

Towards Digital Forensics 4.0: A Multilevel Digital Forensics Framework for Internet of Things (IoT) Devices

Yaman Salem

Department of Natural Engineering and Technology Sciences, Arab American University (AAUP), Ramallah, Palestine
E-mail: y.salem3@student.aaup.edu
ORCID iD: <https://orcid.org/0000-0002-4737-5112>

Majdi Owda

Faculty of Data Science, Arab American University (AAUP), Ramallah, Palestine
E-mail: majdi.owda@aaup.edu
ORCID iD: <https://orcid.org/0000-0002-7393-2381>

Amani Yousef Owda*

Department of Natural Engineering and Technology Sciences, Arab American University (AAUP), Ramallah, Palestine
E-mail: amani.owda@aaup.edu
ORCID iD: <https://orcid.org/0000-0002-6104-9508>

*Corresponding author

Received: 10 December, 2023; Revised: 20 February, 2024; Accepted: 05 March, 2024; Published: 08 April, 2024

Abstract: The Internet of Things (IoT) driven Industrial Revolution 4.0 (IR4.0) and this is impacting every sector of the global economy. With IoT devices, everything is computerized. Today's digital forensics is no longer limited to computers, mobiles, or networks. The current digital forensics landscape demands a significantly different approach. The traditional digital forensics frameworks no longer meet the current requirements. Therefore, in this paper, we propose a novel framework called "Multi-level Artifact of Interest Digital Forensics Framework for IoT" (MAoIDFF-IoT). The keynote "Multi-level" aims to cover all levels of the IoT architecture. Our novel IoT digital forensics framework focuses on the Artifact of Interest (AoI). Additionally, it proposes the action/detection matrix. It encompasses the advantages of the previous frameworks while introducing new features specifically designed to make the framework suitable for current and future IoT investigation scenarios. The MAoIDFF-IoT framework is designed to face the challenges of IoT forensic analysis and address the diverse architecture of IoT environments. Our proposed framework was evaluated through real scenario experiments. The evaluation of the experimental results reveals the superiority of our framework over existing frameworks in terms of usability, inclusivity, focus on the (AoI), and acceleration of the investigation process.

Index Terms: Industrial Revolution 4.0 (IR4.0), Internet of Things (IoT), Artifact of Interest (AoI), Multi-level Forensics, IoT Forensics 4.0, Action/Detection (A/D) Matrix, Framework.

1. Introduction

In the fourth industrial revolution (IR 4.0), humans, governance, and businesses are impacted with the four items being IoT, cloud computing, cybersecurity, and big data [1,2]. Hence, the digital forensic community should be prepared to face IR 4.0 challenges [3]. One of the main challenges is dealing with sophisticated Internet of Things (IoT) environments [3,4]. The Internet of Things (IoT) refers to all the devices connected to the internet using various standardized communication [5]. IoT is applied to healthcare, education, smart cities, smart home, industry, markets, transportation, vehicles, and supply chain [5]. IoT devices could bring threats from less secure public networks to private networks. These threats include data leakage, identity theft, denial of service (DOS), phishing, and stealing personal data [3,4,6–9]. Many traditional digital forensics techniques and frameworks are not sufficient to conduct reliable digital investigations on IoT devices [2], due to several reasons such as the huge volume of extracted and

generated data from IoT environments for investigation analysis [4]. In addition, the increased number of devices needed to be analyzed in IoT environments, and the variety of data structures and standards for IoT devices [3,4]. With the lots of proposed digital forensics frameworks in the literature, there are no common standards or rules for digital forensics investigation targeting the IoT environment [10]. Some proposed frameworks are too general, while others frameworks focus on a specific scenario [11]. This presents a need to develop a successful IoT digital forensics framework and implement best practices when carrying out IoT investigations to fit the unique characteristics of IoT systems [2].

This paper aims to develop a novel IoT digital forensic framework. The main research question is: What is the most effective framework for IoT digital forensics that fits the era of IR 4.0? This study makes several contributions to the field of IoT forensics. The novel framework for IoT digital forensics, named “Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT),” was proposed. The proposed framework was initially designed based on literature analysis. It was then fine-tuned using an experimental approach to align with the characteristics of the IoT. Additionally, it was compared to previous frameworks. Moreover, MAoIDFF-IoT proposed the Action/Detection (A/D) matrix, which is used to find artifacts of interest based on the actions performed during the experimental testing. Four types of extracted artifacts were proposed, including Missed Artifact (MA), No Artifact (NA), Useful Artifact (UA), and Artifact of Interest (AoI). The proposed framework was evaluated through real scenarios case studies.

This paper is structured as follows: Section 2 includes the background of IoT architecture, a comparison between IoT forensics and traditional forensics, and the challenges of IoT forensics. In addition, frameworks and case studies on IoT forensics were explored. Section 3 describes the methodology used and presents the proposed framework. In Section 4, the implementation and experiment section, the proposed framework was evaluated through three case studies. This is followed by the results and discussions in Section 5, which elucidate the distinguishing features and novel aspects of the proposed framework in comparison to previous frameworks. Moreover, it stated the limitations of this research. Finally, the conclusion and future work are stated in Section 6.

2. Background

This section includes four subsections: (2.1) introduces the IoT architecture, and (2.2) discusses IoT digital forensics versus traditional digital forensics. (2.3) explores the challenges of IoT digital forensics in the era of IR 4.0, including challenges at three levels of IoT architecture: physical, network, and application levels. Finally, (2.4) reviews studies and frameworks related to IoT digital forensics.

2.1. IoT Architecture

The general IoT architecture can be divided into three levels: (1) physical or device, (2) network, and (3) application [12-16]. Invented levels stated in the literature such as processing [12], and middleware layers [17,18]. (1) The physical or the device level is the bottom layer in the IoT architecture. It contains devices such as actuators, sensors, and microcontrollers. It aims to collect data from physical devices. It connects to an IoT network to measure, process, and transmit information into the upper layer via interfaces [12-15]. (2) The network level or named the transmission level is the middle layer in the IoT architecture. It includes communication technologies (WiFi, Bluetooth, etc.), devices (switching, gateway, etc.), and protocols needed for transmitting data between the physical level and application level [13]. (3) The application level, or the business level, is the top layer in IoT architecture, it receives data from the network level to provide the needed services. It contains the interface for the services offered to the end users [12,14-16]. The application level includes the application programming interfaces (APIs) that collect, analyze usage statistics, control access, and report performance. In addition, the application level might include the cloud service, the mobile app, and web dashboards that control IoT devices [13].

2.2. IoT Digital Forensics vs Traditional Digital Forensics

The traditional digital forensic phases can be applied to IoT forensics in different ways [19–29] as IoT forensics is considered part of digital forensics [6]. However, IoT digital forensics has multi-levels that should be considered in the IoT investigation, being device, network, and application levels [6], [31-33]. Therefore, IoT forensics presents several

Table 1. IoT digital forensics vs traditional digital forensics

Comparison Item	IoT Digital Forensics	Traditional Digital Forensics
Number of Devices	Depending on the IoT environment, this may exceed billion of IoT devices [31]	A few devices, typically, computers, USB, or/and other related devices [3]
Source of Evidence	IoT devices, network traffic, the cloud service that is connected with the IoT, the web interface, and the mobile app that controls the IoT devices [35]	Computers, mobile phones, social networks, logs, and other clues/items included in the crime scene [35]
Quantity of extracted data	A huge amount of data depends on the IoT devices' types and IoT environment [31]	Typically, less data. Depending on the number of components involved in the investigation such as desktops, smartphones, and laptops [35]
Format of extracted data	It might be a complicated format due to the diversity of IoT manufacturers [31]	Standard format, it might be encrypted [35]
Network Boundary	Blurry, unclear network boundary [31]	Relatively a clear and defined network boundary [31]

differences which affect the traditional forensics phases, these differences should be considered while conducting IoT forensics [34]. The following Table 1 describes the differences between IoT forensics and traditional forensics in terms of the number of devices, evidence sources, types of evidence, the quantity of extracted data, the format of extracted data, and the network boundary [31,34,35].

2.3. *IoT Digital Forensics Challenges in the Era of IR 4.0*

In a survey conducted by [36] targeting people with a digital forensics background, 27% of responders marked that they were involved in IoT investigation, and most of the IoT cases were related to smart home appliances, infotainment systems from vehicles, and smart health devices. Responders stated several challenges while conducting IoT forensics. For instance, lack of technical training, lack of education, and software issues hold the highest rank, whereas cloud data storage, funding, and legal issues have a lower rank. Moreover, the responders pointed out that the research should be focused on cloud forensic data, IoT volatile data, IoT forensic tools, and encryption. On the other hand, 73% of responders thought that IoT data acquisition techniques needed improvement [36]. The sophisticated evidence acquisition process, the cloud's multi-tenant nature [37], the lack of an IoT dataset for training, and the lack of methodologies for IoT data acquisitions are all considered challenges faced by investigators [35,38]. The volume of data, legal aspect, and forensic automation are the most three important challenges faced by IoT technology [39]. Moreover, IoT devices are always connected to the internet, hence, they lack security controls [40]. Users usually don't change IoT default passwords, and manufacturers do not send updates and patches to IoT devices. Therefore, IoT is considered an easy target for hackers [40]. In addition, IoT forensics has multi-levels, including device, network, and application levels [31,33]. Therefore, digital investigators face several challenges surrounding each level. The following sub-sections state the challenges for each level.

1) *IoT Digital Forensics Challenges at the Physical Device Level*

IoT forensics challenges at the device level include data format variety, multiple vendors, various platforms, and different standards [38]. Extracting digital artifacts from IoT devices is a big challenge for investigators as IoT data could be stored in several locations, on the cloud or network, or in the physical device. In addition, IoT data might be encrypted [41]. Also, the time of evidence surviving is short and could be overwritten [38]. The IoT operating system, IoT file system, IoT internal memory storage, and IoT external memory storage are components of interest included in the IoT forensics process at the IoT device level [42]. The investigator can't usually image the storage of IoT devices as some IoT devices don't have ports for connection to the workstation, which poses a challenge to examining the internal storage, file system, or operating system [43]. Moreover, security and privacy are considered significant issues, as IoT devices are relatively small and don't have enough storage for installing security tools and processing real-time log investigation solutions [43]. The variety of filesystems and operating systems used in IoT devices leads to other challenges as the investigator needs to be aware of the different IoT filesystems' structures to define and locate critical artifacts [44,45].

2) *IoT Digital Forensics Challenges at the Network Level*

The complex architecture of IoT networks and fast network traffic of the IoT environment raise obstacles in the path of digital investigations [46]. Most of the time evidence of IoT networks is inaccessible [43]. The mobility of network IoT traffic poses hurdles in defining the artifact's location or acquisition of artifacts during the investigation [35,47]. The huge amount of network traffic generated; therefore, it is difficult to define the most relevant data to be investigated. In addition, this traffic needs a huge storage capacity to be stored for analysis [43,46,47]. Keeping the integrity of captured network traffic is another challenge for network investigators as this traffic could be affected by software and hardware errors or could be modified by intruders [46]. In addition, extracting artifacts from encrypted traffic is a challenge for investigators [4].

3) *IoT Digital Forensics Challenges at the Application Level*

In IoT architecture, the application level includes mobile devices, web interfaces, and cloud services that are connected to IoT devices [12,14]. In the cloud acquisition, the investigator needs the user's credentials, to get access to the mobile data, and two-factor authentication poses a challenge [48,49]. Some IoT devices are configured to be fully dependent on cloud services which leads to other challenges in investigations [35]. Moreover, certain legal obstacles could appear when geographical boundaries are crossed in the case of cloud services [35]. Mobile investigators face several challenges such as the different kinds of mobiles, manufacturers, and operating systems [50]. Further, passcode recovery, built-in security, and encryption [51], in addition to the complexity of mobile structure [50], and the different standards available are all considered challenges for mobile forensics experts [52]. Thus, special skills are required to acquire and examine all types of devices [51]. Usually, most IoT devices are controlled by mobile applications, these mobile applications might be downloaded on the Android or the iPhone operating system (iOS). Therefore, investigators should be aware of iOS and Android security features. Moreover, digital investigators need to be aware of data acquisition types for mobile devices including (1) physical acquisition, (2) logical acquisition, (3) cloud acquisition, (4) chip-off acquisition, (5) and manual acquisition [48,53].

2.4. Studies and frameworks related to IoT digital forensics

Several studies have investigated different IoT devices and suggested frameworks and models for conducting IoT digital forensics [6, 31-33,43,45,49,54-69]. Table 2 compares several IoT forensics frameworks and case studies in terms of the used investigated levels: the device, the network, and the application (mobile, cloud).

Table 2. Studies and frameworks related to IoT digital forensics in the literature

Frameworks and case studies related to IoT	Device Level	Network Level	App Level (Cloud)	App Level (Mobile)	Comments describe the study
S. Zawoad and R. Hasan [6]	✓	✓	✓		Contains a centralized evidence repository, a conceptual model for IoT forensics
E. Oriwoh et al., [31]	✓ Internal network	✓ External and middle network	✓ External network	✓	Contains three zones for evidence extraction, the external, the middle, and the internal zones
H. Chung et al., [32]	✓		✓	✓	Investigated the Amazon Alexa ecosystem
A. Awasthi et al., [33]	✓	✓	✓	✓	Investigated the Almond smart home hub
F. Servida and E. Casey [43]	✓	✓	✓	✓	An experimental study that conducted a digital investigation over four IoT devices, artifacts generated by IoT devices can be found on the device, smartphones, networks, and cloud
C. Meffert et al., [54]	✓		✓		Contains a centralized Forensic State Acquisition Controller (FSAC), openHAB controller was used
L. Babun et al., [56] [55]	✓	✓	✓	✓	Focuses on forensic-relevant data only (applied on 22 IoT devices)
F. Bouchaud et al., [57]	✓	✓	✓	✓	A forensics framework for an ecosystem contains three stacks, (1) IoT layers such as the sensing layer, network layer, service layer, and interface layer, and (2) the components of IoT ecosystems. (3) the possible forensic options
A. Nieto et al., [58]	✓	✓	✓	✓	Combines privacy requirements (ISO/IEC 29100:2011) and focuses on the potential surrounding devices to collect evidence
T. Zia et al., [59]	✓	✓	✓		Follows NIST Guide for DF process, applied on Wearables, Smart Home, and Smart City
M. A. Saleh et al., [60]					Based on the metamodeling method and blockchain rather than IoT levels
M. Hossain et al., [61]					Based on a digital ledger rather than IoT levels
W. A. Mahrous et al., [62]					Based on the blockchain technique rather than IoT levels.
M. J. Islam et al., [49]	✓	✓	✓		Proposed a comprehensive framework for IoT investigation, that is not dependent on the network logs and the Cloud Service Provider
V. R. Kebande et al., [63]	✓	✓	✓		Proposed for the IoT ecosystem
M. Hossain [64]					Provides digital forensics examination, access control, authentication, and network attack mitigation for IoT infrastructure
S. Li et al., [65]	✓	✓	✓	✓	Investigates Amazon Echo, the evidence is collected from sensing, network, cloud, service, and interface layers.
E. Oriwoh and P. Sant [66]		✓		✓	Provides forensics and security services for IoT smart home devices
V. R. Kebande and I. Ray [67]	✓	✓	✓		Depending on the proactive/ reactive process, it complies with the ISO/IEC 27043: 2015
J. P. Sandvik et al., [45]	✓				Investigates a coffee file system over Contiki OS
J. M. C. Gómez et al., [68]				✓	Investigated nonvolatile memory of windows IoT core operation system
N. Koroniotis et al., [69]		✓			A proposed network forensic framework based on deep learning for IoT networks
J. Song and J. Li [34]					It depends on classifying and examining data from different sources. It converted data into unstructured, semi-structured, and structured rather than depending on IoT levels

Several IoT digital forensic frameworks and case studies were explored, stated, and compared according to the three levels of IoT architecture (the device level, the network level, and the application level). As noticed from Table 2, some frameworks and case studies examined the IoT at the device levels or network level or included all levels for investigation. On the other hand, other studies didn't include any level but they used a different approach for investigation such as blockchain [60-62], or depended on classifying data according to the data structure [34]. Other studies focus on access control, authentication, and network attack mitigation for IoT infrastructure [64] rather than

focusing on the investigation at IoT levels. As a result, the literature review inspired the researcher to design and propose a novel IoT digital forensics framework. The proposed framework was adapted to suit the unique characteristics of IoT devices throughout all its phases. These characteristics include focusing on the Artifact of Interest (AoI), exploring the IoT environment, and considering the multi-level structure of IoT devices during the phases. The methodology used is presented in the following section.

