

A GENERIC FRAMEWORK FOR IOT FORENSIC INVESTIGATION



By

Abeer Gauher

00000274980-MSIS-11-2018

Supervisor

Dr. Yousra Javed

DEPARTMENT OF COMPUTING

A thesis submitted in partial fulfillment of the requirements for the degree of
Masters in Information Security (MSIS)

In

School of Electrical Engineering and Computer Science

National University of Sciences and Technology (NUST)

Islamabad, Pakistan

(September 2020)

Approval

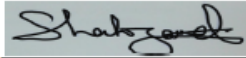
It is certified that the contents and form of the thesis entitled "A generic framework for IoT forensic investigation" submitted by ABEER GAUHER have been found satisfactory for the requirement of the degree.

Advisor: Dr. Yousra Javed

Signature: 

Date: 03-Oct-2020

Committee Member 1: Dr. Shahzad Saleem

Signature: 

Date: 06-Oct-2020

Committee Member 2: Dr. Hasan Tahir

Signature: 

Date: 04-Oct-2020

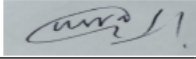
Committee Member 3: Dr. Mehdi Hussain

Signature: 

Date: 05-Oct-2020

THESIS ACCEPTANCE CERTIFICATE

Certified that final copy of MS/MPhil thesis entitled "A generic framework for IoT forensic investigation" written by ABEER GAUHER, (Registration No 00000274980), of SEecs has been vetted by the undersigned, found complete in all respects as per NUST Statutes/Regulations, is free of plagiarism, errors and mistakes and is accepted as partial fulfillment for award of MS/M Phil degree. It is further certified that necessary amendments as pointed out by GEC members of the scholar have also been incorporated in the said thesis.

Signature: _____

Advisor: Dr. Yousra Javed

Date: 03-Oct-2020

Signature (HOD): _____

Date: _____

Signature (Dean/Principal): _____

Date: _____

DEDICATION

This dissertation is dedicated to my parents and my mentors who have been with me throughout and guided me along each and every step.

Certificate of Originality

I hereby declare that this submission titled "A generic framework for IoT forensic investigation" is my own work. To the best of my knowledge it contains no materials previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any degree or diploma at NUST SEecs or at any other educational institute, except where due acknowledgement has been made in the thesis. Any contribution made to the research by others, with whom I have worked at NUST SEecs or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except for the assistance from others in the project's design and conception or in style, presentation and linguistics, which has been acknowledged. I also verified the originality of contents through plagiarism software.

Student name: ABEER GAUHER

Signature: 

ACKNOWLEDGEMENT

Firstly, I would like to thank my parents for always being with me, supporting me and for letting me pursue my dreams without whom I wouldn't be where I am today. I also am truly grateful for my supervisor Dr. Yousra Javed whose supervision and patience made it possible for me to be able to complete my thesis. I couldn't have asked for a better supervisor. I would also like to thank all my committee members Dr. Hasan Tahir, Dr. Mehdi Hussain and Dr. Shahzad Saleem for guiding me along the way and helping me to successfully complete my thesis.

Table of Contents

1. INTRODUCTION	1
1.1 Historical Background	1
1.1.1 Forensic Science	2
1.1.2 Digital Forensics	2
1.1.3 Types of Digital Forensics	3
1.1.4 Digital Evidence	4
1.1.5 Handling Digital Evidence.....	5
1.1.6 Internet of Things (IoT)	5
1.1.7 Characteristics of IoT.....	6
1.1.8 IoT architecture.....	7
1.1.9 Security challenges in IoT	8
1.1.10 IoT Forensics	9
1.1.11 Challenges in IoT Forensics.....	9
1.1.12 The need for an appropriate IoT Forensic framework	11
1.2 Motivation	12
1.3 Research Questions	12
1.4 Problem Statement	13
1.5 Goals and Objectives	13
1.6 Intended Audience	13
1.7 Organization of Thesis	14
2. LITERATURE REVIEW	15
2.1 Introduction	15
2.2 Differentiating between frameworks, methodology, architecture and processes	15
2.3 Analysing IoT forensic frameworks	16
2.4 Examining Google Home	20
3. RESEARCH METHODOLOGY	22
3.1 Introduction	22
3.2 The Research Process	22
3.3 Steps of the Research Process.....	23
3.3.1 Identifying the research problem	24
3.3.2 Literature review	25

3.3.3 Purpose of the research	25
3.3.4 Designing the framework.....	25
3.3.5 Collecting data	26
3.3.6 Extracting and analysing evidence following the framework.....	26
3.3.7 Presenting the results	27
4. EXPERIMENTATION	28
4.1 Introduction	28
4.2 Specification of the devices	28
4.2.1 Google Home Mini	28
4.2.2 Mobile Device.....	28
4.2.3 Forensic Workstation.....	28
4.3 Tools and Technologies	29
4.3.1 Mobile Device.....	29
4.3.2 Forensic Workstation.....	29
4.4 Data Collection	29
4.4.1 Setting up the Google Home Mini	30
4.4.2 Performing use cases.....	30
5. THE PROPOSED FRAMEWORK	33
5.1 Introduction	33
5.2 Case for investigation	33
5.3 Overview of the complete the framework	33
5.4 The proposed framework	36
5.4.1 Pre – Investigation Phase	36
5.4.1.1 Planning the investigation	36
5.4.1.2 Preparing for the investigation	37
5.4.2 The Acquisition Phase	38
5.4.2.1 Evidence Identification Process	39
5.4.2.2 Evidence Collection Process	40
5.4.2.3 Evidence Acquisition Process	41
5.4.2.3.1 Google Home Mini Architecture	41
5.4.2.3.2 Acquiring Evidence	42
5.4.2.4 Evidence Storage and Preservation Process	49
5.4.3 The Investigative Phase	50
5.4.3.1 Evidence Analysis Process	51

5.4.3.2 Classifying the evidence	86
5.4.3.3 Reporting	87
5.4.3.4 Presentation.....	90
5.4.3.5 Investigation Closure	90
5.4.4 The Concurrent Phase	90
5.4.4.1 Obtaining Authorization	91
5.4.4.2 Documentation	91
5.4.4.3 Chain of Custody	92
5.4.4.4 Preserving Chain of Custody	94
5.4.4.5 Maintaining Integrity of the evidence	94
5.4.4.6 Creating a Timeline	94
6. RESULTS AND DISCUSSION.....	96
6.1 Introduction	96
6.2 Evaluating the research questions.....	96
6.2.1 RQ – 1	96
6.2.2 RQ – 2	96
6.2.3 RQ – 3	97
6.2.4 RQ – 4	97
6.2.5 RQ – 5	97
6.3 Comparative analysis of the framework	97
7. CONCLUSION AND FUTURE WORK.....	100
7.1 Introduction	100
7.2 Conclusion	100
7.3 Future Work	101
8. REFERENCES	102

List of tables

Table 2-1 Differences between frameworks, methodology, architecture and processes	15
Table 2-2 Limitations in the existing frameworks	20
Table 4-1 Performing use cases	31
Table 5-1 Details of the devices found	40
Table 5-2 Commands to capture packets	48
Table 5-3 Events table	55
Table 5-4 EventsRawTimes table	56
Table 5-5 Instances table	56
Table 5-6 view_events table	57
Table 5-7 Details in the Events table	61
Table 5-8 Commands found in My Activity	72
Table 5-9 Timeline to maintain chain of custody for the evidence	93
Table 5-10 Creating a Timeline	95
Table 6-1 Comparing frameworks	98

List of figures

Figure 1-1 Types of digital forensics	3
Figure 1-2 Number of IoT devices by 2025.....	6
Figure 1-3 IoT Architecture	8
Figure 1-4 Challenges in IoT forensics.....	11
Figure 3-1 Research Process	23
Figure 3-2 Identify a research problem.....	24
Figure 4-1 Wi-Fi connection error.....	30
Figure 5-1 Overview of A Generic Framework for IoT Forensic Investigation.....	35
Figure 5-2 Pre – Investigation Phase	37
Figure 5-3 The Acquisition Phase.....	39
Figure 5-4 Google Home Architecture	42
Figure 5-5 Connection of the mobile device.....	43
Figure 5-6 Backup of the mobile device.....	43
Figure 5-7 Conversion to .tar format	43
Figure 5-8 Root Checker.....	45
Figure 5-9 adb shell command.....	45
Figure 5-10 adb forward command.....	46
Figure 5-11 Forward mobile’s data to the forensic workstation.....	46
Figure 5-12 Receive mobile’s data using nc.....	46
Figure 5-13 Physical image successfully acquired	46
Figure 5-14 Setup to capture packets.....	48
Figure 5-15 The Investigative Phase.....	50
Figure 5-16 Two main folders found in the logical image	51
Figure 5-17 View of the apps folder	52
Figure 5-18 View of the shared folder.....	52
Figure 5-19 Chromecast folder	53
Figure 5-20 View of the XML file.....	54
Figure 5-21 Text file 0_dump_com.android.providers.calendars.....	54
Figure 5-22 Sync_state table.....	55
Figure 5-23 CalendarCache table.....	55
Figure 5-24 Reminders table.....	57

Figure 5-25 Volume names and sector occupied.....	58
Figure 5-26 Google Home folder.....	59
Figure 5-27 Chromecast folder in app	59
Figure 5-28 Calendar folder in data	60
Figure 5-29 Sync_state table in calendar.db	60
Figure 5-30 Calendars table in calendar.db	61
Figure 5-31 Events table in calendar.db	61
Figure 5-32 Calendars table in cal_v2a	62
Figure 5-33 Calendar preferences XML	62
Figure 5-34 Chromecast folder in data	63
Figure 5-35 Accounts table	63
Figure 5-36 Clearcut Events Table	64
Figure 5-37 Home graph.....	64
Figure 5-38 Bluetooth audio in home graph file.....	64
Figure 5-39 Account menu XML file	65
Figure 5-40 App preferences XML file	65
Figure 5-41 App preferences no backup XML file.....	65
Figure 5-42 Blob table in content store.....	66
Figure 5-43 Commands found	67
Figure 5-44 Reminder set by the user	67
Figure 5-45 Geller key table	67
Figure 5-46 Entries table.....	68
Figure 5-47 Recently folder	68
Figure 5-48 Device Info table	69
Figure 5-49 Network to Device table.....	69
Figure 5-50 Account table in reminders.db	69
Figure 5-51 Reminders table in reminders.db.....	70
Figure 5-52 Details of a command found in My Activity	71
Figure 5-53 JSON files	75
Figure 5-54 Google Nest Partner Connections JSON.....	75
Figure 5-55 Home app JSON file	76
Figure 5-56 Owner Create Timestamp conversion.....	76

Figure 5-57 Version timestamp conversion.....	76
Figure 5-58 Home app JSON file 2	77
Figure 5-59 Home History JSON file	77
Figure 5-60 Shopping list.....	78
Figure 5-61 Voice recordings	78
Figure 5-62 IP address and Protocol used.....	79
Figure 5-63 Port used by Google Home Mini	80
Figure 5-64 MDNS Protocol.....	80
Figure 5-65 Service string used in MDNS.....	81
Figure 5-66 MDNS query response	81
Figure 5-67 MDNS query response detailed view.....	81
Figure 5-68 Additional records as viewed in Wireshark	82
Figure 5-69 Googlezone service	82
Figure 5-70 Response generated using googlezone service	83
Figure 5-71 Bluetooth audio casted	83
Figure 5-72 News being casted.....	84
Figure 5-73 News being casted from a different news channel.....	84
Figure 5-74 Alarm being casted.....	85
Figure 5-75 Different tune of alarm being casted.....	85
Figure 5-76 Asking questions	86
Figure 5-77 Classification of the evidence	87
Figure 5-78 The Concurrent Phase	91

ABSTRACT

The advancement in technology along with the increase in the network bandwidth has not only given people the opportunity to be interconnected but devices as well. These devices that can now communicate with each other are now known as the Internet of Things (IoT). Since their inception, IoT devices have been on the rise and are now closely integrated with one's daily life allowing one to perform tasks efficiently. Unfortunately, this increased usage of the IoT devices makes it a viable target for attackers which allows them not to compromise one but all the devices connected through the same network.

A forensic investigator needs to carry out an investigation following an attack that enables the investigator to acquire the relevant digital evidence in a sound manner. This requires the use a framework that needs to be followed by the forensic investigator. This research is aimed at developing a generic forensic framework for the investigators, especially in the IoT forensics domain as IoT forensics is not a widely explored domain yet.

The proposed forensic framework has been tested and verified by using an IoT device where evidence was gathered and results were obtained by following the framework. The proposed framework has been compared with four existing IoT forensic framework which shows that the framework contains steps that were not included in the existing frameworks. The framework will serve as an important guideline for the forensic investigators that are involved in investigations containing IoT devices.

Keywords:

Cloud forensics, Digital Forensics, Digital Forensic Investigation, Forensic Investigation Framework, IoT forensics, Mobile forensics, Network forensics

CHAPTER 1

INTRODUCTION

This chapter contains basic information that will aid in building an understanding about this research. This information will provide a base that will help any kind of audience to acquire the knowledge needed to understand this particular research work. The chapter includes the motivation behind this research, the research questions and the problem statement of this research. Furthermore, the goals and objectives, the intended audience is also included. The chapter concludes by describing on how the thesis is organized. The following sections are in this chapter:

Section 1.1: Historical Background

Section 1.2: Motivation

Section 1.3: Research Questions

Section 1.4: Problem Statement

Section 1.5: Goals and Objectives

Section 1.6: Intended Audience

Section 1.7: Organization of the Thesis

1.1 Historical Background

This section provides a general overview of digital forensics, that will assist the audience that have little or no background in this particular domain. First, the important concepts are discussed, such as what digital forensics is, how it can be categorized and how digital evidence should be handled. Moving on, this section provides an introduction of IoT and further information on IoT architecture, IoT characteristics before discussing about IoT forensics, the challenges faced in IoT forensics and the growing need for an appropriate IoT forensic framework.

1.1.1 Forensic Science

The word “science” is defined as the study that involves an understanding of how natural and man-made processes take place by observing and carrying out experimentations. Forensic science is the practice of implementing the principles of science, so that past events can be analysed through the retrieved evidence and can be used in courts to catch criminals. The term “forensic” is derived from a Latin word “forensis” and is associated with a Roman business place known as the forum [1].

Over the years, forensic science has been classified into various categories and has been used to catch suspects in different cases. This not only includes computer-related crimes but also integrates DNA samples that are examined in laboratories; hence it is quite possible that an investigation may involve various branches of forensic science.

1.1.2 Digital Forensics

Digital forensics is a subdivision of the forensic science branch, and is proving to be of the utmost importance with the increased usage of digital devices. These devices such as computers, laptops, hard drives, and smartphones store data and fall within the category of digital forensics. The definition of digital forensics according to National Institute of Standards and Technology (NIST) is *“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”* [2].

Digital forensics is a process which is concerned with recovering and analyzing artifacts that have been obtained from the electronic devices [3]. The objective of the process is to identify, collect and preserve the evidence retrieved during an investigation aiding in reconstruction of the events [4]. It can be conducted according to the guidelines and methodologies defined by organizations such as NIST, International Standards of Organization (ISO), Scientific Working Group on Digital Evidence (SWDGE) which solely work on developing standards for the digital community. These practices ensure that the evidence collected and presented during legal investigations is sound and can be relied upon to identify the culprit.

1.1.3 Types of Digital Forensics

With the advancement in technology, the field of digital forensics is also growing as different types of devices are being used by people which means that the volume of data being created is increasing along with the difference in data formats being generated by these electronic devices. This has led to the need of classifying digital forensics into individual categories to cater the different data formats [5]. Figure 1-1 shows some types of digital forensics.

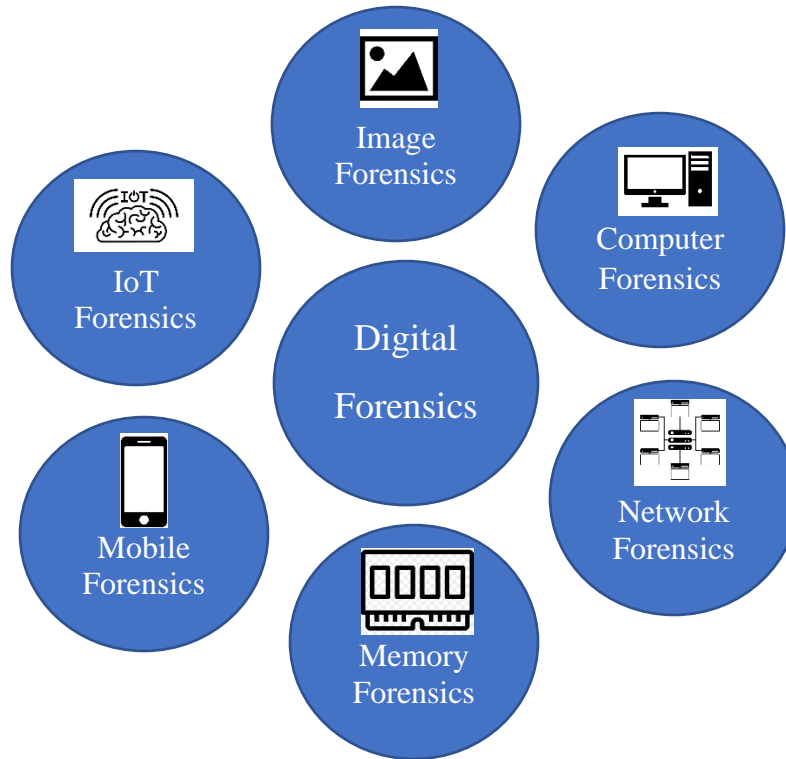


Figure 1-1 Types of digital forensics

Image forensics

Image forensics comprises of collecting and examining digital images to gather important information related to a particular image. This information is usually known as metadata and contains information about the image that can help prove the authenticity of the image and its related timestamps.

Computer forensics

The domain of computer forensics comprises of investigating computers and laptops during legal proceedings. The evidence deemed important is identified, collected, analysed and then presented

in the court of law during criminal investigations. Computer forensics aids in carrying out a well-defined investigation that not only points out the person responsible for carrying out the crime but also provides procedures for maintaining a chain of custody for the obtained evidence [6].

Network forensics

Network forensics is concerned with identifying abnormal activities such as intrusions in a network, malwares, botnets, security breaches and abnormal traffic patterns. These activities can be found out by monitoring, capturing and analysing the network traffic and also by looking at alerts generated by Intrusion Detection Systems. The analysis of the network traffic can help in finding out where and who carried out the attack.

Memory Forensics

The evaluation of volatile data that is retained in a computer's memory is known as memory forensics or live acquisition. A forensic investigator needs to conduct memory forensics as certain attacks and malicious activities do not leave a trace on the computer's hard drive.

Mobile forensics

The process of retrieving evidence from smartphones, SIM cards, Personal Digital Assistant (PDAs) and gaming devices is categorized as mobile forensics. The mobile devices are important as they store information such as contacts, photos, calendars, location information, web browsing history and much more that can prove useful in catching the suspect.

IoT Forensics

Internet of things forensics is the investigation of smart devices like smart thermostats, smart speakers, smart watches and many more devices that help an investigator in gathering evidence from the IoT devices and the sensors. The evidence gathered can reveal important details about the actions performed using the device and finding out who originated the attack.

1.1.4 Digital Evidence

The term digital evidence refers to any data or information that is stored, transmitted or received by any digital device and is useful during an investigation. This means that digital evidence can be obtained whenever any electronic device is acquired in an investigation. Digital evidence can not

only be collected from smartphones, laptops, and computers, but any digital device be it a television, a Personal Digital Assistant (PDA) or gaming consoles. All such devices can prove to be important sources for extracting digital evidence. The important features of digital evidence are as follows [7]:

- Is hidden like DNA and fingerprints
- Can cross jurisdictional borders
- Can be modified and damaged quite easily
- Is time sensitive

1.1.5 Handling Digital Evidence

The proliferation of the number of electronic devices means that the volume of digital evidence obtained will be huge. As stated before, computers, laptops and mobile phones are not the only digital devices that need to be analysed. Removable storage media and CD or DVDs are equally important. Hence, handling such huge volume of extracted digital evidence needs to be done in a proper manner. The core points in handling digital evidence are [8]:

- Evidence should be acquired in such a manner that the integrity of the evidence is maintained.
- The forensic investigator examining the digital evidence should be well trained.
- All the processes related to collecting, preserving, examining, reporting and storing of the evidence should be well documented. This makes it easy to maintain a chain of custody.
- The forensic investigator should follow standard methodologies while collecting and examining the evidence, so that the results are acceptable during legal proceedings.

1.1.6 Internet of Things (IoT)

The term “Internet of Things” is not new as it was introduced by Kevin Ashton in 1999 while working at Procter & Gamble. Kevin wanted to present a new technology to the management that was about RFID and he named the presentation “Internet of Things” as Internet had gained quite a lot of popularity in those days [9].

The idea of IoT then started to rise in 2010 and has been on the rise till date. According to Gartner, utilities will be one of the highest endpoints in IoT in 2020 reaching 1.37 billion endpoints

which is an increase of 17% compared with 2019 that included 1.17 billion endpoints [10]. Figure 1-2 shows the increase in the number of connected devices by the year 2025.

The Internet of Things comprises of a number of devices that are connected with each other and the Internet. A formal definition for IoT as such does not exist, so Gartner defines IoT as [11] *“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.”* These devices vary in shapes and sizes and include smart watches, smart refrigerators, smart thermostats, smart locks, smart motion sensors, smart microwaves and so on [12]. These connected devices share and collect data through the network that they are connected with.

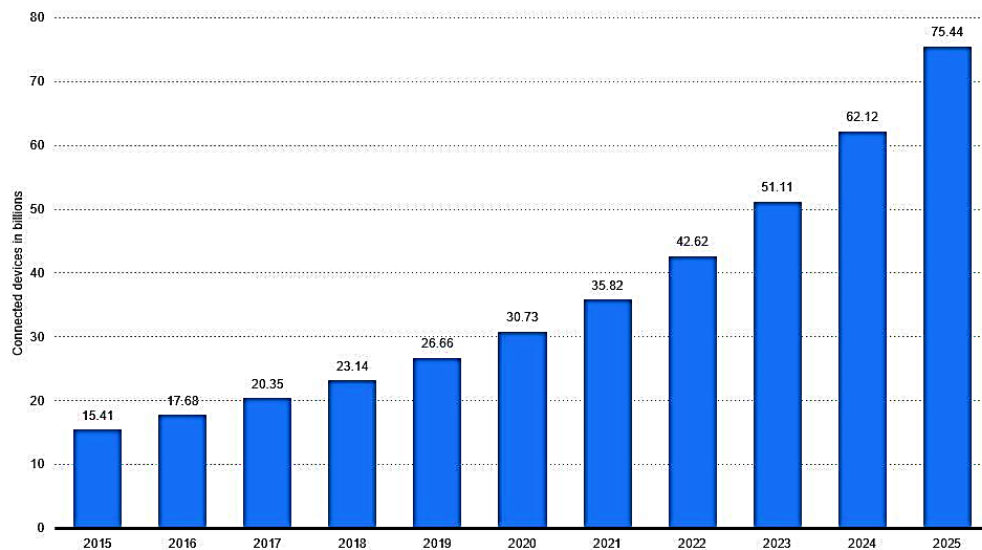


Figure 1-2 Number of IoT devices by 2025

1.1.7 Characteristics of IoT

With the proliferation in the number of connected devices, the IoT system has grown enormously and can now be segregated into different domains. Each domain has its own specific characteristics that differentiates it from the other. However, some of the general characteristics can be identified as follows [13] [14]:

1) Connectivity

Connectivity ensures that all the IoT devices are connected with each other which provides compatibility and also ensures network accessibility. It is this feature which makes it possible to add new IoT devices that can be connected through the network.

2) Dynamic Nature

IoT devices have been designed to collect and transmit data about their environment that changes according to a change in the environment such as temperature, and location, as well as state changes like on and off.

3) Sensing

IoT devices contain sensors that enable these devices to interact and collect data from the environment.

4) Heterogeneity

There are various types of IoT devices and each of these devices have been designed with a particular hardware and software system. One of the important factors when designing a heterogeneous device is to assure interoperability.

5) Intelligence

The IoT devices have been designed in such a way that these devices contain software, hardware and algorithms that make them smart. This allows the devices to carry out certain activities and respond according to the situation.

1.1.8 IoT Architecture

As the IoT environment has evolved, a number of different architectures have been proposed by researchers. There is no standard architecture for IoT, although the most basic architecture comprises of three layers. These three layers are the perception, network and the application layer [15]. Figure 1-3 shows the architecture.

1) Perception Layer

The perception layer contains sensors that are responsible for collecting information whenever a change is detected in the environment. These sensors also detect other IoT objects that are in the environment.

2) Network Layer

The network layer is responsible for assuring that the IoT devices are connected to the network and the servers. This connectivity makes it possible to transmit and receive data.

3) Application layer

This layer includes all the applications where IoT is used such as smart homes, smart cities, smart agriculture, smart health and many more. The application layer is the layer that provides the user with particular services.

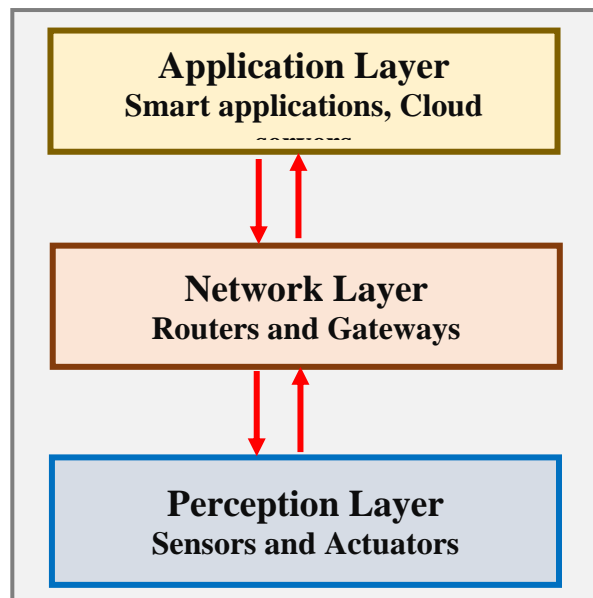


Figure 1-3 IoT Architecture

1.1.9 Security challenges in IoT

The three basic security requirements that should exist in all secure systems can be defined through the CIA triad which stands for Confidentiality, Integrity and Availability. However, there are additional security requirements such as non-repudiation, authenticity, authorization which are needed to ensure maximum security for a system. Unfortunately, since IoT devices are different from traditional systems, the security requirements differ for these IoT devices [16]. This means that the security measures deployed in these devices will be specific to a certain type of IoT device, due to the heterogenous platforms. As a result, this exposes IoT devices to different types of threats and attacks, as it is difficult to implement specific security measures for each type of IoT device.

