Team bi0s

Amrita Vishwa Vidhyapeetham

Amritapuri Campus

DFRWS Forensic Challenge

– IoT Forensic Challenge 2018-2019 –

Authors

E T Karthik Nambiar (kartik997@gmail.com)

P Abhiram Kumar (abhiram1999@gmail.com

Harikrishnan R (hr4hkr@gmail.com)

Jaswanth B (jassu.bommidi@gmail.com)

Contents

Introduction

The DFRWS 2018 challenge is about Internet of Things (IoT), defined generally to include network and Internet connected devices usually for the purpose of monitoring and automation tasks. Consumer-grade "Smart" devices are increasing in popularity and scope. These devices and the data they collect are potentially interesting for digital investigations, but also come with a number of new investigation challenges.

This DFRWS Forensic Challenge aspires to motivate new approaches to forensic analysis and has four levels of participation:

1. ***Device Level Analysis:*** Developing methods and tools to forensically process digital traces generated by IoT devices, including on mobile devices.

2. ***Network Level Analysis:*** Dev1. eloping methods and tools to forensically process digi2. tal traces generated by IoT devices on networks.

3. ***Correlation and Analysis:*** Developing methods and supporting tools that combine information from various data sources and automatically compute, visualize, or otherwise expose patterns of potential interest.

4. ***Evaluating and Expressing Conclusions:*** Assigning the probability of the results given two competing propositions (e.g. The

prime suspect committed the offense, versus some unknown person did).

1.1 Challenge Scenario

On 17 May 2018 at 10:40, the police were alerted that an illegal drug lab was invaded and unsuccessfully set on fire. The police respond promptly, and a forensic team is on scene at 10:45, including a digital forensic specialist.

The owner the illegal drug lab, Jessie Pinkman, is nowhere to be found. Police interrogate two of Jessie Pinkman's known associates: D. Pandana and S. Varga. Pandana and Verga admit having access to the drug lab's WiFi network but deny any involvement in the raid. They also say that Jessie Pinkman's had the IoT security systems installed because he feared attacks from a rival gang and that Jessie kept the alarm engaged in "Home" mode whenever he was inside the drug lab. Within the drug lab (** see diagram) the digital forensic specialist observes some IoT devices, including an alarm system (iSmartAlarm), three cameras (QBee Camera, Nest Camera and Arlo Pro) as well as a smoke detector (Nest Protect). An Amazon Echo and a WinkHub are also present.

The digital forensic specialist preserves the diagnostic logs from the iSmartAlarm base station, and acquires a copy of the filesystem of the WinkHub. He also collects the iSmartAlarm and Arlo base stations to perform an in-depth analysis at the forensic laboratory.

Back at the forensic laboratory, the digital forensic specialist uses the bootloader to collect a memory image of the two base stations as well as an archive of some folder of interest of the Arlo base station.

Jessie Pinkman's Samsung Galaxy Edge S6 is found at the scene,

likely dropped during the raid. The digital forensic specialist acquires a physical image of this Samsung device.

1.2 Challenge Questions

The Attorney General needs answers to the following questions:

a.) At what time was the illegal drug lab raided?

b.) Could any of the two friends of Jessie Pinkman have been involved in the raid?

If ***YES:***

1. Which friend?
2. What is the confidence in such hypothesis?

c.) How was the QBee camera disabled?

1.3 Devices recovered from crime scene

(1.) Physical extraction of Jessie Pinkman's Samsung phone
File/Folder: Samsung `GSM_SM-G925F` Galaxy S6 Edge.7z
SHA256: ae83b8ec1d4338f6c4e0a312e73d7b410904fab504f7510723362efe6186b757

(2.) iSmartAlarm – Diagnostic logs
File/Folder: ismartalarm/diagnostics/`2018-05-17T10_54_28`/`server_stream`
SHA256: 8033ba6d37ad7f8ba22587ae560c04dba703962ed16ede8c36a55c9553913736

(3.) iSmartAlarm – Memory images: 0x0000'0000 (`ismart_00.img`), 0x8000'0000(`ismart_80.img`)
File/Folder: dump/`ismart_00.img`,
SHA256: b175f98ddb8c79e5a1e7db84eeaa691991939065ae17bad84cdbd915f65d9a10
dump/`ismart_80.img`

SHA256: b175f98ddb8c79e5a1e7db84eeaa691991939065ae17bad84cdbd915f65d9a10

(4.) Arlo – Memory image
File/Folder: arlo/`dfrws_arlo.img`
SHA256: 3b957a90a57e5e4485aa78d79c9a04270a2ae93f503165c2a0204de918d7ac70

(5.) Arlo – NVRAM settings
File/Folder: arlo/nvram.log
SHA256: f5d680d354a261576dc8601047899b5173dbbad374a868a20b97fbd963dca798

(6.) Arlo – NAND: TAR archive of the folder /tmp/media/nand
File/Folder: arlo/`arlo_nand.tar.gz`
SHA256: 857455859086cd6face6115e72cb1c63d2befe11db92beec52d1f70618c5e421

(7.) WinkHub – Filesystem TAR archive
File/Folder: wink/wink.tar.gz
SHA256: 083e7428dc1d0ca335bbcfc11c6263720ab8145ffc637954a7733afc7b23e8c6

(8.)Amazon Echo – Extraction of cloud data obtained via CIFT
File/Folder: echo/`(2018-07-01_13.17.01)_CIFT_RESULT.zip`
SHA256: 7ee2d77a3297bb7ea4030444be6e0e150a272b3302d4f68453e8cfa11ef3241f

(9.)Network capture
File/Folder: `network/dfrws_police.pcap`
SHA256: 1837ee390e060079fab1e17cafff88a1837610ef951153ddcb7cd85ad478228e

1.4 Concept Diagram

Illegal Drug Laboratory: This is the picture of the crime scene according to the list of digital devices and the interrogation of D. Pandana and S. Varga. Only three of these people, Jessie Pinkman and the other two had access to this lab and also they had access to the security systems too.

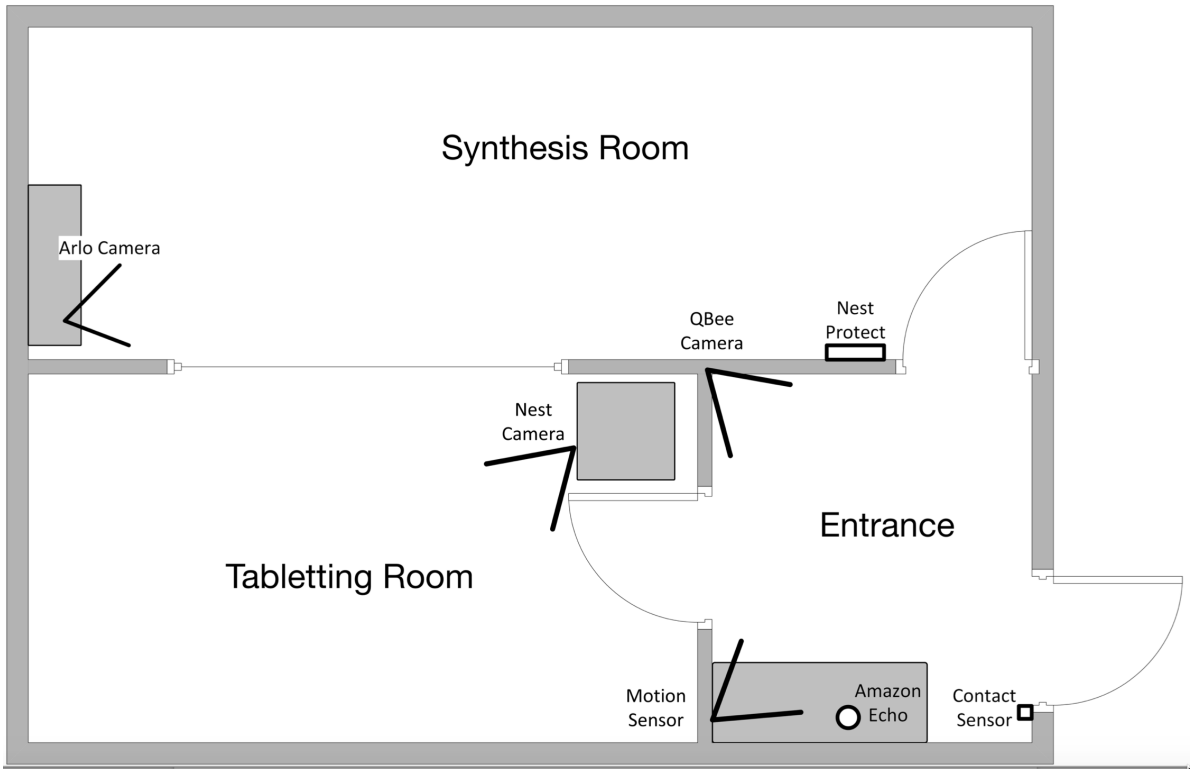


Figure 1.1: Drug Lab Overview

Overview of Challenge data

2.1 Image of Samsung Galaxy device

The Samsung Galaxy S6 Edge is an Android smartphone manufactured and marketed by Samsung Electronics.

