bandwidth environments, making it ideal for devices that transmit small amounts of data over unreliable networks. However, MQTT is susceptible to several types of attacks, such as:
  - Man-in-the-middle attacks: Attackers can intercept or manipulate messages between IoT devices and brokers, leading to data tampering or unauthorized access.
  - Lack of encryption: Although encryption is possible with MQTT, many implementations do not encrypt the payload or the transport layer, making the data vulnerable to eavesdropping.
  - Evaluation: Forensic readiness in MQTT-based environments requires specialized tools that can capture and analyze encrypted or manipulated MQTT traffic. Tools like Wireshark can capture MQTT packets, but decryption and analysis of payload data require advanced techniques or access to cryptographic keys.
  - Real-world scenario: In a smart home scenario, attackers may exploit MQTT vulnerabilities to inject malicious messages into the communication stream between devices, potentially altering device behavior (e.g., tampering with a smart thermostat's settings). Forensic tools would need to capture MQTT traffic, trace anomalies, and identify potential malicious activity.
- CoAP (Constrained Application Protocol): CoAP is another protocol commonly used in IoT devices, particularly in resource-constrained environments. It is designed to work efficiently in low-power, low-bandwidth settings. However, like MQTT, CoAP has vulnerabilities, including:
  - Denial of Service (DoS) attacks: Attackers can flood CoAP-enabled devices with requests, overwhelming them and potentially disrupting critical operations.
  - Security weaknesses: CoAP's security mechanisms, such as DTLS (Datagram Transport Layer Security), are not always implemented correctly, leaving devices open to exploits.
  - Evaluation: Forensic investigators must be aware of the vulnerabilities specific to CoAP, especially when analyzing network traffic. Tools like PRTG Network Monitor can be employed to monitor for unusual CoAP traffic patterns that might indicate attacks such as DoS. However, the specialized nature of CoAP traffic often requires custom analysis techniques and tools.
  - Real-world scenario: In a smart agriculture setting, a DoS attack targeting a CoAP-based irrigation system could cause severe disruptions to water distribution. Forensics investigators need tools capable of distinguishing between legitimate CoAP requests and attack traffic, enabling them to reconstruct attack timelines.

3. Existing methodologies and tools in IoT forensics

As IoT devices become more prevalent, the methodologies and tools used for forensics need to adapt. In this section, we critically evaluate the effectiveness of key tools and techniques employed in IoT forensics, comparing their performance in real-world scenarios to highlight their strengths, limitations, and practical applications.

3.1. Data acquisition techniques

Effective data acquisition is crucial in IoT forensics, but the tools and techniques employed must be evaluated based on their ability to handle the diversity of IoT devices, their communication protocols, and data formats. Below is a comparison of the most widely used methods.

3.1.1. Network-based data acquisition

- Wireshark: Wireshark is a widely used network traffic analysis tool. It excels at packet sniffing and can capture traffic from IoT devices in real-time, allowing forensic experts to examine data exchanges. In environments where devices communicate over standard protocols (e.g., HTTP, MQTT), Wireshark provides a detailed breakdown of packet headers and payloads, making it highly effective for understanding communication patterns and identifying vulnerabilities [14,15].
    - Evaluation: While Wireshark is effective in capturing traffic, its performance can be limited in environments using encrypted communication or proprietary protocols. Real-world cases have shown that it struggles to provide clear insights when IoT devices use encryption, as the packet contents are obfuscated. Moreover, analyzing vast amounts of data from multiple devices can overwhelm investigators without proper filtering or segmentation of the data streams.
    - Case study: In a smart home security breach, Wireshark was used to capture traffic between compromised smart cameras and a central hub. The tool helped identify a vulnerability in the device's firmware. However, due to the encryption, much of the payload remained unreadable without further decryption efforts, highlighting Wireshark's limitation in encrypted communications.
- PRTG network monitor: PRTG offers real-time network traffic analysis, providing a more comprehensive view of device communications. It is particularly useful for monitoring large-scale IoT networks where a wide variety of devices interact with each other.
    - Evaluation: PRTG's performance in real-world scenarios has been positive, especially in environments where continuous monitoring is needed. It helps detect anomalies like unusual data flow, potential security breaches, and performance issues. However, its effectiveness diminishes when dealing with highly dynamic IoT systems, where devices are added or removed frequently, or in environments that employ multiple types of communication protocols.