In the first half of 2019, 100 million attacks were detected on IoT endpoints which demonstrates that IoT devices are vulnerable and can be compromised. The most popular types of attacks are Mirai (39%) and NyaDrop (38.6%) which is also a type of Mirai attack. Mirai attacks can then be used to launch Distributed DoS attacks which can hinder the functioning of the IoT device [17]. The increasing number of connected devices means that the percentage of attacks will continue to rise in the near future as each device will have its own vulnerabilities that needs to be catered for.

1.1.10 IoT Forensics

The crimes involving IoT devices are increasing rapidly because IoT devices have become quite integrated into one's daily live. This change can be easily observed as not only one's room is equipped with smart devices but different types of smart devices can be found in the kitchen, smart locks have been installed in doors, smart cameras and doorbells on the main doors, smart plugs and the list goes on. This complicates the situation as the IoT devices will be connected to a single home network and the compromise of one device means that all other connected devices will also be vulnerable to an attack. This is where IoT forensics comes into play.

IoT forensic includes processes that are carried after an attack has been carried out that involves IoT devices. These processes contain multiple steps that help a forensic investigator to identify the devices that have been compromised, be able to collect evidence, interpret the gathered evidence, present the findings and then finally preserve the evidence for future use [18].

1.1.11 Challenges in IoT Forensics

IoT forensics brings with it a multitude of challenges that have been discussed in the existing literature. These challenges often tend to complicate and present difficulties during an IoT forensic investigation [19] [20]. Figure 1- 4 illustrates the challenges faced in IoT forensics. The challenges faced during an IoT forensic investigation are as follows:

Types of devices

An IoT forensic investigation will contain multiple devices. These devices will not only include IoT devices but will also include computers, laptops, mobile phones, tablets or any other digital device that was connected with any IoT device.

Number of devices

The rise in the number of connected devices means that IoT forensic investigations will comprise of a number of IoT devices unlike traditional digital forensics that includes computers, mobile devices and different storage mediums.

Quantity and type of data

As IoT forensics encompasses different categories of devices, this introduces difficulties because this means that each device will have its own operating system and will operate differently, so finding evidence will not be easy as data will be stored differently on each device. Moreover, this also means that the data formats of each device will be different, hence a forensic investigator should be able to understand those data formats.

Storage in IoT devices

IoT devices have limited storage capacities, so it is highly possible that data will be overwritten at some point. This adds a layer of difficulty in the investigations because this means that important data could have been deleted which might have been helpful for the investigation.

Cloud storage

The data that is generated from an IoT device is also stored on the cloud servers with which they are connected. The cloud servers will be located in different locations and data of many users might be stored together. Different locations will introduce jurisdictional problems and separating each user's data is not an easy task as there is a possibility of modifications or deletions during this process.

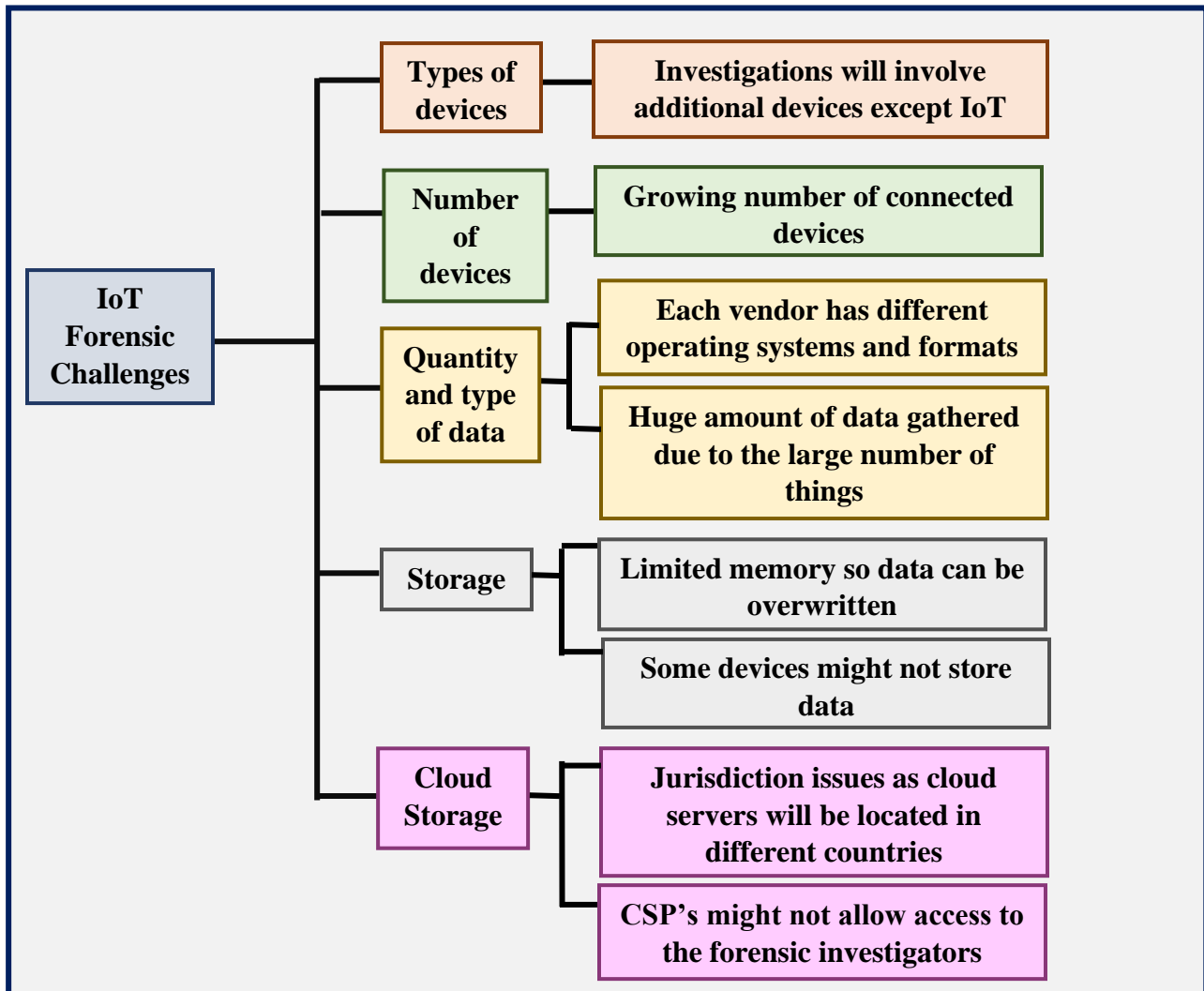


Figure 1-4 Challenges in IoT forensics

1.1.12 The need for an appropriate IoT forensic framework

The rise in attacks involving IoT devices requires an investigation to be carried out such that the culprit who carried out the attack is identified properly. Recent attacks involve an attack where a smart home setup by a couple based in Milwaukee was hacked by an adversary in September 2019. The attacker had gained access to the video system and used it to play inappropriate music at a very high volume. The attacker was also able to gain access to the smart thermostat and was able to change the thermostat's temperature. Another attack was carried out in December 2018 where a wireless baby monitor was compromised and the attacker used this to scare the parents that their baby had been kidnapped [21]. The investigation that is being done will comprise of certain steps

that are part of a forensic investigation framework. The steps that are included in the framework should be such that an investigator is able to obtain all the valuable evidence without the evidence being modified or deleted and also be able to maintain a record of all the steps that were carried out to avoid any issues that might arise during the legal proceedings. This can be possible only if the forensic framework that is being followed is appropriately designed and verified so as not to introduce any problems in the investigation.

1.2 Motivation

The number of connected devices has increased exponentially especially during the past couple of years. In fact, the total number of connected devices is more when compared to the number of people. This escalation has only been made possible because people have started using IoT devices to perform their everyday tasks transforming cities and homes into smart cities and smart homes. Hence, IoT devices have become quite ubiquitous, allowing users to be connected with their IoT devices, even remotely.

The connectivity feature of the IoT devices can be exploited and multiple devices can be compromised at any given time. This compromise can allow the attacker to access the device and change the settings or malfunction the device, so that it stops working. Thus, any compromise means that a forensic investigation needs to be performed to reach the culprit. This forensic investigation will involve collecting evidence from the IoT devices as well.

In order to carry out the IoT forensic investigation, the forensic examiner will need to follow a well-structured forensic framework as it will provide assurance to the examiner that all the evidence has been collected and interpreted in a reliable way. Following the framework will also make it easier for the examiner to present his findings and conclusions in the court of law.

1.3 Research Questions

This research is aimed at providing a generic forensic framework for the digital forensic investigators. For the digital forensic investigators and readers, the following research questions will be answered in this work:

- Is the proposed framework generic or designed for a specific type of IoT device?
- Has the proposed framework been tested and verified on any IoT device?

- Will the forensic investigator be able to gather evidence by following the framework during an active investigation?
- Can the forensic investigator perform additional tasks during the investigation or does one need to follow only the steps defined in the framework?
- Does the framework address chain of custody and evidence integrity?

1.4 Problem Statement

The field of IoT forensics is an understudied area and relatively few IoT forensic investigation frameworks exist to assist the investigators. The number of crimes involving IoT devices is increasing with the increased usage of IoT devices. This rise in the rate of attacks on the IoT devices means that the forensic investigator will need to adhere to proper forensic investigation frameworks that will enable the investigator to gather the evidence required for the investigation and at the same time be able to create a timeline of when, how and who was responsible for the attack.

1.5 Goals and Objectives

The goal of this study is to aid forensic investigators and examiners in conducting investigations that involve IoT devices.

The objective of this research is to provide forensic investigators and examiners with a proper forensic investigation framework that will make it easier for the forensic investigators to find the culprit and justify their findings in the court of law. Moreover, it will also enable other forensic investigators to see the processes that were carried out during the entire investigation.

1.6 Intended Audience

The audience for this research involves forensic investigators and end users. The forensic investigators will be the main entity that most benefits from this research as this research provides these investigators with a step by step guideline on how investigations involving IoT devices should be carried out. In addition, it also tells investigators where the artifacts are to be found and how they should be extracted. The benefit that the end user will gain from this research is that they will know how much data about them is stored and can be retrieved during forensic investigations.

1.7 Organization of the Thesis

The thesis is organized into eight different chapters all of which contain multiple sections and sub – sections that each contain information about the research conducted.

Chapter 1 “Introduction” contains the historical background that will help researchers to develop a basic understanding about the domain. In addition, this chapter includes the motivation for carrying out this research, the problem statement, the goals and objectives and finally the intended audience for this research.

Chapter 2 “Literature Review” contains the differences between frameworks, methodology, architecture and processes. The chapter also includes existing work done in the domain.

Chapter 3 “Research Methodology” contains the research methodology followed along with how each of these steps were executed.

Chapter 4 “Experimentation” contains the devices that were used with their specifications. Details on how data was collected for this research is also present.

Chapter 5 “The Proposed Framework” contains the framework in detail which includes all the steps in the framework. It entails on how each step in the framework was carried out.

Chapter 6 “Results and Discussion” includes the comparison between the existing and the proposed framework.

Chapter 7 “Conclusion and Future Work” concludes the thesis and also contains directions for future work.

Chapter 8 “References” contains the bibliographic sources that were used.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents the prior research work conducted in the area of IoT forensics, specifically focused on existing IoT forensic frameworks. This aids in building a base for this research and comprises of recent research in this domain. This chapter contains the following contents:

Section 2.2: Differentiating between frameworks, methodology, architecture and processes

Section 2.3: Analysing IoT forensic frameworks

Section 2.4: Examining Google Home

2.2 Differentiating between frameworks, methodology, architecture and processes

This research is aimed at developing a generic and a comprehensive IoT forensic framework that will serve as a guideline for forensic investigators, allowing them to acquire all the important evidence that will identify the right culprit. It has become increasingly important to design such a framework as it will provide a standard way for the forensic investigators for carrying out investigations. Moreover, a framework provides interconnectivity between different components that are included and can also be modified depending on the current scenario. The table below lists the differences between frameworks, methodology, architecture and processes.

	Framework	Methodology	Architecture	Processes
Definition	Enables an idea, a concept or an architecture to be implemented.	Set of rules, activities, or deliverables that demonstrate on a how a particular problem can be solved.	Gives an overall view which entails the components and modules that are to be incorporated.	Detailed steps that instruct on a how a specific task will be executed.

Objectives	Describes how components will be maintained and involved. It also states the input and output for each component.	Aids in validating the outcome of a research as it presents an appropriate way of how something is to be done.	Represents the design of how an application or a framework is ordered. It defines a logical view but not on how these different components should be deployed.	Processes define the behaviour of the current system by showing the timing of when a step has to be performed and the interdependence between them.
Example	The NIST Cyber Security Framework contains five important components that are Identify, Protect, Detect, Respond and Recover. Each of these components contain additional steps on how each module is to be implemented.	The most appropriate methodology used is known as the design science methodology. Many design science methodologies have been proposed by researchers and can be used based on the scenario.	Enterprise Information Security Architecture (EISA) provides details on the structure and behaviour of an organization's security processes It provides solutions for business, information and security.	The processes that can help an organization to maintain security are maintaining audit information, deploying firewalls and IDS, having appropriate incident response plans.

Table 2-1 Differences between frameworks, methodology, architecture and processes

2.3 Analysing IoT forensic frameworks

IoT forensics is a relatively new and developing domain, hence the reason that much research work has not yet been conducted in this domain. IoT forensics is becoming increasingly important as the use of IoT devices is on the rise. Research has been conducted on IoT devices but little importance has been given to how Digital Forensic investigation techniques can be incorporated in IoT-based scenarios. This has been mainly because existing digital forensic techniques are incompetent with the nature of IoT devices, making it difficult to acquire and present the evidence

during court proceedings. The existing research work shows that little effort has been made on developing a standard framework for IoT forensic investigators.

The authors in [22] propose an IoT based digital forensic model. The model starts with the planning stage. Planning involves obtaining a warrant and proper authorization to start a forensic investigation. The investigators then identify the base device and how it communicated with the other devices. The next step is to extract the data from routers, gateways and the cloud environment known as the triage examination. Once the evidence is collected, it is analyzed, processed and reported, and finally stored. However, the proposed model has not been tested on a real scenario and also does not address privacy concerns.

In [19] the authors highlight the fact that IoT consists of different domains which include the cloud environment, mobile device, sensors, fixed computing and networks. Based on this, a 1-2-3 zone approach is proposed which is combined with a Next-Best-Thing (NBT) triage model that can be used with the zone- based approach. Zone 1 is the internal zone that includes all the software, hardware and the networks. Zone 2 contains the devices at the border of the network and also serves as a medium for internal and external networks, while zone 3 has all the hardware and software that are outside the network.

The IoT forensic investigation methodology in this research contains of four phases that are preparation, acquisition, investigation, reporting and storage. Preparation involves all the security requirements that are made before an incident occurs. It includes the setting up of security software and also determining attack and possible evidence location. Acquisition is the step where the data is acquired from the IoT devices. The proposed NBT model is used in the investigation stage which facilitates in collecting evidence from devices that were directly connected or were connected at some point before being removed. In this stage, a report is prepared based on the obtained evidence which is then presented to the concerned authorities. Finally, the evidence is stored for future reference. A major drawback of working with the zone approach is that it only identifies where possible evidence can be found, but does not state the processes on how that evidence can be collected.

Malek and Asif [23] proposed a theoretical framework that is built on the forensic models proposed in [19] [22]. This theoretical framework comprises of a LoS (Last on Scene) algorithm that enables to identify the last thing that was involved in any kind of communication. Once the

LoS algorithm is executed, different zone investigations need to be done. Then the digital forensic procedure is to be carried out which contains multiple steps. These steps outline the evidence that has to be collected, the tools used for investigation, making a backup of the evidence and presenting a report after obtaining the results. The model needs to be verified and tested based on the LoS algorithm and legal consideration also needs to be integrated for the digital forensic procedure.

Victor and Indrakshi [24] developed an IoT forensic framework that was generic and detailed, hence could be mapped to any investigation involving IoT devices known as Digital Forensic Investigation Framework (DIFF-IoT). The proposed framework is divided into three components namely, proactive process, IoT forensics and the reactive process and also includes processes that run simultaneously. The proactive process involves multiple sub-processes to be taken before an incident occurs. The reactive process incorporates tasks that are concerned with initializing, identifying, collecting, analyzing and then finally reporting the evidence. The concurrent processes include obtaining authorization to carry out investigation, maintaining chain of custody and physical investigation to link the processes. However, the framework has not been tested and verified yet.

Victor et. al. [25] modified the framework that was proposed in [24] by adding new components. These components included: 1. Things, 2. Device Connectivity and Communication 3. IoT Management Platform, 4. IoT Policy and 5. IoT Standards and protocols. The things in IDFI-IoT could be an object or a device that transmits data over the network. The Device connectivity includes sensors or devices that are connected through WiFi, Bluetooth, cellular connection or so on. IoT Management Platform allows the connectivity of the devices. IoT policies define how organization should carry out IoT related tasks. There are no accepted IoT standards but the framework uses existing ISO standards that have been designed for Digital Forensics. Unfortunately, no implementation has been carried out, thus the framework has not been evaluated to identify important forensic features.

Tanveer, Peng and Weili [26] focused on developing a model that integrates digital and application forensics for the three most popular IoT applications. These three applications include smart home, wearables and smart city. The proposed model contains three different components that are Application-Specific Forensics, Digital Forensics and Forensics Process. The application

specific forensics is for a particular application that involves extracting data without causing any data destruction. The digital forensic procedure involves network, cloud and things forensics. Finally, the forensic process will involve the traditional approach on evidence identification, collection, preservation and chain of custody. The proposed model hasn't been applied in this research.

In [27] a framework is proposed that can help a forensic investigator to collect important artifacts from different IoT devices. Two different applications were developed that included an Android application and a desktop application. The Android application was designed to help users extract artifacts from the mobile phone, while the desktop application was created to build a timeline by combining artifacts of different formats. The framework was tested in two different scenarios that were smart homes and smart factory with a 3D printer. The artifacts of the IoT devices in the smart home were obtained from the smartphone using the application developed. In the smart factory scenario, Arduino was used to collect data from the sensors. The desktop application was then used to parse the data obtained from both the scenarios that resulted in a timeline of the incident. Although, the framework proposed does claim to obtain data from the cloud and the network but the use case used to test this framework doesn't give any detail on how evidence was collected from the cloud and the network. Furthermore, no figure has been given of the framework, so there is no information of the components that are included in this framework.

In [28] the authors proposed a holistic digital forensic readiness framework which is based on the ISO 27043 standard. The readiness process in digital forensic investigation comprises of all the processes which makes sure that an organisation can use the digital forensic evidence properly. The IoT-FR contains individual processes. The first is the organisational process that ensures that IoT digital forensic readiness is applied in a consistent manner throughout the organisation. The next is the readiness process that allows all important and likely digital forensic data to be identified, gathered and stored based on the guidelines in the organisational processes. The IoT security layer process assures the security of the IoT and the digital forensic data by implementing the security requirements such as confidentiality, integrity and availability. The authors discussed a use case using a FitnessMe campaign designed for the research. As, the authors themselves state the limitation that the proposed framework has not been implemented with a real organisation.

The table 2-2 summarizes all the limitations that exist in the frameworks already proposed that have been discussed in this section.

Reference	Framework	Limitations
[19]	Internet of Things forensics: Challenges and Approaches	<ul style="list-style-type: none"> ▪ Only identifies where possible evidence can be found but does not state the processes on how that evidence can be collected.
[22]	Internet Of Things (IoT) Digital Forensic Investigation Model: Top- Down Forensic Approach Methodology	<ul style="list-style-type: none"> ▪ The proposed model has not been tested. ▪ Does not include evidence analysis, documentation, reporting and presentation processes.
[23]	An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I: A Theoretical Framework	<ul style="list-style-type: none"> ▪ The model needs to be verified and tested based on the LoS algorithm.
[24]	Digital Forensic Investigation Framework (DIFF-IoT)	<ul style="list-style-type: none"> ▪ The framework has not been tested and verified
[26]	Application – Specific Digital Forensics Investigative Model in Internet of Things	<ul style="list-style-type: none"> ▪ The proposed model has not been applied and verified in this research ▪ Only possible data that can be collected has been mentioned.
[27]	A Framework for IoT Data Acquisition and Forensics Analysis	<ul style="list-style-type: none"> ▪ No detail on how evidence was collected from the cloud and the network. ▪ No figure has been given of the framework, so there is no information of the components that are included in this framework.
[28]	IoT Forensic Readiness Framework	<ul style="list-style-type: none"> ▪ The proposed framework has not been implemented with a real organization.

Table 2-2 Limitations in the existing frameworks

2.4 Examining Google Home

Google Home is a smart speaker introduced by Google. It works by allowing the user to give commands using their voice and then responds to the given commands. Google Home was originally released in November 2016 but then later on in October 2017 Google Home Mini and Google Home Max were released [29]. Since the Google Home Mini has not been around for

very long, quite little work has been done on it especially in the digital forensics domain which was one of the main motivations for choosing it.

Ilkan, Erkan and Mehmet [30] analyse the two most used smart speakers that are Google Home and Amazon Alexa. Forensic and anti-forensic activities were performed with these speakers to examine what data can be retained by the associated applications. Different use cases were performed and then the digital evidence was extracted. It was seen that Google Home and Amazon Alexa maintain a history of all the activities performed by the user on the mobile and the web applications. The time of each activity and the response from both the speakers are also recorded in the history. The research done provides little information as the devices and the mobile applications have not been investigated for both the speakers.

In addition, Steven [31] also analysed the Google Home and the Amazon Echo smart speakers. Google Home Mini was used along with its companion Android Application. Different commands were given to the Google Home Mini which included setting up reminders, alarms and controlling other devices to populate data. The next part was to extract and examine the data from the application. The analysis of the Google Home application revealed the email address linked with the device. Further analysis showed the reminders that were set, the time, date, day, location and the occurrence of the reminder. The client side in the cloud environment was analysed and it was seen that Google stores all the commands that are performed using the Google Home Mini. The commands stored contain the day, time, location and the text transcription of the command. The major drawback of this research was that forensic analysis that was conducted on Google Home Mini was not detailed and was also missing device and network analysis.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

Research methodology is the specific process that is followed while conducting a research as it allows to collect and evaluate the data that enables the researchers to reach to a conclusion. This chapter discusses the research methodology that was followed for this research. It contains the following sections:

Section 3.2: The Research Process

Section 3.3: Steps of the Research Process

3.2 The Research Process

Conducting a research to produce fruitful results can only be possible if researchers follow a well-defined process throughout the research. Over the years, researchers have proposed various research methodologies that can be and have been followed by researchers to successfully conduct their research. The research process contains different steps that assist in finding the results in a particular research. The research process that was followed contains the following steps listed below:

- 1) Identifying the research problem
- 2) Literature review
- 3) Purpose of the research
- 4) Designing the framework
- 5) Collecting data
- 6) Extracting and analysing evidence following the framework
- 7) Presenting the results

The following research process has been taken from the book “Educational Research” [32]. However, the process has been tweaked in accordance with the research although majorly it includes the steps that were in the original research process. Figure 3-1 shows the research process.

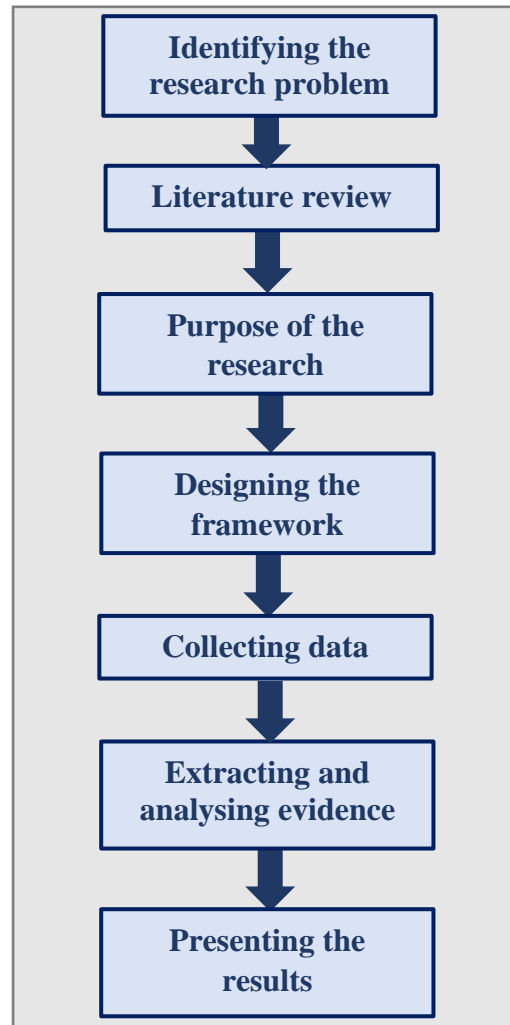


Figure 3-1 Research Process

3.3 Steps of the Research Process

This section contains all the seven steps that were involved in the research process along with the details on how each step was executed. Any sub-phases that were a part of the step is also included in the details.

3.3.1 Identifying the research problem

Before any research can be conducted, the first and the foremost thing that needs to be done is to define a domain that is of interest to the researcher. Once the domain has been identified, the next task for the researcher is to explore that particular domain thoroughly to further narrow down the area that can be explored in that domain. One of the ways that this can be done by the researcher is by finding areas that have minimal research work done in that domain so that the researcher can find problems which they can address through their research.

The same procedure was followed for this research to find out the research problem. The domain of interest for this particular research was “IoT Forensics”. The next phase was then to find out the area in IoT forensics that have had little research carried out. For this, an in-depth analysis was undertaken and it was found that the domain “IoT Forensics” is itself an under explored domain as IoT has become common in the past few years. Furthermore, narrowing down to the research problem, results showed that adversaries have started to take advantage of these IoT devices to launch attacks. According to a report published in Forbes, security researchers at F-Secure found that there has been an increase in the attack traffic leading up to 2.9 billion events in 2019 [33]. This meant that forensic investigators needed to conduct investigations to reach to the culprit and to do this efficiently a standard framework would be needed to extract evidence that can be justified in court proceedings. An in-depth examination showed that a handful of researchers have proposed such investigative frameworks that can be further improved aiding investigators in extracting all the relevant evidence. Figure 3-2 shows the phases in identifying the research problem.

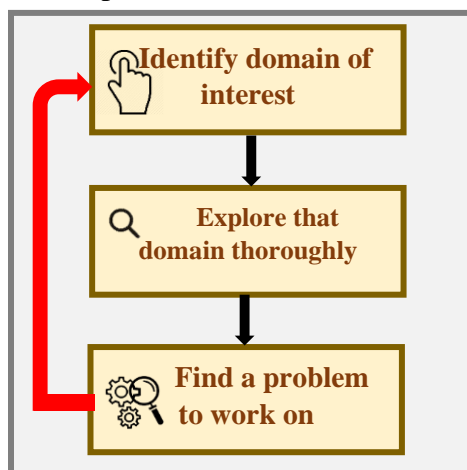


Figure 3-2 Identify a research problem

3.3.2 Literature review

After the identification of the research problem, the next step is to study the existing literature that gives a detailed picture of the work that has already been done. This helps find out the gap that can be filled with further research. In addition, it also prevents researchers from carrying out the same research work that has already been done before.