Table 2.1: Samsung Galaxy S6 Edge Specifications.

Specifications	**Details**
Network	GSM / HSPA / LTE
Launch	2015, March
Display	Super AMOLED capacitive touchscreen, 16M colors
Platform	Android 5.0.2 (Lollipop), upgradable to 7.0 (Nougat); TouchWiz UI
Memory	32/64/128 GB, 3 GB RAM(Internal)
Battery	Non-removable Li-Ion 2600 mAh battery
Features	Fingerprint (front-mounted), accelerometer, gyro, proximity, compass, barometer

We have been given a 32GB dump file, which contains **screenshots, Ogg files**(audio- Whatsapp voice msgs), **videos and photos** taken by **NEST camera** and **Arlo Pro.**
Autopsy tool can be used to analyse the Samsung phone dump.There are lots of important data including app data used for controlling the security systems.

2.2 Memory image of Arlo camera

Arlo Pro is a 100 % wire-free, IP65 certified weather-resistant, rechargeable HD smart security camera with audio enabled. Adjustable sensitivity, automatic email alerts and push notifications are some of it's features.Cloud storage of data is also enabled within it.

We have been provided with a ***Arlo Pro Base Station file system*** along with some log file too. We use Log Parser as well as JSON Parser for analysing the evidence files.

2.3 iSmartAlarm Memory images and Diagnostic logs

iSmartAlarm is a do-it-yourself (DIY) smart home security system controlled with a user's smartphone. The system and devices are designed and manufactured by iSmart Alarm, Inc, a start-up based in Sunnyvale, California. The system uses a hub connected to a home's router to allow users control of home security and home automation devices, including multiple wireless devices. Users can arm and disarm their system, and receive a push notifications, phone call, email, and text message if the system is triggered. The iSmartAlarm system is to be used as a self-monitored solution with no monthly fees and no contracts, as opposed to traditional monitored systems such as ADT or Vivint. iSmartAlarm is currently a closed ecosystem, only operating with its own devices.

There are primarily two directories in the file we got. One is diagnostics with `server_stream` file which is possibly the log data of instructions passed to iSmartAlarm. The firmware data of the device is also given. It was analyzed primarily using binwalk. The files found are: `server_stream` : This is possibly the log data of

instructions passed to the iSmartAlarm device. `ismart_00.img` : This is the firmware file of the device. `ismart_80.img` : This is the firmware file of the device.

2.4 Network Traffic Capture Logs

A tcpdump file typically stores dumped data or packet headers delivered to and from the specified NIC (Network Information Center). It is mainly used to check whether the network and ethernet are abnormal. In this scenario, a tcpdump file was obtained to investigate packets from the SmartHome network traffic.

Here we have been given a police captured data traffic which we would be analysing using **Wireshark**

2.5 Amazon Echo Cloud data

Amazon Echo is a brand of smart speakers developed by Amazon.The features of the device include: voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, and playing audiobooks, in addition to providing weather, traffic and other real-time information. It can also control several smart devices, acting as a home automation hub.

Some of the data we received inside Amazon Echo include:

- VOICE FILES: There are 52 voice files. There are various instructions like that ask Alexa to make iSmartAlarm to ARM the lab system, other queries like the date etc. Basically saved voice data from various users are stored.
- JSON FILES: instructions and information regarding the user like

email ID and the device ID are present in these files.

- DATABASE FILE: This DB file stores around 12 tables, that also contains data regarding the timeline of instructions that were passed.
- CSV FILES: These files also had the data which were present in the JSON and DB files. All the commands are given to Alexa and the response given are all stored in an order of chronology.

2.6 Wink Hub File System Dump

Wink is the quick and simple way to connect you and your home. Manage hundreds of smart products from the best brands in one simple app. Faster, more reliable and more secure, wink hub 2 is the next generation of the wink hub. Hub 2 is compatible with more smart home technologies, so you can buy the devices you like from the brands you trust and know they'll work seamlessly with wink.We have been given a Wink File system which seems to have connections with other security appliances. Some of the data we found in the given dump are :

- BIN - There are files that are symbolic link to busybox and also many ELF files.

- DEV - In this directory also there are some empty files and symbolic links to tty files.

- ETC - This directory have system files like bluetooth that has the config files for the device.

Forensic level Analysis

In this section, we discuss the forensic analysis in device, cloud and network level.

Table 3.1: List of Tools used for our Analysis.

Tool	**Version**	**Usage**
Autopsy	4.4.0	Analyzing the Samsung device dump
Ghex	3.18.3	Analyzing bin files
Wireshark	2.6.6	Analyzing network traffic
Tcpdump	4.9.2	Analyzing network traffic
Ranger	1.8.1	Exploring the firmware
DB Browser	3.11.0	Viewing the DB files
Ghidra	1.0	Reversing binary files

3.1 Device Level Analysis

3.1.1 Samsung S6 Edge

We use Autopsy for the device level analysis of Samsung S6 Edge. The dump given was the entire partition of the mobile and Autopsy is the best tool to analyze these kinds of dumps. We can find all the information about the device like Bluetooth and WiFi mac addresses with Autopsy. We find all the media in the device, log files and app databases, all the web cookies and the web history with the help of

autopsy.

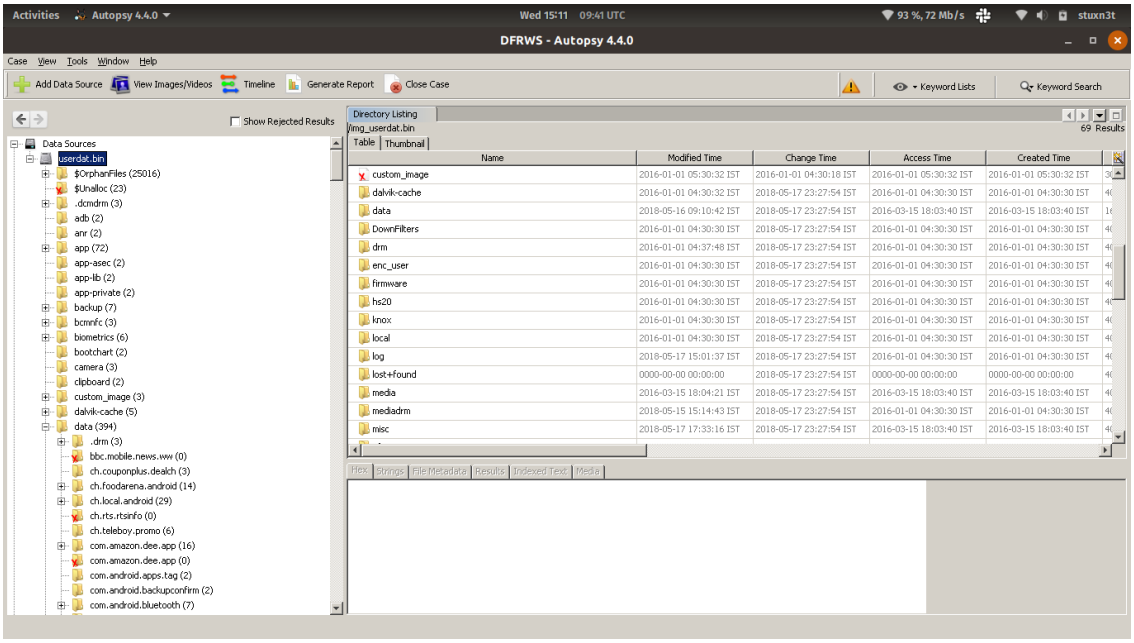


Figure 3.1: Samsung Dump Overview

3.1.2 Arlo Pro Camera

The base station Image of the Arlo Smart Camera and the "/tmp" folder of it are given. We use JSON parser tool for analyzing the JSON files present in the VZDAEMON.