3.1.2. Device-based data acquisition

- FTK imager: FTK Imager is one of the most widely used tools for physical data extraction [16,17], offering detailed access to IoT device storage. It can recover deleted files, including those from proprietary file systems, making it valuable for a deep forensic investigation.
  - Evaluation: FTK Imager's ability to extract data from various devices (e.g., smart cameras, wearables) makes it a robust tool for device-based data acquisition. However, challenges arise when dealing with encrypted data or devices with secure boot mechanisms, which may require additional techniques or decryption keys. In cases involving devices with non-standard file systems, FTK Imager's effectiveness is limited, and a tailored forensic approach may be necessary.
  - Case study: In a forensic investigation involving a compromised medical device, FTK Imager was used to extract data from the device's internal storage, uncovering patient records. However, the device's encryption made full data access difficult, requiring the use of additional decryption tools, highlighting FTK Imager's dependency on device-specific characteristics.
- Cellebrite UFED: Cellebrite UFED is highly effective in extracting data from mobile devices and wearables. It supports logical extraction through device interfaces and offers physical extraction for more comprehensive access to device storage.
  - Evaluation: Cellebrite UFED's success in acquiring data from mobile devices is well-established, especially for user-generated content (e.g., messages, photos, GPS data). However, its application to IoT devices outside mobile ecosystems (e.g., industrial sensors or smart appliances) is more limited, as these devices may not conform to the same operating systems or data storage structures. Additionally, handling encryption can be cumbersome, as specialized decryption keys may be required [17].

3.1.3. Cloud-based data acquisition

- X1 cloud collector: This tool is designed for extracting data from cloud services where IoT devices store their information. It supports various platforms (e.g., AWS, Google Cloud, Microsoft Azure), allowing investigators to access cloud-based logs, sensor data, and other relevant information stored by IoT devices [18].
  - Evaluation: X1 Cloud Collector performs well in environments where IoT data is synchronized with cloud platforms. However, the tool's performance can be hindered by strict cloud service provider security measures, such as multi-factor authentication or complex encryption protocols. Real-world cases have shown that the process can be time-consuming, and data access may be limited if proper credentials or authorization tokens are not available.
  - Case study: In a smart city IoT security investigation, X1 Cloud Collector was used to retrieve sensor data from the cloud. While the tool effectively extracted temperature and traffic data, its access to real-time surveillance

video data was limited due to restrictions imposed by the cloud service provider, demonstrating a limitation of cloud-based forensics tools in accessing proprietary cloud data.

3.2. Data analysis techniques

The analysis of IoT data is critical to uncovering evidence and establishing timelines. Below are a few commonly used tools and techniques, evaluated based on their effectiveness and real-world application.

3.2.1. Data parsing and reconstruction

- EnCase: EnCase is often used for data carving, a technique that reconstructs fragmented or corrupted files. It is highly effective in recovering deleted or hidden data from storage devices [19].
  - Evaluation: EnCase is generally effective when dealing with IoT devices that use standard file systems. However, its performance can degrade when dealing with proprietary file systems used by certain IoT devices (e.g., custom Linux-based systems in industrial IoT devices). Moreover, EnCase's ability to parse and reconstruct data may be hindered if the data is encrypted or fragmented across multiple storage locations.
  - Case study: During an investigation of a compromised smart home network, EnCase was used to recover fragmented files from a corrupted network video recorder (NVR). The tool successfully retrieved video files, although some portions were inaccessible due to encryption, illustrating EnCase's limitations in dealing with encrypted data.

3.2.2. Log analysis

- Splunk: Splunk is used extensively for analyzing log files generated by IoT devices. It is known for its scalability and ability to handle large datasets in real-time, making it a suitable choice for IoT environments where devices generate vast amounts of log data [16,20].
  - Evaluation: Splunk excels in environments where continuous monitoring and rapid data analysis are required. However, in cases with limited resources or where devices generate highly diverse log formats, configuring Splunk to extract useful insights can be challenging. Moreover, Splunk's effectiveness diminishes when dealing with IoT devices that don't generate standardized logs.
  - Case study: During an investigation of a connected vehicle system, Splunk was used to analyze logs generated by the vehicle's IoT sensors. The tool helped establish a timeline of events leading to a crash. However, discrepancies in the log formats from different vehicle models made data aggregation and analysis complex, showcasing the challenge of handling diverse IoT log formats.

3.2.3. Behavioral analysis

- MITRE ATT&CK: This framework is used to analyze device behaviors and detect anomalies indicative of malicious activity. It is effective in identifying

known attack patterns and behaviors that deviate from the normal operating conditions of IoT devices [21].

- Evaluation: MITRE ATT&CK provides a structured way to assess device behaviors, making it invaluable in identifying potential security incidents. However, it requires constant updates to account for evolving attack vectors. In environments with rapidly changing IoT ecosystems, using MITRE ATT&CK alone may not be sufficient to catch all emerging threats.
- Case study: In a security breach involving an industrial IoT network, MITRE ATT&CK was used to identify abnormal communication patterns indicative of a cyberattack. The framework successfully flagged suspicious activities, but the rapid adaptation of the attack techniques required continuous updates to the analysis, demonstrating the need for dynamic threat intelligence in IoT environments.

3.3. Challenges and limitations

Despite the strengths of these tools and techniques, several challenges remain in IoT forensics.