The literature review in this research was done by first finding research papers (from last 10 years) that are related to the problem. After this, the abstract and the conclusion were read for each paper to find out the most relevant papers and those papers were shortlisted. These shortlisted papers were studied thoroughly and helped in building this research. The detailed literature review can be found in Chapter 2.

3.3.3 Purpose of the research

The purpose of the research can be best described by focusing the research on solving a specific problem in a specific domain. The purpose of this research is to propose a generic IoT forensic framework to aid investigators in carrying out investigations and falls in the domain of IoT forensics. Furthermore, the purpose statement can be further narrowed down by formulating research questions. The research questions of this work can be found in Chapter 1.

3.3.4 Designing the framework

The outcome for this particular research was to propose an IoT forensic framework, hence the most important part was designing that framework. It was of utmost importance that the framework was designed appropriately as this framework had to be followed throughout the research.

- The first step in designing the framework was to study existing frameworks that had been proposed and how each process was carried out in that framework. This was done through literature review and summaries of all those frameworks were written simultaneously.
- The next step was to find flaws in those existing frameworks that could be improved by this research. Finding flaws was done by pointing out processes that were missed in those frameworks and could prove essential during an investigation. These missing processes could be added in this framework. This included an in-depth study of how forensic

investigations are carried out. It involved looking at ISO standards that are designed for forensic investigations and the processes that are part of those standards.

- After finding flaws, the framework was designed that included processes from the previous framework as well as the new processes. The detailed framework is discussed in Chapter 5.

3.3.5 Collecting data

Once the framework had been designed, an IoT device needed to be picked for testing the framework. The first choice for an IoT device was a mesh Wi-Fi system as suggested by this article [34]. The most popular mesh Wi-Fi system was that of NETGEAR Orbi, however due to its unavailability in Pakistan, the next most used mesh router Google Wi-Fi was procured. Unfortunately, after multiple unsuccessful attempts of setting up the router, the switch to Google Home Mini was made. The issues faced during setting up the Google Wi-Fi router included compatibility problems as the device had not been manufactured in Pakistan.

Google Home Mini was the IoT device that was used in this research. The device was setup using the Google Home mobile application and was used to perform different activities that helped in collecting data for this research. Data collection using Google Home Mini is discussed in Chapter 4.

3.3.6 Extracting and analysing evidence following the framework

The next step in this research was to extract and analyse the evidence by following the proposed framework. As stated before, data was collected by performing different activities using the Google Home Mini which meant that data of the user would be stored by the mobile application, on the cloud and would be transmitted through the network when the user was using the device. This data that can be classified as evidence in the forensic world needs to be obtained by the investigator, so that analysis can be performed and a conclusion is reached. Moreover, the investigator needs to gather all the evidence to justify his conclusions in court proceedings.

The framework was followed and evidence was obtained from different domains that included the mobile, the network and the cloud. Once all the evidence was gathered, this evidence was analysed manually and important information was found such as user names, email addresses, timestamps and so on. The details on extraction and analysis can be found in Chapter 5.

3.3.7 Presenting the results

After all the experimentation had been done, the final and the most important part of this research was to present the results and the findings. The results for this research can be divided into two categories which are as follows:

- The first category of results was the extraction and analysis of the evidence that has been done by following the proposed framework. This can be found in Chapter 5.
- The next category of results was comparing the proposed framework with existing frameworks to see the improvements that the proposed framework provides. This comparison can be found in Chapter 6.

CHAPTER 4

EXPERIMENTATION

4.1 Introduction

This chapter will focus on the tools that were used for experimentation and also on how these tools were setup to conduct the research. The following sections are included in this chapter:

4.2: Specification of the devices

4.3: Tools and Technologies

4.4: Data Collection

4.2 Specification of the devices

In this research, three different devices were used. These devices comprised of a smart speaker, in particular Google Home Mini, a mobile device and a computer which was the forensic workstation for this research. The specification of these devices are listed as follows:

4.2.1 Google Home Mini

Model: Google Home Mini H0A

Device ID: A4RH0A

4.2.2 Mobile device

Model: LG Nexus 5x

Android 8.1.0

4.2.3 Forensic Workstation

Lenovo ideapad 330 Core i5

RAM 8GB

4.3 Tools and Technologies

Different software programs were required to be used during the research as and when needed. The tools that were used for the smartphone and the forensic workstation are discussed in this section.

4.3.1 Mobile Device

- Google Home Mini Android Application
- Magisk Manager
- TWRP
- Root checker

4.3.2 Forensic Workstation

- Microsoft Windows 10 (64 bit)
- Android Studio
- Java Development Kit (JDK) v13.0.1
- Wireshark
- DB Browser for SQLite
- Netcat 1.11
- Autopsy 4.13.0
- Epoch Convertor

4.4 Data collection

Data collection is one of the most important and crucial process while conducting research. This is because the results are obtained by working on the collected data. Unlike other research domains, where the data that is collected is used for modeling, running simulations or is put to test using different algorithms, data collection for a forensic research largely relies upon how the collected data can be extracted from different sources. The extracted data then undergoes a thorough investigation where different attributes of that data are examined and analysed. Similarly, since this research is focused on the forensic domain, data collection was done by using an IoT device, namely the Google Home Mini smart speaker. This section entails how the Google Home Mini was setup and the different use cases that were performed by using the smart speaker.

4.4.1 Setting up the Google Home Mini

The first step in setting up the Google Home Mini was to download the Google Home application from the Google Play store. Once the application was downloaded, the Google Home application was opened. The following steps were followed for setting up the smart speaker:

The first step was to link an account with the Google Home. The Google Home application gives an option of the account to which the Google Play store is already linked but any other email account can also be added. It is important that only a google account is given because any other account will not be accepted such as Microsoft or Yahoo.

After adding the account, Google Home needed to be setup. The device was automatically detected and the address and the nickname were then added. The device then needed to be connected with the Wi-Fi network. Some issues were faced while connecting the speaker to the current Wi-Fi network as shown in figure 4-1. Hence, the speaker was then connected with another Wi-Fi network that worked.

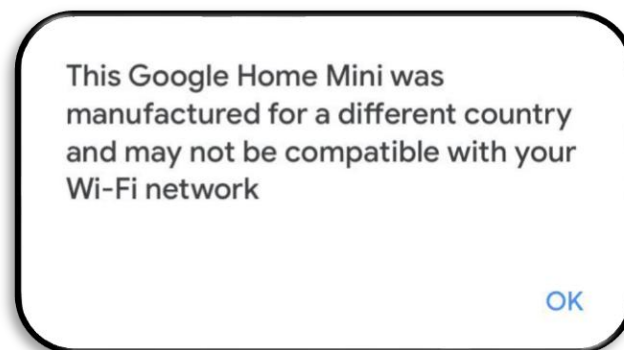


Figure 4-1 Wi-Fi connection error

- The final step was to then train the Google Home with my voice, so that Google Home can recognize me each time I send a command. This was done by saying a sample command three times after which the training was complete. Once the training was complete, the Google Home Mini was ready to use.

4.4.2 Performing use cases

There are a multitude of commands that can be given to the Google Home. These commands can be used to create data or to collect data which can then be used for the research. Similarly,

commands were given to the Google Home Mini smart speaker that was used for this research. These commands were then executed by the smart speaker. The commands that were given can be seen in the table. These commands are categorized into different use cases.

Sr.No	Use Cases (Commands)
1.	Asking a set of questions which included: <ul style="list-style-type: none"> ➤ The current location ➤ The current time or time in any other place ➤ The weather in a specific city or country ➤ Getting updates about the traffic conditions ➤ How to make a certain recipe ➤ Asking Google Home Mini questions about specific topics ➤ Asking Google Home Mini the latest news
2.	<ul style="list-style-type: none"> ➤ Setting up alarms and deleting an alarm ➤ Setting reminders and deleting reminders ➤ Setting calendar events and deleting calendar events
3.	<ul style="list-style-type: none"> ➤ Turning the volume up or down ➤ Pair Bluetooth
4.	Creating shopping lists <ul style="list-style-type: none"> ➤ Adding items in the shopping list ➤ Deleting items in the shopping list ➤ Asking Google to tell the items in the shopping list
5.	Asked recommendations: <ul style="list-style-type: none"> ➤ Best restaurants to visit ➤ Best tourist spots to visit ➤ Restaurants to visit ➤ Recommended movie and seasons to watch ➤ What should I have for breakfast, lunch or dinner ➤ Where should I go for the weekend ➤ Where should I spend my vacations
6.	Google Home Mini speaker can remember information and can be asked later. This included: <ul style="list-style-type: none"> ➤ Name ➤ Favourite colour ➤ Favourite food

	<ul style="list-style-type: none"> ➤ Favourite book ➤ Where important belongings are kept
7.	<p>Google Home Mini can also entertain. Commands that were given were:</p> <ul style="list-style-type: none"> ➤ Tell a story ➤ Tell a joke ➤ Play music ➤ Tell a riddle ➤ Tell a poem ➤ Sing for me ➤ Tell a quote
8.	<p>Google Home mini was also used to ask some mathematical questions. These were:</p> <ul style="list-style-type: none"> ➤ Count from 0 to 10 ➤ Give a random number between 0 to 100 ➤ Conversion questions ➤ Performing calculations

Table 4-1 Performing use cases

CHAPTER 5

THE PROPOSED FRAMEWORK

5.1 Introduction

This chapter contains an in – depth detail on the framework that is proposed in this research and how each step in the proposed framework was performed. It has the following sections:

5.2: Case for investigation

5.3: Overview of the proposed framework

5.4: The proposed framework

5.2 Case for investigation

In order to test and verify the framework, a case had to be formulated so that an investigation could be carried out by following the proposed framework to ensure that following the framework would give investigators the required evidence and find the real culprit. Since working on an actual case was out of bounds, a case had to be made up and investigations were then carried out on that case.

The case that was made is as follows: *“A Google Home Mini smart speaker and a mobile device were found by the higher authorities. Both of these devices were seized by the authorities and were taken as evidence. These devices were then given to a digital forensic investigator to extract the relevant artifacts that could help reach to the culprit and can be presented in the court of law.”* The case was then investigated in the research using the proposed generic framework for IoT forensic investigation.

5.3 Overview of the proposed framework

The framework that has been proposed in this research is named as **“A Generic Framework for IoT forensic investigation”**. The reason that the framework contains the word generic is because the framework has been designed in such a way that it can be used in investigations that involve any kind of IoT devices as the framework is not based on a specific IoT device, unlike previously proposed frameworks that have been specifically designed for a specific IoT device. Moreover,

previously proposed frameworks did not address the different domains that are involved in IoT that include the network, the cloud and the IoT device itself which have all been addressed in this framework. Adding to this, the frameworks have been very concise which makes it highly possible that the investigator could miss any important artifact during the investigation.

The proposed framework is a comprehensive one and is divided into four major phases. These phases can be seen in figure 5-1 that shows an overview of the complete framework. Each of these phases contain multiple steps that need to be executed as appropriately as possible. These steps further contain multiple sub – steps that need to be followed during the investigation. The reason that the framework was divided into phases was to make it easier for the investigator to separate the different activities during the investigation such as gathering the evidence in one phase and then analysing that evidence in a later phase. The four major phases that are part of this framework are as follows:

- 1. Pre – Investigation Phase** – This is the phase that takes place before the investigation commences. It occurs once a case has been handed over to the digital forensic investigator. This phase includes activities that state on how the investigation should be planned and carried out
- 2. The Acquisition Phase** – In the acquisition phase, the devices that could contain evidence and would prove useful in the investigation are seized or handed to the forensic investigator. The forensic investigator then has the responsibility to acquire and gather evidence, depending on the type of devices. The acquired evidence is then investigated to retrieve crucial artifacts.
- 3. The Investigative Phase** – This phase is one of the most important phases of the entire investigation. This is where the acquired evidence is thoroughly analysed to find important artifacts that could lead the investigator to the right culprit. Once the evidence has been analysed, reports are made and presented during court proceedings.
- 4. Concurrent Phase** – The concurrent phase is the phase that runs in parallel to all the other phases. This phase contains activities that are to be done simultaneously that includes documenting, maintaining a chain of custody and maintaining the integrity of the evidence.

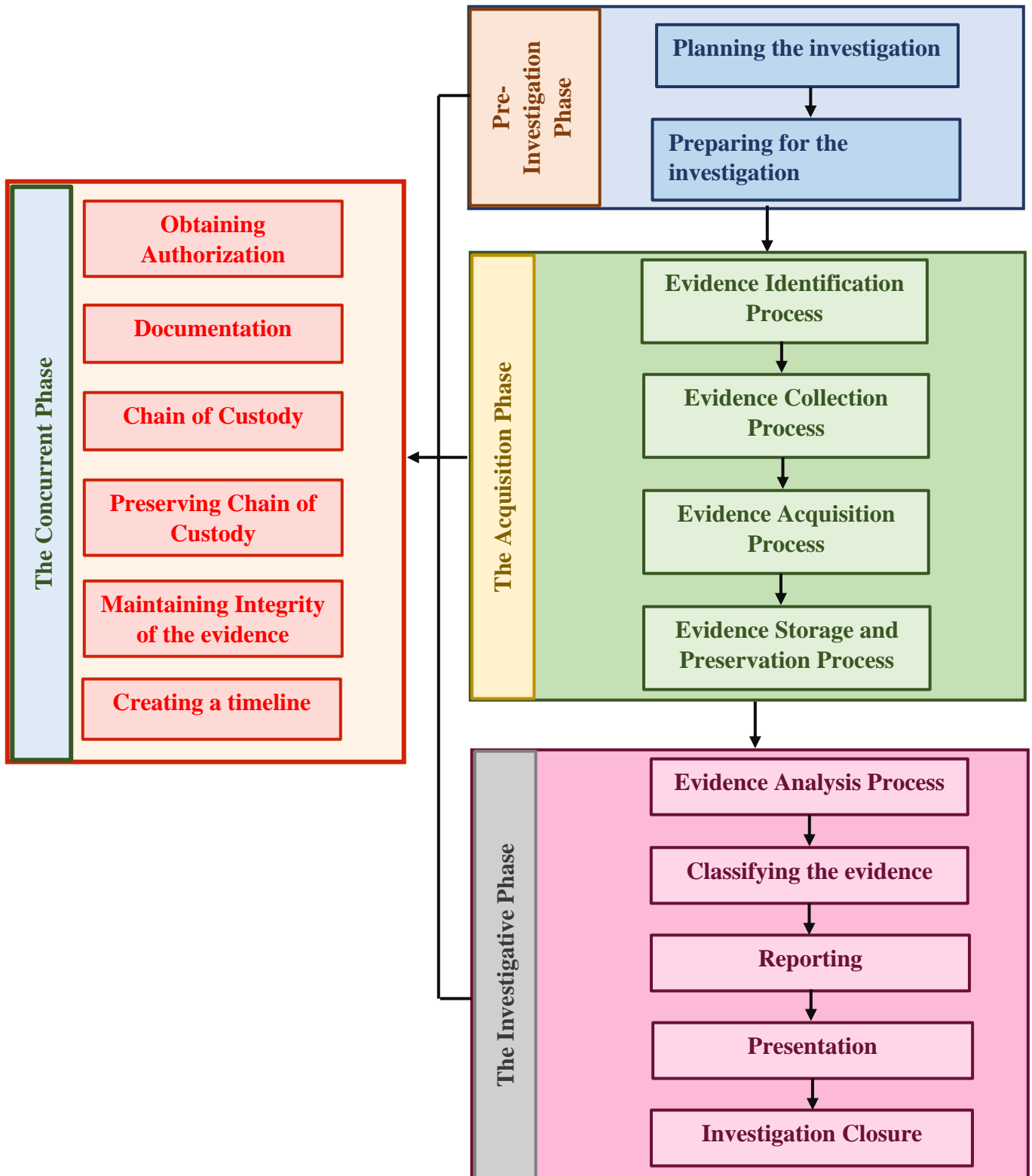


Figure 5-1 Overview of A Generic Framework for IoT Forensic Investigation

5.4 The proposed framework

This sub – section contains details on each step of the proposed framework and how each step was carried out during the case investigation. As mentioned before, the framework is divided into four main phases where each phase contains steps and multiple sub – steps. These four phases and their steps have been discussed in this section in length.

The proposed framework named as “**A Generic Framework for IoT forensic investigation**” has been designed by combining different frameworks that had certain flaws and were missing some crucial steps that were deemed important for the forensic investigation. The missing steps were then included in the proposed framework and once the framework had been completely designed, investigation was then started by following the proposed framework. The complete detailed view of the framework of each phase is shown within each phase.

5.4.1 Pre – Investigation Phase

The pre – investigation phase as stated before is the phase which takes place before the investigation starts and is the first phase in the framework. In this phase, a case has been identified and the next step to take in this phase is to plan and prepare for the investigation in hand. The case for investigation in this framework has already been mentioned in section 5.2. Hence, the next thing that was done was to follow the steps in this phase. The two steps in this phase are planning and preparing for the investigation which were followed in a sequential manner as seen in figure 5-2.

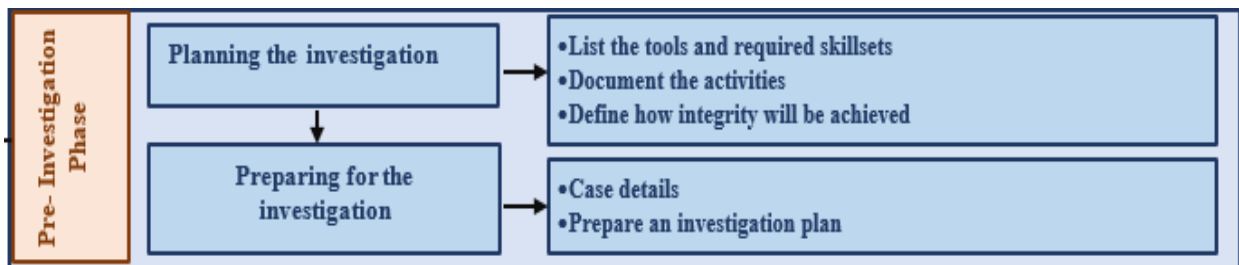


Figure 5-2 Pre – Investigation Phase

5.4.1.1 Planning the investigation

Planning for the digital investigation involved a lot of resources that were needed to carry out the investigation. To proceed with the digital investigation, different tools and special skill sets are

needed for the investigator for an effective digital investigation [35]. The planning for this investigation included the following:

- 1) Listing down all the forensic tools that will be used for the investigation and these tools can be found in Chapter – 4.
- 2) The other important thing that needs to be taken care of is to find the proper skillsets so that the right expertise is available. In this investigation, the primary investigator was me with external help as and when needed that included my teachers.
- 3) All the activities that took place during the investigation were documented so that the process can be repeated.
- 4) In order to maintain integrity of the evidence obtained in the investigation, a copy of the original evidence was used for analysis rather than the original evidence to prevent any wanted or unwanted changes. This included any images and the data packets that were captured.

5.4.1.2 Preparing for the investigation

Once the investigation has been planned, the next step is to prepare which ensures that the infrastructure is appropriate for the investigation [36]. The activities that were part of the preparation stage included the following:

- 1) The first aspect that was considered while preparing for the investigation was the case details.
 - This included finding out the nature of the case which was an unknown criminal.
 - The specifics about the case included details such as the role of the mobile device which was to use the Google Home Mini via the Android application.
 - Other details about the case included the type of evidence which was a mobile device and the Google Home Mini smart speaker.
 - The operating system used was Android.
- 2) The next step was to prepare an investigation plan. This investigation plan further included:
 - Searching should be done according to a well devised plan. In this investigation, the search was centered around finding user related data.
 - Evidence collection should also be planned before evidence is started to be gathered. The evidence collection in this investigation had to be done through the

mobile device, capturing data packets in transit, and collecting evidence from the client's side in the cloud environment. Moreover, evidence preservation needs to be thought beforehand. The evidence for this investigation was stored on the forensic workstation.

- The evidence examination also needs to be planned. In this investigation, evidence can be examined manually and by using tools.

5.4.2 The Acquisition Phase

The acquisition phase is the phase where the data is acquired through different methods depending on the device from which the data needs to be gathered. In this process, forensic images are made from different media such as hard drives, servers, removable hard drives, mobile devices and so on. While forensic images are being made it is important that none of the data alters during the process, as alterations would create challenges for the forensic investigator [37].

The acquisition phase can be performed through various ways and it depends on the needs of the investigation, i.e., which method or a combination of methods could be used. The investigator can use hardware and software tools while performing data acquisition. Some of the methods are as follows:

- 1) Manual Acquisition – In manual acquisition, the forensic investigator uses the user interface to examine the contents on the screen whether it is a mobile device or a computer. The device is examined through the touchscreen or navigated through the menu options and if the forensic investigator finds an item of interest, then the forensic investigator takes a picture of that item to make a record.
- 2) Logical and Physical Acquisition – To acquire evidence logically, a copy is supposed to be made of the logical storage [38]. This acquisition method is commonly used for mobile devices along with the physical acquisition methods which makes a bit – by – bit copy of the mobile device.
- 3) Live Acquisition – Live acquisition process is where evidence is acquired when the system is running as shutting down systems might delete volatile data that could be useful during the investigation. Live acquisition is also commonly used to acquire evidence from the network environment when it is operational [39].

The evidence acquisition phases contains multiple steps that were followed sequentially to acquire evidence for this investigation as seen in figure 5-3. In addition, a combination of evidence acquisition methods were used to acquire the evidence as different domains were involved in this investigation.

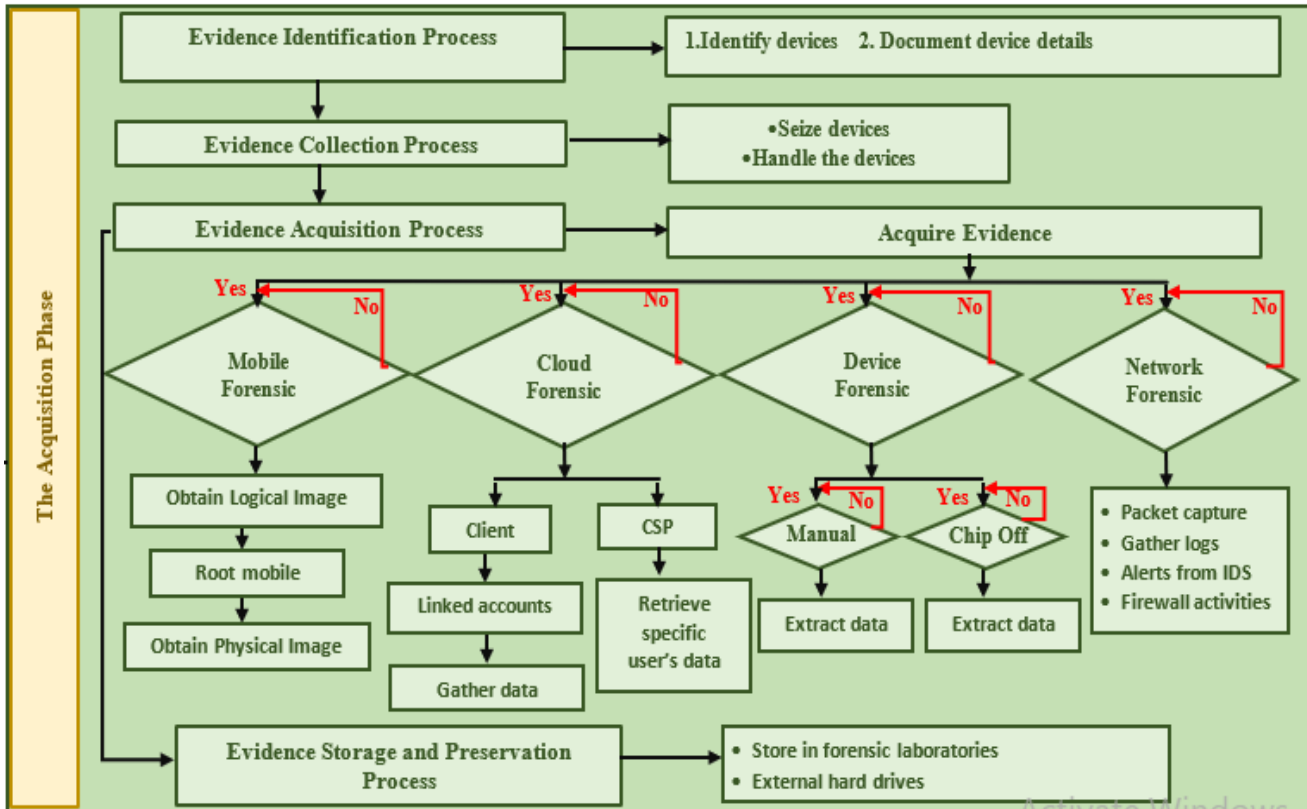


Figure 5-3 The Acquisition Phase

5.4.2.1 Evidence Identification Process

The evidence identification step is where the devices that need to be investigated are identified and their complete details are documented by the forensic investigator or any other personnel that is involved in the investigation. These devices are those that could potentially prove useful in the investigation as they would contain the required artifacts [40]. This step involves further two sub – processes that were performed for the investigation. These steps are:

- 1) **Identification of the digital devices** – This step involved identifying the IoT device and the mobile device. The IoT device that was found was the “Google Home Mini” and the mobile device was an Android based operating system.

2) **Documenting details of the identified devices** – Once the devices had been identified, the details of those devices were noted down as shown in the table 5-1.



Device	Model	Device_id	Device Image
Smart speaker	Google Home Mini H0A	A4RH0A	
Mobile device	LG Nexus 5X	Serial number:010e9d1be3841fd8	

Table 5-1 Details of the devices found

5.4.2.2 Evidence Collection Process

In this step, the evidence is collected whether from the actual on – site location of where the crime occurred or through proper legal proceedings, if someone fails to co-operate or when needed. Since this investigation is performed for research purposes no such task was required to be performed. The evidence collection process in this framework has two sub – steps. These sub – steps are:

- 1) **Seize the identified evidence** – Once the devices had been identified, the next step was to seize the devices, so that the investigation could be conducted. Both the IoT device and the mobile device were seized so as to investigate and extract artifacts. In actual investigations, a court order is usually required to seize the required devices.
- 2) **Handling the devices** – After the devices had been seized, the investigation was started on those devices. However, the devices can either be transported and stored in a forensic laboratory or they can be given to an appropriate forensic investigator that possesses the expertise to investigate those devices.

5.4.2.3 Evidence Acquisition Process

This step in the acquisition phase is where the evidence is acquired from different domains and in different ways depending on the domain from which the evidence is gathered. This includes obtaining forensic images, data packets, or carrying out a manual acquisition. However before, the evidence is acquired it is important to understand the underlying architecture of the IoT device that is to be investigated. This is important as it will help the forensic investigator understand the environment in which the IoT device operates and where data resides while the IoT device is functional. The IoT device as mentioned before is the Google Home Mini and the architecture of Google Home Mini is discussed here.

5.4.2.3.1 Google Home Mini Architecture

Google Home Mini operates through voice commands sent by the user. These voice commands are interpreted by the Google Assistant which is an AI based program [41]. Google Home Mini has its own mobile application through which the device is controlled. The AI based Google Assistant can learn and remember which makes using the Google Home Mini a wonderful experience.