There are :

- Modes
- Schedules
- Rules

Modes for the Arlo Camera:

Figure 3.2: Different Modes of Arlo Camera

Example: mode0.json

Modes for the Arlo Camera:

{"name":"","id":"mode0","type":"disarmed","rules":[],"objVersion":"1.0","fromAutomationconv":true}

Figure 3.3: Dump Overview

Rules for the Arlo Camera:

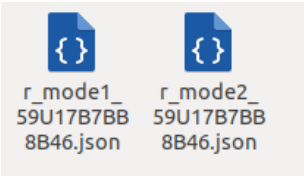


Figure 3.4: Dump Overview

Here we can see the schedule being assigning the camera which mode to use at what time.
And we can also see the base station configuration data.

Figure 3.5: Dump Overview

The base station Config file:

{"objVersion":"2.0","autoUpdate":true,"timeZone":"CET-1CEST,M3.5.0,M10.5.0/3","olsonTimeZone":"Europe/Amsterdam","antiFlicker":{"mode":0},"lowBatteryAlert":{"enabled":true},"lowSignalAlert":{"enabled":false},"claimed":true,"mcsEnabled":true,"apIdentifier":{"eth0":"B8:27:EB:0E:3B:45"},"apInvalidated":false,"authTokenType":2,"authToken":"","authTokenV2":"G/+QEd+cJk2nUBIct9y2gscK+sPgGFbUo7o/2BHhY97i9xrP1ONNR6EWakNb23HX","recoveryRebootCount":2}

Figure 3.6: Dump Overview

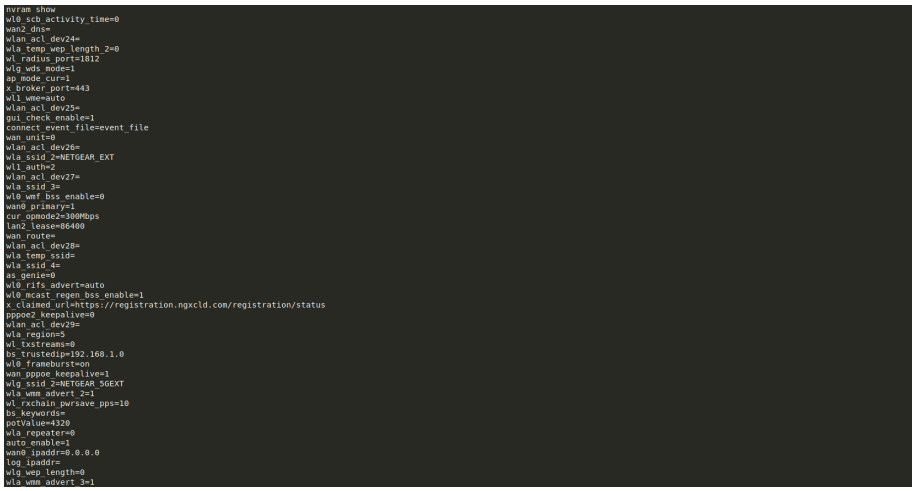


Figure 3.7: Dump Overview

We can see the NVRAM log file of the camera given in **Fig 3.7**

3.1.3 iSmartAlarm

We are provided with the firmware of the device in two SPIFF FLASH image files.

We get the firmware from the image file with a recursive binwalk extract and use ranger tool to explore the firmware. Now, from the

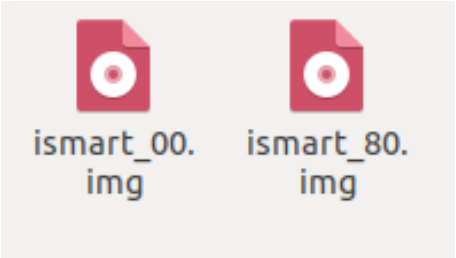


Figure 3.8: Evidence Files

extracted folders, we can see all the file system contents. We can also view all the configuration, library, lib files.

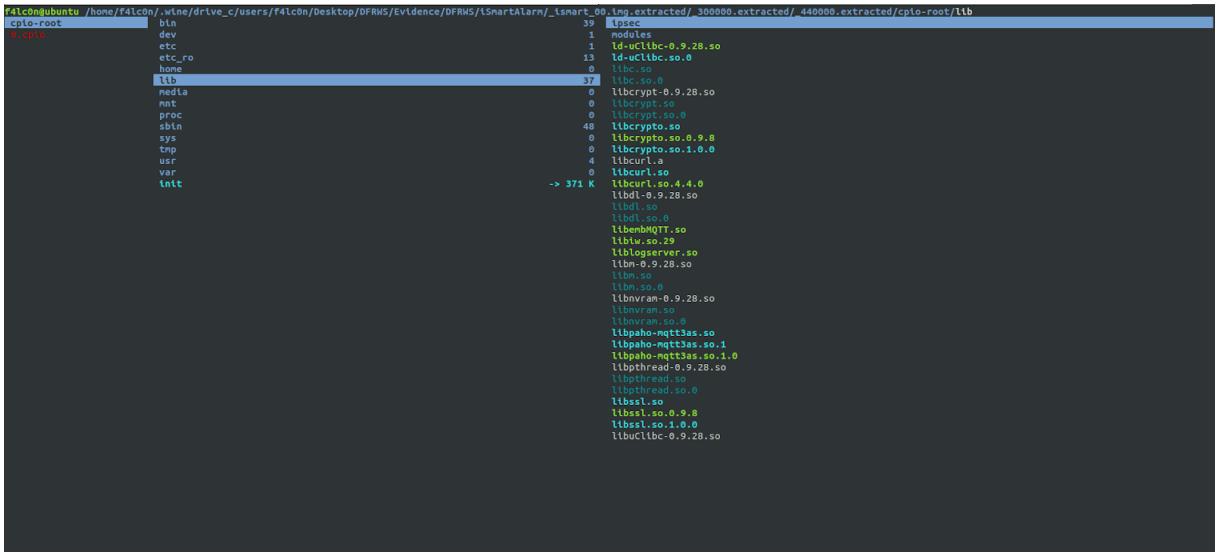


Figure 3.9: Dump Overview

Default network Config file of the camera is given in **Fig 3.10:**

Code signing certificates of the firmware is given in **Fig 3.11**

The Public key for Firmware Architecture update is given in **Fig 3.12**.