3.3.1. Device diversity and proprietary systems

Challenge: The proliferation of diverse IoT devices, each with unique operating systems, firmware, and communication protocols, makes it difficult to standardize forensic investigations.

Real-world case study: The Mirai botnet attack.

The Mirai botnet attack is one of the most significant examples of IoT-related cybersecurity breaches. In this case, thousands of IoT devices (like cameras and routers) were compromised and used in a massive DDoS attack. Many of these devices had proprietary systems and firmware, making it difficult for traditional forensic tools like Cellebrite UFED (used mainly for mobile devices) to extract data. Instead, investigators had to resort to custom-built solutions, such as JTAG (Joint Test Action Group) analysis, to extract data from these proprietary systems. This highlighted the challenge of adapting forensic tools to work with devices that do not adhere to standard protocols [22].

Tools and techniques:

- JTAG: Used to directly access the memory of IoT devices with proprietary systems.
- Autopsy: Applied in some instances to analyze filesystem data from non-standard IoT devices.
- Custom extractors**:** Often built in response to proprietary device formats, requiring advanced programming and reverse-engineering skills.

3.3.2. Data volume and real-time data analysis

Challenge: The vast volume and continuous nature of data generated by IoT devices make it difficult to keep pace with forensic investigations. Real-time data analysis is often necessary for identifying incidents as they occur [23].

Real-world example: Stuxnet attack.

The Stuxnet malware, which targeted industrial control systems (ICS), leveraged IoT devices in critical infrastructure to monitor and sabotage industrial processes. Forensic investigators had to sift through a massive volume of data from control systems and IoT sensors to identify the malware's behavior. The malware's presence on IoT devices like PLCs (Programmable Logic Controllers) meant that real-time data analysis tools had to be deployed to identify the specific anomalies triggered by Stuxnet.

Tools Used:

- Splunk: Used for real-time event and log monitoring in large-scale environments.
- Wireshark: Employed for network traffic analysis to trace the propagation of the malware.
- PRTG network monitor: Deployed to identify unusual data flows from critical IoT devices.

These tools are essential for investigating large-scale IoT-related incidents in real time. However, they require advanced filtering techniques and custom analytics to separate useful evidence from noise.

3.3.3. Security measures

The robust security mechanisms built into many IoT devices, such as encryption, authentication, and secure boot processes, can significantly hinder data access and analysis. In cases where encryption or proprietary protocols are used, investigators may need to bypass these protections using specialized decryption tools, which can be time-consuming and legally complicated. Moreover, attacks targeting IoT-specific protocols like MQTT or CoAP, such as man-in-the-middle attacks or DoS attacks, can further complicate the process of evidence acquisition. Investigators may face challenges in identifying manipulated or lost data due to these attacks, making it necessary to have tools that can analyze and verify the integrity of data transmitted over these protocols [24].

3.4. Comparison of existing tools and techniques (revised)

As IoT forensics continues to evolve, a range of tools and techniques have been developed to address the unique challenges presented by IoT ecosystems. However, the effectiveness of these tools depends heavily on the specific scenario and environment in which they are applied. Below, we compare some of the most commonly used tools and techniques in IoT forensics, evaluating their accuracy, efficiency, and scalability, while also considering their strengths and limitations in different real-world contexts.

3.4.1. Network-based forensics tools

Wireshark

- Accuracy: High. Wireshark provides in-depth packet-level analysis and is effective in capturing network traffic and protocols like MQTT, CoAP, and HTTP.
- Efficiency: Moderate. While it is highly accurate, the tool can become inefficient in high-traffic environments or when analyzing large datasets due to its reliance on real-time packet capture.

- Scalability: Low. In large-scale IoT environments with thousands of devices, Wireshark may become overwhelmed by the volume of data and struggle to provide actionable insights without significant manual intervention.
- Strengths: Ideal for capturing network traffic in smaller to medium-sized IoT environments. It supports numerous protocols and is free and open-source.
- Limitations: It may not provide sufficient detail when investigating proprietary IoT communication protocols or encrypted data.

Splunk

- Accuracy: High. Splunk excels in indexing and searching large datasets, allowing forensic investigators to pinpoint relevant information with high accuracy.
- Efficiency: High. Splunk is designed for real-time log analysis, making it efficient for quickly identifying patterns in massive datasets generated by IoT devices.
- Scalability: Very high. Splunk is built for large-scale data environments and can easily scale to handle billions of events, which makes it suitable for IoT ecosystems that generate significant amounts of data.
- Strengths: Its ability to process and analyze logs from across a distributed network of devices is unmatched, making it ideal for network-based investigations.
- Limitations: Its cost can be prohibitive for smaller investigations. It also requires significant resources to set up and maintain.