There are a number of things that can be done through Google Home Mini such as asking questions, listening to music, setting alarms and reminders and creating shopping lists. The architecture can be seen in figure 5-4 [42]. The user sends a command which is converted to text by the Google Assistant using a combination of algorithms of Natural Language Processing and Machine Learning. The extracted text is then matched from the training phases and a response is generated by using the correct logic. The response is converted into speech and is then heard by the user as an output from the speaker. As can be seen in the architecture, using the Google Home Mini means that a mobile device is involved along with the cloud environment, the network and the speaker itself. Once the architecture was clarified, four different domains were identified that were already made part of the framework as the IoT architecture aided in identifying these domains. This was done when the framework was being designed.

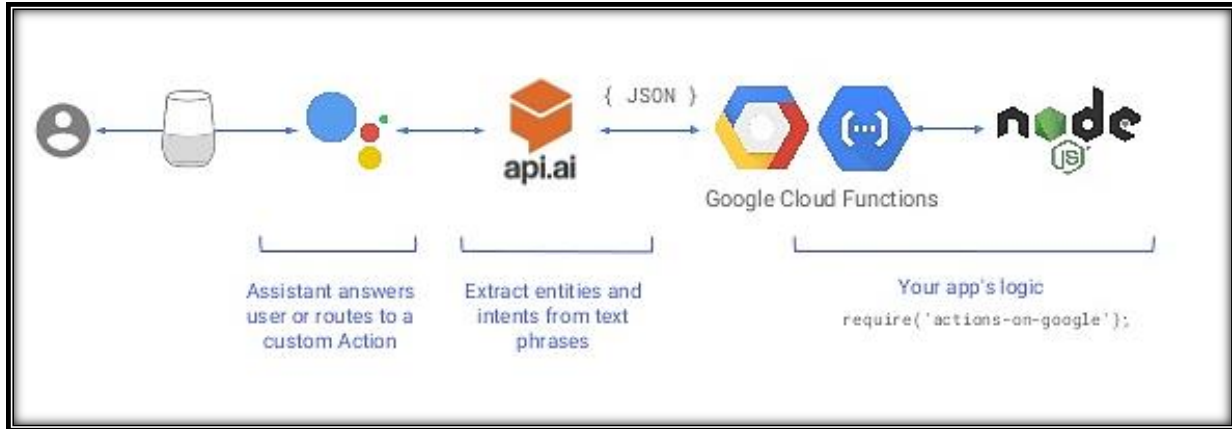


Figure 5-4 Google Home Architecture

5.4.2.3.2 Acquiring Evidence

Evidence acquiring comprises of carrying out investigations in four different domains. These domains are mobile, network, device and cloud. Each of these domains were thoroughly examined one by one and evidence was gathered from each of these domains respectively.

1) Mobile Forensics

IoT devices can now be controlled remotely because many IoT devices have companion applications for Android and iOS platforms. These applications enable the IoT device to be controlled from anywhere. It is necessary to analyse mobile phones in order to see what and how much data is stored in these applications and the mobile device. Acquiring data from the mobile device can be done by obtaining a logical and physical image of the internal storage. Similarly, both logical and the physical images were acquired. The process for acquiring is discussed here.

Logical Image Acquisition

The logical image of the device was obtained by using the Android Debug Bridge (ADB). Before accessing the mobile device through ADB, USB debugging had to be enabled and OEM had to be unlocked.

➤ Enabling USB debugging and unlocking OEM

The following steps were followed as listed:

1. Navigate to Settings in the mobile device.
2. Then About.
3. Tap on the build number 7 times which will enable Developer Options.

4. Then in Developer Options, enable USB debugging and unlock OEM.

The mobile device was then connected physically with the forensic workstation. The mobile was accessed through ADB by executing some commands. The first command to execute is “*adb devices*” that can be seen in figure 5-5. This shows the mobile device that is connected.

```
C:\Users\LENOVO\AppData\Local\Android\Sdk\platform-tools>adb devices
List of devices attached
010e9d1be3841fd8      device
```

Figure 5-5 Connection of the mobile device

Then, the logical image was obtained by performing a backup of the mobile device. The command “*adb backup -apk -shared -all -f*” followed by the name that one needs to give to the backup file as shown in the figure 5-6. The backup file was made in “.ab” format and was found in the following location: C:\Users\LENOVO\AppData\Local\Android\Sdk\platform-tools.

```
C:\Users\LENOVO\AppData\Local\Android\Sdk\platform-tools>adb backup -apk -shared -all -f new1backup.ab
WARNING: adb backup is deprecated and may be removed in a future release
Now unlock your device and confirm the backup operation...
```

Figure 5-6 Backup of the mobile device

Since the backup file has a format and cannot be investigated, it needed to be compressed to be converted to .tar format. The command to convert the backup into .tar format is “*java -jar abe.jar unpack*” followed by the name of the original backup file name, new backup file name and the password that was used while obtaining the backup. This created a zip file that was then uncompressed using any zip converter. The uncompressed files and folders were then stored on the forensic workstation to be investigated later.

```
C:\Users\LENOVO\AppData\Local\Android\Sdk\platform-tools>java -jar abe.jar unpack new1backup.ab new1backup.tar thesis2020
```

Figure 5-7 Conversion to .tar format

Physical Image Acquisition

The physical image of the mobile device is a bit – by – bit copy of the operating system which contains information that is not found in the logical image of the mobile device. Physical images cannot be obtained until the mobile device is rooted which gives complete control of the mobile device. Once the mobile device is rooted, it gives super – user privileges allowing access with complete permissions [43]. The process of rooting the mobile device obtained during the evidence collection process is discussed here.

Rooting the mobile device

Before the mobile is rooted, it is important to make sure that the mobile is charged above 75% to prevent the mobile turning off and interrupting the process. The other thing is to make a backup of the data to prevent any data loss.

Similarly, the mobile device was completely charged and a backup was made. USB debugging and OEM had already been unlocked while acquiring the logical image, so it did not need to be done again. Magisk zip and TWRP recovery file was downloaded and copied into the phone’s memory [44][45]. After this the first step was to unlock the bootloader which was done by using ADB and FastBoot.

➤ Unlocking Bootloader

1. The mobile device was turned off and FastBoot mode was enabled by pressing Volume Down + Power buttons at the same time.
2. The Volume Up button was pressed, once the warning message appeared.
3. The mobile was connected to the forensic workstation.
4. The Command Prompt was opened and “*fastboot devices*” command was run to see if the device was connected or not. Then “*fastboot oem unlock*” was entered in the command prompt and unlock bootloader was selected on the mobile device to complete the process.

After the bootloader was unlocked, the next step was to flash TWRP using the TWRP file present in the phone’s memory.

➤ Flashing using TWRP

1. The first two steps of unlocking the bootloader were followed.

2. The mobile device was connected to the forensic workstation and fastboot was opened in the command prompt. The following command *“fastboot flash recovery recovery.img”* was entered.
3. The mobile was booted into TWRP mode. Then Install was selected to install Magisk.
4. After the installation was complete, the mobile was rebooted.
5. Root Checker was installed to verify that the mobile had been rooted or not as seen in figure 5-8.

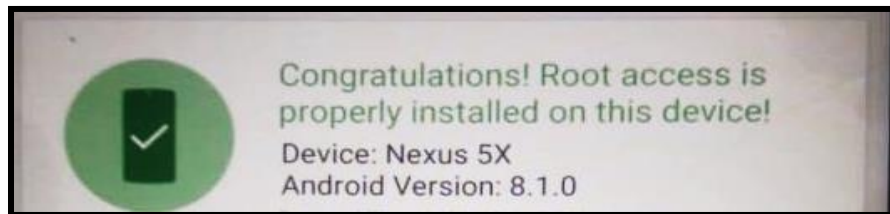


Figure 5-8 Root Checker

Once the rooting was successfully done, the physical image could be extracted. To extract the physical image, the mobile device was switched to flight mode to prevent any interference which could modify the forensic image during extraction and the mobile device was charged completely.

➤ **Extracting the physical image**

1. The mobile device was connected with the forensic workstation and accessed through adb.
2. To check root access the command *“adb shell”* was run. Then *“su”* was entered and the dollar sign (\$) changed to hash (#) which showed that root access was enabled in the mobile device as seen is figure 5-9.

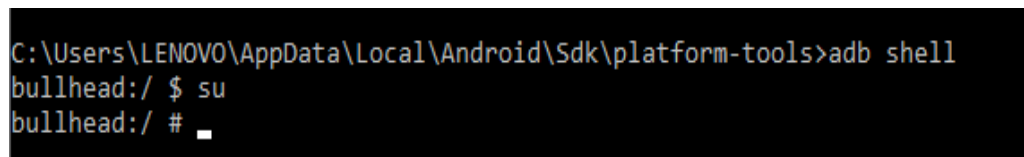


Figure 5-9 adb shell command

3. Then two command windows were opened where one was for the mobile device and the other was for the workstation. In the first command window which was for the forensic workstation *“adb forward tcp:8888 tcp:8888”* was run to so that data can be shared on port 8888 as seen in figure 5-10.

```
C:\Users\LENOVO\AppData\Local\Android\Sdk\platform-tools\netcat-1.11>adb forward tcp:8888 tcp:8888  
8888
```

Figure 5-10 adb forward command

4. In the second command window which was for the mobile device the dd command was run. The command that was run was “*dd=/if/dev/block/mmcblk0 | toybox -l -p 8888*” to forward data on port 8888 for the mmcblk0 partition as seen in figure 5-11.

```
C:\Users\LENOVO\AppData\Local\Android\Sdk\platform-tools\netcat-1.11>adb shell  
bullhead:/ $ su  
bullhead:/ # dd if=/dev/block/mmcblk0 | toybox nc -l -p 8888
```

Figure 5-11 Forward mobile’s data to the forensic workstation

5. Then in the first command window which was for the forensic workstation the nc command was run to receive the mobile device’s image using the IP 127.0.0.1 and port 8888. The “*nc 127.0.0.1 8888>physical-image1.dd*” was run and the physical image was made in the Sdk directory named as physical-image1 as given in the command which is shown in figure 5-12.

```
C:\Users\LENOVO\AppData\Local\Android\Sdk\platform-tools\netcat-1.11>nc 127.0.0.1 8888>physical-image1.dd
```

Figure 5-12 Receive mobile’s data using nc

6. After the physical image had been successfully acquired, the command window for the mobile device showed the complete details that included the total bytes transferred and the total time taken to acquire the image as seen in figure 5-13.

```
C:\Users\LENOVO\AppData\Local\Android\Sdk\platform-tools\netcat-1.11>adb shell  
bullhead:/ $ su  
bullhead:/ # dd if=/dev/block/mmcblk0 | toybox nc -l -p 8888  
30777344+0 records in  
30777344+0 records out  
15758000128 bytes transferred in 703.807 secs (22389660 bytes/sec)
```

Figure 5-13 Physical image successfully acquired

7. A copy of the original physical image was made and saved on the forensic workstation for analysis later in the investigative phase.

2) Cloud Forensics

IoT devices are connected to the cloud platform where the cloud servers and the client side store the user's data. Both the client and the server side needs to be included in the investigation to obtain data that has been retained as the data can prove useful in the investigation.

Cloud acquisition for Google Home Mini can be done on the client and the server side. Acquiring data that is stored on the server side needs access to the Google cloud servers which was not possible in this research. The only acquisition that could be done in the cloud for the Google Home Mini was on the client's side. Once the user account credentials were obtained then a manual acquisition was performed by taking screenshots of the most important evidence. These screenshots were then saved on the forensic workstation to be analysed later. Cloud forensic tools are supported only for the cloud owner's side and not for the public or the client's side, hence cloud forensic acquisition was done manually on the client's side.

3) Network Forensics

The IoT devices are connected through a network to the cloud servers and are also interconnected to the other devices. The network devices such as routers are also able to store a certain amount of data that also needs to be extracted and included in the investigation as it can help the forensic investigator in building a timeline. Furthermore, the servers, firewalls and alerts from Intrusion Detection Systems needs to be inspected as it can help to gain an insight of when an unknown activity was detected.

The network forensic acquisition for Google Home can be done in two ways. A live network forensic analysis can be performed that can be done through packet capture and the other would be to examine logs at the server. Carrying out a live network forensic acquisition involves packet capturing that can help the investigator in finding out the source of the attack and also provide a real time view of the network. Examining logs at the server requires access to Google's servers which was not possible in this research, so a live network forensic acquisition was conducted.

To capture the packets that were sent through Google Home Mini, Wireshark was used. The setup to capture the packets was done by connecting the laptop to the Internet. The hotspot for the laptop was enabled and then the mobile phone with the Google Home application was

connected to the laptop’s hotspot [46]. The laptop was used as an access point to route the traffic to the Google Home Mini speaker. The setup can be seen in the figure 5-14.

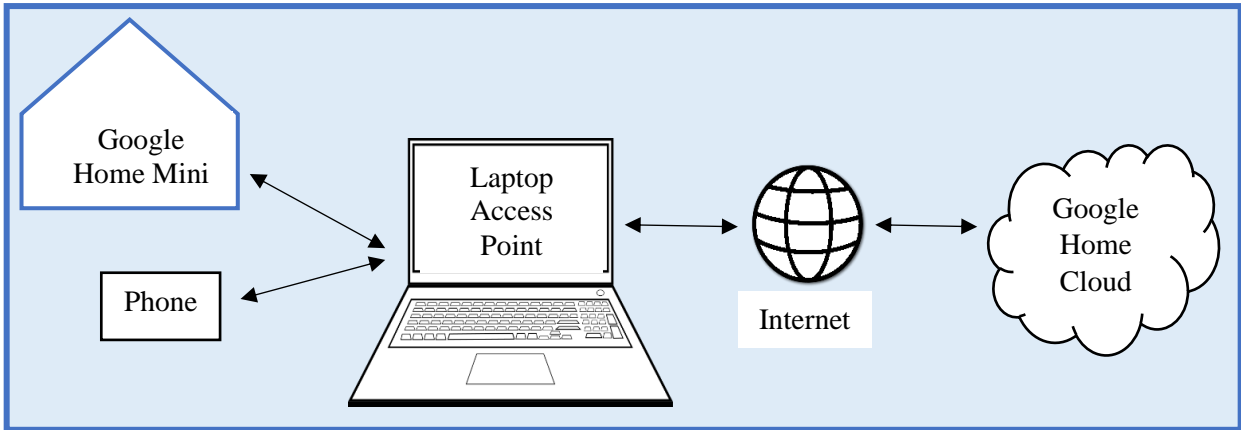


Figure 5-14 Setup to capture packets

The Google Home Mini was used and commands were sent to it. The packets were captured when different types of commands were issued to Google Home Mini. The captured packets were then analysed in the next phase. These commands can be found in the table 5-2.

Sr No.	Commands issued to capture packets
1.	Capturing packets while using Google Home Mini to cast Bluetooth Audio.
2.	Capturing packets while using Google Home Mini to cast news while listening to different news channels.
3.	Capturing packets while using Google Home Mini to cast an alarm which included personalized alarms.
4.	Capturing packets while using Google Home Mini to ask questions.

Table 5-2 Commands to capture packets

4) Device Forensics

IoT devices are known for having a limited memory capacity. Even though the memory capacity is quite limited, it is important to analyse and read the data that would be stored in the memory. Analysing the IoT devices will involve a chip analysis that will require the investigator to remove the chip from the IoT device and then extract the data from it. According to the framework, device forensics can be done in two ways which includes manual and chip – off.

Manual Acquisition

In manual acquisition, the data can be extracted by connecting the device to a computer, if possible and then navigating through the folders or files if they are visible. The Google Home Mini was connected to the forensic workstation with a USB cable. However, the device was not detected by the forensic workstation. Even after installing drivers, none of the contents within the device were visible so no data was able to be acquired from the speakers.

Chip – Off Acquisition

The next task in device forensics was to gather data from the internal storage of the smart speaker. Google Home Mini has a NAND flash memory with a storage capacity of around 256 MB. Unfortunately, since removing the chip, extracting data from the chip and parsing was out of the scope in this research, so it was not possible to acquire data from the chip in Google Home Mini. However, in a real investigation proper expertise is present so maximum efforts should be made to extract data from the device's internal storage.

5.4.2.4 Evidence Storage and Preservation Process

After the evidence has been acquired, it is important that the evidence is stored in a safe and secure location, so that no modifications take place which maintains the preservation of the evidence. In an investigation, the acquired evidence can be stored in the forensic labs and external storage media's such as hard drives.

It is important to make copies of the obtained evidence and examine the copy rather than the original evidence. This makes sure that the original evidence is not tampered and can later be compared with the copy of the evidence ensuring that no alterations took place during the investigation.

The procedure followed for this investigation was that copies were made of the extracted artifacts which were then examined in the analysis phase rather than the original forensic images and the packet captures that were made. The original evidence acquired was stored in the hard drive of the forensic workstation. In addition, to maintain integrity after the examination, the hashes of the obtained evidence was compared with the examined evidence assuring that no changes were made intentionally or unintentionally to the evidence.

5.4.3 The Investigative Phase

The investigative phase is the third phase in the framework. This is one of the most important and crucial phase in the investigation, once evidence has been acquired in the most efficient way possible. This is the phase where the forensic investigator retrieves all the evidence that has been stored and preserved and thoroughly examines it to extract the most valuable artifacts that can lead the forensic investigator in the right direction. The investigator can use the right tools to examine the obtained evidence which can be either forensic images, screenshots, network packets, server logs or the examination can be done manually, if no such tool is required. However, the forensic investigator needs to be very careful that no modifications should be made while investigating.

The evidence obtained in this investigation in the acquisition phase comprised of forensic images which included logical backups, physical images, cloud artifacts from the client's side and the network packets that were captured in real time. The evidence was acquired using different tools after which the evidence was preserved for analysis. As seen in the framework, the evidence was acquired from three different domains, hence inspection was done using different tools. The investigative phase in this framework contains five different steps that were all performed in a sequential manner as seen in figure 5-15.

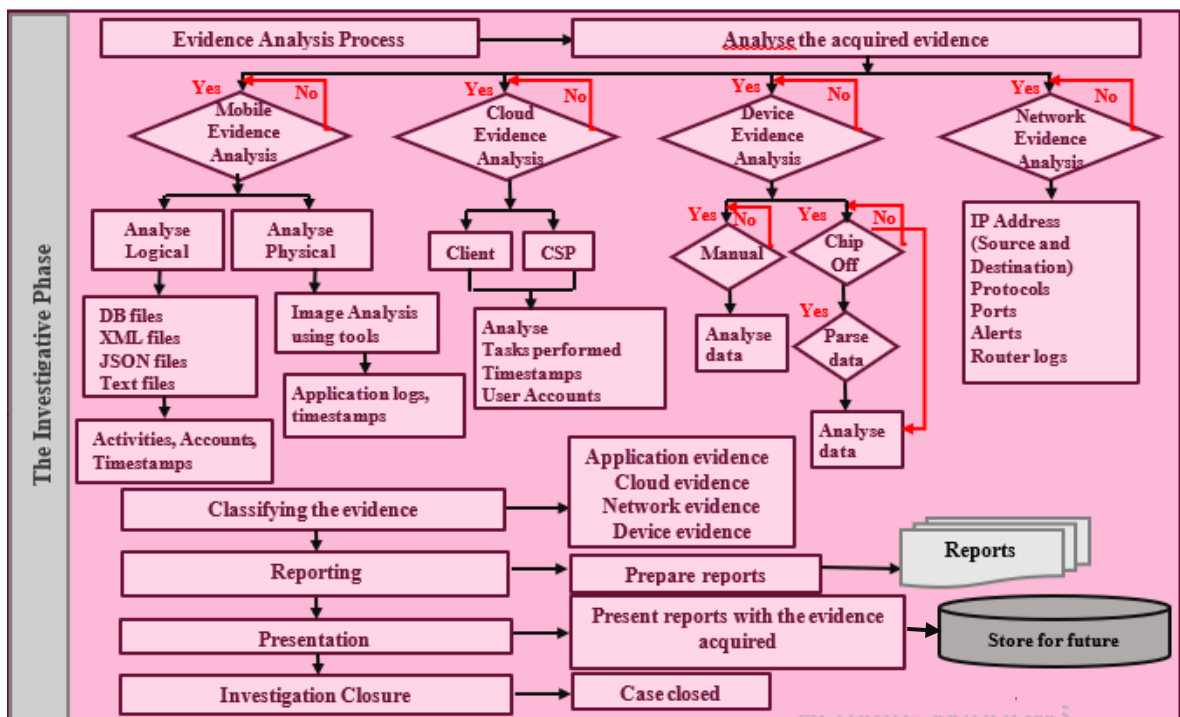


Figure 5-15 The Investigative Phase

5.4.3.1 Evidence Analysis Process

The evidence analysis process in the framework shows the process of examining the evidence in each of these domains. There are four different domains that are included and analysis of the evidence was carried out in each of these domains that is discussed here.

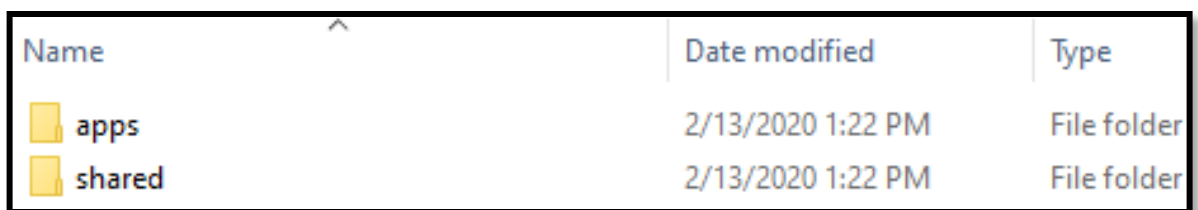
1) Mobile Evidence Analysis

Examining the evidence obtained from the mobile included the detailed examination of the logical and the physical images.

Logical Image Analysis

First the logical image obtained from the mobile device was examined. The procedure on how the logical image was obtained has been described in the evidence acquisition process. The logical image obtained from the mobile device was simple to analyse. It didn't require any tools to observe the image. The logical image contained simple folders of the applications that were installed in the mobile device. The folders contained XML files and database files that were examined one by one. Some valuable information was found from these files and this is discussed in detail in this section. The only disadvantage of the logical image is that it contains very limited information, hence the need for obtaining a physical image that makes a bit by bit copy of the mobile's operating system.

The zip file that was obtained after the conversion was unzipped. The uncompressed zip file revealed two folders that are apps and shared and can be seen in figure 5-16.



Name	Date modified	Type
apps	2/13/2020 1:22 PM	File folder
shared	2/13/2020 1:22 PM	File folder

Figure 5-16 Two main folders found in the logical image

The apps folder contained different folders of the application that were installed on the mobile device as seen in figure 5-17.

com.android.bips	2/13/2020 1:22 PM	File folder
com.android.bluetoothmidiservice	2/13/2020 1:22 PM	File folder
com.android.bookmarkprovider	2/13/2020 1:22 PM	File folder
com.android.captiveportallogin	2/13/2020 1:22 PM	File folder
com.android.carrierdefaultapp	2/13/2020 1:22 PM	File folder
com.android.cts.ctsshim	2/13/2020 1:22 PM	File folder
com.android.cts.priv.ctsshim	2/13/2020 1:22 PM	File folder
com.android.dreams.basic	2/13/2020 1:22 PM	File folder
com.android.dreams.phototable	2/13/2020 1:22 PM	File folder
com.android.egg	2/13/2020 1:22 PM	File folder
com.android.emergency	2/13/2020 1:22 PM	File folder
com.android.externalstorage	2/13/2020 1:22 PM	File folder
com.android.htmlviewer	2/13/2020 1:22 PM	File folder
com.android.internal.display.cutout.emu...	2/13/2020 1:22 PM	File folder
com.android.internal.display.cutout.emu...	2/13/2020 1:22 PM	File folder
com.android.internal.display.cutout.emu...	2/13/2020 1:22 PM	File folder
com.android.managedprovisioning	2/13/2020 1:22 PM	File folder
com.android.mtp	2/13/2020 1:22 PM	File folder
com.android.pacprocessor	2/13/2020 1:22 PM	File folder
com.android.providers.calendar	2/13/2020 1:22 PM	File folder
com.android.providers.downloads.ui	2/13/2020 1:22 PM	File folder
com.android.providers.partnerbookmarks	2/13/2020 1:22 PM	File folder
com.android.providers.telephony	2/13/2020 1:22 PM	File folder

Figure 5-17 View of the apps folder

The shared folder contained folders that can also be seen when a mobile device is connected to a laptop or a computer to transfer files as seen in figure 5-18.

Name	Date modified	Type
.face	2/13/2020 1:22 PM	File folder
Alarms	2/13/2020 1:22 PM	File folder
DCIM	2/13/2020 1:22 PM	File folder
Download	2/13/2020 1:22 PM	File folder
Movies	2/13/2020 1:22 PM	File folder
Music	2/13/2020 1:22 PM	File folder
Notifications	2/13/2020 1:22 PM	File folder
Pictures	2/13/2020 1:22 PM	File folder
Podcasts	2/13/2020 1:22 PM	File folder
Ringtones	2/13/2020 1:22 PM	File folder
Samsung	2/13/2020 1:22 PM	File folder

Figure 5-18 View of the shared folder

Analysing the chromecast app folder

The apps folder needed to be investigated as it contained certain database and xml files that could reveal important information. A folder named **“com.google.android.apps.chromecast.app”** was found. Originally Google’s streaming services were named as “Google cast”, hence the folder for Google Home application is named as chromecast. This folder further contained two other folders that were “a” and “sp” and these folders can be seen in figure 5-19.

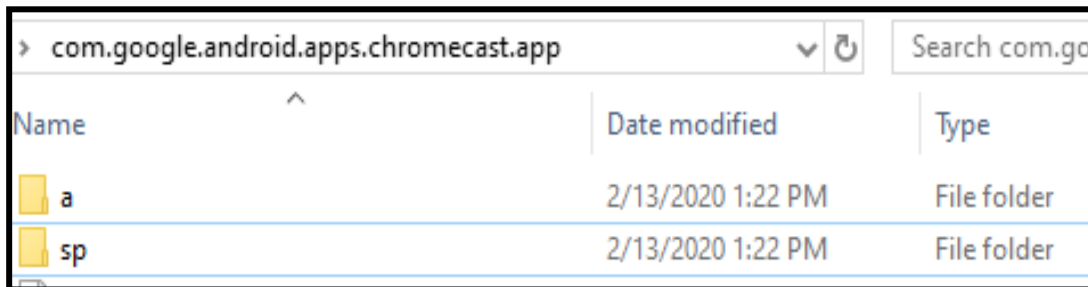


Figure 5-19 Chromecast folder

The first folder that was the “a” folder contained an apk file named as base.apk. The base.apk files are the files that are downloaded when the application is installed, so this base.apk file was for the Google Home application.

The second folder that was the “sp” folder contained an XML file named com.google.android.apps.chromecast.app_preferences. This XML file contained data in plaintext and was viewed using a text editor. The figure 5-20 shows the information that the XML file contained. Some important information was obtained from this XML document.

1. The first and foremost key information that was found was the linked account and it was found in the string name variable. The account linked was agrocks.gauher@gmail.com.
2. The next item of interest was the version of the Google Home application and it was found in the int name variable. The version of the application was 21601100.
3. Another important information that was found was within the Boolean name variable was that an assistant Device Discovered. Google Home listens through the Google Assistant after which the command is converted through Natural Language Processing

and the response is given. This value shows evidence that Google Home was used. The other value that was found was a setup salt value in the variable string name.

```

com.google.android.apps.chromecast.app_preferences - Notepad
File Edit Format View Help
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="THIRD_PARTY_AGENT_INFO_FILE_CREATION_TIMESTAMP_agrocks.gauher@gmail.com">1581491904782</string>
  <int name="appVersion" value="21601100" />
  <boolean name="history_refresh_needed" value="true" />
  <long name="hatsResponseTimeMs" value="1580365935691" />
  <boolean name="feed_immediate_refresh_ready" value="false" />
  <boolean name="is_child_account" value="false" />
  <int name="prefs_version" value="1" />
  <boolean name="showHatsResponse" value="false" />
  <boolean name="hendrixDiscovered" value="true" />
  <boolean name="assistantDeviceDiscovered" value="true" />
  <string name="setup-salt">38a2a962-dc8f-4264-a644-ea1f2f1dd4ea</string>
  <long name="live_card_received_time" value="1581578741591" />
  <boolean name="content_default_getapps" value="false" />
  <boolean name="content_whatson_enabled" value="true" />
  <boolean name="live_card_refresh_needed" value="true" />
  <boolean name="content_getapps_enabled" value="true" />
  <string name="live_card_consistency_token"></string>
  <boolean name="feed_refresh_needed" value="true" />
  <boolean name="audioDeviceDiscovered" value="true" />
</map>

```

Figure 5-20 View of the XML file

Analysing the calendar folder

The next folder that was examined was the “**com.android.providers.calendar**” folder. This folder contained different folders that have some database files, xml files and text files.

The text file `0_dump_com.android.providers.calendars` contained the email account that is synced with the calendar. The name of the account can be found in the `account_name=agrocks.gauher%40gmail.com` and the type of the account can be found in `account_type=com.google` as seen in figure 5-21.

```

oogle.android.syncadapters.calendar, uri = /events?account_name=agrocks.gauher%40gmail.com&account_type=com.google&caller_
oogle.android.syncadapters.calendar, uri = /extendedproperties?account_name=agrocks.gauher%40gmail.com&account_type=com.go
oogle.android.syncadapters.calendar, uri = /syncstate/1?account_name=agrocks.gauher%40gmail.com&account_type=com.google&ca
oogle.android.syncadapters.calendar, uri = /event_entities?account_name=agrocks.gauher%40gmail.com&account_type=com.google&

```

Figure 5-21 Text file `0_dump_com.android.providers.calendars`

The calendar database file also revealed some important information about the events that had been set by the user. The `_sync_state` table in the database showed the account associated with the calendar as seen in figure 5-22. The `account_name` column included the name of the account.

Table: <code>_sync_state</code>		
<code>_id</code>	<code>account_name</code>	<code>account_type</code>
Filter	Filter	Filter
1 1	agrocks.gauher@gmail.com	com.google

Figure 5-22 Sync_state table

The `CalendarCache` table gave the information of the timezone that was associated with the Calendar as seen in figure 5-23. The timezone was set as Asia/Karachi as seen in id 4.

<code>_id</code>	<code>key</code>	<code>value</code>
Filter	Filter	Filter
1	-2140311132	timezoneData...
2	-495220580	timezoneInsta...
3	1126213331	timezoneType
4	1167965829	timezoneInsta...

Figure 5-23 CalendarCache table

The `Events` table in the database file contained information about the events created using Google Home. The table 5-3 shows the key information that was found in the `Events` table such as the title, date start, date end and the organizer.

<code>_id</code>	254
<code>_sync_id</code>	5oirk7uldrijmpbj8aglo3tpg
<code>calendar_id</code>	2
<code>title</code>	Hangout with friends
<code>dtstart</code>	1581750000000 (Saturday, February 15, 2020 12:00:00 PM)
<code>dtend</code>	1581753600000 (Saturday, February 15, 2020 1:00:00 PM)
<code>eventTimezone</code>	Asia/Karachi
<code>hasAlarm</code>	1
<code>organizer</code>	agrocks.gauher@gmail.com

Table 5-3 Events table

The EventsRawTimes table also contained some information about the event created. The event id is 254 which links to the id found in the Events table for a particular event. The table 5-4 shows the information found.

_id	99
event_id	254
dtstart2445	20200215T120000
dtend2445	20200215T130000
lastDate2245	20200215T130000

Table 5-4 EventsRawTimes table

The next table of interest was the Instances table. The Instances table can also be used to extract information about the events that had been created by the user. It contained similar information that was found in the Events table such as the date which over here was stored in begin and end. Some additional information such as the start day, end day, start minute and end minute was also found. The table 5-5 shows the information that was present in the Instances table.

_id	87
event_id	254
begin	1581750000000 (Saturday, February 15, 2020 12:00:00 PM)
end	1581753600000 (Saturday, February 15, 2020 1:00:00 PM)
startDay	2458895 (28 days, 11 hours, 1 minutes and 35 seconds)
endDay	2458895 (28 days, 11 hours, 1 minutes and 35 seconds)
startMinute	720 (12 minutes 0 seconds)
endMinute	780 (13 minutes 0 seconds)

Table 5-5 Instances table

The Reminders table has information that tells us the number of methods that a user will be reminded of the event. A user is reminded of an event created by using Google Home Mini in two methods as can be seen in the figure 5-24. The first reminder of the event is given to the user 30 minutes before the actual time of the event. This is in the form of an email notification that the user receives on the account linked with the Google Home Mini. The second reminder is given on the actual time of the event that was set by the user, so there is a difference of 30 minutes between the first and the second reminder. As can be seen for event id 254 two methods were used for reminding with a difference of 30 minutes.

	_id	event_id	minutes	method
	Filter	Filter	Filter	Filter
1	1	251	30	1
2	2	251	30	2
3	3	252	30	2
4	4	252	30	1
5	5	253	30	1
6	6	253	30	2
7	7	254	30	1
8	8	254	30	2

Figure 5-24 Reminders table

The view_events table also gives information about the details of the events that were created. The table 5-6 shows the details that were found in the table.

_id	254
title	Hangout with friends
dtstart	1581750000000 (Saturday, February 15, 2020 12:00:00 PM)
dtend	1581753600000 (Saturday, February 15, 2020 1:00:00 PM)
eventTimezone	Asia/Karachi
hasAlarm	1
lastDate	1581753600000 (Saturday, February 15, 2020 1:00:00 PM)
organizer	agrocks.gauher@gmail.com
account_name	agrocks.gauher@gmail.com
account_type	com.google
name	agrocks.gauher@gmail.com
calendar_timezone	Asia/Karachi

Table 5-6 view_events table

Physical Image Analysis

The physical image that was acquired during the acquisition phase was analysed here to be able to extract the most important artifacts. The analysis of the physical image was done using Autopsy, since Autopsy recognizes forensic images with dd extension.

➤ Using Autopsy to open a physical image

1. A new case was created in Autopsy.
2. The case details were filled in.

3. After the case details had been completed, the data source needed to be selected which was a disk image.
4. The location of the data source was selected next.
5. Then the data source was added.

Analysing the physical image

The physical image was then analysed once Autopsy had loaded the image as the data source. The first thing that was noticed was the different volumes along with the sectors that they had occupied as seen in figure 5-25. Further information included the name of each volume, the ID of each volume, the starting sector, length of the sectors and flags which provided information whether the volume was allocated or unallocated.

Name	ID	Starting Sector	Length in Sectors
vol1 (Unallocated: 0-16383)	1	0	16384
vol4 (modem: 16384-192511)	4	16384	176128
vol5 (Unallocated: 192512-196607)	5	192512	4096
vol6 (pmic: 196608-197631)	6	196608	1024
vol7 (sbl1: 197632-199679)	7	197632	2048
vol8 (tz: 199680-201727)	8	199680	2048
vol9 (sdi: 201728-202751)	9	201728	1024
vol10 (hyp: 202752-203775)	10	202752	1024
vol11 (rom: 203776-204799)	11	203776	1024

Figure 5-25 Volume names and sector occupied

Analysing the Google Home folder

The next volume that needed to be examined was volume 46 (system) and the Google Home folder needed to be examined in this volume. The path for this folder was `/img_physical-image1.dd/vol_vol46/app/GoogleHome`. The folder contained three more folders and the `GoogleHome.apk` file where the `.apk` extension means that the application is an Android application as seen in figure 5-26.

Name	S	C	Modified Time	Change Time	Access Time
[current folder]			2009-01-01 13:00:00 PKT	2009-01-01 13:00:00 PKT	2009-01-01 13:00:00 PKT
[parent folder]			2009-01-01 13:00:00 PKT	2009-01-01 13:00:00 PKT	2009-01-01 13:00:00 PKT
oat			2009-01-01 13:00:00 PKT	2009-01-01 13:00:00 PKT	2009-01-01 13:00:00 PKT
GoogleHome.apk			2009-01-01 13:00:00 PKT	2009-01-01 13:00:00 PKT	2009-01-01 13:00:00 PKT

Figure 5-26 Google Home folder

Analysing the chromecast app folder in app

The next volume that needed to be analysed was volume 52 (userdata) and the path for this volume was **/img_physical-image1.dd/vol_vol52**. This volume contained many folders. The first folder that was examined was the chromecast folder found in the app folder as chromecast is the folder created for the Google Home and the path was **/img_physical-image1.dd/vol_vol52/app/com.google.android.apps.chromecast.app**. It contained a few folders and some apk files as seen in figure 5-27. However, no important details were found in any of these folders or in the apk files.

Name	S	C	Modified Time	Change Time	Access Time
[current folder]			2020-04-01 15:42:09 PKT	2020-04-01 15:42:09 PKT	2020-04-01 15:41:38 PKT
[parent folder]			2020-08-25 20:24:14 PKT	2020-08-25 20:24:14 PKT	1970-01-03 06:04:23 PKT
lib			2020-04-01 15:42:08 PKT	2020-04-01 15:42:09 PKT	2020-04-01 15:42:08 PKT
oat			2020-04-01 15:42:09 PKT	2020-04-01 15:42:09 PKT	2020-04-01 15:42:09 PKT
base.apk			2020-04-01 15:41:53 PKT	2020-04-01 15:42:09 PKT	2020-04-01 15:41:52 PKT
split_config.arm64_v8a.apk			2020-04-01 15:42:08 PKT	2020-04-01 15:42:09 PKT	2020-04-01 15:42:07 PKT
split_config.en.apk			2020-04-01 15:41:56 PKT	2020-04-01 15:42:09 PKT	2020-04-01 15:41:56 PKT
split_config.xxhdpi.apk			2020-04-01 15:41:55 PKT	2020-04-01 15:42:09 PKT	2020-04-01 15:41:55 PKT
stream..config.arm64_v8a.apk			2020-04-01 15:42:08 PKT	2020-04-01 15:42:09 PKT	2020-04-01 15:42:07 PKT

Figure 5-27 Chromecast folder in app

Analysing the calendars folder in data

The next folder that was examined was the data folder in this volume and the path was **/img_physical-image1.dd/vol_vol52/data**. This data folder contained many folders of the

applications that were installed on the mobile device. The first folder to be examined was the calendars folder where the path was **/img_physical-image1.dd/vol_vol52/data/com.android.providers.calendars** which contained six more folders as seen in figure 5-28.

Name	S	C	Modified Time	Change Time	Access Time
[current folder]			2020-01-23 01:20:02 PKT	2020-01-23 01:20:02 PKT	1970-01-03 06:04:52 PKT
[parent folder]			2020-04-14 14:25:59 PKT	2020-08-19 11:56:52 PKT	1970-01-03 06:04:23 PKT
cache			1970-01-03 06:04:52 PKT	1970-01-03 06:04:52 PKT	1970-01-03 06:04:52 PKT
code_cache			1970-01-03 06:04:52 PKT	1970-01-03 06:04:52 PKT	1970-01-03 06:04:52 PKT
databases			2020-01-23 01:20:02 PKT	2020-01-23 01:20:02 PKT	2020-01-23 01:20:02 PKT
shared_prefs			2020-01-23 01:20:02 PKT	2020-01-23 01:20:02 PKT	2020-01-23 01:20:02 PKT

Figure 5-28 Calendar folder in data

The databases folder in the calendar folder contained a calendar.db file that had different tables. The tables were examined one by one. The first table to be examined was `_sync_state` table which contained the account name and the account type to which the calendar had been synced with as seen in figure 5-29.

_id	account_name	account_type
1	agrocks.gauher@gmail.com	com.google

Figure 5-29 Sync_state table in calendar.db

The other table to be examined was the Calendars table which contained the account name, account type, name and calendar display name as seen in figure 5-30 in id 4.

_id	account_name	account_type	name	calendar_displayName
1	agrocks.gauhe...	com.google	Abeer Gauhar Bio & CS Timetable	Abeer Gauhar Bio & CS Timetable
2	agrocks.gauhe...	com.google	Contacts	Contacts
3	agrocks.gauhe...	com.google	Holidays in Pakistan	Holidays in Pakistan
4	agrocks.gauhe...	com.google	agrocks.gauher@gmail.com	agrocks.gauher@gmail.com

Figure 5-30 Calendars table in calendar.db

The Events table was examined next which contained all the events that were created using the Google Home Mini. The important information about the event was present that included the title of the event, date start, date end, event time zone and the organizer email as seen in figure 5-31. The table 5-7 shows the details that were found in the Events table for one of the events that was created by the user. As observed, these same details of the same event were also found during the logical image analysis.

_id	_sync_id	calendar_id	title	eventStatus	selfAttention	dtstart	dtend
480	20200425_60o32o9m6oo30c1g60o30dr56g	0	Ramazan Bank Holiday	1	0	1587772800000	1587859200000
481	20200522_60o32e16ko30c1g60o30dr56g	0	Eid-ul-Fitr Holiday	1	0	1590105600000	1590192000000
482	20200523_60o32e16ko30c1g60o30dr56g	0	Eid-ul-Fitr Holiday	1	0	1590192000000	1590278400000
483	20200524_60o30dhl74o30c1g60o30dr56g	0	Eid-ul-Fitr	1	0	1590278400000	1590364800000
484	20200525_60o32ohg74o30c1g60o30dr56g	0	Eid-ul-Fitr Holiday	1	0	1590364800000	1590451200000
485	e18b0hi29mr5jlvgotspcg42b4	0	It's hike	1	0	1580410800000	1580414400000
486	vulcnp2b269n24kmse9k6j72ok	0	Alia's birthday	1	0	1583856000000	1583859600000
487	nll9pofob7y5a8mg0ep36hk2e18	0	Weekend	1	0	1581094800000	1581098400000
488	5oirk7uldrijmpbj8aglro3tpg	0	Hangout with friends	1	0	1581750000000	1581753600000

Figure 5-31 Events table in calendar.db

_id	488
_sync_id	5oirk7uldrijmpbj8aglro3tpg
calendar_id	4
title	Hangout with friends
dtstart	1581750000000 (Saturday, February 15, 2020 12:00:00 PM)
dtend	1581753600000 (Saturday, February 15, 2020 1:00:00 PM)
eventTimezone	Asia/Karachi
organizer	agrocks.gauher@gmail.com

Figure 5-7 Details in the Events table

Another calendars folder was also found in the data folder. It mostly contained the same files and folders as the previous one and had the path that was **/img_physical-image1.dd/vol_vol52/data/com.google.android.providers.calendars**. The databases folder was examined again and a cal_v2a file was examined. It contained a Calendars table which contained the account ID, the calendar ID and owner access as seen in figure 5-32. The fourth record in the table shows the owner access value as 1 which means true and the owner has access to create calendar events made using Google Home Mini.

AccountId	CalendarId	HasOwnerAccess
101963401235301094846	en.pk#holiday@group.v.calendar.google.com	0
101963401235301094846	addressbook#contacts@group.v.calendar.google.com	0
101963401235301094846	vmkfg586ng5mbc2onrutfpseck@group.calendar.google.com	0
101963401235301094846	agrocks.gauher@gmail.com	1

Figure 5-32 Calendars table in cal_v2a

This calendar folder also contained sync_logs which contained the timestamps for when the calendar had been synced with respect to the registered email account. The shared_prefs folder contained an XML file named as **.com.google.android.calendar_preferences.xml** which mainly contained sync details and the calendar account as seen in figure 5-33.

```

<string name="preferences_last_display_tz">Asia/Karachi</string>
<boolean name="uss_mod_shipshape" value="true" />
<boolean name="notify_on_this_device" value="true" />
<boolean name="vibrate" value="false" />
<string name="preference_defaultCalendarAccountId">agrocks.gauher@gmail.com</string>
<string name="calendar_sync_stats_uss_events">2020-08-21 19:19:37+0500 (agrocks.gauher@gmail.com): Chime
(agrocks.gauher@gmail.com): Chime tickle for calendar agrocks.gauher@gmail.com. &#10;2020-08-21 19:22:00+0500
&#10;2020-08-21 19:29:41+0500 (agrocks.gauher@gmail.com): [SyncAdapter] Sync succeeded. &#10;2020-08-22 15:46
succeeded. &#10;2020-08-22 16:02:43+0500 (agrocks.gauher@gmail.com): System sync requested. &#10;2020-08-22 1
7:37:08+0500 (agrocks.gauher@gmail.com): [SyncAdapter] Sync succeeded. &#10;2020-08-24 23:26:46+0500 (agrocks
agrocks.gauher@gmail.com): System sync requested. &#10;2020-08-24 23:27:55+0500 (agrocks.gauher@gmail.com):
(agrocks.gauher@gmail.com): [SyncAdapter] Sync succeeded. &#10;2020-08-26 20:30:48+0500 (agrocks.gauher@gmail

```

Figure 5-33 Calendar preferences XML

Analysing the chromecast app folder in data

The second folder to be examined in the data folder was the chromecast folder and the path for this folder was **/img_physical-image1.dd/vol_vol52/data/com.google.android.apps.chromecast.app**. This folder contained eleven more folders as seen on figure 5-34.

Name	S	C	Modified Time	Change Time	Access Time
[current folder]			2020-04-01 18:42:19 PKT	2020-04-01 18:42:19 PKT	2020-04-01 15:43:11 PKT
[parent folder]			2020-04-14 14:25:59 PKT	2020-08-19 11:56:52 PKT	1970-01-03 06:04:23 PKT
app_google_tagmanager			2020-04-01 15:43:21 PKT	2020-04-01 15:43:21 PKT	2020-04-01 15:43:19 PKT
app_textures			2020-04-01 16:25:37 PKT	2020-04-01 16:25:37 PKT	2020-04-01 16:25:37 PKT
app_webview			2020-08-23 17:49:10 PKT	2020-08-26 20:47:06 PKT	2020-04-01 16:25:37 PKT
cache			2020-04-01 15:43:19 PKT	2020-04-01 15:43:19 PKT	2020-04-01 15:43:16 PKT
code_cache			2020-04-01 18:42:19 PKT	2020-04-01 18:42:19 PKT	2020-04-01 18:42:19 PKT
databases			2020-08-26 21:41:50 PKT	2020-08-26 21:41:50 PKT	2020-04-01 15:43:16 PKT
files			2020-08-26 20:30:32 PKT	2020-08-26 20:30:32 PKT	2020-04-01 15:43:16 PKT
no_backup			2020-04-01 15:43:22 PKT	2020-04-01 15:43:22 PKT	2020-04-01 15:43:16 PKT
shared_prefs			2020-08-26 20:47:13 PKT	2020-08-26 20:47:13 PKT	2020-04-01 15:43:16 PKT

Figure 5-34 Chromecast folder in data

The databases folder was analysed in the chromecast folder and it contained many databases where each one was opened to see if any important information could be found. The accounts.notifications.db contained a table accounts which contained the account name to which the notifications are sent as seen in figure 5-35.

Table: accounts		1 entries
_id	account_name	
1	agrocks.gauher@gmail.com	

Figure 5-35 Accounts table

The growthkit.db also contained many tables out of which the clearcut events table provided some valuable information such as the account, the timestamps in UNIX of when the user had logged in and used the application and the package name which was chromecast as seen in figure 5-36.

account	timestamp_ms	log_source	event_code	package_name
agrocks.gauher@gmail.com	1597912142212	130	999999	com.google.android.apps.chromecast.app
agrocks.gauher@gmail.com	1597912165461	130	1	com.google.android.apps.chromecast.app
agrocks.gauher@gmail.com	1597912165487	130	108	com.google.android.apps.chromecast.app
agrocks.gauher@gmail.com	1597912165499	130	999999	com.google.android.apps.chromecast.app
agrocks.gauher@gmail.com	1597912221495	130	1	com.google.android.apps.chromecast.app

Figure 5-36 Clearcut Events Table

Next the files folder was examined in the chromecast folder. The home_graph file contained some important information which included the nick name the speaker had been given, the address, the email address, the name of the speaker and the actions that the speaker can perform and the truncated local network Id as seen in figure 5-37. The home_graph file also contained information about what had been played through Bluetooth pairing using the Google Home Mini as seen in figure 5-38.

```

$a7a5a4b2-e625-4335-9ca6-bdd372fa8877
  Hostelite
  #NUST University, Islamabad, Pakistan
  w?R@
  "Asia/Karachi"
  agrocks.gauher@gmail.comZ
  #d904460a-41a9-43ba-a83d-e4454bec85b9
  #google.com:api-project-498579633514
  1C9B0E1A6C5389921302E2125A806DF7"
  Abeer's Room speaker2
  action.devices.types.SPEAKER:
  action.devices.traits.Cast:
  action.devices.traits.Assistant:#action.devices.traits.RemoteDucking:'action.devices.traits.CommunicationCall:
  CommunicationVideoCallR
  1019634012353010948468
  Google Home Mini
  Abeer's Room speaker
  truncatedLocalNetworkId
  1B4A1FE638B1
  
```

Figure 5-37 Home graph file

```

Bluetooth Audio ██████████
*6Demi Lovato - Give Your Heart a Break (Official Video)2
DemiLovatoVEVOH
██████████
  
```

Figure 5-38 Bluetooth audio in home graph file

The shared_prefs folder was examined next in the chromecast folder and it contained an XML file named as accountmenu.AccountSelectionRestorer.selectedAccount.xml that contained the name of the account in the string tag as seen in figure 5-39.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="selected_account_id">agrocks.gauher@gmail.com</string>
</map>
```

Figure 5-39 Account menu XML file

The other XML file of interest in shared_prefs folder was the .com.google.android.apps.chromecast.app_preferences.xml which had information about the email address used for the Google Home Mini and the application version as seen in figure 5-40.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="THIRD_PARTY_AGENT_INFO_FILE_CREATION_TIMESTAMP_agrocks.gauher@gmail.com">
  <int name="appVersion" value="21901180" />
```

Figure 5-40 App preferences XML file

The next XML file that contained important information in the shared_prefs folder was the .com.google.android.apps.chromecast.app_preferences_no_backup.xml that revealed details such as the current home id, current account name and the name of the network that the Google Home Mini was connected to as seen in figure 5-41.

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="current_home_id_agrocks.gauher@gmail.com">a7a5a4b2-e625-4335-9ca6-bdd372fa8877</string>
  <string name="ph_server_token"
>CAES2QEAsotIfJgVX0g500D_r9ZfKw7MYcemohJxKf6rZWBuLfUatUubX8JDr3xD0tJ10SR9CtPh80gX2v39xMUmONY1bk8n9Vbfhx7lgJyog5FVayCIw0Puff
-A2pMDznIoI1JZ1xKeOk1geFRMfIiGiQng-ARZQfmaco7ZIHbnAHNRDenD8IXRbRsmh7jQwfUldfC1N5WnDr5p69tBhUIA_Up7NdoI9MIUYnl_w-JsoyrKnHRRc
  <long name="home_graph_last_refreshed_agrocks.gauher@gmail.com" value="1598369067024" />
  <boolean name="permission_requested_android.permission.ACCESS_FINE_LOCATION" value="true" />
  <string name="current_account_name">agrocks.gauher@gmail.com</string>
  <boolean name="TERMS_ACCEPTED" value="true" />
  <string name="p-n">[{"&quot;n&quot;:&quot;HUAWEI-DUP7&quot;,&quot;p&quot;:&quot;*****&quot;,&quot;s&quot;:3}]</string>
```

Figure 5-41 App preferences no backup XML file

Analysing google quick search box folder in data

The next folder that was analysed was the google quick search box folder in the data folder with the path **image1.dd/vol_vol52/data/com.google.android.googlequicksearchbox**. This folder contained multiple different folders. The first folder of interest was the app_si folder that had the path **image1.dd/vol_vol52/data/com.google.android.googlequicksearchbox/app_si**. The folder opa_content_store contained some important databases and files in the app_si folder. The contentstore.db file had a table named as blob_table which contained an ID and blob_key. The blob_key column contained the email address associated with a blob key as seen in figure 5-42.

_ID	blob_key
162	null_PCP_PROACTIVE_DATA_LIST_AAAAAGw==
163	null_PCP_PROACTIVE_DATA_LIST_AAAAACw==
164	null_PCP_PROACTIVE_DATA_LIST_AAAAAAw==
165	null_PCP_PROACTIVE_DATA_LIST_AAAAABw==
258	agrocks.gauher@gmail.com_DEVICE_OPA_TIMESTAMP_YWdyb2Nrcy5nYXVoZXJAZ21haWwuY29tX2
274	agrocks.gauher@gmail.com_ZERO_STATE_ZERO_STATE_EMBEDDED_ASSISTANT_RESPONSE_
275	agrocks.gauher@gmail.com_ZERO_STATE_ZERO_STATE_CLIENT_RESPONSE_TUFJTl9BUFA=
276	agrocks.gauher@gmail.com_PCP_PROACTIVE_DATA_LIST_AAAAACw==
277	agrocks.gauher@gmail.com_PCP_PROACTIVE_DATA_LIST_AAAAAAw==
278	agrocks.gauher@gmail.com_PCP_PROACTIVE_DATA_LIST_AAAAAAg==
279	agrocks.gauher@gmail.com_PCP_PROACTIVE_DATA_LIST_AAAAABw==
280	agrocks.gauher@gmail.com_DEVICE_OPA_TIMESTAMP_YWdyb2Nrcy5nYXVoZXJAZ21haWwuY29tX2

Figure 5-42 Blob table in content store

The other file of interest was opa_content_store_blob_518082148806008382.bin file. This file contained key information which included a summary of the commands that were

sent by the user to the Google Home in a week. Along with each command a default id was also associated as well as a hash tag that can be seen in figure 5-43.

```

THIS WEEK
Nshopping_list_7c3d751b35241f695ab6926ca58672541c787756969584aa5a8d80e8298aceb4
Kdefault_id_90a7500fclff3d013f4a427333745180fdcc5a7c6d2c830fclcd880cl3933805
Afternoon, Abeer!2Kdefault_id_2e915df7cd5111958b4b7ef48891a06ffe71e8226032163472b25efb76c331a1R
Ihash_tag_e3b0c44298fclcl49afb4c8996fb92427ae41e4649b934ca495991b7852b855
'Hope your evening's going well, Abeer2Kdefault_id_7efca7a14d8411d14c0da4a28c877bc6e3029460b263alec7e6a08a86fdfea6eF
Ihash_tag_e3b0c44298fclcl49afb4c8996fb92427ae41e4649b934ca495991b7852b855
%TGIB! (Thank goodness it's bedtime)2Kdefault_id_4b0e33a32e9fd15d7fe627df05alb79bad4aa619fcb41b43108fcb6801e0ec47R
Ihash_tag_e3b0c44298fclcl49afb4c8996fb92427ae41e4649b934ca495991b7852b855
Here to help2Kdefault_id_db737c7aedd47ad080056b35015f1267f50fde1519281ae77280f9f612b8662R
Ihash_tag_e3b0c44298fclcl49afb4c8996fb92427ae41e4649b934ca495991b7852b855
Morning2Kdefault_id_d76655b8152a7ec70657cf39aac0a2c263496dcef7c9589096ede049e9414f29R
Ihash_tag_e3b0c44298fclcl49afb4c8996fb92427ae41e4649b934ca495991b7852b855
Good afternoon, Abeer!2Kdefault_id_8bd930f842e33a86647338027c5a7803c520b71ae79bc13924dca5f529863426R
    
```

Figure 5-43 Commands found

The file also revealed the reminder set by the user as seen in figure 5-44. The reminder was titled as “clean my room” and the time for the reminder was 4:15 PM.

```

Reminder
Qhttps://ssl.gstatic.com/assistant-visuals/dev/reminder_card_header_icon_light.png
clean my room"
Today, 4:15 PM(
intent:#Intent;S.com.google.opa.QUERY=Show all reminders;S.com.google.opa.DISPLAY_QUERY=Show all reminders;scheme=http;B.com.google.opa.
SHOULD_REQUEST_TTS_HINT=false;end;
    
```

Figure 5-44 Reminder set by the user

The databases folder was analysed next. It contained a database file named as geller_agrocks.gauher@gmail.com.db although the database was empty and none of the tables were populated. The other database file found to contain relevant evidence was portable_geller_agrocks.gauher@gmail.com.db file. It had a table named as geller_key_table that contained the data type, a column named as key showing what activities were taken place and the timestamp in UNIX format as seen in figure 5-45.

Table: geller_key_table		
data_type	key	timestamp_micro
PRIVACY_SETTINGS	VOICE_AND_AUDIO_ACTIVITY	1598012075632209
PRIVACY_SETTINGS	WEB_AND_APP_ACTIVITY	1598012075632209
PRIVACY_SETTINGS	SEARCH_AND_ASSISTANT	1598012075632209
PRIVACY_SETTINGS	DASHER_POLICY	1598012075632209
PRIVACY_SETTINGS	PERSONAL_RESULTS	1598012075632209
PRIVACY_SETTINGS	WEB_AND_APP_ACTIVITY	1598012277989674

Figure 5-45 Geller key table

The other database of interest was the opa_history database which contained two tables that were populated. One of the table was the accounts table which had the account associated with the Google Home Mini that was the “**agrocks.gauher@gmail.com**” account as previously stated. The other table was the entries table which contained all the conversations exchanged between the Google Home Mini and the user but it was all in BLOB format as seen in figure 5-46.

id	turn_id	entry
1	113	BLOB Data not shown
2	113	BLOB Data not shown
3	113	BLOB Data not shown

Figure 5-46 Entries table

The files folder was analysed next in the google quick search box folder. It contained a folder named as recently which had information about the account that was most recently used with the Google Home as seen in figure 5-47. As seen in the figure the account agrocks.gauher@gmail.com has been the most recently used email account

Name	S	C	Modified Time	Change Time	Access Time
[current folder]			2020-08-26 20:44:36 PKT	2020-08-26 20:44:36 PKT	2020-02-05 13:56:06 PKT
[parent folder]			2020-08-26 20:44:47 PKT	2020-08-26 20:44:47 PKT	2020-01-23 01:19:50 PKT
agrocks.gauher@gmail.com			2020-08-26 20:44:36 PKT	2020-08-26 20:44:36 PKT	2020-08-26 20:44:36 PKT
agrocks.gauher@gmail.com.new			2020-08-26 20:44:36 PKT	2020-08-26 20:44:36 PKT	2020-08-26 20:44:36 PKT

Figure 5-47 Recently folder

Analysing gms folder in data

The gms folder was examined and the path for this folder was **/img_physical-image1.dd/vol_vol52/data/com.google.android.gms**. It contained many more folders and the databases folder was examined. The cast.db database was analysed and was found to have a table named

as DeviceInfo. This table contained information about the Google Home Mini which included the device id, the friendly name of the speaker as set, last published time in UNIX format which tells when the device was last used, the model name, the service address which was an IP address, the service port used and the service instance name which included the model name combined with the device id. This can be seen in figure 5-48.

device_id	friendly_name	last_published_timestamp_millis	model_name	service_address	service_port	service_instance_name
0405737ec26d511030577a81d093271c	Abeer's Room speaker	1598368516715	Google Home Mini	192.168.18.33	8009	Google-Home-Mini-0405737ec26d511030577a81d093271c

Figure 5-48 Device Info table

The NetworkToDevice table in cast.db database contained the network id to which the Google Home Mini was connected and the device id which had the id of the Google Home Mini as seen in the previous DeviceInfo table in the device id column.

_id	network_id	device_id
19	28:41:c6:46:86:c4	0405737ec26d511030577a81d093271c

Figure 5-49 Network to Device table

The next database file of relevance was the reminders.db database file. It contained a table named account which revealed the account associated with the reminders as seen in figure 5-50. The account_name was **agrocks.gauher@gmail.com** and the id for this entry was 8.

_id	account_name
8	agrocks.gauher@gmail.com

Figure 5-50 Account table in reminders.db

Reminders.db had a table named as reminders which had all the reminders that were created by the user using the Google Home Mini speaker. The table included an id for each reminder, the account id which had the value 8 as found in the account table, client assigned id, title of the reminder, created time and archived time in UNIX format as seen in figure 5-51. The created time is the time when the reminder is created by the user and the archived time is the actual time when the reminder rings.

_id	account_id	client_assigned_id	title	created_time_millis	archived_time_ms
48	8	assistant_5e649f5f_0000_2192_9c62_240588792408	... we can be friends	1581576160232	
49	8	assistant_5f186964_0000_207c_88a8_089e08281c94	... breakfast with friends	1581160974029	
50	8	assistant_5e7ed8be_0000_27ba_8455_2405887aab34	... x	1581057246914	
51	8	assistant_5e4e3e2c_0000_278a_b927_089e082f8a94	... take a shower	1580971778240	
52	8	assistant_5f4733ad_0000_203c_9281_883d24f28e04	... send an email	1598021583334	
53	8	assistant_5f44c98c_0000_2d71_a894_30fd3817528c	... contact my friend	1598021609460	1598455405433
54	8	assistant_5f89b61b_0000_2918_95b2_2405887a98e4	... clean my room	1598093202597	1598094916844
55	8	assistant_5fec3f43_0000_2612_8ca3_24058870a338	... call my friend	1598186866126	1598455360626
56	8	assistant_5f60bfb2_0000_223a_bc3c_240588791e54	... clean my wardrobe	1598362224049	1598364443582

Figure 5-51 Reminders table in reminders.db

2) Cloud Evidence Analysis

The client side can be analysed when the account(s) associated with the speaker are obtained. Then these accounts can be analysed to see how much information about the user’s command is stored on the client’s side. The account associated with this particular Google Home Mini was a gmail account. The particular gmail account was found when the mobile’s logical image was analysed.

The analysis was then performed on the account that was linked with the Google Home Mini. The account was a gmail account “**agrocks.gauher@gmail.com**”. Since analysing the Google Cloud servers was not possible in this research, therefore a manual account analysis was performed.

Examining My Activity

Google keeps a record of all the activities and applications that are used within the mobile. This feature can be found in the gmail account under My Activity. To access My Activity on the Google account the following steps were followed: Click on the profile at the top right corner → Manage your Google Account → Data and Personalization → Activity and timeline

box → My activity. My activity shows all the activities that are performed with the particular account. However, this information can only be viewed, if the user hasn't purposely deleted the activity from the account. The Google Home android application also maintains a record of all the commands given by a user in the application under "My Activity".

All the commands that are issued to Google Home Mini can be found along with additional details in My Activity. The figure 5-52 shows the information that was found for a particular command. The details that can be found for the particular command were the following:

- The date and the time that the command was issued
- The command that was issued
- Google Home Mini's response
- The application Google Home was used
- View recording

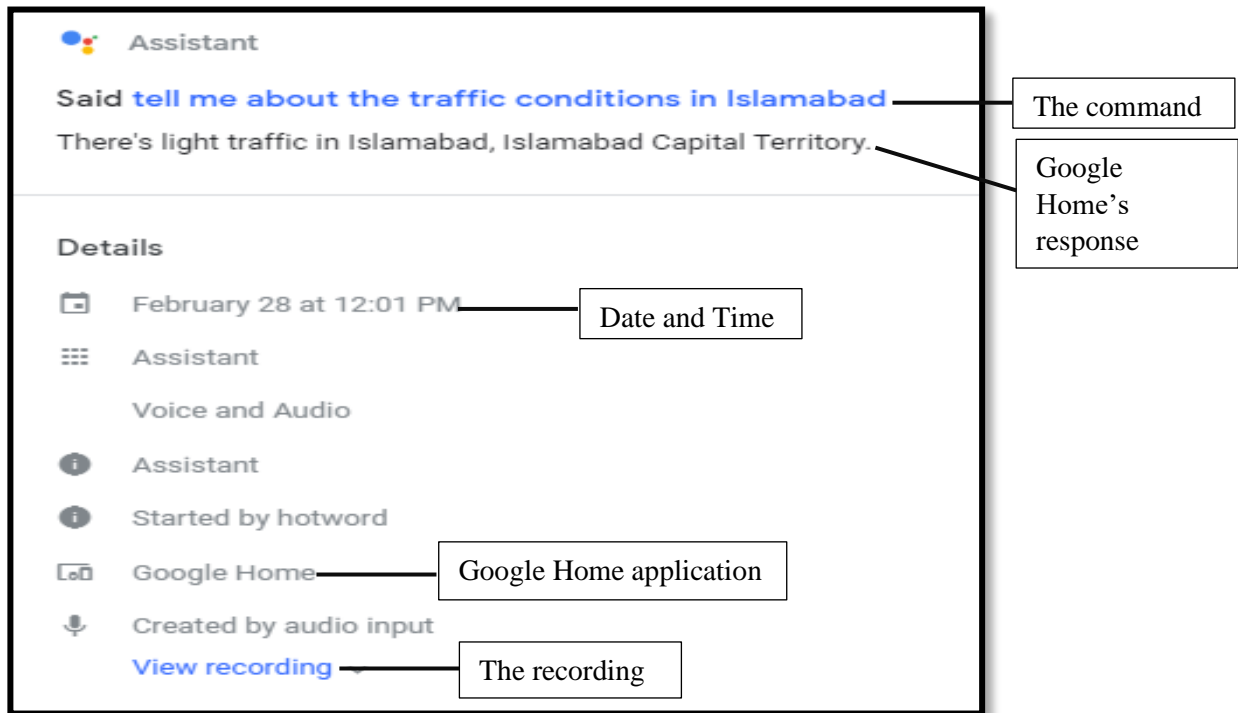


Figure 5-52 Details of a command found in My Activity

The table 5-8 shows a detailed view of the commands that were given to the Google Home Mini. The table only lists some of the commands but in fact many commands had been issued to the Google Home.

Sr.No	Commads given	Commands found in My Activity
1.	Good morning!	<p>Said good morning</p> <p>The time is 11:27 AM. And tomorrow, it'll be rainy. Currently in Islamabad it's seventy-one and partly cloudy. Today, it'll be partly cloudy, with a forecasted high of seventy-six and a low of fifty-seven. Have a great day!</p>
2.	Play news	<p>Said play news</p> <p>Here's the latest news.</p>
3.	Asking about the weather update	<p>Said what's the weather update</p> <p>Right now it's eighty with a thunderstorm. The forecast tonight is around eighty-one with a thunderstorm. Due to the current humidity, it feels like it's 87.</p>
4.	Asking about the traffic conditions	<p>Said can you tell me about the traffic conditions</p>
5.	Asking name	<p>Said what's my name</p> <p>Your name is Abeer.</p>
6.	Asking favourite food	<p>Said what's my favourite food</p> <p>You told me that you like pizzas</p>
7.	Asking favourite colour	<p>Said what's my favourite colour</p> <p>You told me that you like Black</p>
8.	Asking favourite book	<p>Said what's my favourite book</p> <p>You told me that you like Angels and Demons by Dan Brown</p>

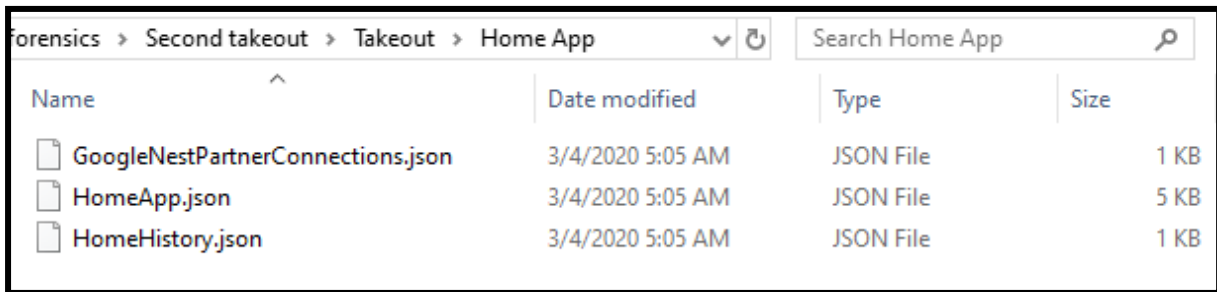
9.	Pair Bluetooth	<p>Said pair Bluetooth</p> <p>Got it.</p> <p>To connect, open bluetooth settings and look for the device called: Abeer's Room speaker.</p>
10.	Asking what to eat	<p>Said can you tell me what should I eat for dinner today</p> <p>I'm no foodie, but I can help you search for recipes</p>
11.	Asking seasons to watch	<p>Said can you suggest me some good seasons to watch</p>
12.	Asking the best tourist spots	<p>Said can you tell me the best tourist spots</p>
13.	Add items in the shopping list	<p>Said can you at toothpaste in my shopping list</p>
14.	Set an alarm	<p>Said can you set an alarm for me</p> <p>Alright, when's the alarm for?</p>
15.	Set a reminder	<p>Said can you set a reminder for me today</p> <p>Alright, today.</p> <p>At what time?</p>
16.	Create calendar event	<p>Said can you create a calendar event for me</p>
17.	Tell a joke	<p>Said tell me a joke</p> <p>What happens when a frog's car breaks? It gets toad.</p> <p>12:24 PM • Details • ↕</p>

18.	Tell a quote	<p>Said tell me a quote</p> <p>Dr. Seuss once said We're all a little weird, and life's a little weird. And when we find someone whose weirdness is compatible with ours, we join up with them and fall in mutual weirdness and call it love.</p>
19.	Tell a riddle	<p>Said tell me a riddle</p> <p>If you have one, you don't share it; if you share it, you don't have it...What is it? A secret</p>
20.	Tell an interesting fact	<p>Said tell me an interesting fact</p> <p>According to NASA, astronauts grow up to 3 percent taller during their time in space</p>
21.	Tell a poem	<p>Said tell me a poem</p> <p>Here's a poem from Lit to Go, from a collection called Lyrics of Lowly Life. It's read by Rick Kistner</p>
22.	Listen a story	<p>Said hey Google Jungle day</p> <p>Jungle Adventure Here's Jungle Adventure.</p>
23.	Sing a song for me	<p>Said hey Google sing a song for me</p> <p>I'd love to hear you sing, but your lyrics may confuse me</p>
24.	Count from 0 to 10	<p>Said count from 0 to 10</p> <p>OK: Zero, one, two, three, four, five, six, seven, eight, nine, ten</p>
25.	Tell a random number.	<p>Said tell me a random number from 0 to 100</p> <p>Here's a random number: twenty-two.</p>

Table 5-8 Commands found in My Activity

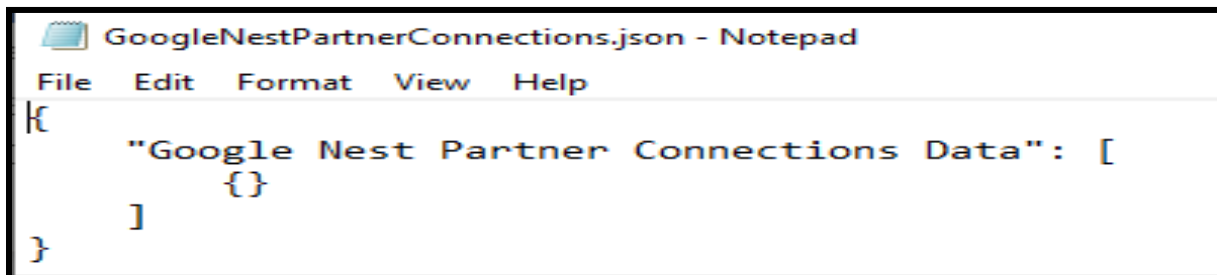
Extracting artifacts using the Google Takeout service

Google provides a Google Takeout service that can be used to extract data linked to various Google services such as the Google Play Store, Google Calendar, Google Photos, Google Home, Google Maps and the other services which are linked to Google. Google Takeout was used to extract data from the Google Home application. Google zips the file which can then be downloaded and unzipped to view the folders. The Home App folder was examined in the takeout. It contained three JSON files as can be seen in figure 5-53. Each of these files were then separately analysed. The Google Nest Partner Connections JSON file was empty as can be seen in figure 5-54.



Name	Date modified	Type	Size
GoogleNestPartnerConnections.json	3/4/2020 5:05 AM	JSON File	1 KB
HomeApp.json	3/4/2020 5:05 AM	JSON File	5 KB
HomeHistory.json	3/4/2020 5:05 AM	JSON File	1 KB

Figure 5-53 JSON files



```
GoogleNestPartnerConnections.json - Notepad
File Edit Format View Help
{
  "Google Nest Partner Connections Data": [
    {}
  ]
}
```

Figure 5-54 Google Nest Partner Connections JSON

The next JSON file Home App was examined and it contained some significant information about the Google Home Mini speaker. As can be seen in figure 5-57 the information that was found contained:

- Owner email

- Owner create time in seconds in UNIX format which was 1580366055. This translated into Thursday, January 30, 2020 11:34:15 AM as seen in figure 5-55. This time shows when the owner first created the account.

```
GMT : Thursday, January 30, 2020 6:34:15 AM
Your time zone : Thursday, January 30, 2020 11:34:15 AM GMT+05:00
```

Figure 5-55 Owner Create Timestamp conversion

- Name of the speaker
- Personalized nickname
- The address that the user has entered in the Home application
- The version timestamp in UNIX format which was 1580890168553. The timestamp was converted into readable format which translated to Wednesday, February 5, 2020 1:09 PM as seen in figure 5-56.

```
Assuming that this timestamp is in milliseconds:
GMT : Wednesday, February 5, 2020 8:09:28.553 AM
Your time zone : Wednesday, February 5, 2020 1:09:28.553 PM GMT+05:00
```

Figure 5-56 Version timestamp conversion

- The time zone

```
{
  "Home App Data": [
    {
      "full_structures": [{
        "owner_emails": ["agrocks.gauher@gmail.com"],
        "owner_create_times": [{
          "value": {
            "seconds": 1580366055,
            "nanos": 581000000
          },
          "key": "agrocks.gauher@gmail.com"
        }],
        "structure": {
          "create_time": {
            "seconds": 1580366057,
            "nanos": 249974000
          },
          "name": "Hostelite",
          "personalized_nicknames": ["Hostelite"],
          "physical_location": {
            "geo_coordinate": {
              "lng_degrees": 72.9916884,
              "lat_degrees": 33.6458516
            },
            "description": "NUST University, Islamabad, Pakistan",
            "version_timestamp": 1580890168553,
            "time_zone": "Asia/Karachi"
          }
        }
      }],
    }
  ]
}
```

Figure 5-57 Home app JSON file 1

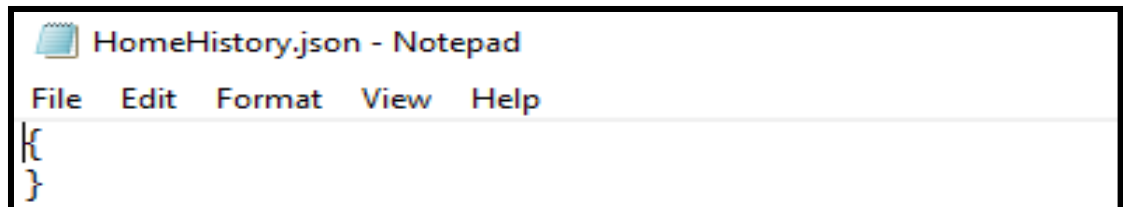
Further information was also found in this JSON file which can be seen in figure 5-58. This information helped to know the following:

- The device model id
- The model
- The creator's email
- The device's name
- The type of device that is associated
- The actions that are supported with this device which are Cast, Assistant, Remote Ducking, Communication Call, Communication Video Call

```
"device_info": {  
  "device_model_id": "Google Inc..mushroom.Google Home Mini",  
  "model": "Google Home Mini"  
},  
"create_time": {  
  "seconds": 1514271537,  
  "nanos": 702327000  
},  
"creator_emails": ["agrocks.gauher@gmail.com"],  
"agent_device_names": {"name": "Abeer\u0027s Room speaker"},  
"type": "action.devices.types.SPEAKER",  
"supported_traits": [  
  "action.devices.traits.Cast",  
  "action.devices.traits.Assistant",  
  "action.devices.traits.RemoteDucking",  
  "action.devices.traits.CommunicationCall",  
  "action.devices.traits.CommunicationVideoCall"  
]
```

Figure 5-58 Home app JSON file 2

The third JSON file Home History was examined but it didn't contain any data and turned out to be an empty file as seen in figure 5-59.

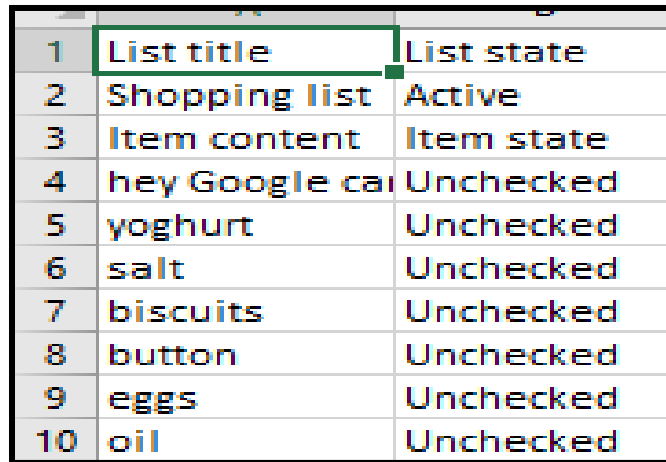


```
HomeHistory.json - Notepad  
File Edit Format View Help  
{  
}
```

Figure 5-59 Home History JSON file

The other folder that was included in the Google Takeout was the Assistant Notes and List folder. This folder contained an Excel sheet named Shopping List 2020-02-

13T07_11_24.829. The Excel sheet contained the shopping list that was created and all the items that were added to the shopping list as seen in figure 5-60.



1	List title	List state
2	Shopping list	Active
3	Item content	Item state
4	hey Google car	Unchecked
5	yoghurt	Unchecked
6	salt	Unchecked
7	biscuits	Unchecked
8	button	Unchecked
9	eggs	Unchecked
10	oil	Unchecked

Figure 5-60 Shopping list

The next folder that was examined was the My Activity folder. The My Activity folder contained additional folders and the Assistant folder was analysed. It contained all the recordings of all the commands that were issued to the Google Home Mini as seen in figure 5-61.

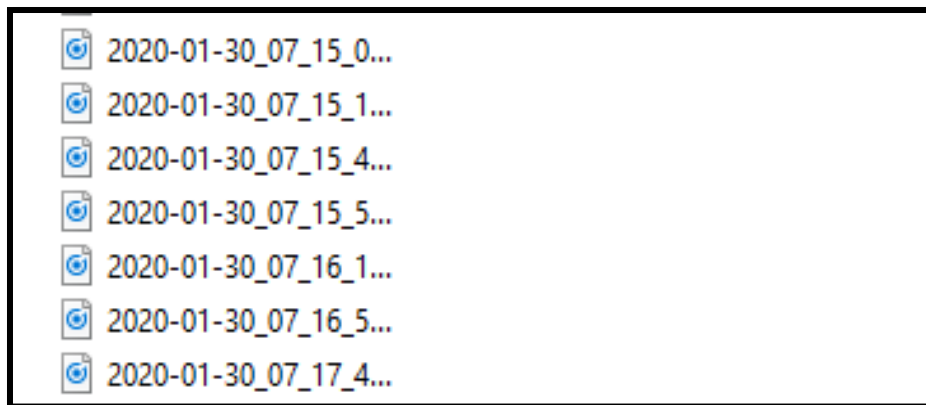


Figure 5-61 Voice recordings

3) Device Evidence Analysis

The device evidence analysis has to be carried out on the evidence that has been obtained either through a manual acquisition from the device or on the evidence that has been obtained from the chip in the device. It is highly possible that data that is retrieved from the chip would need to be parsed as it would be in a different format but can be overlooked if parsing is not needed.

However, as device forensics was out of the scope in this research, hence no evidence was acquired from the device and no analysis needed to be carried out. Since the IoT device could contain important evidence that is the reason that it needed to be part of the framework.

4) Network Evidence Analysis

The network packets were captured when the commands were issued to Google Home Mini. These packets that were captured during the acquisition phase were then analysed to find out the IP addresses that are involved in the communication along with the protocols that are used while communicating with a Google Home Mini.

Finding the IP addresses

The first important thing was to identify the IP address of the network that the forensic workstation was connected to. The IP address of the network was found in the properties of the desired network in the forensic workstation. The IP address of the network was 192.168.8.101. This meant that communications with the IP address 192.168.8.101 need to be filtered out. The protocol used for communication was TLS v1.2, hence all the traffic that was captured was encrypted. The IP address and the protocol that was used can be seen in figure 5-62.

Source	Destination	Protocol	Length	Info
192.168.8.1	239.255.255.250	SSDP	460	NOTIFY * HTTP/1.1
192.168.8.1	239.255.255.250	SSDP	460	NOTIFY * HTTP/1.1
wn-in-f188.1e100.net	192.168.8.101	TLSv1.2	332	Application Data

Figure 5-62 IP address and Protocol used

Finding the protocols used by Google Home Mini

Another protocol that Google Home Mini used for communication was the TCP protocol. The figure 5-63 shows that Google Home is communicating using TCP. The Google Home Mini's IP address was 192.168.8.100 and when the IP address was resolved it resulted in 0405737e-c26d-5110-3057-7a81d093271c.local. The port that Google Home Mini often used was the

8009 port and the same port was being used as was observed in the packet capture files that was done multiple times to verify the result.

Source	Destination	Protocol	Length	Info
0405737e-c26d-5110-...	192.168.8.101	TCP	74	8009 → 62295 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1460 SACK_PERM=1 TSval=44152 TSecr=2143147 WS=64
192.168.8.101	0405737e-c26d-5110-...	TCP	66	62295 → 8009 [ACK] Seq=1 Ack=1 Win=87680 Len=0 TSval=2143156 TSecr=44152
192.168.8.101	0405737e-c26d-5110-...	TCP	236	62295 → 8009 [PSH, ACK] Seq=1 Ack=1 Win=87680 Len=170 TSval=2143159 TSecr=44152 [TCP segment of a reassembl...
0405737e-c26d-5110-...	192.168.8.101	TCP	66	8009 → 62295 [ACK] Seq=1 Ack=171 Win=15552 Len=0 TSval=44154 TSecr=2143159
0405737e-c26d-5110-...	192.168.8.101	TCP	213	8009 → 62295 [PSH, ACK] Seq=1 Ack=171 Win=15552 Len=147 TSval=44154 TSecr=2143159 [TCP segment of a reassembl...
192.168.8.101	0405737e-c26d-5110-...	TCP	66	62295 → 8009 [ACK] Seq=171 Ack=148 Win=88704 Len=0 TSval=2143163 TSecr=44154
192.168.8.101	0405737e-c26d-5110-...	TCP	117	62295 → 8009 [PSH, ACK] Seq=171 Ack=148 Win=88704 Len=51 TSval=2143167 TSecr=44154 [TCP segment of a reasem...
0405737e-c26d-5110-...	192.168.8.101	TCP	66	8009 → 62295 [ACK] Seq=148 Ack=222 Win=15552 Len=0 TSval=44163 TSecr=2143167

Figure 5-63 Port used by Google Home Mini

The other protocol that Google Home Mini used during the communication over the network was the MDNS protocol as shown in figure 5-64. MDNS is Multicast Domain Name System and it operates over smaller networks and not on the Internet. MDNS and DNS both operate in the application layer and both of these use UDP. MDNS is used in networks that are trusted and some of the information transmitted using this protocol is visible. MDNS works by caching which prevents the network from flooding with a lot of traffic. The query is broadcasted to all the hosts that are on the network. The IP address that the Google Home Mini always communicates with using the MDNS protocol was 224.0.0.251[47].

Source	Destination	Protocol	Length	Info
LiteonTe_da:ee:f9	HuaweiTe_7a:b4:54	ARP	42	192.168.8.101 is at 50:5b:c2:da:ee:f9
0405737e-c26d-5110-...	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
0405737e-c26d-5110-...	224.0.0.251	MDNS	132	Standard query 0x0000 SRV google-home-mini-0405737ec26d511030577a81d093271c...
0405737e-c26d-5110-...	224.0.0.251	MDNS	410	Standard query response 0x0000 PTR Google-Home-Mini-0405737ec26d511030577a81...
0405737e-c26d-5110-...	224.0.0.251	MDNS	199	Standard query response 0x0000 SRV, cache flush 0 0 8009 0405737e-c26d-5110-...
0405737e-c26d-5110-...	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlezone._tcp.local, "QM" question

Figure 5-64 MDNS Protocol

The next observation made about the MDNS protocol was the query and responses that were sent and received. The query that was sent used the googlecast.tcp.local service string to cast the speaker[48]. As can be seen in figure 5-65, MDNS reveals information about the name along with the service string used to generate the query.

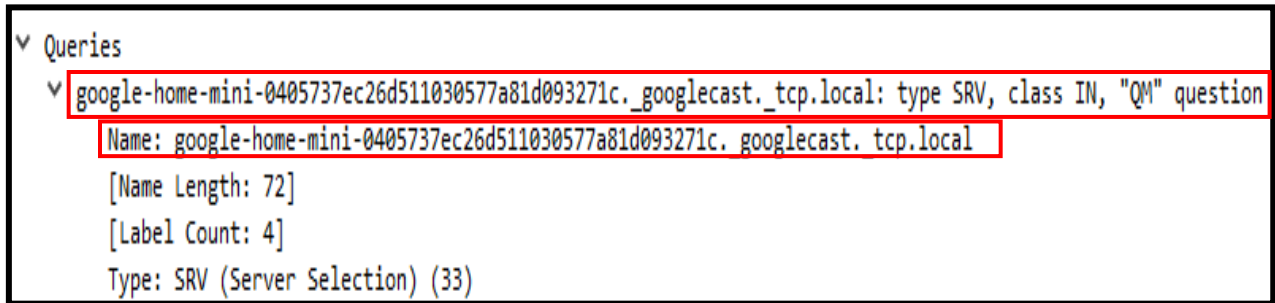


Figure 5-65 Service string used in MDNS

The response for this MDNS query was also received and it can be seen in figure 5-66. This response is due to the googlecast.tcp.local query that was sent. Further information, about this response can also be seen in the answers and additional records that Wireshark provides. The figure 5-67 shows the information that were found in the answers section of the query response. The name as seen is _googlecast._tcp.local and the domain name is Google-Home-Mini=0405737ec26d511030577a81d093271c._googlecast._tcp.local from which the response had been received.

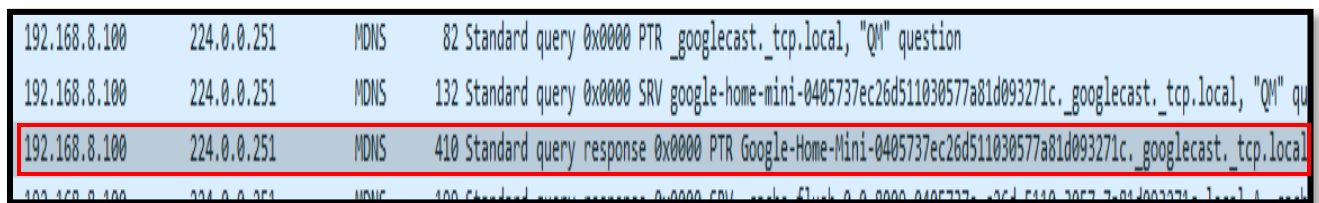


Figure 5-66 MDNS query response

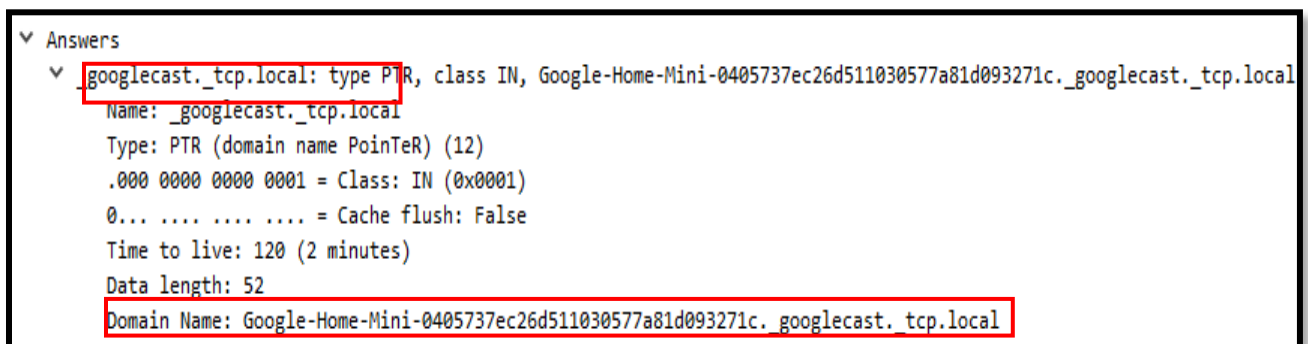


Figure 5-67 MDNS query response detailed view

The additional records revealed some important information which was not encrypted and can be seen in the figure 5-68. The first was the name, second was the unique id of the device, third was the version of the protocol which was 5, fourth was the model that was used, fifth was the path of the icon associated with the device and sixth was the friendly name used for the speaker.

```
Additional records
  Google-Home-Mini-0405737ec26d511030577a81d093271c._googlecast._tcp.local: type TXT, class IN, cache flush
    Name: Google-Home-Mini-0405737ec26d511030577a81d093271c._googlecast._tcp.local
    Type: TXT (Text strings) (16)
    .000 0000 0000 0001 = Class: IN (0x0001)
    1... .... .... .... = Cache flush: True
    Time to live: 4500 (1 hour, 15 minutes)
    Data length: 185
    TXT Length: 35
    TXT: id=0405737ec26d511030577a81d093271c
    TXT Length: 35
    TXT: cd=1C9B0E1A6C5389921302E2125A806DF7
    TXT Length: 3
    TXT: rm=
    TXT Length: 5
    TXT: ve=05
    TXT Length: 19
    TXT: md=Google Home Mini
    TXT Length: 18
    TXT: ic=/setup/icon.png
    TXT Length: 23
    TXT: fn=Abeer's Room speaker
    TXT Length: 9
```

Figure 5-68 Additional records as viewed in Wireshark

The MDNS protocol also sends queries and receives responses using another service which was the googlezone service. The googlezone is used for the Google Zone Cast services as it lists the speakers into individual zones using the Google Home application. These zones are assigned by the googlezone services whenever the speaker is used and can be seen in figure 5-69. The response for this query was received. As can be seen in figure 5-70 the name shows the id of the Google Home Mini along with the service that was used to generate the response to the query which was the googlezone.tcp.local service.

```
Queries
  _googlezone._tcp.local: type PTR, class IN, "QM" question
    Name: _googlezone._tcp.local
    [Name Length: 22]
    [Label Count: 3]
    Type: PTR (domain name PoinTeR) (12)
```

Figure 5-69 Googlezone service


```

v Additional records
  v 0405737e-c26d-5110-3057-7a81d093271c._googlezone._tcp.local: type TXT, class IN, cache flush
    Name: 0405737e-c26d-5110-3057-7a81d093271c._googlezone._tcp.local
    Type: TXT (Text strings) (16)
    .000 0000 0000 0001 = Class: IN (0x0001)
    1... .... .... .... = Cache flush: True
    Time to live: 4500 (1 hour, 15 minutes)
  
```

Figure 5-70 Response generated using googlezone service

Analysing packets captured while casting Bluetooth Audio

Google Home Mini can also be connected with the laptop by using Bluetooth. This was done by enabling Bluetooth on the forensic workstation and then pairing it with the speaker. Once the pairing was successful, then any audio that was played on the laptop was casted to the Google Home Mini speaker. Since the MDNS protocol is able to show some unencrypted information, it does show that Bluetooth Audio is being casted through the speaker. The certification authority used can also be seen in “ca”. This is shown in the figure 5-71.

```

v Additional records
  v Google-Home-Mini-0405737ec26d511030577a81d093271c._googlecast._tcp.local: type TXT, class IN, cache flush
    Name: Google-Home-Mini-0405737ec26d511030577a81d093271c._googlecast._tcp.local
    Type: TXT (text strings) (16)
    .000 0000 0000 0001 = Class: IN (0x0001)
    1... .... .... .... = Cache flush: True
    Time to live: 4500 (1 hour, 15 minutes)
    Data length: 200
    TXT Length: 35
    TXT: id=0405737ec26d511030577a81d093271c
    TXT Length: 35
    TXT: cd=1C9B0E1A6C5389921302E2125A806DF7
    TXT Length: 3
    TXT: rm=
    TXT Length: 5
    TXT: ve=05
    TXT Length: 19
    TXT: md=Google Home Mini
    TXT Length: 18
    TXT: ic=/setup/icon.png
    TXT Length: 23
    TXT: fn=Abeer's Room speaker
    TXT Length: 9
    TXT: ca=198660
    TXT Length: 4
    TXT: st=1
    TXT Length: 15
    TXT: bs=FA8FCA7A8607
    TXT Length: 4
    TXT: nf=1
    TXT Length: 18
    TXT: rs=Bluetooth Audio
  
```

Figure 5-71 Bluetooth audio casted

Analysing packets captured while casting news

Google Home Mini can be used to listen to the news. The MDNS query response using the googlecast service showed that news is being casted to the Google Home Mini along with the name of the news company as seen in figure 5-72. If a different news company is being used to cast news that was also visible in the additional records of the MDNS protocol as seen in figure 5-73.

```
TXT: md=Google Home Mini
TXT Length: 18
TXT: ic=/setup/icon.png
TXT Length: 23
TXT: fn=Abeer's Room speaker
TXT Length: 9
TXT: ca=215044
TXT Length: 4
TXT: st=1
TXT Length: 15
TXT: bs=FA8FCA7A8607
TXT Length: 4
TXT: nf=1
TXT Length: 35
TXT: rs=Casting: Headlines from BBC News
```

Figure 5-72 News being casted

```
TXT: ic=/setup/icon.png
TXT Length: 23
TXT: fn=Abeer's Room speaker
TXT Length: 9
TXT: ca=215044
TXT Length: 4
TXT: st=1
TXT Length: 15
TXT: bs=FA8FCA7A8607
TXT Length: 4
TXT: nf=1
TXT Length: 20
TXT: rs=Casting: Sky News
```

Figure 5-73 News being casted from a different news channel

Analysing packets captured while casting alarm

Google Home Mini can be used to set an alarm. The MDNS query response using the googlecast service showed that the alarm is being casted to the Google Home Mini along with the tune of the alarm that was being casted as seen in figure 5-74.

```
Name: Google-Home-Mini-0405737ec26d511030577a81d093271c.googlecast.tcp.local
Type: TXT (Text strings) (16)
.000 0000 0000 0001 = Class: IN (0x0001)
1... .... .... .... = Cache flush: True
Time to live: 4500 (1 hour, 15 minutes)
Data length: 206
TXT Length: 35
TXT: id=0405737ec26d511030577a81d093271c
TXT Length: 35
TXT: cd=1C9B0E1A6C5389921302E2125A806DF7
TXT Length: 3
TXT: rm=
TXT Length: 5
TXT: ve=05
TXT Length: 19
TXT: md=Google Home Mini
TXT Length: 18
TXT: ic=/setup/icon.png
TXT Length: 23
TXT: fn=Abeer's Room speaker
TXT Length: 9
TXT: ca=215044
TXT Length: 4
TXT: st=1
TXT Length: 15
TXT: bs=FA8FCA7A8607
TXT Length: 4
TXT: nf=1
TXT Length: 24
TXT: rs=Casting: LEGO Friends
```

Figure 5-74 Alarm being casted

Similarly, if a different type of tune is selected as the alarm then that was visible as seen in figure 5-75. However, if no special tune for the alarm is selected then no information is visible.

```
Name: Google-Home-Mini-0405737ec26d511030577a81d093271c.googlecast.tcp.local
Type: TXT (Text strings) (16)
.000 0000 0000 0001 = Class: IN (0x0001)
1... .... .... .... = Cache flush: True
Time to live: 4500 (1 hour, 15 minutes)
Data length: 203
TXT Length: 35
TXT: id=0405737ec26d511030577a81d093271c
TXT Length: 35
TXT: cd=1C9B0E1A6C5389921302E2125A806DF7
TXT Length: 3
TXT: rm=
TXT Length: 5
TXT: ve=05
TXT Length: 19
TXT: md=Google Home Mini
TXT Length: 18
TXT: ic=/setup/icon.png
TXT Length: 23
TXT: fn=Abeer's Room speaker
TXT Length: 9
TXT: ca=215044
TXT Length: 4
TXT: st=1
TXT Length: 15
TXT: bs=FA8FCA7A8607
TXT Length: 4
TXT: nf=1
TXT Length: 21
TXT: rs=Casting: LEGO Life
```

Figure 5-75 Different tune of alarm being casted

Analysing packets captured while asking questions

The packets were also captured when questions were asked to the Google Home Mini. However, the behaviour that was observed when the packets were analysed that the MDNS protocol only reveals information about what is being casted to the speaker such as news, Bluetooth audio or special type of alarms. No information is displayed when the Google Home Mini answers questions and that can be seen in figure 5-76.

```

Google-Home-Mini-0405737ec26d511030577a81d093271c._googlecast._tcp.local: type TXT, class IN, cache flush
Name: Google-Home-Mini-0405737ec26d511030577a81d093271c._googlecast._tcp.local
Type: TXT (Text strings) (16)
.000 0000 0000 0001 = Class: IN (0x0001)
1... .... .... .... = Cache flush: True
Time to live: 4500 (1 hour, 15 minutes)
Data length: 185
TXT Length: 35
TXT: id=0405737ec26d511030577a81d093271c
TXT Length: 35
TXT: cd=1C9B0E1A6C5389921302E2125A806DF7
TXT Length: 3
TXT: rm=
TXT Length: 5
TXT: ve=05
TXT Length: 19
TXT: md=Google Home Mini
TXT Length: 18
TXT: ic=/setup/icon.png
TXT Length: 23
TXT: fn=Abeer's Room speaker
TXT Length: 9
TXT: ca=198660
TXT Length: 4
TXT: st=0
TXT Length: 15
TXT: bs=FA8FCA7A8607
TXT Length: 4
TXT: nf=1
TXT Length: 3
TXT: rs= No information is displayed

```

Figure 5-76 Asking questions

5.4.3.2 Classifying the evidence

Evidence classification is the process which makes it easier to categorize the evidence as it reduces any kind of complexity that might arise due to evidence gathering from different devices and areas. The evidence gathered from different domains can be stored separately so as to prevent any mixing. The classification in this investigation was done into four categories as seen in figure 5-77 that were Application evidence, Cloud evidence, Network evidence, Device evidence and all the evidence was stored separately.

- 1) Application evidence – This included all the evidence that was obtained through the mobile device by the logical and the physical forensic images such as the account, user’s address, events, reminders, network information and associated timestamps.
- 2) Cloud evidence – This included all the screenshots that were gathered by examining the client’s side such as user’s activities, shopping lists, voice recordings, user’s address, device information like model id, name of the device and owner email linked to it.
- 3) Network evidence – This included all the packets that were captured by using a packet sniffer that revealed IP addresses, ports and protocols, services used, protocol version, certificate authority used, friendly name of the speaker and model name.
- 4) Device evidence – This should have included all the evidence that should have been obtained from the IoT device.

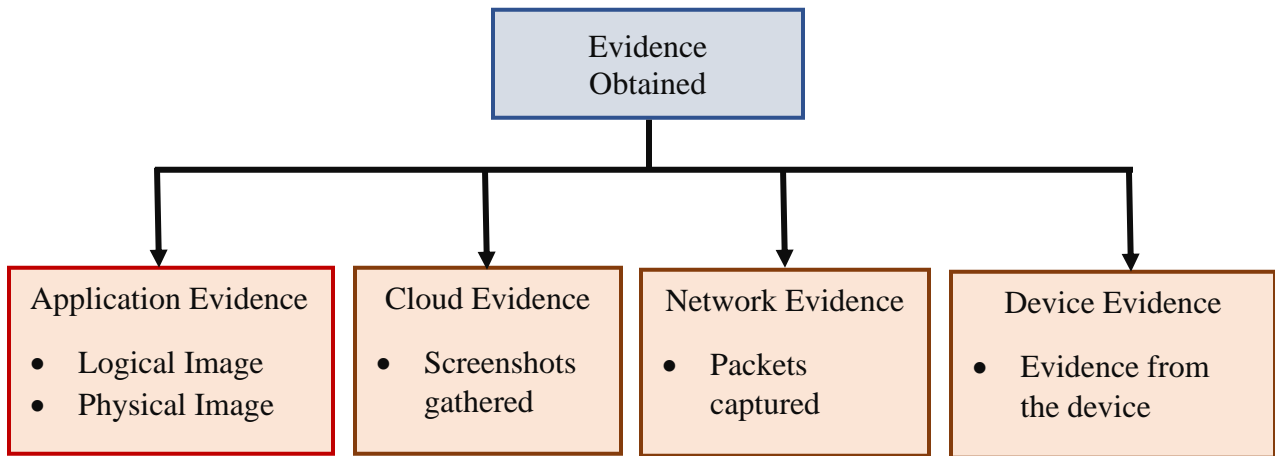


Figure 5-77 Classification of the evidence

5.4.3.3 Reporting

As a part of the investigation, it is very important for the digital forensic investigator to make reports that will be read by juries, judges, lawyers, clients and so on [49]. Since the report will be read by many different types of people, it is of utmost importance to make the report in a simple manner and use as less technical terms as possible [50]. The report can contain many different types of sections but usually forensic reports contain the case summary, forensic acquisition, findings and the conclusion. These four sections should be found in the report and these sections were part of the report that were made for the investigation in this research. The report can be found in this section.

REPORT

Case Summary

On 25th February 2020, I was contacted to be a lead investigator for a case involving an IoT device. The officials had found a Google Home Mini along with a mobile device that were handed over to me so that I could conduct a digital forensic investigation. A thorough investigation was requested to retrieve all the important artifacts from these devices.

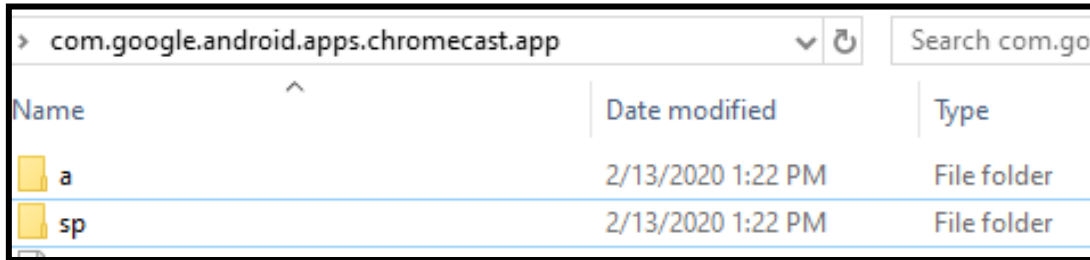
Forensic Acquisition

1. On 28th February 2020, I began to obtain a logical image of the mobile device. Before I started to obtain the forensic image, I documented all the details of the mobile device such as the make and model along with taking a picture of the mobile device to establish the chain of custody.
2. To acquire the logical image of the mobile device I had to connect it with my forensic workstation and use Android Debug Bridge to make a connection with the mobile device. After the connection was made successfully, I had run some commands that allowed me to acquire the logical image of the mobile device. The image was stored on the forensic workstation.
3. Once the logical image was acquired, to preserve the integrity of the image I made a copy of the image by using the copy and paste commands, since the logical image contained regular files and folders.

Findings

1. Once I had successfully acquired the logical image and made a copy, I had to analyse the image to extract the artifacts. As the image contained folders and files no tools were required to be used for the analysis process.

- The folders and the files were then investigated one by one. A folder named com.google.android.apps.chromecast.app was found. This folder further contained two other folders that were “a” and “sp” and these folders can be seen in the figure below .



The Chromecast folder

The first folder that is the “a” folder contained an apk file named as base.apk. The base.apk files are the files that are downloaded when the application is installed, so this base.apk file is for the Google Home application. The second folder that is the “sp” folder contained an XML file named com.google.android.apps.chromecast.app_preferences. This XML file contained data in plaintext and was viewed using a text editor and can be seen in the figure below. The XML file revealed the user’s account along with the version of the application.



The XML file

Conclusion

According to the findings, the user's account was revealed and the activities that the user had performed using the device were also found. Based on this, the user of the device can be easily confirmed to be as shown in the findings section which can be seen in the evidence that was found during the investigation.

5.4.3.4 Presentation

The next step after reporting is presentation. The forensic investigators present the reports that have been made in the reporting step. These reports are written formally that are read by many different people that include lawyers, judges, juries, law enforcement personnel's and any other person that is part of the investigation [51]. Similarly, in this investigation the report that was made in the reporting step was presented to the concerned authorities.

5.4.3.5 Investigation closure

Investigation closure is the last step in this phase. This is the final step where the court has adjourned the right criminal in presence of all the evidence. Once the criminal has been convicted depending on the law of each country and on the impact of the crime, the case can then be closed. Although all the evidence can be stored for future use if needed. In this research, since evidence was found against a single user then it can be concluded that this single user had committed the crime but in a real investigation multiple suspects are involved.

5.4.4 The Concurrent Phase

The concurrent phase is the phase which is carried out in parallel to all the other phases. This phase includes activities that are performed simultaneously with the other activities in the other phases. This phase included activities such as documentation, establishing a chain of custody and maintaining a chain of custody as seen in figure 5-78. Now since all the steps in this phase are performed simultaneously, so steps in these phases need not necessary be performed in a sequential manner. All the steps in this phase are discussed in this section.

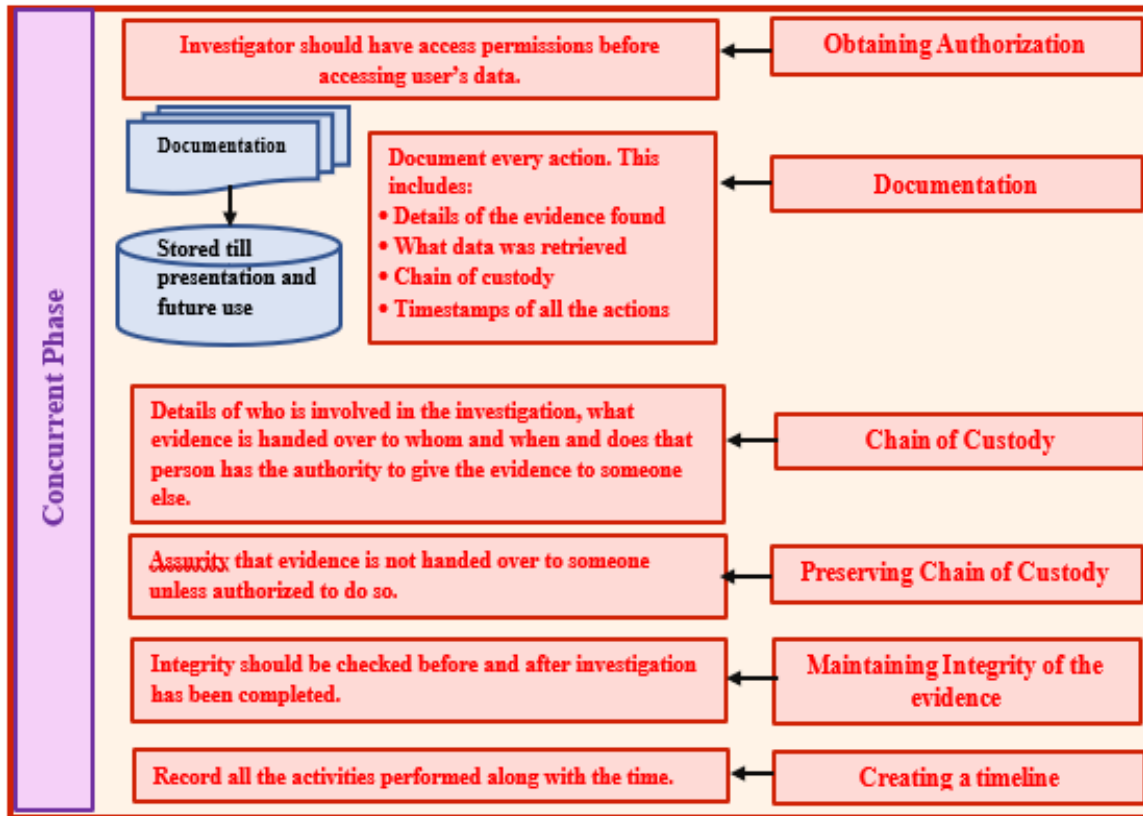


Figure 5-78 The Concurrent Phase

5.4.4.1 Obtaining authorization

In digital forensic investigations, authorization is concerned with having permissions by the digital forensic investigator to retrieve the relevant digital evidence, how and where to store the gathered evidence and know which data can be accessed and examined by the investigator which is part of the chain of custody [52]. Search warrants are also a way to obtain authorization by the investigator to search and seize any evidence if such circumstances arise.

In this research, as mentioned before the primary investigator was myself, thus all the authorization for collecting the evidence, storing and analysing was taken by me. As the digital forensic investigator, all the processes that were required to be carried out were carried out by me.

5.4.4.2 Documentation

Documentation is one of the most important process that needs to be carried out during the complete investigation which can be either done manually or done using a computer. Lately, special computer softwares have been designed such as Forensic Notes that can automate and

simplify the documentation process. The reason that documentation is carried out is that it helps to maintain a record of all the information and all the processes that are being carried out in the digital investigation, hence it is a continuous process [53]. The process of documentation includes physical and digital scene documentation. The documentation in this investigation was also done for both the physical and digital investigation as the investigation progressed.

First, the physical documentation was carried out which involved documenting all the device details that were found along with taking their pictures. The IoT device that was found was a Google Home Mini smart speaker and its details were recorded. The mobile device details were documented too. The mobile device had an Android operating system and the version of Android was 8.1. All the device documentation details was done in the evidence identification process in the acquisition phase.

Digital evidence documentation was done once the forensic images and the network packets were analysed. While documenting digital evidence folder names were recorded along with the file names inside the folders. Screenshots were taken of all the important evidence as can be seen in the image analysis for mobile forensics in the investigative phase. The names of the database files were also written that contained user related information. For the network packets that were captured, all the IP addresses and protocols that were being used were noted down. Furthermore, any unencrypted information that was found was documented as can be seen in the packet capture during the network evidence analysis phase such as the speaker's name and the ID of the speaker. The screenshots that were taken during the cloud investigation were analysed and all the information that was found during the analysis phase such as the commands given by the user, the user's account information, the name of the speaker, when the account was created was all documented during the cloud analysis step.

5.4.4.3 Chain of Custody

Establishing a chain of custody is one of the most important task that needs to be done in a digital forensic investigation as it helps to keep a record of who has what evidence currently and where this evidence was before and who has the authority to transfer the evidence and to whom. There should be certain steps taken that helps to establish the chain of custody and these steps were taken to establish a chain of custody in this investigation [54]. The steps that were taken are as follows:

- 1) Make copies of the original evidence: In a digital forensic investigation, to preserve the original evidence and prevent from causing any modifications, copies should be made of the original evidence. In this investigation, copies were made of the logical images and network packets that were captured and all the analysis was performed on the copies of the evidence rather than on the original evidence.
- 2) Capture photos of the physical evidence: It is important to take pictures of any physical evidence that is part of the investigation as it helps in making the chain of custody more authentic. The devices that were part of this investigation were all documented along with their details and pictures in the acquisition phase, precisely in the evidence identification step.
- 3) Taking screenshots of the digital evidence: Screenshots can be taken by the digital forensic investigator where no images can be acquired and these screenshots can be later examined. While acquiring evidence from the cloud environment, no forensic images could be made so screenshots were taken of the user's activities which were later analysed.
- 4) Documenting date and time: A forensic investigator should always document the date and time whenever he starts examining the evidence and when the evidence was handed over to another forensic investigator. This helps in building a timeline so that any discrepancies in the timeline can be looked into, if ever needed. In this investigation also a timeline was maintained of when and by whom the evidence had been investigated. The timeline can be seen in table 5-9. The timeline was recorded manually, since it was a small investigation, but softwares can be used to automate the process.

Evidence	Name of the forensic investigator	Date when the evidence was given	Start date of the evidence examination	End date of the evidence examination	Was the evidence given to someone else?
Captured network packets	Abeer Gauher	1 st March 2020	2 nd March 2020	12 th March 2020	No
Screenshots taken from the user's account	Abeer Gauher	15 th March 2020	16 th March 2020	26 th March 2020	No
Logical Image	Abeer Gauher	1 st April 2020	3 rd April 2020	10 th April 2020	No

Table 5-9 Timeline to maintain chain of custody for the evidence

5.4.4.4 Preserving Chain of Custody

Once this chain of custody is established, it is important to ensure that this chain is preserved and not disturbed in any way. Maintaining chain of custody assures that the evidence is not modified in any way which would present challenges in the court [55]. In addition, when the chain of custody is maintained properly, evidence can only be accessed by people who have permissions and evidence can only be transferred by someone who has the authority to do so. The chain of custody can be preserved by following all the procedures appropriately while establishing the chain of custody and by the help of the authorities who can constantly check on who has the evidence and how it is being handled. Preserving chain of custody in this investigation was done by following all the steps while establishing the chain of custody and since only a primary investigator was involved the evidence was not transferred to anybody else.

5.4.4.5 Maintaining Integrity of the evidence

One of the key points in a digital forensic investigation is to ensure that all the evidence that has been extracted from the devices is not modified in any way during the investigation that is the integrity of the evidence is maintained throughout. This is one of the reasons that maintaining the integrity is a parallel process that happens throughout the investigation. The integrity of the evidence needs to be maintained while the evidence is being extracted and analysed. The most common method is to generate hashes for the retrieved forensic images or to use a copy of the original evidence. The integrity in this investigation was maintained by making a copy of all the forensic images that included the logical and physical images obtained from the mobile device and the copy was used for analysis rather than the original forensic images. In addition, when the forensic images were being obtained from the mobile device, the mobile was put in airplane mode so as to prevent any modifications from the mobile network. Further, a copy was also made for all the network packets and screenshots that were taken from the client's side in the cloud environment and then those were analysed.

5.4.4.6 Creating a Timeline

Building a timeline during the digital forensic investigation, gives an overview of what activities occurred when. This helps other investigators to co – operate and know of what activities started when and by whom. Creating a timeline is a process that happens simultaneously as the

investigators perform their tasks and this can be recorded either manually, on a computer or a mobile depending on the scale and the nature of the evidence. Since the investigation in this research took place on a small scale and just involved one investigator, hence the timeline was built manually and can be found in the table 5-10. The timeline just gives an idea of how the investigators can record their activities.

TIMELINE		
Activity Performed	Date when the activity was performed	Duration
Case recorded by officials	1 st March 2020	1 day
Contacted to be investigator on this case	2 nd March 2020	1 day
Started with the investigation	4 th March 2020	1 day
Pre – Investigation Phase		
Planning the investigation	5 th March 2020 – 8 th March 2020	4 days
Preparing for the investigation	10 th March – 15 th March 2020	6 days
The Acquisition Phase		
Evidence Identification Process	18 th March 2020 – 19 th March 2020	2 days
Evidence Collection Process	20 th March 2020	1 day
Evidence Acquisition Process	21 st March 2020 – 30 th March 2020	10 days
Evidence Preservation and Storage	1 st April 2020	1 day
The Investigative Phase		
Evidence Analysis Process	3 rd April 2020 – 20 th April 2020	18 days
Classifying the evidence	21 st April 2020 – 25 th April 2020	5 days
Reporting	26 th April 2020 – 5 th May 2020	10 days
Presentation	6 th May 2020	1 day
Investigation close	6 th May 2020	1 day

Table 5-10 Creating a Timeline

CHAPTER 6

RESULTS AND DISCUSSION

6.1 Introduction

In this chapter, the results have been discussed along with the evaluation of the research questions that were designed for this research and can be found in Chapter – 1. The following sections are included in this chapter:

6.2: Evaluating the research questions

6.3: Comparative analysis of the framework

6.2 Evaluating the research questions

Primarily five research questions were designed which were the basis for conducting this research. After the research had been completed successfully and the results were obtained, then the answers to these research questions were made possible based on the results. The research questions have been answered in a descriptive way in this section.

6.2.1 RQ – 1

Is the proposed framework generic or designed for a specific type of IoT device?

The proposed framework has been specifically designed to aid digital forensic investigators to carry out investigations that involve any kind of IoT device. As can be seen in the framework which can be found in Chapter – 5 that no specific device has been mentioned in the framework which implicates that the framework has not been designed for a special IoT device but can be used for any kind of IoT device.

6.2.2 RQ – 2

Has the proposed framework been tested and verified on any IoT device?

Yes, the proposed framework has been tested and verified on an IoT device which was the Google Home Mini smart speaker. Testing ensured that all evidence was able to be acquired that would be needed for the investigation.

6.2.3 RQ – 3

Will the forensic investigator be able to gather evidence by following the framework during an active investigation?

Yes, the forensic investigator will be able to gather evidence by following the framework as the framework contains evidence acquisition phase which includes steps to gather evidence from different domains during the investigation.

6.2.4 RQ – 4

Can the forensic investigator perform additional tasks during the investigation or does one need to follow only the steps in the framework?

The advantage with designing frameworks are that they can be altered depending on the investigation, so if additional tasks are needed to be performed then those can be performed. The proposed framework contains all the basic steps that if followed will result in a successful investigation.

6.2.5 RQ – 5

Does the framework address chain of custody and evidence integrity?

Yes, the framework addresses chain of custody and evidence integrity as these are one of the most important activities during forensic investigation. Although, one thing that needs to be noted is that the way these activities are performed can differ from investigation to investigation.

6.3 Comparative analysis of the framework

This research was aimed at developing a generic forensic investigation framework that would help investigators in successfully acquiring evidence and reaching conclusions based on the that evidence. The proposed framework was designed in such a way that it would cater for the flaws that existed in the already proposed frameworks by previous researches. To demonstrate this fact, the framework has been compared with the most recent and the most important frameworks to

show what the proposed framework provides. The detailed comparison can be seen in table 6-1. The first column of the table is the framework that has been proposed in this research while the other three columns contain the framework that have been proposed by previous researches. Since the framework is divided into four different phases, the table also contains the four different phases and comparison has been made on those phases. Each of these phases contain all the steps that have been performed in this research. All the three frameworks were studied appropriately to understand what steps had been followed in those frameworks, so that a correct comparison could have been made.

Processes	Generic Framework for IoT Forensic Investigation	IoT digital forensic model (2015)	Digital Forensic Investigation Framework for Internet of Things (2016)	Framework for IoT Data Acquisition and Forensics Analysis (2018)	IoT – Forensic Readiness Framework (2020)
Pre-Investigation Phase					
Planning the investigation	✓	✓	✓		
Preparing for the investigation	✓				
The Acquisition Phase					
Evidence Identification Process	✓		✓	✓	✓
Evidence Collection Process	✓	✓	✓	✓	✓
Evidence Acquisition Process	✓				
1.Mobile Forensics	✓		✓	✓	✓
2.Cloud Forensics	✓	✓	✓	✓	
3.Device Forensics	✓	✓		✓	✓
4.Network Forensics	✓		✓		✓
Evidence Storage and Preservation Process	✓		✓		
The Investigative Phase					
Evidence Analysis Phase	✓				

1.Mobile Evidence Analysis	✓			✓	✓
2. Cloud Evidence Analysis	✓		✓	✓	
3.Device Evidence Analysis	✓		✓		✓
4.Network Evidence Analysis	✓		✓		✓
Classifying the evidence	✓				
Reporting	✓		✓		✓
Presentation	✓		✓		✓
Investigation closure	✓		✓		
The Concurrent Phase					
Obtaining authorization	✓	✓	✓		
Documentation	✓		✓		
Chain of Custody	✓	✓			
Preserving chain of custody	✓		✓		
Maintaining Integrity of the evidence	✓		✓		
Creating a timeline	✓				

Table 6-1 Comparing frameworks

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Introduction

This chapter concludes the thesis and discusses future directions that can be carried out for this research. It contains the following sections:

7.2: Conclusion

7.3: Future Work

7.2 Conclusion

The improvement in technology has allowed for a sharp increase in bandwidth in just a couple of years. This has made it possible for people to be connected with other people and simultaneously with a range of electronic devices that provide connectivity through the Internet. These devices have progressed and have been known as smart devices leading to the creation of Internet of Things which primarily makes it possible for people and devices to be connected from anywhere and at any time.

From then onwards, IoT devices have become quite an essential part of one's life enabling one to perform basic everyday functions. This is where the problem arises. The inter connectivity of these devices poses a threat and creates opportunities for adversaries to perform malicious actions. Whenever a malicious action is performed that threatens user's privacy or causes malfunction or any other harmful effect that means a digital forensic investigation needs to be conducted. To carry out a successful digital forensic investigation the forensic investigator needs proper guidelines on how the investigation should proceed. This guideline can be provided through investigation frameworks that ensures effective evidence gathering and analysis procedures.

In this research, a generic forensic investigation framework was proposed that was targeted at aiding investigators in carrying out investigations that involved any kind of an IoT device. This generic framework had been specifically designed to cater for the missing components in the

previous investigation framework. The framework is comprehensive as it contains detailed sub – steps for each step and how each step is executed which hasn't been explored in length in any of the previous researches.

Along with proposing the framework, the framework has also been tested on an investigation that was designed specifically for this research which included an actual IoT device. The investigation was carried by following all the steps in the framework which made it possible to retrieve important artifacts in relation to the IoT device. In addition, other important procedures were also carried out that were establishing and maintain a chain of custody, documenting and maintaining evidence integrity.

7.3 Future Work

The future work for this research can include a myriad of possibilities. Firstly, even though gathering and analysing evidence from the IoT device is part of the framework it wasn't carried out, so the device can explored and data can be retrieved from the IoT device. This can reveal the data that the IoT device can store. Secondly, obtaining data from the cloud servers was not possible as access wouldn't have been provided, so the cloud servers need to be also examined which would reveal further information about the user and the activities performed by the user. Moving on to the framework, the framework can include additional steps such as incident detection and other legal formalities that are needed to be fulfilled during an investigation. Incident can be added in the first phase of the framework where whenever an incident is detected investigations can be started as soon as possible.

CHAPTER 8

REFERENCES

- [1] Open Learn, “What is forensic science”, 2015. [Online], Available: <https://www.open.edu/openlearn/science-maths-technology/what-forensic-science>. [Accessed: 6th February 2020].
- [2] NIST, “Computer Security Resource Center”, [Online]. Available: <https://csrc.nist.gov/glossary/term/digital-forensics>. [Accessed: 6th February 2020].
- [3] Dr. A. Singh, C. Kent, “The What, Why and How of Digital Forensics”, 2018. [Online]. Available: <https://www.lawtechnologytoday.org/2018/05/digital-forensics/>. [Accessed: 6th February 2020].
- [4] Techopedia, “Digital Forensics”, [Online]. Available: <https://www.techopedia.com/definition/27805/digital-forensics>. [Accessed: 6th February 2020].
- [5] Open Learn, “Different types of digital forensics”, [Online]. Available: <https://www.open.edu/openlearn/science-maths-technology/digital-forensics/content-section-4.3>. [Accessed: 7th February 2020].
- [6] M. Rouse, “Computer forensics (cyber forensics)”, 2013. [Online]. Available: <https://searchsecurity.techtarget.com/definition/computer-forensics>. [Accessed: 7th February 2020].
- [7] A Simplified Guide to Digital Evidence, “Introduction”, [Online]. Available: <http://www.forensicssciencesimplified.org/digital/>. [Accessed: 11th February 2020].
- [8] Athena Forensics, “Digital Evidence and Legal Proceedings”, 2018. [Online]. Available: <https://athenaforensics.co.uk/digital-evidence-and-legal-proceedings/>. [Accessed: 11th February 2020].

- [9] K. L. Luth. “Why the Internet of Things is called Internet of Things: Definition, history, disambiguation”, 2014. [Online]. Available: <https://iot-analytics.com/internet-of-things-definition/>. [Accessed: 11th February 2020].
- [10] EGHAM, “Gartner Says 5.8 Billion Enterprise and Automotive IoT Endpoints Will Be in Use in 2020”, 2019. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2019-08-29-gartner-says-5-8-billion-enterprise-and-automotive-io>. [Accessed: 11th February 2020].
- [11] Gartner, “Internet of Things”, [Online]. Available: <https://www.gartner.com/en/information-technology/glossary/internet-of-things>. [Accessed: 11th February 2020].
- [12] J. Clark, “What is the Internet of Things?”, 2016. [Online]. Available: <https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/>. [Accessed: 11th February 2020].
- [13] K. Chandrashekhar, “Internet of Things (IoT) Characteristics”, 2016. [Online]. Available: <https://www.linkedin.com/pulse/internet-things-iot-characteristics-kavyashree-g-c>. [Accessed: 12th February 2020].
- [14] WEBCO, “Fundamental characteristics that makes the ‘Internet of Things’ what it is:”, [Online]. Available: <https://www.webchoiceonline.com.au/fundamental-characteristics-that-makes-the-internet-of-things-what-it-is/>. [Accessed: 12th February 2020].
- [15] P. Sethi and S. R. Sarangi, “Internet of Things: Architectures, Protocols, and Applications”, *Journal of Electrical and Computer Engineering*, vol.2017, 2017
- [16] N. H. N. Zulkipli, A. Alenezi, G. B. Wills, “IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things”, in *2nd International Conference on Internet of Things, Big Data and Security*, vol.1, pp. 315-324, Portugal, 2017
- [17] P. Muncaster, “Over 100 Million IoT Attacks Detected in 1H 2019”, [Online]. Available: <https://www.infosecurity-magazine.com/news/over-100-million-iot-attacks/>. [Accessed: 12th February 2020].
- [18] R. Dunn, “IoT Applications in Forensics”, 2019. [Online]. Available: <https://www.linkedin.com/pulse/internet-things-iot-characteristics-kavyashree-g-c>. [Accessed: 17th February 2020].

- [19] E. Oriwoh, D. Jazani, G. Epiphaniou, P. Sant, “Internet of Things Forensics: Challenges and Approaches”, in *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Austin, USA, 2013
- [20] S. Alabdulsalam, K. Schaefer, T. Kechadi, N. A. L. Khac, “INTERNET OF THINGS FORENSICS: CHALLENGES AND CASE STUDY”, *IFIP International Conference on Digital Forensics*, Digital Forensics 2018: Advances in Digital Forensics XIV, pp 35-48,
- [21] “Attacks on Internet of Things. How to Reduce Cost and Improve Safety of IoT?”, 6 Mar, 2020 [Online]. Available: <https://lifars.com/2020/06/iot-device-attacks/>. [Accessed: 15th February 2020]
- [22] S. Perumal, N. Md Norwawi, V. Raman, “Internet Of Things(IoT) Digital Forensic Investigation Model: Top-Down Forensic Approach Methodology”, in *Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, Sierre, Switzerland, 2015
- [23] M. Harbawi, A. Varol, “An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I: A Theoretical Framework”, in *5th International Symposium on Digital Forensic and Security (ISDFS)*, Tirgu Mures, Romania, 2017
- [24] V. R. Kebande, I. Ray, “A Generic Digital Forensic Investigation Framework for Internet of Things(IoT)”, in *IEEE 4th International Conference on Future Internet of Things and Cloud*, Vienna, Austria, 2016
- [25] V. R. Kebande, N. M. Karie, A. Michael, S. Malapane, I. Kigwana, H.S.Venter, R. D. Wario, “Towards an Integrated Digital Forensic Investigation Framework for an IoT-Based Ecosystem”, in *IEEE International Conference on Smart Internet of Things*, Xian, China, 2018
- [26] T. Zia, P. Liu, W. Han, “Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)”, in *12th International Conference on Availability, Reliability and Security(ARES '17)*, pp 1–7, 2017
- [27] H. Chi, T. Aderibigbe, B. C. Granville, “A Framework for IoT Data Acquisition and Forensics Analysis”, in *IEEE International Conference on Big Data (Big Data)*, Seattle, USA, 2018

- [28] V. R. Kebande, P.P. Mudau, R.A.Ikuesan,H.S.Venter, K.K.R.Choo “Holistic digital forensic readiness framework for IoT-enabled organizations ,” *Forensic Science International:Reports*, vol.2, 2020.
- [29] From Wikipedia, the free encyclopedia. “Google Nest (smart speakers)”, [Online]. Available:[https://en.wikipedia.org/wiki/Google_Nest_\(smart_speakers\)#Original_Google_Home_speaker](https://en.wikipedia.org/wiki/Google_Nest_(smart_speakers)#Original_Google_Home_speaker). [Accessed: 10th March 2020].
- [30] I. Yildirim, E. Bostanci, M. S. Guzel, “Forensic Analysis of Amazon Alexa and Google Assistant Built-In Smart Speakers”, *International Journal of Innovation Engineering and Science Research*, vol.3, issue 3, pp 59 – 67, 2019
- [31] S. Engelhardt, “Smart Speaker Forensics (2019)” Business/Business Administration. [Online]. Available: https://scholarsarchive.library.albany.edu/honorscollege_business/56 . [Accessed: 12th March 2020].
- [32] J. W. Creswell, Educational research: Planning, conducting, and evaluating quantitative and qualitative research, vol. 4. 2012.
- [33] Z. Doffman, “Cyberattacks On IOT Devices Surge 300% In 2019, ‘Measured In Billions’, Report Claims”, [Online]. Sep 14, 2019, Available: <https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/#45444d858926>. [Accessed: 18th March 2020].
- [34] Software Testing Help, “18 Most Popular IoT Devices In 2020 (Only Noteworthy IoT Products)”, [Online]. Apr 16, 2020, Available: <https://www.softwaretestinghelp.com/iot-devices/> [Accessed: 20th April 2020].
- [35] Dr B. Parsons, “Five Key Steps For Digital Forensics and Incident Response”, [Online]. Oct 28, 2016, Available: <https://www.informationsecuritybuzz.com/articles/five-key-steps-digital-forensics-incident-response/>. [Accessed: 25th April 2020].
- [36] S. Abdalla, S. Hazem, S. Hashem, “Guideline Model for Digital Forensic Investigation”, *Annual ADFSL Conference on Digital Forensics, Security and Law*, 2007

- [37] Universal Data Forensics, “DATA ACQUISITION”, [Online]. Available: <http://www.forensiccomputerservice.com/general-services/data-acquisition.aspx>. [Accessed: 30th April 2020].
- [38] S. Tahiri, “Android Forensic Logical Acquisition”, [Online]. Available: <https://resources.infosecinstitute.com/android-forensic-logical-acquisition/#gref>. [Accessed: 2nd May 2020].
- [39] D. Nelson, Pratum, “Why Consider Live Acquisition for Your Next Digital Forensics Case”, [Online]. Jul 1, 2020 Available: <https://pratum.com/blog/454-why-consider-live-acquisition-for-your-next-digital-forensics-case> [Accessed: 5th May 2020].
- [40] “What is Digital Forensics? History, Process, Types, Challenges”, [Online]. Available: <https://www.guru99.com/digital-forensics.html#4>. [Accessed: 7th May 2020].
- [41] H. Keller, “Everything You Need to Know About Google Home”, [Online]. Available: <https://www.architecturaldigest.com/story/google-home-assistant-smart-home-hub>. [Accessed: 10th May 2020].
- [42] Cdunn, Alexa Dev Group, “Developing for Google Home”, [Online]. Aug 16,2018 Available: <http://www.alexadevgroup.com/developing-for-google-home/>. [Accessed: 11th May 2020].
- [43] C. O Nolan, Obtaining Forensic Images from Android Devices, [Online]. Available: <https://study.com/academy/lesson/obtaining-forensic-images-from-android-devices.html#:~:text=Having%20a%20forensic%20image%20will,objects%20plus%20any%20deleted%20files.&text=Most%20methods%20of%20forensic%20imaging,cable%20to%20a%20host%20computer>. [Accessed: 12th May 2020].
- [44] S. Ganesh, “Download Magisk.zip and Magisk Manager App All Versions”, [Online]. May 9, 2020, Available: <https://www.androidinfotech.com/magisk-versions-download/>. [Accessed: 14th May 2020].
- [45] TeamWin – TWRP “Download twrp-3.3.1-0-bullhead.img”, [Online]. Available: <https://dl.twrp.me/bullhead/twrp-3.3.1-0-bullhead.img.html>. [Accessed: 14th May 2020].
- [46] M. Park, J. I. James, “Preliminary Study of a Google Home Mini”, in *Journal of Digital Forensics*, vol.12, issue 1, June 2018

- [47] “Packet sniffing a Google Home”, [Online]. Oct 28, 2018 Available: <https://itp.beverlychou.com/packet-sniffing-a-google-home/>. [Accessed: 15th May 2020].
- [48] “Chromecast as mDNS Service in order to Cast Screen Configuration on WLC”, Jan12, 2017 [Online]. Available: <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-mobility/119017-config-chromecast-mdns-wlc-00.html>. [Accessed: 15th May 2020].
- [49] Computer Forensics Investigation – A Case Study, Apr 6, 2018 [Online]. Available: <https://resources.infosecinstitute.com/computer-forensics-investigation-case-study/#gref>. [Accessed: 19th May 2020].
- [50] B. Garnet, “Intro to Report Writing for Digital Forensics”, 25 Aug 2010, Available: <https://www.sans.org/blog/intro-to-report-writing-for-digital-forensics/>. [Accessed: 20th May 2020].
- [51] J. Ahearne, “Digital Forensic Process—Presentation”, [Online]. Apr 4, 2018 Available: <https://drivesaversdatarecovery.com/blog/digital-forensic-process-presentation/>. [Accessed: 24th May 2020].
- [52] Norwich University Online, “5 Steps for Conducting Computer Forensics Investigations”, [Online]. Sep 11,2017 Available: <https://online.norwich.edu/academic-programs/resources/5-steps-for-conducting-computer-forensics-investigations>. [Accessed: 28th May 2020]
- [53] T. M. J. Abbas, “Studying the Documentation Process in Digital Forensic Investigation Frameworks/ Models”, *Journal of Al-Nahrain University*, vol.18, issue 4, pp.153-162, December, 2015
- [54] Computer Forensics: Chain Of Custody, [Online]. 2019 Available: <https://resources.infosecinstitute.com/category/computerforensics/introduction/areas-of-study/legal-and-ethical-principles/chain-of-custody-in-computer-forensics/#gref>. [Accessed: 1st June 2020]
- [55] Discovery Services, “Preserving Chain of Custody in E-Discovery”, White Paper