Arab American University Palestine
Faculty of Graduate Studies

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

By

Yaman Monther Moneer Salem

Supervisor

Dr. Majdi Owda

Co-Supervisor

Dr. Amani Owda

This Thesis was Submitted in Partial Fulfillment of the Requirements for the Master's Degree in Cybercrimes and Digital Evidence Analysis

2023

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

By

Yaman Monther Moneer Salem

This thesis was defended successfully on 8th February 2023 and approved by:

Committee members	Signature
1. Dr. Majdi Owda	
2. Dr. Amani Owda	
3. Internal examiner: Dr. Mohammad Hamarsheh	
4. External examiner: Dr. Osama Mansour	

Declaration

I declare that the thesis titled "Towards Digital Forensics 4.0: A Multilevel Digital Forensics Framework for Internet of Things (IoT) Devices" is my work, it does not contain work from other researchers and has not been submitted for any other degree or qualification, this thesis is conducted for the Master's Degree in Cybercrimes and Digital Evidence Analysis at Arab American University Palestine.

Eng. Yaman Monther Salem
Student ID Number: 202012601
Date: 10/8/2023

Acknowledgments

Undertaking this thesis has been a valuable addition, reinforced my previous experiences, and enrich my work experience, I taught that a person should always keep learning and never stop. This work would not have been possible without the support that I received from many people. First of all, I would like to express my gratitude to the advisors, Dr. Majdi Owda and Dr. Amani Owda, for their advice, help, support, knowledge, and valuable time spent reviewing and correcting my work. Despite their busy schedule, they were able to meet me regularly with comments and suggestions on every page. I'd also like to thank my dissertation committee for their precious feedback. I was lucky to have an impressive research environment with great colleagues and supervisors at the Arab American University.

My warm thanks to my father, my mother, and my sister Ann for my spiritual support throughout my study. Your prayer was what sustained me thus far.

Last but not least, I want to thank my beloved husband Dr. Ahmad Abdelhaq, and my sons Hashem, Faris, and Salma for their support, patience, and faith in me, which was, in the end, what made this thesis possible.

To my parents, my husband, and my children

Abstract

The advent of the industrial revolution (IR) 4.0 has brought many benefits to business and our daily lives. IR 4.0 includes the development of the Internet of Things (IoT) devices. Although IoT brings benefits to human life, the exponential growth of IoT devices and the weak security structure of IoT devices create new opportunities for intruders to commit digital crimes, break privacy, and conduct or planing unlawful activities. The massive generated data from IoT devices may contain valuable artifacts for the crime scene. Hence, the sophisticated IoT environment, the variety of standards and vendors of IoT devices, and the lack of IoT forensics tools pose challenges to digital forensic investigators and create obstacles to finding criminals. Therefore, the digital forensic community needs to be prepared to handle IoT-related incidents in the era of IR 4.0.

This thesis aims to propose and evaluate a novel IoT digital forensics framework that fits the needs of the era of IR 4.0. A systematic literature review (SLR) was conducted to achieve this goal. The results from SLR indicated that the IoT architecture mainly has three levels (device level, network level, and application level), and many challenges surround each level. The "Multilevel Artifact of Interest Digital Forensics Framework for IoT" (MAoIDFF-IoT) was designed and proposed to overcome the IoT challenges and to face the heterogeneous architecture of IoT environments. It provides investigators with guidelines for conducting IoT forensics at the multilevel. Furthermore, real scenario experiments evaluated and tested the proposed framework. The evaluation of the experimental results reveals the advantages and superiority of the MAoIDFF-IoT framework over existing frameworks in terms of usability, inclusivity, focusing on the artifact of interest, and speeding up the investigation process.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

IoT	Internet of Things
OS	Operating System
IR 4.0	Industrial Revolution 4.0
DOS	Denial of Service
DDoS	Distributed Denial of Service
MIT	Massachusetts Institute of Technology
NIST	National Institute of Standards and Technology
API	Application Programming Interface
OEM	Original Equipment Manufacturer
FAT32	File Allocation Table 32
SD card	Secure Digital card
C	Components involved in the scene
EA	Expected Artifacts
ET	Expected Threats
MAoIDFF – IoT	Multilevel Artifact of Interest Digital Forensics Framework for IoT
MA	Missed Artifact
NA	No Artifact
UA	Useful Artifact
AoI	Artifact of Interest
ID	Identity
RFID	Radio Frequency Identification
Wi-Fi	Wireless Fidelity
LTE	Long-Term Evolution
JTAG	Joint Test Action Group
ISO/IEC	International Organization for Standardization/ International Electrotechnical Commission
IP	Internet Protocol
iOS	iPhone Operating System
FDE	Full Disk Encryption
MAC	Mandatory Access Control

ASLR	Address Space Layout Randomization
TEE	Trusted Execution Environment
USB	Universal Serial Bus
ADB	Android Debug Bridge

Chapter 1

1 Introduction

The first Industrial Revolution (IR) began in the 18th century. It referred to the transition from hand production to machine production through the use of steam power [1]. The second Industrial Revolution (IR 2.0) began in the 19th century through the discovery of electricity [1]. The third Industrial Revolution (IR 3.0) occurred in the late 20th century, also known as the "Digital Revolution", and referred to the extensive use of computers and digital electronics to automate processes [1]. The recent Fourth Industrial Revolution (IR 4.0) will fundamentally change the way we communicate, live, and work. In IR 4.0, humans, governance, and business are impacted with the four items being IoT, cloud computing, cybersecurity, and big data. These items are applied to the manufacturing sector [2, 3].

The appearance of the Industrial Revolution (IR4.0) brings facilities and advantages to people in daily life; however, it leads to more challenges, especially for digital forensic investigation [1]. Cybercriminals are exploiting IoT environments to conduct illegal activities [4]. On the other hand, digital forensics is a science concerned with identifying, analyzing, and examining generated data from digital devices to extract artifacts to be submitted to the court [4]. The artifact is any type of valuable information extracted from digital devices and presented as evidence in the court [4]. Hence, the digital forensic community should be prepared to face IR 4.0 challenges. One of the main challenges is dealing with sophisticated Internet of Things (IoT) environments [4]. In addition to the weak security structure of IoT devices and the huge data generated that include rich sources of evidence to find cybercriminals [4].

The Internet of Things (IoT) refers to all the devices connected to the internet using various standardized communication. IoT is applied to different domains; healthcare, education, smart cities, smart home, industry, markets, transportation, vehicles, and supply chain. IoT devices could bring threats from less secure public networks to private networks. These

threats include data leakage, identity theft, denial of service (DOS), and phishing [4]. For example, researchers found a weakness in LG smart vacuum, which detects roams for cleaning, this weakness allows access to live stream video at home [5]. A malware called Mirai compromised IoT devices in 2016, and it caused distributed denial of service (DDoS) [4]. In 2017, US food and drug administration announced that a heart arrhythmia device was hacked [4]. As technology evolves more and more, the heterogeneous environments that are made up of billions of connected devices can communicate with other devices across different networks and frameworks [6]. This presents lots of challenges in terms of digital forensics perspectives. Many traditional digital forensics techniques are not sufficient to conduct reliable digital investigations on IoT devices [3, 4]. Therefore, investigators need to implement digital forensics frameworks and best practices when carrying out their investigation of IoT devices to fit the unique characteristics of IoT systems.

This chapter is organized as follows, first, the problem statement and motivation are presented in Section 1.1. Then, the research objectives are stated in Section 1.2. The research method and questions are presented in Section 1.3. The main contributions of this thesis are summarized in Section 1.4. Finally, the thesis structure is presented in Section 1.5.

1.1 Problem Statement and Motivation

IoT is vastly used in many domains in our daily life. Although IoT devices bring benefits to human life, they are exposed to lots of threats, and they can be exploited for illegal purposes as they have a weak security structure [4, 5]. This presents an urgent need to develop a successful IoT digital forensics framework to analyze, collect and present evidence from IoT environments. Thus, IoT devices are targeted by digital forensics investigators to find artifacts when working on criminal cases. While IoT devices are commonly used in many environments [7], the digital forensic community needs to develop, improve, and build several effective ways and frameworks for IoT digital forensics [3]. Therefore, the following were the motivation for undertaking this study:

- The traditional digital forensic frameworks no longer meet the recent needs [4, 5]. In the fourth industrial revolution, IoT devices have merged into almost everything in human life, thus, they provide rich sources of evidence [3].
- IoT devices are considered an attractive target for attackers, due to the weak security structure of IoT devices, and lack of IoT security awareness which leads to being easily exploited by intruders [5].
- Criminals are developing and innovating new ways to invade people's privacy and conduct illegal activities by exploiting IoT environments [4, 5].
- The huge volume of extracted and generated data from IoT environments for investigation analysis [5].
- The increased number of devices needed to be analyzed in IoT environments [3].
- The variety of data structures, brands, and standards for IoT devices [4, 5].

All mentioned above poses a need for digital forensics investigators to be prepared for IoT-related incidents. Digital forensics techniques and methods are not sufficient to perform reliable investigations on IoT devices [4, 5], Some of the proposed frameworks tend to be too general while others frameworks focused on a specific scenario [8]. 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 [9]. For that reason, investigators need to implement digital forensics frameworks and best practices when carrying out their IoT investigation to fit the unique characteristics of IoT systems [3].

1.2 Objectives

This study aims to develop and apply a novel IoT digital forensic framework, hence, the following objectives in this study were stated:

- Propose an effective and novel framework for IoT digital forensics.
- Propose a new method for finding and classifying artifacts.
- Compare IoT forensics frameworks with the proposed framework.
- Apply and evaluate the proposed framework to real scenario experiments.

1.3 Research Method and Questions

The main aim of this study is to propose an effective IoT digital forensics framework. A mix of qualitative and quantitative methods was used to achieve this goal. A systematic review was conducted and concluded from the literature available in trusted journals. This thesis explored the IoT history, definitions, architecture, and IoT-related attacks. In addition, it explored IoT digital forensics in terms of frameworks, case studies, and challenges at device, network, and application levels.

Hence, the proposed framework was designed initially based on the literature analysis, and then the framework was tuned based on the experimental result analysis. An experimental approach is conducted to test and evaluate the proposed framework, and a set of real-world scenarios in the experimental work were set, conducted, and documented.

The main research question in this thesis:

What is the effective framework for IoT digital forensics that fits the era of IR 4.0?

The sub-questions in this thesis can be concluded as follows:

- What are the available digital forensics frameworks?
- What are the available IoT digital forensics frameworks?
- What are the challenges of IoT digital forensics?
- What is the proposed IoT digital forensics framework?
- What distinguishes the proposed framework from the existing IoT frameworks?
- How can the proposed IoT forensics framework be applied to real IoT environments?

1.4 Contribution

This thesis includes several contributions in the field of IoT digital forensics:

(1) Digital forensics frameworks in general and IoT forensics frameworks in particular which are available in previous studies are explored, in addition, traditional digital forensics are compared with IoT digital forensics. Moreover, the IoT digital forensics challenges at three levels are explored according to the IoT architecture

being the device, the network, and application levels, aiming to develop a novel IoT forensics framework to fit the needs of IoT environments.

(2) The novel framework for IoT digital forensics named "Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT)" is proposed. This framework has several advantages, it focuses on Artifacts of interest (AoI) to save time and effort, and it explores the IoT environment by defining the components (C), the expected threats (ET), and expected artifacts (EA) related to the IoT devices. The proposed framework includes the traditional digital forensics process with additional phases to fit the heterogeneous nature of the IoT environment. It maintains integrity as the documentation should be done through all the investigation phases. Moreover, the proposed framework is flexible and inclusive as it covers all the IoT levels (device, network application) to avoid missing any critical artifacts.

(3) A new method for finding artifacts according to the conducted actions is proposed in the (examining & analyzing) phase. The researcher played the role of the user and the investigator, thus, four types of extracted artifacts were invented, the extracted artifacts were classified into four: missed artifact (MA), no artifact (NA), the useful artifact (UA), or artifact of interest (AoI).

(4) The proposed framework is evaluated and tested through three case studies included; (1) an experiment on a smart camera at the device level, (2) an experiment on a smart camera at the application level, and (3) an experiment on a smart environment containing seven IoT devices at the application level, including smart plug, a temperature & humidity sensor, smart motion sensor, remote control, smart gas detector, smart smoke detector, and a smart led bulb. In each case study, several scenarios were conducted by playing the role of user and investigator at the same time. The researcher found the artifact types according to the conducted actions and concluded the results.

(5) Guidelines, recommendations, and notes at the end of the investigation process are an additional sub-phase in reporting phase as each IoT device has it is own features.

Thus, the investigator might have additional notes to facilitate the investigation process for other investigators in the future.

1.5 Thesis Structure

The remainder of the thesis is organized as follows.

Chapter 2. The history of the internet of things (IoT), the definitions of IoT, the IoT architecture, and the common IoT attacks are introduced. Then, an overview of the digital forensics process and its definitions are stated, in addition, different proposed frameworks and methodologies of the digital forensics process are reviewed. Then, IoT digital forensics versus traditional digital forensics are compared based on the literature review. Many IoT digital forensics frameworks are presented, compared, and discussed. Moreover, IoT digital forensics challenges on device, network and application levels are reviewed. Therefore, in this chapter, a large number of IoT digital forensics-related research efforts are stated and discussed.

Chapter 3. A novel IoT digital forensic framework named "Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT)" is proposed. The advantages of the proposed framework are stated, then the phases in the proposed framework are presented, and each phase is explained in detail. A new method in the (examining & analyzing) phase for finding artifacts according to the conducted actions is presented, thus, four types of extracted artifacts are invented, the missed artifact (MA), no artifact (NA), the useful artifact (UA), and the artifact of interest (AoI). In addition, additional features and advantages of the MAoIDFF-IoT proposed framework are stated and explained.

Chapter 4. In this chapter, the proposed framework is tested through three case studies. In each case study, several scenarios are conducted by simultaneously playing the role of user and investigator. The researcher finds the artifact types according to the conducted actions and concluded the results. All the proposed phases are applied in this chapter.

Chapter 5. Finally, the work in this thesis is summarized and open issues for further studies are presented. Key challenges faced while conducting this thesis are also stated.

Chapter 2

2 Literature Review

2.1 Introduction

The growth of the internet and technology in the Industrial Revolution 4.0 (IR4.0) era increased the need for digital forensics investigation. Computers, mobile devices, operating systems, IoT devices, and forensics tools are changing very quickly. Moreover, cybercriminals commit and invent different types of attacks. Thus, digital forensics experts must be updated and involved in these changes [10]. This chapter aims to

- Present IoT history and IoT definitions.
- Present IoT architecture and common IoT attacks.
- Summarize several digital forensics frameworks and IoT digital forensics frameworks.
- Compare the IoT digital forensics frameworks.
- Compare IoT digital forensics with traditional digital forensics.
- State the IoT digital forensics challenges at the device, network, and application levels.

2.2 IoT History and Definitions

Over the last decade, the term Internet of Things (IoT) has attracted attention. The future of communications and computing is represented by the Internet of Things [7]. In the 1980s, a Coke machine at Carnegie Melon University was the first internet appliance, users could connect to the machine over the internet, to check whether or not there is a cold drink inside the machine [11].

The term “Internet of Things” was set out by Kevin Auston, the executive director of Auto-ID Labs at Massachusetts Institute of Technology (MIT) in 1999. Then the concept of IoT became very popular in 2003 in the market [11]. Recently, the Internet of Things is a technological revolution. There are many things or objects connected to the internet for various purposes which make human life more comfortable [7].

There are several definitions for IoT introduced by researchers and innovators [12], for example, according to Gartner,

“The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.” [13].

According to NIST, the Internet of Things is :

“*The network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information.”*[14].

According to Jeffry Voas, a computer scientist at the National Institute of Standards and Technology (NIST),

“The IoT is the network of physical objects that contain embedded technology to communicate and interact with the external environment. The IoT encompasses hardware (the “things” themselves), embedded software (software running on, and enabling, the connected capabilities of the things), connectivity/ communications services, and information services associated with the things (including services based on analysis of usage patterns and sensor or actuator data)” [12].

All the definitions share the same idea, which can be summarized as, IoT is a network of components, objects, or things with embedded sensors connected to the internet, which enables the communication between things to things, humans to things, and humans to human, to facilitate human life. IoT includes hardware (the thing), embedded software,

information services, and communication services [7, 10]. IoT covers wireless, wired, and mobile devices, in addition to radio frequency identification (RFID) sensors [10].

2.3 IoT Architecture

The general IoT architecture can be divided into three layers: physical, network, and application [13 – 17]. Invented layers stated in the literature such as the processing layer [15], and middleware layer [18, 19]. Figure 2.1 clarifies the IoT layers which are further described in the following:

- The perception layer, the physical layer, the device layer, or named the sensor layer, is the bottom layer in the IoT architecture. It contains devices such as actuators, sensors, microcontrollers, etc., and 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 [13 – 16].
- The network layer or named the transmission layer is the middle layer in the IoT architecture. It includes communication technologies (WiFi, Bluetooth, Long-Term Evolution (LTE), etc.), devices (switching, hub, gateway, etc.), and protocols needed for transmitting data between the perception layer and application layer [16]. The network layer determines the routes to transmit data among the heterogeneous IoT networks [15].
- The processing layer was invented in recent research to be an additional layer between the network and the application that stores and processes data received from the network layer. Due to the large amount of collected data, it is important to process and analyze data using several techniques, such as cloud computing and intelligent processing [15].
- The middleware layer stores data received from the network layer in the database and it works as a service management [18, 19].
- The application layer, or named the business layer, is the top layer in IoT architecture, it receives data from the network layer to provide the needed services. It contains the interface for the services offered to the end users [13], [15 – 17]. The

application layer includes the application programming interfaces (APIs) that collect, analyze usage statistics, control access, and report performance. In addition, the application layer might include the cloud service, the mobile app, and web dashboards that control IoT devices [16].

Main IoT Levels	Additional IoT Levels	Level Description
Application/ Business Level		Web Portal, Dashboard, API management, Mobile App, Cloud services
	Middleware Layer	Intelligent data processing solutions
	Processing Layer	
Network/ Transmission Level		Switches, Routers, Protocols, communication technologies (Wi-Fi, Bluetooth..)
Physical/ Sensor/ Device Level		IoT devices, Sensors, Storage

Figure 2.1. Description of IoT architecture.

The main four IoT communication models include (1) the Device-to-Device Model, (2) the Device-to-Cloud Model, (3) the Device-to-Gateway Model, (4) the Back-End Data-Sharing Model, these models are outlined in other studies [20 – 22]. The following Figure 2.2 illustrates each model.

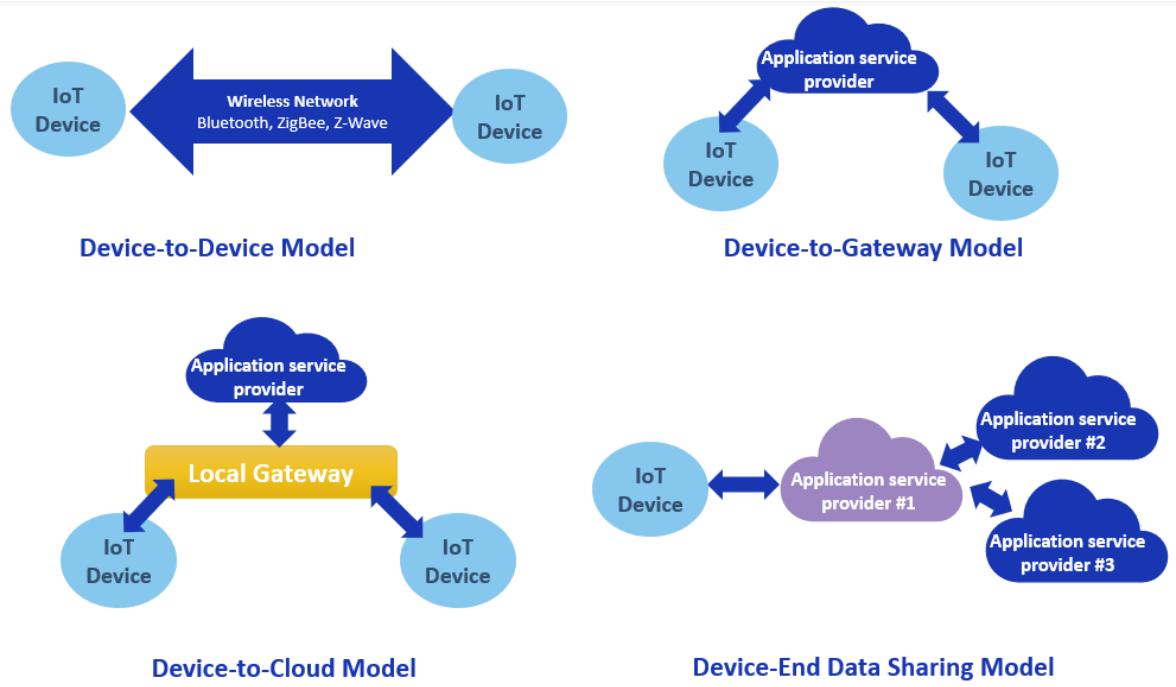

Figure 2.2. The main four IoT communication models.

The result from the literature review related to the IoT architecture can be concluded as follows, the IoT architecture has three main levels that should be considered in the IoT investigation including:

- The device level: it contains the physical device, external memory, internal memory, file system, and operating system.
- The network level: it contains network devices, IoT protocols, and traffic.
- The application level: it contains the service that controls the IoT devices which could be the mobile App, the web interface, and the cloud.

2.4 Common IoT Attacks

Any digital forensics investigator needs to be aware of IoT attacks before involving in the investigation. The objective of knowing IoT-related attacks is to identify the flaws present in the different IoT levels to facilitate rebuilding crime scenes that happened in the IoT environment. Many attacks could target IoT environments such as wireless reconnaissance,

protocol attacks, physical attacks, and application attacks [23, 24]. This section states a description of some of the IoT attacks that are related to IoT environments, Figure 2.3 clarifies IoT attacks according to the IoT levels.

IoT Levels	IoT Attacks
Application Level	Software / Application attacks, ex: encryption attacks, DoS, injection malicious scripts (viruses, spyware)
Network Level	Network attacks, ex: wireless reconnaissance, protocol attacks, traffic analysis, eavesdropping, DDOS
Device/ Physical Layer	Hardware/ Physical attacks, ex: delete/ edit internal or external storage by accessing ports and storage, destroy or steal the IoT device

Figure 2.3. IoT attacks according to the IoT levels.

2.4.1 IoT Attacks at the Physical/ Device Level

Physical security is usually overlooked by IoT vendors which are only focusing on designing equipment, and appliances to be attractive and easy to use [23, 24]. Physical security attacks include penetrating the IoT hardware to gain access to its memory devices, processor, and other sensitive components [25]. Usually, intruders can detect communication ports that are open and badly protected, and get access over an IoT device's exposed interfaces (for example, JTAG), Joint Test Action Group (JTAG) is an advanced data acquisition technique, which includes directing the processor to transfer the data stored on the device by connecting to specific device's ports. Hence, they can easily access the IoT device's components [26]. Further, the attacker can access the IoT device physically, and compromise privacy by accessing the personal information stored in the internal or external storage of IoT devices. The intruder can hide the crime by deleting the internal or external storage, destroying the IoT device, or stealing it.

Several techniques exist to protect IoT devices from physical penetration. for example, automatic wiping of memory, smart card chips, authentication, access control, and many

other types of cryptographic techniques that protect device identity and data from compromise [16, 24].

2.4.2 IoT Attacks at the Network Level

IoT devices usually have a limited storage capacity, and a low computation capability, which makes them targeted and vulnerable to lots of threats at the network layer [18], a replay attack is a kind of attack that targeted IoT devices by spoofing, modifying, or replaying the identity data of one of the devices in IoT environments [16, 25]. Moreover, a node capture attack may happen when the intruder takes over the node and captures all data, he can then send malicious data or deny the node from sleep mode which maintains the energy. This leads the energy exhaustion and DoS attack [27].

Wireless reconnaissance is usually the first technique hackers use before conducting actual attacks. Nmap is a commonly utilized tool by attackers for network scanning to gather information about ports, hosts, and protocols in networks. Z-Wave, ZigBee, WiFi 802.11, Bluetooth-LE, and others are wireless communication protocols used in IoT devices. Intruders could exploit these protocols. For example, a low-flying drone outfitted with a custom ZigBee protocol scanner is used to identify lots of ZigBee-enabled IoT device beacon requests [26].

The protocol specification, configuration, and implementation play a role in preventing attacks against vulnerabilities. Understanding the limitations of IoT protocols is imperative from a digital forensics perspective to think about possible attack scenarios conducted by intruders to exploit and get access to IoT devices. For example, a ZigBee protocol used in IoT was designed for easy usage and setup. However, it has a vulnerability that allows intruders to sniff the exchanged network key through the ZigBee pairing transaction and gain control of the ZigBee IoT device [26]. In addition, a denial of service (DOS) attack which denies the service could affect the IoT network layer.

The intruders can compromise privacy and confidentiality at the IoT network layer through traffic analysis, passive monitoring, and eavesdropping. The key exchanged in IoT architecture should be secure enough to avoid any additional attacks, such as Man in middle attacks which could be followed by passive monitoring [18].

2.4.3 IoT Attacks at the Application Level

IoT devices do not have universal standards that control the development of applications. Thus, there are many issues related to IoT application security. IoT applications have different authentication techniques, which makes ensuring data privacy and identity authentication difficult. Additionally, the large amounts of connected IoT devices that share and analyze the data could affect the availability of IoT services [18].

IoT devices can be targeted through their application endpoints such as mobile device applications (for example, iPhone, and/or Android) that control the device [26]. Users interact with IoT devices by application interfaces, thus, they must be aware of how to utilize the IoT applications to protect IoT environments and prevent any potential attacks that might happen because of user negligence and lack of knowledge [18]. Attackers can conduct encryption attacks to get valuable information, they can inject malicious scripts, viruses, or spyware to gain access to the IoT device, or deny users from accessing the application layer [25].

2.5 Digital Forensics Process and Frameworks

Over the last decade, the number of cybercrimes has increased, as a result, digital forensics is needed for handling unexpected incidents, and unusual operational problems to respond to suspected events and crimes that involve any digital device [28]. Organizations usually include general methodologies, guidelines, and procedures for performing digital forensics and acting on incidents, these methodologies could be modified and changed based on each situation [28].

Digital forensics has many definitions [28], according to NIST, digital forensics, could be known as computer and network forensics. NIST defines digital forensics as follows:

“ It is considered the application of science to the identification, collection, examination, and analysis of data while preserving the integrity of the information and maintaining a strict chain of custody for the data.” [28].

Another definition for digital forensic investigation by Brian Carrier [29] is "*a process that uses science and technology to examine digital objects and that develops and tests theories, which can be entered into a court of law, to answer questions about events that occurred*" [29].

Digital forensic Science is defined by the digital forensics research workshop as [30]:
"The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations." [30].

A digital investigator may analyze several formats of digital data. The types of data analysis include media analysis, filesystem analysis, application analysis, network analysis, operation system (OS) analysis, executable analysis, image analysis, and video analysis [29].

Several enhanced digital investigation frameworks have been proposed since 1984 either for incident response or for court admissibility, particularly, when the FBI laboratory and other agencies began to promote programs to examine digital evidence [29, 30]. Some of the proposed frameworks tend to be too general while others are quite details, some frameworks focused on a specific scenario while others focused on a wider scope [8]. With the lots of proposed digital forensics frameworks in the literature, there are no common standards or rules for digital forensics investigation. Therefore each country or organization tends to select its practices [9].
Lots of proposed digital forensics frameworks have been stated by researchers [29, 31]. Therefore, the objective of this section is to identify, and explore some of the digital investigation frameworks stated in the literature, and present the commonly shared phases rather than choosing which framework is the best. In this research, the term "framework" is

used for general digital investigation structure, while the term “phase” is used to present components in the framework. “Activities” term is used to present actions in each phase of the framework. Table 2.1 concludes the proposed digital forensics frameworks in the literature.