3.4.2. Device-based forensics tools

Cellebrite UFED

- Accuracy: Moderate to high. While highly effective for mobile forensics, Cellebrite's support for proprietary IoT devices is limited, and results may vary.
- Efficiency: Moderate. The tool is efficient in extracting data from standard devices but can struggle with non-standard or obscure IoT systems.
- Scalability: Low to moderate. Although the tool supports a wide range of devices, it is not optimized for large-scale IoT ecosystems with thousands of diverse devices.
- Strengths: Highly effective for mobile devices, such as smartphones, which are often integral parts of IoT ecosystems.
- Limitations: It is not well-suited for many IoT devices that use proprietary operating systems and communication protocols.

FTK imager

- Accuracy: High. FTK Imager is highly accurate for device-based forensic investigations, including data recovery from flash storage and IoT devices.
- Efficiency: High. It can extract data rapidly from supported devices, and its support for disk imaging speeds up data retrieval.
- Scalability: Moderate. While it can be used for numerous devices in parallel, FTK Imager is not specifically designed to scale in large IoT environments with diverse devices and network structures.

- Strengths: It is especially effective for capturing data from devices with file systems, making it suitable for IoT devices with file storage capabilities.
- Limitations: FTK Imager may not be effective for handling volatile data or devices with non-standard communication protocols.

3.4.3. Cloud and edge computing forensics

PRTG network monitor

- Accuracy: Moderate to high. PRTG excels at monitoring network health and can accurately capture large volumes of IoT data, but it may struggle with pinpointing the precise source of anomalies or malicious activity in large-scale environments.
- Efficiency: High. PRTG allows real-time monitoring of network traffic and performance metrics, providing efficient detection of performance issues in IoT systems.
- Scalability: High. PRTG can scale to accommodate large numbers of devices, making it well-suited for large-scale IoT networks and edge computing systems.
- Strengths: Ideal for continuous monitoring of devices across IoT ecosystems, including edge devices, and provides real-time data on performance and traffic.
- Limitations: Its effectiveness in forensic investigations is limited to monitoring rather than in-depth forensic analysis or data recovery.

Fog computing forensics

- Accuracy: Varies. Fog computing, a paradigm where data is processed on local nodes rather than cloud servers, introduces complexity in tracing data sources. The accuracy depends on the tools used to capture data from fog nodes and edge devices.
- Efficiency: Low to moderate. Investigating data from fog-enabled devices requires efficient tools that can quickly analyze both local and cloud-stored data, but current tools struggle to analyze such distributed systems in real time.
- Scalability: Moderate. While fog computing can scale to edge devices, conducting forensic investigations at scale across numerous fog nodes introduces challenges due to the distribution of data.
- Strengths: Offers low-latency processing and reduced dependency on cloud services for data storage, improving overall efficiency.
- Limitations: Difficulty in collecting evidence across multiple distributed devices and fog nodes, especially in dynamic environments where data may be transient or ephemeral.

3.4.4. Blockchain and IoT forensics

Blockchain in IoT Forensics

- Accuracy: High. Blockchain offers immutable data storage, which ensures that any data captured from IoT devices remains unchanged and verifiable, providing high forensic value.
- Efficiency: Moderate. Blockchain data can be difficult to analyze at scale, as it requires the use of specialized blockchain explorers and tools to track transactions across distributed ledgers.

- Scalability: High. Blockchain, being decentralized, can theoretically scale across millions of IoT devices, as each transaction is recorded and verified in a distributed ledger.
- Strengths: Offers immutable and transparent data storage, ensuring data integrity during forensic investigations.
- Limitations: Analysis tools are still evolving, and analyzing massive amounts of transaction data in real-time remains challenging.

4. Gaps in current research

Despite advancements in IoT forensics, several gaps remain that hinder the effective investigation of IoT-related incidents. Identifying and addressing these gaps is crucial for developing robust forensic practices that can keep pace with evolving technologies. The following are key areas where improvements are needed.

4.1. Lack of standardization

The absence of standardized methodologies for data acquisition and analysis remains one of the most significant gaps in IoT forensics. Investigations are often hindered by the lack of uniform protocols, resulting in inconsistencies and reliability issues. While this paper highlights the need for standardization, it is essential to take concrete steps toward developing frameworks that can be adopted universally [24].

To address this gap, a collaborative approach between forensic experts, IoT manufacturers, and standardization bodies is needed. Potential steps include:

- Development of universal protocols: Establishing industry-wide standards for data collection from IoT devices, ensuring that forensic tools can operate across a variety of platforms, whether mobile, sensor-based, or cloud-based.
- IoT forensic certification programs: Instituting certifications for forensic tools and personnel, ensuring that investigators are equipped with the necessary skills to handle IoT devices effectively.
- Creation of a unified forensic framework: A formalized framework that outlines common methodologies for data acquisition, preservation, analysis, and reporting. This framework should cover everything from device data storage (local or cloud-based) to methods for analyzing real-time data streams generated by edge computing devices.