3. Methodology

3.1. The Proposed Framework

This study proposes a novel IoT digital forensic framework named “Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT)”. The MAoIDFF-IoT framework is constructed based on a literature analysis and then it is refined using an experimental approach to align with the characteristics of the IoT. The framework considers the traditional phases of the digital investigation process, and it integrates the benefits of previous frameworks [21,57,63,65,70-72]. Moreover, new features and subphases were added based on the experimental analysis to enhance the framework's effectiveness. Fig.1. clarifies how the MAoIDFF-IoT framework is built. Moreover, the main structure of this framework is illustrated in Fig.2.

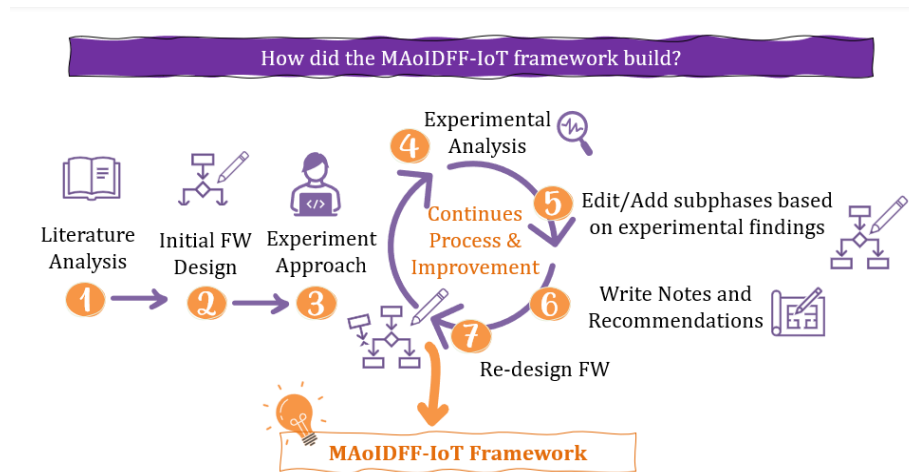


Fig.1. The methodology used in building the proposed framework, MAoIDFF-IoT.

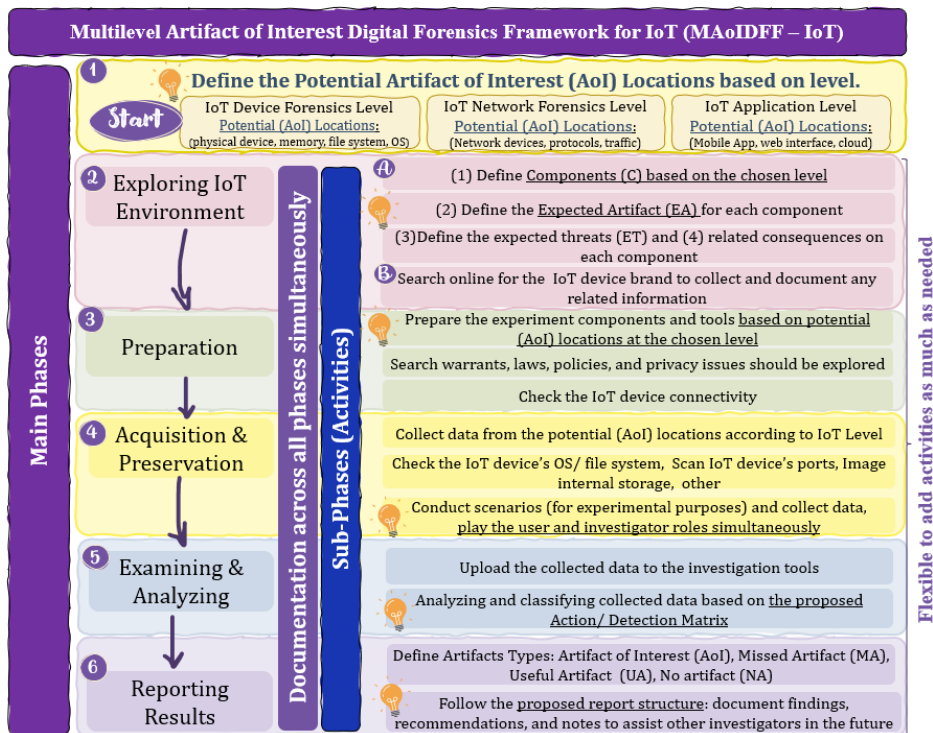


Fig.2. The Proposed Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT).

3.2. Phases of (MAoIDFF-IoT) Framework

MAoIDFF-IoT framework has 6 main phases each supported by expanded sub-phases, in addition to the documentation phase that should be done in parallel with all phases to maintain integrity and to ensure admissibility in court. The phases are stated as follows.

- Phase 1: Define the potential Artifact of Interest (AoI) locations based on the chosen level/ Documentation
- Phase 2: Exploring IoT environment/ Documentation
- Phase 3: Preparation/ Documentation
- Phase 4: Acquisition & preservation/ Documentation
- Phase 5: Examining & analyzing/ Documentation
- Phase 6: Reporting/ Documentation

The phases in the proposed MAoIDFF-IoT framework are explained in detail in the following:

1) Phase 1: Define the Potential Artifact of Interest (AoI) Locations Based on Level/ Documentation

The huge amount of data required to be analyzed is the biggest challenge in forensic analysis [71]. Thus, focusing on the (AoI) differentiates the proposed framework from previous frameworks, making the investigation process more effective and saving time and effort. The researcher was motivated and inspired by the Digital Forensic Data Reduction and Data Mining Framework [71] to focus on the (AoI) but with a different perspective and approach.

The artifact is any type of valuable information extracted from digital devices and presented as evidence in court [3]. On the other hand, the (AoI) in this research refers to any valuable information extracted from IoT devices at three levels, from all potential artifact locations. Since the IoT environment has a three-level architecture (physical, network, and application) [12-16], several studies [57,63,68] have explored different levels of the IoT architecture. On the other hand, the proposed framework is more inclusive because it suggests exploring all potential locations of artifacts at each IoT level to find (AoI). This approach considers commonly cited artifact locations, such as the locations of deleted or hidden data. Each level of IoT has multiple artifact locations. Therefore, if any artifacts were missed from locations at any level, it's possible to find them at locations on different levels. Table 3 indicates the potential AoI locations based on the IoT levels. AoI can be extracted from three main levels, including (1) the IoT device level, which includes artifact locations such as the physical device, memory, filesystem, and operating system. (2) IoT network level, which has artifact locations such as network devices, protocols, and traffic. (3) IoT application level, the artifact locations include web interface, mobile app, and cloud.

Table 3. The potential AoI locations according to the IoT levels

IoT Levels	Device level	Network level	Application level
Potential Artifact of Interest (AoI) Locations	<ul style="list-style-type: none"> • Physical device • Internal memory • External memory • Operating system • File system 	<ul style="list-style-type: none"> • Network Traffic • Protocols • Network devices (router, server, switch) 	<ul style="list-style-type: none"> • Web interface • Mobile IoT Application • Cloud

To ensure that the proposed framework is suitable for current and future IoT digital crime investigations, and addresses the variety of IoT structures, and features, and does not overlook any artifacts of interest (AoI), this phase is implemented at this stage. To define the AoI, the investigator should consider the following three main points:

(1) Explore the IoT device to choose the appropriate investigation level/levels: The investigator decides the level or levels of investigation based on the features of the IoT device and its environment. Thus, choosing the level of investigation is crucial because each IoT device has different features and services. For example, some IoT devices are connected to the cloud, while others are not. Some IoT devices have internal and/or external memories, while others do not. Furthermore, IoT devices have various file systems, and not all IoT devices are connected to web interfaces and/or mobile applications. Hence, depending on the IoT device, the investigator should select the level or levels of investigation to focus on. Fig.3 clarifies the proposed flowchart for selecting the investigation level. First, the investigator should examine whether the IoT device has ports or internal/external memories. If it does, then the investigation should include the device level. If it does not, the investigator should check if the IoT device is sending streaming data via the network. If it is, then the investigation should include the network level. Lastly, the investigator checks if the IoT device is connected to the cloud, mobile app, or web interface. If it is, then the investigation process should include application-level investigation.

(2) Investigate the chosen level to extract the AoI from the potential artifact locations specified in Table 3: It is important to note that each chosen level should be investigated individually. The investigator should determine only one level and then proceed with the remaining phases of the proposed framework.

(3) Conduct a multi-level investigation to avoid missing any artifacts: Thus, if any artifact is missed at one level, it is possible to find it at another level. For example, a camera device is connected to the internet and sends streaming

videos via the network (network level). Additionally, the camera has external storage (device level) and a mobile app for control (application level). Hence, this camera has three levels targeted by the investigator: the device, the network, and the application levels. In this case, the investigator can choose to investigate either one level or all levels. If the extracted artifact from one level is sufficient, there is no need to investigate other levels. However, investigating multiple levels will prevent missing any artifact and confirm the validity of the artifact.

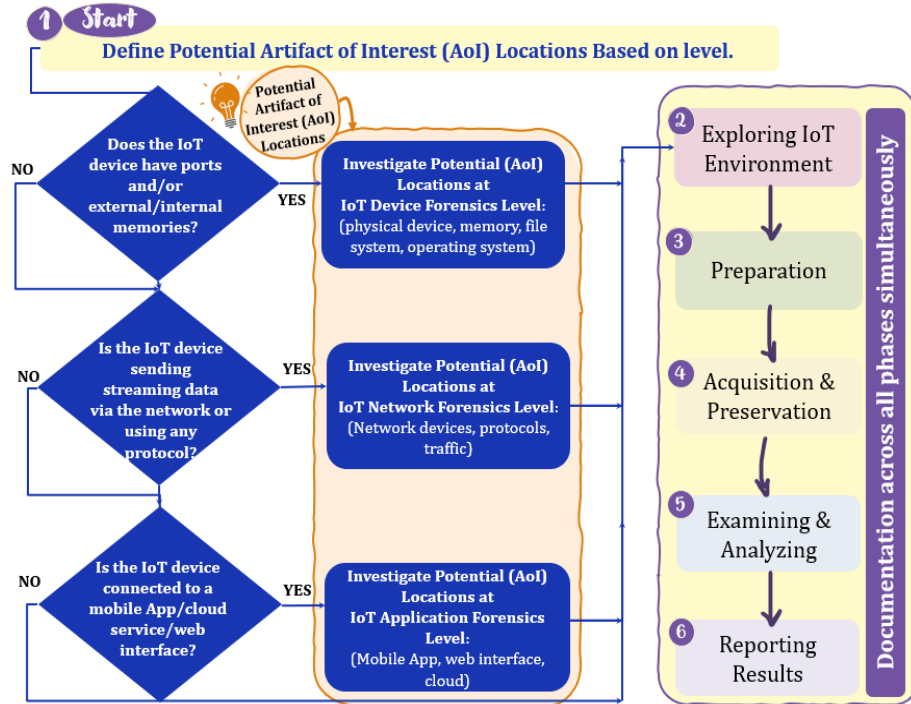


Fig.3. Define the Artifact of Interest (AoI) based on level.

To enhance the effectiveness of the investigation and save time and effort, the investigator can select a specific level of focus and exclude other levels based on the IoT device and the case at hand. In some cases, investigating at the IoT device level is crucial to gather complete data that has not yet been transmitted to the network or cloud. In this case, the investigation at the network level could be excluded if the gathered artifact from the device level is sufficient. However, the investigation at the network level could be included to check the data integrity and compare the artifact with other artifacts gathered from the device or application level [40].

2) Phase 2: Exploring the IoT Environment/ Documentation

The identification phase, which involves exploring the environment, has been addressed in several studies using different methods [57,59,63,69,72]. On the other hand, the development of the (MAoIDFF-IoT) took a different approach. It ensures the avoidance of missing any artifacts by exploring and gaining an initial understanding of the IoT environment at several phases. In the first phase, the initial exploration aimed to define the targeted level of investigation. But, in this phase, the second exploration aims to define four main parts at the targeted/chosen level:

- The Components (C), which include any element involved in the scene at the chosen level.
- The Expected Artifacts (EA), include artifact locations or any other information related to the chosen level.
- The Expected Threats (ET) for each component, are any potential actions done by users on the IoT device, such as unauthorized access to the device.
- The consequences of the expected threats may affect confidentiality, integrity, availability, and privacy.

All these four parts should be defined and documented. Fig.4 illustrates an example of exploring the IoT environment. In addition, the investigator should conduct an online search for the IoT device to examine its characteristics, operating system type, file system type, and any other relevant information that could assist in the investigation. All the gathered information from this phase should be documented.

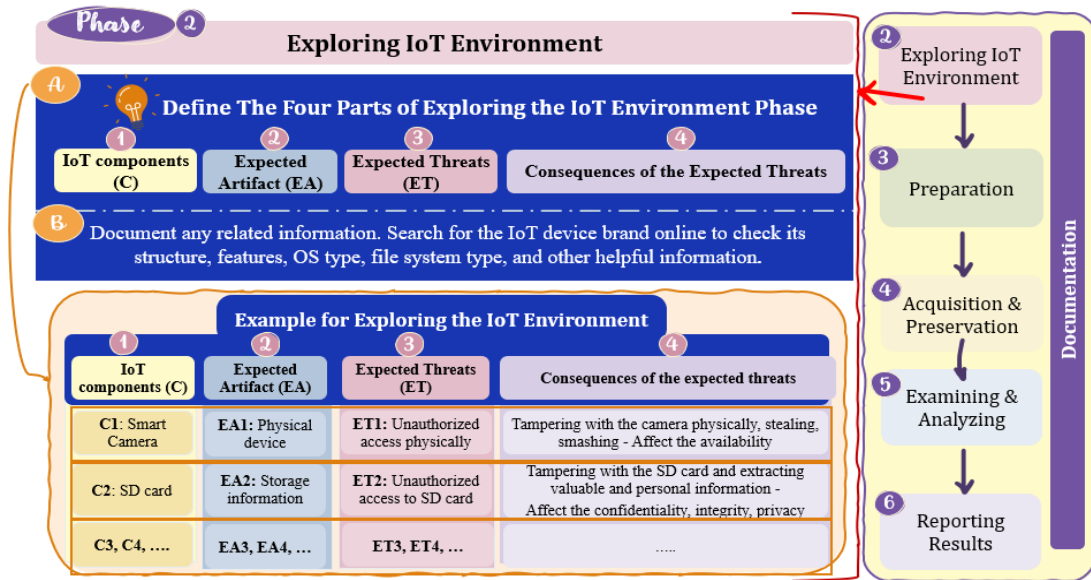


Fig.4. An example of exploring the IoT environment.