Table 2.1. The proposed digital forensics frameworks in the literature

Digital Forensic Framework	Year	Phases
Computer Forensic Investigative Process [32]	1995	Acquisition, identification, evaluation, admission
Digital Forensics Research Workshop (DFRWS) Investigative Model [30]	2001	Identification, preservation, collection, examination, analysis, presentation, and decision
Abstract Digital Forensic Model (ADFM) [33]	2002	Identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, returning evidence
Integrated Digital Investigation Process (IDIP) [34]	2003	Readiness, deployment, physical/digital crime investigation, review
Enhance the Integrated Digital Investigation Process (EIDIP) [35]	2004	Readiness, deployment, trackback, dynamite, review It aims to separate the scene into the primary scene (the computer) and the secondary scene (the physical scene)
An event-based digital forensic investigation framework [29]	2004	Based on the causes of events it has 3 main phases: (preservation /documentation, searching/documentation, and reconstruction/documentation). Evidence searching has 4 phases (target definition, data extraction and interpretation, data comparison, and knowledge update)
Extended Model of Cybercrime Investigation (EMCI) [36]	2004	It has (13) phases: Awareness, authorization, planning, notification, search for and identify evidence, collection of evidence, transport of evidence, storage of evidence, examination of evidence, hypothesis, presentation of hypothesis, proof/defense of hypothesis, and archive storage. It focuses on evidence processing and management aspect
A Hierarchical, Objective-Based Framework for the Digital Investigation [37]	2004	Preparation, incident response, data collection, data analysis, presentation of findings, and incident closure.
Binding Computer Intelligence to the Current Computer Forensic Framework [38]	2005	Survey, extraction, examination, presentation. It explains the need for intelligence technology. Such as automatic evidence extraction
Guide to Integrating Forensic Techniques into Incident Response -	2006 – updated	Preservation, Data collection, examination, analysis, reporting

NIST Special Publication 800-86 [28]	2014	
Computer Forensic Field Triage Process Model (CFFTPM) [39]	2006	Planning, triage (rank evidence according to priority), user usage profile (home, file properties, registry), chronology timeline, internet (browser, email, instant message), case-specific.
Framework for a Digital Forensic Investigation [40]	2006	Preparation, investigation (identify, collect, store, examine, analyze), presentation
Dual Data Analysis Process [41]	2007	Access, acquire, analyze, and report
A Common Process Model for Incident Response and Computer Forensics (CPMICF) [42]	2009	Pre-analysis phase, analysis phase, post-analysis phase (report, resolution)
Generic Process Model for Network Forensics [43]	2010	Preparation, detection, incident response, collection, preservation, examination, analysis, investigation presentation
Generic Computer Forensic Investigation Model (GCFIM)[8]	2011	Pre-process, acquisition & preservation, analysis, presentation, post-process
Digital Forensic Model for Digital Forensic Investigation (DFMDFI) [44]	2011	First tier (preparation, identification, authorization, communication) The second tier (collection, preservation, documentation) Third tier (examination, exploratory, testing, analysis) Fourth tier (result, review, report)
Systematic Digital Forensic Investigation Model (SDFIM) [45]	2011	Preparation, securing a scene, survey& recognition, documentation of the scene, communication shielding, evidence collection, preservation, examination, analysis, presentation, result & review
Integrated Digital Forensic Process Model (IDFPM) [46][47]	2012	Documentation, preparation, incident, incident response, digital forensic investigation, and presentation. It meets the ISO 27037:2012 standard [48]
ISO/IEC 27037:2012 [49][48]	2012	Scope, identification, collection, acquisition, preservation
Digital Forensic Data Reduction and Data Mining Framework [50]	2014	It provides a rapid triage, intelligence analysis, review, and storage methodology to support the different phases of digital investigation. It has 10 phases: Scope, preparation, identification and collection, preservation, reduction & storage, review & data mining, open & closed source data, evidence analysis, presentation, and completion.
Framework for Reliable Experimental Design (FRED) [51]	2018	Plan, implement, evaluate, repeat the process, analyze, confirm
A Framework for Digital Forensic Investigation of Big Data [52]	2020	It has 3 parts: digital forensics technology, intermediate technology, and big data technology

Next Generation Digital Forensic Investigation Model (NGDFIM) [53]	2021	Taking into account big data, privacy, and technological advances challenges, it has 3 phases; the On-site triage phase (secure the scene to maintain the integrity of the artifact), the analysis phase, and the presentation phase

The following Table 2.2 states the most common names of phases in the digital forensics process that are stated in the literature, the phases marked with a star are the most repeated phase in the research:

Table 2.2. The Most Common Names for Digital Investigation Phases

Access	Awareness	Identification*	Analysis*	Approach Strategy	Examination*
Acquisition*	Case-Specific Analysis	Chronology Timeline Analysis	Planning*	Deployment	Detection
Digital Crime Investigation	Dissemination of Information	Dynamite	Evaluation	Authorization	Hypothesis creation
Admission	Incident Closure	Incident Response	Readiness*	Notification	Physical Crime Investigation
Collection*	Post-Analysis	Pre-Analysis	Preparation*	Presentation*	Preservation*
Proof & Defense	Investigation*	Recognition	Reconnaissance	Reconstruction	Triage
Returning Evidence	Review*	Search & Identify	Traceback	Transport & Storage	Report*

Thus, the basic phases of the digital forensic framework include preparation, acquisition & preservation, examining, analyzing, and reporting [26, 28, 31, 33, 54]. The activities included in each phase may vary based on the investigation case. First, during the preparation phase, the investigator should prepare all related tools and tasks needed before the investigation is done. Second, during the acquisition & preservation phase, all the suspected devices and the event-related data are identified, recorded, imaged, and their integrity is maintained. Third, in the examining phase, all collected data are inserted into the investigation workstation for analysis. Fourth, in the analysis phase, all digital evidence

collected in the previous phase is interpreted and analyzed. Finally, the forensic investigation findings are presented and reported [28]. Each digital forensic phase can be applied differently according to the digital investigation case and the related policies and laws [28].

As shown in Figure 2.4, during the digital forensics process, the collected media is transformed into data and then data is transformed into information through the analysis phase, then the information is transformed into evidence which is needed for court presenting and other internal usages [28].

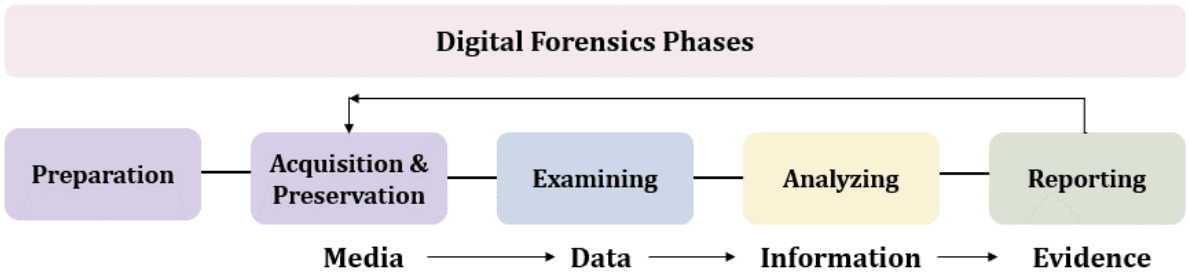

Figure 2.4. The Basic phases of the digital forensics process.

2.6 IoT Digital Forensics vs Traditional Digital Forensics

The previously mentioned traditional digital forensic phases can be applied to IoT forensics in different ways, as IoT forensics is considered part of digital forensics [6]. However, IoT digital forensics has multi-levels that should be considered in the IoT forensics investigation, being device level, network level, and application level [6], [55]–[57]. Therefore, IoT digital forensics presents several differences which will affect the traditional digital forensics phases, these differences should be taken into consideration while conducting IoT forensics, the traditional digital forensic frameworks no longer meet the recent needs [52]. A new framework for IoT forensics is urgently needed because of the increasing number of devices in one case, the increasing volume of data, the increasing complexity of analysis, and the diversity of data structure [52]. The following Table 2.3

describes the differences between IoT digital forensics and traditional digital forensics in terms of several areas, such as the number of devices, evidence sources, types of evidence, the quantity of extracted data, the format of extracted data, and the network boundary [5, 58].

Table 2.3. 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 [55]	A few devices, typically, computers, USB drives, or/and other related devices [4]
Source of Evidence	IoT devices, the IoT network traffic, the cloud service that is connected with the IoT, the web interface, and the mobile app that control the IoT devices [58]	Computers, mobile phones, social networks, logs, and other clues/items included in the crime scene [58]
Quantity of extracted data	A huge amount of data depends on the IoT devices' types and IoT environment/ architecture [55]	Depends on the crime scene and the number of components involved in the investigation process [58]
Format of extracted data	It might be a complicated or ununderstandable format due to the diversity of IoT manufacturers and lots of IoT commercial brands [55]	Standard format, it might be encrypted [58]
Network Boundary	Blurry, unclear network boundary [55]	Relatively a clear and defined network boundary [55]

- **Number of Devices**

Traditional digital forensics may include a few devices such as computers, USB drives, external storage, or other related devices that may exist at the crime scene. On the other hand, the number of devices in IoT digital forensics may include billion of devices, this depends on the IoT architecture and IoT environment, as the IoT devices are interconnected with each other internal and external environments [4, 55].

- **Source of Evidence**

In traditional digital forensics, the investigator might extract evidence from several devices, computers, mobile phones, social networks, logs, and other clues included in the crime

scene. With IoT digital forensics the investigation could be more complicated as the investigator may have lots of IoT devices that are connected, and these devices might be connected to the internet, thus the investigator might extract the evidence from IoT devices or the IoT network traffic, or even from other connected IoT devices [58]. In addition, the cloud service connected with the IoT might have a rich source of evidence, also the web interface and the mobile app that controls the IoT devices are considered a good source of evidence from a digital investigator perspective [55].

- **Quantity and Format of Extracted Data**

The investigator might extract a huge amount of data from IoT environments for analysis [7, 55]. Moreover, the retrieved data format from the IoT environment might be understandable due to the diversity of IoT standards and lots of IoT commercial brands. Further, some specific and additional tools need to be used to extract the correct evidence [58]. While the retrieved data format from traditional forensics could be a normal format or an encrypted format.

- **Network Boundary**

The network boundary is usually clearly defined in traditional digital forensics, such as the number of devices to be acquired, and the number of people involved in the communications. On the other hand, with IoT digital forensics, the networks bleed into each other as people that connect with IoT devices move from place to place, thus the network boundaries are blurred [55].

2.7 IoT Digital Forensics Frameworks

In section 2.5, several digital forensic frameworks were reviewed. This section aims to review IoT digital forensics in particular. Digital forensic investigators tend to build or design procedures, methods, and frameworks to reconstruct the criminal scenario effectively [38]. Several studies have investigated different IoT devices and suggested frameworks and models for conducting IoT digital forensics [6], [55 – 57], [59 – 76].

For example, a study by [6] considered IoT forensics a particular branch of digital forensics. It identified IoT forensics as a combination of three levels: device, network, and cloud forensics, where the investigator can collect evidence from these levels. Further, it suggested a Forensics-aware IoT (FAIoT) model for investigating IoT devices, it's a conceptual model that contains a centralized evidence repository that handles huge datasets collected from the cloud, network, and device. The data set is managed by Hadoop distributed File system (HDFS) which is an open-source used to store a large set of data. The repository produces the provenance record for evidence. Thus, the evidence can be easily accessed using API service and easily collected and analyzed.

A study by [55] proposed a three zones model to investigate IoT. Zone one includes all hardware, software, and networks. Zone two includes all the border devices between an external and internal network, and zone three covers all devices outside the network. In addition, it stated two potential sources of evidence in IoT cases including (1) the internal evidence source such as hardware, and network perimeter devices, and (2) external evidence sources such as cloud, web, and network. The proposed model is suggested to be applied through the digital forensics process being the preparation, the acquisition, the investigation, and the reporting. For its future work, it suggested applying the proposed framework to IoT devices.

A study by [56] investigated the Amazon Alexa ecosystem, this system interacts with third-party applications and IoT devices, and it is considered a rich source of evidence as it interacts through voice commands. The study combined cloud and client forensics. In the client forensics part, the researcher extracted artifacts from mobile applications and web browsers, and the conducted experiments were done on Andriod, iOS, OS X, and Windows that are associated with the Amazon Echo system. The findings showed the location of the artifact for each operating system. Another study by [57] investigated the Almond smart home hub through the cloud, smartphone application, web interface, local storage, and network, the study stated some challenges such as the volatility data obtained from the

device. Further, the researcher stated some recommendations for forensic investigators related to almond smart home hubs.

Forensic State Acquisition from the Internet of Things (FSAIoT) [72] is another proposed framework, it contains a centralized Forensic State Acquisition Controller (FSAC) developed in three collection modes: controller to IoT device, controller to the cloud, and controller to controller. The controllers are connected to multiple IoT devices to be controlled and managed, in this study, an open-source controller which is openHAB [77] was used to be installed on the workstation.

A forensics framework for the IoT ecosystem was presented by [74], which contained three stacks: (1) the first stack presents the IoT layers such as the sensing layer, network layer, service layer, and interface layer, and (2) the middle stack presents the components of IoT ecosystems such as sensors, device, media, and privacy and security. (3) The third stack presents possible forensic options such as log analysis, memory cash analysis, and fingerprint collection.

Another proposed model for smart environments, IoTDots [73], the framework contained two main parts, (1) IoTDots-Modifier (ITM) and (2) IoTDots-Analyzer (ITA). ITM gathers forensically- relevant data from smart applications. Then, these logs will be sent to the IoTDots Logs Database (ITLD) at runtime. Later, in a case of a forensic investigation, the ITA applies data processing methods to the ITLD data for forensic analysis. IoTDots applies data processing methods to detect evidence from users' actions, smart devices, and apps.

A Privacy-aware IoT-Forensic Model (PRoFIT) is another proposed model which combined privacy requirements according to (ISO/IEC 29100:2011) [75]. The PRoFIT focused on the potential surrounding devices to collect evidence from the crime scene, and it defines six phases; "(1) Preparation (planning and environment set up), (2) Context-based collection, (3) Data analysis and correlation, (4) Information Sharing, (5) Presentation and (6) Review" [75].

An application-specific digital forensics investigative model [76] contained three components, (1) the application-specific forensics which specifies the type of IoT, (2) digital forensics which deals with extracting artifacts from the cloud, network, and devices, and (3) the forensics process which is based on digital forensics phases from the NIST guide; data collection, data examination, data analysis, and reporting. The data flow between these three components differs according to the type of IoT application. This model is applied to three examples of IoT; Wearables, Smart homes, and Smart Cities.

Common Investigation Process Model (CIPM) is another model proposed recently for IoT forensics which is based on the metamodeling method [59], CIPM is based on four phases of digital forensics including preparation, collection, analysis, and final report. In addition, improved IoT digital forensics models based on blockchain are developed recently [60, 61]. For example, [60] developed a forensic investigation framework for IoT (FIF-IoT) based on a digital ledger, all evidence collected and stored as transactions in decentralized, public, and distributed blockchains. This guarantees the confidentiality, integrity, and availability of the evidence. On the other hand, [61] used hashing for authentication. In addition, [62] proposed a comprehensive framework for IoT digital investigation, this framework is not dependent on the network logs and the Cloud Service Provider (CSP) at the investigation runtime. [63] proposed a model for IoT digital investigation for the IoT ecosystem named Integrated Digital Forensic Investigation Framework (IDFIF-IoT), the framework consisted of mainly four phases, (1) proactive process, (2) IoT forensics, and (3) reactive process. In the IoT forensics phase, the researchers focused on extracting evidence from the cloud, network, and device levels.

While [64] proposed an IoTCurator framework that provides digital forensics examination, access control, authentication, and network attack mitigation for IoT infrastructure. A study by [65] proposed IoT forensic model and applied this model to the Amazon Echo device, which is a smart home IoT device that controls other IoT services by voice recognition commands. The evidence is collected from sensing, network, cloud, service, and interface layers through the following digital forensics phases: (identification, preservation, analysis,

and presentation). Another study by [66] introduced a Forensics Edge Management System (FEMS) which is a design that provides (1) forensics services, and (2) security services for IoT smart home devices. Security services focused on network monitoring, intrusion detection/prevention systems, and data logging to detect anomalies. While forensic services focused on data parsing of captured data, timeline creation, alerting, and result in presentation. Its design depends on three layers; application, network, and perception layers. For its future work, it suggested applying its design to crime scenarios, including IoT devices, and conducting a set of an experiment to test the efficiency of FEMS design. [67] addressed a generic digital forensic investigation framework for IoT (DFIF-IoT), further it compared the previous models for IoT forensics with its proposed model, which depended on three modules; which are the proactive process, reactive process, and IoT forensics. The last module included IoT forensics for three layers, the cloud, the device, and the network. In addition, it complies with the ISO/IEC 27043: 2015.

A study by [71] investigated artifacts from different four smart home IoT devices including two cameras, an alarm system, and a smoke detector. It provided methods for extracting and analyzing artifacts from smartphone applications associated with IoT devices. The findings showed that artifacts generated by IoT devices can be found on physical devices, smartphones, networks, and the cloud. Artifacts found had value from a digital forensic perspective including events logs, images, and videos recorded by IoT devices. At the physical device level, file system images, and memory images were extracted for analysis. The main challenge faced was the limited storage available for storing artifacts. Additionally, the study discovered vulnerabilities in these devices.
Contiki is a lightweight operating system designed for constrained environments [68]. A study by [68] investigated a coffee file system over Contiki OS that is used widely in IoT devices. It developed a COFFER tool for recovering the modified and deleted files. The digital investigation included the device level.

A study by [69] explored the reasons for the increasing breaches of IoT devices among them the weakness in security measures. Further, it stated that the traditional forensic

approach needs to be improved to be compatible with IoT environments. It recognized that analyzing IoT devices are considered an effective approach for forensic investigation. It applied this approach and investigated the nonvolatile memory of the Windows IoT core operation system, it located all related artifacts from the NTFS file system, registry, system events, users, browsers, and Apps. In addition, it provided a module to collect all information from the non-volatile memory of the Windows IoT core. For future work, it is suggested to analyze volatile memory, network traffic, and other operating systems for the IoT devices, in addition to developing forensic tools that automate the investigation process and provide guidelines for investigating other IoT devices.

A recent study by [70] presented a practical forensic method for the smart environment named VERITAS which has two parts: Collector and Analyzer. The Collector automatically collects forensically relevant information from the smart environment. Later, the Analyzer uses a First Order Markov Chain model to extract valuable data from the collected data. VERITAS was tested through 22 smart devices and sensors implemented in an actual smart environment. The experimental results enabled the detection of malicious forensic actions with high accuracy.

A Framework for Digital Forensic Investigation of Big Data [52] has three main parts: (1) digital forensics technology, (2) intermediate technology, and (3) big data technology. The first part is digital forensics technology which includes collecting, preserving, and examining data from different sources, including unstructured, semi-structured, and structured data. While the second part, the intermediate technology, connects forensics technology with big data technology and ensures the digital forensics process's security, feasibility, legitimacy, and accuracy. The third part is big data technology involves the technology that processes the large volume of data to be investigated. The study stated the Hadoop ecosystem as an example of big data technology.

Table 2.4 states several studies and frameworks related to IoT digital forensics. The table compares in terms of investigated levels: the device, the network, and the application

(mobile, cloud, web interface). As noticed, some frameworks and studies examined the IoT at the device levels or network level or included all levels for investigation. While other studies are used a different approach for investigation such as blockchain [59]–[61], or depend on classifying data according to the data structure [52]. Other studies focus on access control, authentication, and network attack mitigation for IoT infrastructure rather than focusing on the investigation at IoT levels [64]. As a result, the gathered literature review inspired the researcher to design and propose a novel IoT digital forensics framework encompassing the advantages of the previous frameworks and overcoming IoT forensics challenges with additional new features.

Table 2.4. Studies and frameworks related to IoT digital forensics in the literature

IoT framework	Device Level	Network Level	App Level (Cloud)	App Level (Mobile)	Other
S. Zawoad and R. Hasan - FAIoT [6]	✓	✓	✓		Contains a centralized evidence repository, a conceptual model for IoT forensics
E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant - Three Zones Model [55]	✓ Internal network	✓ External and middle network	✓ External network		Contains three zones for evidence extraction, the external, the middle, and the internal zones
H. Chung, J. Park, and S. Lee [56]	✓		✓	✓	Investigated the Amazon Alexa ecosystem
A. Awasthi, H. O. L. Read, K. Xynos, and I. Sutherland [57]	✓	✓	✓	✓	Investigated the Almond smart home hub
F. Servida and E. Casey [71]	✓	✓	✓	✓	In 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, D. Clark, I. Baggili, and F. Breitinger - FSAIoT [72]	✓		✓		Contains a centralized Forensic State Acquisition Controller (FSAC), openHAB controller was used
L. Babun, A. K. Sikder, A. Acar,	✓	✓	✓	✓	Focuses on forensic-relevant data

and A. S. Uluagac -IoTDots [73]					only (applied on 22 IoT devices)
F. Bouchaud, G. Grimaud, and T. Vantroys [74]	✓	✓	✓	✓	A forensics framework for an IoT ecosystem contains three stacks, (1) IoT layers such the as sensing layer, network layer, service layer, and interface layer, and (2) the components of IoT ecosystems. (3) the possible forensic options
A. Nieto, R. Rios, and J. Lopez - PRoFIT [75]	✓	✓	✓	✓	Combines privacy requirements (ISO/IEC 29100:2011) and focuses on the potential surrounding devices to collect evidence
T. Zia, P. Liu, and W. Han- An application-specific digital forensics investigative model [76]	✓	✓	✓		Follows NIST Guide for DF process, applied on Wearables, Smart Home, and Smart City
CIPM [59]					Based on the metamodeling method and blockchain
M. Hossain, Y. Karim, and R. Hasan – **FIF-IoT** [60]					Based on a digital ledger
W. A. Mahrous, M. Farouk, and S. M. Darwish [61]					Based on the blockchain technique, it used hashing for authentication and focused on forensic examination and evidence integrity.
M. J. Islam, M. Mahin, A. Khatun, B. C. Debnath, and S. Kabir [62]	✓	✓	✓		Proposed a comprehensive framework for IoT digital investigation, that is not dependent on the network logs and the Cloud Service Provider (CSP).
V. R. Kebande - IDFIF-IoT [63]	✓	✓	✓		Proposed for the IoT ecosystem
IoTCurator [64]					Provides digital forensics examination, access control, authentication, and network attacks mitigation for IoT infrastructure
S. Li [65]	✓	✓	✓	✓	Use case IoT forensics for Amazon Echo, the evidence is collected from sensing, network, cloud, service, and interface layers.

E. Oriwoh and P. Sant - FEMS [66]		✓		✓	Provides forensics and security services for IoT smart home devices
V. R. Kebande and I. Ray - DFIF-IoT [67]	✓	✓	✓		Depending on the proactive process, and reactive process, it complies with the ISO/IEC 27043: 2015
J. P. Sandvik, K. Franke, H. Abie, and A. Årnes [68]	✓				Investigated a coffee file system over Contiki OS
J. M. C. Gómez, J. R. Gómez, J. C. Mondéjar, and J. L. M. Martínez [69]				✓	Investigated nonvolatile memory of Windows IoT core operation system
N. Koroniotis, N. Moustafa, and E. Sitnikova [78]		✓			A new network forensic framework based on deep learning for Internet of Things networks: A particle deep framework
J. Song and J. Li **A Framework for Digital Forensic Investigation of Big Data [52] – recent 2020**					It has 3 parts: digital forensics technology, intermediate technology, and big data technology. It depends on classifying and examining data from different sources and converted into unstructured, semi-structured, and structured rather than depending on cloud, device, network, and mobile levels
L. Babun, A. K. Sikder, A. Acar, and S. Uluagac - VERITAS [73][70]	✓	✓	✓	✓	Uses data collected from the smart environment to conduct forensic investigations, these data are automatically analyzed using a First Order Markov Chain model. (applied on 22 IoT devices)

2.8 IoT Digital Forensics Challenges in the Era of IR 4.0

IoT forensics includes investigating cybercrime perpetrated in an IoT environment. The heterogeneous IoT environments are made up of several connected IoT devices which communicate with other IoT devices across different networks and frameworks [6]. The literature review in this thesis indicates that IoT forensics has multi-levels that should be considered in the IoT digital forensics investigation, including device, network, and application levels [55, 57]. Therefore, digital investigators face several challenges surrounding each level in the IoT environment. The investigator should investigate either

one level or multi-level according to the IoT device when dealing with IoT forensics cases, the investigator might be interested in (1) IoT device forensics, (2) IoT network forensics, and (3) IoT application forensics which include mobile forensics, Web interface and/or cloud forensics. This section stated the challenges for each level:

- General IoT Digital Forensics Challenges.
- IoT Digital Forensics Challenges at the Device Level.
- IoT Digital Forensics Challenges at the Network Level.
- IoT Digital Forensics Challenges at the Application Level.

2.8.1 General IoT Digital Forensics Challenges

In a survey conducted by [79] targeting people with a digital forensics background, 27% of responders marked that they were involved in IoT forensics investigation, most of the IoT cases were related to smart home appliances such as Amazon Alexa, IP cameras, CCTV, and smart TV, in addition to infotainment systems from vehicles and smart health devices. From the provided cases, responders stated several challenges while conducting IoT forensics, for instance, lack of technical training, lack of education, and software issues hold the highest rank in IoT forensic challenges. Whereas cloud data storage, funding, and legal issues had a less rank in IoT forensic challenges. Moreover, the responders pointed out that the research should be focused on cloud forensic data, IoT volatile data, and IoT forensic tools. Another group of responders stated that encryption should grab good attention for coming research. While 73% of responders thought that IoT data acquisition techniques needed improvement.

According to NIST, the two challenges for IoT devices are the sophisticated evidence acquisition process and the cloud's multi-tenant nature [80]. Other studies stated that forensics automation is the third most important challenge faced by IoT technology [81].

IoT devices are always connected to the internet, hence, they lack security controls, 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, as they can exploit the weakness in IoT devices to lunch attacks [82].

Another challenge is the lack of IoT forensic tools, traditional digital forensics tools do not support IoT devices, as sometimes the acquired IoT data is not readable or accessible with the existing digital forensic tools [4, 58]. Some IoT devices use encryption techniques. Thus, it is difficult to collect evidence. Moreover, the lack of an IoT dataset for training, the lack of methodologies and frameworks for IoT data acquisitions, and different IoT wireless transmission protocols are all considered challenges faced by investigators [4, 83].

Each phase in digital forensics has different challenges regarding the IoT environment. For example, in the acquisition phase, it is difficult to collect all evidence as data is usually stored in multiple locations. Also, sometimes it's hard to image the storage of IoT devices. IoT data might be encrypted, and it is hard to be explained. The lack of IoT forensics tools and the variety of standards and vendors create obstacles when it comes to the examining and analyzing phases. Figure 2.5 clarifies and concludes general challenges in the IoT forensics process.

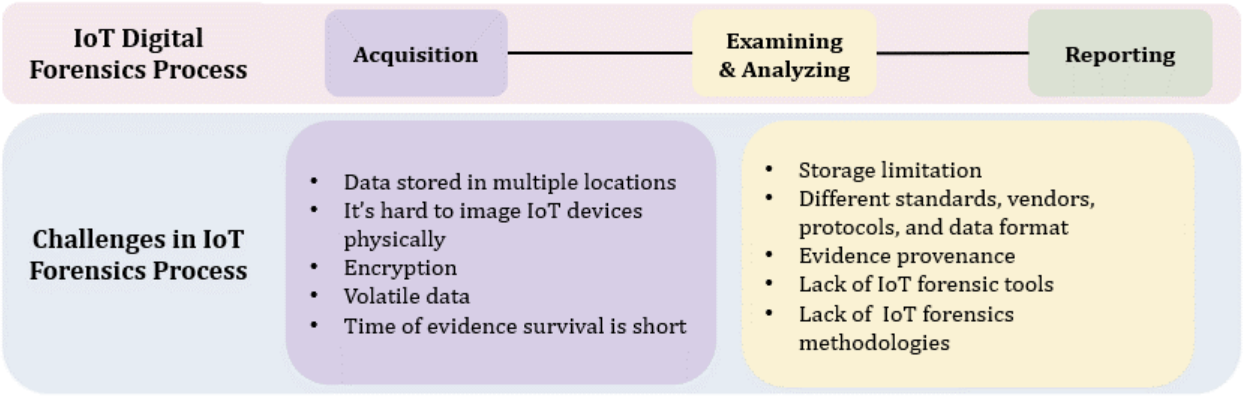

Figure 2.5. Challenges in IoT forensics process.

2.8.2 IoT Digital Forensics Challenges at the Device Level

Several IoT forensics challenges were stated in the literature, including, data format variety, multiple vendors, various platforms, and different standards [83]. 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, also, the time of evidence surviving is short and could be overwritten [83]. Forensics over the IoT device level is vital

to gather complete data that has not yet been sent to the cloud, to check the data integrity, and to compare it with other gathered artifacts from the application and network levels [82]. RAM, Flash memory, microcontroller, and networking capabilities (Bluetooth, WiFi, GSM), are components of interest included in the IoT forensics process [84]. At the IoT device level, the investigator could be interested in investigating the operating system, file system, and internal/ external memories as they are considered a good place for investigation and contain rich evidence that can be presented to the court. Some IoT devices don't have ports for connection to the investigation workstation which poses a challenge for investigators to examine the internal storage, file system, or operating system [71], In addition, the investigator can't usually image the storage of IoT devices physically as most IoT devices have different standards and structures [85]. 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 [71]. Additionally, the limited storage available for storing artifacts [5, 71].

There are several OS used in IoT devices, the most common are TinyOS, Contiki, LiteOS, Riot OS, and Andriod [68]. The file system enables users to store and access data from the operating system, the file system is considered a valuable source of evidence as it keeps track of user activity such as files deleted, created, and modified [86]. Many file systems are available, and each one has a different structure, size, and features [86]. YAFFS2, HRFS, LittleFS, JFFS2, FreeTROS +, FAT, Reliance Edge, Reliance Nitro, and Coffee are file systems designed for flash memory and resource-constrained devices [68]. The variety of filesystems and operating systems used in IoT devices leads to other challenges for investigators as the investigator needs to be aware of the IoT filesystem structure to define and locate critical artifacts.

2.8.3 IoT Digital Forensics Challenges at Network Level

The complex architecture of IoT networks and fast network traffic of the IoT environment raise new obstacles in the path of digital investigations. In addition, most of the time IoT networks are physically inaccessible, and the evidence is highly distributed over networks, this makes evidence barely collected and hardly preserved [71]. The mobility of network

IoT traffic poses hurdles in defining the artifact's location or acquisition of artifacts during the investigation [43, 58].

IoT environments generate amounts of data that can be considered potential artifacts in investigations. Hence, there is a need to reduce artifacts during acquisition, examination, and analysis because it is impractical to handle huge amounts of data [58]. IoT digital forensics challenges at the network level could be concluded in the following:

- Storage: 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 [59, 87, 43].
- Network Speed: The high speed of data transmission over networks causes capturing incomplete traffic, thus, the identification of attacks becomes harder [87].
- Data Integrity: Keeping the integrity of captured network traffic is a challenge for network investigators as this traffic could be affected by software and hardware errors or could be modified by intruders [87].
- Data Privacy: Privacy is considered one of the challenges for investigators, as the collected data could contain sensitive information, thus, network traffic should be gathered without affecting user privacy and organization policies, the attacker can exploit data privacy issues in IoT devices to do malicious activities such as eavesdropping, phishing or/and control hijacking [4, 5, 87].
- Source IP: Recognizing the source of IP addresses, as the intruders can use spoofed IPs to conduct their attacks, conduct man-in-the-middle attacks, and hide traces [87].
- Data Extraction: Extracting network data from different network locations and several devices, the investigator should choose the right device, the appropriate location and time, and suitable tools to extract the related evidence, on the other hand, the attacker can manipulate the data [4, 43], In addition to the extracting artifacts from encrypted traffics could be another challenge for investigators [5].

2.8.4 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 [13, 15]. Mobile forensics is part of digital forensics interested in techniques that extract and present evidence from mobile devices [88, 89]. The mobile forensics process mainly includes the seizure step, acquisition step, and analysis step. Mobile forensics investigators face several challenges at each step such as the different kinds of mobiles, manufacturers, and operating systems [90]. Further, passcode recovery, lack of forensics tools, built-in security, encryption, and privacy features, and anti-forensic techniques [88]. Moreover, the complexity of mobile structure [90], collecting evidence, and the different standards available are considered challenges for mobile forensics experts [91]. Thus, special skills are required from forensic experts to acquire and examine all types of devices [88]. Usually, most IoT devices are controlled by mobile applications, these mobile applications might be downloaded on the Android operating system or the iPhone operating system (iOS). Thus, digital forensics should be aware of iOS and Android security features, Moreover, the digital investigator needs to be aware of data acquisition types for mobile devices and the challenges for each type. The following subsection reviewed (1) the iOS security features, (2) the Android security features, and (3) data acquisition challenges for mobile devices that have both iOS and Android operating systems.

2.8.4.1 iOS security features

iOS is an operating system that's only supported by Apple company and the related manufactured hardware [92]. The different versions of Andriod require different acquisition methods, while in iOS, there is not such a wide diversity of devices and operating system versions [92]. iOS has several security features that any investigator should be aware of. Table 2.5 concludes the security features provided by iOS [88].

Table 2.5. Security features in the iOS

Security Feature	Description
Passcodes, Face ID, and Touch ID	Restricting unauthorized access to the device
Code signing	Preventing from downloading and installing unauthorized applications on the

	device
Sandboxing	Applications installed on iOS are sandboxed, which means that each application can not access the data stored by another
Encryption	In iOS, the entire data dump is encrypted with a key stored between the hardware levels and the OS of the device
Data protection	An encryption key generated by a passcode and the device hardware encryption is used to encrypt data at rest
Address Space Layout Randomization (ASLR)	A mechanism that makes memory exploitation difficult by randomizing the data location in the memory
Privilege separation	The principle of least privilege is used in iOS, the important applications run with root user privilege while all other applications run with mobile user privilege
Stack-smashing protection	A technique for protecting against buffer overflow attacks by placing a random value between the control data and a buffer on the stack
Data wiping	A technique for deactivating and recovering the deleted data removes the encryption keys from the device to wipe all content and settings
Activation Lock	Introduced with iOS 7 to prevent device theft by using "Find My iPhone" which activates the lock and erases the device remotely

2.8.4.2 Android security features

Android is an open-source operating system (OS), and it is considered the most popular OS for mobile devices [88]. The first version of the Andriod OS was launched in 2008 and is based on Linux [88]. The extraction of data from Android was very easy in the initial versions because Full Disk Encryption (FDE) was not used. With the updates, the security features were developed and data extraction become more difficult. Forensic investigators need to understand the internals of Android security, Android has several security features. Table 2.6 concludes the security features provided by Android [93].

Table 2.6. Android security features

Security Features	Description
App Sandbox	Isolates app resources
App signing	Each app must be signed, this lets developers identify the app author and creates updates without permissions
Authentication	Guarantees authorized access to devices and apps using passwords, patterns, and other authentication methods
Biometrics	Implements authentication into devices and apps

Encryption	Guarantees control access by an unauthorized party
Keystore	Provides key generation for symmetric and asymmetric keys for data encryption and decryption
Security-Enhance Linux	Activates mandatory access control (MAC) overall processes
Trusted Execution Environment (TEE)	An isolated area ensures the security of data stored inside
Verified Boot	Guarantees codes come from a trusted source

2.8.4.3 Data Acquisition Challenges for Mobile Devices (iOS and Android)

For digital forensics investigators, it is crucial to know where the artifact is stored, information in mobile devices is stored in different places which poses a challenge for digital investigators. Typically, there are several ways to collect data from mobile devices including (1) physical acquisition, (2) logical acquisition, (3) cloud acquisition, (4) chip-off acquisition, (5) and manual acquisition [89].

The physical acquisition is considered the most complete source of evidence among all acquisitions as it offers lots of advantages such as access to all data stored in the device, the guaranteed timeframe, and the relatively high acquisition speed, in addition to the potential access to deleted data [89]. The physical acquisition could be done on most Android devices and older Apple versions, and the recent Apple devices and Android devices with a known passcode. While it is difficult to get physical acquisition from recent Apple devices and recent Android devices [92]. To do the physical acquisition, the mobile devices must be jailbroken in iOS, or rooted in Android [92]. Jailbreaking in iOS devices and rooting in Android devices are techniques that remove the limitations on the devices, and allow unsigned code and unapproved apps to gain access to the root and run. Jailbreaking or rooting helps in forensic physical acquisition in some cases but the warrant is no longer valid when jailbreaking is conducted on iOS devices or when rooting is conducted on Android devices [88]. Although there are many tools available for jailbreaking such as TaiG, Electra, and Pangu, however, not all iOS versions are jailbreakable [88]. On the other

hand, rooting Android devices depends on the manufacturer's device. Logical and cloud acquisition offer access to the most of data stored in the device, but it doesn't guarantee a recovery timeframe or access to the deleted files [89].

In the cloud acquisition, the investigator needs the user's credentials, to get access to the mobile data, two-factor authentication poses other challenges, and the amount of data extracted is limited. Cloud acquisition does not need rooting in Andriod or jailbreaking in iOS [92].

Collecting, extracting, and analyzing IoT evidence from distributed networks and the cloud is a challenging task due to the huge volume of data, high-speed data transmission, lacking data integrity, and difficulty in accessing IP addresses [62]. Some IoT devices are configured to be fully dependent on cloud services which leads to other challenges in forensic investigations [58]. In some cases, it is easy to acquire artifacts from the cloud especially when the investigator has credentials, while, in other cases, it is hard to seize artifacts from the cloud or sometimes it's inaccessible [92]. Hence, the identification of artifact location via the cloud is a big challenge in IoT forensics. Moreover, certain legal challenges could also appear when geographical boundaries are crossed in the case of cloud services [58].

Logical acquisition is another type of acquisition used for mobile devices, which is used frequently, the mobile device is connected to the investigation workstation using wireless (e.g. WiFi or Bluetooth) or wired (e.g. USB) to extract data [89]. In iOS, it is possible to find backups of data via iTunes or iCloud applications [88]. On the other hand, it is possible to acquire data from Android devices directly using acquisition tools. There are many tools used for logical acquisition such as Magnet AXIOM, UFED Physical Analyzer, Belkasoft Acquisition Tool, MOBILedit, Autopsy, and other tools. In addition, there are several techniques for extracting data logically from Android devices, such as Android Debug Bridge (ADB) pull data extraction, ADB is a command line tool that allows the connection of Android devices to the workstation through a USB cable. USB debugging

option should be enabled and the device should be unlocked in order to extract data successfully [92].

Chip-off acquisition is another type of acquisition that needs special skills and hardware, as the data is extracted directly from the memory chips [92]. The investigator needs to carefully remove the memory chip by desoldering the chip from the device's circuit board and attempting to read it, thus it is hard to restore the device to the original state, and the heat used to remove the chip could damage the data [92]. Joint Test Action Group (JTAG) is an advanced data acquisition technique, which includes connecting to specific ports on the device to transfer the data stored on the device for analyzing purposes, by this method, a full physical image of a device can be collected. The investigator should be experienced and trained before trying JTAG as the device may be destroyed if not handled properly [92].

Manual acquisition is a type used for data acquisition from mobile devices, this type of acquisition is not accurate and subject to human errors, as the investigator navigates the device and views the data stored manually, he records the evidence but he can't access the deleted files. These data could be recorded using an external camera, the data may be modified, overwritten, or deleted when the examiner does the manual extraction [89]. Table 2.7 concludes the comparison between mobile devices acquisition methods [92, 89]:

Table 2.7. Comparison between mobile devices acquisition methods

	Physical Acquisition	**Logical Acquisition**	**Cloud Acquisition**	**Chip-off Acquisition**	**Manual Acquisition**
Access to deleted files	It can be accessed	Can't be accessed	Can't be accessed	Can't be accessed	Can't be accessed
Access to stored data	It can be accessed to all stored data	It can be accessed to part of the stored data, user data, and filesystem	It can be accessed to part of the stored data	It can be accessed to part of the stored data	It can be accessed to the stored data in the device's memory
Issues	Some devices must be jailbroken or rooted	Complex passwords may prevent the data recovery	Credentials (Password, ID) are required	Encrypted data is non-recoverable and non-decryptable	Time-consuming

				The chip-off acquisition is not available for most devices	
Tool used	Mobile forensics tools	Mobile forensics tools	Mobile forensics tools	Mobile forensics tools, special skills, and hardware	Mobile interface

2.9 Summary

In this chapter, an overview of IoT history, IoT definitions, IoT architectures, and common IoT attacks were presented. Moreover, several previous digital forensic frameworks were reviewed. Many IoT digital forensic frameworks were explored, stated, and compared according to the three levels of IoT architecture (the device level, the network level, and the application level). IoT digital forensics was compared with traditional digital forensics. In addition, IoT digital forensics challenges for each IoT level were stated. Moreover, iOS and Android security features were stated. A comparison between mobile device acquisition methods was explored. As a result, the gathered literature review in this chapter inspired the researcher to invent, design, and propose a novel IoT digital forensics framework encompassing the advantages of the previous frameworks and overcoming IoT forensics challenges with additional new features. The proposed framework is presented in the next chapter.

Chapter 3

3 Methodology of the Proposed Framework

3.1 Introduction

The previous chapter presents an overview of IoT history, definitions, IoT architectures, and common IoT attacks. Additionally, it reviews the previous digital forensic frameworks in general, and IoT digital forensic frameworks in particular, IoT digital forensics was compared with traditional digital forensics, in addition, IoT digital forensics challenges were stated, and as a result, the novel IoT digital forensics framework was invented and proposed. Thus, this chapter aims to

- Present the proposed framework for IoT digital forensics named "Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT)".
- Present the advantages of the (MAoIDFF-IoT) framework which overcomes the IoT digital forensics challenges.
- Explain each phase of the proposed framework in detail.

3.2 The Structure of 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 main structure of this framework is clarified in Figure 3.1. The MAoIDFF-IoT framework is built based on the literature analysis, it stated the traditional phases of the digital investigation process, in addition to new subphases and features that were added to the proposed framework based on the experimental analysis to fit the structure of the IoT environments and to face the IoT digital investigation challenges.

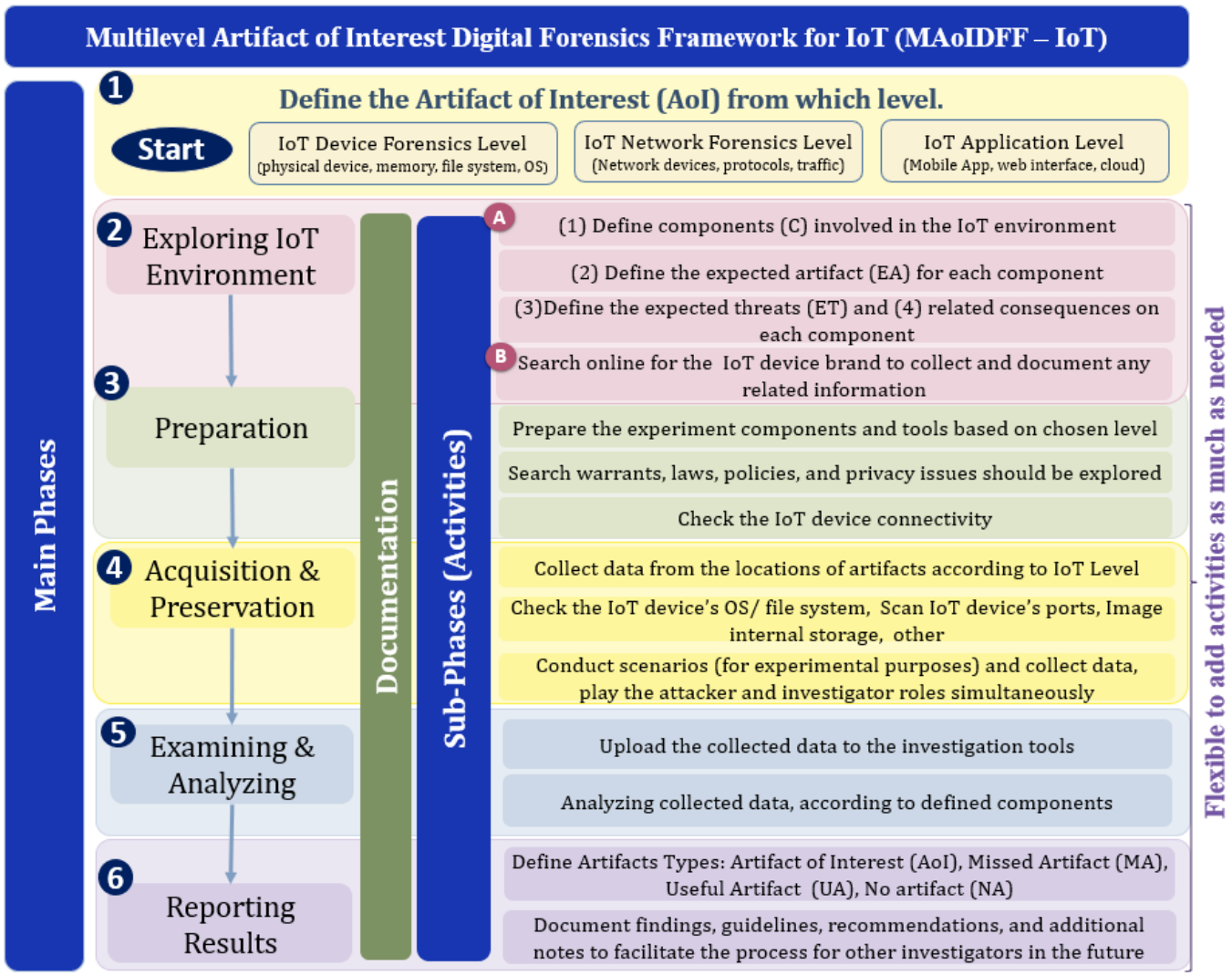

Figure 3.1. The Proposed Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT).

3.3 Phases of (MAoIDFF-IoT) Framework

Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT) has 6 main phases as shown in Figure 3.1, in addition to the documentation phase that should be done in parallel with all phases. The phases are stated as follows.

- Define the Artifact of Interest (AoI) based on the level/ Documentation
- Exploring IoT environment/ Documentation

- Preparation/ Documentation
- Acquesition & preservation/ Documentation
- Examining & analyzing/ Documentation
- Reporting/ Documentation

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

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

To make the proposed framework fit the recent and future possible IoT digital crime investigations, overcome the diversity of IoT standards, brands, structures, and features, and avoid missing any artifacts of interest, this phase comes in this place. This phase includes defining the investigation scope which is a very imperative phase since each IoT device has different features and services, for example, some IoT devices have connected to the cloud and others are not. Some IoT devices have internal or/and external memories, while other IoT devices don't, further IoT devices have different file systems, and not all IoT devices are connected to the web interface, or/and mobile applications, thus according to the IoT device, the investigator can define the investigation level.

Each level has several artifact locations, thus, if artifacts were missed from locations at any level it’s possible to find them on other level locations. Lots of artifacts can be extracted from IoT environments, these artifacts might be extracted from three main levels includes (1) IoT device level, the artifact locations in the IoT device level include: 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 related application level involves web interface, mobile app, and cloud. Table 3.1 clarifies artifact locations according to the IoT levels. Depending on the artifact of interest, the investigator should choose which level/levels to be focused on since each level has its forensics tools, for example, Wireshark is used for network forensics while FTK imager is used for capturing memory images from the device level.

To make the investigation more effective, the investigator should determine just one level, then proceed with the rest phases. If the IoT device has more than one level, for example, a camera device is connected to the internet and sends streaming videos via the network, also, it has external storage and it has a mobile app for controlling. Thus, this camera has three levels targeted by the investigator which are the device, the network, and the application levels. In this case, the investigator can choose all these levels, but he must investigate each level separately, as mentioned each level has its procedure and tools. Once the investigator chooses one level he can proceed with the rest phases. Then he can go to the next level and do the rest phases. Figure 3.2. clarifies the flow chart of this phase. All activities in this phase should be documented very well before being submitted to the court.

Table 3.1. Artifact locations according to the IoT levels

IoT Levels	Device level	Network level	Application level
Artifact Locations	• Physical device • Internal memory • External memory • Operating system • File system	• Network Traffic • Protocols • Network devices (router, server, switch)	• Web interface • Mobile IoT Application • Cloud

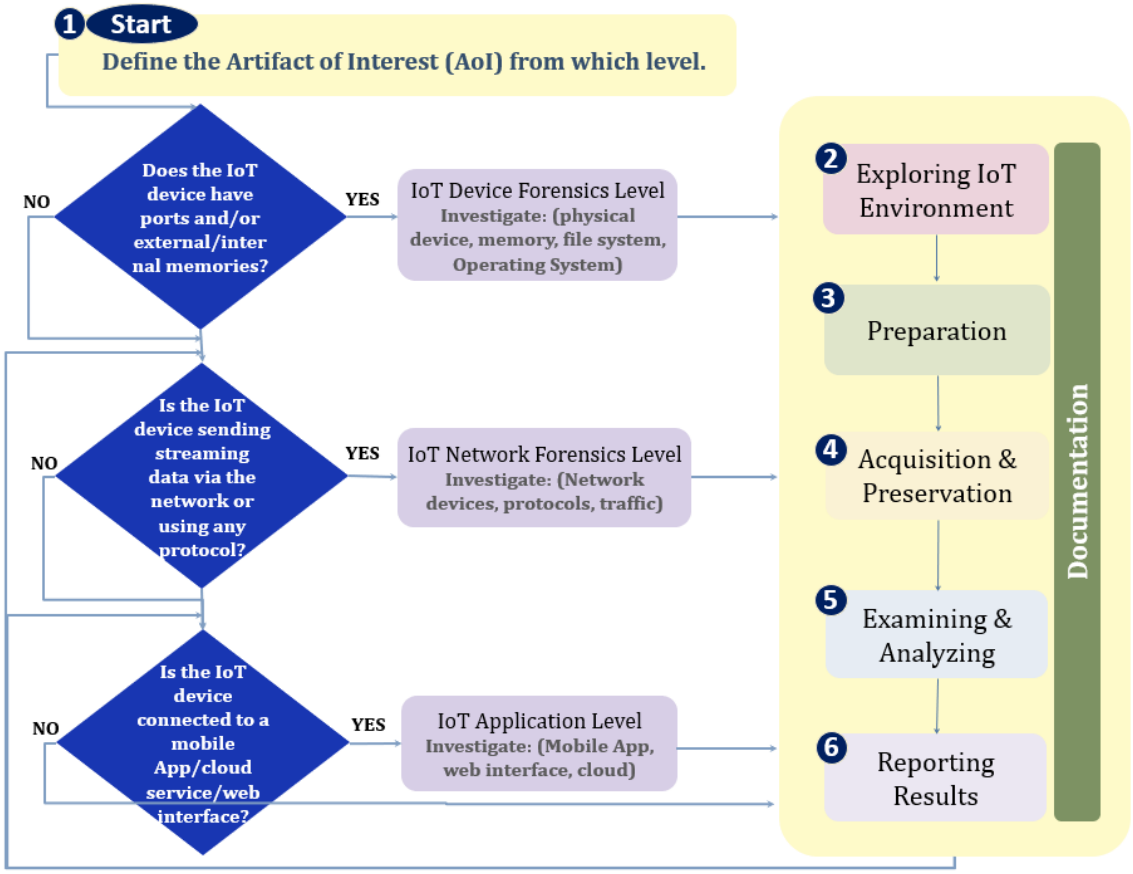

Figure 3.2. Define the Artifact of Interest (AoI) based on level.

3.3.2 Phase 2: Exploring the IoT Environment/ Documentation

To avoid missing any artifacts, the investigator should explore the IoT environment very well. The proposed framework focused on getting an initial understanding of the IoT environment, by defining the four main parts; (1) the components involved in the scene, (2) the expected artifacts (EA), (3) the expected threats (ET) for each component, and (4) the consequences of the expected threats. All these parts in the IoT environment should be defined and documented. Figure 3.3 clarifies an example of exploring the IoT environment. In addition, the investigator can search online for the IoT device brand to check its structure, features, OS type, file system type, and any other useful information that might help in the investigation, all gathered information should be documented.

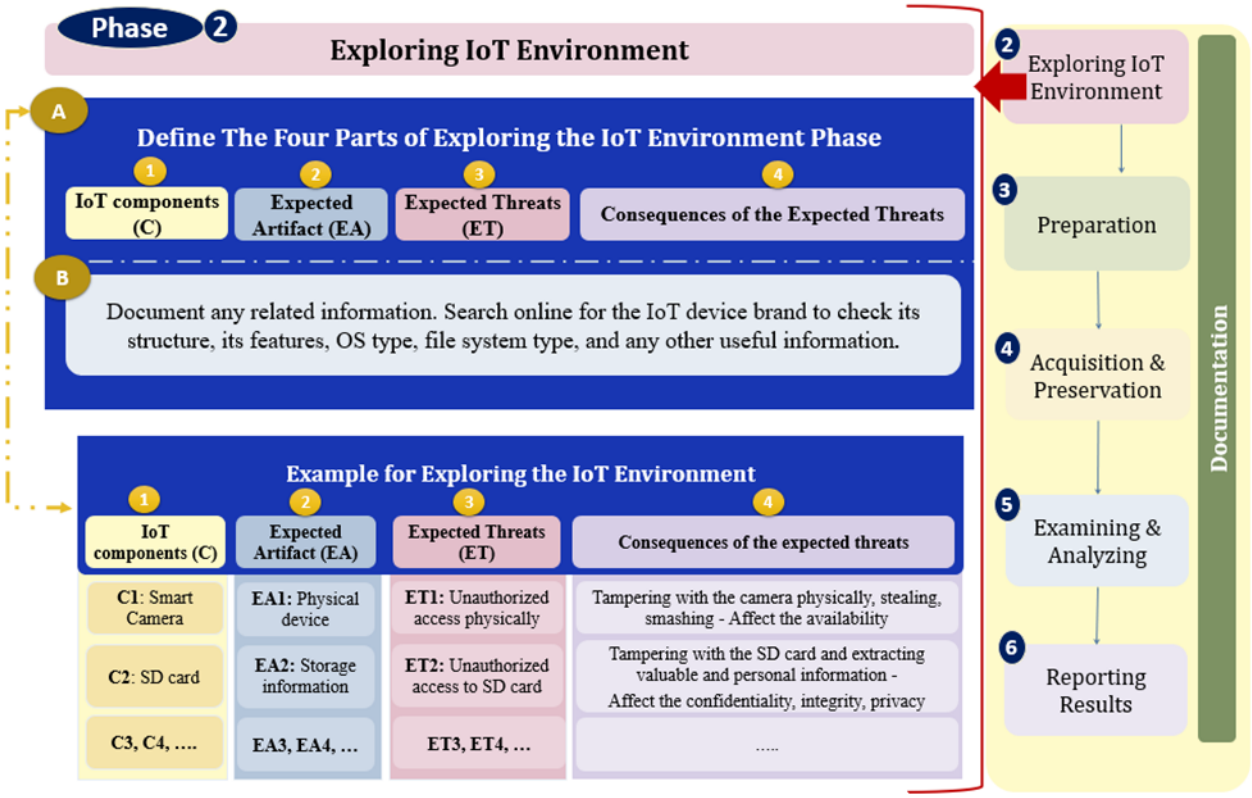

Figure 3.3. An example of exploring the IoT environment.

3.3.3 Phase 3: Preparation/ Documentation

Before carrying out the investigation, the investigator should prepare the investigation workstation and the appropriate investigation tools based on the chosen level and locations to prevent delayed investigation. In addition, the IoT device connection should be checked, also, the investigator should explore the search warrant, laws, policies, and privacy issues in this phase [33]. Preparation is considered the starting point of an incident response. Lack of preparation leads to the loss of critical artifacts such as volatile information [58]. The investigator should document the type of used workstations and tools and any other related information included in this phase. Figure 3.4 clarifies phase three according to the proposed MAoIDFF-IoT framework.

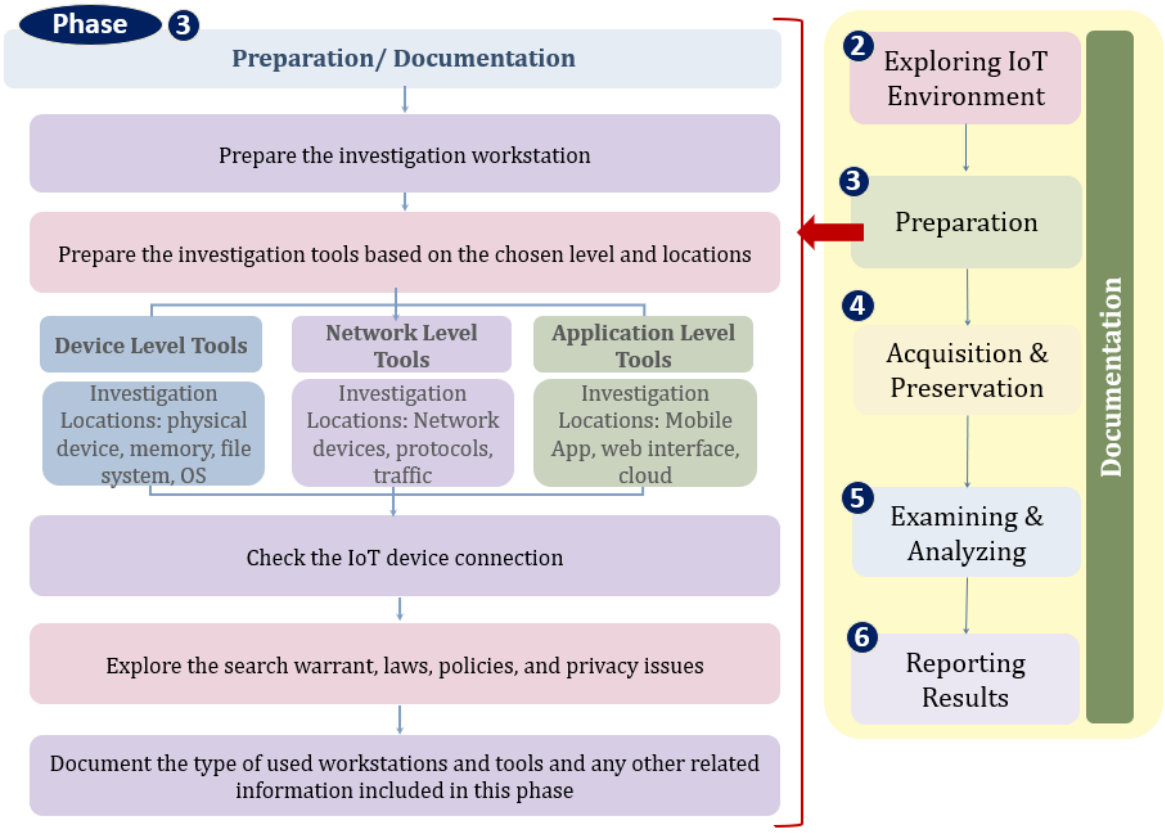

Figure 3.4. Phase three according to the proposed MAoIDFF-IoT framework.

3.3.4 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 might be both digital and physical artifacts [33], and both artifacts need to be preserved and investigated [58]. In addition, collecting volatile and non-volatile data with preserving the integrity of the collected data is a vital process to ensure admissibility in court [45]. The data should be collected from several locations according to the chosen level, if the chosen level was an application level, it is good to define the type of acquisition whether it is physical, logical, the cloud, chip off, or manual acquisition. Also, backups and calculating hashes should be conducted for all the gathered data before proceeding with the next phase [28]. The proposed framework focused on an additional part in the (acquisition & preservation) phase, which is a good part for experimental purposes that run several

scenarios by simultaneously playing the role of user and investigator. All the collected data from the predefined scenarios should be collected for analysis in the next phase. Further, all activities in the (acquisition & preservation) phase should be well documented to be submitted to the court. Figure 3.5 clarifies phase four according to the proposed MAoIDFF-IoT framework.

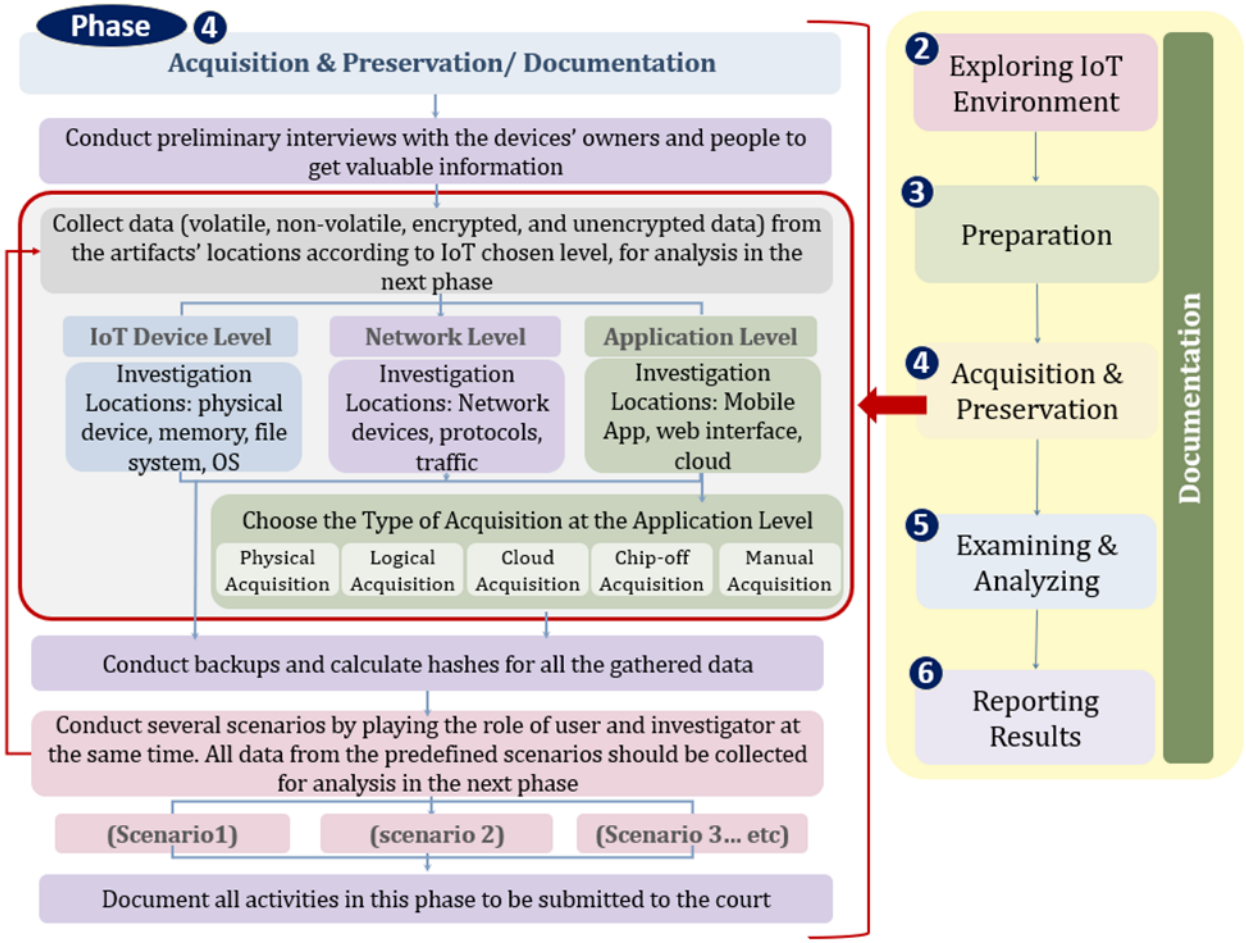

Figure 3.5. Phase four according to the proposed MAoIDFF-IoT framework.

3.3.5 Phase 5: Examining & Analyzing/ Documentation

All the collected data in the previous phase should be examined and analyzed by the investigator and the investigation tools, this includes data in-depth, data searching, data organizing, artifact locating, artifact identifying, information filtering, hidden data, deleted data, and keyword searching concerning the nature of the IoT environment and the crime

scene [26, 33]. The investigator should read, understand and analyze all gathered information such as calendars, text messages, voice messages, pictures, documents, file extensions, and other data, in addition, to extracting other information like hidden files, passwords, and emails [45].

Encrypted data was considered in the proposed framework, for example, at the network level, the investigator might gather encrypted traffic, thus, analyzing encrypted traffic may be required using specific tools.

Reverse engineering for IoT mobile apps also was added and considered in the proposed framework. At the application level, some of the IoT devices are controlled by mobile Apps, if the investigator can't find the related artifact from the IoT app, thus reverse engineering may be needed to analyze how the app acts and recognize where the app stores related data.

In addition, several IoT devices have filesystems, thus, the MAoIDFF-IoT framework suggested four steps for IoT file system analysis which are: (step1) analyze the boot sector, (step2) analyze root directory, (step3) analyze 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 [58]. More additional activities might be needed and all the analysis findings should be explained and accurately documented [45]. The MAoIDFF-IoT framework focused on an additional part in the (examining & analyzing) phase which is examining and analyzing the results from predefined scenarios conducted in the previous phase. Recalling the previous phase the researcher played the role of user and investigator at the same time. The investigator tries to find artifacts according to the conducted actions, the extracted artifacts should be classified into four: missed artifact (MA), no artifact (NA), the useful artifact (UA), or artifact of interest (AoI), thus, four types of extracted artifacts were proposed, these artifacts types were described in Table 3.2. Phase five according to the proposed MAoIDFF-IoT framework is clarified in Figure 3.6.

Table 3.2. 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
Artifact of Interest (AoI)	When there is an action and the investigator proves the action and extracts the artifact correctly

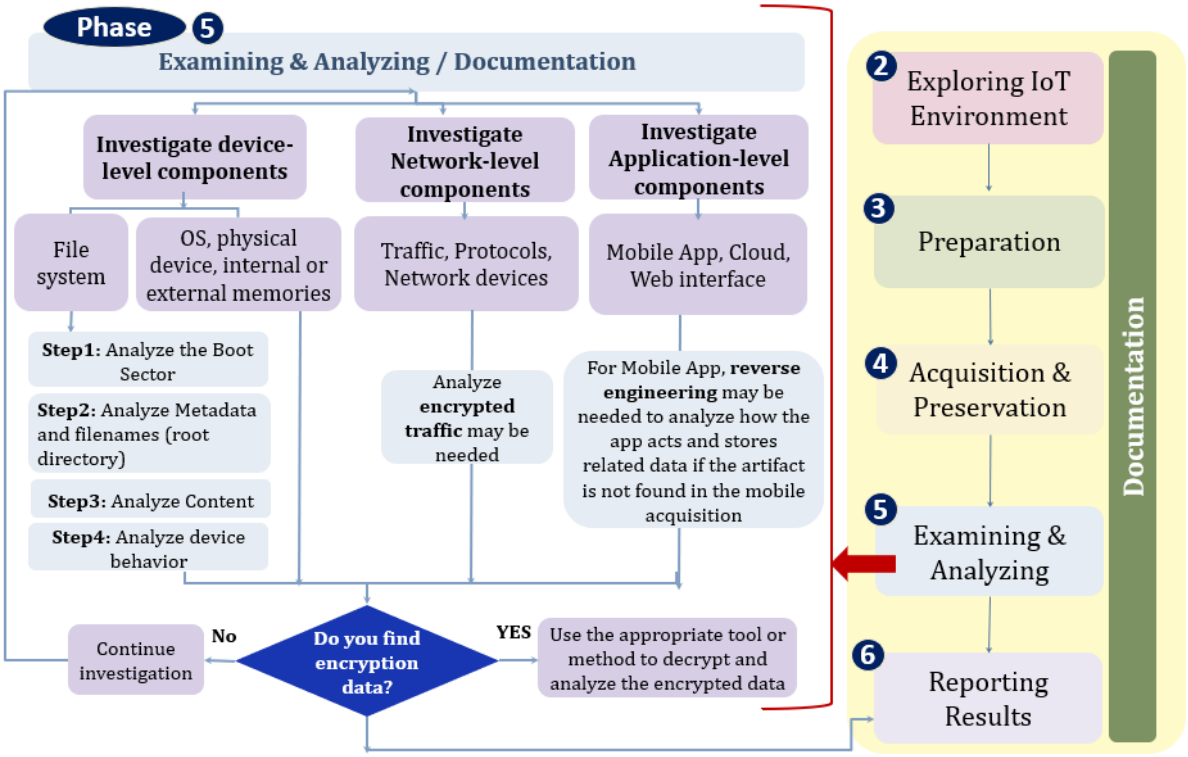

Figure 3.6. Phase five and phase six according to the proposed MAoIDFF-IoT framework.

3.3.6 Phase 6: Reporting the Results/ Documentation

The investigator should document the result of all gathered information from previous phases, the devices, the observations, and the actions concisely and clearly by

photographing them in a report to be submitted to the court [26, 33]. All the artifacts types (MA), (NA), (UA), and (AoI) should be defined according to the conducted scenarios and documented. To avoid missing any artifact, the documentation should be a continuous process, it should be done during all investigation phases [29]. 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 [58]. It's vital to classify people as witnesses, victims, and suspects. Several forensics tools have built-in reporting features. However, the examiner should be able to report and document his analysis and perspective. The report may include, the case ID, case examiner, date of report, data of received case, ID and signature of the examiner, description of case items, methods, and tools used. In addition to the steps taken during the investigations, details of analyzing evidence, findings, and finally, the conclusion which includes the offense name, suspect names, artifacts of interest (AoI), and the related cybercrime law. Proper documentation is important to be submitted in court and helps in reviewing the crime case anytime [89]. It's important to know that documentation is a continuous activity required in all investigation phases for preserving the proper chain of custody [45]. Guidelines, recommendations, and additional notes related to the case should be stated at the end of the report to facilitate the process for other investigators in the future, this is an additional activity proposed in the MAoIDFF-IoT framework. Phase six according to the proposed MAoIDFF-IoT framework is clarified in Figure 3.7.

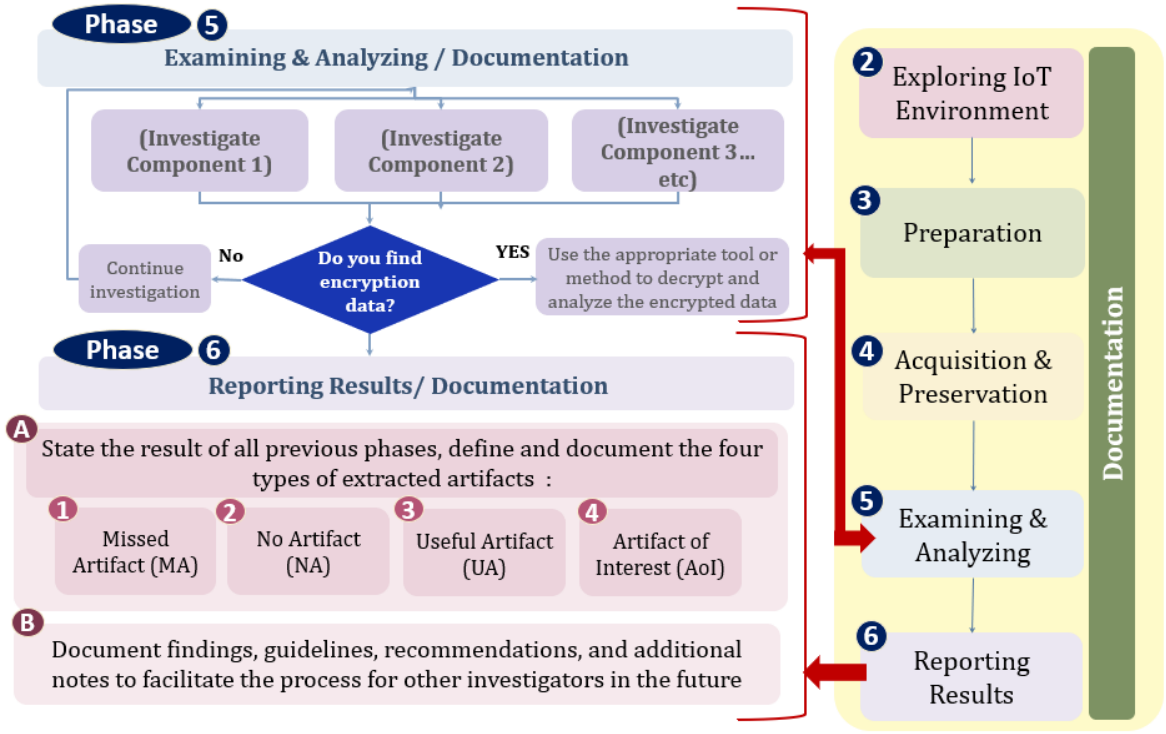

Figure 3.7. Phase six according to the proposed MAoIDFF-IoT framework.

The suggested structure for the expert witness report based on (MAoIDFF-IoT) framework that should be submitted to the court is clarified in Table 3.3 as follows:

Table 3.3. The 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 offense name, case name, case number, the tools used, date of request, date of conclusion, and date of the published report. • Result paragraph This includes the offense name, suspect 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 AoI 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.

The MAoIDFF-IoT framework has been designed to assist the digital forensic community in setting up appropriate activities when dealing with IoT digital forensic cases, in addition to overcoming the IoT forensics challenges. It provides rapid and intelligent analysis, and it supports the different traditional phases of the digital investigation process. It has an organized structure which makes it easy to understand and apply. In addition, it is flexible as it has six main phases and the investigator can add activities in sub-phases as much as the case needed. Moreover, the advantages of the proposed framework are ensuring integrity by preserving the extracted artifacts and documenting every activity done during the investigation. Also, the development of the proposed IoT digital forensics framework involves the forensic analysis of all kinds of possible digital crime scene investigations that are related to the IoT environments. Because it explores the IoT environment and covers all the possible IoT levels needed in the investigation (ex: device level, network level, and application level) to extract Artifacts of Interest (AoI) for each level. This avoids consuming time and effort and at the same time avoid missing any critical artifacts.

The proposed MAoIDFF-IoT framework encompasses the advantages of the previous digital forensics frameworks [28, 29, 33, 50, 63, 65, 74], as well as new features that were added to make it an effective framework. Table 3.4 clarifies the superiority and advantages of the MAoIDFF-IoT framework over existing frameworks.

Table 3.4 The advantages of the proposed MAoIDFF-IoT framework in comparison with previous frameworks

Framework Advantage	The proposed framework MAoIDFF-IoT	Quick et al., 2014 [50]	Carrier and Spafford, 2004 [29]	Kebande *et al.*, 2018 [63]	Li et al., 2019 [65]	(Kebande and Ray, 2016 [67]	Babun et al., 2021 [70]	Bouchaud et al., 2018 [74]
Focus on the Artifact of Interest (AoI)	✓	✓						
Identification phase to explore the environment	✓			✓	✓	✓	✓	✓
Cover the traditional digital forensics process	✓	✓	✓	✓	✓	✓	✓	✓
Maintain the integrity	✓		✓	✓	✓	✓	✓	✓
Consider the Analyze of encrypted data	✓				✓		✓	

Have not been addressed by others:

- **Cover all the IoT levels, and choose a targeted investigation level to avoid missing any critical artifact**
- **Define the types of artifacts (Artifact of Interest - AoI, Useful Artifact - UA, Missed Artifact -MA, No Artifact - NA)**
- **Understand and define the components (C), the expected artifacts (EA), and the expected threats (ET) for each component.**
- **Consider the reverse engineering for mobile Apps in case the artifact was not found in mobile acquisition.**
- **Suggest a structure for the expert witness report.**

3.4 Advantages of MAoIDFF-IoT Proposed framework

The following sub-sections explain the advantages of the proposed framework as follows:

3.4.1 Focusing on AoI to Save Time and Efforts

Digital Forensic Data Reduction and Data Mining Framework [50] motivates and inspires the researcher to focus on the Artifact of Interest (AoI) as the size of data is the greatest challenge to forensic analysis [50]. The framework has 10 phases: Scope, preparation, identification & collection, preservation, reduction & storage, review & data mining, open & closed source data, evidence analysis, presentation, and completion. It stated the problem of the huge gathered data required to be analyzed in a digital forensics investigation. Thus, focusing on the Artifact of Interest (AoI) makes the investigation process more effective and saves time and effort. In the first phase of the MAoIDFF-IoT framework, the AoI from which level is defined**,** multi-level is included since if any artifact from one level was missed, it can be caught at another level. Thus, MAoIDFF-IoT is focusing on analyzing and examining AoI, not all the data generated from IoT devices.

3.4.2 The Importance of Exploring the Scope and the Expected Threats and Artifacts

Abstract Digital Forensic Model (ADFM) [33] has 9 main phases, being identification, preparation, approach strategy, preservation, collection, examination, analysis, presentation, and returning evidence. The design of the ADFM framework attempts to be applied to all recent digital crimes, in addition to any unrealized crimes of the future. On the other hand, the development of the proposed IoT digital forensics framework (MAoIDFF-IoT) involves the forensic analysis of all kinds of digital crime scene investigations that are related to the IoT environments. The identification phase for exploring the IoT environment is an imperative phase to understand and define the investigation scope, in the proposed framework, four main parts were proposed in the exploring IoT environment phase being; (1) the components involved in scene (C), (2) the expected artifacts (EA), (3) the expected threats (ET) for each component and (4) the consequences of the expected threats. In

addition, searching for IoT devices online to get related information that may help in the investigation process. Figure 3.8 clarifies the four parts of exploring the IoT environment.

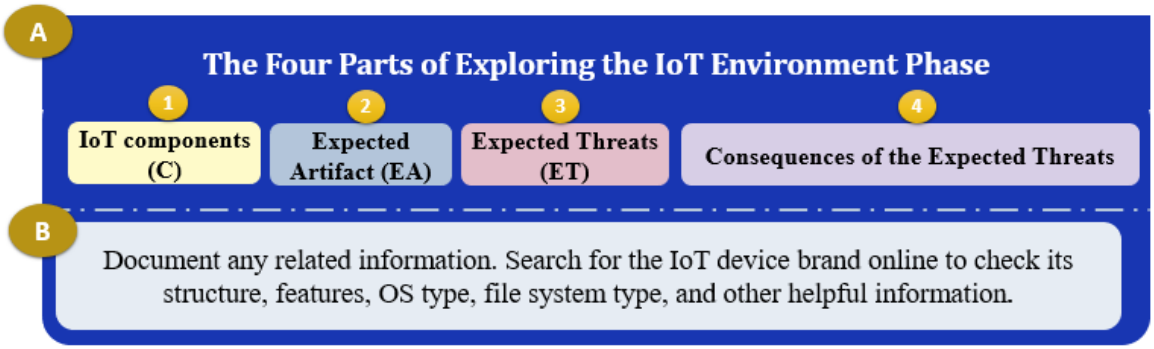

Figure 3.8. Four parts of exploring the IoT environment in the proposed framework (MAoIDFF-IoT).

3.4.3 The Organized Structure With a Generalized, and Standardized Framework

Guide to Integrating Forensic Techniques into Incident Response by NIST Special Publication 800-86 [28] has a simple framework that contained five phases: Preservation, collection, examination, analysis, and reporting. The preparation, preservation, collection, examination, analysis, and presentation phases from (ADFM) [33] and NIST [28] frameworks were taken into account in the proposed framework (MAoIDFF-IoT). These main phases are commonly used in most of the previous digital forensics frameworks [27, 28], [33]–[37], [42] as they are guaranteed success and inclusiveness in digital forensics investigations. However, in MAoIDFF-IoT, these traditional phases included additional sub-phases to fit the heterogenous nature of IoT environments.

3.4.4 Maintains the Integrity

An event-based digital forensic investigation framework [29] stated that documentation is an important phase that should be done through all the investigation phases. Thus, documentation is continuous in nature records, and conducting documentation in all IoT digital forensics phases also is considered in the proposed framework to prevent losing any artifact during the investigation [29]. In addition, conducting a backup of extracted artifacts ensures preserving the integrity of artifacts.

3.4.5 Inclusive, Covering all the IoT Levels, to Avoid Missing Any Critical Artifact

Since the IoT environment has an architecture of mainly three levels (physical, network, and application) [15]–[19], it is good to explore the potential locations to find artifacts of interest (AoI), taking into consideration the commonly cited artifact locations such as the locations of deleted, and hidden files. In addition to determining the types of extracted artifacts such as device information, images, stored data, credential logins, and other valuable information.

The studies by [63], [74], and [65] inspired the researcher to propose a framework based on different levels of IoT architecture. [74] focused on investigating the sensing layer, the network layer, the service layer, and the interface layer, while [63] focused on extracting artifacts from the cloud, network, and device layers. [65] proposed IoT forensic model and applied this model to the Amazon Echo device. The evidence is collected from sensing, network, cloud, service, and interface layers through digital forensics phases: (identification, preservation, analysis, and presentation).

The proposed framework is more holistic and inclusive of recent and future possible IoT digital crime investigations as it explores all possible locations of artifacts based on the main IoT architecture. These artifacts might be extracted from three main levels includes (1) IoT device level (artifact locations: physical device, memory, filesystem, OS), (2) IoT network level (artifact locations: network devices, protocols, traffic), (3) IoT application level (artifact locations: web interface, mobile app, cloud). See Figure 3.9. Exploring all possible locations of artifacts based on the main IoT architecture is a good practice for digital investigators and it is supported in the proposed framework which adds value when developing an inclusive IoT digital framework.

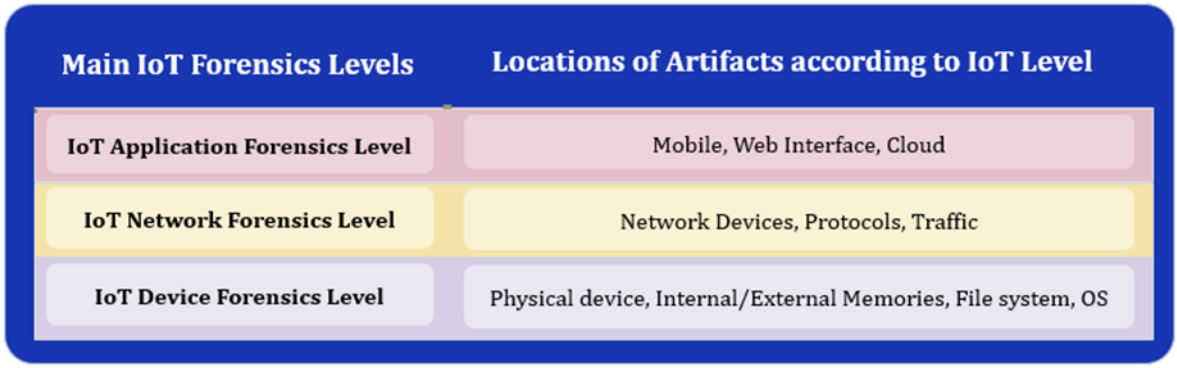

Figure 3.9. The multilevel structure of the proposed framework (MAoIDFF-IoT).

The following Table 3.5 concludes the features proposed in MAoIDFF-IoT according to the related challenges.

Table 3.5. The features in proposed in MAoIDFF-IoT according to the related challenges

IoT digital forensics Challenge	**The features in the MAoIDFF-IoT framework that handles the challenge**
The huge gathered data required to be analyzed makes extracting AoI more difficult	• In phase one, MAoIDFF-IoT focuses on analyzing and examining AoI, not analyzing all the generated data from IoT devices. Thus, time and effort were saved.
Some artifacts might be missed. • At the device level, some IoT devices don't have ports for connection to the workstation which poses a challenge for investigators to examine the internal storage, file system, or operating system. • The time of evidence surviving is short and could be overwritten. • It is difficult to collect all evidence from IoT devices as data is usually stored in multiple locations.	• In phase one of the MAoIDFF-IoT framework, the AoI from which the level was defined, multi-level was included as if any artifact is missed from one level, it can be caught at another level. • In Phase two, four main parts in the exploring IoT environment phase were proposed which are; (1) the components involved in scene (C), (2) the expected artifacts (EA), (3) the expected threats (ET) for each component and (4) the consequences of the expected threats. • Phase four, the acquisition, explores all possible locations of artifacts based on the main IoT architecture. • Phase six, reporting results that define and document the four types of extracted artifacts (AoI, MA, NA, UA). • Thus, the MAoIDFF-IoT framework is inclusive and holistic. It covers all the IoT levels, defines four types of artifacts (AoI, MA, NA, UA), and

	explores four main parts of the IoT environment.
The extent of its use, the framework could be applied to all recent digital crimes and any unrealized crimes of the future.	• In phase two, four main parts in the exploring IoT environment phase were proposed which are; (1) the components involved in the scene (C), (2) the expected artifacts (EA), (3) the expected threats (ET) for each component and (4) the consequences of the expected threats. Thus, understanding and defining the investigation scope. • In phase six, guidelines, recommendations, and additional notes are suggested to be documented, to facilitate the process for other investigators in the future. • It is flexible to add subphases and activities as much as case needed.
Data format variety, multiple vendors, and different standards	• In phase two, exploring the IoT environment, search online for the IoT device brand to check its structure, features, OS type, file system type, and any other useful information. Document any related information. • In phase six, guidelines, recommendations, and additional notes are suggested to be documented, to facilitate the process for other investigators in the future.
Encrypted data gathered from IoT devices	• In phase five, analyzing & examining, the framework states using the appropriate tool or method to decrypt and analyze the encrypted data.
Maintains integrity through all investigation processes	• In phase four, acquisition & preservation, conducting backups, and calculating hashes for all the gathered data. • The framework states the documentation phase which should be conducted through all phases.
The Simplicity and usability	• The framework includes the traditional, generalized, and standardized phases, and the additional sub-phases to fit the heterogenous nature of IoT environments.

3.5 Summary

In this chapter, the structure of the novel proposed framework named “Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT)” was stated and explained in detail. Mainly, this framework has six major phases; (1) defining the AoI according to

the level/ documentation, (2) exploring the IoT environment/ documentation, (3) preparation/ documentation, (4) acquisition & preservation/ documentation, (5) examining & analyzing/ documentation, (6) reporting/ documentation. The documentation is an important phase that should be conducted through the six phases which helps maintain the integrity and build a rich and detailed report to be submitted to the court. Each major phase has sub-phases for additional activities which enrich the framework and make it effective, holistic, and inclusive.

The MAoIDFF-IoT framework encompasses the advantages of the previous digital forensics frameworks, in addition to the additional new features that are designed to make it more usable and applicable to real, recent, and future IoT investigation senses, for example, it covers all the IoT levels, to avoid missing any critical artifact needed in the investigation which are the device level, the network level, and the application level. It highlights extracting Artifacts of Interest (AoI) for each level which avoids consuming time and effort and at the same time, avoids missing any critical artifacts. In addition, it defines the components (C), the expected artifacts (EA), and the expected threats (ET) for each component which make the exploring of IoT environments more understandable. Further, it defines the types of artifacts (Artifact of Interest - AoI, Useful Artifact - UA, Missed Artifact -MA, No Artifact - NA). Thus, the MAoIDFF-IoT framework has several advantages that attract digital investigators to apply and use it.

Chapter 4

4 Implementation, Experiment, and Results

4.1 Introduction

The previous chapter stated the structure of the proposed framework (MAoIDFF-IoT). The framework advantages and its phases were explained in detail. In this section, the proposed framework is evaluated by three case studies. In each case, the researcher conducted several scenarios by simultaneously playing the role of user and investigator. The IoT environment was explored by defining the components, the expected artifacts (EA), the expected threats (ET) for each component, and the consequences of the expected threats. In addition, artifacts according to the conducted actions were found, and the extracted artifacts were classified into four according to the proposed framework: missed artifact (MA), no artifact (NA), useful artifact (UA), or artifact of interest (AoI). All the suggested phases in the proposed framework were applied in this section. The following sub-sections state the three case studies, the first case in (section 4.2) is an experiment on a smart camera at the device level. The second case in (section 4.3) is an experiment on a smart camera at the application level. The third case in (section 4.4) is an experiment on a smart environment containing 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.

4.2 Smart Camera at Device Level Case Study

The first case study is for a smart camera. In the experiment, the researcher investigated according to the proposed framework MAoIDFF-IoT. The following sections clarify phases

applied according to the MAoIDFF-IoT framework. Figure 4.1 clarifies the study framework for the smart camera at the device level case study.

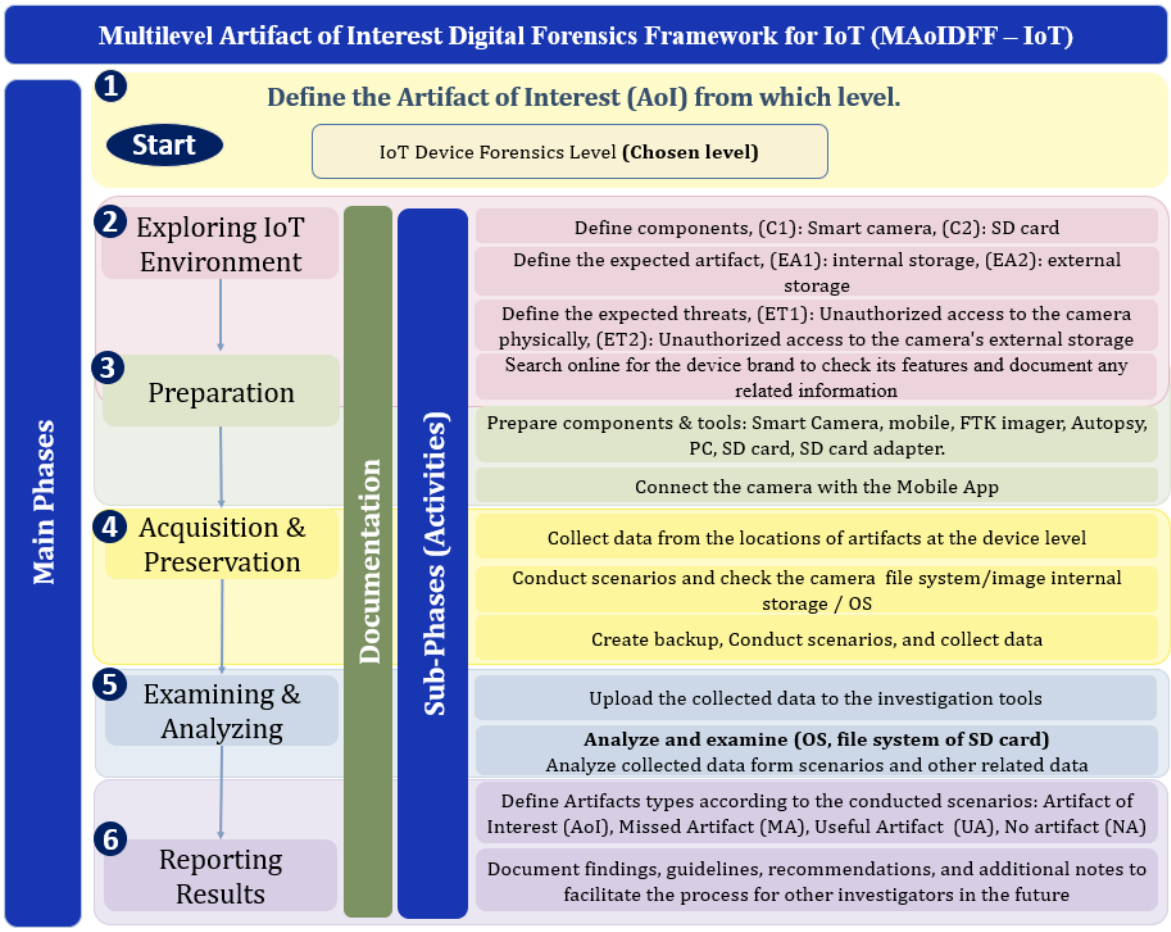

Figure 4.1. Applying the proposed multilevel artifact of interest digital forensics framework on a smart camera at the IoT device level.

4.2.1 Phase one: Define the Artifact of Interest (AoI) from Which Level/ Documentation.

The very first phase is defining the artifact of interest by choosing which level needed to be investigated. According to the MAoIDFF-IoT framework, Figure 3.2 in the previous chapter. The IoT device level is chosen to be investigated in this case study, while the investigator can choose the IoT network forensic level in case the camera is connected to the internet and sends streaming video to the related mobile app. But in this case, the device

level was chosen for investigation, because the camera doesn't have any ports for connection to the workstation but it has an external memory. Thus, (1) the operating system, (2) the external memory, and its filesystem were determined to be investigated at the device level, see Figure 4.2. According to the MAoIDFF-IoT framework, once the investigation at the device level is finished, the investigator can move to investigate other levels such as the network IoT forensics level or application IoT forensics level.

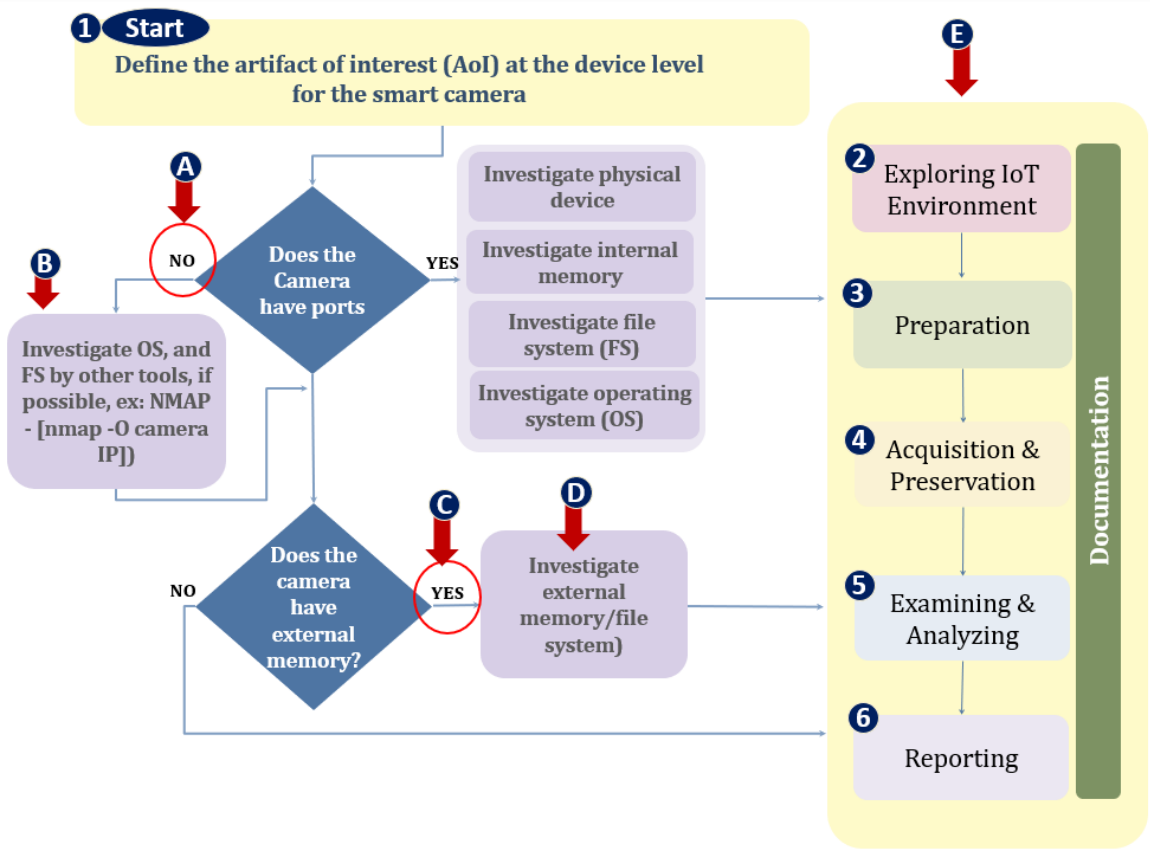

Figure 4.2. Define the artifact of interest (AoI) at the device level for the smart camera.

4.2.2 Phase two: Exploring the IoT Environment/ Documentation

After defining the investigation level which is the device level for the smart camera, 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 threads to understand the IoT environment, see Table 4.1.

Table 4.1. Explore the IoT environment of the smart camera case study at the IoT device level

Component (C)	Expected Artifact (EA)	Expected Threat (ET)	Consequences of the Expected Threats (breaches of 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 - SD card	EA2: Valuable information on the SD card such as videos, images, and other information	ET2: Unauthorized access to the camera SD card	Tampering with the camera via SD card 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 [94].
- C2: The external memory, the camera has local storage (SD card) of up to 128 GB which is inserted into the camera, and it provides 1080p definition video. The camera features were explored online via its official website [94][94]. The camera features are concluded in Table 4.2.

Table 4.2 Detail Information about the Smart Camera Collected from the Internet

Camera Name	Pan/Tilt Home Security Wi-Fi Camera
Camera model	Tapo C200
The manufacture	TpLink 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)
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/

In this case, the expected artifacts (EA) are the internal storage (EA1) and the external storage (EA2) which may contain valuable artifacts to be submitted to the court including videos, images, camera credentials, the status of the camera, and other information.

The main expected threats (ET) by attackers to exploit the camera device are the following:

- ET1: Unauthorized access to the camera physically, the attacker can tamper with the camera physically by deleting its content and hiding the evidence, he can also change the camera status by making the camera OFF/ON, and /or resetting the camera.
- ET2: Unauthorized access to the camera's external storage, the attacker can remove the external storage and explore or edit its content.

The consequences of the expected threats:

- The attacker can breaches availability by changing the camera status by making the camera OFF/ON.
- The attacker can breach confidentiality by unauthorized access to the camera credentials (username, password).
- The attacker can breach privacy by unauthorized access to the camera's personal information (recorded images, recorded videos).
- The attacker can breach the integrity by tampering with the data and personal information (recorded images, recorded videos).

4.2.3 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. Also, the search warrant, laws, policies, and privacy issues should be explored in this phase. In this case, the camera is investigated at the device level. The tools used in this experiment are stated in Table 4.3, at the device level, the FTK imager tool could be used for image internal or external memory, the Autopsy tool could be used for analyzing the extracted images, in addition, the SD card adapter could be used to transfer data between the SD card

and the investigation workstation. A USB cable or any other type of cable was not needed as the camera doesn't have any port for connection to the workstation. Figure 4.3 clarifies the structure used in the experiment to investigate the smart camera at the device level.

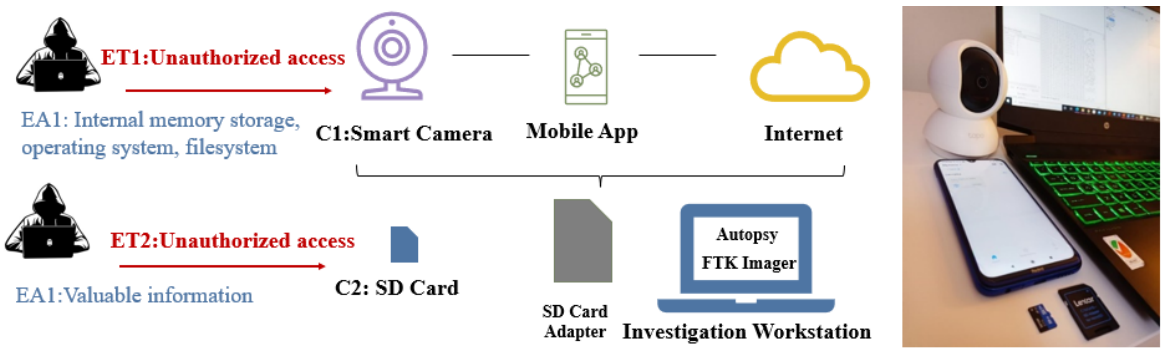

Figure 4.3. The structure used in the experiment to investigate the smart camera at the device level.

Table 4.3. 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
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

First, the mobile App that related to the Tapo camera was downloaded on the mobile and connected to the smart camera. A new user account was created. See Figure 4.4 (a). A new SD card was formatted FAT32 and inserted into the camera, then, the SD card was formatted again by the camera mobile app, according to the camera instruction, the SD card should be formatted using the mobile app for the first usage from App > camera settings > microSD card > format. The camera app has many features that enable users to control the camera. See Figure 4.4 (b), (c), and (d).

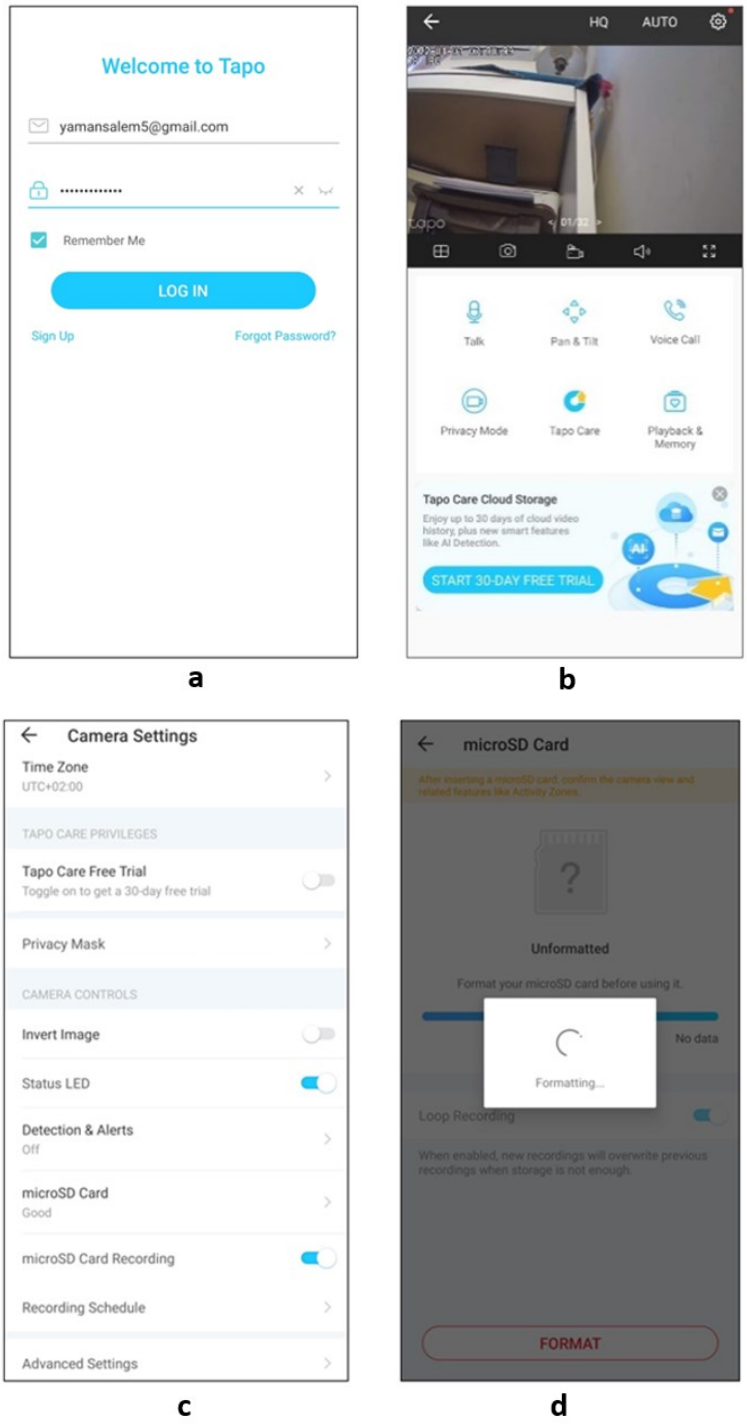

Figure 4.4. Log in to the App; (b) Main Interface; (c) Camera Settings; (d) Format SD card via App.

4.2.4 Phase 4: Acquisition & Preservation/ Documentation

To investigate the smart camera, and collect data generated from the smart camera at the device level, several scenarios that might be happened were conducted by the researcher, the scenarios are clarified in Table 4.4. In the first scenario, a new SD card with a FAT32 file system was formatted and imaged using the FTK imager, in the second scenario, the smart camera was ON for five minutes in the idle mode, then, the camera was plugged off and the SD card was imaged again using the FTK imager. In the third scenario, the smart camera was ON for another five minutes, two images were captured, and two minutes of video were captured. In the fourth scenario, the SD card was formatted and imaged again. Finally, in the fifth scenario, the SD card was inserted into the camera and put on privacy mode. Then, the SD card was imaged again. All images obtained from the mentioned scenarios were backed up to preserve their integrity and uploaded into Autopsy for analysis and clarified in Table 4.4.

Table 4.4. Scenarios are conducted on the smart camera at the device level.

Scenarios	User Role (actions)	Investigator Role	Camera Operation Time	Image time	SD- card image name	Comments
First Scenario	A new SD card with a FAT32 file system was formatted	SD-card was imaged using the FTK imager tool	Format	0:21:42	EmptyImage1.E01	There are no files as the SD card is empty
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	5 min (Idle mode)	0:21:48	After5minON.E01	Camera settings: MicroSD card recording (ON) The camera recorded a 20-sec video for the first usage
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	5 min (Capture video and images)	0:21:23	Second5minON.E01	settings: MicroSD card recording (ON)
Fourth Scenario	The SD card was formatted	The SD card was imaged again using the FTK imager tool	Format	0:20:25	Format2.E01	

Fifth Scenario	The SD card was inserted into the camera and put on privacy mode.	the SD card was imaged again	10 min (Privacy mode)	0:18:49	Privacymode10Min.E01	Camera settings: MicroSD card recording (ON), privacy mode (ON)

4.2.5 Phase 5: Examining & Analyzing/ Documentation

First, the operating system is explored, and second, the external memory file system was analyzed. See Figure 4.5. Thus, this section aims to analyze the operating system and analyze the FAT32 file system of all external memory images of the smart camera that were collected through a set of mentioned previous scenarios in Table 4.4/ section 4.2.4.

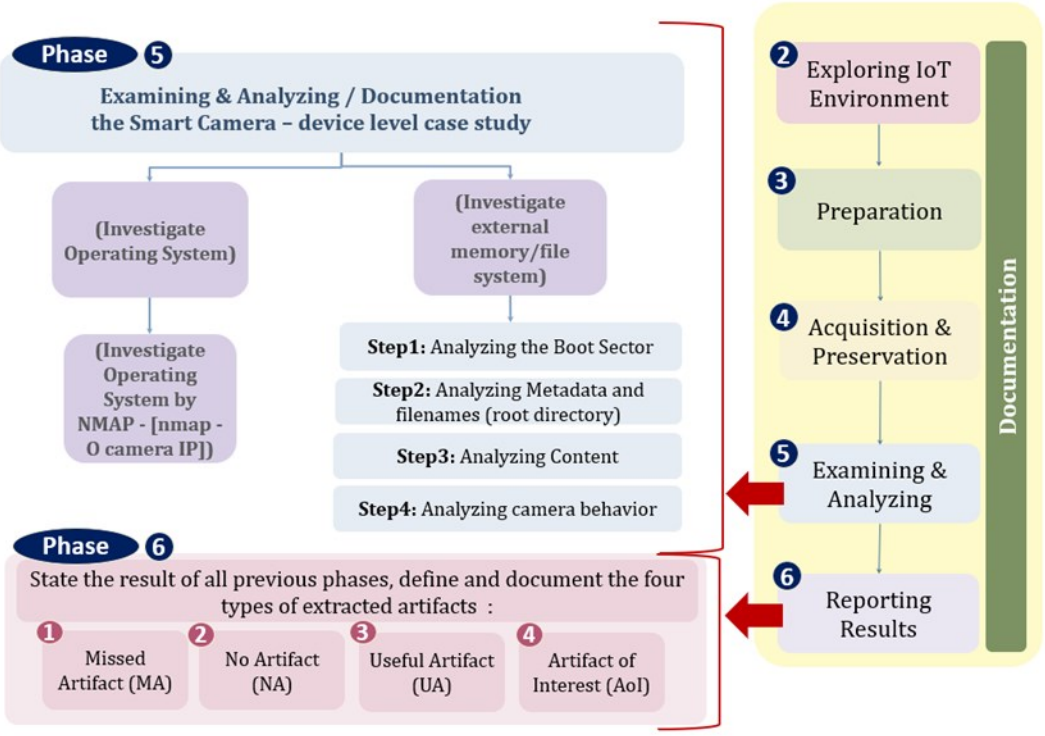

Figure 4.5. Examining & Analyzing / Documentation phase for the smart camera at the device level.

4.2.5.1 Examining and analyzing operating system/ Documentation

The smart camera doesn't have a USB port or any other ports for data collection or for connecting to the workstation, according to the MAoIDFF-IoT framework, if the IoT device doesn't have any port for connection to the workstation, it is possible to use other

tools for investigating the internal of the IoT device, thus, in this case, to check and explore the operating system of the smart camera, the NMAP tool over Kali Linux was used as an attempt to find any artifact related to the OS, a command [nmap -O camera IP] was used, the result showed that this camera has an unknown OS as illustrated in Figure 4.6.

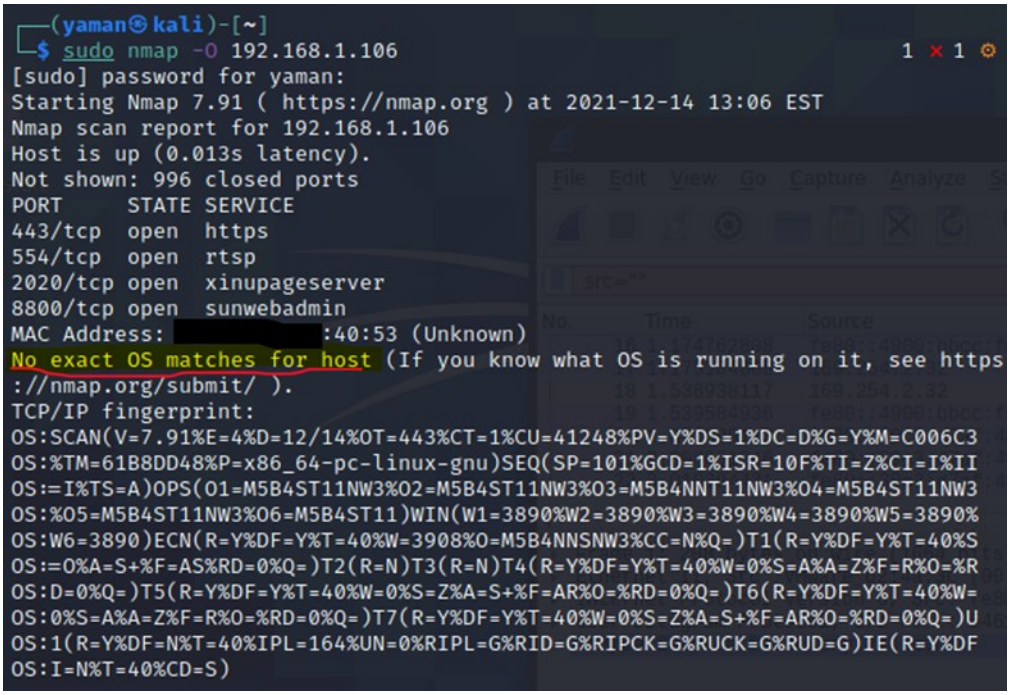

Figure 4.6. Checking the operating system of the smart camera using the NMAP tool.

4.2.5.2 Examining and analyzing the file system

In this experiment, the FAT32 file system on the external memory was analyzed, and all images of the external memory acquired in the previous phase (section 4.2.4) were loaded into the Autopsy tool for the analysis process. External memory has a FAT32 file system.

The FAT file system has three physical areas; (1) the reserved area, (2) the FAT area, and (3) the data area. See Figure 4.7. The reserved area contains the boot sector which describes information about the file system, this area has one sector in FAT12 and FAT16 while it has many sectors in FAT32. 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 [86]. In FAT12/16 root directory locates at the beginning of the data area, while the root directory in FAT32 can be anywhere in the data area. The address of the root directory in FAT32 is determined in the boot sector [86].

To define the artifact location in the FAT32 SD card, the investigator should be aware of the physical structure of the FAT32 file system. Figure 4.7 clarifies the physical structure of the FAT file system.

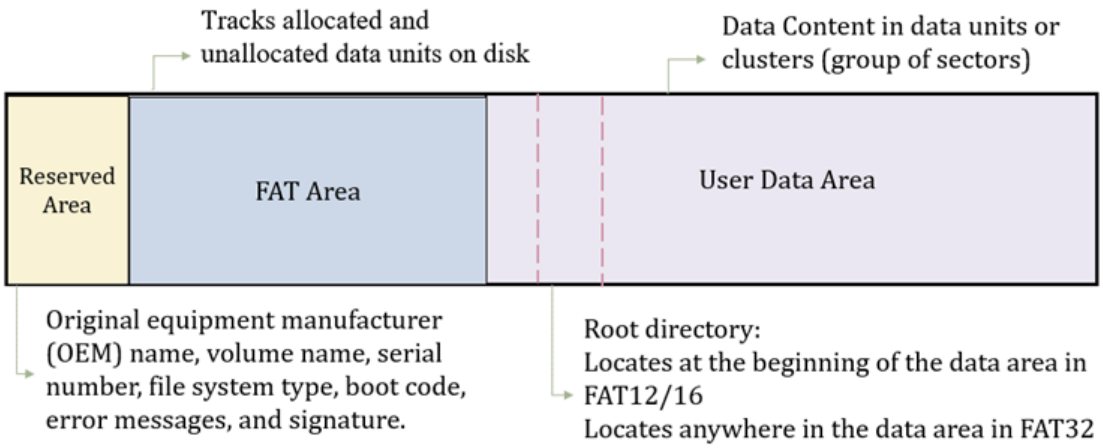

Figure 4.7. The Physical Structure of the FAT File System [86].

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 [86] was taken into the consideration, Brain Carrier suggested a model for analyzing any file system based on five categories, including filesystem, content, metadata, file name, and application. Thus, 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 (Analyze 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. Figure 4.8 shows a capture from Autopsy which clarifies the boot sector in FAT32 which is located in the first 215 bytes of the image. 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 [86]. All information was extracted and explored for all SD card images. According to encoding tables, Table 6.1, and Table 6.2, the information was extracted and clarified in Figure 4.8. SD card volume size can be calculated as follows: Volume size = Number of sectors (byte 32-35 in boot sector) * sector size (byte 11-12 in boot sector), volume size = 61952000*512 = 30.25 GB

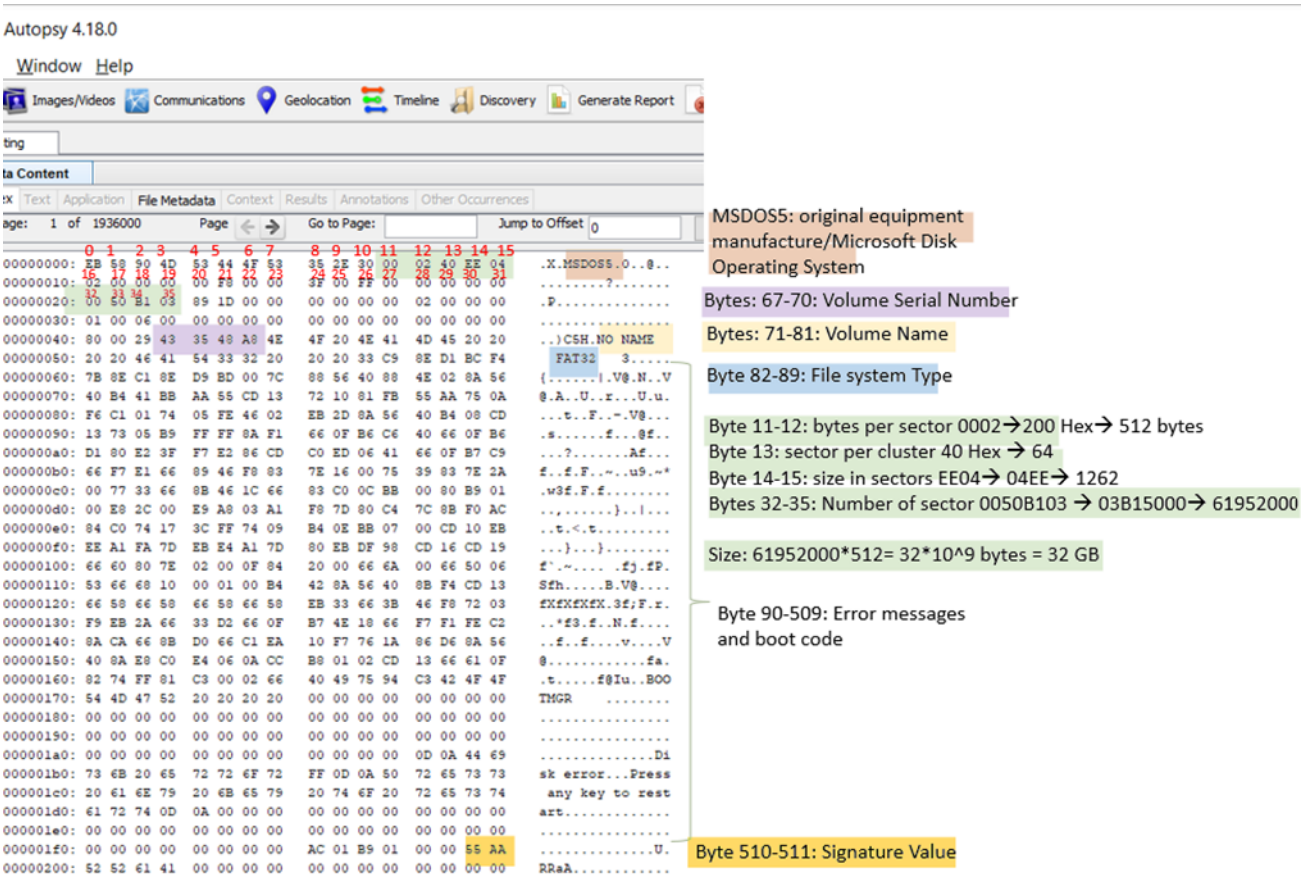

Figure 4.8. Boot sector for FAT32 from SD card image of the smart camera.

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 [86]. 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. Figure 4.9 shows a screenshot from the "After5minON.E01" image that clarifies the file name and metadata in the root directory for one of the selected files. Each file in the FAT32 file system directory has a long file entry and a basic file entry that contains a file name, file size, and MAC

(modify/access/created) times and dates. Figure 4.10 clarifies all data extracted according to the encoding tables (Table 6.3, Table 6.4, and Table 6.5).

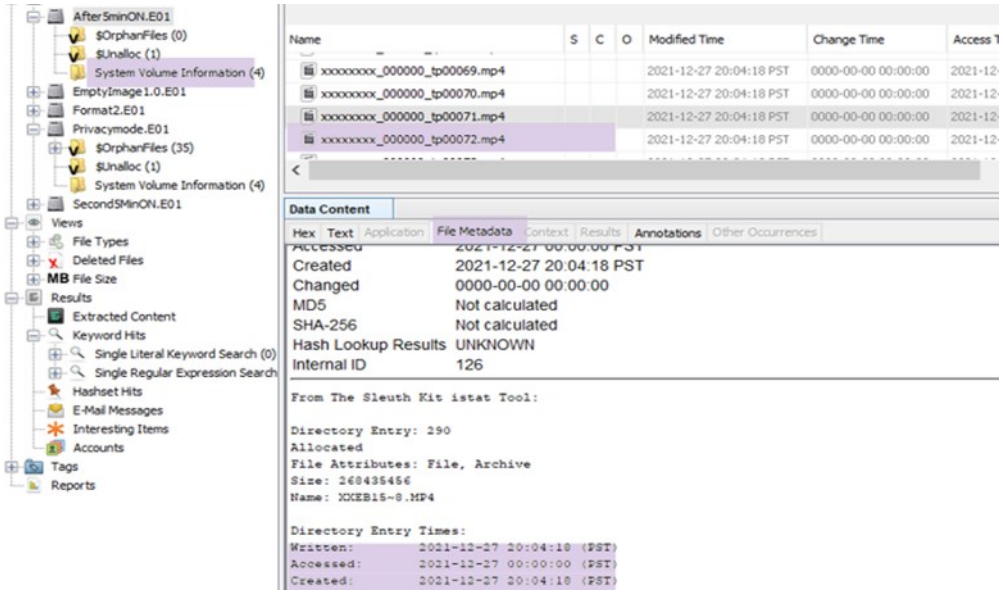

Figure 4.9. a screenshot from the "After5minON.E01" image clarifies metadata for one file in the root directory.

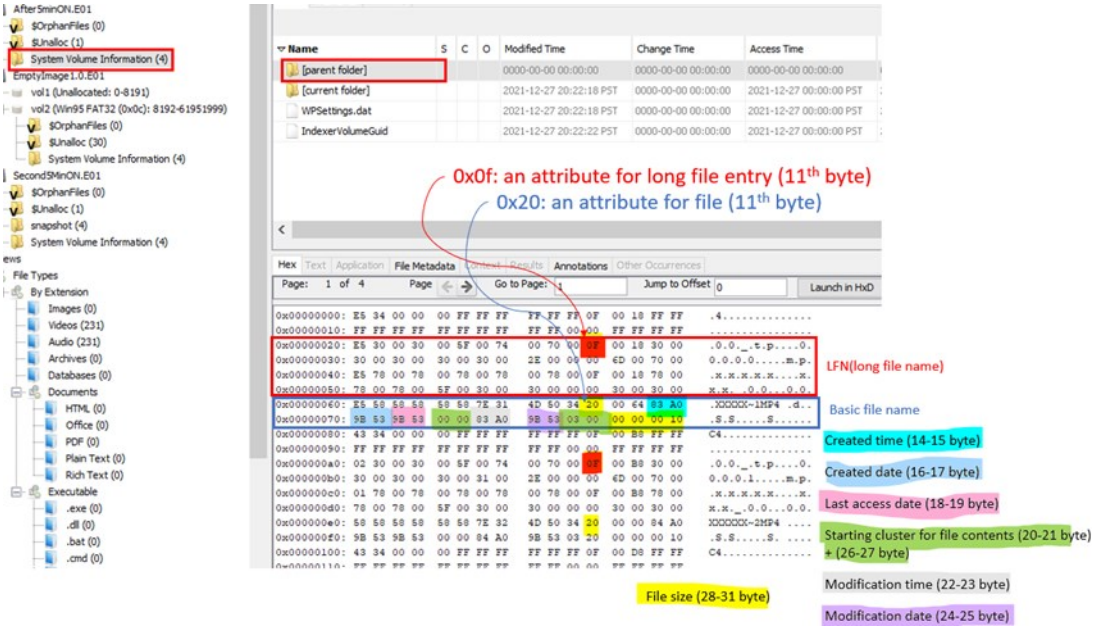

Figure 4.10. a screenshot from the "After5minON.E01" image clarifies all data extracted according to the encoding tables such as long and basic file names and MAC dates.

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, Figure 4.11 shows the content for a video accessed from the "Second5MinON.E01" image.

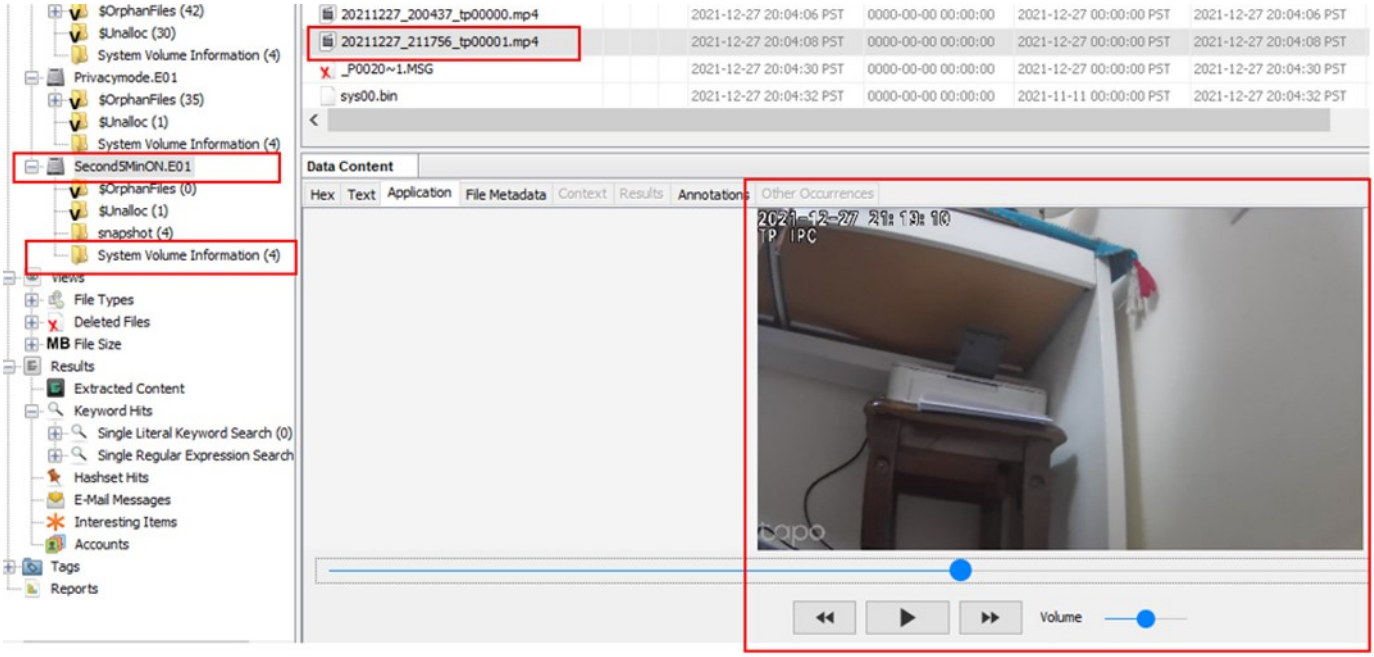

Figure 4.11. Access content from the root directory of the "Second5MinON.E01" image.

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

During the investigation, the camera's behavior was recognized. For the first usage of a smart 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. This recorded video was recognized. 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.

A good feature of the Autopsy is that it creates a timeline for file activity. The timeline for file activity in Autopsy was analyzed for all SD card images which helped in analyzing the

activities conducted on the camera Figure 4.12 shows a screenshot for a timeline for a file activity in Autopsy.

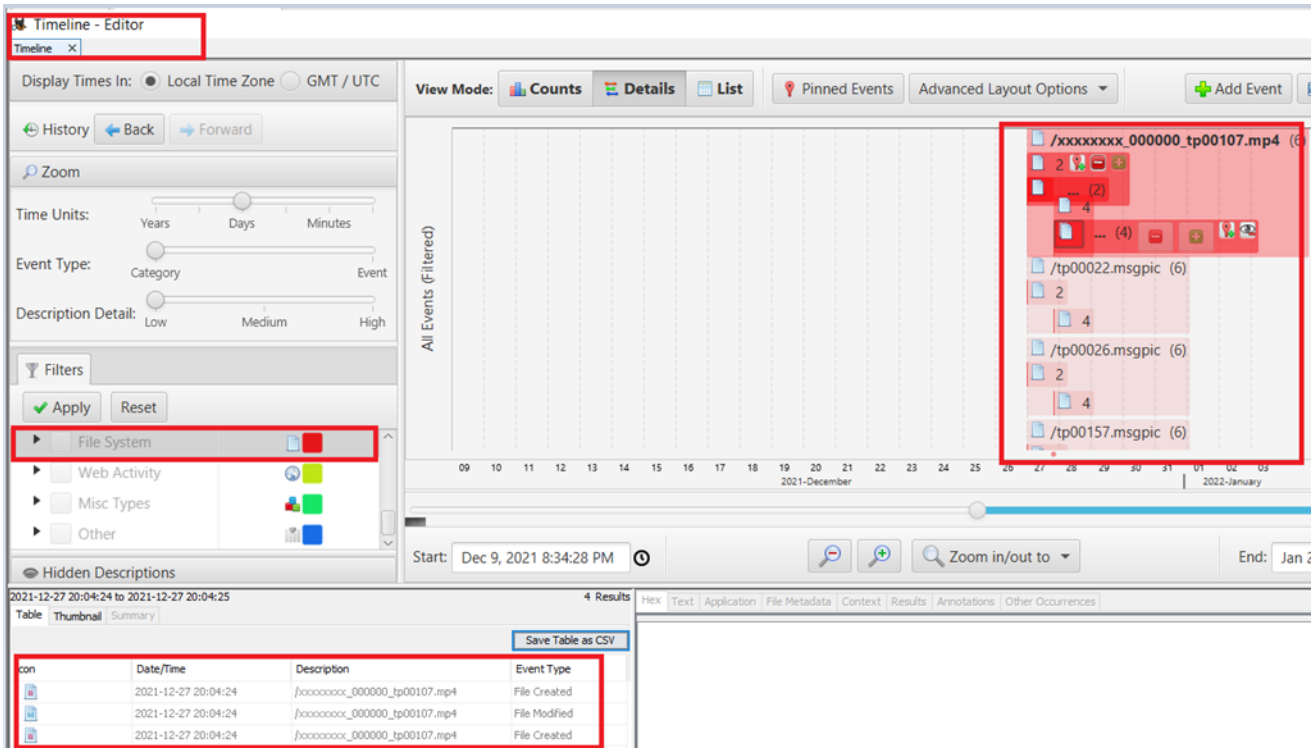

Figure 4.12. A timeline for file activity in Autopsy.

4.2.6 Phase 6: Reporting the Results / Documentation

The smart camera was connected to the mobile App, 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 Figure 4.13.

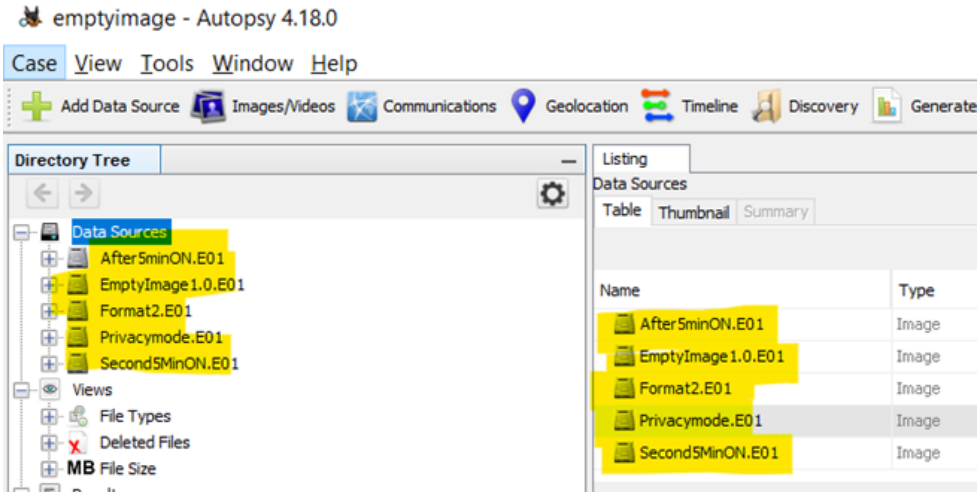

Figure 4.13. All SD-card images of the smart camera were collected through a set of mentioned scenarios.

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 according to the proposed framework (MAoIDFF – IoT) which are: missed artifact (MA), no artifact (NA), useful artifact (UA), and artifact of interest (AoI). Autopsy extracted all files automatically and recovered all deleted and overwritten files. All videos captured via a smart camera were found on the SD card which is considered an artifact of interest (AoI). While the captured images were not found which are considered missed artifacts (MA). In addition, all related metadata files were obtained which are considered useful artifacts (UA). Further, the camera OS was checked using the Nmap tool, the result showed that there were no exact operating system matches for the camera which is a useful artifact (UA). The following Table 4.5 concludes the artifact types according to the conducted scenarios.

Table 4.5. The artifacts types according to the conducted scenarios on the smart camera

Scenarios	User Role (actions)	Investigator Role	SD- card image name	Type of Artifact (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),	the SD card was imaged again using the FTK	After5minON.E01	The camera recorded a 20-sec video for the first usage, this video was found **(Artifact of**

	Then, the camera was plugged off	imager tool		**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 a useful artifact (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 time. This recorded video was recognized from the "After5minON.E01" image after putting the camera on idle mode for the first five minutes, this video is considered an Artifact of Interest (AoI). See Figure 4.14 which clarifies the first twenty-second of the video from the "After5minON.E01" image.

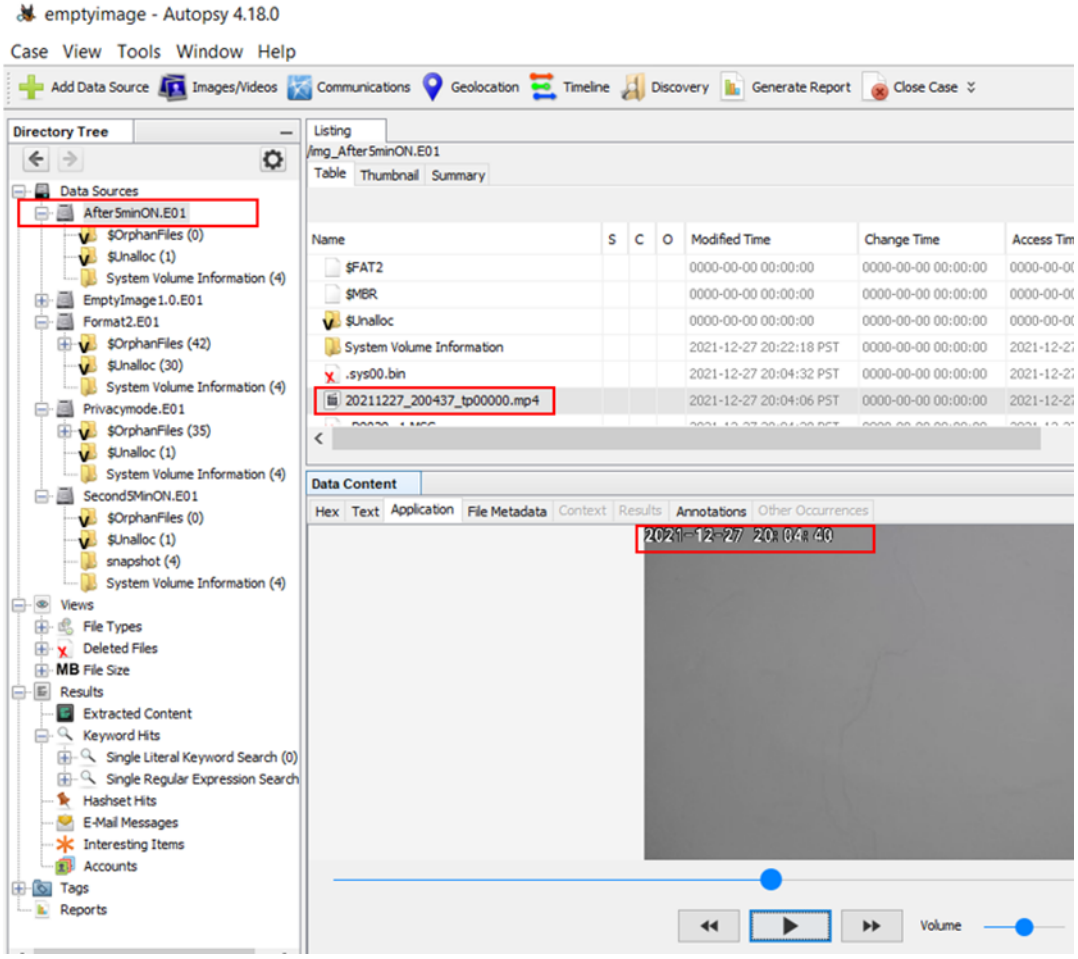

Figure 4.14. The first twenty seconds of the video from “After5minON.E01”.

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 is in usage this is considered as a useful artifact (UA). This result was obtained after putting the camera ON for another five minutes in the third scenario and analyzing the “second5MinON.E01” image. See Figure 4.15 which shows a screenshot of the overwritten files obtained from the third scenario. 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 Artifact of Interest (AoI). See Figure 4.16 which shows a screenshot of an unallocated file that was recovered from “Format2.E01”.

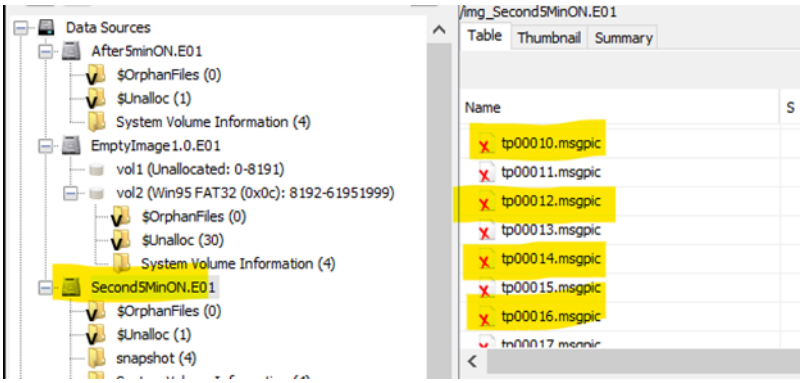

Figure 4.15. Overwritten files on the SD card were cleared in the "second5MinON.E01" image.

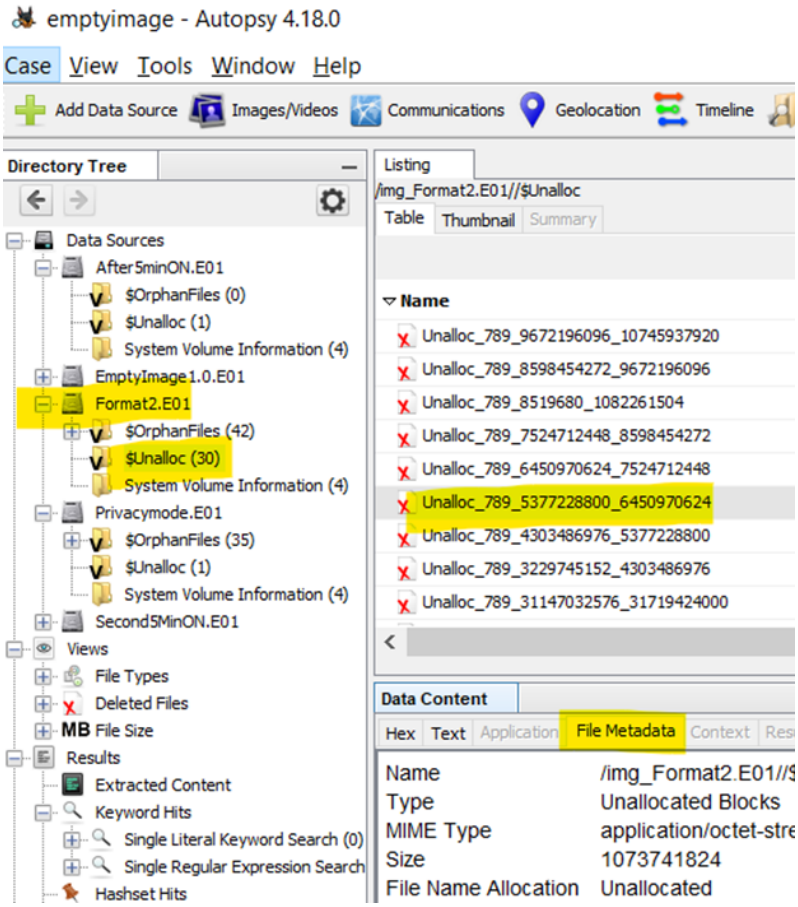

Figure 4.16. Unallocated files recovered from "Format2.E01".

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. See Figure 4.17 which shows a captured screenshot from

the “Privacymode10Min.E01” image clarifies that the camera doesn't record anything in privacy mode, this is considered a useful artifact (UA). However, it records on the SD card when the user clicks the button of capturing via mobile App. All videos recorded were found in the “Second5minON.E01” image while the recorded images were not found. Figure 4.18 shows recovered recorded videos found in the “Second5minON.E01” image.

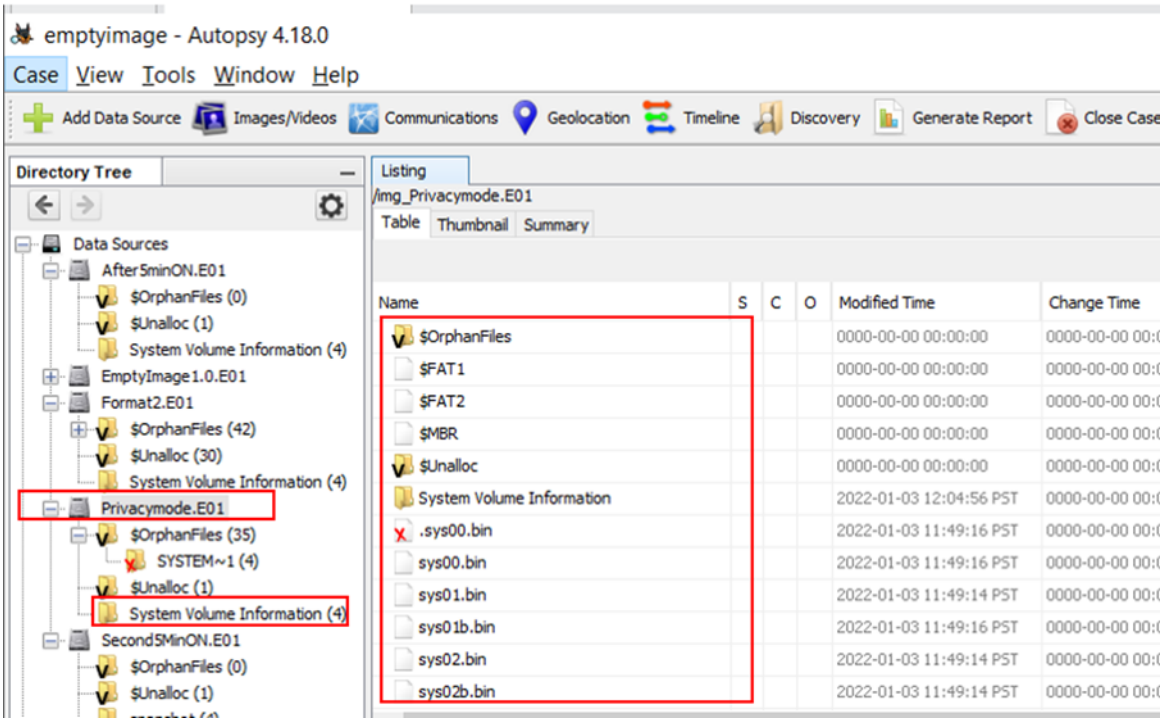

Figure 4.17. Captured screenshot from the “Privacymode10Min.E01” image clarifies that the camera doesn't record anything in privacy mode.

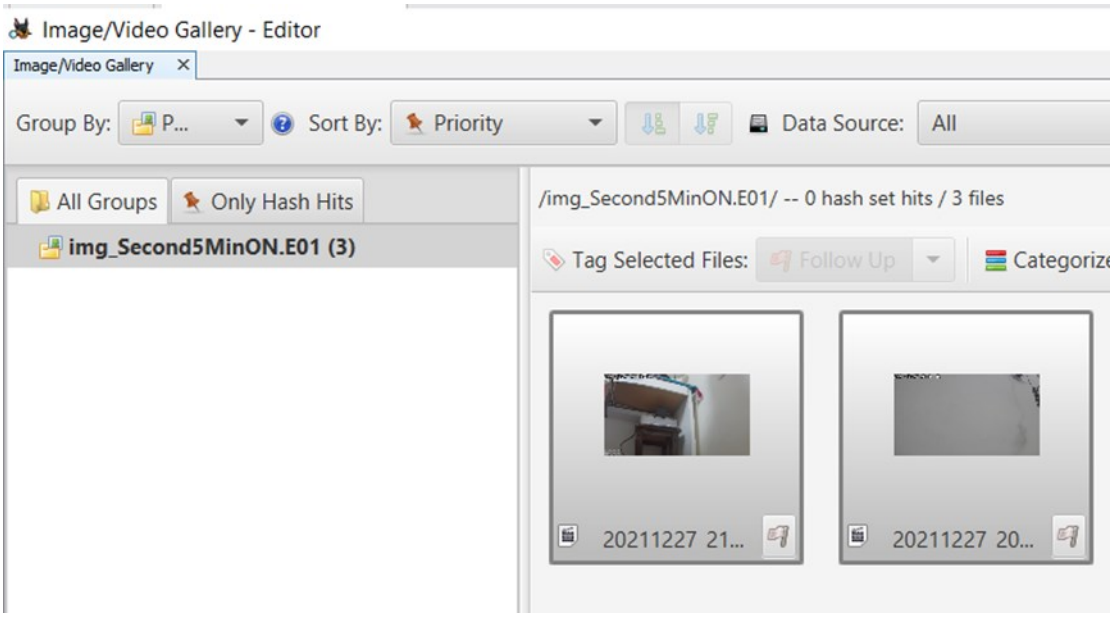

Figure 4.18. Recovered recorded videos found in the "Second5minON.E01" image.

According to (MAoIDFF – IoT) framework, that documentation is a continuous activity required in all investigation phases for preserving the proper chain of custody. Hence, in this case, all previous phases were recorded and explained, and then the results from all previous phases were presented in the last phase, which is the reporting phase, with the related screenshots that clarify the investigation process to be submitted to the court. In addition, the date and time for each action, 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 were taken during the investigations, and details of analyzing evidence should be logged in the report [89]. Proper documentation is important to help in reviewing the crime case anytime [45]. Table 4.6 clarifies the expert witness report structure for the smart camera case study according to the MAoIDFF – IoT framework.

Table 4.6. The expert witness report structure for the smart camera case study according to the MAoIDFF – IoT framework

First Page	• Report name: Expert witness report: A Smart Camera investigation at the device level. • Investigator name: Eng. Yaman Salem

	• Submitted to IoT digital investigation research public
Second Page	• Investigator detailed paragraph (Name, its experience briefly, city and country) o Eng Yaman Salem, BSc. Telecom. Engineer, Info. Security Consultant. o Certified in Linux, Network+, CCNA Security, CPTE, CIHE, o Master's degree in CyberCrime and digital forensics o Ramallah Palestine • Case details paragraph (This includes the offense name, case name, case number, the tools used, date of request, date of conclusion, and date of the published report.) • Result paragraph, This includes the offense name, offense name, suspect names, the related cybercrime law, and artifacts of interest (AoI) as follows o A recorded video (2 min) was found o Unlocated and deleted files were found o The camera recorded a 20-sec video for the first usage, this video was found
Third page	Document Contents.
Fourth page	Introduction, an overview of the case (section 4.2).
The rest of the report (Stated in the previous subsections)	Includes the six phases of the proposed framework (MAoIDFF-IoT): • Phase 1: Define the AoI based on the Level/ Documentation (section 4.2.1) • Phase 2: Exploring the IoT environment/ Documentation (section 4.2.2) • Phase 3: Preparation/ Documentation (section 4.2.3) • Phase 4: Acquisition & preservation/ Documentation (section 4.2.4) • Phase 5: Examining & Analyzing/ Documentation (section 4.2.5) • Phase 6: Reporting the result/ Documentation (section 4.2.6)
	Guidelines, recommendations, and additional notes to facilitate the process for other investigators in the future
Appendix	Any other screenshots, images, and documents should be stated in the appendix. (Table 6.1, Table 6.2, Table 6.3, Table 6.4, and Table 6.5).

4.2.7 Recommendations and Notes

Smart Cameras are widely used to monitor different environments. This case focused on investigating Tapo smart camera according to the proposed framework (MAoIDFF-IoT) to

extract artifacts at the device level. All proposed phases were applied easily. Thus, the MAoIDFF-IoT framework facilitates the investigation mission and guides digital investigators with similar future cases.

IoT devices have different filesystems and operating systems. FAT32 was analyzed in detail in this case while the operating system was unknown. Thus it is an excellent step to explore more about IoT filesystems and OS investigation. Reading about IoT devices' brands via the web and user reviews will help the investigation process. In this case, the investigation was at the device level. The captured images were not found in this case, while they were found in the following case in section 4.3, which stated the investigation of the smart camera at the mobile level. This indicated the effectiveness of the multilevel investigation proposed in the MAoIDFF-IoT framework. If some of the artifacts were missed at a level they can be caught at another level.

4.3 Smart Camera at Application Level Case Study

In this case study, the Tapo smart camera at the application level was explored and investigated. The following sub-sections clarify the phases applied in the experiment according to the MAoIDFF-IoT framework.

4.3.1 Phase one: Define the Artifact of Interest (AoI) from Which Level/ Documentation.

In this phase, the application level was chosen to be investigated. According to the MAoIDFF-IoT framework, Figure 3.2 in the previous chapter, the application level includes a mobile, web interface, and cloud investigation. The examiner focused on the mobile investigation at the application level, as the mobile app controls the camera via Wi-Fi. Web interface and cloud investigation were excluded as they are not connected to the camera. The device investigation level was conducted and documented in (section 4.2).

4.3.2 Phase two: Exploring the IoT Environment/ Documentation

After defining the investigation level, which is the application level, 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 threads to understand the IoT environment. Table 4.7 clarify the component in this phase. In this case study, the researcher focused on mobile-level investigation, thus the mobile app component 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 4.2), Table 4.2.

Table 4.7. 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.

4.3.3 Phase 3: Preparation/ Documentation

In this phase, the investigator should prepare the investigation workstation and the appropriate investigation 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 4.10 clarifies the tools used in the investigation.

Table 4.8. 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

4.3.4 Phase 4: Acquisition & Preservation/ Documentation

To investigate the smart camera and collect data generated from the camera at the mobile level, the researcher conducted several scenarios that might be happened, which is clarified in Table 4.9.

4.3.5 Phase 5: Examining & Analyzing/ Documentation

In this phase, the researcher examined and analyzed the Tapo mobile app connected to the camera. According to the MAoIDFF-IoT framework, at the mobile investigation level, analyzing and examining gathered data from IoT devices could happen manually via a mobile app connected to the IoT devices or via forensics tools that can take logical or physical mobile images. The researcher used the manual acquisition method to investigate the camera device via mobile device. In addition to the logical acquisition method by the Belkasoft Evidence Center tool. The results from this phase are clarified in Table 4.9.

The logical acquisition method was conducted for the mobile by the Belkasoft Evidence Center tool, the logical image was analyzed and the data the related smart camera data was found in the path: filesystem > android > data > com.tplink.iot > files > memory. All captured videos and images were found. Figure 4.19 clarifies the extracted camera artifacts from the logical mobile image by Belkasoft Evidence Center.

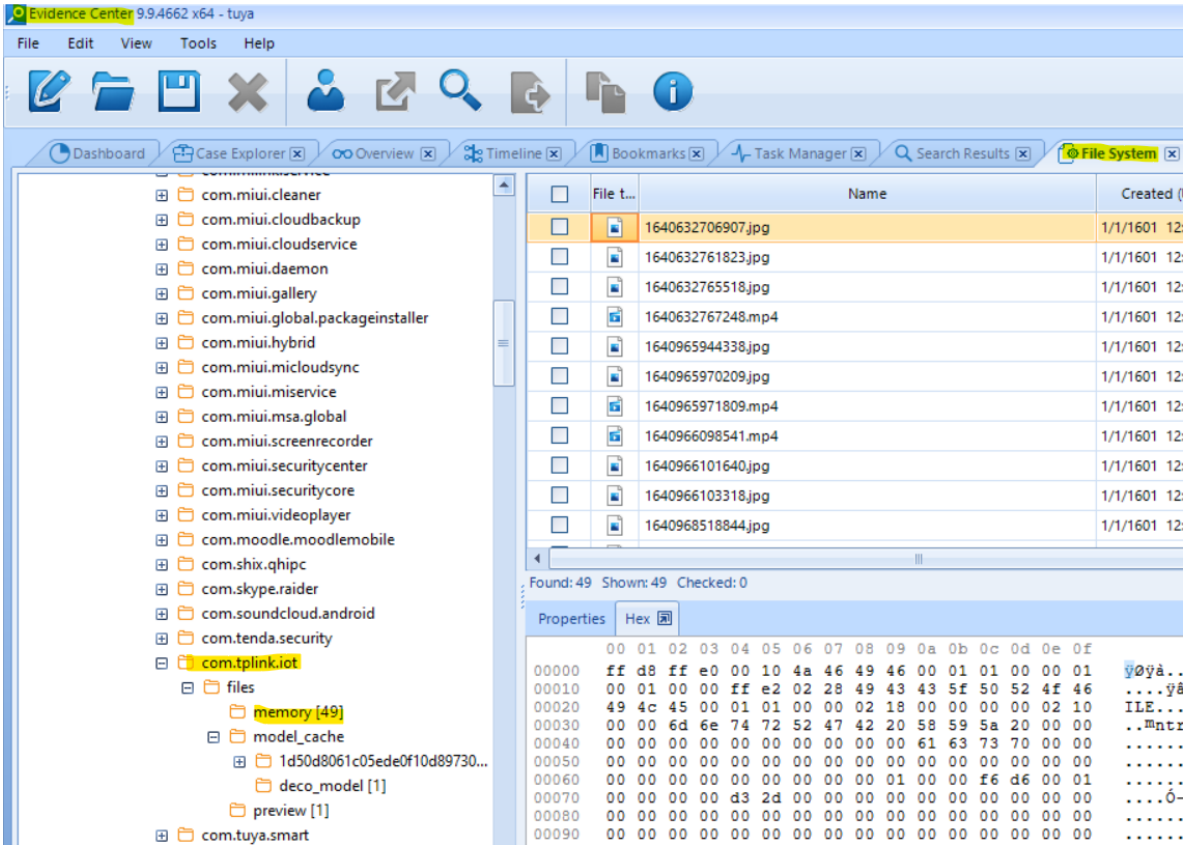

Figure 4.19. the extracted camera artifacts from the logical mobile image by Belkasoft Evidence Center

The mobile device was explored in the manual acquisition method, and the Tapo app was viewed manually. From the IoT mobile app, the investigator was able to access the recorded images and videos, and he knew the camera status, 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. Figure 4.20 clarifies artifacts that were extracted manually such as camera settings, log data, and camera features.

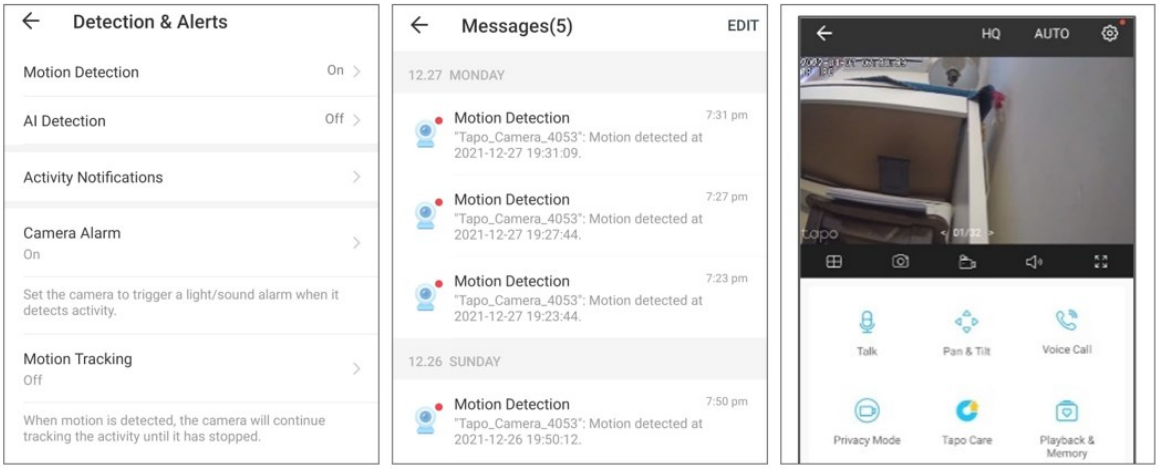

Figure 4.20. (a) Camera settings; (b) Log data; (c) Camera features

4.3.6 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. According to (MAoIDFF – IoT) framework, documentation is a continuous activity required in all investigation phases. Thus, in this case, all previous phases were recorded and explained. In the reporting phase, the type of artifacts for each scenario was documented and clarified in Table 4.9. Finally, the expert witness report should be documented, and the structure for the report according to the MAoIDFF – IoT framework was described in section 4.2, Table 4.6.

Table 4.9. Scenarios are conducted on the smart camera at the mobile level.

Scenarios	User Role (actions)	Investigator Role	Type of Artifact (AoI, MA, UA, NA)
Scenarios on Wi-Fi 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).
	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	All captured images and videos were found via manual and logical
	Then the camera was	The output at the mobile App	

	plugged off	via manual acquisition: camera status is OFF	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)

4.3.7 Recommendations and Notes

This case proved the effectiveness of the investigation at multilevel that proposed by the MAoIDFF-IoT framework, as the images recorded via the smart camera were not found in the SD card at the device level (the first case study in section 4.2), but they were found via manual and logical acquisition at the mobile investigation level, in addition, the mobile level investigation found more information about the camera app via log files.

In this case, the artifacts from the Tapo app were extracted and analyzed by the Belkasoft tool. At the same time, it is possible to use other tools besides Belkasoft to get more artifacts, as the output from each forensic tool may differ. It was easy to find the location of images and videos from the Tapo app. In some cases, finding the location of artifacts might be challenging as each camera has its features, and each IoT app has its behavior in the mobile device. Thus, if the artifacts were not found, it is recommended to conduct reverse engineering for IoT apps as the proposed framework suggested to know where the app stores its data on the mobile and to recognize the IoT app behavior.

Moreover, searching online for the Tapo camera device helped find the device's features, the IoT filesystem, and other helpful information that helped in the investigation. All proposed phases were applied. Thus, the MAoIDFF-IoT framework facilitates the investigation mission and guides digital investigators who have similar cases in the future.

4.4 Smart Environment Case Study

In this case study, seven smart IoT devices were involved in the IoT environment, the smart devices include 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 Wi-Fi smart led bulb.

The following sections clarify the phases applied in the experiment according to the MAoIDFF-IoT framework. The framework has six main phases: (1) defining the AoI according to the level/ documentation, (2) exploring the IoT environment/ documentation, (3) preparation/ documentation, (4) acquisition & preservation/ documentation, (5) examining & analyzing/ documentation, (6) reporting/ documentation.

4.4.1 Phase one: Define the Artifact of Interest (AoI) from Which Level/ Documentation.

This phase includes defining the artifact of interest by choosing which level to investigate. The IoT application level was chosen to be investigated in this case study. The examiner focused on the mobile investigation at the application level, as the mobile app controls all the IoT devices via Wi-Fi. According to the MAoIDFF-IoT framework, Figure 3.2 in the previous chapter, cloud investigation was excluded as the cloud is not connected to these devices. In addition, the network investigation level was excluded as none of the IoT devices is sending streaming data via the network. The investigation excluded the device level, as none of these IoT devices had any internal or external memory or operating system. Thus, this experiment focused on investigating IoT devices at the application level, particularly mobile app investigation.

4.4.2 Phase two: Exploring the IoT Environment/ Documentation

After defining the investigation level, which is the mobile level, 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 threads to understand the IoT environment. Figure 4.21 clarifies the general architecture of the IoT smart environment case study. Table 4.10 concludes this phase.

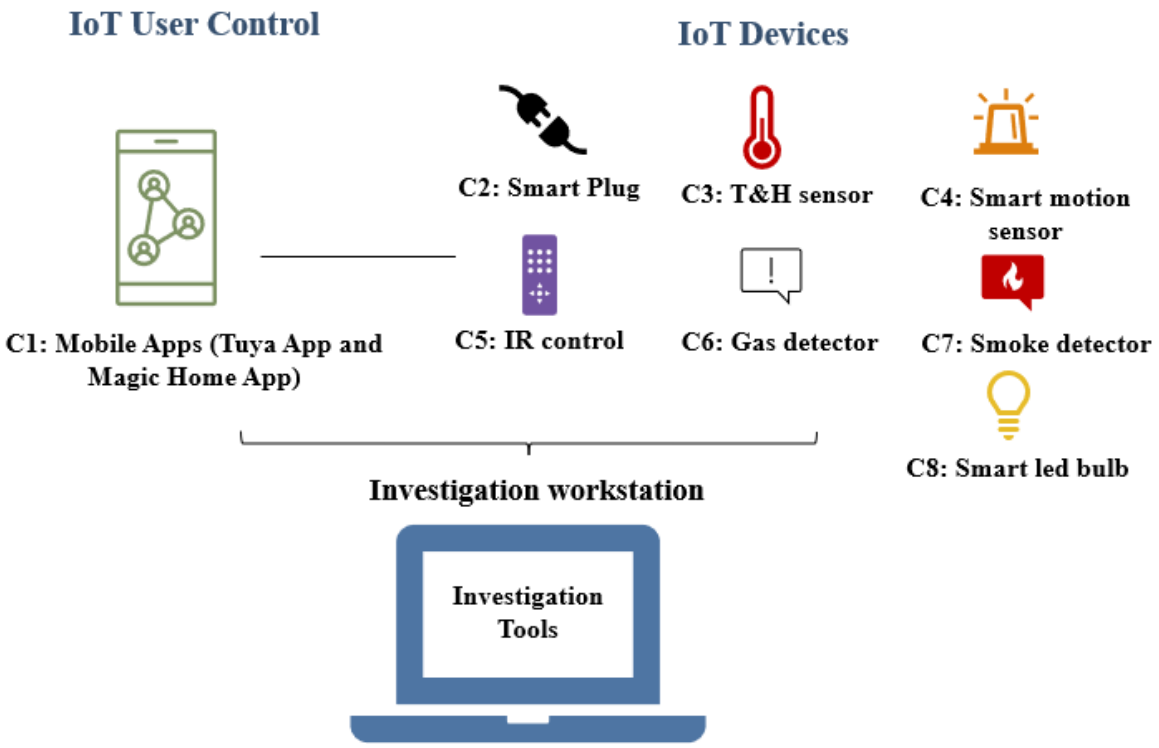

Figure 4.21. General Architecture of IoT smart environment case study

Table 4.10. Explore the IoT devices of the smart environment case study.

Component (C)	Expected Artifact (EA)	Expected Threat (ET)	Consequences of the Expected Threats
C1: Mobile Device/ Mobile IoT App	EA1: Screenshots from mobile apps, information in logs files that connected with the IoT app	ET1: Unauthorized access to the IoT App	Tampering with the IoT devices via the mobile app also, extracting personal information, editing the mobile app This breaches confidentiality, integrity, availability & privacy.
C2: Wi-Fi 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: Wi-Fi temperature & humidity sensor	EA3: Logs files indicating device operating time and other relevant information.	ET3: 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.

C4: Wi-Fi smart motion sensor	EA4: Logs files indicating device operating time and other relevant information.	ET4: 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.
C5: Wi-Fi Remote control	EA5: Logs files indicating device operating time and other relevant information.	ET5: 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.
C6: Wi-Fi smart gas detector	EA6: Logs files indicating device operating time and other relevant information.	ET6: 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.
C7: Wi-Fi smart smoke detector	EA7: Logs files indicating device operating time and other relevant information.	ET7: 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.
C8: Wi-Fi smart led bulb	EA8: Logs files indicating device operating time and other relevant information.	ET8: 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.

In this case, the main components are the mobile App and the smart devices, which 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. 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 4.11 concludes the information about the IoT devices collected from the internet.

Table 4.11. Information about the IoT devices

IoT device	Brand	Application level	Devices Features
Wi-Fi smart plug	Elivco	✓ (Tuya Mobile App)	Wi-Fi connection, App control, energy monitoring, voice control
Wi-Fi smart	Unknown	✓ (Tuya	Wi-Fi connection, App control, message

Temperature & Humidity Sensor		Mobile App)	notifications, alarm
Wi-Fi smart motion sensor	Unknown	✓ (Tuya Mobile App)	Wi-Fi connection, App control, message notifications, log events page
Wi-Fi Universal Remote control	Unknown	✓ (Tuya Mobile App)	Support multiple home appliances, Wi-Fi connection, App control, voice control
Wi-Fi smart gas detector	Unknown	✓ (Tuya Mobile App)	Wi-Fi connection, App control, On-Site alarm, fault self-checking, log events page
Wi-Fi smart smoke detector	Unknown	✓ (Tuya Mobile App)	Wi-Fi connection, App control, On-Site alarm, easy installation, log events page
Smart led Bulb	Unknown	✓ (magic home – smart home Mobile App)	Wi-Fi connection, App control, timer, bright control

4.4.3 Phase 3: Preparation/ Documentation

In this phase, the investigator should prepare the investigation workstation and the appropriate investigation tools based on the chosen level, which is the mobile level in this case. The tools used in this experiment are stated in Table 4.12. A USB cable was needed to connect the mobile to the workstation. Figure 4.22 clarifies the IoT devices used in the investigation experiment, The mobile App that related to each IoT device was downloaded on the mobile. The connection between the mobile app and the IoT devices was checked.

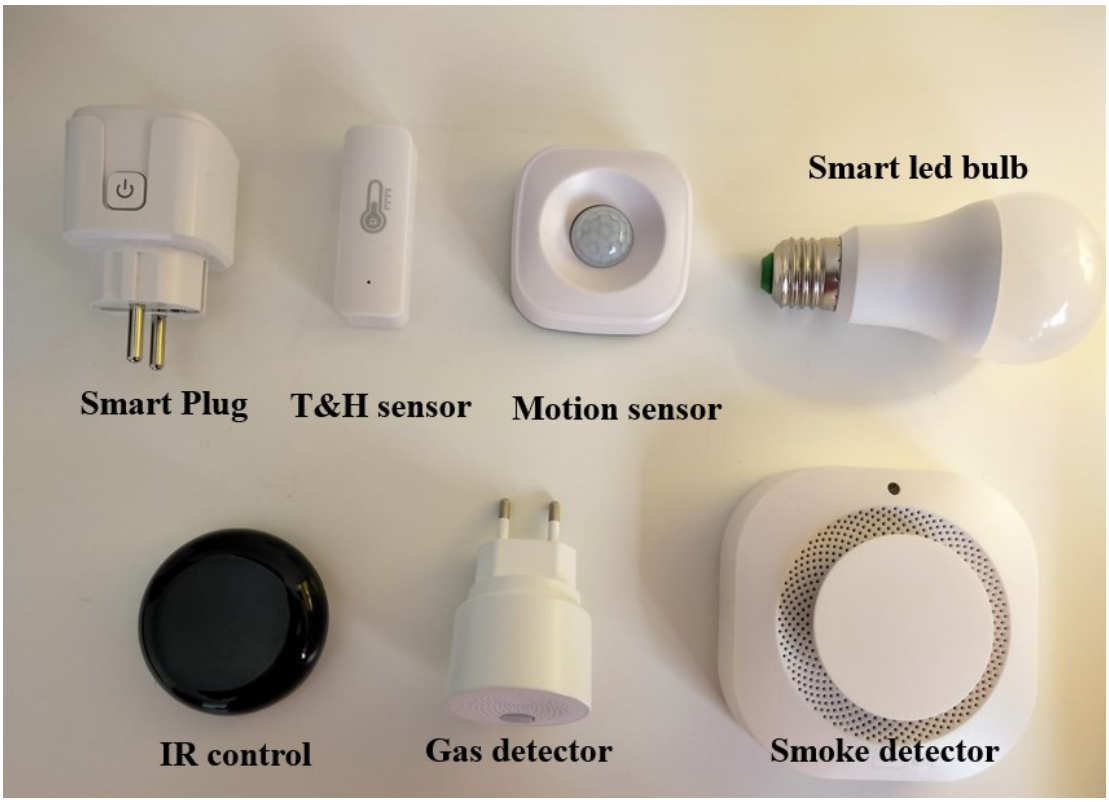

Figure 4.22. The IoT devices used in the investigation experiment

Table 4.12. Tools used in the investigation experiment at the device 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 to connect with the IoT devices
Mobile App	Tuya App and Magic Home App
USB cable	This is used to connect the mobile with the workstation

4.4.4 Phase 4: Acquisition & Preservation/ Documentation

In the experiment, the researcher played the investigator role and the user role at the same time. According to the proposed framework MAoIDFF-IoT, 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 were clarified in Table 4.13.

4.4.5 Phase 5: Examining & Analyzing/ Documentation

In this phase, the researcher examined and analyzed the mobile apps that were connected to IoT devices. According to the MAoIDFF-IoT framework, at the mobile investigation level, analyzing and examining gathered data from IoT devices could happen manually via mobile apps connected to the IoT devices or via forensics tools that can take logical or physical mobile images.

The researcher navigates the IoT apps, Tuya app, and Magic Home app to investigate the IoT devices via the mobile device. Figure 4.23 clarifies artifacts extracted by the manual acquisition method, including IoT devices connected with the Tuya App in Figure 4.23 (a), smart bulb connected with the Magic home app in Figure 4.23 (b,c), the smart switch log page which indicates the status of the switch with the timestamp in Figure 4.23 (d). Motion detection records in Figure 4.23 (e), the smart sensor log page which indicates the temperature and the humidity with the timestamp in Figure 4.23 (f), Smoke detector alarm in Figure 4.24 (a), and gas detector alarm in Figure 4.24 (b). The investigator's roles over the IoT devices are clarified in Table 4.13.

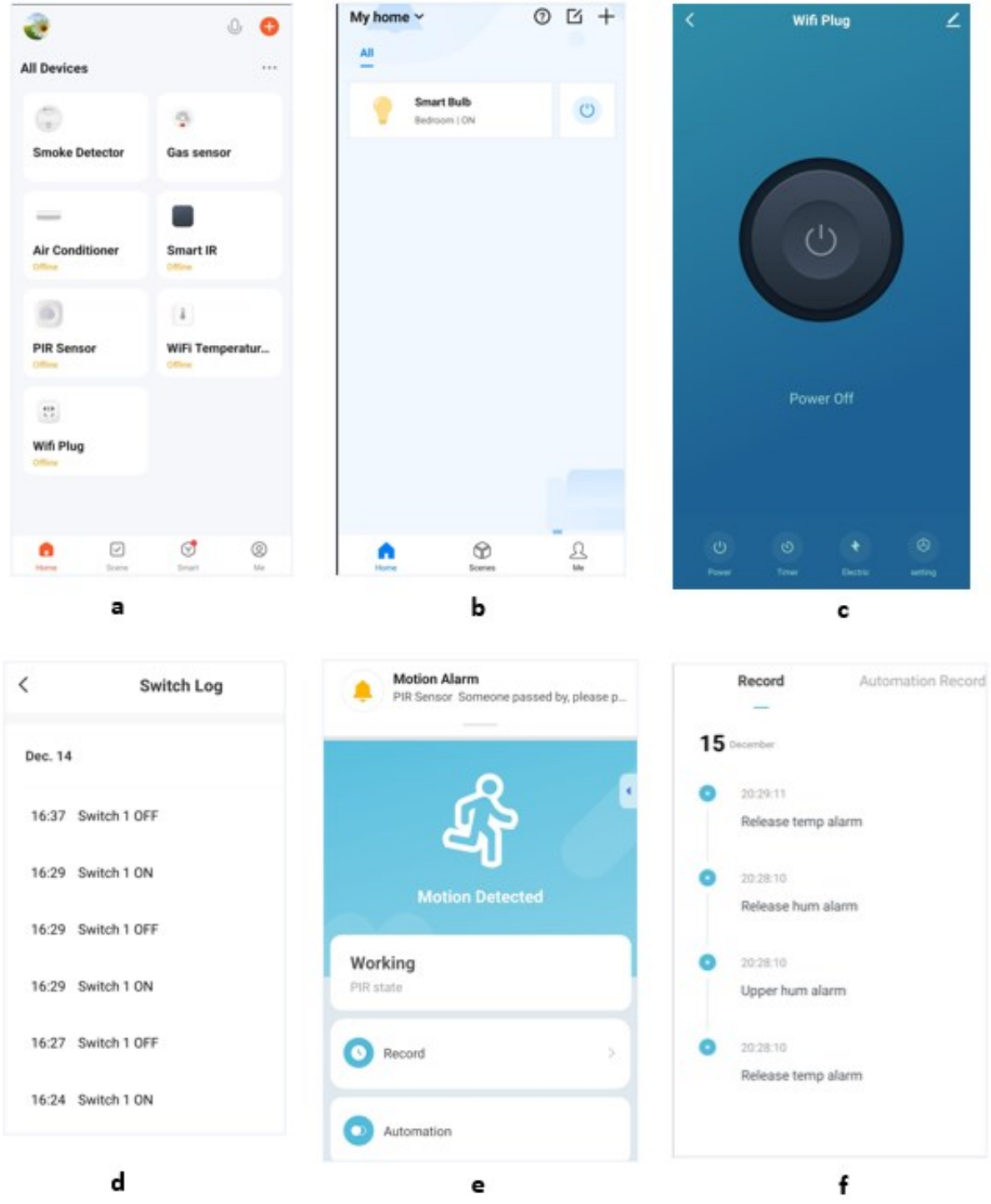

Figure 4.23. Artifacts extracted; (a) IoT devices connected with the Tuya App, (b,c) Smart bulb connected with the Magic home app, (d) The smart switch log page, (e) Motion detection records, (f) T & H sensor log page

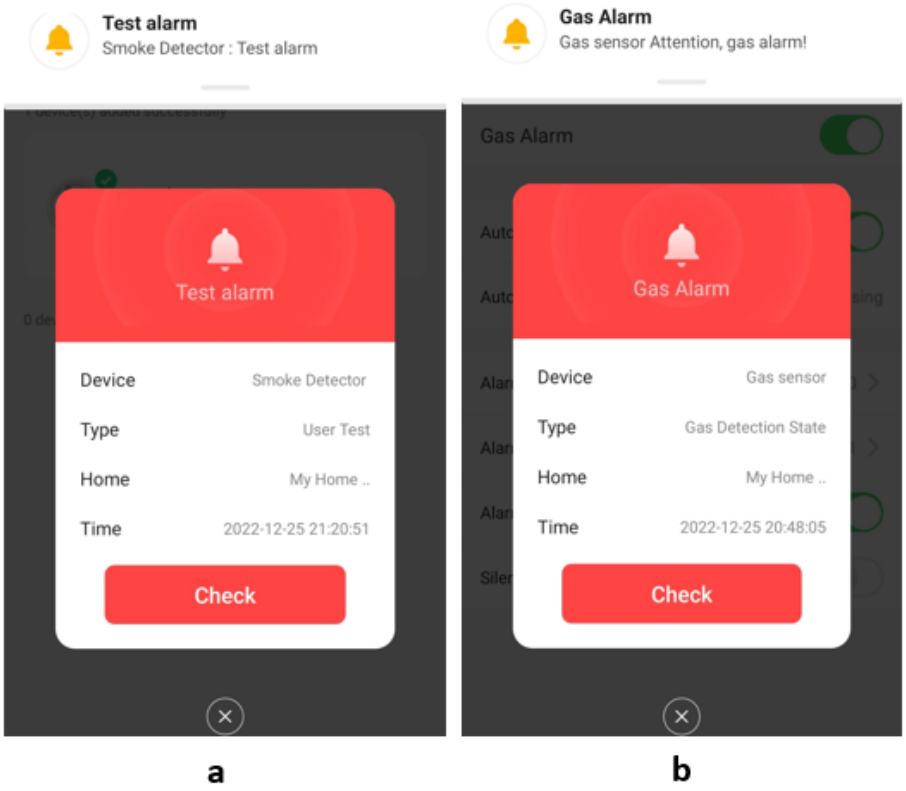

Figure 4.24. Artifacts extracted; (a) Smoke detector alarm, (b) Gas detector alarm.

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/Andriod/data/com.tuya.smart, Filesystem/Andriod/data/com.magichome.smart, as shown in Figure 4.25. Moreover, the MAGNET AXIOM tool was used in conducting mobile logical acquisition and analyzing the IoT apps. Artifacts were found including the alarms timestamp generated from the IoT apps as shown in Figure 4.26. In addition, the logs files for Tuya and magic home apps as shown in Figure 4.27.

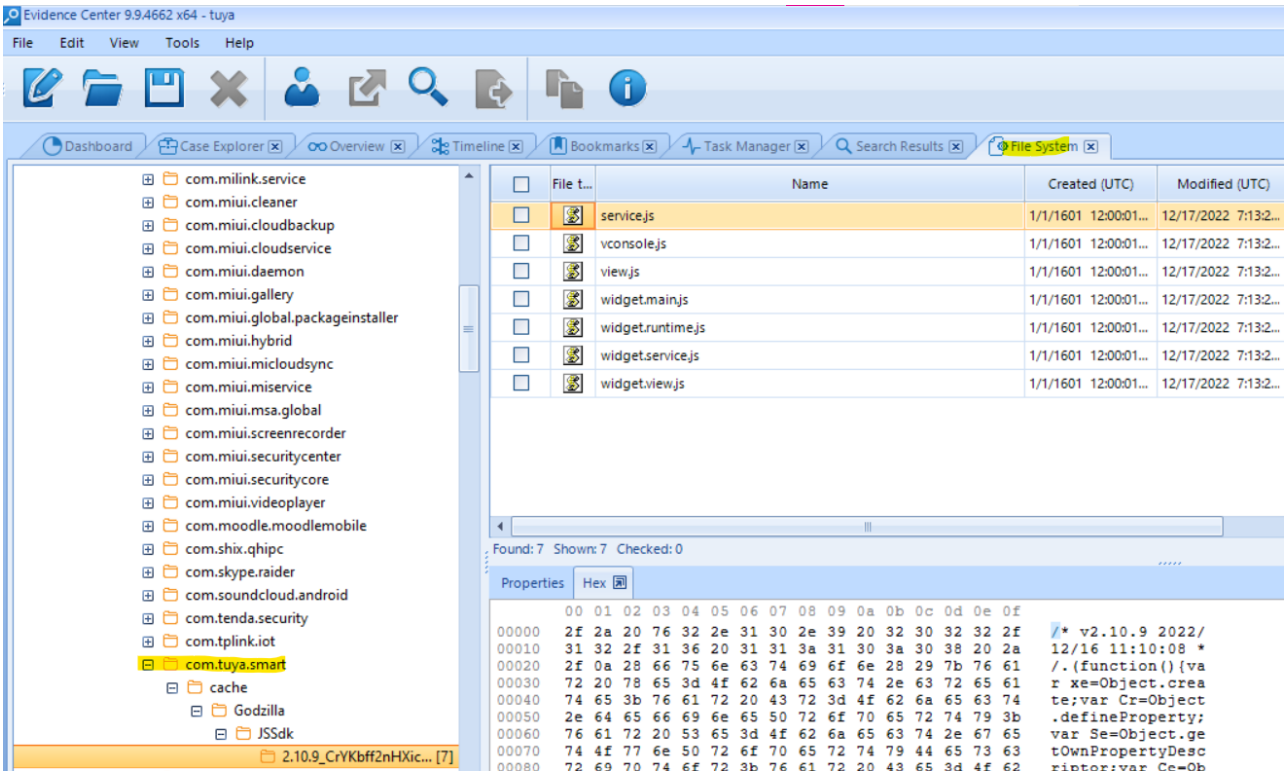

Figure 4.25. Data about the Tuya application from logical acquisition using the Belkasoft tool

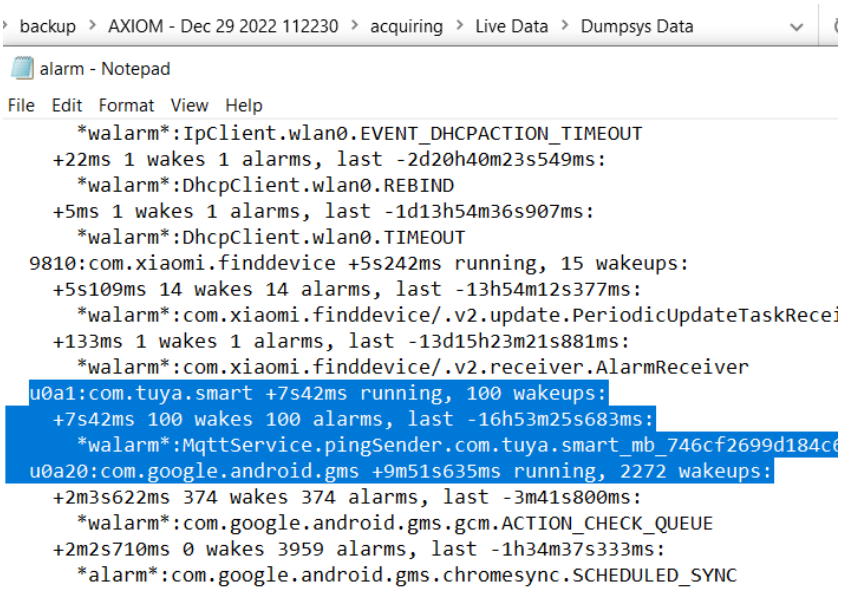

Figure 4.26. The alarms timestamp generated from the IoT apps from AXIOM tool

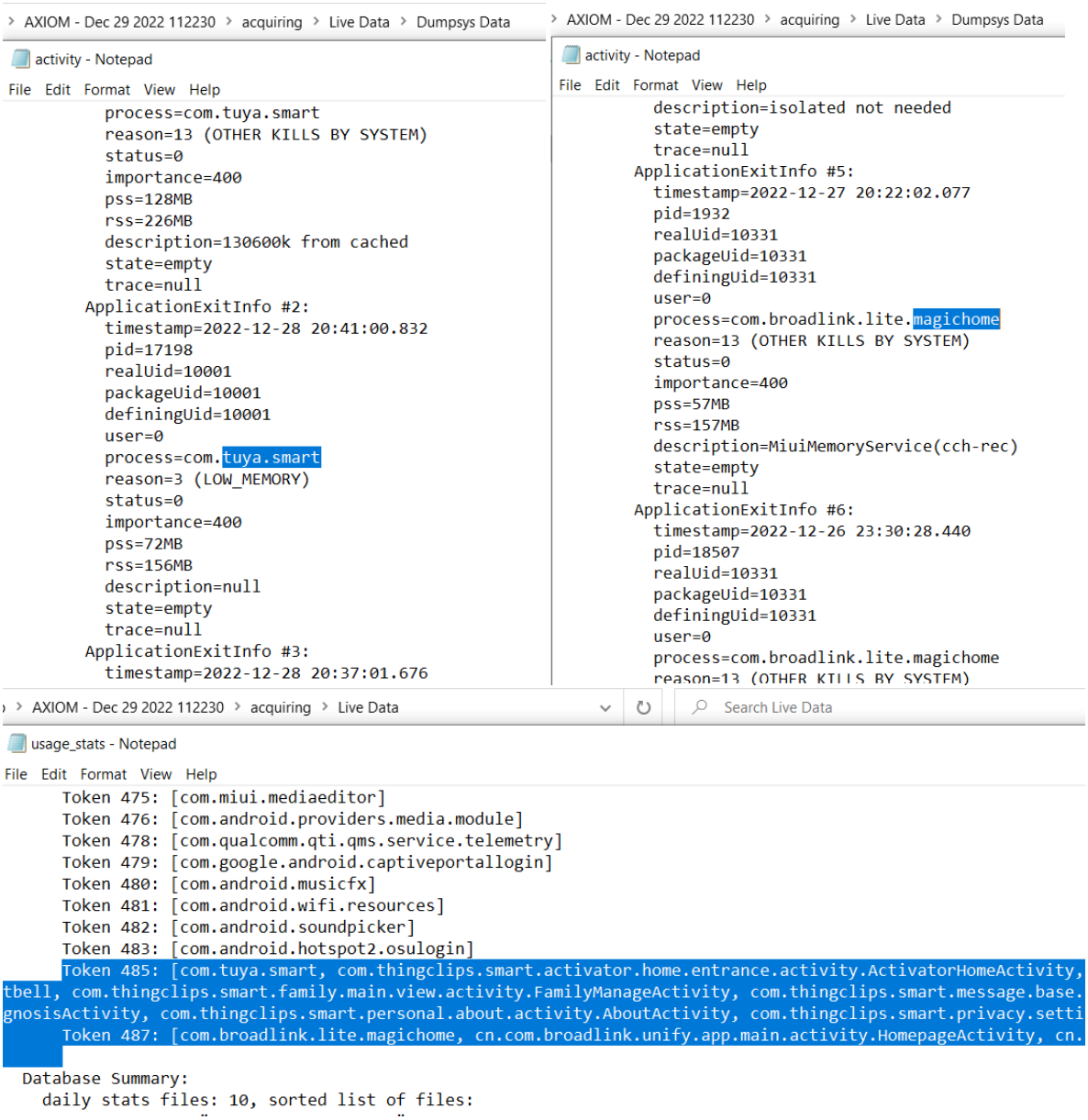

Figure 4.27. Log files indicated information about Tuya and Magic home Apps from the AXIOM tool

4.4.6 Phase 6: Reporting the Results/ Documentation

All IoT devices in this case study were connected to the related mobile App and then a set of scenarios were conducted over the devices. According to (MAoIDFF – IoT) framework, documentation is a continuous activity required in all investigation phases. Thus, in this

case, all previous phases were recorded and explained. In the reporting phase, the type of artifacts for each scenario was documented and clarified in Table 4.13.

Table 4.13. Type of artifacts according to the scenarios conducted on the IoT devices.

Scenarios	User Role (actions)	Investigator Role	Type of Artifact (AoI, MA, UA, NA)
Scenarios on Wi-Fi 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 Wi-Fi 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 Wi-Fi 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 Wi-Fi 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	
	First, the device is ON once	The gas detector status is	

Scenarios on Wi-Fi Smart gas detector	connected	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 Wi-Fi 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 Wi-Fi 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, there were obtained from AXIOM tools which are considered (AoI)
No actions were conducted	--	--	Additional information about the app and the mobile was extracted from the logical acquisitions via AXIOM and Belkasoft tools, this is considered useful artifacts (UA)

Table 4.14 clarifies the expert witness report structure for the IoT environment case study according to the MAoIDFF – IoT framework.

Table 4.14. The expert witness report structure for the IoT environment case study according to the MAoIDFF – IoT framework

First Page	• Report name: Expert witness report: A Smart IoT environment investigation • Investigator name: Eng. Yaman Salem • Submitted to IoT digital investigation research public

Second Page	• Investigator detailed paragraph (Name, its experience briefly, city and country)
	  o Eng Yaman Salem, BSc. Telecom. Engineer, Info. Security Consultant.
	  o Certified in Linux, Network+, CCNA Security, CPTE, CIHE,
	  o Master's degree in CyberCrime and digital forensics
	  o Ramallah Palestine
	• Case details paragraph (This includes the offense name, case name, case number, the tools used, date of request, date of conclusion, and date of the published report.)
	• The resulting paragraph, includes the offense name, offense name, suspect names, the related cybercrime law, and artifacts of interest (AoI) clarified in Table 4.13.

Third page	Document Contents.
Fourth page	Introduction, an overview of the case (section 4.4).
The rest of the report (Stated in the previous subsections)	Includes the six phases of the proposed framework (MAoIDFF-IoT): • Phase 1: Define the AoI based on the Level/ Documentation (section 4.4.1) • Phase 2: Exploring the IoT environment/ Documentation (section 4.4.2) • Phase 3: Preparation/ Documentation (section 4.4.3) • Phase 4: Acquisition & preservation/ Documentation (section 4.4.4) • Phase 5: Examining & Analyzing/ Documentation (section 4.4.5) • Phase 6: Reporting the result/ Documentation (section 4.4.6)
	Guidelines, recommendations, and additional notes to facilitate the process for other investigators in the future
Appendix	Any other screenshots, images, and documents should be stated in the appendix.

4.4.7 Recommendations and Notes

In this case study, seven IoT devices were investigated, and it was concluded that each app has its features and its behavior over the mobile device. It is easy to extract IoT-related artifacts from some IoT devices, while others require more examination and search. Also, the output from each forensic tool may differ. The log files were found via AXIOM for the Tuya app, while the javascript files were obtained from the Belkasoft tool. Hence, it is recommended to use different tools to get the best results. In addition, it is recommended to conduct reverse engineering for IoT apps if the investigator doesn't find apparent artifacts, as the proposed framework suggested, to know where the app store the related data on the mobile, and to recognize the IoT app behavior. Also, it is good to search online

for the IoT device, which helps find the device's features and reviews about the device, and other helpful information that helps in the investigation. All proposed phases in the MAoIDFF-IoT framework were applied and documented which facilitated the investigation mission and guided the investigator.

4.5 Summary

In this chapter, the proposed framework (MAoIDFF-IoT) was evaluated and tested by conducting a digital investigation on three case studies. The first one was performed on a smart camera at the device level. In this case, the researcher focused on investigating the content and the external memory file system, FAT32. The operating system (OS) was first examined and analyzed using the NMAP tool to find any artifact from the OS, as the camera doesn't have any port for connection to the workstation. Second, the FAT32 file system in the external memory was examined and analyzed. The FAT32 in-depth was analyzed through four main steps mentioned in the proposed framework; (1) analyze the boot sector, (2) analyze metadata and file names, (3) analyze the content, and (4) analyze the camera behavior.

The second case study was conducted on a smart camera at the mobile level. The researcher made the logical and manual acquisition to extract artifacts from the mobile camera app. The third case study was conducted on a smart environment that contained 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. The researcher focused on extracting artifacts from the mobile apps that control these IoT devices. The network and device levels investigation were excluded in this case, as the devices don't have any external or internal memories. Also, they don't send any streaming data via the network.

All the proposed phases in the MAoIDFF-IoT framework were applied in all case studies, starting from defining the Artifact of Interest (AoI), then exploring the IoT environment by defining the components (C), the expected artifacts (EA), the expected threats (ET) for each component, and (4) the consequences of the expected threats. In addition to the preparation

phase, which included preparing the appropriate investigation tools according to the chosen levels. In the acquisition & preservation phase, the researcher played the role of user and investigator at the same time by conducting several actions on the IoT devices, while in the examining & analyzing phase, the researcher verified these actions by analyzing data obtained after each scenario to find artifacts according to the conducted actions, the extracted artifacts are classified into four according to the proposed framework: missed artifact (MA), no artifact (NA), the useful artifact (UA), or artifact of interest (AoI). Finally, the reporting phase was stated, and the documentation phase was included in all phases. Hence, all the suggested phases in the proposed framework were applied in this section. As a result, the proposed framework (MAoIDFF-IoT) is applicable and easy to use by any digital investigator who has an IoT digital investigation case. Table 4.15 summarizes the IoT devices used in case studies with related investigation levels.

Table 4.15. The IoT devices used in case studies with related investigation level

IoT device	Device level investigation	Network level investigation	Application level investigation
Smart Camera	✓	--	✓ (Tapo mobile App)
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)

Chapter 5

5 Conclusion and Future Work

The IoT-driven industrial revolution that is taking place right now is doing so more rapidly than any tech innovation in history. It is gradually impacting every sector of the global economy and daily life. With IoT devices, everything and everyone is computerized. Thus, digital forensics is one of the main concerns for numerous businesses and human life.

Today's digital forensics is more than just concerned with computers, mobiles, or networks. The current digital forensics landscape requires a drastically different approach, transitioning from "traditional digital forensics" to "IoT multilevel digital forensics", where IoT Digital forensics frameworks should be designed and built to face the heterogeneous architecture of IoT environments. This is why the framework "Multilevel Artifact of Interest Digital Forensics Framework for IoT" (MAoIDFF-IoT) was proposed.

The keynote 'Multilevel' in (MAoIDFF-IoT) framework aims to cover all the levels of IoT architecture: the device level, the network level, and the application level. The application level might include a web interface, a cloud service, or a mobile application that controls IoT devices. The novel IoT digital forensics framework encompasses the advantages of the previous frameworks with additional new features designed to make it more usable and applicable to actual, recent, and future IoT investigation senses. This thesis calls for the digital forensics community to focus on multilevel digital forensics when dealing with contemporary crime scenes in the era of the Fourth Industrial Revolution (IR4.0).

5.1 Conclusion

In this thesis, a particular focus on IoT digital forensics was given. Chapter 2 presents an overview of IoT history, IoT definitions, IoT architectures, and common IoT attacks. Moreover, several previous digital forensic frameworks were reviewed. In addition, the IoT digital forensic frameworks are explored, stated, and compared according to the three levels

of IoT architecture (the device level, the network level, and the application level). IoT digital forensics with traditional digital forensics was compared. In addition, IoT digital forensics challenges in IR 4.0 were presented.

In chapter three, the structure of the proposed framework, named "Multilevel Artifact of Interest Digital Forensics Framework for IoT (MAoIDFF-IoT)," was stated and explained. Mainly, this framework has six significant phases; (1) defining the AoI according to the level/ documentation, (2) exploring the IoT environment/ documentation, (3) preparation/ documentation, (4) acquisition & preservation/ documentation, (5) examining & analyzing/ documentation, (6) reporting/ documentation. The documentation is a critical phase that should be conducted through the six phases, which help maintain the integrity and document the report to be submitted to the court. Each primary phase has sub-phases for additional activities, which enrich the framework and make it practical and inclusive.

To avoid missing any critical artifacts needed in the investigation, MAoIDFF-IoT covers all the IoT levels. It focuses on Artifacts of Interest (AoI) for each level to avoid consuming time and effort. In addition, it defines the components (C), the expected artifacts (EA), and the expected threats (ET) for each component which make the exploring of IoT environments more understandable. The proposed framework defines the types of artifacts (AoI, Useful Artifact - UA, Missed Artifact -MA, No Artifact - NA). These artifact types were invented in this framework, which is considered a good addition. Thus, the MAoIDFF-IoT framework has several features that attract digital investigators to apply and use.

In chapter four, the proposed (MAoIDFF-IoT) framework was evaluated by three case studies; (1) the digital investigation experiment on a smart camera at the device level, (2) the digital investigation experiment on a smart camera at the application level, and (3) the digital investigation experiment on a smart environment contained seven IoT devices at the application level. All the proposed phases in the framework were applied, starting from

defining the Artifact of Interest (AoI), then exploring the IoT environment. In addition to the preparation phase, which included preparing the appropriate investigation tools.

In the acquisition & preservation phase, the researcher played the role of user and investigator at the same time by conducting several actions on the IoT devices, while in the examining & analyzing phase, these actions were verified by analyzing the obtained data after each scenario to extract artifacts. The extracted artifacts are classified into four according to the proposed framework: missed artifact (MA), no artifact (NA), useful artifact (UA), or artifact of interest (AoI). Finally, the reporting phase was stated, and the documentation phase was included in all phases. Further, a proposed report structure for court submission was stated at the end. Hence, all the proposed phases in the MAoIDFF-IoT framework were applied. Real scenarios experiments tested the proposed framework. As a result, the evaluation of the experimental results reveals the superiority and advantages of the MAoIDFF-IoT framework over existing frameworks in terms of usability, inclusivity, focusing on the artifact of interest, and speeding up the investigation process.

5.2 Key Challenges

The following challenges were faced while conducting this research:

- Extracting artifacts and finding the source of 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 used for analyzing, such as Autopsy, Belkasoft, and AXIOM and these tools did a satisfactory job. Still, 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.

5.3 Future Work

The following are promising ideas that appeared during the research which could be considered to extend this work:

Apply the framework to more realistic scenarios. The framework was evaluated and applied, and its effectiveness was proved. However, it is an excellent step to conduct more real scenarios 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 and enjoy the advantages of well-organized phases and structure of the MAoIDFF-IoT framework.

Focusing on other types of IoT OS and filesystems. Recall that chapter two presents the digital forensics challenges at the IoT device level. Among them is the variety of IoT devices' brands and standards. The IoT devices could have several operating systems and filesystems, which poses a challenge for digital investigators, so it would be an excellent step to focus on investigating and exploring different types of OS and filesystems related to the IoT devices. In this thesis, the experimental results showed that the IoT device, the camera device, has an unknown OS, and the type of file system in the external memory was FAT32. Thus investigating FAT32 was the focus.

Focusing on analyzing and examining volatile and encryption data from IoT devices. Some IoT devices store encryption data or generate volatile data. Thus, it is challenging for digital investigators to analyze and extract artifacts from these IoT devices with these capabilities. The MAoIDFF-IoT framework proposed that if any encrypted data was found, then it is suggested to use the appropriate tool or method to decrypt and analyze the encrypted data as stated in the flowchart (Figure 3.6). However, it is a good addition if

the researchers dig more to find details about decrypting generated encryption data from IoT devices.

Developing IoT digital investigation tool for multilevel structure. Developing an investigation tool specialized for IoT devices will facilitate the investigation work. The tool should apply the six suggested phases in the proposed framework and consider the multilevel structure of the MAoIDFF-IoT framework with the proposed output report structure.

References

[1] M. Xu, J. M. David, and S. H. Kim, “The fourth industrial revolution: Opportunities and challenges,” *International Journal of Financial Research*, vol. 9, no. 2, pp. 90–95, 2018, doi: 10.5430/ijfr.v9n2p90.

[2] 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.

[3] 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.

[4] 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.

[5] S. Alabdulsalam, K. Schaefer, T. Kechadi, and N. A. Le, “Internet of Things Foresnsics: Challenges and Case Study,” in *IFIP International Conference on Digital Forensics*, 2018, vol. 13, pp. 35–48.

[6] S. Zawoad 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] L. Coetzee and G. Olivri, “Inclusion Through the Internet of Things,” *Assistive Technologies*, vol. 31, 2012, doi: 10.5772/31929.

[8] 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.

[9] 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.

[10] B. Nelson, A. Phillips, and C. Steuart, *Guide to Computer Forensics and Investigations*. 2018.

[11] S. Madakam, R. Ramaswamy, and S. Tripathi, “Internet of Things (IoT): A Literature Review,” *Journal of Computer and Communications*, vol. 03, no. 05, pp. 164–173, 2015, doi: 10.4236/jcc.2015.35021.

[12] J. Voas, “Demystifying the Internet of Things,” *Computer*, vol. 49, no. 6, pp. 80–83, 2016, doi: 10.1109/MC.2016.162.

[13] Gartner, “Internet of Things (IoT) - Gartner Glossary,” 2022. https://www.gartner.com/en/information-technology/glossary/internet-of-things (accessed May 01, 2022).

[14] NIST, “Internet of Things (IoT) - NIST Definition,” 2022. https://csrc.nist.gov/glossary/term/internet_of_things_IoT (accessed May 01, 2022).

[15] 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.

[16] J. Lin, W. YU, N. Zhang, X. Yang, H. Zhang, and 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] K. Rose, S. Eldridge, and L. Chapin, “The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World,” *The Internet Society*, vol. 1–54, p. 54, 2015, [Online]. Available: http://electronicdesign.com/communications/internet-things-needs-firewalls-too.

[23] N. S. Swamy, S. Nayak, and V. M. N, “Analysis on IoT Challenges, Opportunities, Applications and Communication Models,” *International Journal of Advanced Engineering, Management and Science (IJAEMS)*, vol. 2, no. 4, pp. 75–78, 2016.

[24] V. Tkachenko, A. Goriushkina, and M. Kolisnyk, “Communication Messaging Models in IoT/WoT: Survey and Application,” *Communication Messaging Models in IoT/WoT: Survey and Application. In 2018 International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T)*, pp. 417–422, 2018.

[25] J. Deogirikar and A. Vidhate, “Security attacks in IoT: A survey,” *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, vol. 6, pp. 32–37, 2017, doi: 10.1109/I-SMAC.2017.8058363.

[26] B. Russell and D. Van Duren, *Practical Internet of Things SecuritySecond Edition*. 2018.

[27] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: Current status and open issues," *2014 International Conference on Privacy and Security in Mobile Systems, PRISMS 2014 - Co-located with Global Wireless Summit*, vol. 8, no. May, pp. 1–8, 2014, doi: 10.1109/PRISMS.2014.6970594.

[28] 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.

[29] 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.

[30] 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.

[31] F. Jafari and R. S. Satti, "Comparative Analysis of Digital Forensic Models," *Journal of Advances in Computer Networks*, vol. 4, no. 1, pp. 82–86, 2015, doi: 10.7763/jacn.2015.v3.146.

[32] 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.

[33] 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.

[34] 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.

[35] V. Baryamureeba and F. Tushabe, "The Enhanced Digital Investigation Process Model," 2004, [Online]. Available: http:/dfrws.org.

[36] 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%5Cnhttps://utica.edu/academic/institutes/ecii/publications/articles/A0B70121-FD6C-3DBA-0EA5C3E93CC575FA.pdf.

[37] N. Beebe, J. Clark, N. L. Beebe, and J. G. Clark, "A Hierarchical, Objectives-Based Framework for the Digital Investigations Process," 2004.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

[42] 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.

[43] 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.

[44] 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.

[45] 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.

[46] 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.

[47] M. D. K, "Integrated Digital Forensic Process Model," *Computers & Security*, vol. 38, no. November, pp. 103–115, 2013.

[48] 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.

[49] A. Ajijola, P. Zavarsky, and R. Ruhl, "A Review and Comparative Evaluation of Forensics Guidelines of NIS T SP 800-101 Rev. 1 :2014 and ISO/IEC 27037:2012," *World Congress on Internet Security*, vol. 1–8, p. 8, 2014.

[50] 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.

[51] 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.

[52] 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.

[53] 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.

[54] P. M. Dimpe and O. P. Kogeda, "Generic Digital Forensic Requirements," *2018 Open Innovations Conference, OI 2018*, pp. 240–245, 2018, doi: 10.1109/OI.2018.8535924.

[55] 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.

[56] 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.

[57] 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.

[58] M. S. Kirmani and M. T. Banday, "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.

[59] 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.

[60] 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.

[61] 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.

[62] 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.

[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/JIOT.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. 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.

[69] 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.

[70] 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.

[71] 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.

[72] C. Meffert, D. Clark, I. Baggili, and F. Breitinger, “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.

[73] 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.

[74] 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.

[75] A. Nieto, R. Rios, and J. Lopez, “A Methodology for Privacy-Aware IoT-Forensics,” *2017 IEEE Trustcom/BigDataSE/ICESS*, vol. 7, pp. 626–633, 2017, doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.293.

[76] 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.

[77] "OpenHAB Controller," 2022. https://www.openhab.org/ (accessed Jun. 01, 2022).

[78] 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.

[79] T. Wu, F. Breitinger, 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.

[80] 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.

[81] 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.

[82] 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.

[83] 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.

[84] 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.

[85] T. Wu, "Digital Forensic Investigation of IoT Devices : Tools and Methods," *(Doctoral dissertation, University of Oxford).*, 2020.

[86] B. Carrier, *File System Forensic Analysis*, vol. 511. 2005.

[87] 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.

[88] R. Tamma, O. Skulkin, H. Mahalik, and S. Bommisetty, *Practical Mobile Forensics: Forensically investigate and analyze iOS, Android, and Windows 10 devices*. 2014.

[89] 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.

[90] A. Y. Mahmoud, "Theory and Practice of Forensics Techniques for Smartphones," 2018.

[91] 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.

[92] O. Afonin and V. Katalov, *Mobile Forensics – Advanced Investigative Strategies*. 2016.

[93] Source Android, "Android Security Features." https://source.android.com/security/features (accessed Jun. 01, 2022).

[94] Tapo, "Tapo Smart Camera," 2022. https://www.tapo.com/us/product/smart-camera/tapo-c200/ (accessed Mar. 15, 2022).

6 Appendix

6.1 Appendix A: Addition Decoding Tables

Table 6.1. Encoding Table for the first 36 bytes of boot sector in FAT 12/16/32 [86].

Byte Range	Description
0–2	Assembly instruction to jump to boot code. No (unless it is a bootable file system)
3–10	OEM Name in ASCII
11–12	Bytes per sector. Allowed values include 512, 1024, 2048, and 4096.
13–13	Sectors per Cluster (data unit). Allowed values are powers of 2, but the cluster size must be 32KB or smaller.
14–15	Size in sectors of the reserved area
16–16	Number of FATs. Typically, two for redundancy, but according to Microsoft, it can be one for some small storage devices.
17–18	Maximum number of files in the root directory for FAT12 and FAT16. This is 0 for FAT32 and typically 512 for FAT16.
19-20	16-bit value of the number of sectors in the file system. If the number of sectors is larger than can be represented in this 2-byte value, a 4-byte value exists later in the data structure, and this should be 0.
21-21	Media type. According to Microsoft documentation, 0xf8 should be used for fixed disks and 0xf0 for removable.
22-23	16-bit size in sectors of each FAT for FAT12 and FAT16. For FAT32, this field is 0.
24–25	Sectors per track of storage device.
26–27	A number of heads in the storage device.
28–31	Number of sectors before the start of the partition
32–35	32-bit value of several sectors in the file system. Either this value or the 16-bit value above must be 0.

Table 6.2. Encoding Table for 36-512 bytes of boot sector in FAT 32 [86].

Byte Range	Description
0-35	Table 6
36-39	32-bit size in sectors of one FAT.
40-41	Defines how multiple FAT structures are written to. If bit 7 is 1, only one of the FAT structures is active and its index is described in bits 0–3. Otherwise, all FAT structures are mirrors of each other.
42-43	Defines how multiple FAT structures are written to. If bit 7 is 1, only one of the FAT structures is active and its index is described in bits 0–3. Otherwise, all FAT structures are mirrors of each other.
44-47	Cluster where root directory can be found.
48-49	The sector where FSINFO structure can be found.
50-51	The sector where the backup copy of the boot sector is located (default is 6).
52-63	Reserved.
64-64	BIOS INT13h drive number.
65-65	Not used.
66-66	Extended boot signature to identify if the next three values are valid. The signature is 0x29.
67-70	Volume serial number, which some versions of Windows will calculate based on the creation date and time.
71-81	Volume label in ASCII. The user chooses this value when creating the file system.
82-89	File system type label in ASCII. Standard values include "FAT32," but nothing is required.
90-509	Not used.
510-511	Signature value (0xAA55).

Table 6.3. Encoding table for a basic FAT12/16/32 directory [86].

Byte Range	Description
0-0	The first character of the file name in ASCII and allocation status (0xe5 or 0x00 if unallocated)
1-10	Characters 2 to 11 of the file name in ASCII
11-11	File Attributes (see Table 7.4)
12-12	Reserved
13-13	Created time (tenths of a second)
14-15	Created time (hours, minutes, seconds)
16-17	Created day
18-19	Accessed day
20-21	High 2 bytes of first cluster address (0 for FAT12 and FAT16)

22-23	Written time (hours, minutes, seconds)
24-25	Written day
26-27	Low 2 bytes of first cluster address
28-31	Size of file (0 for directories)

Table 6.4**.** Flag values for attributes in a basic FAT12/16/32 entry directory (byte No. 11) [86].

Flag Value	Description
0x01	Read-only
0x02	Hidden file
0x04	System file
0x08	Volume label
0x0f	Long filename
0x10	Directory
0x20	Archive

Table 6.5. Encoding table for LFN FAT12/16/32 directory entry [86].

Byte Range	Description
0-0	Sequence number (ORed with 0x40) and allocation status (0xe5 if unallocated)
1-10	File name characters 1–5 (Unicode)
11-11	File attributes (0x0f)
12-12	Reserved
13-13	Checksum
14-25	File name characters 6–11 (Unicode)
26-27	Reserved
28-31	Reserved

الملخص

أدى ظهور الثورة الصناعية الرابعة (IR4.0) إلى العديد من الفوائد على صعيد الأعمال وحياتنا اليومية. تتضمن الثورة الصناعية الرابعة تطوير أجهزة إنترنت الأشياء (IoT). على الرغم من أن إنترنت الأشياء تجلب العديد من الفوائد لحياة الإنسان، إلا أن النمو الهائل لأجهزة إنترنت الأشياء والهيكل الأمني الضعيف لأجهزة إنترنت الأشياء تخلق فرصًا جديدة للمتطفلين لارتكاب جرائم الكترونية، وكسر الخصوصية، وإجراء أو التخطيط لأنشطة غير قانونية. قد تحتوي البيانات الضخمة التي يتم إنشاؤها من أجهزة إنترنت الأشياء على أدلة قيمة لمسرح الجريمة. وبالتالي، فإن بيئة إنترنت الأشياء المعقدة، وتنوع المعايير والمطورين، والافتقار إلى أدوات التحليل الجنائي لإنترنت الأشياء تشكل تحديات أمام محققي الطب الشرعي الرقمي وتخلق عقبات أمام العثور على المجرمين. لذلك من الأهمية بمكان أن يستعد مجتمع الطب الشرعي الرقمي للتعامل مع الحوادث المتعلقة بإنترنت الأشياء في عصرالثورة الصناعية الرابعة (IR4.0).

تهدف هذه الأطروحة بعنوان "نحو الطب الشرعي الرقمي 4.0: إطار عمل للطب الشرعي الرقمي متعدد المستويات لأجهزة إنترنت الأشياء" إلى اقتراح وتقييم إطار عمل جديد للطب الشرعي الرقمي لإنترنت الأشياء يناسب احتياجات عصر الثورة الصناعية الرابعة، ولتحقيق هذا الهدف، تم إجراء مراجعة منهجية للأدبيات (SLR). أشارت نتائج المراجعة إلى أن بنية إنترنت الأشياء تتكون أساسًا من ثلاثة مستويات (مستوى الجهاز ومستوى الشبكة ومستوى التطبيق) ، وكل مستوى محاط بالعديد من التحديات. صممنا واقترحنا إطار عمل الطب الشرعي الرقمي متعدد المستويات لإنترنت الأشياء ويركزعلى الأدلة محل الاهتمام (MAoIDFF-IoT). هذا الإطار تم تصميمه للتغلب على تحديات إنترنت الأشياء، ولمواجهة البنية غير المتجانسة لبيئات إنترنت الأشياء، فهو يوفر للمحققين إرشادات لإجراء الطب الشرعي لإنترنت الأشياء في ثلاث مستويات. علاوة على ذلك ، تم تقييم الإطار المقترح واختباره من خلال تجارب حقيقية. يكشف تقييمنا للنتائج التجريبية عن تفوق ومزايا إطار عملنا على الأطر الحالية من حيث قابليته للاستخدام والشمولية بالإضافة إلى التركيز على الأدلة محل الاهتمام وتسريع عملية التحقيق.