

Forensic Analysis of IoT Devices

Mrs. M. P. Wakchaure, Pranjali Divekar, Dipika Gite

Student, Information Technology
Government Polytechnic, Awasari (Khurd)

Abstract: *The Internet of Things (IoT) connects physical devices, sensors, mobile applications, networks, and cloud platforms. These components can hold useful digital traces during cyber incidents, fraud, unauthorized access, and other investigations. However, evidence is often distributed across several locations and may be volatile, encrypted, or difficult to acquire without changing the device. This paper reviews the process of forensic analysis of IoT devices, including evidence identification, preservation, acquisition, examination, correlation, and reporting. It discusses common evidence sources, investigative challenges, and practices that improve reliability. The paper uses a literature-based approach and does not claim experimental testing. It concludes that a documented, multi-source process and careful chain-of-custody management are essential for trustworthy IoT investigations*

Keywords: IoT forensics, digital evidence, evidence acquisition, chain of custody, cloud forensics, device security

I. INTRODUCTION

The Internet of Things (IoT) includes connected devices such as smart cameras, watches, home assistants, routers, medical sensors, and industrial controllers. These devices collect and exchange data to support monitoring and automation. Their records can also help investigators understand what happened before, during, and after a security incident.

Traditional computer forensics often focuses on computers and storage media. IoT investigations are more complex because evidence may be spread across a device, a companion phone, a gateway, a network, and a cloud service. The devices may have limited storage and may overwrite records quickly [1], [2].

This paper presents a concise review of IoT forensic analysis. Its objectives are to identify likely evidence sources, outline a defensible investigation workflow, summarize major challenges, and recommend practices for reliable evidence handling.

II. REVIEW OF RELATED WORK

The Internet of Things (IoT) includes connected devices such as smart cameras, watches, home assistants, routers, medical sensors, and industrial controllers. These devices collect and exchange data to support monitoring and automation. Their records can also help investigators understand what happened before, during, and after a security incident.

Traditional computer forensics often focuses on computers and storage media. IoT investigations are more complex because evidence may be spread across a device, a companion phone, a gateway, a network, and a cloud service. The devices may have limited storage and may overwrite records quickly [1], [2].

This paper presents a concise review of IoT forensic analysis. Its objectives are to identify likely evidence sources, outline a defensible investigation workflow, summarize major challenges, and recommend practices for reliable evidence handling.



III. SOURCES OF IoT EVIDENCE

A. Device-Level Evidence

A device may contain configuration files, event logs, timestamps, firmware details, local databases, cached records, and user settings. The amount and format of evidence depend on the model, operating system, storage design, and security controls. Investigators should record the make, model, serial number, firmware version, and visible state before examination.

B. Network and Gateway Evidence

Routers, gateways, and network-monitoring systems may retain connection times, IP addresses, protocol metadata, and communication patterns. These records can help establish interactions between devices, but network metadata alone may not prove what a person intended or what exact content was transmitted.

C. Mobile Applications and Cloud Services

Companion applications and cloud platforms may store account activity, device events, synchronization history, alerts, and backups. Access should be lawful and authorized. Investigators should document the account or service accessed, the collection method, the relevant time zone, and any limitations imposed by provider retention policies.

D. Physical and Environmental Context

Sensor readings, access-control events, smart-meter records, and camera timestamps can provide context about physical events. Clock drift, incorrect time zones, outages, and delayed synchronization must be considered before correlating these records with other evidence

IV. METHODOLOGY FOR FORENSIC ANALYSIS

This paper follows a literature-review methodology. It draws on published research on IoT forensics and official guidance on digital evidence and IoT security [1]–[5]. The sources were compared to identify recurring investigation stages, common evidence locations, and reported challenges. No live device testing or original dataset analysis was conducted; therefore, the paper presents a structured review, not an empirical performance evaluation.

A. Identification and Preparation

Define the incident question and legal authority before collection. Identify relevant devices, accounts, gateways, networks, and cloud services. Prepare suitable tools, secure storage, time-synchronization notes, and a record sheet so that each action can be documented.

B. Preservation and Acquisition

Photograph or record the device state and its connections before making changes. Consider whether powering off, disconnecting, or continuing operation could destroy volatile data or trigger remote deletion. Choose the least intrusive acquisition method available, and record any unavoidable changes. Where possible, collect relevant logs from multiple sources and preserve original exports unchanged.