3) Phase 3: Preparation/ Documentation

Before carrying out the investigation, the investigator should prepare the investigation workstation and the appropriate tools based on the chosen level to avoid any delays in the investigation process. Each level has its forensics tools. For example, Wireshark is used at the network forensics level, while FTK imager is used for capturing memory images at the device level. In addition, the investigator should check the connection of the IoT device. Furthermore, they should explore the search warrant, laws, policies, and privacy issues in this phase [72]. Preparation is considered the starting point of an incident response. Lack of preparation leads to the loss of critical artifacts such as volatile information [35]. The investigator should document the type of workstations and tools used, as well as any other related information during this phase. Fig.5 clarifies phase three according to the proposed MAoIDFF-IoT framework.

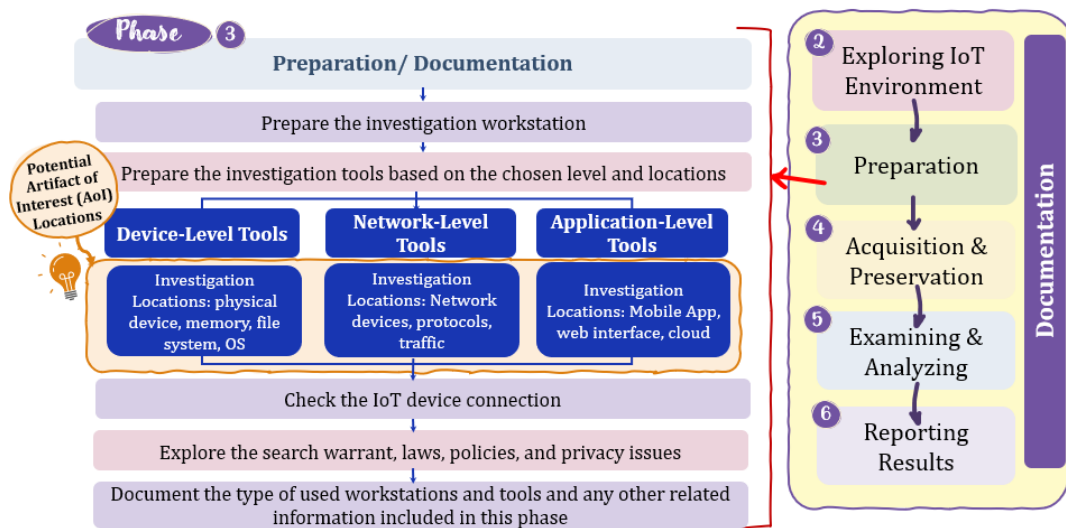


Fig.5. Phase three according to the proposed MAoIDFF-IoT framework.

4) Phase 4: Acquisition & Preservation/ Documentation

This phase involves conducting preliminary interviews with the devices' owners and people to get valuable information without violating policies. In any cybercrime, there may be both digital and physical artifacts [72], and both artifacts need to be preserved and investigated [35]. In addition, collecting volatile and non-volatile data while preserving the integrity of the collected data is a vital process to ensure admissibility in court [73]. MAoIDFF-IoT framework proposed collecting data from several locations based on the chosen level. If the selected level is an application level, it is important to specify the type of acquisition, such as physical, logical, the cloud, chip-off, or manual acquisition [53]. Also, backups and calculating hashes should be conducted for all the gathered data before

proceeding with the next phase [21]. What sets this framework apart from previous frameworks at this phase is the experimental approach that relies on defining predefined scenarios by the researcher. In this approach, the researcher simulates the role of the user by executing various actions on the IoT device. Simultaneously, the researcher investigates, detects, and verifies these actions to ensure the authenticity of the artifacts. All data collected from the predefined scenarios should be gathered for analysis in the next stage. Further, all actions in this phase should be thoroughly documented. Fig. 6 clarifies phase four per the proposed MAoIDFF-IoT framework.

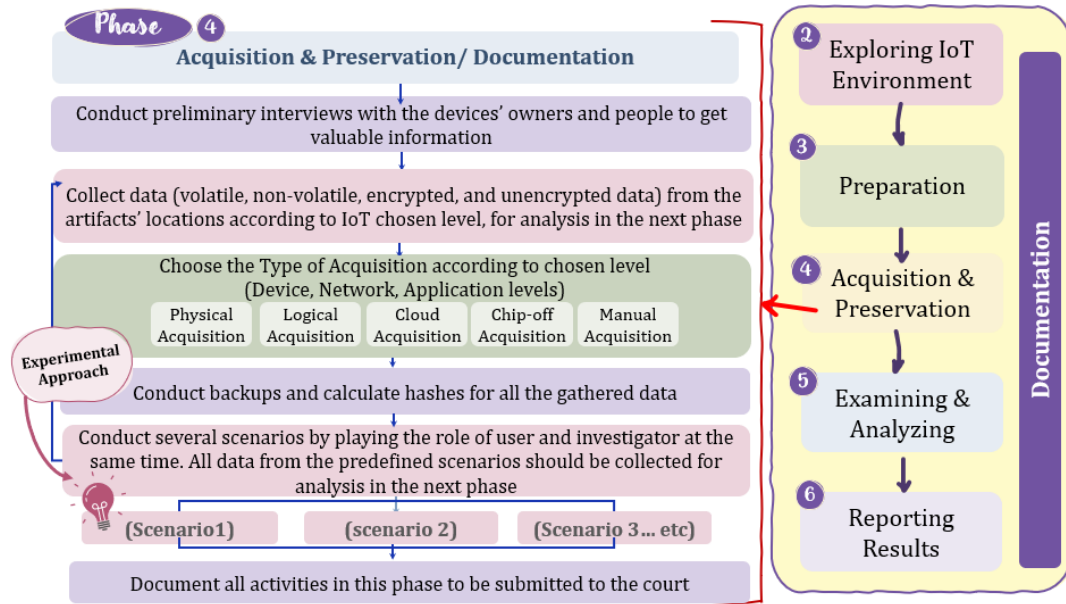


Fig. 6. Phase four according to the proposed MAoIDFF-IoT framework.

5) Phase 5: Examining & Analyzing/ Documentation

All the collected data from the previous phase should be examined and analyzed by the investigator using appropriate investigation tools. The collected data includes in-depth data analysis, data searching, artifact locating, artifact identifying, information filtering, hidden data, and deleted data related to the IoT environment and the crime scene [23,72]. The investigator should read, understand, and analyze all gathered information [73]. In this phase, the MAoIDFF-IoT framework considers the encrypted data. For example, at the network level, the investigator might gather encrypted traffic. Therefore, analyzing encrypted traffic may be required using specific tools. Reverse engineering for IoT mobile apps was also added and considered in the proposed framework. At the application level, some IoT devices are controlled by mobile apps. If the investigator can't find the related artifact from the IoT app, reverse engineering is needed to analyze how the app acts and recognize where the app stores the related data. In addition, several IoT devices have filesystems. Therefore, the MAoIDFF-IoT framework suggests four steps for IoT file system analysis: (step1) analyze the boot sector, (step2) analyze the root directory, (step3) analyze the content, (step4) analyze the IoT device behavior. The result from the (analyzing & examining) phase includes obtaining the relationships between all elements and rebuilding the event based on extracted data [35]. All the analysis findings should be explained and accurately documented [73].

The MAoIDFF-IoT framework focuses on an additional part in the (examining & analyzing) phase which involves examining and analyzing the results obtained from predefined scenarios conducted in the previous phase. Recalling the previous phase, the researcher simultaneously played the roles of user and investigator. The investigator tries to find artifacts based on the actions conducted. The MAoIDFF-IoT framework proposes an Action/ Detection (A/D) matrix that defines four types of extracted artifacts; missed artifact (MA), no artifact (NA), useful artifact (UA), or artifact of interest (AoI), these artifact types were described in Fig.7 and Table 4. Phase five according to the proposed MAoIDFF-IoT framework, is clarified in Fig.8.

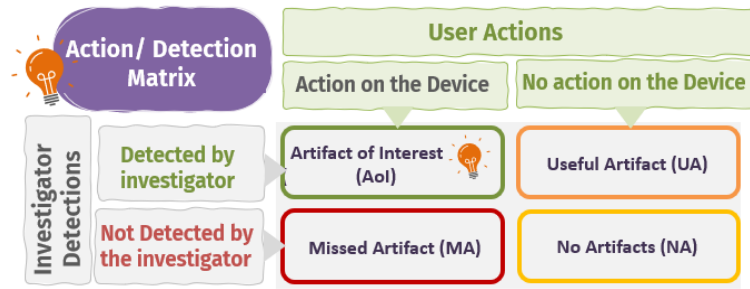


Fig.7. The Proposed Action/ Detection (A/D) Matrix by the MAoIDFF-IoT FW classified the extracted artifacts into 4 types

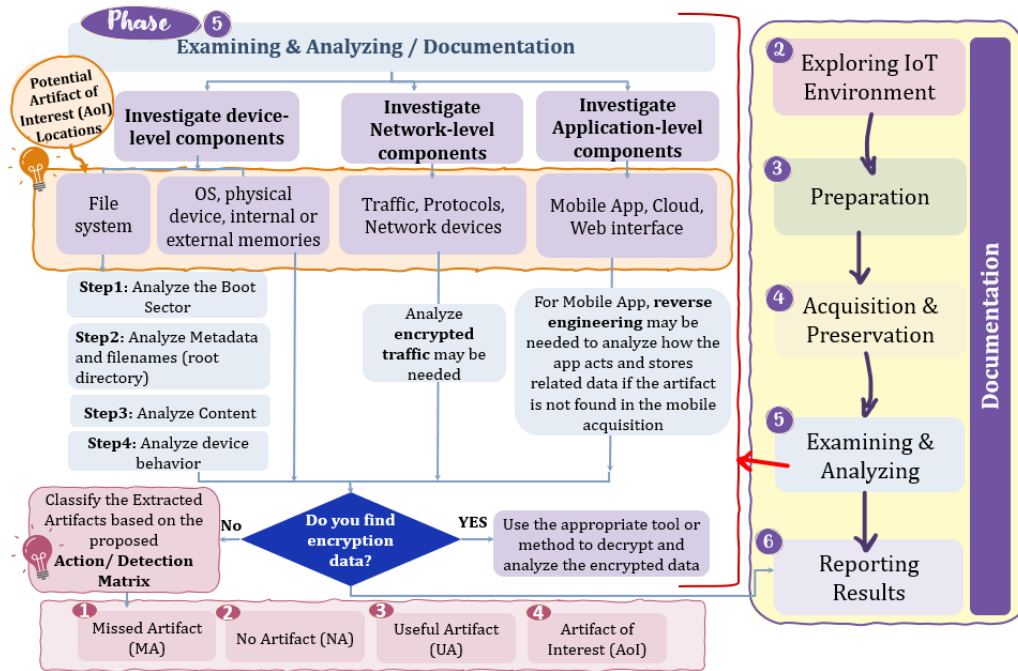


Fig.8. Phase five and phase six according to the proposed MAoIDFF-IoT framework.

Table 4. The description of the four types of extracted artifacts according to the proposed MAoIDFF-IoT framework

Artifact Type	Description
Missed Artifact (MA)	When there is an action and the investigator can't prove the action and can't extract the artifact it is the most dangerous state.
No artifact (NA)	When there is no action and the investigator can't prove that there is no action
Useful Artifact (UA)	When there is no action and the investigator extracts the artifact, this artifact may help in the investigation, for example, (Type/ features of the device is UA)
Artifact of Interest (AoI)	When there is an action and the investigator proves the action and extracts the artifact correctly

6) Phase 6: Reporting the Results/ Documentation

Documentation is an important phase, it is a continuous process that should be done through all the investigation phases to preserve the proper chain of custody and to avoid missing any artifacts [71,74]. The investigator should document the result of all gathered information from previous phases concisely and clearly by photographing them in a report to be submitted to the court [23,72]. All the artifact types (MA), (NA), (UA), and (AoI) should be defined and documented. The investigator also should record, explain, and present the results of investigations, the date and time for each action should be logged in the report [35]. The examiner should document his analysis and perspective. The report include, the case ID, case examiner, date of report, data of received case, ID and signature of the examiner, description of case items, methods, tools used and steps taken during the investigations, details of analyzing evidence, findings, and finally, the conclusion which includes the offense name, suspects names, (AoI), and the related cybercrime law. Proper documentation is important to be submitted in court and helps in reviewing the crime case anytime [53]. Guidelines, recommendations, and additional notes related to the case is an additional activity proposed in the MAoIDFF-IoT framework which should be stated at the end of the report to facilitate the process for other investigators in the future. Phase six according to the proposed MAoIDFF-IoT framework is clarified in Fig.9.

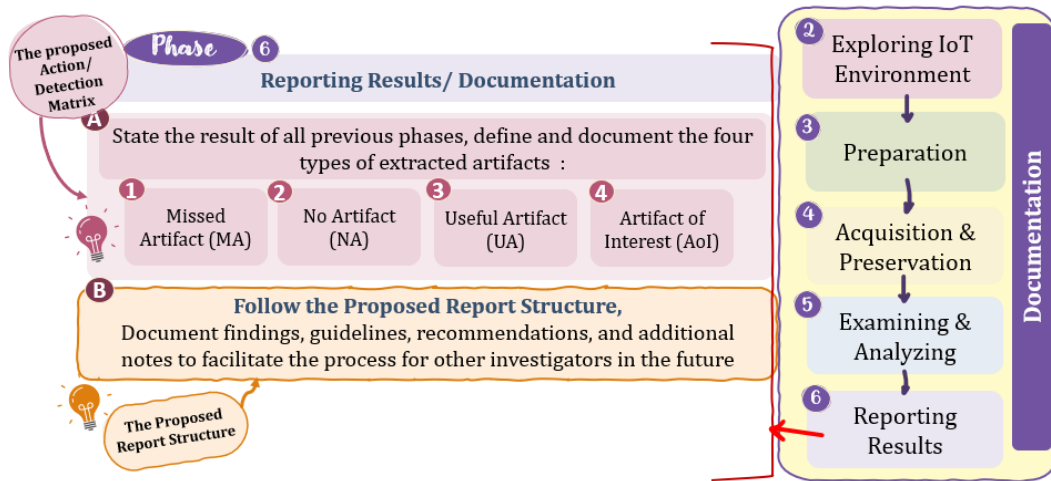


Fig.9. Phase six according to the proposed MAoIDFF-IoT framework.

The suggested structure for the expert witness report based on (MAoIDFF-IoT) framework that should be submitted to the court is clarified in Table 5 as follows:

Table 5. The proposed structure of the expert investigation report according to the (MAoIDFF-IoT) framework

First Page	Report name: Expert witness report: Case name Investigator name Submitted to: Entity name.
Second Page	Investigator detailed paragraph: (Name, its experience briefly, city and country.) Case details paragraph: This includes the accused name, offense name, case name, case number, the tools used, date of request, and date of the published report. Result paragraph: This includes the offense name, suspected names, artifacts of interest (AoI), and the related cybercrime law.
Third page	Document contents, list of tables, and list of figures
Fourth page	Introduction, an overview of the case.
The rest of the report	Includes the six phases of the proposed framework (MAoIDFF-IoT): Phase 1: Define the Potential AoI Locations Based on the Level/ Documentation Phase 2: Exploring the IoT Environment/ Documentation Phase 3: Preparation/ Documentation Phase 4: Acquisition & Preservation/ Documentation Phase 5: Examining & Analyzing/ Documentation Phase 6: Reporting the Result/ Documentation
Additional page	Guidelines, recommendations, and additional notes to facilitate the process for other investigators in the future.
Appendix page	Any other screenshots, images, and documents should be stated in the appendix.

4. Implementation and Experiments

To demonstrate the effectiveness of the framework, all suggested phases in the proposed framework were implemented in this section. The following subsections present three case studies. The first case in (section 4.1) is an experiment on a smart camera at the device level. The second case in (section 4.2) is an experiment on a smart camera at the application level. The third case in (section 4.3) is an experiment on a smart environment containing seven IoT devices.

4.1. Smart Camera at Device Level Case Study (1st Case Study)

In this experiment, the proposed framework was applied. The following sub-sections clarify all phases.

1) Phase 1: Define the Potential Artifact of Interest (AoI) Locations Based on the Chosen Level/ Documentation.

The very first phase is defining the potential AoI locations by choosing which level needs to be investigated. The IoT device level is chosen to be investigated in this case, because the camera doesn't have any ports for connection to the workstation but it has an external memory. Therefore, (1) the operating system, (2) the external memory, and its filesystem were the potential AoI locations that were determined to be investigated at the device level. See Fig. 10.

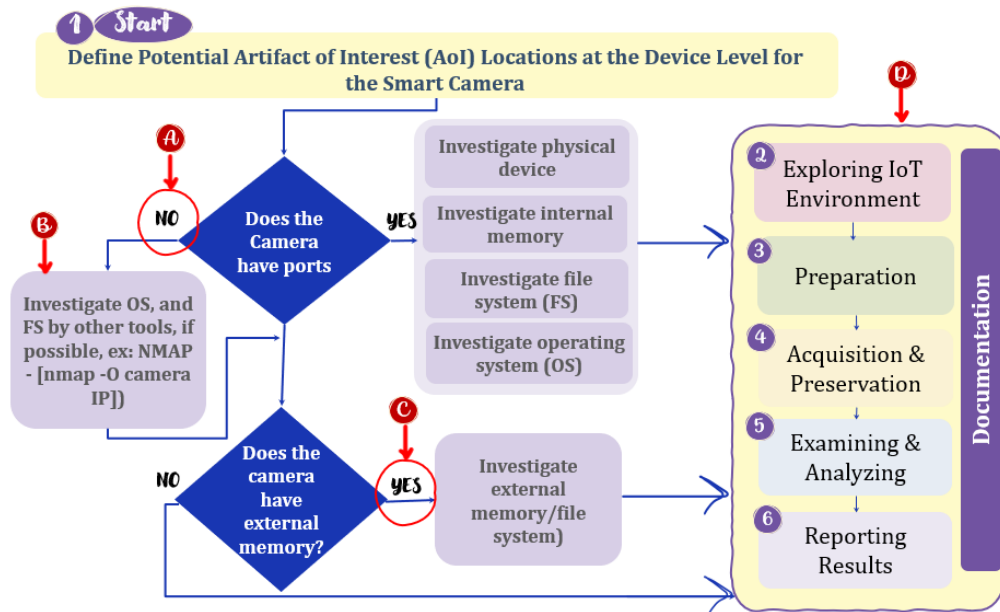


Fig. 10. Define the potential artifact of interest (AoI) locations at the device level for the smart camera.

2) Phase 2: Exploring the IoT Environment/ Documentation

After defining the investigation level and the potential AoI locations, the next phase is exploring the IoT environment by defining (1) the components (C), (2) the expected artifacts (EA), (3) the expected threats (ET), and (4) the consequences of the expected threads for each component to understand the IoT environment see Table 6.


Table 6. Explore the IoT environment of the smart camera at the IoT device level

Component (C)	Expected Artifact (EA)	Expected Threat (ET)	Consequences of the Expected Threats that affect the confidentiality, integrity, availability & privacy.
C1: Smart Camera	EA1: Internal memory storage, operating system, filesystem, and other related content	ET1: Unauthorized access to the camera physically	Tampering with the camera physically, stealing the device, smashing the device, and/or extracting valuable information
C2: External memory (Secure Digital card - SD card)	EA2: Valuable information on the memory such as videos, images, and other information.	ET2: Unauthorized access to the camera memory	Tampering with the camera via memory and extracting valuable and personal information

In this case, the main components are:

- C1: The smart camera is considered the main physical asset. The smart camera model is Tapo C200 [74].
- C2: The external memory, the camera has local storage (Secure Digital card - SD card) of up to 128 GB. The camera features were explored online via its official website [74] which concluded in Table 7.

Table 7. Detail information about the smart camera that collected from the internet

	Camera Name	Pan/Tilt Home Security Wi-Fi Camera
	Camera model	Tapo C200
	The manufacture	TP-Link Company
	Default Password	Not available
	Default Username	Not available
	Wireless protocols	IEEE 802.11b/g/n, 2.4 GHz
	Adapter input	100-240 V, 50/60 Hz 0.3 A
	Adapter output	9.0 V, 0.6 A (DC power)
	External memory (SD card)	SD card is inserted into the camera, Type: Lexar High-Performance, class 10, 633x 32GB microSDHC with FAT32 file system
	Official Website	https://www.tapo.com/us/product/smart-camera/tapo-c200/

3) Phase 3: Preparation/ Documentation

Before the actual investigation, the investigator should prepare the investigation workstation and the appropriate investigation tools based on the chosen level. The tools used in this experiment are stated in Table 8. The FTK imager tool was used for imaging the external memory, the Autopsy tool was used for analyzing the extracted images. In addition, the SD card adapter was used to transfer data between the memory and the investigation workstation. Fig.11

clarifies the structure used in the experiment to investigate the potential AoI locations for the camera at the device level.

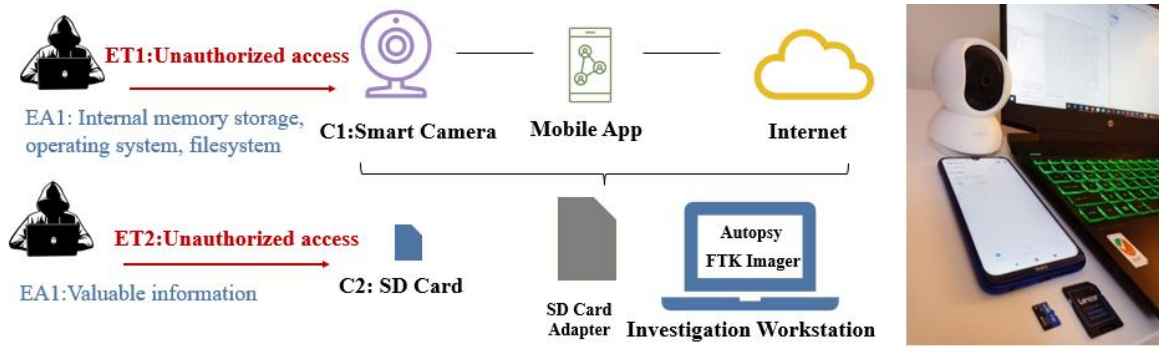


Fig.11. The structure used in the experiment to investigate the smart camera at the device level.

Table 8. Tools used in the investigation at the device level

Tool Name	Description
FTK imager 3.1.1.8	Imager tool
Autopsy 4.19.1	Digital forensic analyzer tool
Investigation Workstation	PC – Windows 10, CPU - AMD with Radeon Graphics 2.9 GHz, 8 Cores
Smart Camera	Tapo C200, Wi-Fi camera
Mobile	Camera App is downloaded on “Xiaomi Redmi Note 8” mobile to connect with the camera
Secure Digital card (SD card)	SD card is inserted into the camera, Type: Lexar High-Performance, class 10, 633x 32GB microSDHC with FAT 32 file system
SD card Adapter	It transfers data between SD and investigation workstation, Type: Lexar C10/UHS-i

4) Phase 4: Acquisition & Preservation/ Documentation

To collect data generated from the smart camera at the device level, several scenarios were conducted by the researcher, the scenarios are clarified in Table 9. All images obtained from the scenarios were backed up to preserve their integrity and uploaded into Autopsy for analysis.

5) Phase 5: Examining & Analyzing/ Documentation

In this phase, the potential AoI locations were investigated. First, the operating system was explored, and second, the file system of the external memory (SD card) which is the File Allocation Table (FAT32) was analyzed. See Fig.12.

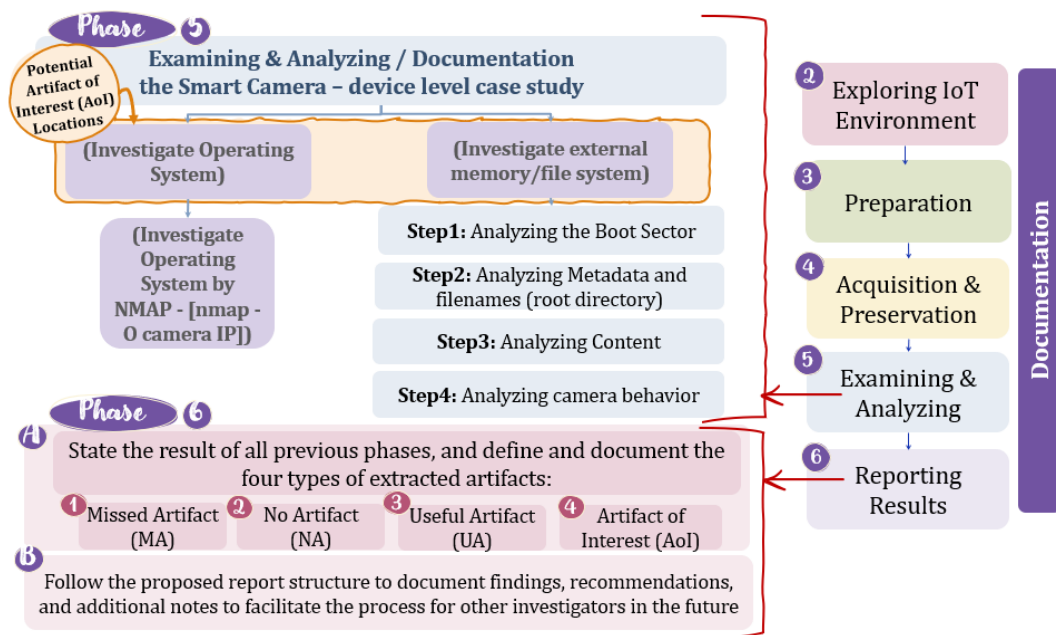


Fig.12. Examining and analyzing / Documentation phase for the smart camera at the device level.

- *Examining and analyzing operating system (OS):* according to the MAoIDFF-IoT framework, if the IoT device doesn't have any ports for connection to the workstation, it is possible to use other tools to investigate the internal of the IoT device. In this case, the camera doesn't have any ports to connect to the workstation. Therefore, the NMAP tool on Kali Linux was used to check and explore the camera's OS and to identify any artifacts related to the OS. A command [nmap -O camera IP] was used. The result showed that this camera has an unknown OS.
- *Examining and analyzing the file system:* in this experiment, the FAT32 file system on the SD card was analyzed, and all images of the SD card acquired in the previous phase were loaded into the Autopsy tool for the analysis process. To define the artifact location in the FAT32 SD card, the investigator should be aware of the physical structure of the FAT32 file system. The FAT file system has three physical areas; (1) the reserved area, (2) the FAT area, and (3) the data area. The reserved area contains the boot sector which describes information about the file system. The second area is the FAT area which tracks allocated and unallocated data units on disk. The third area is the data area, which contains data content and allocates the directory entries [44]. The root directory in FAT32 can be anywhere in the data area [44]. To analyze and extract artifacts from FAT32 SD card images, the basic model for analyzing file systems from Brain Carrier book, the "File System Forensic Analysis" book [44] was taken into consideration, Carrier suggested a model for analyzing any file system based on five categories, including filesystem, content, metadata, file name, and application. According to the proposed framework in Fig.12, the following steps were conducted based on the basic model:
 - Step 1: Locate and read vital information from the boot sector (Analyze File System).
 - Step 2: Locate the root directory to extract all files and folder entries (Analyze Metadata and File Names).
 - Step 3: Access and explore files and folders using information from the root directory (Analyze Content).
 - Step 4: Explore the camera behavior. The following subsections clarify each step:

Step 1: Locate and read vital information from the boot sector (Analyze File System)

In the FAT32 file system, all information about the file system is located in a reserved area or boot sector area. The boot sector contains information about the original equipment manufacturer (OEM) name, volume name, volume size, serial number, file system type, boot code, error messages, and signature [44]. All information was extracted and explored for all SD card images.

Step 2: Locate the root directory to extract all files and folders entries (Analyze metadata and file names)

The root directory is located in the user data area in the FAT32 file system. The root directory contains entries of 32 bytes in size that store metadata for files and folders such as timestamps, name, physical location, attributes, and file size information [44]. The root directory could be viewed in Autopsy from the system volume information > parent folder. All root directories were explored for all SD card images.

Step 3: Access files and folders using information from the root directory (Analyze content)

The content is located in the user data area in the FAT32 file system. Files and folders in the root directory were explored and accessed in all SD Card images.

Step 4: Explore the camera behavior (Analyze Camera Behavior)

During the investigation, the camera's behavior was recognized. For the first usage of the camera, the camera notifies the user to format the SD card using the mobile app settings, and the lens of the camera rotates 180°. When the SD card is inserted into the camera, the camera records the first twenty-second of the video when it is ON for the first time. In addition, the data in the camera's SD card is deleted and overwritten while the camera is in use. When the camera is put on privacy mode, it doesn't record anything on the SD card. However, it records on the SD card when the user clicks the button of capturing via mobile App.

6) Phase 6: Reporting the Results/ Documentation

The smart camera was connected to the mobile App, and then, a set of scenarios were conducted over the camera, all SD card images were obtained after conducting scenarios using the FTK tool, then the images (EmptyImage1.0.E01, After5minON.E01, Second5MinOn.E01, Format2.E01, and Privacy mode.E01) were loaded into the Autopsy tool for analyzation process. See Fig.13.

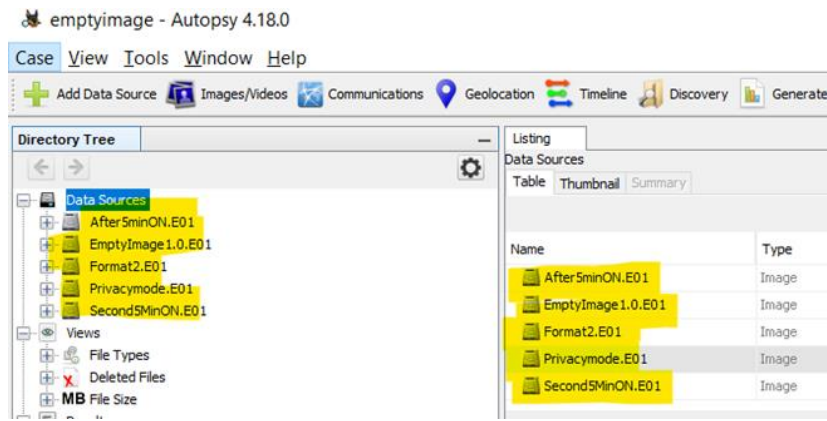


Fig.13. All external memory images of the smart camera were collected through a set of mentioned scenarios.

For each image, the FAT32 file system was analyzed including the boot sector, root directory, metadata, and files' content. The extracted artifacts were classified into four (MA), (NA), (UA), and (AoI). Autopsy extracted all files automatically and recovered all deleted and overwritten files. All videos captured via a smart camera found on the SD card are considered artifacts of interest (AoI). On the other hand, the captured images that were not found are considered missed artifacts (MA). In addition, all related metadata files obtained are considered useful artifacts (UA). The following Table 9 concludes the artifact types according to the conducted scenarios.

Table 9. The artifact types according to the conducted scenarios on the smart camera

Scenarios	User Role (actions)	Investigator Role	SD- card image name	Types of Extracted Artifacts based on A/D matrix (AoI, MA, UA, NA)
First Scenario	A new SD card with a FAT32 file system was formatted	SD-card imaged using the FTK imager tool	EmptyImage1.E01	There are no files as the SD card is empty (Useful Artifact - UA)
Second Scenario	The smart camera was ON for 5 min (idle mode), Then, the camera was plugged off	the SD card was imaged again using the FTK imager tool	After5minON.E01	The camera recorded a 20-sec video for the first usage, this video was found (Artifact of Interest - AoI)
Third Scenario	The smart camera was ON for another 5 min, 2 images were captured 2 min. of video were captured Then the camera was plugged off	the SD card was imaged again using the FTK imager tool	Second5minON.E01	The recorded video (was 2 min) was found (AoI) 2 captured images were not found (Missed Artifact - MA) Unlocated files were found as the camera is overwritten files while in usage (UA)
Fourth Scenario	The SD card was formatted	The SD card was imaged again using the FTK imager tool	Format2.E01	Unlocated and deleted files were found (AoI)
Fifth Scenario	The SD card was inserted into the camera and put on privacy mode.	the SD card was imaged again	Privacymode10Min.E01	No recorded videos were found in privacy mode (UA)

In the first scenario, a new SD card with a FAT32 file system was formatted and imaged using the FTK imager tool, the result obtained from the "EmptyImage1.0.E01" image showed an empty image which is considered (UA). In the second scenario, when the SD card is inserted into the camera, the camera records the first twenty-second of the video when it is ON for the first 5 minutes. This recorded video was recognized from the "After5minON.E01" image, Therefore, this video is considered an (AoI). There was no file deleted in the third scenario, although the Autopsy found some of the deleted and overwritten files in the "second5MinON.E01" image, thus, the SD card was deleted and overwritten data while the camera was in usage, this is considered as a (UA). This result was obtained after putting the camera ON for another five minutes in the third scenario and analyzing the "second5MinON.E01" image.

In the fourth scenario, all unallocated files which represent the deleted files were recovered from "Format2.E01" via Autopsy after formatting the SD card which is considered an (AoI). In the fifth scenario, when the camera is put on privacy mode for 10 minutes, it doesn't record anything on the SD card, this result is recognized after analyzing the "Privacymode10Min.E01" image, this is considered a (UA). However, it records on the SD card when the user clicks the button of capturing via mobile App. All videos recorded found in the "Second5minON.E01" image are considered (AoI) while the recorded images that were not found are considered (MA). In this case study, all phases in the MAoIDFF-IoT framework were applied and documented, and then the results were presented in the reporting phase.

4.2. Smart Camera at Application Level Case Study (2nd Case Study)

The following clarifies the phases applied in this experiment according to the MAoIDFF-IoT framework.

1) Phase 1: Define the Potential Artifact of Interest (AoI) Locations Based on the Chosen Level/ Documentation.

In this phase, the application level was chosen to be investigated. According to the MAoIDFF-IoT framework, the application level includes mobile, web interface, and cloud investigation. The examiner focused on the mobile App (Tapo) as a potential AoI location because the mobile app controls the camera via Wi-Fi. Web interface and cloud investigation were excluded because they are not connected to the camera.

2) Phase 2: Exploring the IoT Environment/ Documentation

This phase includes exploring the IoT environment by defining the components (C), the expected artifacts (EA), the expected threats (ET), and the consequences of the expected threats to understand the IoT environment. Table 10 clarifies the components. In this case, the researcher focused on mobile investigation, thus the mobile app is considered the main component. The Tapo mobile app controls the camera, the camera company is Tp-link. The information about the camera device collected from the internet was clarified in the previous section (section 4.1.2)/Table 7.

Table 10. Explore the IoT environment of the smart camera case study at the IoT application level

Component (C)	Expected Artifact (EA)	Expected Threat (ET)	Consequences of the Expected Threats
C1: Mobile App (Tapo)	EA1: Screenshots, images, videos, and any related information from mobile apps	ET1: Unauthorized access to the camera app	Tampering with the camera via the camera app also extracts personal information and other useful information.

3) Phase 3: Preparation/ Documentation

In this phase, the investigator should prepare the investigation workstation and the appropriate tools based on the chosen level, the mobile in this case. The mobile App related to the Tapo camera was downloaded and connected to the smart camera. The Belkasoft Evidence Center tool was used for examining the mobile App. A USB cable was needed to connect the mobile device to the workstation. Table 11 clarifies the tools used in the investigation.

Table 11. Tools used in the investigation at the mobile level for smart camera

Tool Name	Description
Belkasoft Evidence Center	A Digital forensic tool, used in the acquisition and analyzing
Investigation Workstation	PC – Windows 10, CPU - AMD with Radeon Graphics 2.9 GHz, 8 Cores
Smart Camera	Tapo C200, Wi-Fi camera, Tplink company
Mobile device	Camera App is downloaded on “Xiaomi Redmi Note 8” mobile to connect with the camera
Mobile App	Tapo mobile app is the targeted app for the investigation

4) Phase 4: Acquisition & Preservation/ Documentation

To investigate the smart camera and collect data generated by it, the researcher conducted several scenarios, playing the roles of both the user and investigator, which are clarified in Table 12.

5) Phase 5: Examining & Analyzing/ Documentation

In this phase, the researcher examined and analyzed the Tapo mobile app connected to the camera. The researcher used both the logical acquisition and the manual acquisition methods to investigate the camera via mobile device. The logical acquisition method was conducted by the Belkasoft tool. The logical image was analyzed and the data related to the camera was found in the path: filesystem > android > data > com.tplink.iot > files > memory. All captured videos and images were found. Fig.14 clarifies the extracted camera artifacts from the logical mobile image by Belkasoft tool.

In the manual acquisition method, the mobile device was explored and the Tapo app was viewed manually. From the IoT mobile app, the investigator was able to access the recorded images and videos, and the camera status was recognized, whether it was ON or OFF. In addition, the camera settings, log data, and camera functions were explored. All this information is considered valuable artifacts of interest. Fig.15 clarifies artifacts that were extracted manually such as camera settings, log data, and camera features.

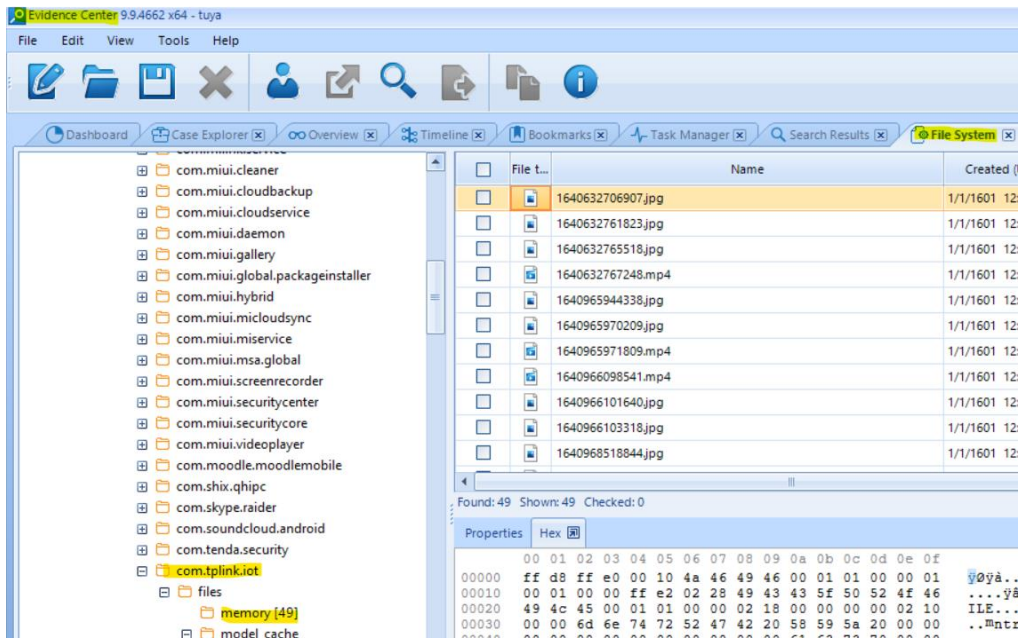


Fig.14. The extracted artifacts from the logical mobile image by Belkasoft Evidence Center Tool

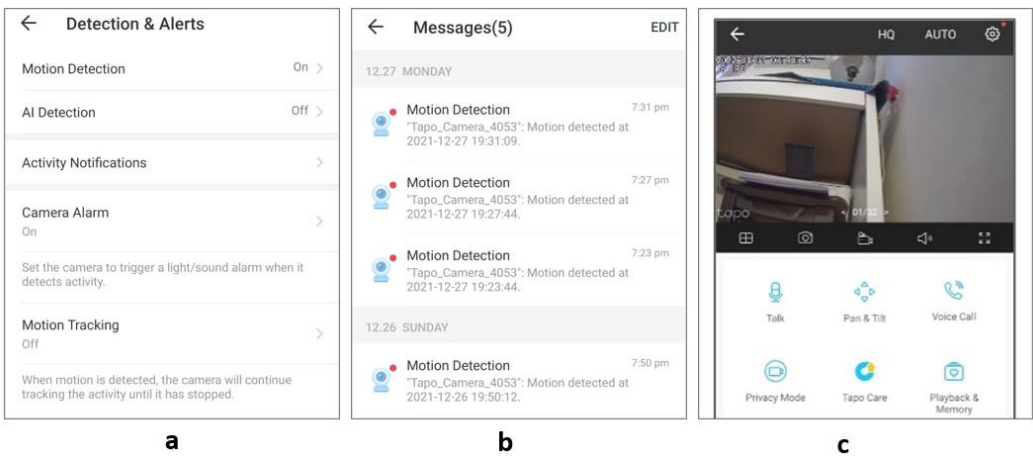


Fig.15. (a) Camera settings; (b) Log data; (c) Camera features

6) Phase 6: Reporting the Results/ Documentation

In this case study, the Tapo mobile app controlled the smart camera, and a set of scenarios were conducted and documented. In the reporting phase, the type of artifacts for each scenario was documented and clarified in Table 12. Finally, the expert witness report should be documented which includes all phases according to the MAoIDFF – IoT framework.

Table 12. Scenarios are conducted on the smart camera at the mobile level.

Scenarios	User Role (actions over the Camera)	Investigator Role	Type of Extracted Artifacts based on A/D matrix (AoI, MA, UA, NA)
Scenarios on Smart Tapo Camera	First, the camera is ON once connected	The output at the mobile App via manual acquisition: camera status is ON	All actions conducted on the camera were proved by the investigator via the mobile app logs page, thus they are all artifacts of Interest (AoI). All captured images and videos were found via manual and logical acquisitions, thus they are all artifacts of Interest (AoI). Additional information about the app and the mobile was extracted from the logical acquisitions, this is considered useful artifacts (UA)
	2 images were captured	The captured images were found in the mobile App via manual and logical acquisitions	
	2 min. of video were captured	The captured video was found in the mobile App via manual and logical acquisitions	
	Then the camera was plugged off	The output at the mobile App via manual acquisition: camera status is OFF	

4.3. Smart Environment Case Study (3rd Case Study)

In this case, seven smart IoT devices were involved in the IoT environment, the smart devices include Wi-Fi smart plug, Wi-Fi temperature & humidity sensor, Wi-Fi smart motion sensor, Wi-Fi remote control, Wi-Fi smart gas detector, Wi-Fi smart smoke detector, and Wi-Fi smart led bulb. The following sub-sections clarify the investigation experiment according to the MAoIDFF-IoT framework.

1) Phase 1: Define the Potential Artifact of Interest (AoI) Locations Based on the Chosen Level/ Documentation.

The IoT application level was chosen to be investigated in this case. The examiner focused on a mobile device as a potential AoI because the mobile app controls all the IoT devices via Wi-Fi. Cloud investigation was excluded because the cloud is not connected to these devices. The network investigation level was excluded because none of the IoT devices are sending streaming data via the network. The investigation excluded the device level because none of these IoT devices had any internal or external memory or operating system. Therefore, this experiment investigated IoT devices at the application level, specifically focusing on the investigation of mobile apps as a potential AoI location.

2) Phase 2: Exploring the IoT environment/ Documentation

The next phase is exploring the IoT environment by defining the components (C), the expected artifacts (EA), the expected threats (ET) for each component, and the consequences of the expected threats to understand the IoT environment. Fig.16 clarifies the general architecture of the IoT environment case study. Table 13 concludes this phase.

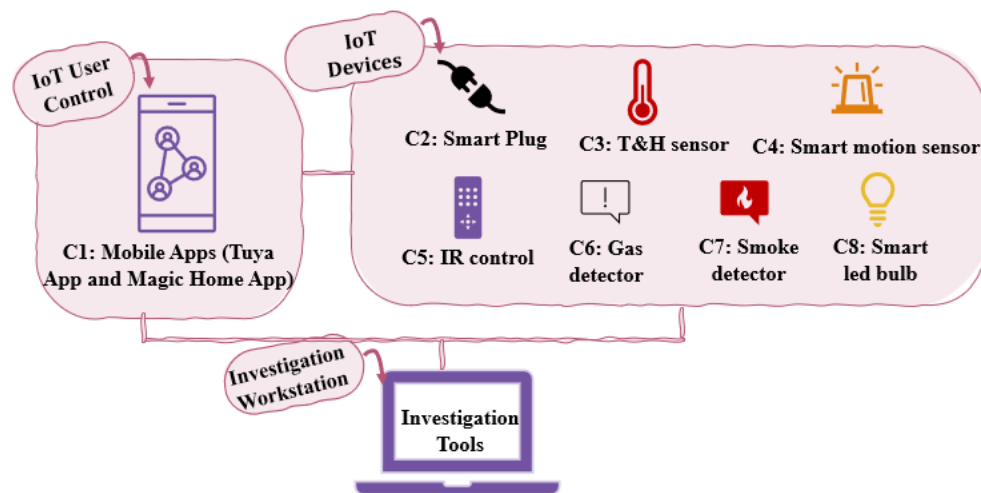


Fig.16. The general architecture of IoT smart environment (3rd case study)

Table 13. Explore the IoT devices of the smart environment according to the MAoIDFF-IoT framework.

Component (C)	Expected Artifact (EA)	Expected Threat (ET)	Consequences of the Expected Threats
C1: Mobile Device/ Mobile IoT App	EA1: Screenshots from mobile apps, logs files information from the IoT app	ET1: Unauthorized access to the IoT App	Tampering with the IoT devices via the mobile app also, extracting personal information, and editing the mobile app configuration.
C2: Smart plug	EA2: Logs files indicating device operating time and other relevant information.	ET2: Unauthorized access to the App and control of the IoT device	Tampering with the IoT device via mobile app, and extracting valuable and personal information This breaches confidentiality, integrity, availability & privacy.
C3: Temperature & humidity sensor			
C4: Smart motion sensor			
C5: Remote control			
C6: Smart gas detector			
C7: Smart smoke detector			
C8: Smart led bulb			

In this case, the main components are the mobile App and the seven smart devices. According to the MAoIDFF-IoT framework, these components should be explored via the internet to find any related or valuable information that may help in the investigation process. The following Table 14 concludes the information and features of the IoT devices collected from the internet.

Table 14. Information about the IoT devices

IoT device	Brand	Application	Devices Features
Smart plug	Elivco	Tuya Mobile App	Wi-Fi connection, App control, energy monitoring, voice control
Smart T&H Sensor	Unknown		Wi-Fi connection, App control, message notifications, alarm
Smart motion sensor	Unknown		Wi-Fi connection, App control, message notifications, log events page
Remote control	Unknown		Support multiple home appliances, Wi-Fi connection, App control, voice control
Smart gas detector	Unknown		Wi-Fi connection, App control, On-Site alarm, fault self-checking, log events page
Smart smoke detector	Unknown		Wi-Fi connection, App control, On-Site alarm, easy installation, log events page
Smart led Bulb	Unknown	Magic Home App	Wi-Fi connection, timer, bright control

3) Phase 3: Preparation/ Documentation

In this phase, the investigator should prepare the investigation workstation and the appropriate tools based on the chosen level (the application level in this case). The tools used in this experiment are stated in Table 15. A USB cable was needed to connect the mobile to the workstation. Fig. 17 clarifies the IoT devices used in the investigation experiment, the mobile app related to each IoT device was downloaded on the mobile. The connection between the mobile app and the IoT devices was checked.

Fig. 17. The IoT devices used in the investigation experiment (3rd case study)

Table 15. Tools used in the investigation experiment at the application level

Tool Name	Description
Belkasoft Evidence Center	Digital forensic tool
MAGNET AXIOM	Digital forensic tool
Investigation Workstation	PC – Windows 10, CPU - AMD with Radeon Graphics 2.9 GHz, 8 Cores
Smart IoT devices	Seven IoT devices, including Wi-Fi smart plug, a Wi-Fi temperature & humidity sensor, Wi-Fi smart motion sensor, Wi-Fi remote control, Wi-Fi smart gas detector, Wi-Fi smart smoke detector, and a Wi-Fi smart led bulb.
Mobile Device	IoT App is downloaded on “Xiaomi Redmi Note 8” mobile
Mobile App	Tuya App and Magic Home App which connected to IoT devices
USB cable	This is used to connect the mobile with the workstation

4) Phase 4: Acquisition & Preservation/ Documentation

Several scenarios that might be happened were conducted by the researcher. The researcher used the manual acquisition method in addition to the logical acquisition method to investigate IoT devices. Both Belkasoft and AXIOM tools were used in the data acquisition. The scenarios conducted on the IoT devices were clarified in Table 16.

5) Phase 5: Examining & Analyzing/ Documentation

In this phase, the researcher examined and analyzed the mobile apps that were connected to IoT devices. The IoT apps, Tuya app, and Magic Home app were navigated manually to investigate the IoT devices. Fig. 18 clarifies artifacts extracted by the manual acquisition method, including IoT devices connected with the Tuya App in Fig. 18 (a), and the smart bulb connected with the Magic home app in Fig. 18 (b,c). The status of the switch with the timestamp is clarified in Fig. 18 (d). Motion detection records are clarified in Fig. 18 (e). The temperature and humidity with the timestamp are stated in Fig. 18 (f).

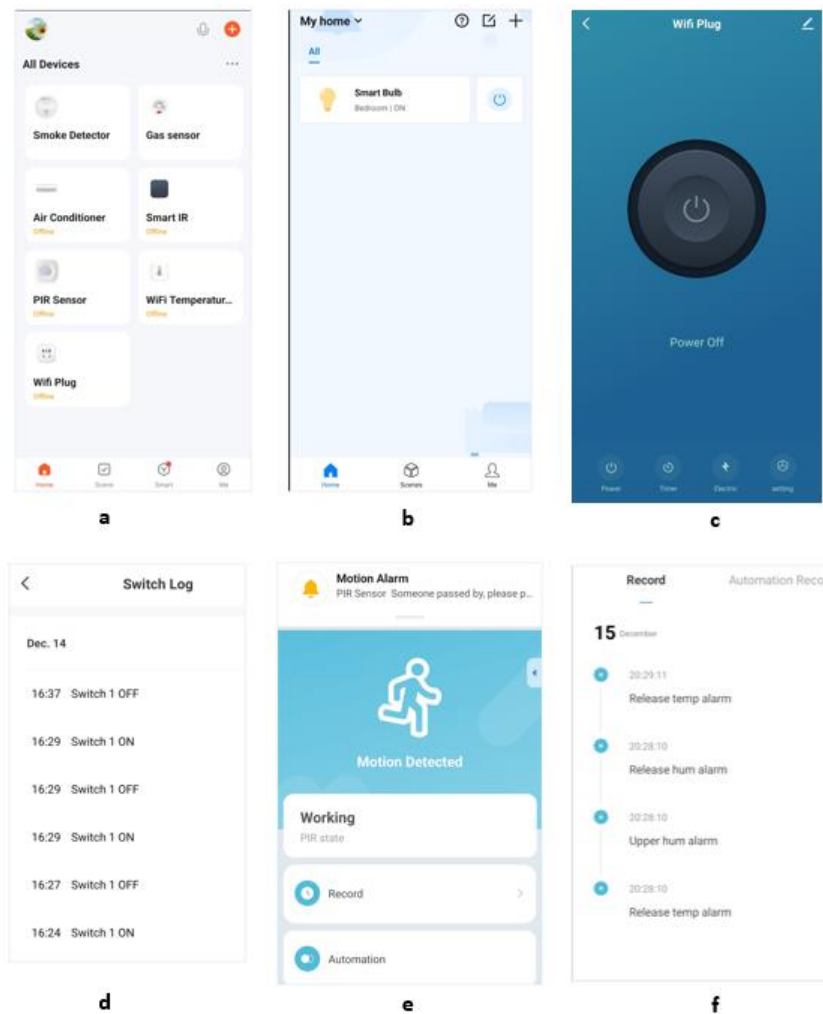


Fig. 18. Artifacts of Interest extracted; (a) IoT devices connected with the Tuya App, (b,c) Smart bulb connected with the Magic home app, (d) The smart switch log page, (e) Motion detection records, (f) T & H sensor log page

The logical acquisition was conducted and analyzed using the Belkasoft Evidence Center tool. Data about the Tuya and Magic Home applications were found from the path: Filesystem/Android/data/com.tuya.smart, Filesystem/Android/data/com.magichome.smart. Moreover, the MAGNET AXIOM tool was used in conducting mobile logical acquisition and analyzing the IoT apps. Artifacts of interest were found including the alarm timestamp generated from the IoT apps as shown in Fig. 19. In addition, the logs files for Tuya and magic home apps.

```

> backup > AXIOM - Dec 29 2022 112230 > acquiring > Live Data > Dumpsys Data
alarm - Notepad
File Edit Format View Help
*walarm*:IpClient.wlan0.EVENT_DHCPACTION_TIMEOUT
+22ms 1 wakes 1 alarms, last -2d20h40m23s549ms:
*walarm*:DhcpClient.wlan0.REBIND
+5ms 1 wakes 1 alarms, last -1d13h54m36s907ms:
*walarm*:DhcpClient.wlan0.TIMEOUT
9810:com.xiaomi.finddevice +5s242ms running, 15 wakeups:
+5s109ms 14 wakes 14 alarms, last -13h54m12s377ms:
*walarm*:com.xiaomi.finddevice/.v2.update.PeriodicUpdateTaskRecei
+133ms 1 wakes 1 alarms, last -13d15h23m21s881ms:
*walarm*:com.xiaomi.finddevice/.v2.receiver.AlarmReceiver
u0a1:com.tuya.smart +7s42ms running, 100 wakeups:
+7s42ms 100 wakes 100 alarms, last -16h53m25s683ms:
*walarm*:MqttService.pingSender.com.tuya.smart_mb_746cf2699d184cf
u0a20:com.google.android.gms +9m51s635ms running, 2272 wakeups:
+2m3s622ms 374 wakes 374 alarms, last -3m41s800ms:
*walarm*:com.google.android.gms.gcm.ACTION_CHECK_QUEUE

```

Fig. 19. The alarm timestamp generated from the IoT apps from the AXIOM tool

6) Phase 6: Reporting the Results/ Documentation

All IoT devices in this case were connected to the related mobile App, and then a set of scenarios were conducted over the devices. Thus, all previous phases were recorded and explained. In the reporting phase, the types of extracted artifacts according to the “Action/Detection matrix” for each scenario were documented and clarified in Table 16. All actions performed by the user and verified by the investigator were considered (AoI).

Table 16. Type of artifacts according to the scenarios conducted on the IoT devices.

Scenarios	User Role (actions over IoT devices)	Investigator Role	Type of Extracted Artifacts based on A/D matrix (AoI, MA, UA, NA)
Scenarios on Smart plug	First, the switch is ON once connected	The output at the mobile App Switch log: 16:24 Switch ON	All actions were proved by the investigator via the mobile app switch log, thus they are all artifacts of Interest (AoI).
	The switch is off after 3 min schedule automatically	The output at the mobile App Switch log: 16:27 Switch OFF	
	The switch is on after 2 min schedule automatically	The output at the mobile App Switch log: 16:29 Switch ON	
	The switch is off manually from the App	The output at the mobile App Switch log: 16:29 Switch OFF	
	The switch is on manually from the App	The output at the mobile App Switch log: 16:29 Switch ON	
	The countdown is set to be switched off after 8 min	The output at the mobile App Switch log: 16:37 Switch ON	
Scenarios on Smart Temperature & Humidity Sensor	First, the sensor is ON once connected	The output at the mobile App log: The temperature is 27 The humidity is 58%, and the sensor status is ON	All actions were proved by the investigator via the mobile app log, thus they are all artifacts of Interest (AoI).
	The sensor is off	A message from the app clarifies that a notification will be sent after 30 min of the offline status	
Scenarios on Smart Motion Sensor	First, the sensor is ON once connected	The sensor status is ON via Mobile App	All actions were proved by the investigator via the mobile app, thus they are all artifacts of Interest (AoI).
	A motion is conducted near the sensor	A message from the app clarifies that a motion is conducted.	
	The sensor is off	The sensor status is OFF via Mobile App	
Scenarios on Smart IR control	First, the device is ON once connected	The sensor status is ON via Mobile App	All actions were proved by the investigator via the mobile app, thus they are all artifacts of Interest (AoI).
	An Air condition is connected, and it was turned ON by the IR controller	The Air condition status is ON via Mobile App	
	An Air condition was turned OFF by the IR controller	The Air condition status is OFF via Mobile App	
Scenarios on Smart gas detector	First, the device is ON once connected	The gas detector status is ON/normal via Mobile App	All actions were proved by the investigator via the mobile app, thus they are all artifacts of Interest (AoI).
	A gas was released near the device	A notification gas alarm with a timestamp is logged via the mobile app clarifying that gas was detected	
	The detector is OFF	The gas detector status is OFF via the mobile App	
Scenarios on Smart smoke detector	First, the device is ON once connected	The smoke detector status is ON/normal via the mobile App	All actions were proved by the investigator via the mobile app, thus they are all artifacts of Interest (AoI).
	Smoke was released near the device	A notification smoke alarm with a timestamp is logged via the mobile app clarifying that smoke was detected	
	The detector is OFF	The smoke detector status is OFF via the mobile App	
Scenarios on Smart led light bulb	First, the bulb is ON once connected	The smart bulb status is ON via the mobile App	All actions were proved by the investigator via the mobile app, thus they are all artifacts of Interest (AoI).
	The bulb is OFF	The smart bulb status is OFF via the mobile App	
General activities from IoT Apps	--	--	Notifications, alarms, and other activities from Tuya and the Magic Home app were found in the log files, obtained from the AXIOM tool which are considered (AoI)
No actions were conducted	--	--	Additional info. about the app and the mobile was extracted from the logical acquisitions via AXIOM and Belkasoft, this is considered useful artifacts (UA)

4.4 Key Challenges in the Experiments

The following challenges were faced while conducting the experiments:

- Extracting artifacts at each level of the IoT device is a big challenge as there are different types of brands, standards, protocols, FS, and OS related to the IoT devices. Thus, the investigator should be closely informed of the latest developments in the Internet of Things.
- The researcher didn't find any investigation tool specialized for the IoT devices that encompasses the multi-level structure of the IoT devices. Computer forensics tools such as Autopsy, Belkasoft, and AXIOM did a satisfactory job. However, it would be better to have a tool for IoT investigation that considers the structure of the IoT devices.
- Technical issues were faced while experimenting, such as device connection and other technical problems, and they were overcome.

4.5. Recommendations

The 2nd case study proved the effectiveness of the MAoIDFF-IoT framework's multilevel investigation approach, which helped to identify more valuable (AoI) that were missed in the 1st case study. For example, the pictures recorded via the camera were not found in the external memory at the device investigation level in (1st case study - section 4.1), but they were found via manual and logical acquisition at the mobile investigation level in (2nd case study - section 4.2). In addition, at the mobile level investigation, the investigator found more information about the camera app via log files. Therefore, it is recommended to investigate multilevel to avoid missing artifacts and find additional (AoI).

In the 3rd case, (section 4.3) the researcher noted that each app has its own features and behavior over the mobile device. It is easy to extract IoT-related artifacts from some IoT devices, while others require more examination and search. Therefore, it is recommended to conduct reverse engineering for IoT apps in case the investigator doesn't find apparent artifacts, to know where the app stores the related data on the mobile. The extracted artifacts from each forensic tool may differ. For example, the log files for the Tuya app were found via the AXIOM tool, while the javascript files for the IoT app were obtained from the Belkasoft tool. Therefore, it is recommended to use various tools to achieve optimal results. It is advisable to search online for helpful information about IoT devices. Moreover, the well-organized phases in the MAoIDFF-IoT framework facilitated the investigation process and can be beneficial to other investigators in the future. It guided the researcher when the experiment was repeated with other different IoT devices.

5. Results and Discussion

The proposed framework (MAoIDFF-IoT) was evaluated and tested by three case studies. The 1st case was performed on a smart camera at the device level. In this case, the researcher focused on investigating the operating system (OS) and the external memory file system, FAT32. The FAT32 in-depth was analyzed through four main steps mentioned in the proposed framework. The 2nd case was conducted on a smart camera at the application level. The researcher made the logical and manual acquisition to extract artifacts from the mobile camera app. The 3rd case was conducted on a smart environment that contained seven IoT devices. The researcher focused on extracting artifacts from the mobile apps that control these IoT devices. Table 17 summarizes the three case studies with related chosen investigation levels.

Table 17. The IoT devices used in case studies with related chosen investigation level

IoT device	Device level investigation	Network level investigation	Application level investigation	
Smart Camera	✓ (1 st case study)	--	✓ (2 nd case study)	
Wifi smart plug	--	--	✓ (Tuya Mobile App)	
Wifi Temperature & Humidity Sensor	--	--	✓ (Tuya Mobile App)	
Motion Sensor	--	--	✓ (Tuya Mobile App)	
Wi-Fi Universal Remote control	--	--	✓ (Tuya Mobile App)	
Gas detector	--	--	✓ (Tuya Mobile App)	
Smoke detector	--	--	✓ (Tuya Mobile App)	
Smart led Bulb	--	--	✓ (magic home – smart home Mobile App)	(3 rd case study)

5.1. Features and Novel Aspects of MAoIDFF-IoT Proposed Framework

The proposed framework was adapted to suit the unique characteristics of IoT devices. The experimental analysis and results demonstrate the effectiveness and advantages of the proposed framework throughout its phases, which are clarified in the following.

1) *Focusing on AoI to save time and efforts*

The MAoIDFF-IoT framework introduces (AoI) investigation in a manner not previously presented. In the first phase, the targeted investigation level should be selected based on the structure and case of the IoT. Thus, MAoIDFF-IoT focuses on analyzing and examining the potential locations of AoI, not all the data generated by IoT devices to accelerate the investigation process and make it more efficient.

2) *The importance of exploring at several phases*

The proposed framework explores the IoT environment at various phases. In the first phase, the initial exploration aimed to define the potential AoI at the targeted level of investigation. In the second phase, the exploration aims to define Expected Artifacts (EA) at the targeted/chosen level. Also, by searching online for IoT devices, relevant information can be gathered to assist in the investigation process. Exploration at several phases is essential for defining the scope of the investigation. Thus, defining AoI precisely.

3) *The organized structure with a standardized framework*

The traditional phases of digital forensics, including preservation, collection, examination, analysis, and reporting, are commonly used in most previous digital forensics frameworks [23,70,72,75–80]. These traditional phases have been proven to be successful and inclusive in digital investigations. However, in MAoIDFF-IoT, these traditional phases include additional new sub-phases that have been added to fit the heterogeneous nature of IoT environments.

4) *Maintains the integrity*

Documentation is considered essential during all phases of IoT digital forensics to prevent the loss of any (AoI) during the investigation [70]. What sets this framework apart from previous frameworks is that it suggests a well-organized structure for the expert witness report containing the proposed MAoIDFF-IoT phases. Also, It emphasizes the importance of documentation across all phases. This is important for court submissions.

5) *Inclusive, covering all the IoT levels, to avoid missing any critical artifact.*

The MAoIDFF-IoT framework considers multi-level investigation because if any artifact from one level is missed, it can be detected at another level. Moreover, it explores all potential (AoI) locations based on the targeted investigation level which is a good practice supported in the proposed framework. This practice adds value when developing an inclusive IoT digital forensics framework. The potential (AoI) might be extracted from three main levels, including (1) device level (AoI locations: physical device, memory, filesystem, OS), (2) network level (AoI locations: network devices, protocols, traffic), and (3) application level (AoI locations: web interface, mobile app, cloud). Further, in phase five, analyzing & examining, the framework emphasizes the use of appropriate tools and methods to decrypt and analyze the encrypted data. In addition, reverse engineering is considered for extracting critical artifacts.

6) *Define types of extracted artifacts based on the Action/ Detection Matrix.*

The experimental approach employed in this research differs from previous studies. In the acquisition & preservation phase, the researcher played the role of both user and investigator by conducting several actions on the IoT devices. In the examining & analyzing phase, the researcher verified these actions by analyzing the data obtained after each scenario and classifying extracted artifacts according to the conducted actions. The MAoIDFF-IoT framework introduces an (A/D) matrix and four types of extracted artifacts: missed artifact (MA), no artifact (NA), useful artifact (UA), or artifact of interest (AoI). The matrix utilized is novel and has not been addressed in prior literature.

7) *Usability*

The MAoIDFF-IoT framework has the potential to be utilized for all current and future digital crimes. Phase six of the framework includes guidelines, recommendations, and notes to assist and support future investigators. The framework is well-organized, and flexible, and can be modified to include additional sub-phases and activities needed for each specific case. Table 18 provides a comparison between the MAoIDFF-IoT and other existing frameworks. This comparison emphasizes the distinctive characteristics of the proposed framework in contrast to its predecessors.

Table 18. MAoIDFF-IoT framework in comparison with previous frameworks

Framework Advantage	The proposed framework MAoIDFF-IoT	Quick et al., 2014 [71]	Carrier and Spafford, 2004 [70]	Kebande et al., 2018 [63]	Li et al., 2019 [65]	Kebande and Ray, 2016 [67]	Babun et al., 2021 [55]	Bouchaud et al., 2018 [57]
Focus on the Artifact of Interest (AoI)	✓	✓						
Identification phase to explore the environment	✓			✓	✓	✓	✓	✓
Cover the traditional digital forensics process	✓	✓	✓	✓	✓	✓	✓	✓
Maintain the integrity	✓		✓	✓	✓	✓	✓	✓
Consider the analysis of encrypted data	✓				✓		✓	
The distinctive characteristics of the MAoIDFF that have not been addressed by others: <ul style="list-style-type: none"> It covers all levels of IoT and selects a specific level for investigation based on the case. It is advisable to conduct a multi-level investigation to avoid missing any artifacts. This approach ensures that if any artifact is missed at one level, it may be discovered at another level. It proposes investigating the potential AoI locations based on the chosen level. It considers the exploration process at several phases to determine AoI precisely by defining the potential AoI locations, the components (C), and the expected artifacts (EA). It defines the types of extracted artifacts (Artifact of Interest - AoI, Useful Artifact - UA, Missed Artifact -MA, No Artifact - NA) based on the proposed (A/D) matrix. It suggests a well-organized structure for the expert witness report. 								

5.2. Limitations in this Research

While our research provides a valuable addition to the field of IoT digital forensics, several limitations should be acknowledged. Firstly, the MAoIDFF-IoT framework was evaluated and applied, and its effectiveness was demonstrated through three case studies. However, it is an excellent step to conduct more real scenario experiments and test the proposed framework on different types of IoT devices. This emphasizes the applicability and usability of this framework. Any digital investigator can benefit from and enjoy the advantages of the well-organized phases and structure of the MAoIDFF-IoT framework. Additionally, IoT devices could have various operating systems and file systems, which poses a challenge for digital investigators. Therefore, it would be beneficial to prioritize investigating and exploring different types of operating systems and file systems associated with IoT devices. Moreover, the MAoIDFF-IoT framework proposes that if any encrypted data is found, it is suggested to use the appropriate tool or method to decrypt and analyze the encrypted data. However, it would be a valuable addition if researchers delve deeper to uncover details about decrypting the encryption and investigate volatile data generated by IoT devices.

6. Conclusion and FutureWork

The focus of this research was on IoT digital forensics. A novel framework named "Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT)" was proposed. This framework consists of six main phases, each accompanied by enhanced sub-phases, to ensure a thorough and effective investigation. The documentation phase is critical across all six phases for maintaining integrity and submitting a report to the court. MAoIDFF-IoT covers all levels of IoT (device, network, application) and focuses on Artifacts of Interest (AoI) for each level, aiming to save time and effort. The framework was evaluated through case studies and found to be effective in extracting artifacts and accelerating the investigation process. The proposed action/detection matrix and the artifact types (MA, NA, UA, and AoI) were considered additions to the framework. The experimental results indicate that the MAoIDFF-IoT framework has attractive features. Future work should involve applying the MAoIDFF-IoT framework to more realistic scenarios to demonstrate its applicability and usability. Other types of IoT filesystems, as well as volatile and encrypted data from IoT devices, should also be analyzed. In addition, for future work, it would be valuable to develop an investigative IoT tool and merge artificial intelligence techniques considering the multilevel structure of the MAoIDFF-IoT framework, along with the proposed reporting structure. This paper presents three case studies investigating various IoT devices at both the device and application levels. However, the network level was not investigated or included in the case studies. Therefore, it is recommended to conduct several scenarios and apply the proposed framework to the IoT device that sends streaming traffic via the network in future research.

References

- [1] C. Maxim, Z. Sherali, B. Zubair, and W. Andrew, "Internet of Things Forensics: The Need, Process Models, and Open Issues," *IT Professional*, vol. 20, pp. 40–49, 2018, doi: 10.1109/MITP.2018.032501747.
- [2] K. A. Z. Ariffin and F. H. Ahmad, "Indicators for Maturity and Readiness for Digital Forensic Investigation in Era of Industrial Revolution 4.0," *Computers and Security*, vol. 105, p. 102237, 2021, doi: 10.1016/j.cose.2021.102237.
- [3] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," *IEEE Communications Surveys and Tutorials*, vol. 22, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.
- [4] S. Alabdulsalam, K. Schaefer, T. Kechadi, and N. A. Le, "Internet of Things Forensics: Challenges and Case Study," in *IFIP International Conference on Digital Forensics*, 2018, vol. 13, pp. 35–48.
- [5] J. Voas, "Demystifying the Internet of Things," *Computer*, vol. 49, no. 6, pp. 80–83, 2016, doi: 10.1109/MC.2016.162.
- [6] S. Zawood and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," in *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, 2015, vol. 7, pp. 279–284, doi: 10.1109/SCC.2015.46.
- [7] Y. Salem, M. Owda, and A. Owda, "An Experimental Approach for Locating WhatsApp Digital Forensics Artifacts on Windows 10 and the Cloud," *International Journal of Electronic Security and Digital Forensics*, vol. 15, no. 1, p. 1, 2023, doi: 10.1504/ijesdf.2023.10051774.
- [8] Y. Salem, M. Moreb, and K. S. Rabayah, "Evaluation of Information Security Awareness among Palestinian Learners," in *2021 International Conference on Information Technology (ICIT)*, 2021, pp. 21–26, doi: 10.1109/icit52682.2021.9491639.
- [9] P. S. Lee, M. Owda, and K. Crockett, "The detection of fraud activities on the stock market through forward analysis methodology of financial discussion boards," *Advances in Intelligent Systems and Computing*, vol. 887, no. April, pp. 212–220, 2019, doi: 10.1007/978-3-030-03405-4_14.
- [10] K. Kyei, P. Zavarsky, D. Lindskog, and R. Ruhl, "A review and comparative study of digital forensic investigation models," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 114 LNICST, pp. 314–327, 2013, doi: 10.1007/978-3-642-39891-9_20.
- [11] Y. Yusoff, R. Ismail, and Z. Hassan, "Common Phases of Computer Forensics Investigation Models," *International Journal of Computer Science and Information Technology*, vol. 49, no. 3, pp. 17–31, 2011, doi: 10.5121/ijcsit.2011.3302.
- [12] M. Wu, T. Lu, F.-Y. Ling, L. Sun, and H.-Y. Du, "Research on the application-driven architecture in internet of things," *2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE) Research*, vol. 4, pp. 458–465, 2010, doi: 10.3233/978-1-61499-722-1-458.
- [13] J. Lin, W. YU, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," *IEEE internet of things journal*, vol. 18, pp. 1125–42, 2017, doi: 10.1109/I-SMAC.2018.8653708.
- [14] L. Li, "Study on Security Architecture in the Internet of Things," *Proceedings of 2012 international conference on measurement, information and control*, vol. 4, pp. 374–377, 2012, doi: 10.1016/B978-0-12-804458-2.00002-0.
- [15] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, vol. 6, pp. 336–341, 2015, doi: 10.1109/ICITST.2015.7412116.
- [16] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," *Proceedings - IEEE Symposium on Computers and Communications*, vol. 8, pp. 180–187, 2015, doi: 10.1109/ISCC.2015.7405513.
- [17] L. Patra and U. P. Rao, "Internet of Things-Architecture, applications, security and other major challenges," *Proceedings of the 10th INDIACom; 2016 3rd International Conference on Computing for Sustainable Global Development, INDIACom 2016*, vol. 6, pp. 1201–1206, 2016.
- [18] M. U.Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A Critical Analysis on the Security Concerns of Internet of Things (IoT)," *International Journal of Computer Applications*, vol. 6, pp. 1–6, 2015, doi: 10.5120/19547-1280.
- [19] M. Pollitt, "Computer Forensics: an approach to evidence in cyberspace," *Proceedings of the National Information Systems Security Conference*, vol. 5, 1995, doi: 10.1201/9780849305627.
- [20] G. Ruibin, C. K. Yun, and M. Gaertner, "Case-Relevance Information Investigation : Binding Computer Intelligence to the Current Computer Forensic Framework," *International Journal*, vol. 4, no. 1, pp. 1–13, 2005, [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.81.4278&rep=rep1&type=pdf>.
- [21] K. Kent, S. Chevalier, T. Grance, and H. Dang, "Guide to Integrating Forensic Techniques into Incident Response," *The National Institute of Standards and Technology*, pp. 800–86, 2006.
- [22] M. K. Rogers *et al.*, "Computer Forensics Field Triage Process Model," *Journal of Digital Forensics, Security and Law*, vol. 1, no. 2, pp. 1–21, 2006, [Online]. Available: <https://commons.erau.edu/jdfsl/vol1/iss2/2>.
- [23] M. Kohn, E. JHP, and M. Olivier, "Framework for a Digital Forensic Investigation," *Information and Computer Security Architectures Research Group (ICSA) Department of Computer Science ,University of Pretoria*, vol. 64, pp. S33–S34, 2006, doi: 10.14943/jjvr.64.suppl.s33.
- [24] B. Derek and H. Ewa, "Computer Forensic Analysis in a Virtual Environment," *International journal of digital evidence* 6.2, vol. 6, no. 2, pp. 143–151, 2007, doi: 10.1109/SEW.2003.1270737.
- [25] I. O, D. Chris, and D. David, "A New Approach of Digital Forensic Model for Digital Forensic Investigation," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 12, pp. 175–178, 2011, doi: 10.14569/ijacsa.2011.021226.
- [26] M. D. Kohn, M. M. Eloff, and J. H. P. Eloff, "Integrated digital forensic process model," *Computers and Security*, vol. 38, pp. 103–115, 2013, doi: 10.1016/j.cose.2013.05.001.
- [27] M. D. K, "Integrated Digital Forensic Process Model," *Computers & Security*, vol. 38, no. November, pp. 103–115, 2013.
- [28] D. Sudyana, "Analysis and Evaluation Digital Forensic Investigation Framework Using Iso 27037:2012," *International Journal of Cyber-Security and Digital Forensics*, vol. 8, no. 1, pp. 1–14, 2019, doi: 10.17781/p002464.

- [29] G. Horsman, "Framework for Reliable Experimental Design (FRED): A research framework to ensure the dependable interpretation of digital data for digital forensics," *Computers & Security*, vol. 25, pp. 1–24, 2018.
- [30] A. A. Thakar, K. Kumar, and B. Patel, "Next Generation Digital Forensic Investigation Model (NGDFIM) - Enhanced, Time Reducing and Comprehensive Framework," *Journal of Physics: Conference Series*, vol. 1767, no. 1, pp. 1–10, 2021, doi: 10.1088/1742-6596/1767/1/012054.
- [31] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of Things Forensics: Challenges and approaches," in *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2013, vol. 7, pp. 608–615, doi: 10.4108/icst.collaboratecom.2013.254159.
- [32] H. Chung, J. Park, and S. Lee, "Digital Forensic Approaches for Amazon Alexa Ecosystem," *DFRWS 2017 USA - Proceedings of the 17th Annual DFRWS USA*, vol. 22, pp. S15–S25, 2017, doi: 10.1016/j.diin.2017.06.010.
- [33] A. Awasthi, H. O. L. Read, K. Xynos, and I. Sutherland, "Welcome pwn: Almond Smart Home Hub Forensics," *Proceedings of the Digital Forensic Research Conference, DFRWS 2018 USA*, vol. 26, pp. S38–S46, 2018, doi: 10.1016/j.diin.2018.04.014.
- [34] J. Song and J. Li, "A Framework for Digital Forensic Investigation of Big Data," *2020 3rd International Conference on Artificial Intelligence and Big Data, ICAIBD 2020*, vol. 5, pp. 96–100, 2020, doi: 10.1109/ICAIBD49809.2020.9137498.
- [35] M. S. Kirmani and M. T. Bandy, "Digital Forensics in the Context of the Internet of Things," *Cyber Warfare and Terrorism*, vol. 24, no. January, pp. 1178–1200, 2020, doi: 10.4018/978-1-7998-2466-4.ch069.
- [36] T. Wu, F. Breitingner, and I. Baggili, "IoT Ignorance is Digital Forensics Research Bliss: A Survey to Understand IoT Forensics Definitions, Challenges and Future Research Directions," *Proceedings of the 14th International Conference on Availability, Reliability and Security*, vol. 16, pp. 1–15, 2019, doi: 10.1145/3339252.3340504.
- [37] N. I. of Standards and T. (NIST), "NIST Cloud Computing Forensic Science Challenges," 2014, [Online]. Available: http://safegov.org/media/72648/nist_digital_forensics_draft_8006.pdf.
- [38] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, "Internet of Things Forensics: Recent Advances, Taxonomy, Requirements, and Open Challenges," *Future Generation Computer Systems*, vol. 92, pp. 265–275, 2019, doi: 10.1016/j.future.2018.09.058.
- [39] Y. Y. Teing, A. Dehghantanha, and K. K. R. Choo, "CloudMe Forensics: A Case of Big Data Forensic Investigation," *Concurrency and Computation: Practice and Experience*, vol. 13, pp. 1–12, 2018, doi: 10.1002/cpe.4277.
- [40] M. M. Salim, S. Rathore, and J. H. Park, "Distributed Denial of Service Attacks and its Defenses in IoT: A Survey," *Journal of Supercomputing*, vol. 76, pp. 5320–5363, 2020, doi: 10.1007/s11227-019-02945-z.
- [41] T. Wu, "Digital Forensic Investigation of IoT Devices: Tools and Methods," (*Doctoral dissertation, University of Oxford*), 2020.
- [42] S. Watson and A. Dehghantanha, "Digital Forensics: The Missing Piece of the Internet of Things Promise," *Computer Fraud and Security*, vol. 6, pp. 5–8, 2016, doi: 10.1016/S1361-3723(15)30045-2.
- [43] F. Servida and E. Casey, "IoT Forensic Challenges and Opportunities for Digital Traces," *Digital Investigation*, vol. 28, pp. S22–S29, 2019, doi: 10.1016/j.diin.2019.01.012.
- [44] B. Carrier, *File System Forensic Analysis*, vol. 511. 2005.
- [45] J. P. Sandvik, K. Franke, H. Abie, and A. Årnes, "Coffee forensics — Reconstructing data in IoT devices running Contiki OS," *Forensic Science International: Digital Investigation*, vol. 37, 2021, doi: 10.1016/j.fsidi.2021.301188.
- [46] S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, and I. Ahmad, "Network forensics: Review, taxonomy, and open challenges," *Journal of Network and Computer Applications*, vol. 66, pp. 214–235, 2016, doi: 10.1016/j.jnca.2016.03.005.
- [47] E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digital Investigation*, vol. 7, no. 1–2, pp. 14–27, 2010, doi: 10.1016/j.diin.2010.02.003.
- [48] O. Afonin and V. Katalov, *Mobile Forensics – Advanced Investigative Strategies*. 2016.
- [49] M. J. Islam, M. Mahin, A. Khatun, B. C. Debnath, and S. Kabir, "Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach," *1st International Conference on Advances in Science, Engineering and Robotics Technology 2019, ICASERT 2019*, vol. 5, pp. 1–6, 2019, doi: 10.1109/ICASERT.2019.8934707.
- [50] A. Y. Mahmoud, "Theory and Practice of Forensics Techniques for Smartphones," 2018.
- [51] R. Tamma, O. Skulkin, H. Mahalik, and S. Bommisetty, *Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices*. 2014.
- [52] M. Faheem, T. Kechadi, and N. A. Le-Khac, "The State of the Art Forensic Techniques in Mobile Cloud Environment," *International Journal of Digital Crime and Forensics*, vol. 7, no. 2, pp. 1–19, 2015, doi: 10.4018/ijdcf.2015040101.
- [53] R. Ayers, W. Jansen, and S. Brothers, "Guidelines on mobile device forensics (NIST Special Publication 800-101 Revision 1)," *NIST Special Publication*, p. 85, 2014, [Online]. Available: <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf>.
- [54] C. Meffert, D. Clark, I. Baggili, and F. Breitingner, "Forensic State Acquisition from Internet of Things (FSAIoT): A General Framework and Practical Approach for IoT Forensics through IoT Device State Acquisition," *Proceedings of the 12th International Conference on Availability, Reliability and Security*, vol. 13, pp. 1–12, 2017, doi: 10.1145/3098954.3104053.
- [55] L. Babun, A. K. Sikder, A. Acar, and S. Uluagac, "The Truth Shall Set Thee Free: Enabling Practical Forensic Capabilities in Smart Environments," in *The Network and Distributed System Security (NDSS) Symposium*, 2022, no. April, pp. 1–17, doi: 10.14722/ndss.2022.24133.
- [56] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, "IoTdots: A Digital Forensics Framework for Smart Environments," *ArXiv preprint arXiv:1809.00745*, vol. 13, pp. 2–15, 2018, [Online]. Available: <http://arxiv.org/abs/1809.00745>.
- [57] F. Bouchaud, G. Grimaud, and T. Vantroys, "IoT Forensic a Digital Investigation Framework for IoT Systems," in *2018 10th international conference on electronics, computers and artificial intelligence (ECAI)*, 2018, vol. 5, pp. 1–4, doi: 10.1145/3230833.3233257.
- [58] A. Nieto, R. Rios, and J. Lopez, "A Methodology for Privacy-Aware IoT-Forensics," *2017 IEEE Trustcom/BigDataSE/ICSS*, vol. 7, pp. 626–633, 2017, doi: 10.1109/Trustcom/BigDataSE/ICSS.2017.293.
- [59] T. Zia, P. Liu, and W. Han, "Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)," *ACM International Conference Proceeding Series*, vol. Part F1305, pp. 1–7, 2017, doi: 10.1145/3098954.3104052.

- [60] M. A. Saleh, S. Hajar Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Common Investigation Process Model for Internet of Things Forensics," *2021 2nd International Conference on Smart Computing and Electronic Enterprise: Ubiquitous, Adaptive, and Sustainable Computing Solutions for New Normal, ICSCEE 2021*, vol. 5, pp. 84–89, 2021, doi: 10.1109/ICSCEE50312.2021.9498045.
- [61] M. Hossain, Y. Karim, and R. Hasan, "FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger," *Proceedings - 2018 IEEE International Congress on Internet of Things, ICIOT 2018 - Part of the 2018 IEEE World Congress on Services*, vol. 8, pp. 33–40, 2018, doi: 10.1109/ICIOT.2018.00012.
- [62] W. A. Mahrous, M. Farouk, and S. M. Darwish, "An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash," *IEEE Access*, vol. 9, pp. 151327–151336, 2021, doi: 10.1109/ACCESS.2021.3126715.
- [63] V. R. Kebande *et al.*, "Towards an Integrated Digital Forensic Investigation Framework for an IoT-based Ecosystem," *2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018*, vol. 6, pp. 93–98, 2018, doi: 10.1109/SmartIoT.2018.00-19.
- [64] M. Hossain, "Towards a Holistic Framework for Secure, Privacy-aware, and Trustworthy Internet of Things Using Resource-efficient Cryptographic Schemes," *Doctoral dissertation, The University of Alabama at Birmingham*, vol. 1–371, p. 371, 2018, doi: 10.13140/RG.2.2.33117.72165.
- [65] S. Li, K. K. Raymond, Q. Sun, W. J. Buchanan, and J. Cao, "IoT Forensics: Amazon Echo as a Use Case," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6487–6497, 2019, doi: 10.1109/IIOT.2019.2906946.
- [66] E. Oriwoh and P. Sant, "The forensics edge management system: A concept and design," *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*, pp. 544–550, 2013, doi: 10.1109/UIC-ATC.2013.71.
- [67] V. R. Kebande and I. Ray, "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)," *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, vol. 7, pp. 356–362, 2016, doi: 10.1109/FiCloud.2016.57.
- [68] J. M. C. Gómez, J. R. Gómez, J. C. Mondéjar, and J. L. M. Martínez, "Non-Volatile Memory Forensic Analysis in Windows 10 IoT Core," *Entropy*, vol. 29, pp. 1–28, 2019, doi: 10.3390/e21121141.
- [69] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 16, pp. 91–106, 2020, doi: 10.1016/j.future.2020.03.042.
- [70] B. Carrier and E. Spafford, "An event-based digital forensic investigation framework," *Digital forensic research workshop*, pp. 1–12, 2004, [Online]. Available: http://www.digital-evidence.org/papers/dfrws_event.pdf.
- [71] D. Quick and K.-K. C. Raymond, "Data reduction and data mining framework for digital forensic evidence: Storage, intelligence, review and archive," vol. 11, pp. 1–11, 2014.
- [72] G. Reith, M., Carr, C., & Gunsch, "An Examination of Digital Forensic Models," *International Journal of Digital Evidence*, vol. 13, pp. 1–12, 2002, doi: 10.1109/SADFE.2009.8.
- [73] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," *International Journal of Computer Science and Security (IJCSS)*, vol. 5, no. 1, pp. 118–131, 2011, [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.227.8647&rep=rep1&type=pdf>.
- [74] Tapo, "Tapo Smart Camera," 2022. <https://www.tapo.com/us/product/smart-camera/tapo-c200/> (accessed Mar. 15, 2022).
- [75] G. Palmer, "DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research," *Digital Forensics Workshop (DFRWS)*, vol. 49, 2001, doi: 10.1016/0032-3950(82)90064-8.
- [76] B. Carrier and E. H. Spafford, "Getting Physical with the Investigative Process," *International Journal of Digital Evidence Fall*, vol. 2, no. 2, pp. 1–20, 2003, [Online]. Available: <https://pdfs.semanticscholar.org/915b/524318e2f0689b586ba7ae89ea39e9b22ce3.pdf>.
- [77] V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model," 2004, [Online]. Available: <http://dfrws.org>.
- [78] S. Ciardhuáin, "An extended model of cybercrime investigations," *International Journal of Digital Evidence*, vol. 3, no. 1, pp. 1–22, 2004, [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.1289&rep=rep1&type=pdf%5Chttps://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf>.
- [79] N. Beebe, J. Clark, N. L. Beebe, and J. G. Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," *Digital Investigation*, pp. 147–167, 2005.
- [80] F. C. Freiling and B. Schwittay, "A Common Process Model for Incident Response and Computer Forensics," *Imf*, vol. 7, no. 2007, pp. 19–40, 2007, [Online]. Available: <http://www1.cs.fau.de/filepool/publications/imf2007-common-model.pdf>.

Authors' Profiles



Yaman Salem works as a 'Content Development and Authoring Subject Matter Expert' at Security First Company in Dubai. Her professional journey in information security started in 2015 as an 'Associate Information Security Consultant' at IT Security C&T company, progressing to the role of 'Security Awareness Content Team Leader,' managing an information security content team. She gained an MSc in Cybercrime and Digital Forensics from the Arab American University in Palestine in 2022, and she has a bachelor's in Telecommunications Engineering. She is certified in CIHE, CPTE, CCNA Security, CCNA, and Network+.



Majdi Owda an Associate Professor in Computer Science and Dean of Faculty in Data Science at Arab American University. In addition, he is a UNESCO Chair for Data Science for Sustainable Development. Worked as a head of Department of Natural, Engineering, and Technology Sciences at Arab American University. Worked in School of Computing, Mathematics, and Digital Technology at Manchester Metropolitan University. He gained an MSc in Computer Science from Manchester Metropolitan University and a Ph.D. in Computer Science. His research interest is in Digital Forensics Processes and Frameworks and Internet of Things Digital Forensics Artefacts and Security.



Amani Yousef Owda is an Assistant Professor in Computer Engineering and Data Science at the Arab American University. She worked as a head of department of Natural, Engineering, and Technology Sciences at Arab American University. She worked as a research associate at the University of Manchester. In addition, she worked as a lecturer at Manchester Metropolitan University. She received her MSc. degree from The University of Manchester, and her Ph.D. from Manchester Metropolitan University. She has published more than 46 articles. She leads research in multi-disciplinary fields with a focus on security screening, cyber security and AI.

How to cite this paper: Yaman Salem, Majdi Owda, Amani Yousef Owda, "Towards Digital Forensics 4.0: A Multilevel Digital Forensics Framework for Internet of Things (IoT) Devices", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.14, No.2, pp. 27-54, 2024. DOI:10.5815/ijwmt.2024.02.03