Standardized frameworks could also incorporate edge computing environments, ensuring that data from decentralized networks can be securely captured and analyzed without losing integrity, thereby enhancing forensic readiness in the context of modern IoT systems.

4.2. Data privacy and encryption

Many IoT devices employ sophisticated encryption techniques to protect user data, which presents significant challenges for forensic analysis. The process of decrypting encrypted data without compromising its integrity is a major hurdle for forensic investigators. Advanced encryption methods are designed to safeguard data from unauthorized access, but they also complicate efforts to retrieve and analyze data during an investigation. Privacy concerns related to the extraction and use of

personal data from IoT devices can lead to legal and ethical dilemmas [25]. Balancing the need for forensic investigation with the protection of individual privacy rights remains a complex issue, necessitating the development of strategies that address both technical and ethical considerations. Additionally, attacks targeting IoT-specific protocols like MQTT and CoAP complicate the issue further. Man-in-the-middle attacks on these protocols can manipulate data in transit, causing loss of evidence or introducing ambiguity into the investigation process. Investigators need to develop specific methods for identifying compromised data in these protocols.

4.3. Real-time data analysis

The dynamic nature of IoT environments, characterized by continuous data generation and transmission, creates a pressing need for real-time analysis capabilities. Current forensic tools and methodologies often struggle to keep pace with the rapid influx of data, making it challenging to provide timely insights during investigations [26]. The ability to analyze data as it is generated is crucial for identifying and responding to security incidents promptly. However, many existing solutions are designed for static data analysis, which can hinder their effectiveness in environments where data is continuously evolving. Additionally, edge computing environments, by nature, process data locally in real-time. This requires new forensic tools to handle the unique challenges of analyzing edge data streams, which might not be captured centrally, leaving gaps in the investigation if not properly addressed.

4.4. Device diversity and proprietary systems

The vast array of IoT devices, each with its proprietary operating systems and data formats, poses a significant challenge for forensic analysis. Many forensic tools are tailored to specific types of devices or systems, which can limit their applicability across the diverse IoT landscape. The proprietary nature of many IoT systems complicates the development of comprehensive forensic solutions that can effectively address the full spectrum of IoT technologies. This diversity requires forensic practitioners to have specialized tools and expertise for each type of device, making it difficult to establish a unified approach to IoT forensics. Additionally, as IoT devices adopt newer technologies like 5G and edge computing, the forensic landscape will need to evolve to account for the distinct behaviors and data flows of devices in these advanced environments.

4.5. Scalability issues

Scalability is a critical concern in IoT forensics. As the number of IoT devices continues to grow, forensic tools and methodologies must be capable of handling larger volumes of data and more complex networks. Current solutions often lack the scalability needed to manage investigations involving numerous devices and extensive data sources. The ability to scale forensic processes effectively is essential for addressing the challenges posed by large-scale IoT environments, ensuring that investigations can accommodate the growing complexity and data volume associated with modern IoT ecosystems. With the rise of technologies like edge computing, which enables more localized data processing, investigators will need scalable

solutions that can handle distributed data and maintain coherence across geographically dispersed devices.

4.6. Remote desktop tools and their impact on IoT forensics

The integration of remote desktop tools such as AnyDesk and TeamViewer within IoT ecosystems introduces additional challenges for forensic investigations [27–29]. These tools enable users to access and control IoT devices remotely, which can lead to the alteration or deletion of digital evidence. The use of remote desktop tools creates extra layers of obfuscation, including encrypted communication and volatile data that may be difficult to recover. Forensic analysts must account for the impact of these tools when investigating IoT-related incidents, particularly in terms of maintaining the integrity and reliability of collected evidence. The presence of remote access capabilities complicates the forensic process, requiring careful consideration of how these tools affect data preservation and analysis. Investigators may also need specialized techniques to account for remote access interactions with IoT devices and to assess any potential data alterations or security breaches that may have occurred during remote operations.

Addressing these gaps involves ongoing research and development in forensic methodologies and tools, aiming to enhance the effectiveness of IoT forensics in an ever-evolving technological landscape. By tackling these challenges, the field of IoT forensics can progress towards more robust and adaptable investigative practices.

4.7. Relevant and emerging research in IoT forensics

In addition to addressing the gaps in standardization, real-time analysis, and scalability, there are some recent developments in the IoT field that provide valuable insights into the challenges and solutions for IoT forensics. These works are particularly relevant to ensuring the security and forensic readiness of IoT systems.

4.7.1. IoT fog-enabled multi-node centralized ecosystem for real-time screening and monitoring of health information

Recent research has explored the use of fog computing to create a multi-node, decentralized IoT ecosystem capable of real-time health monitoring. This system utilizes fog nodes positioned at the edge of the network to process data locally, reducing latency and improving the speed of data screening and analysis in healthcare settings. The integration of fog computing into IoT forensics allows for better real-time decision-making and the immediate identification of potential security breaches in health data. This approach supports the forensic need for analyzing health data in real time and can be critical in responding to cyber threats in healthcare IoT environments.

4.7.2. Blockchain Internet of Things (BIoT): Secured, device-to-device architecture and simulation scenarios

Blockchain technology has been proposed as a solution for securing IoT environments through BIoT (Blockchain IoT). Blockchain ensures a secure, transparent, and decentralized architecture for IoT devices, enabling device-to-device communication with integrity and tamper-proof features. BIoT enhances data security, making it more reliable for forensic analysis by guaranteeing that the data

logs maintained by devices cannot be altered without detection. It also provides a way to trace actions and events back to their source, which is crucial for ensuring forensic readiness in IoT ecosystems. Recent works have simulated these BIoT architectures in real-world IoT scenarios, providing valuable insights into their practical application in forensic investigations.

4.7.3. IoT-based monitoring for the growth of basil using machine learning

IoT sensors combined with machine learning algorithms are being used in agricultural monitoring systems to track the growth of plants, such as basil. The IoT system monitors environmental factors like temperature, humidity, and soil moisture, while the machine learning models predict the optimal conditions for plant growth. The integration of IoT in agriculture presents an opportunity to explore how machine learning can assist in predictive forensics, where IoT systems are used to not only collect data but also predict and alert for anomalies or potential threats. In forensic investigations, machine learning algorithms could be employed to analyze historical data from IoT devices, identifying suspicious patterns indicative of a security breach.

4.7.4. A secure and efficient signature scheme for IoT in healthcare

The healthcare sector, one of the most prominent applications for IoT, faces significant security concerns due to the sensitivity of medical data. A secure and efficient signature scheme has been proposed to ensure the authenticity and integrity of data exchanged between IoT-enabled healthcare devices. This scheme utilizes cryptographic techniques to verify the authenticity of both the devices and the data they transmit. By implementing such a scheme, the IoT ecosystem in healthcare can ensure that any data used for forensic investigation has not been tampered with, providing strong evidence in legal and regulatory contexts.

4.8. Addressing the standardization gap in IoT forensics

The lack of standardization in IoT forensics hinders effective investigations and collaboration. While existing tools and methodologies are valuable, their limited interoperability and application across diverse devices create inefficiencies and inconsistencies in forensic practices. To overcome these challenges, the development of standardized frameworks and protocols is critical. Below are several potential solutions that could help address the gap in standardization.

Potential frameworks for IoT forensics

1) Unified IoT forensic framework (UIFF): A standardized forensic framework would provide a common set of procedures for investigating IoT-related incidents. This framework would include protocols for data acquisition, preservation, and analysis across various device types, including those using proprietary operating systems and communication protocols. The UIFF could be developed collaboratively by organizations like the National Institute of Standards and Technology (NIST) and the Internet Engineering Task Force (IETF).
2) Forensic data acquisition protocol (FDAP): A uniform protocol for data acquisition in IoT devices could help investigators collect data in a consistent manner, regardless of the device type or manufacturer. FDAP would outline the

steps for extracting data from both physical and cloud-based devices and ensuring evidence integrity through cryptographic signatures.

3) Collaborative IoT forensics consortium (CIFC): A collaborative approach involving IoT manufacturers, law enforcement agencies, and forensic practitioners could help bridge the standardization gap. The CIFC would focus on the development of common protocols for IoT data acquisition, preservation, and analysis. This consortium could also work on establishing certification programs for forensic tools and training.

4.9. Proposed IoT forensic framework (UIFF)

To streamline the forensic process across IoT ecosystems, the unified IoT forensic framework (UIFF) would consist of the following key components.

4.9.1. Data acquisition standards

- Adopt standardized interfaces for data extraction from various device types, including sensors, mobile IoT, and wearables. These interfaces would ensure seamless compatibility between devices and forensic tools.
- Develop a standardized API for data collection from both cloud-based and edge devices, providing clear guidelines for investigators on how to extract relevant evidence from different environments.

4.9.2. Data preservation techniques

- Establish protocols for the preservation of volatile data (e.g., real-time sensor readings) from edge devices, ensuring that evidence is captured before it is lost or overwritten.
- Incorporate cryptographic hashing techniques for verifying the integrity of data during the preservation phase.

4.9.3. Data analysis protocols

- Create standardized algorithms for parsing data formats specific to IoT devices, ensuring that forensic tools can analyze data consistently across different device types.
- Develop collaborative analysis platforms where forensic experts can share insights and methodologies for tackling unique IoT challenges, such as encrypted communications or proprietary protocols.

4.10. Comparative table of forensic tools and capabilities

To further illustrate the capabilities of existing forensic tools and how they address IoT-specific challenges, we propose the following comparative table. This will summarize the accuracy, efficiency, and scalability of various tools, highlighting their strengths and limitations in specific scenarios (See **Table 1**).