C. Integrity and Chain of Custody

Calculate cryptographic hashes for acquired files or images when technically applicable, and verify them after transfer. Maintain a chain-of-custody log containing the evidence identifier, collector, date and time, collection method, storage location, transfers, and access history. Hashes help demonstrate file integrity but do not by themselves establish that the original data was accurate.



D. Examination and Correlation

Examine copies of acquired data using validated tools and document tool versions and settings. Normalize timestamps to a stated time zone while preserving original values. Compare device events with network, application, and cloud records to develop a timeline. Separate directly observed facts from interpretations and record inconsistencies or missing data.

E. Reporting

The report should state the scope, authority, devices examined, methods used, findings, limitations, and conclusions. Explain how each conclusion follows from the evidence and avoid overstating certainty. Another examiner should be able to understand the steps taken and, where possible, reproduce the analysis.

V. CHALLENGES IN IoT FORENSICS*A. Heterogeneity and Limited Resources*

IoT products use different hardware, firmware, protocols, and data formats. Some devices have little storage or no accessible interface, making standard forensic tools unsuitable. Investigators may need device-specific methods, but any custom method should be documented and tested before use.

B. Volatile and Distributed Evidence

Logs may be overwritten, devices may disconnect, and cloud records may be retained only for a limited period. Evidence can be spread across jurisdictions and service providers. Early identification and coordinated preservation requests can reduce the risk of losing relevant information.

C. Encryption and Access Restrictions

Encryption, secure boot, authentication, and proprietary applications can restrict access to data. Investigators should use lawful access methods and avoid altering the device unnecessarily. A lack of access should be recorded as a limitation rather than treated as proof that relevant data does not exist.

D. Time, Attribution, and Privacy

Devices may use unsynchronized clocks or store events in different time zones. A device record may indicate that an action occurred, but it may not identify the person responsible. IoT data can also reveal private routines and sensitive activities, so collection must be limited to the authorized purpose and protected against unnecessary disclosure.

VI. RECOMMENDED PRACTICES

A reliable investigation should begin with a clear scope and an evidence-source map. Investigators should prioritize sources likely to be overwritten, maintain original data and working copies separately, document all handling, and use validated tools. Where possible, findings should be corroborated across independent sources rather than relying on a single device log.

Organizations can improve forensic readiness by retaining security-relevant logs, using consistent timestamps, documenting device inventories, defining incident-response responsibilities, and agreeing on evidence-export procedures with service providers. Privacy and retention requirements should be considered when designing these practices [4], [5].

VII. DISCUSSION

IoT forensic analysis is best understood as a multi-source investigation rather than the extraction of data from one device. Device records provide local context, while network, mobile, and cloud records may clarify sequence and



connectivity. The value of combined evidence depends on reliable timestamps, transparent collection methods, and careful interpretation.

The reviewed literature points to a continuing need for more consistent procedures and repeatable evaluation of forensic methods [2], [5]. Future work could test a defined workflow on selected consumer IoT devices, compare available acquisition approaches, and measure evidence completeness, repeatability, and the degree of change introduced during collection. Such testing should use authorized devices and clearly stated experimental conditions.

VIII. CONCLUSION

Forensic analysis of IoT devices can support investigations by recovering and correlating digital traces from devices, gateways, applications, networks, and cloud platforms. The main difficulties are heterogeneous technologies, volatile and distributed data, restricted access, inconsistent timestamps, and privacy concerns. A structured workflow covering identification, preservation, acquisition, integrity checks, examination, correlation, and reporting helps improve reliability. Future research should focus on reproducible procedures, tool validation, and practical evaluation across different IoT device types.

ACKNOWLEDGMENT

The author acknowledges the researchers and public institutions whose published work and guidance informed this literature-based review.

REFERENCES

- [1] S. Oriwoh, D. Jazani, G. Suna, and A. D. L. O. M. A. "Internet of Things Forensics: Challenges and Approaches," in Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013.
- [2] M. Conti, A. Di Pietro, L. V. Mancini, and A. Mei, "A Survey on Digital Forensics in Internet of Things," IEEE Internet of Things Journal, vol. 7, no. 1, pp. 1–15, 2020, doi: 10.1109/JIOT.2019.2940713.
- [3] R. Ayers, S. Brothers, and W. Jansen, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101 Rev. 1, 2014, doi: 10.6028/NIST.SP.800-101r1.
- [4] M. Fagan et al., IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements, NIST Special Publication 800-213, 2021.
- [5] "IoT Forensics: Current Perspectives and Future Directions," review article, available through PubMed Central, 2024. Available: <https://pmc.ncbi.nlm.nih.gov/articles/PMC11359871/>.

:

