Vol. 8, No. 1, February 2026

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

A Layered IoT Forensics Investigation Framework: A Smart Home Camera Case Study

Desylo Santicho[1], Ahmad Luthfi[2], Tito Yuwono[3]

[1,2]Master of Informatics Program, Faculty of Industrial Technology, Islamic University of Indonesia, Yogyakarta, Indonesia

[3]Department of Electrical Engineering, Faculty of Industrial Technology, Islamic University of Indonesia, Yogyakarta, Indonesia

Received:
December 10, 2025
Revised:
February 4, 2026
Accepted:
February 26, 2026
Published:
March 3, 2026

Corresponding Author:
Author Name*:
Ahmad Luthfi
Email*:
ahmad.luthfi@uii.ac.id

DOI:
10.63158/journalisi.v8i1.1468

Abstract. The rapid adoption of Internet of Things (IoT) technology in various sectors, such as smart homes, healthcare, and transportation, has provided significant efficiency. Nevertheless, many IoT devices are developed without a serious review of security standards, and forensic readiness consideration. As a result, these IoT devices are vulnerable to cyber-attacks that can potentially lead to malware attacks, and system manipulation. This study aims to propose and validate a digital forensic investigation framework in the IoT ecosystem. The framework layers designed in this study consist of the device layer, network layer, and cloud layer. Validation is carried out through a simulated crime scenario recorded by the Mi 360° smart home camera. Meanwhile, the analysis phase focuses on data source artifacts from the device layer, video metadata, technical attributes, and cryptographic integrity verification using hash values (MD5 and SHA-1) documented in the Chain of Custody (CoC) method. The experimental results of this study indicate that digital evidence artifacts sourced from across layers have reliable temporal and structural consistency in reconstructing the chronology of events. This framework successfully correlated artifacts across three layers to reconstruct a complete event timeline, demonstrating its practical validity in distributed IoT forensic investigation.

Keywords: IoT Forensics, Framework, Chain of Custody, Digital Evidence, Home Security Camera

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

1. INTRODUCTION

In today's digital age, a new era of connectivity is taking shape, driven by the widespread use of Internet of Things (IoT) technology. The IoT is crucial for promoting automation, improving efficiency, and generating new opportunities across various sectors, such as industry and healthcare [1], [2]. This technology has permeated almost every aspect of human life, driven by the interconnection of tens of billions of IoT devices worldwide. Examples include smart homes that adjust temperatures according to user preferences and sophisticated healthcare systems that enable real-time patient monitoring [3], [4].

The development of the IoT, while presenting multiple advantages, additionally creates unexpected challenges. The global expansion of IoT-connected devices is projected to approximate 75 billion units by 2025 [5]. This expansion, in turn, engenders potential security vulnerabilities, thereby underscoring the swift evolution of the global digital landscape. Despite the inherent benefits of IoT devices concerning both convenience and operational efficiency, a considerable number continue to pose substantial risks [6], [7]. The production of IoT devices, including smart homes, is carried out without considering adequate security procedures. Manufacturers are more focused on strategies for minimizing costs and accelerating marketing distribution [8].

At the same time, this strategy certainly creates significant opportunities for malicious actors to exploit weaknesses inherent in IoT devices, operating systems, applications, and network architectures [8]. The implications of such exploitation can result in disruption of industrial control systems and violations of personal privacy, as demonstrated by unauthorized access to residential security cameras. In other cases, security vulnerabilities affecting IoT-enabled medical devices, such as pacemakers, or surgical surveillance cameras can substantially damage human safety and the reputation of hospitals [9], [10].

The rapid growth of the IoT necessitates security as a major concern due to the increasing potential for serious risks it poses. Based on a 2020 Business Insider investigation, global spending on IoT security from 2019 to 2024 is estimated to total around US$5 trillion, underscoring the urgency of investing in protecting digital infrastructure, including the IoT sector [11]. Palo Alto Networks' Unit 42 also reported in

the same year that nearly 98% of IoT data traffic remains unprotected with strong encryption methods, plus approximately 57% of devices were identified as vulnerable to attacks with moderate to extreme severity [12]. These discoveries, furthermore, confirmed that security incidents in IoT environments are unavoidable. Therefore, in addition to preventative measures, the ability to conduct systematic post-incident investigations is essential to identify attacks, gather digital evidence, and support law enforcement.

Due to these considerations and challenges, the significance of the role of digital forensics, especially in the IoT ecosystem, is a necessity [13], [14]. Investigating evidence of crime using computers and smartphones with conventional techniques has proven to be unreliable, especially when applied to IoT devices due to inherent differences in device architecture, operating systems, and types of communication protocols used [15]. Therefore, there is a need for the availability of flexible and adaptive methodologies that are specifically designed to accommodate the dynamic and heterogeneous features of IoT [16].

On the other hand, the massive adoption of IoT devices in various fields such as smart homes, smart transportation, and smart logistics creates vulnerabilities to cyberattacks [14]. Several factors such as relatively low production costs, limited computing resources, and minimal security standards are triggers for vulnerabilities in IoT networks. As a result, IoT devices become the main entry point for attackers to exploit vulnerabilities including sensitive data theft, sabotage, or even large-scale botnet attacks [12], [13].

In the case of an IoT network attack incident, a digital forensic investigation is absolutely necessary to gather evidence, understand the attack method, identify the alleged perpetrator, and prepare a legal prosecution report [14]. However, direct investigations in complex and widely distributed IoT ecosystems pose unique challenges [17], [18], [19]. Based on empirical studies, various generic frameworks have been proposed for investigating attacks in IoT ecosystems [15], [20], [21], [22]. These empirical and existing frameworks generally emphasize prosedural pahases but do not explicitly structure artifact across the network layer, cloud services, and on the devices themselves. As a result, the investigation process carries a high risk of crucial findings and evidence being incomplete or even missing altogether.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

A layered forensic investigation approach is crucial because each layer in the IoT ecosystem stores different types and contexts of evidence. The device layer provides local data and system logs, the network layer stores communication information between devices, and the cloud layer stores historical data and service metadata. Without a structured, layered approach, the integrity and completeness of forensic evidence are difficult to guarantee. This study uses a smart security camera as an IoT device used as a case study or ideal scenario because it is integrated with physical devices, networks, and cloud services [23].

The main objective of this study is to develop and validate a structured layered digital forensic investigation framework tailored to distributed IoT environment. This study addresses the gap in existing frameworks that lack explicit cross-layer artifact correlation mechanisms and structured evidential vaidation procedures. This framework systematically structures the investigation process starting from data collection, digital evidence analysis, and reporting while maintaining the integrity of the evidence for reproducibility and recognition in the eyes of the law.

The primary contributions of this paper are decomposed into three elements. First, the design of a structured three-layer forensic investigation framework consisting of device, network, and cloud layers. Second, this study provides empirical validation through a smart home case study that utilizes controlled forensics acquisition and in-depth analysis. Third, the implementation of a cross-layer artifact correlation procedure supported by CoC and cryptographic integrity verification.

2. METHODS

This research is applied research using a case study approach that focuses on the development and testing of a specific framework for digital forensic investigations in IoT environments. The case study approach used in this research aims to test the framework's reliability using a real-life case of a smart home camera as an IoT device. Meanwhile, the research process was conducted systematically, considering the possibility of iteration. Consequently, each stage is interconnected and can be revised based on considerations of previous processes. The proposed investigative framework is not only conceptual but also contextual in its application to digital forensic investigations

in IoT environments. Rather than an intrusion response evaluation model, this study provides a baseline forensic preparedness approach that focuses on organized artifact identification and preservation during normal operational settings. Figure 1 illustrates the research process flow, considering the iterative process.

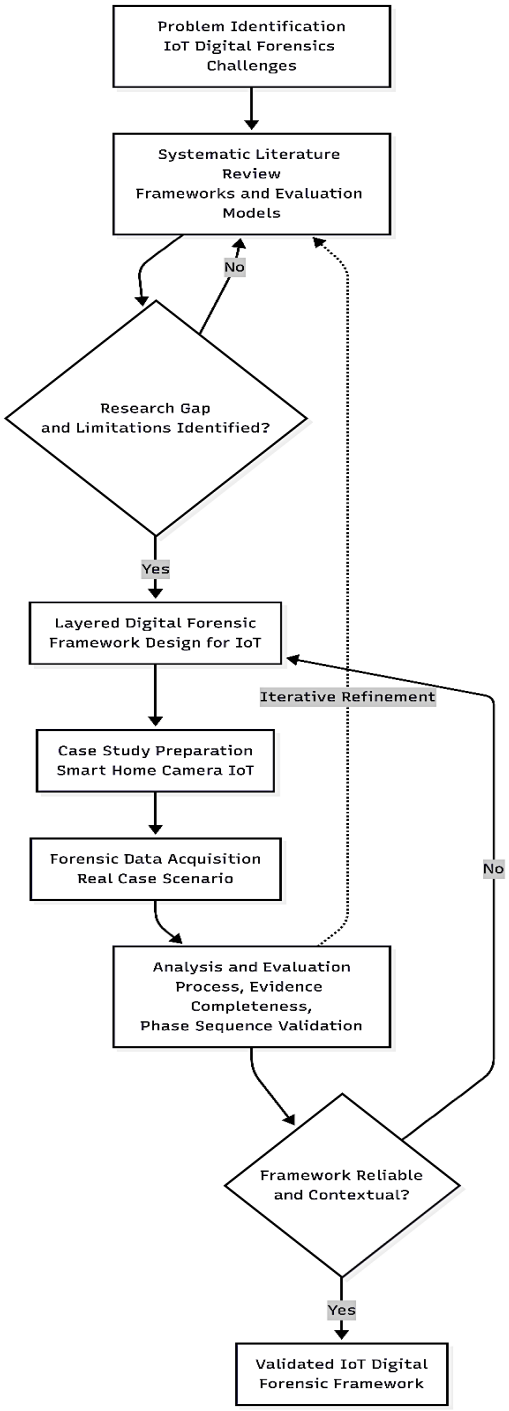

Figure 1. Research Workflow and Iterative Refinement

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

This investigation begins by identifying key issues related to current digital forensics, particularly in the IoT ecosystem. This investigation encompasses challenges related to the heterogeneity of IoT devices and the complexity of data distribution across the device layer, network layer, and application or cloud service layers. To strengthen the research's position, a systematic literature review was conducted to determine the availability of empirical studies related to relevant frameworks, including their evaluation models. This initial identification aims to identify the limitations and weaknesses of existing frameworks. Based on the results of this study, a proposed layered digital investigation framework was designed to suit the unique characteristics of the IoT ecosystem. Once the framework design was complete, the next step was to run investigation scenarios to obtain forensic data from real-world cases. In the final phase, analysis and evaluation mechanisms were implemented to assess the appropriateness of the phase sequence and the completeness of the digital evidence acquired.

This study focuses on IoT devices in the form of smart cameras used in the smart home concept. The specifications of the IoT device used are the Mi 360° smart camera with 2K resolution. This smart camera device was chosen as the object in the research scenario because it can represent the general characteristics of consumer IoT devices that are quite widely used in smart home environments. Moreover, this type of camera has a local Micro SD Card storage media that allows for the acquisition and forensic analysis of stored event recording artifacts. The details and specifications of the smart camera device can be seen in Table 1.

Table 1. Mi 360° Home Security Camera Specifications

Parameter	Specification
Product Name	Mi 360° Home Security Camera 2K
Model Number	MJSXJ09M
Resolution	2304 x 1246
Video Encoding	H.265
Lens Angle	110°
Storage	Micro SD Card, 32 GB
Network & Interface	Wi-Fi IEEE 802.11 a/b/g/n/ac, 2.4 GHz + Bluetooth 4.2

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Furthermore, to simulate a security incident in a smart home environment, this study designed a scenario under normal operational conditions. In this setup, the camera operates naturally connected to the Internet and uses cloud services through an application installed on the homeowner's device. This configuration enables systematic observation of device communication flows, and data exchanges between the camera, user application, and the cloud infrastructure, at the same time. This study focuses on interactions with cloud services during typical operational conditions for identifying potential security-relevant behavior.

Digital artifacts generated during normal IoT device interaction scenarios served as the study's data sources. Potential artifacts on the device side could include system logs, device configuration information, and metadata stored on local storage media like Micro SD cards. The data acquisition approach used in this study was logical acquisition. This logical acquisition approach was chosen due to the need to obtain data without altering the structure and integrity of the IoT device, as well as the limitations of physical access inherent in closed architecture IoT devices such as smart home cameras.

At the network layer, data is obtained from communication traffic between the smart camera device and the server, including several important pieces of information, such as network metadata, destination physical or IP addresses, transmission times, and the protocol used. Under controlled laboratory conditions, network traffic was acquired using Wireshark's passive packet capture approach, with no active attack simulation or traffic modification. Data obtained from this network layer is used to identify relevant artifacts and map normal communication patterns that occur during the interconnection between the layers.

In the meantime, at the cloud layer, the data obtained consists of several data formats such as video recordings, activity logs, user access identities, and camera activity recording synchronization metadata. Figure 2 illustrates the connectivity between the IoT layers and the data flow during activity recording.

Figure 2 presents the workings of the three main layers of the IoT ecosystem: the device layer, the network layer, and the cloud layer, as implemented in an IoT investigation scenario. The investigative approach in this study is based on dividing the IoT

infrastructure layers to map the locations of potential artifacts across the three layers. The illustration in Figure 3 allows this study to explicitly visualize the replication of data source acquisition methods, evidence collection flows, and analysis stages. Afterward, onces data is collected at each layer, the next stage is data analysis. In this phase, data analysis is conducted partially at each layer of the IoT ecosystem, utilizing a suite of digital forensic tools tailored to the characteristics of each layer of the IoT environment architecture [24], [25].

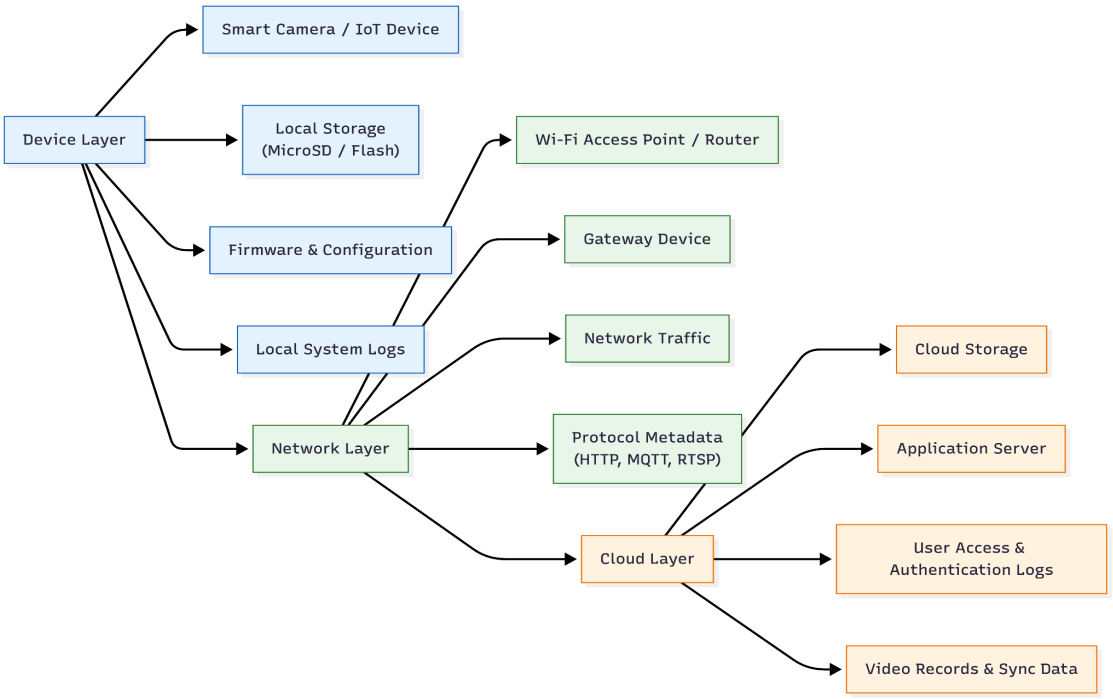

Figure 2. Layered IoT Investigation Process and Data Flow in Smart Home Camera Scenario

At the IoT device layer, analysis focuses on two main aspects: potentially relevant configuration changes and identification of system activity [26], [27]. At the network layer, analysis focuses on identifying communication patterns between IoT devices and potential intrusions or other anomalies [24], [25]. Meanwhile, at the cloud layer, analysis focuses on stored data artifacts and looks for correlations between user activities [28], [29]. The results of this analysis are then correlated to reconstruct events sequentially and chronologically. Table 2 highlights the forensic tools used at each IoT tier, providing clarity on how the proposed framework would be operationalized.

Table 2. The Tools Used per Layered Architecture

Layer	Evidence Type	Tools Used
Device Layer	Local storage artifacts, application data, system logs	Magnet AXIOM (logical extraction), Autopsy (artifact verification)
Network Layer	Traffic metadata, IP addresses, protocol logs	Wireshark (passive packet capture)
Cloud Layer	Video recordings, synchronization logs, user activity metadata	Xiaomi Home export, Vendor portal access, Magnet AXIOM artifact parsing

The final phase of this research is an evaluation of the framework based on its application to a predetermined research scenario. This evaluation focuses on the framework's capabilities and the identification of artifact sources at each layer and ensuring procedural consistency across layer. The evaluation is not focused on intrusion detection performance, but rather artifact traceability, cross-layer consistency, and evidential reliability in the context of forensic readiness. The results of this evaluation are used to assess the effectiveness of the proposed framework in supporting forensic investigations in the IoT ecosystem. This study focuses solely on IoT smart home camera devices, where each layer operates normally without any active network attacks. The research also does not overlap with advanced analysis of IoT network security exploitation.

3. RESULTS AND DISCUSSION

This section presents the design results and analysis of the proposed digital forensics investigation framework for the IoT smart camera ecosystem, arranged vertically and in layers, as shown in Figure 3. This section solely deals with empirical findings gained from the framework's application, with no interpretative comments. To provide a deeper and more comprehensive understanding of the framework's design rationale and background, the discussion focuses on three layers: the device layer, the network layer, and the cloud layer. Each of these layers represents a primary source of digital evidence connected within a single IoT ecosystem network.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

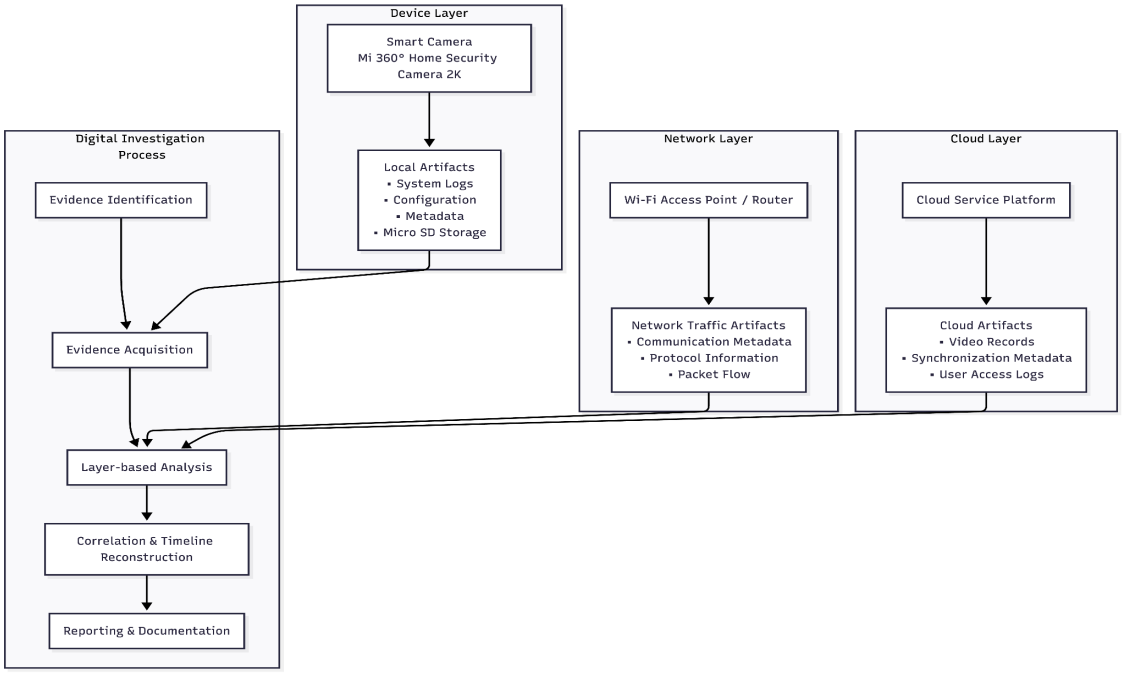

Figure 3. Proposed Framework of IoT Forensics Investigation

The framework design results emphasize the integration of heterogeneous evidence sources from each layer into a single, systematic digital forensics investigation flow. The proposed digital forensics investigation process is designed to include evidence identification, evidence acquisition, layer-based analysis, correlation and time reconstruction, and reporting and documentation. The integration of these three layers contributes to the digital forensic investigation process as a more complex and comprehensive analytical foundation than a single-source or single-layer approach, particularly in terms of event timeline reconstruction. In the discussion section, this research focuses on exploring the implications for the validity, temporal consistency, and integrity of forensic evidence. This session analyzes each integrated component within the framework according to its role and functionality.

3.1. Topology and Data Communication

The topology of the data communication flow at the network layer can be seen in Figure 4. This subsection explains in more detail the topological structure and data communication mechanisms that occur at the network layer. This understanding is crucial because the network layer acts as a connecting protocol between IoT devices, user applications, and cloud services.

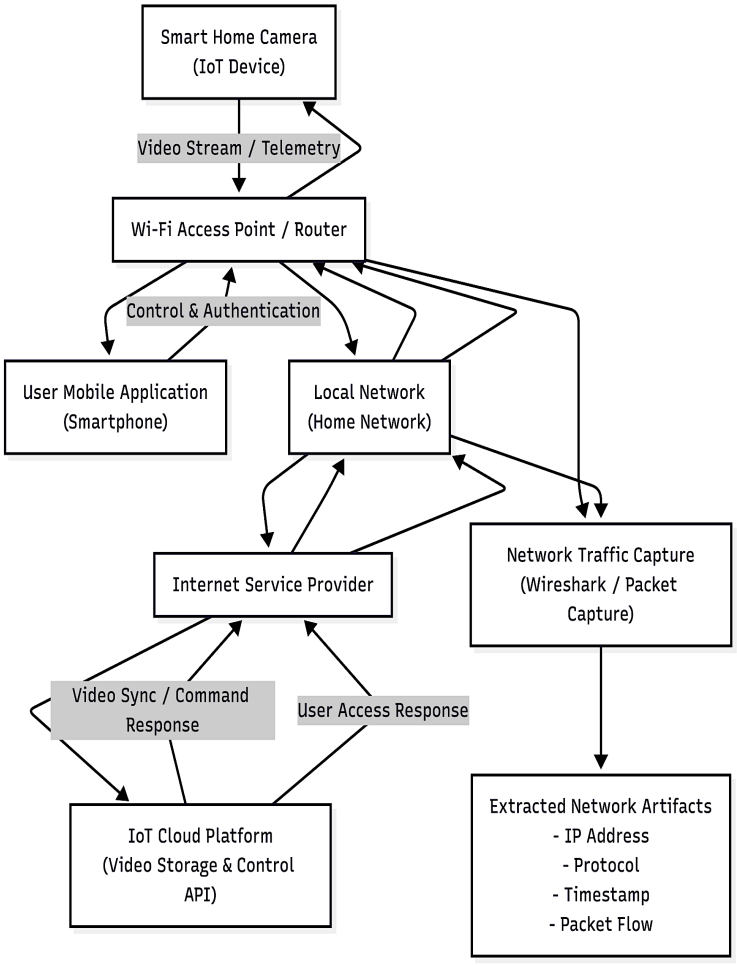

Figure 4. Topology and Data Communication in Network Layer

Referring to the network layer topology presented in Figure 5, the structure of this layer consists of six main components. Firstly, the smart home camera (IoT device) functions as the primary source of video recording and telemetry data. This camera sends data in video stream format along with periodic device status information over a wireless network. Second, the Wi-Fi access point/router serves as a local communication hub and bridge connecting all components in the network layer. Other tasks of the Wi-Fi/router include forwarding data from the smart camera to the external devices. The system includes a network that executes requests from the user application. Third, the user mobile application functions as a gateway for user authentication, video streaming monitoring, and device settings and configuration. This mobile application communicates with the camera indirectly through the router device and a cloud repository service.

Fourth, the local network, or home network, acts as an internal communication channel between IoT devices, user applications, and the router. The local network serves as the primary transit area for data packets before they reach the internet service provider. Fifth, the Internet Service Provider (ISP) acts as a liaison between the local network and external parties, specifically the cloud infrastructure. Sixth, the IoT Cloud Platform serves as a provider of video storage, data synchronization, and a control interface for cloud system devices. Meanwhile, this network layer component can use the stored video recordings, along with the resulting metadata, as digital evidence.

Next, a Wi-Fi network transmits video streaming and telemetry from the IoT smart camera to the router device through the established data communication system. In this case, the user application utilizes the Xiaomi Home App, which operates on Android, iOS, and Mi Cloud operating systems. Upon receiving an authentication request or instruction from the user application, the router then forwards the data packet to the ISP to reach the cloud platform. Upon receiving the data packet, the cloud platform sends the command response, video streaming synchronization, and user access data back to the device and application via the same path.

3.2. Digital Forensics Investigation Process Flow

This subsection presents a detailed process flow for a distributed, multi-source, and multi-component forensic investigation based on the developed framework. The digital forensic investigation process shown in Figure 5 integrates the forensic investigation stages with an analytical approach based on three main layers: the device layer, the network layer, and the cloud layer. This process flow demonstrates the interconnectedness of evidence identification, acquisition, analysis, correlation and timeline construction, examination, and reporting and documentation.

This flow also emphasizes the importance of a clear separation between the evidence collection and security stages and the analysis and interpretation of findings during the investigation. Another important aspect of this process flow is that the framework developed in this study supports cross-layer correlation for reconstructing the timeline of events and strengthening evidence interpretation to meet the principles of digital forensic validity in the context of law enforcement.

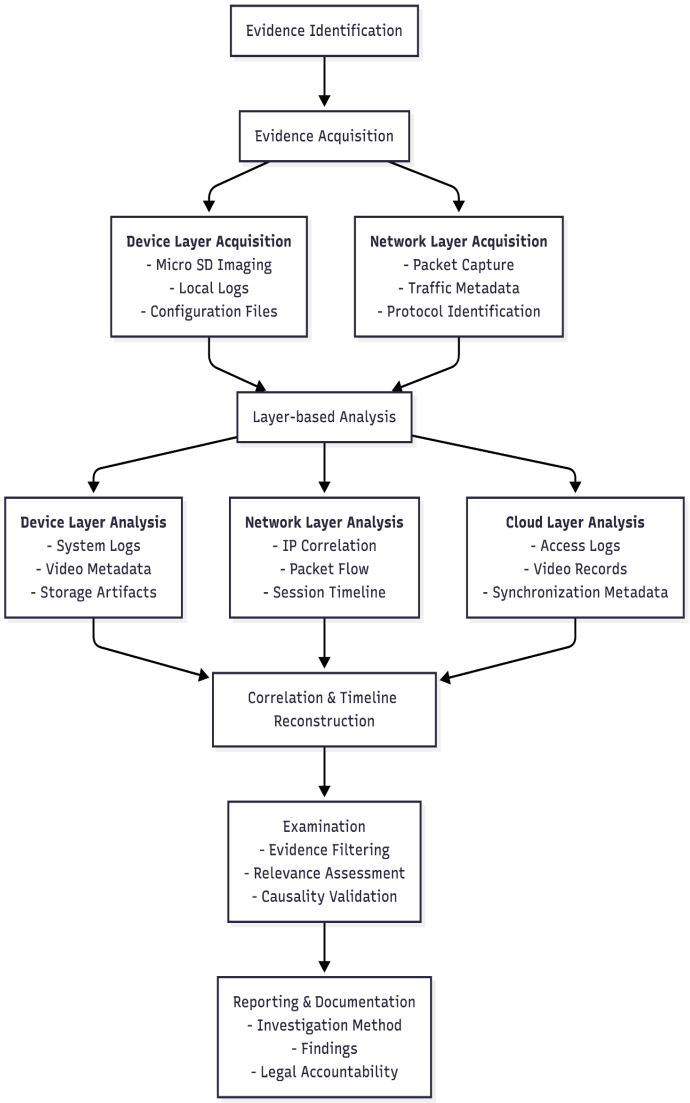

Figure 5. Digital Evidence Investigation in IoT Environment

Based on the digital forensic investigation flow in Figure 5, the process begins with the collection of potential digital evidence or artifacts. The framework proposed in this study is capable of collecting forensic data from multiple evidence sources, representing the diverse characteristics of the distributed IoT ecosystem. At the network layer, data collection is performed through network traffic capture on network communication paths using packet capture tools such as tcpdump, SolarWinds, or Nmap to scan and discover potential digital artifacts. Furthermore, digital evidence data collection is also conducted by acquiring local storage media from smart cameras, such as Micro SD cards. This multi-source approach makes the proposed framework more comprehensive and goes beyond simply scanning data packets in network-layer traffic. Next, after the data

collection or acquisition process is successful, the collected artifacts are secured using a systematic data backup mechanism. This security is known as integrity through hashing techniques and CoC management.

The next stage is extraction, where the raw data from the acquisition is extracted into an artifact format ready for analysis. For this purpose, several extraction tools are used, such as Magnet Axiom, which was used in this study to extract system and application artifacts from devices connected to cloud services. Subsequently, network traffic and communication pattern identification between IoT components can be performed using Wireshark. The result of this extraction process is a structured dataset that represents IoT component activity chronologically and based on a timeline of events.

After the artifacts are extracted, the next stage is analysis to identify anomalous activity in IoT device communication and other potential security incidents. This stage is crucial because investigators need to analyze in layers by linking findings across three layers: the device layer, the network layer, and the cloud layer. The purpose of analyzing all three layers simultaneously is to enable cross-correlation between layers to strengthen the interpretation of evidence. When a significant finding from one layer is identified, investigators can validate and strengthen the arguments for findings from other layers. The evidence or findings from the analysis stage are then filtered and further refined to determine their relevance through the next stage, examination. At this stage, investigators need to retain the value of significant findings or evidence while eliminating irrelevant findings that do not support the initial hypothesis. In this way, the examination stage can clarify causality between events and support an accurate and valid reconstruction of the timeline.

The final stage of a forensic investigation is to prepare a comprehensive and systematic report of the investigation process, including the findings documented during the analysis and examination. The general structure of an investigative report includes a brief chronology, methods, analytical results, and a structured interpretation of the evidence. This stage must ensure the investigation's findings meet the needs of the investigation in a law enforcement context.

3.3. Smart Home Camera Digital Forensics Investigation

This section systematically explains the digital forensic investigation framework proposed in this study with a home security camera as the object of the device layer. The explanation begins by outlining the process of identifying potential evidence sources, the characteristics of the device used, and the operational context of the home security camera used. Next, a detailed description is carried out on the stages of acquisition and preservation of digital artifacts. Preservation techniques to maintain the authenticity and integrity of evidence are presented, and a discussion of the traceability of digital evidence on the device layer device is simultaneously carried out. The next discussion is the analysis and examination of cross-layer artifacts to reconstruct the chronology of the incident with a scenario of suspected theft at a residential location.

C.1 Phase 1: Case and Digital Evidence Identification

In this phase, identifying digital evidence is necessary to establish the context for a digital forensic investigation within the IoT ecosystem. Simultaneously, this phase also defines a case scenario, a simulated burglary incident in a residential environment recorded by a Mi 360° home security camera. This IoT smart home camera was selected based on its general characteristics, which rely on network connectivity and cloud services for its operation.

The case context discussed in this study was established to ensure the digital forensic investigation process adheres to the principles and process flow of the framework developed in this study. In the designed case scenario, the investigation involves several key components: the IoT device, specifically the smart home camera, as the primary source of visual recordings; a supporting application device, a smartphone, to control the camera's functions and configuration; a wireless network environment as a data communication medium; and cloud services for data storage and synchronization. The details of the case study context and the components involved are presented in Table 3 to provide a basic understanding of the implementation phase.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Table 3. Case Identification and Categories

Category	Description
Case Scenario	Simulation of a burglary incident recorded by a Mi 360° Home Security Camera installed in a residential environment.
IoT Device	Mi 360° Home Security Camera 2K (Model: MJSXJ09CM). Functions as a primary evidence source.
Companion Device	Samsung Galaxy S24 FE smartphone running the Xiaomi Home App.
Network Environment	Local Wi-Fi 2.4 GHz connecting both the IoT camera and smartphone.
Cloud Service	Mi Cloud for synchronization and storage of recorded videos.
Expected Evidence	Local video recordings, device logs, Wi-Fi configuration, and application activity data.

To integrate the digital evidence identification process hierarchically and systematically, in this phase the forensic investigation is classified into three domains: device forensics at the device layer, network forensics at the network layer, and application forensics at the cloud layer. The identification phase focuses on finding evidence and the relationship between evidence sources at the three main layers defined in the proposed framework of this study. An illustration of the case scenario built in this study to test the framework is shown in Figure 6.

The case scenario in this study begins with a burglary incident in a residential neighborhood, which serves as the starting point for the investigation. This incident is monitored by the Mi 360 smart home camera, which features motion detection and automatic recording. This then serves as the primary source of digital evidence at the device level. During the incident, the camera automatically triggers video recording of the incident, which is stored locally on a Micro SD card as a system log. In parallel, the recorded incident data and resulting metadata are also sent via the local Wi-Fi network to the home access point or router. This simultaneous communication flow creates artifacts at the network layer, including internal network traffic, ISP connections, and data transmission patterns between devices and external services.

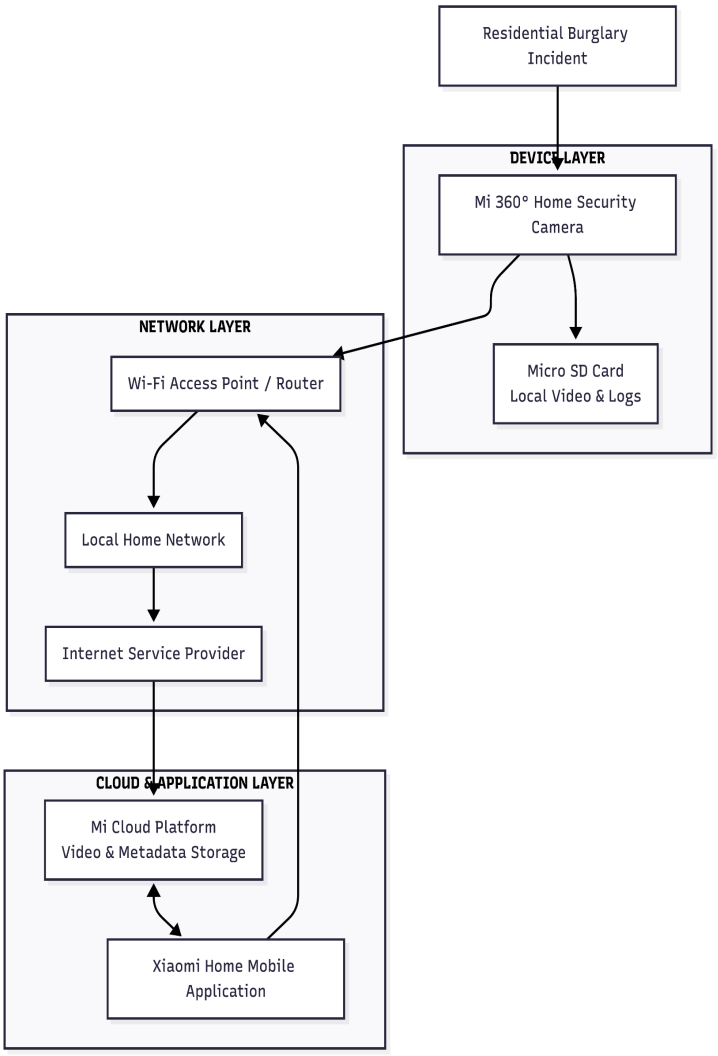

Figure 6. Case Scenario and Digital Evidence Sources

The case scenario in this study begins with a burglary incident in a residential neighborhood, which serves as the starting point for the investigation. This incident is monitored by the Mi 360 smart home camera, which features motion detection and automatic recording. This then serves as the primary source of digital evidence at the device level. During the incident, the camera automatically triggers video recording of the incident, which is stored locally on a Micro SD card as a system log. In parallel, the recorded incident data and resulting metadata are also sent via the local Wi-Fi network to the home access point or router. This simultaneous communication flow creates artifacts at the network layer, including internal network traffic, ISP connections, and data transmission patterns between devices and external services.

Subsequently, the recorded video data and metadata transmitted through the network layer are sent to the Mi Cloud platform via the cloud application layer for storage and synchronization. Through the Xiaomi Home app on a smartphone, users can access the recordings and configure the device. During this interaction, additional artifacts are generated at the cloud and application layers. The interconnections between the components at each layer form a distributed IoT ecosystem with digital resources and generate a distributed digital footprint.

To ensure the focus of the case scenarios in this study is focused and evidence-based, potential digital artifact sources at each layer of the IoT ecosystem were mapped. This mapping aims to link the case scenarios to the types of artifacts produced, including identifying evidence characteristics and different acquisition methods. The results of this identification are then used as a basis for determining digital evidence acquisition and preservation strategies. Details of the sources and types of digital artifacts relevant to the case studies can be seen in Table 4.

Table 4. Digital Artifact Identification Accross Device, Network, and Application Layers

Forensic Layer	Evidence Origin	Artifact Types	Forensic Acquisition Technique
Device Layer	Mi 360° Camera (physical device, firmware, internal SD card)	- Device log files - Local video recordings - Configuration tion information (Wi-Fi SSID, saved credentials) - Embedded firmware and operating system	Obtained through physical acquisition or imaging of SD card memory.
Network Layer	Router / Wi-Fi used by the camera	- Streaming traffic data - Communication protocols (RTSP, HTTP, MQTT, etc.) - Connection metadata (IP, port, and timestamp)	Captured using a packet sniffer (e.g. Wireshark) while the device is active.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Forensic Layer	Evidence Origin	Artifact Types	Forensic Acquisition Technique
Cloud/Application Layer	Xiaomi Home App (Android/iOS), Mi Cloud	- Application activity logs (logins, configurations) - Application cache (credentials, tokens, camera settings) - Cloud backups - API call logs	-Application activity logs (logins, configurations) -Application cache (credentials, tokens, camera settings) - Cloud backups - API call logs

Based on the identification results shown in Table 3, the key artifacts identified include local video recordings, camera device configurations, network communication traffic, and Xiaomi Home app activity logs from user devices and cloud services. These diverse artifacts represent digital evidence obtained from three main layers, each contributing to the evidence source and complementing each other to reconstruct the context of the events outlined in the scenario in this study. This initial identification output serves as a basis for selecting artifacts that are directly related and relevant to the case context, as well as a foundation for ensuring that the subsequent digital evidence acquisition and preservation process is conducted in a focused, valid, and scientifically accountable manner.

C.2 Phase 2: Acquisition and Preservation

The acquisition and preservation phase focuses on collecting and preserving digital evidence from the previous identification phase. In this study, the acquisition process utilizes the Magnet Axiom forensic tool for logical data extraction from a Samsung Galaxy S24 FE smartphone, a user-facing communication device running the Xiaomi Home app. In the pre-acquisition phase, verification of the smartphone's condition is crucial before the acquisition process, including checking its power supply, internet network connectivity, and operating system version. Next, investigators need to determine an appropriate acquisition method. In this scenario, the logical data acquisition method was chosen to avoid the risk of data tampering. Proper preparation of the forensic tools and environment, including the Magnet Axiom configuration and the source storage media for the acquisition results, is essential. At the same time, initial documentation of the

device's condition and recording of information are essential components of the Code of Conduct.

The acquisition subphase focuses on imaging and logical data extraction from the smartphone without actively modifying the system. Artifacts collected through the Xiaomi Home app can include activity logs, temporary local storage caches, system configurations, and synchronized metadata. To minimize the risk of evidence loss or even compromised integrity, the extraction process must be carried out systematically and in a controlled manner. Furthermore, the automatic generation of cryptographic hash values, such as MD5 and SHA-1, is systematically recorded in the CoC document. Details of the acquisition results and the types of artifacts obtained from the three main layers: the device layer, the network layer, and the cloud/application layer, can be seen in Figure 7.

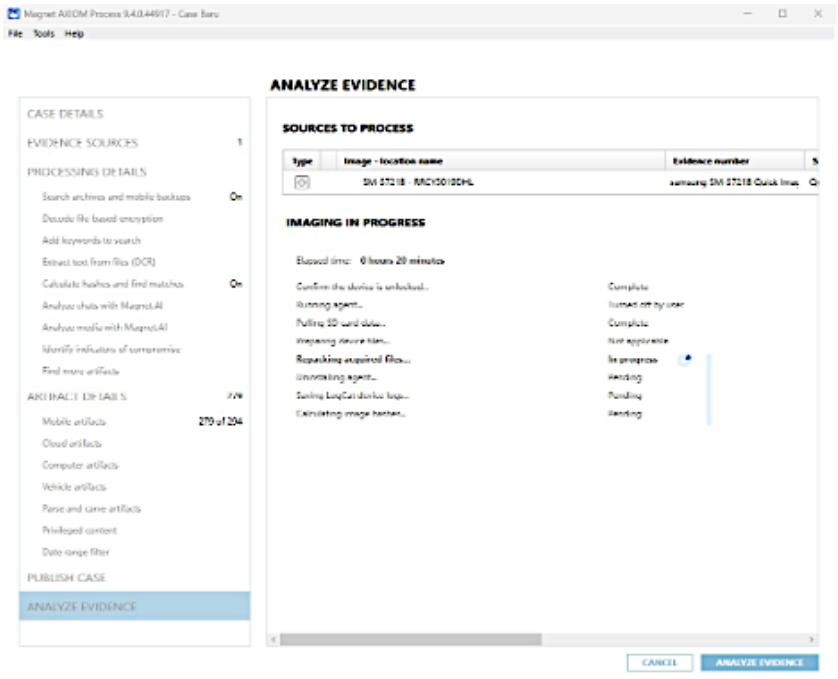

Figure 7. Digital Evidence Acquisition and Imaging Process

In the post-acquisition subphase, a crucial step is to verify the integrity of the acquired digital evidence by checking the conformity of the generated hash values. Furthermore, the acquisition results must be stored with extreme care and security, isolating them from possible electronic or mechanical alteration. Therefore, after a successful

acquisition, it is recommended that the original copy of the acquired evidence be saved and preserved so that investigators can extract and analyze the working copy of the digital evidence.

Moreover, in this phase, the digital evidence acquisition process is systematically conducted across three main layers to ensure the completeness and traceability of the digital evidence. At the device layer, forensics is performed by logical extraction of the smartphone device of the user or smart camera administrator. The primary focus of this investigation is the search for Xiaomi Home app artifacts, cache data, and local device configuration. At the network layer, the focus is on capturing communication metadata between the smart camera and the network protocol. The source of digital evidence comes from the Wi-Fi router connected to the camera, including traffic information and connection timestamps.

At the application/cloud layer, data sources come from Xiaomi Home app artifacts and the Mi Cloud cloud service. Some potential evidence includes user activity logs and other cloud-based artifacts. Meanwhile, the extraction process is carried out logically according to the service's characteristics. A summary of evidence sources, acquisition methods, and mechanisms for preserving the integrity of digital artifacts is presented in Table 5.

Table 5. Summary of Acquisition and Preservation Processes

Forensic Layer	Evidence Origin	Artifact Types	Forensic Acquisition Technique
Device Layer	Samsung Galaxy S24 FE	Logical extraction using Magnet AXIOM	MD5/SHA-1 hash verification
Network Layer	Router Wi-Fi (Camera Mi 360°)	Packet capture using Wireshark	Timestamp and log validation
Cloud/Application Layer	Application of Xiaomi Home and Mi Cloud	Logical extraction	Encrypted storage and procedural documentation

Based on the acquisition and preservation results presented in Table 5, it can be concluded that the acquisition phase generated verified forensic images and application data. Thus, this finding is deemed to have met the requirements for authenticity and integrity and can be continued to the next stage.

C.3 Phase 3: Analysis and Examination

The analysis and examination phase focuses on interpreting and validating artifacts resulting from the acquisition and preservation of digital evidence. The primary objective of this phase is to ensure the integrity, originality, and relevance of key findings at each level. During this phase, each artifact is examined based on several crucial attributes, such as the consistency of hash values and metadata, ensuring the data has not been tampered with. Correlations based on the analysis and examination of digital evidence then serve as the basis for reconstructing the alleged residential burglary incident, as described in the case scenario section.

C.3.1 Verification of Source Devices and IoT Context

The analysis phase begins with verifying the source device acquired and extracted from Magnet AXIOM software. The smartphone device was identified as a Samsung Galaxy S24 FE with model SM-S721B/DS, and the device serial number was consistent with the acquisition and CoC records. This smartphone device is a companion device directly connected to the Mi 360 Home Security Camera application. Thus, this verification establishes a consistent and related forensic link between the physical device, application, and IoT ecosystem.

C.3.2 Device and Application-level Examination

In this phase, artifacts from connected devices, including applications, are examined at each layer. Various device artifacts include information about the operating system used, configured time zones and geographic regions, and device identities and parameters. On the application side, artifacts include application metadata, including user activity records, data storage structures, and synchronization results with IoT cameras and cloud services.

C.3.3 Media Artifact and Metadata Analysis

This stage focuses on the analysis of video artifacts as the primary evidence of the incident, extracted from the Xiaomi Home application, as can be seen in Figure 8. The results of this extraction are video frame representations that support the analysis of the incident content. Methodologically, this subsection aims to explain and interpret the results of the multimedia artifact examination, metadata analysis, and issues related to ensuring the integrity of the evidence.

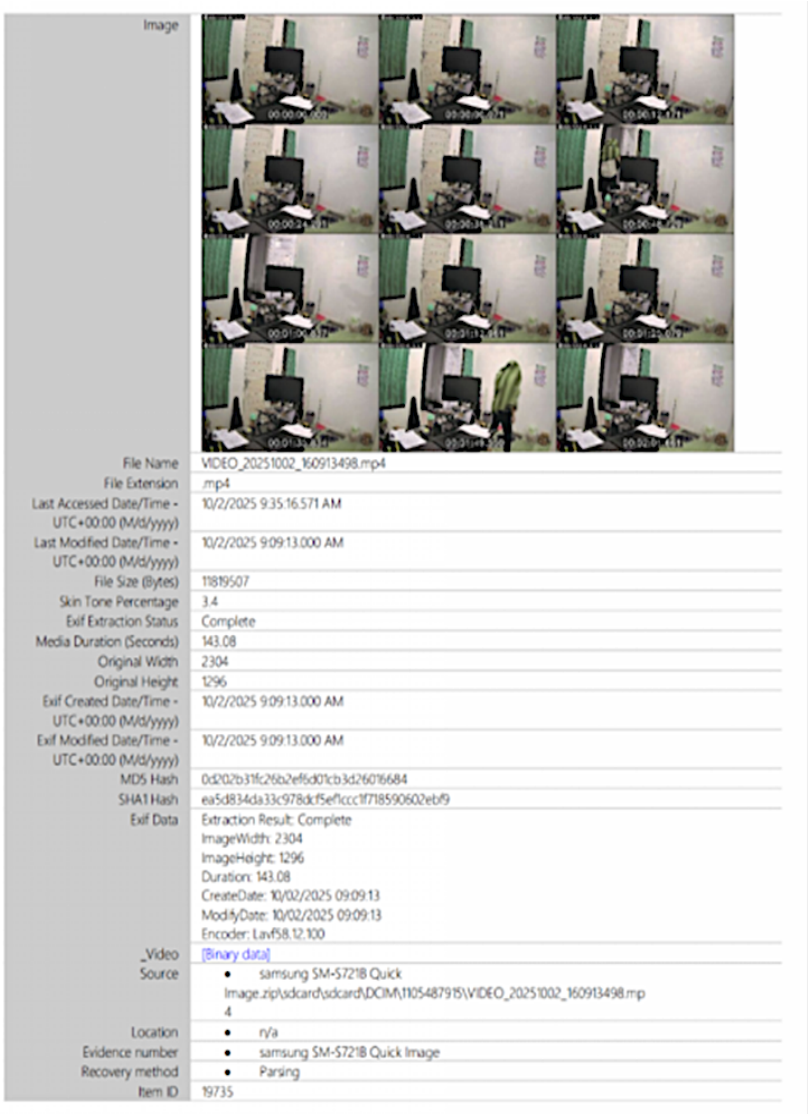

Figure 8. Detailed Attributes of Extracted Video Evidence

Details related to artifact attributes from the extraction and analysis results can be seen in Table 6.

Table 6. Forensic Attributes of Video Media Artifacts

Attribute Categories	Parameter	Value/Description
File Identity	File Name	VIDEO_20251002_160913498.mp4
	File extension	.mp4
	Artefact type	Media Video
	Extraction status	Complete
	Data format	Binnary data
Evidence Source	Device source	Samsung Galaxy S24 FE
	Device model	SM-S721B
	Acquisition method	Logical extraction (Magnet AXIOM)
	Image source	Samsung SM-S721B Quick Image
	File location	/sdcard/DCIM/10548789/
	Evidence number	Samsung SM-S721B Quick Image
	Item ID	19735
	Recovery method	Parsing
Time Attribute (Timestamp)	Last accessed date/time (UTC)	02/10/2025 09:35:16.571
	Last modified date/time (UTC)	02/10/2025 09:09:13.000
	EXIF created date/time (UTC)	02/10/2025 09:09:13
Technical Characteristics of Media	Video duration	143.08 seconds
	Video resolution	2304 × 1296 pixel
	Skin tone percentage	3.4%
	Encoder	Lavf 58.12.100
	EXIF data status	Extraction results complete
Cryptographic Integrity	MD5 hashes	0d20b31c26b26b60fc3b260f684
	SHA-1 hashes	ea5884de335c9780b65bcec17859052be9

Based on the forensic attributes of the video media artifacts presented in Table 5, it can be explained that the video artifact in .mp4 format was fully obtained at the device layer,

with the extraction status complete, from a Samsung Galaxy S24 FE smartphone. To fully recover potential artifacts, the acquisition stage employed a logical extraction method using the Magnet AXIOM tool to maintain data authenticity and integrity, particularly at the device layer. At the application or cloud layer, the physical storage on the device layer, managed by the Xiaomi Home App at the application layer, is located at /sdcard/DCIM/10548789/, with consistent EXIF file timestamps and modified times, indicating no modifications after the video was recorded at the incident location. While there is a difference in the last accessed time, this indicates that access activity at the application or cloud layer has not altered the file content. Furthermore, MD5 and SHA-1 integrity values verify the integrity of the artifact at the device layer and the authenticity and validity of the analysis at the application layer.

C.3.4 Cross-Layer Correlation

In addition to investigating important artifacts across the three layers, it is also important to emphasize the correlation between layers (device, network, and cloud) to establish a complete evidence linkage. First, artifacts obtained from the application/cloud layer connect incident event recordings with IoT devices, namely home security cameras. Second, artifact findings, especially timestamps of interactions and communications between layers, can be utilized to reconstruct the scene and chronology of events. Third, the chain of evidence and evidence integrity through hash values (MD5 and SHA-1) act as validators of the CoC documentation. Fourth, the final results of the analysis presented in this study indicate that the artifacts are valid, consistent, and accountable, so their validity can be accounted for scientifically and legally.

In the discussion section, this paper highlights three key points that spark different perspectives based on the findings and results of the investigation. First, the study results demonstrate that a layer-based digital forensic investigation framework has proven capable and valid in addressing the complexity and heterogeneity of the IoT ecosystem. The framework's design, with its specific separation of three layers—the device layer, the network layer, and the cloud layer—facilitates the identification of data sources, the discovery of potential artifacts, such as video recordings and device interconnection logs, and the reconstruction of the flow of events or criminal incidents. Second, the consistency of the metadata structure, timestamps, and hash values generated in video recording artifacts successfully strengthens the validity and integrity

of digital evidence. The presence of the cloud layer serves as a support for interpreting the historical context that complements the evidence at the device layer. Third, the layered IoT architecture design can facilitate traceability of the investigative process without compromising the principles of international forensic standards, particularly regarding the recording of evidence events and the integrity of digital evidence for legal purposes. However, this study has limitations in terms of the scope of IoT devices used and the scenarios implemented. Therefore, further development is needed to test the framework using a variety of IoT devices and the complexity of the case studies.

4. CONCLUSION

Digital forensic investigations in the IoT ecosystem require a systematic approach that integrates across layers, namely the device layer, network layer, and cloud layer. Obtaining complete digital artifacts while maintaining data integrity and evidence traceability is possible using logical acquisition methods. The analysis results conducted in this study successfully reconstructed the chronology of incident events according to the alleged crime scenario based on video media findings, metadata, and various other technical attributes, including timestamps. The design of three main layers in the proposed framework successfully linked the role of each artifact, including the source device, the recording process, and the resulting media artifact. Furthermore, the validity of digital evidence during the forensic investigation process was verified through valid cryptographic integrity (MD5 and SHA-1). This study demonstrates the suggested framework's actual usefulness as a core forensic preparedness model for systematic evidence collection and cross-layer artifact correlation in IoT contexts. Ultimately, the layer-based digital forensic investigation framework proposed in this study is relevant for application in forensic investigations in complex and evolving IoT environments.

The primary contribution of this study is a structured case study of a smart home camera, which is intended to propose scientific framework and confirm its practical feasibility. Further research direction should assess the framework's compatibility with automated forensic preparedness and monitoring systems, and investigate interactions with real-world incident datasets. Furthermore, the evaluation of operational resilience and scalability within multi-device IoT ecosystems is crucial.

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to the Ministry of Research, Technology, and Higher Education of the Republic of Indonesia (KEMENDIKTISAINTEK) for the financial support provided through the Student Thesis Research Grant (PTM) scheme, under contract number: 047/DirDPPM/70/DPPM/PTM-KEMDIKTISAINTEK/VI/2025.

REFERENCES

[1] A. Salam, "Internet of Things for Sustainable Community Development: Introduction and Overview," in *Springer Nature*, Springer, Cham, 2024, pp. 1–31. doi: 10.1007/978-3-031-62162-8_1.

[2] S. Mishra and A. K. Tyagi, "The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications," in *Springer Nature*, Springer, Cham, 2022, pp. 105–135. doi: 10.1007/978-3-030-87059-1_4.

[3] A. Ullah, S. M. Anwar, J. Li, and L. Nadeem, "Smart cities: the role of Internet of Things and machine learning in realizing a data-centric smart environment," *Complex & Intelligent Systems*, vol. 10, no. 1, pp. 1607–1637, Feb. 2024, doi: 10.1007/s40747-023-01175-4.

[4] H. H. Alshammari, "The internet of things healthcare monitoring system based on MQTT protocol," *Alexandria Engineering Journal*, vol. 69, pp. 275–287, Apr. 2023, doi: 10.1016/j.aej.2023.01.065.

[5] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-Based Methods for Cyber Attacks Detection in IoT Systems: A Survey on Methods, Analysis, and Future Prospects," *Electronics (Basel)*, vol. 11, no. 9, p. 1502, May 2022, doi: 10.3390/electronics11091502.

[6] I. Coston, E. Plotnizky, and M. Nojoumian, "Comprehensive Study of IoT Vulnerabilities and Countermeasures," *Applied Sciences*, vol. 15, no. 6, p. 3036, Mar. 2025, doi: 10.3390/app15063036.

[7] Y. R. Siwakoti, M. Bhurtel, D. B. Rawat, A. Oest, and R. C. Johnson, "Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks, and Countermeasures," *IEEE Internet Things J.*, vol. 10, no. 13, pp. 11224–11239, Jul. 2023, doi: 10.1109/JIOT.2023.3252594.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[8] M. K. Kagita, N. Thilakarathne, T. R. Gadekallu, P. K. R. Maddikunta, and S. Singh, "A Review on Cyber Crimes on the Internet of Things," in *Springer Nature*, Springer, Singapore, 2021, pp. 83–98. doi: 10.1007/978-981-16-6186-0_4.

[9] F. Neves, R. Souza, J. Sousa, M. Bonfim, and V. Garcia, "Data privacy in the Internet of Things based on anonymization: A review," *J. Comput. Secur.*, vol. 31, no. 3, pp. 261–291, May 2023, doi: 10.3233/JCS-210089.

[10] E. Rodríguez, B. Otero, and R. Canal, "A Survey of Machine and Deep Learning Methods for Privacy Protection in the Internet of Things," *Sensors*, vol. 23, no. 3, p. 1252, Jan. 2023, doi: 10.3390/s23031252.

[11] M. A. Albreem, A. M. Sheikh, M. J. K. Bashir, and A. A. El-Saleh, "Towards green Internet of Things (IoT) for a sustainable future in Gulf Cooperation Council countries: current practices, challenges and future prospective," *Wireless Networks*, vol. 29, no. 2, pp. 539–567, Feb. 2023, doi: 10.1007/s11276-022-03133-3.

[12] N. J. Singh, N. Hoque, Kh. R. Singh, and D. K. Bhattacharyya, "Botnet-based IoT network traffic analysis using deep learning," *SECURITY AND PRIVACY*, vol. 7, no. 2, Mar. 2024, doi: 10.1002/spy2.355.

[13] A. O. Akinbi, "Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks," *WIREs Forensic Science*, vol. 5, no. 6, Nov. 2023, doi: 10.1002/wfs2.1496.

[14] M. Kim, Y. Shin, W. Jo, and T. Shon, "Digital forensic analysis of intelligent and smart IoT devices," *J. Supercomput.*, vol. 79, no. 1, pp. 973–997, Jan. 2023, doi: 10.1007/s11227-022-04639-5.

[15] V. R. Kebande and A. I. Awad, "Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions," *ACM Comput. Surv.*, vol. 56, no. 5, pp. 1–37, May 2024, doi: 10.1145/3635030.

[16] H. N. Fakhouri, M. A. AlSharaiah, A. k. Al hwaitat, M. Alkalaileh, and F. F. Dweikat, "Overview of Challenges Faced by Digital Forensic," in *2024 2nd International Conference on Cyber Resilience (ICCR)*, IEEE, Feb. 2024, pp. 1–8. doi: 10.1109/ICCR61006.2024.10532850.

[17] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1–13, 2023, doi: 10.1016/j.iotcps.2022.12.003.

[18] C. Bayılmış, M. A. Ebleme, Ü. Çavuşoğlu, K. Küçük, and A. Sevin, "A survey on communication protocols and performance evaluations for Internet of Things,"

Digital Communications and Networks, vol. 8, no. 6, pp. 1094–1104, Dec. 2022, doi: 10.1016/j.dcan.2022.03.013.

[19] M. Mansour *et al.*, "Internet of Things: A Comprehensive Overview on Protocols, Architectures, Technologies, Simulation Tools, and Future Directions," *Energies (Basel)*, vol. 16, no. 8, p. 3465, Apr. 2023, doi: 10.3390/en16083465.

[20] A. A. Ahmed, K. Farhan, W. A. Jabbar, A. Al-Othmani, and A. G. Abdulrahman, "IoT Forensics: Current Perspectives and Future Directions," *Sensors*, vol. 24, no. 16, p. 5210, Aug. 2024, doi: 10.3390/s24165210.

[21] G. Liang, J. Xin, Q. Wang, X. Ni, and X. Guo, "Research on IoT Forensics System Based on Blockchain Technology," *Security and Communication Networks*, vol. 2022, pp. 1–14, Jun. 2022, doi: 10.1155/2022/4490757.

[22] M. Williams, I. Emeteveke, O. J. Adeyeye, and O. Emehin, "Enhancing Data Forensics through Edge Computing in IoT Environments," *International Journal of Research Publication and Reviews*, vol. 5, no. 10, pp. 2970–2985, Oct. 2024, doi: 10.55248/gengpi.5.1024.2903.

[23] A. A. Maftei, A. Lavric, A. I. Petrariu, and V. Popa, "Massive Data Storage Solution for IoT Devices Using Blockchain Technologies," *Sensors*, vol. 23, no. 3, p. 1570, Feb. 2023, doi: 10.3390/s23031570.

[24] A. Jahangeer, S. U. Bazai, S. Aslam, S. Marjan, M. Anas, and S. H. Hashemi, "A Review on the Security of IoT Networks: From Network Layer's Perspective," *IEEE Access*, vol. 11, pp. 71073–71087, 2023, doi: 10.1109/ACCESS.2023.3246180.

[25] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A Survey of IoT Security Based on a Layered Architecture of Sensing and Data Analysis," *Sensors*, vol. 20, no. 13, p. 3625, Jun. 2020, doi: 10.3390/s20133625.

[26] A. Raj and S. D. Shetty, "IoT Eco-system, Layered Architectures, Security and Advancing Technologies: A Comprehensive Survey," *Wirel. Pers. Commun.*, vol. 122, no. 2, pp. 1481–1517, Jan. 2022, doi: 10.1007/s11277-021-08958-3.

[27] A. Cañete, M. Amor, and L. Fuentes, "Supporting IoT applications deployment on edge-based infrastructures using multi-layer feature models," *Journal of Systems and Software*, vol. 183, p. 111086, Jan. 2022, doi: 10.1016/j.jss.2021.111086.

[28] M. Aldossary, "Multi-Layer Fog-Cloud Architecture for Optimizing the Placement of IoT Applications in Smart Cities," *Computers, Materials & Continua*, vol. 75, no. 1, pp. 633–649, 2023, doi: 10.32604/cmc.2023.035414.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[29] A. Morchid, R. El Alami, A. A. Raezah, and Y. Sabbar, "Applications of internet of things (IoT) and sensors technology to increase food security and agricultural Sustainability: Benefits and challenges," *Ain Shams Engineering Journal*, vol. 15, no. 3, p. 102509, Mar. 2024, doi: 10.1016/j.asej.2023.102509.