Table 1. Comparative table of forensic tools and capabilities.

Tool/Technique	Accuracy	Efficiency	Scalability	Strengths	Limitations
Wireshark	High	Moderate	Low	Detailed packet-level analysis, support for IoT protocols (MQTT, CoAP, HTTP)	Struggles with high-traffic IoT networks, limited support for encrypted data
Splunk	High	High	Very High	Real-time log analysis, capable of handling massive data volumes	Expensive for small-scale investigations, requires significant setup
Cellebrite UFED	Moderate to High	Moderate	Low	Effective for mobile devices, robust for data extraction	Limited support for non-standard IoT devices
FTK Imager	High	High	Moderate	Excellent for imaging and data recovery from standard devices	Limited ability to handle volatile data and proprietary systems
PRTG Network Monitor	Moderate to High	High	High	Ideal for continuous monitoring of network traffic	Not designed for in-depth forensic analysis
Fog Computing Forensics	Varies	Low to Moderate	Moderate	Useful for low-latency processing in distributed IoT environments	Difficulty in accessing dispersed data and tracking evidence across nodes

5. Discussion

The rapidly expanding Internet of Things (IoT) ecosystem presents unique challenges for digital forensics. Unlike traditional systems, IoT devices are characterized by significant heterogeneity, generating vast amounts of data that are often distributed across various devices and cloud services. This fragmentation complicates the process of data collection and analysis, as forensic investigators must contend with a wide range of communication protocols, data formats, and storage mechanisms. Furthermore, the dynamic nature of IoT environments, where data is continuously generated, stored, and transmitted, requires real-time data analysis capabilities—an area where current forensic tools often fall short.

One of the primary challenges in IoT forensics is the lack of standardization. While forensic tools have been developed for mobile devices and computers, IoT devices come with proprietary operating systems and custom communication protocols that are often incompatible with standard forensic methods. This lack of universal frameworks not only hinders interoperability but also undermines the credibility of forensic findings. The development of standardized protocols for data acquisition, storage, and analysis is crucial to addressing these issues and ensuring consistency across investigations.

Moreover, the security measures implemented by many IoT devices, such as encryption and authentication protocols, further complicate the forensic process. While these measures are vital for user privacy and data protection, they create obstacles for forensic investigators trying to access and interpret data. Specialized decryption tools and legal considerations often delay or prevent the effective retrieval of digital evidence, emphasizing the need for methods that can address security concerns without compromising forensic integrity.

In addition to these challenges, the real-time nature of IoT data generation introduces further complexity. Many forensic tools are designed for static data analysis, making it difficult to process and analyze continuous streams of data effectively. This is particularly problematic in situations where investigations must be conducted promptly, as delays in data processing can hinder the ability to respond

to incidents in a timely manner. The integration of artificial intelligence and machine learning technologies could provide new avenues for real-time analysis, improving the speed and accuracy of investigations.

Lastly, scalability remains a significant challenge. The growing number of IoT devices and the increasing complexity of IoT networks mean that forensic tools must be able to handle larger volumes of data and more complex networks. Current forensic solutions often struggle to scale effectively, particularly in large-scale investigations involving multiple devices and diverse data sources. Addressing scalability concerns is essential for developing tools that can keep pace with the expanding IoT landscape.

6. Conclusion

In conclusion, IoT forensics presents a set of challenges that are distinct from traditional digital forensics. The heterogeneous nature of IoT devices, combined with issues related to data volume, security, and real-time analysis, requires the development of specialized forensic methodologies and tools. Standardization is a critical need, as current tools and protocols are ill-equipped to address the unique demands of IoT environments. Additionally, real-time data analysis capabilities and scalability must be prioritized to keep up with the evolving technological landscape.

The lack of universally accepted forensic frameworks has led to inconsistent and unreliable forensic practices, often undermining the integrity of investigations. Moving forward, research and development in IoT forensics should focus on creating standardized protocols, enhancing real-time data analysis capabilities, and improving scalability. Moreover, the integration of emerging technologies, such as artificial intelligence and blockchain, could provide new solutions for the challenges currently faced by forensic investigators.

As IoT continues to expand across all sectors of society, effective forensic practices are essential for ensuring the integrity of digital evidence in criminal investigations. By addressing the gaps identified in this paper and fostering collaboration between IoT manufacturers and forensic experts, the field of IoT forensics can evolve to meet the demands of this rapidly changing technological landscape. Ultimately, the advancement of IoT forensics will be vital for ensuring justice and maintaining the security of increasingly connected environments.

Conflict of interest: The author declares no conflict of interest.