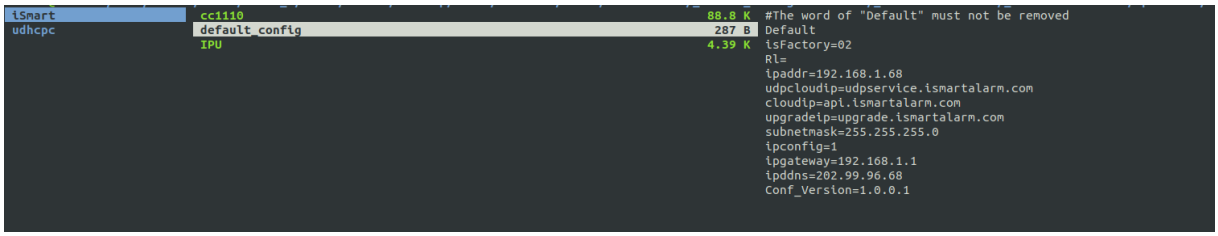


Figure 3.10: Dump Overview

Figure 3.11: Dump Overview

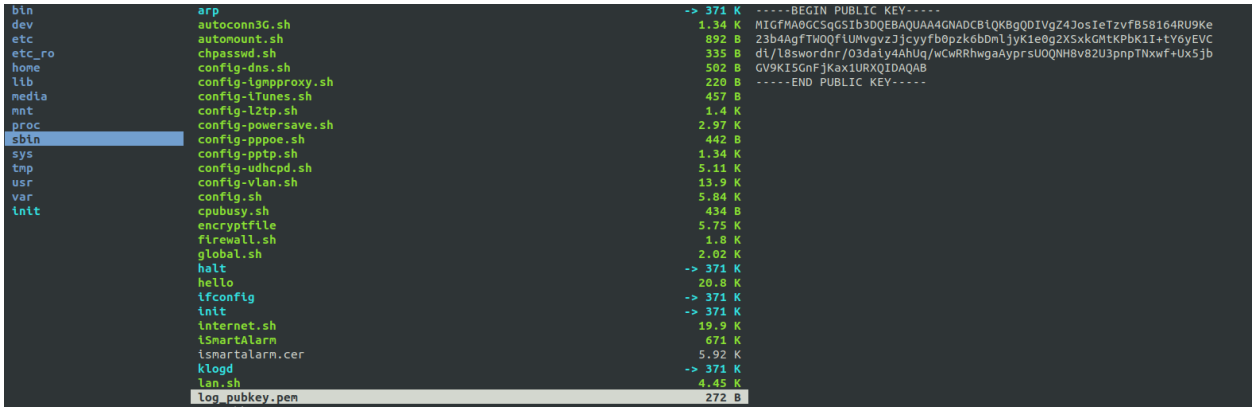


Figure 3.12: Dump Overview

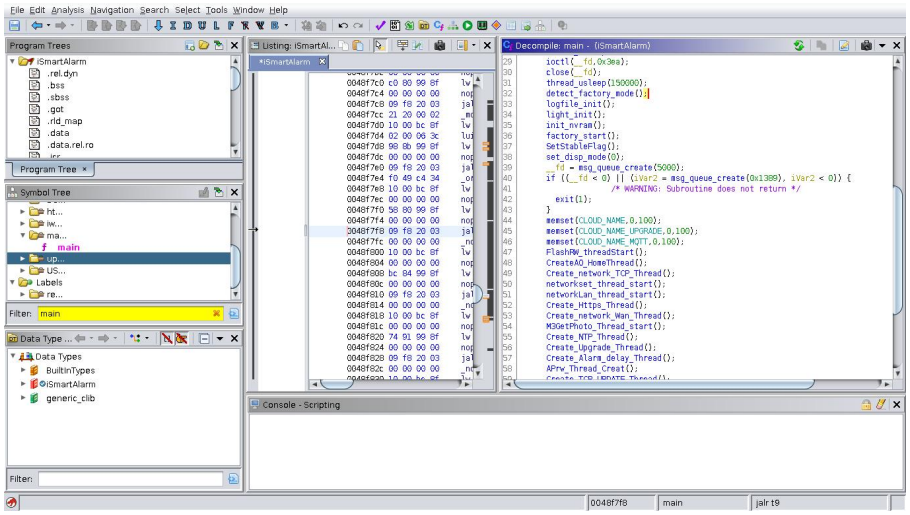


Figure 3.13: Dump Overview

We analysed the MIPS binary file using **Ghidra** and saw that the protocol used is mqtt and fork is used - child process are responsible for functionality (tread). Firmware update can be done through net and through usb device functionality can be found in "/dev/gpio", encryption key for usb is found on "encryptfile /usr/share/IPUlog /mnt/usb/IPUlog /sbin/logpubkey.pem". Also alarm can be sent/receive packets via http

3.2 Cloud Level Analysis

3.2.1 Amazon Echo Cloud data Analysis

The database file provided basically contains all the information about the instructions passed and appropriate responses of the device to these instructions. There are 12 tables in the database file:

- ACCOUNT
- ACQUIRED FILES
- `ALEXA_DEVICE`
- `COMPATIBLE_DEVICE`
- CONTACT
- CREDENTIAL
- OPERATION
- SETTING_MISC
- `SETTING_WIFI`
- SKILL
- TIMELINE
- `sqlite_sequence`

DB Browser for SQLite was used to analyze the database and ongoing through each of these tables give out information about certain features used by Jessie Pinkman. An example is the 'skills' taught to the device which includes integration of other IoT devices like iSmartAlarm and WinkHub which can then be controlled from Amazon Echo.

In the ACCOUNT table we see users that have access to the device which is basically Jessie Pinkman himself and as shown below details regarding his Amazon Echo account can be found here:

The `ACQUIRED_FILES` shows the database dump of all the files that were provided along with the dump files. The voice data, logs, CSV files etc.

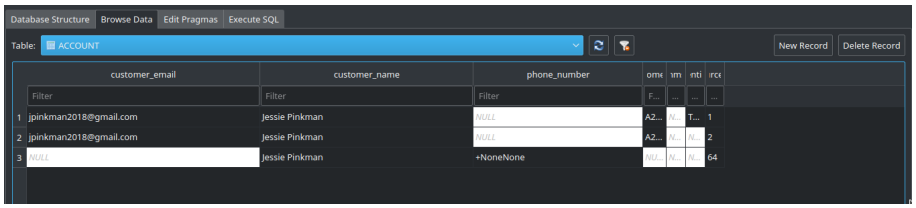


Figure 3.14: Database Overview

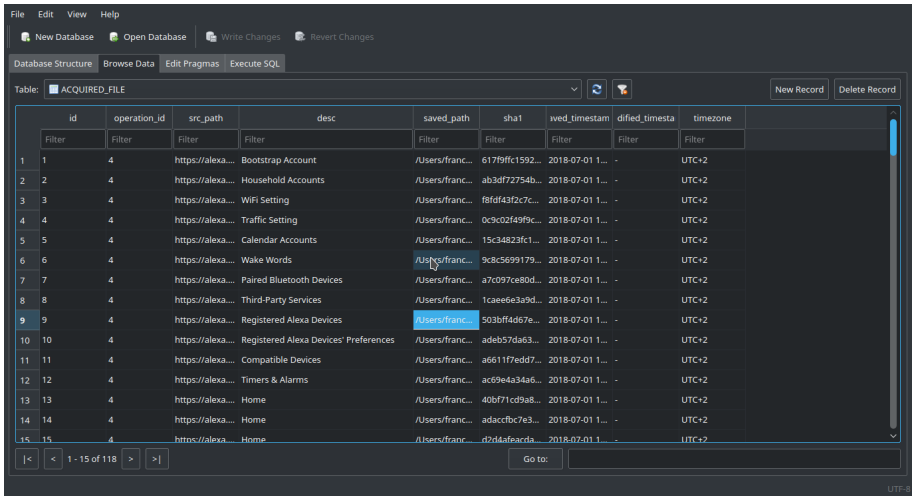


Figure 3.15: Database Overview

The table `ALEXA_DEVICE` contains basic data about the device itself, like the device id, `mac_id`, device type, customer id etc.

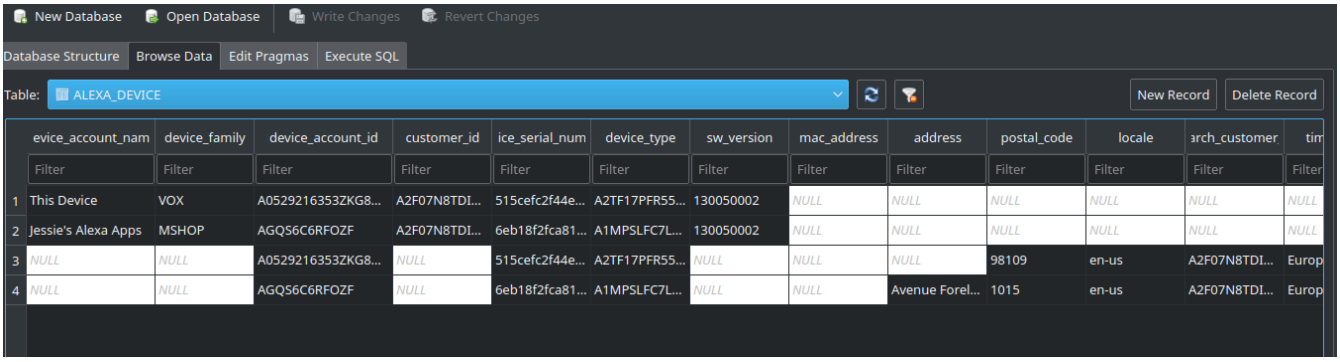


Figure 3.16: Database Overview

OPERATION table:

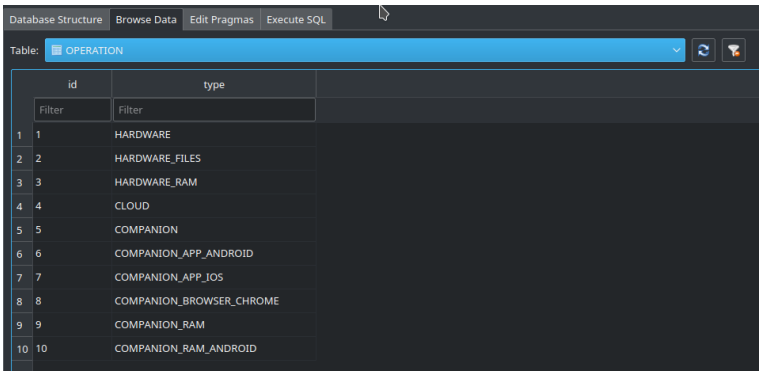


Figure 3.17: Database Overview

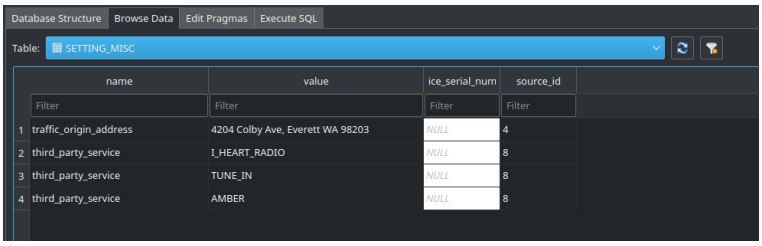


Figure 3.18: Database Overview

Figure 3.19: Database Overview

In both `SETTING_MISC and SETTING_WIFI` tables given above information about third party services and the wifi network is stored.

Inside the SKILLS table, we see that all the other IoT devices that were installed in the laboratory are actually integrated into the Amazon Echo and are controlled using it. Echo acts as the command center for Jessie Pinkman to control all the other devices.

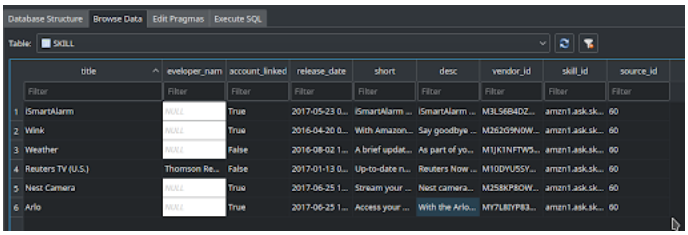


Figure 3.20: Database Overview

There are many devices like the iSmartAlarm, Wink, Arlo Pro, Nest Protect/camera(smoke detector) that were added. This serves as proof that these devices were controlled using amazon echo and gaining control into Echo gives access to the rest of the security system. Although the Qbee camera installed in the lab doesn't seem to be controlled using Echo, hence it can't be accessed via the echo and is controlled separately.

Since many other tables were found empty, to get an overall idea on all the events that could have happened, the TIMELINE table was studied. On analyzing all the data stored on the date of 17th May 2018, the date of the crime, we see that there were casual instructions passed down to the device, like "Play music", "Link Spotify" etc. But he armed the lab by around 10:22 am. He 'arms' the lab usually when he leaves the lab and when the lab is empty.

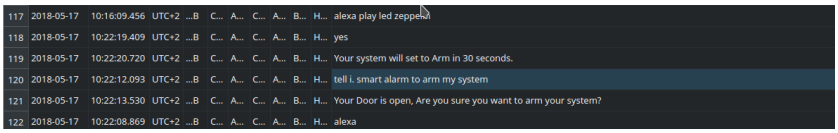


Figure 3.21: Database Overview

3.2.2 WinkHub system data analysis

We are given the root folder of the wink-hub station. The following is a quick look as to what is present in the folder

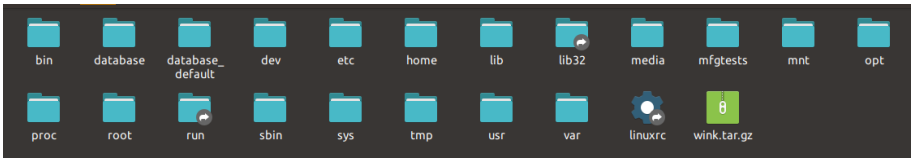


Figure 3.22: Dump Overview

We find a directory with the name database. We looked into it and found some ".db" files. We find a particular lutron.db file in it.

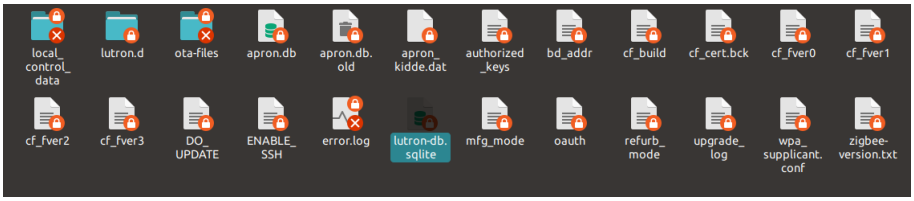


Figure 3.23: Dump Overview

We used SQLite DB Browser to view the file. The only useful thing that we found was the IP address of the lutron.

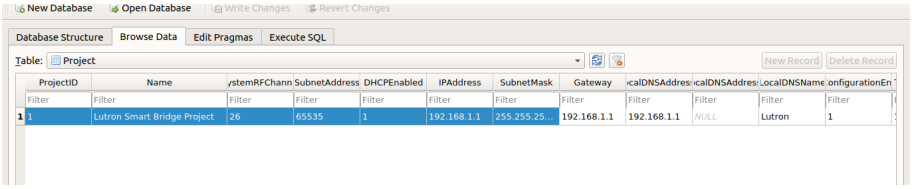
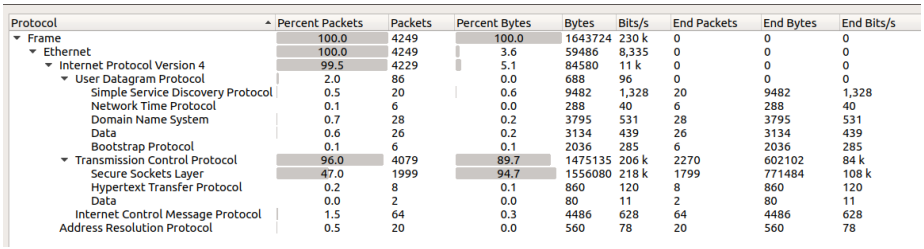


Figure 3.24: Dump Overview

3.3 Network level Analysis

We use Wireshark and tcpdump for the analysis of the police network capture provided. Wireshark is an open source tool for profiling network traffic and analyzing packets. Such a tool is often referred to as a network analyzer, network protocol analyzer or sniffer.

Using the protocol hierarchy option in Wireshark, we see the different types of protocols involved. Below is the screenshot of the same.



Protocol	Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
Frame	100.0	4249	100.0	1643724	230 k	0	0	0
Ethernet	100.0	4249	3.6	59486	8,335	0	0	0
Internet Protocol Version 4	99.5	4229	5.1	84580	11 k	0	0	0
User Datagram Protocol	2.0	86	0.0	688	96	0	0	0
Simple Service Discovery Protocol	0.5	20	0.6	9482	1,328	20	9482	1,328
Network Time Protocol	0.1	6	0.0	288	40	6	288	40
Domain Name System	0.7	28	0.2	3795	531	28	3795	531
Data	0.6	26	0.2	3134	439	26	3134	439
Bootstrap Protocol	0.1	6	0.1	2036	285	6	2036	285
Transmission Control Protocol	96.0	4079	89.7	1475135	206 k	2270	602102	84 k
Secure Sockets Layer	47.0	1999	94.7	1556080	218 k	1799	771484	108 k
Hypertext Transfer Protocol	0.2	8	0.1	860	120	8	860	120
Data	0.0	2	0.0	80	11	2	80	11
Internet Control Message Protocol	1.5	64	0.3	4486	628	64	4486	628
Address Resolution Protocol	0.5	20	0.0	560	78	20	560	78

Figure 3.25: Protocol Hierarchy

The following is a small screenshot of the traffic.

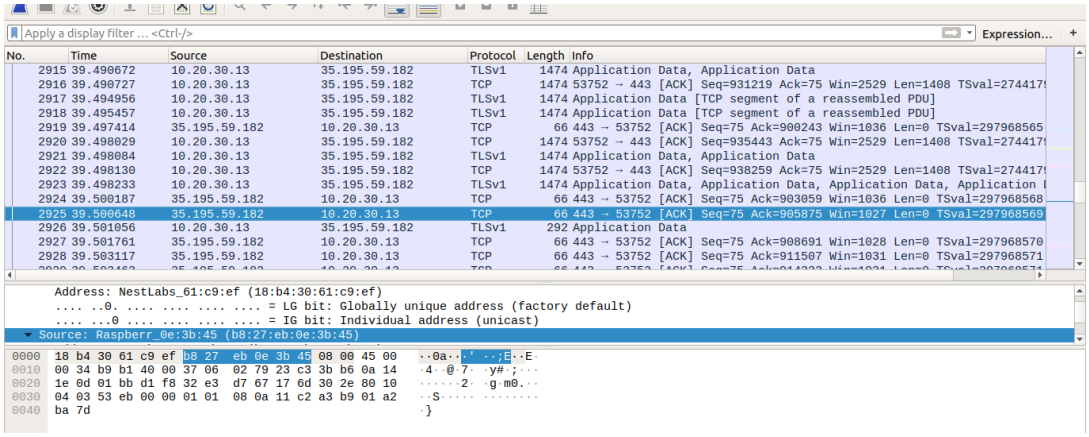


Figure 3.26: Network Traffic Overview

Digital Investigation

In this section, we will be discussing and evaluating evidence found in each device and finally, correlate and conclude the investigation.

4.1 Results of Digital Investigation

4.1.1 Samsung Galaxy S6 Edge

In the provided "userdat.bin" file, we find a lot of media(Images, videos, audio recordings etc..). However, only a small portion of it is relevant/related to the crime.

4.1.1.1 Screenshot of QBee Camera

In the "/system/`recent_images`" directory, we find some really relevant images like the screenshot of the QBee camera in private mode which can help us in concluding how the camera was disabled.

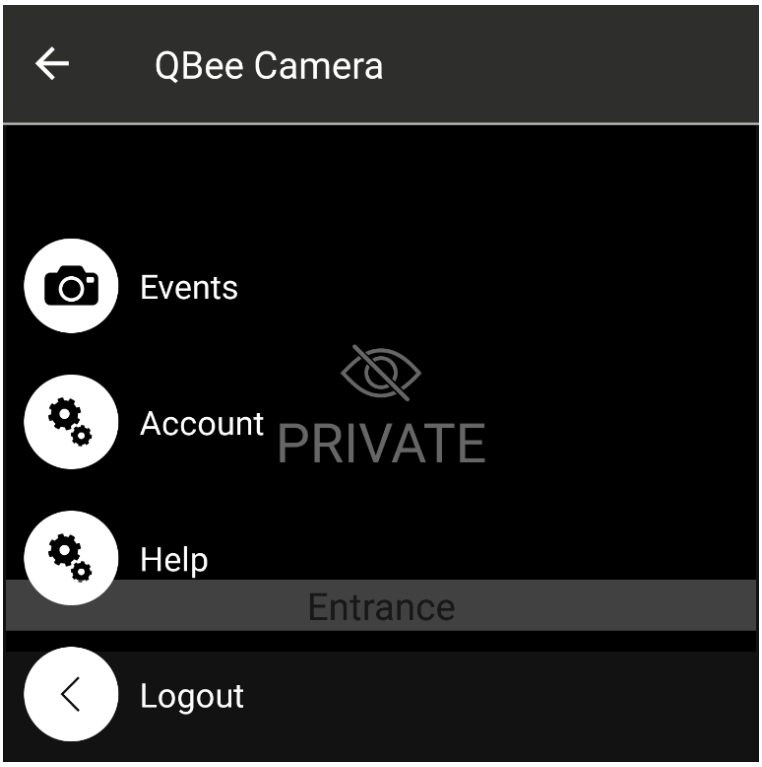


Figure 4.1: QBee Camera Menu

4.1.1.2 Screenshot of iSmart Alarm App

We also find a lot of screen-shots of the iSmart Alarm android app which is helpful in indicating the authorised users who can control the alarm.

From this, we can conclude that when the security settings of the alarm are modified through the App, these changes are done in the name of "The Boss" which is obviously Jessie Pinkman as the phone belongs to him.

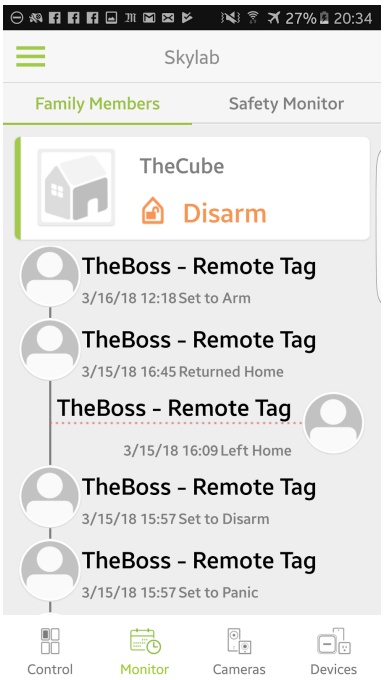


Figure 4.2: App data Overview

4.1.1.3 iSmart Alarm Database

While going through the Samsung dump, we also found a database file related to the iSmart Alarm.

We found the file in "/data/iSA.common/databases". The following screenshot shows the database. The file was viewed using DB Browser for SQLite.

The highlighted text in the screenshot tells us about the users who have access to the alarm system. Jessie Pinkman, The Boss and D Pandana have access to modify the security configuration of the system.

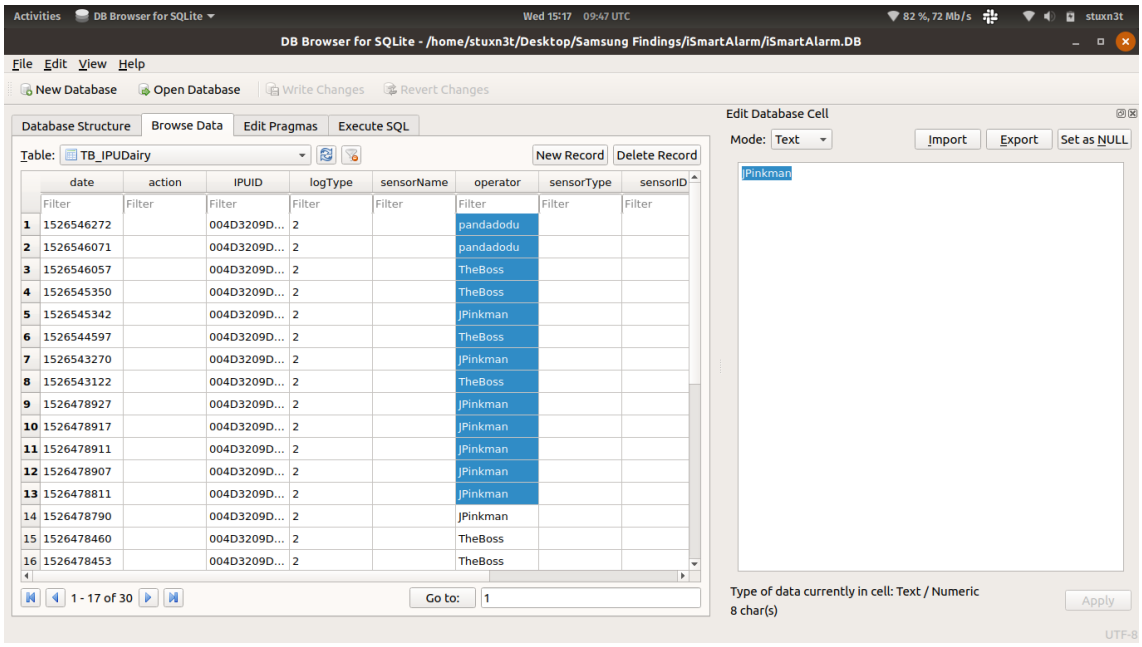


Figure 4.3: iSmart Database Overview

4.1.1.4 iSmartAlarm XML File

We also found an **iSmartalarmdata.xml** in the image of the Samsung device. The password, phone number etc. were stored in plaintext which is a huge security issue. Below is the screenshot of the XML file. The information present is extremely crucial.

As you can see, the password, phone number, country are all stored in plain text.This data could be easily be used by anyone for getting access to the security systems.

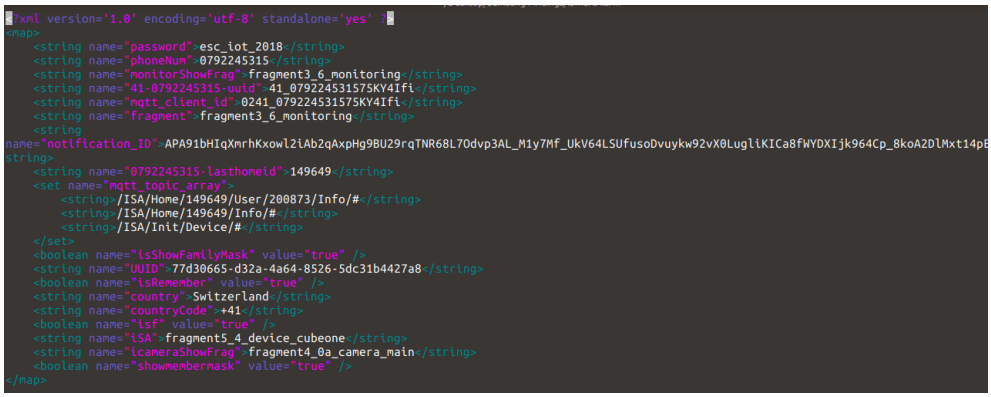


Figure 4.4: XML File Overview

4.1.2 Analysis of Alexa's Database

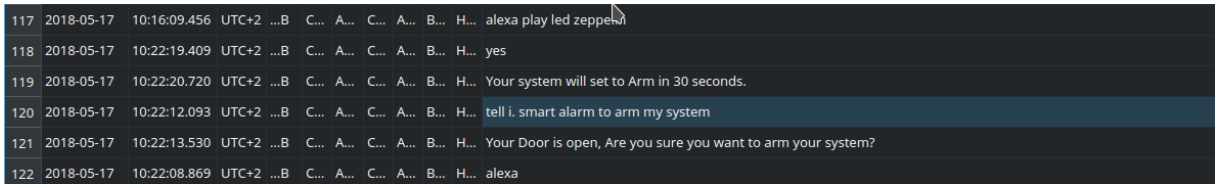


Figure 4.5: Database(Echo) Overview

The above screenshot displays the last commands passed to Amazon Alexa on the day of the raid. If observed closely, the last command passed was to "ARM" the lab security system and that was in the name of "Jessie Pinkman". So we can conclude that Jessie Pinkman was in the lab till 10:22:08 AM on 17/05/2018.

We have also observed that neither D Pandana nor S Varga has access to the device. So, J Pinkman was the sole user of the Amazon Echo device.

Other than the information present above, we did not find anything interesting or worth mentioning in this section which would help in catching the culprit.

4.1.3 Police Network Traffic Analysis

The following screenshots are taken from analyzing the data in the traffic provided. Let us see what the contents are in the HTTP protocol.

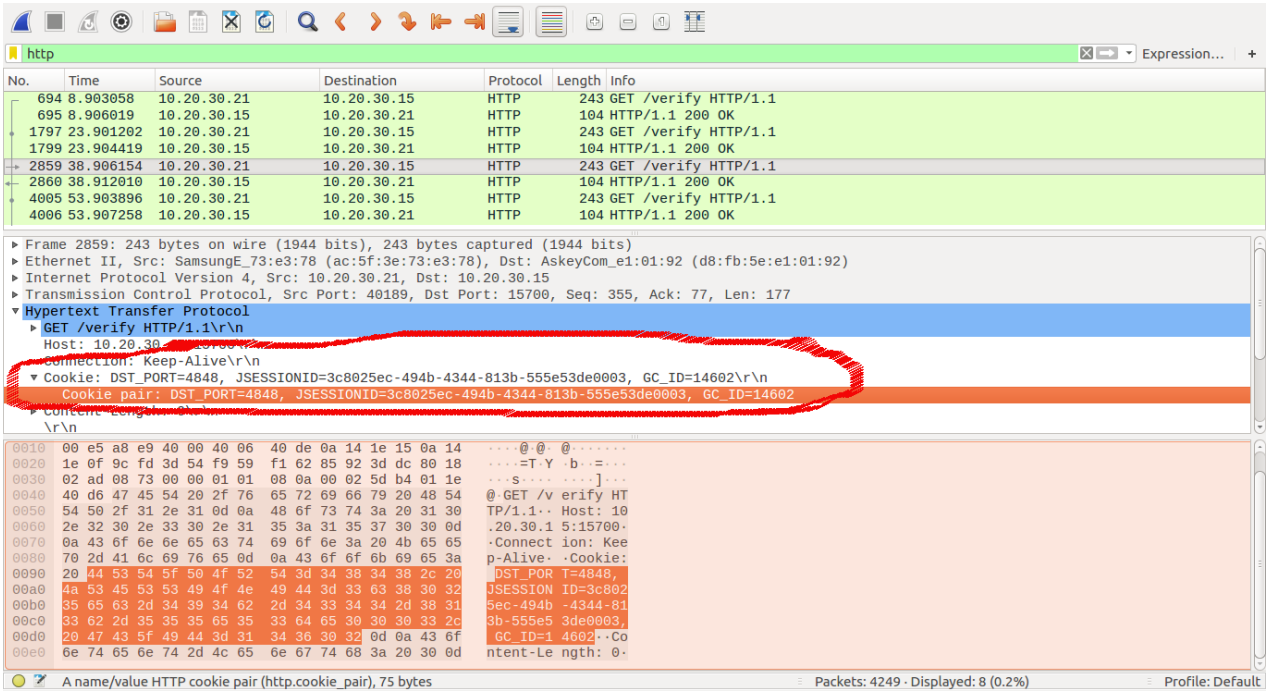


Figure 4.6: Network Traffic Overview

We are able to see the JSESSIONID, `GC_ID` in plain text. This is a serious issue. These packets are coming/going from a device named

"AskeyCom" which is the manufacturer of the QBee camera. Now, let us look at the ICMP protocol.

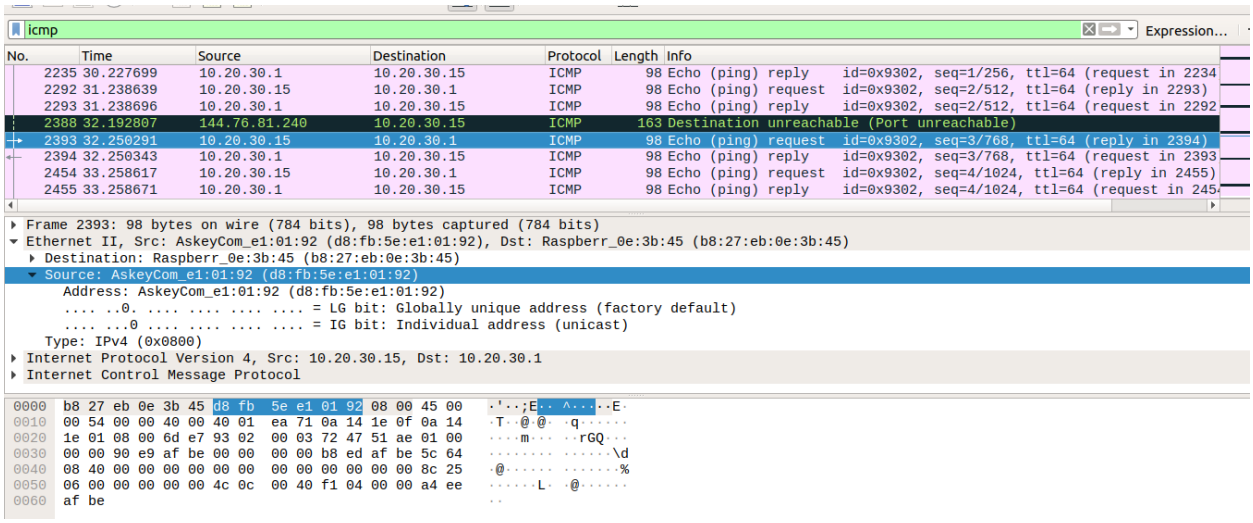


Figure 4.7: Network Traffic Overview

There are a lot of packets being transferred from the Qbee camera to the base station. This means that there is an issue in connecting to the Qbee camera.

The device is vulnerable to HTTP requests as it sends all the session IDs etc. in plain text over the HTTP protocol. Below is a live video demonstration of the vulnerability.

https://www.youtube.com/watch?v=dd8vt0_DJF4

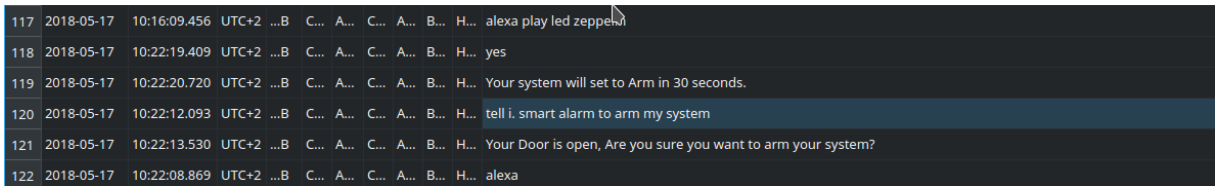
And a blog post by Francesco Servida,

https://blog.francescoservida.ch/2018/10/31/cve-2018-16222-to-16225-multiple-vulnerabilities-in-qbee-and-ismartalarm-products/

Co-relation between various data sources

5.1 iSmart Alarm database in Samsung device and Amazon Echo database

The below figure shows a screenshot of the last commands passed to Alexa before the police were alerted.



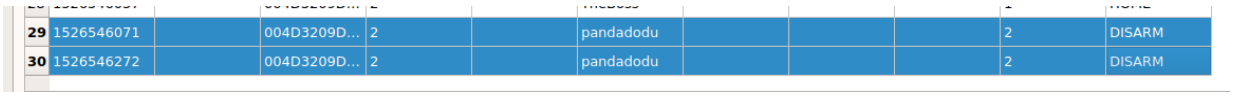
117	2018-05-17	10:16:09.456	UTC+2	...B	C...	A...	C...	A...	B...	H...	alexa play led zeppelin
118	2018-05-17	10:22:19.409	UTC+2	...B	C...	A...	C...	A...	B...	H...	yes
119	2018-05-17	10:22:20.720	UTC+2	...B	C...	A...	C...	A...	B...	H...	Your system will set to Arm in 30 seconds.
120	2018-05-17	10:22:12.093	UTC+2	...B	C...	A...	C...	A...	B...	H...	tell i. smart alarm to arm my system
121	2018-05-17	10:22:13.530	UTC+2	...B	C...	A...	C...	A...	B...	H...	Your Door is open, Are you sure you want to arm your system?
122	2018-05-17	10:22:08.869	UTC+2	...B	C...	A...	C...	A...	B...	H...	alexa

Figure 5.1: DB File(Echo) Overview

The last command passed to Alexa was to “ARM” the system. Clearly, this command was given by Jessie Pinkman before the raid happened. Now, let us look at what the iSmart Alarm database shows us.

Below is the screenshot of the last instructions passed to the iSmart

Alarm. This database file was found in the Samsung device.



29	1526546071		004D3209D...	2		pandadodu				2	DISARM
30	1526546272		004D3209D...	2		pandadodu				2	DISARM

Figure 5.2: DB File in Samsung device

The timestamps are in the **epoch**. When the timestamps are converted to our own standard time, it turns out to exactly point us to the time when the raid occurred. The time of the raid, therefore, is **Thursday, May 17, 2018, 10:37:52 AM**. The police were alerted at 10:40 AM on the same day and they arrive at 10:45 AM. So that gives the culprits around **3-6 mins** to set the lab on fire and also escape. Also, The last instruction given to the iSmart alarm was to **"DISARM"**the security system and it was given by **D Pandana**.

5.2 Conclusion

So we can conclude that D Pandana was involved in the raid. So, by co-relating such crucial pieces of evidence and removing the unnecessary parts, we were able to conclude that the **raid took place close to 10:37 AM and one of Pinkman's assistants, D Pandana was involved in the raid.**

This is our conclusion collected, analyzed and mapped together from various shreds of evidence.

Answering Challenge Questions

At what time was the illegal drug lab raided?

Answer: As concluded from the Digital Investigation section, the lab was raided around 10:37 AM on 17th May, 2018. For more information, please refer the digital investigation section.

Could any of the two friends of Jessie Pinkman have been involved in the raid? If YES,

1. Which friend?
2. What is the confidence in such hypothesis?

Answer: Yes, one of Jessie Pinkman's friend was involved in the raid. His/Her name is **D Pandana**. The proof was obtained from iSmart alarm's database found in the Samsung device. We observe that he was the last person to DISARM the system at 10:37 AM. The time being so close to the time when the lab was raided, leads us to the conclusion that the D Pandana was involved in the raid.

How was the QBee camera disabled?

Answer: The answer to this particular question is really technical. There is a vulnerability in the QBee camera with which it can be changed into the private mode by changing the **session ID**.The technicalties of the vulnerability have been described in the digital investigation section.

6.1 References

- **Wink Hub** https://en.wikipedia.org/wiki/Wink_(platform)
- **Wink Hub Vulnerability**

  https://blog.rapid7.com/2017/09/22/multiple-vulnerabilities-in-wink-and-insteon-smart-home-systems/

  https://motherboard.vice.com/en_us/article/pak3zg/wink-hub-insteon-hub-hacks
- **MIPS Architecture** https://en.wikipedia.org/wiki/MIPS_architecture
- **Autopsy** http://wiki.sleuthkit.org/index.php?title=Autopsy_User%27s_Guide
- **Amazon Alexa** https://courses.csail.mit.edu/6.857/2017/project/8.pdf
- **Ghidra** https://www.ghidra-sre.org/