References

1. Zawoad S, Hasan R. IoT Forensics: Research Challenges and Future Directions. In: Proceedings of the 2015 IEEE International Conference on Services Computing; 27 June to 2 July 2015; New York, USA.
2. Perumal S, Norwawi N, Raman V. Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In: Proceedings of the 2015 Fifth International Conference on Digital Information Processing and Communications; 7–9 October 2015; Sierre, Switzerland.
3. Oriwoh E, Sant P. The forensics edge management system: A concept and design. In: Proceedings of the 2013 International Conference on Adaptive Science & Technology; 25–27 November 2013; Pretoria, South Africa.
4. Daryabar F, Dehghantanha A, Choo KR. Forensics of two cloud storage services: Dropbox and Ubuntu One. Australian Journal of Forensic Sciences. 2015; 47(1): 94–107. doi: 10.1080/00450618.2014.922286

5. Zhou B, Yang F, Rao L. Smartphone Forensics: Enhanced State Consistency with Contextual Information. In: Proceedings of the 2019 IEEE International Conference on Communications; 20–24 May 2019; Shanghai, China.
6. Nawir M, Amir A, Yaakob N, et al. Internet of Things (IoT): Taxonomy of security attacks. In: Proceedings of the 2016 3rd International Conference on Electronic Design; 11–12 August 2016; Phuket, Thailand.
7. Conti M, Dehghantanha A, Franke K, et al. Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems. 2018; 78: 544–546. doi: 10.1016/j.future.2016.11.031
8. Abomhara M, Koien GM. Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security and Mobility. 2015; 4(1): 65–88. doi: 10.13052/jcsm2245-1439.413
9. Weber RH. Internet of Things—New security and privacy challenges. Computer Law & Security Review. 2010; 26(1): 23–30. doi: 10.1016/j.clsr.2009.11.008
10. Granjal J, Monteiro E, Silva JS. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communications Surveys & Tutorials. 2015; 17(3): 1294–1312. doi: 10.1109/COMST.2015.2388550
11. Sivaraman V, Gharakheili HH, Vishwanath A, et al. Network-level security and privacy control for smart-home IoT devices. In: Proceedings of the 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications; 19–21 October 2015; Abu Dhabi, United Arab Emirates.
12. Mahmoud R, Yousuf T, Aloul F, et al. Internet of things (IoT) security: Current status, challenges, and prospective measures. In: Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions; 14–16 December 2015; London, United Kingdom.
13. Hassan NA. Introduction: Understanding Digital Forensics. Digital Forensics Basics. 2019; 1–33.
14. Wireshark. Wireshark User Guide. Available online: https://www.wireshark.org/docs/wsug_html/ (accessed on 2 November 2024).
15. SolarWinds. Network Performance Monitor. Available online: https://www.solarwinds.com/network-performance-monitor (accessed on 2 November 2024).
16. AccessData. FTK Imager. Available online: https://accessdata.com/product-download/ftk-imager-version-4-2-1 (accessed on 2 November 2024).
17. Cellebrite. UFED Physical Analyzer. Available online: https://cellebrite.com/en/ufed-physical-analyzer/ (accessed on 2 November 2024).
18. ElcomSoft. Cloud Explorer. Available online: https://www.elcomsoft.com/Cloud-Explorer.html (accessed on 2 November 2024).
19. OpenText. EnCase Forensic. Available online: https://www.opentext.com/products-and-solutions/products/endpoint-and-investigation/encase-forensic (accessed on 2 November 2024).
20. Splunk. Splunk Enterprise. Available online: https://www.splunk.com/en_us/software.html (accessed on 2 November 2024).
21. MITRE. MITRE ATT&CK Framework. Available online: https://attack.mitre.org/ (accessed on 2 November 2024).
22. Elastic. Elastic Stack (ELK). Available online: https://www.elastic.co/what-is/elk-stack (accessed on 2 November 2024).
23. MSAB. XRY. Available online: https://www.msab.com/products/xry/ (accessed on 2 November 2024).
24. X1. X1 Cloud Collector. Available online: https://www.x1.com/cloud-collector/ (accessed on 2 November 2024).
25. The Sleuth Kit. Autopsy. Available online: https://www.sleuthkit.org/autopsy (accessed on 2 November 2024).
26. Hsu HH, Yang CC. IoT forensics: A survey on challenges and research directions. Journal of Forensic Sciences. 2020; 65(1): 45–59. doi: 10.1111/1556-4029.14238.
27. Soni N, Kaur M, Bhardwaj V. A forensic analysis of AnyDesk Remote Access application by using various forensic tools and techniques. Forensic Science International Digital Investigation. 2024; 48: 301695.
28. Nishchal S. Forensic Analysis of WhatsApp: A review of techniques, challenges, and future directions. Journal of Forensic Science and Research. 2024; 8(1): 19–24.
29. Soni N, Kaur M, Aziz K. Decoding digital interactions: An extensive study of TeamViewer's Forensic Artifacts across Windows and android platforms. Forensic Science International Digital Investigation. 2024; 51: 301838. doi: 10.1016/j.fsidi.2024.301838