Blue teaming project

Forensics case- Jessie Pinkman

In this document I will explore the data given to me and analyze it, trying to help a police investigation by using Forensic techniques.

Ivan Dimitrov Arbaliev

Table of contents

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 Wi-Fi 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 Wink Hub 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 Wink Hub. He also collects the iSmartAlarm and Arlo base stations to perform an in-depth analysis at the forensic laboratory.

The digital forensic specialist also notices that a QBee Camera seems to be disabled, so he collects a sample of the network traffic.

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.

Questions

The Attorney General needs answers to the following questions:

At what time was the illegal drug lab raided?

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

If YES:

- Which friend?
- What is the confidence in such hypothesis?

How was the QBee camera disabled?

Information we have

The police have recovered multiple sources of information that we can investigate. I have listed every item below.

Physical extraction of Jessie Pinkman’s Samsung phone

Samsung GSM_SM-G925F Galaxy S6 Edge.7z
ae83b8ec1d4338f6c4e0a312e73d7b410904fab504f7510723362efe6186b757

iSmartAlarm –Diagnostic logs
ismartalarm/diagnostics/2018-05-17T10_54_28/server_stream
8033ba6d37ad7f8ba22587ae560c04dba703962ed16ede8c36a55c9553913736

iSmartAlarm –Memory images: 0x0000’0000 (ismart_00.img)
dump/ismart_00.img
b175f98ddb8c79e5a1e7db84eeaa691991939065ae17bad84cdbd915f65d9a10

iSmartAlarm –Memory images: 0x8000’0000 (ismart_80.img)
dump/ismart_80.img
b175f98ddb8c79e5a1e7db84eeaa691991939065ae17bad84cdbd915f65d9a10

Arlo –Memory image
arlo/dfrws_arlo.img
3b957a90a57e5e4485aa78d79c9a04270a2ae93f503165c2a0204de918d7ac70

Arlo –NVRAM settings
arlo/nvram.log
f5d680d354a261576dc8601047899b5173dbbad374a868a20b97fbd963dca798

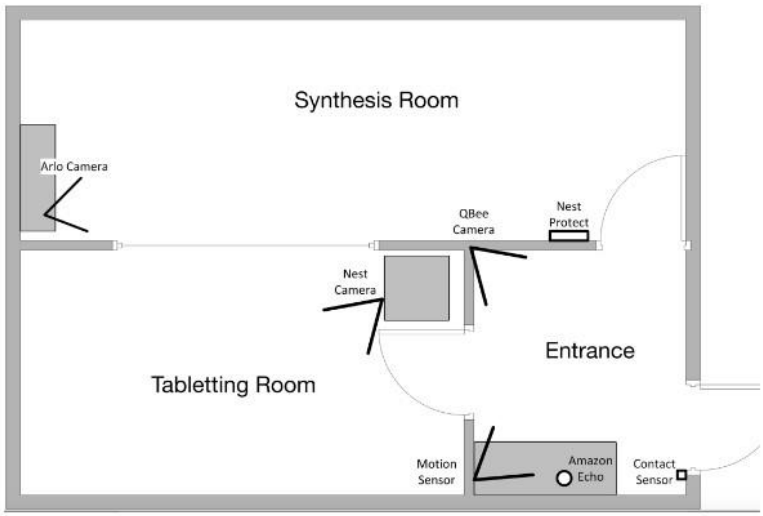
Arlo –NAND: TAR archive of the folder /tmp/media/nand
arlo/arlo_nand.tar.gz
857455859086cd6face6115e72cb1c63d2befe11db92beec52d1f70618c5e421

WinkHub –Filesystem TAR archive
wink/wink.tar.gz
083e7428dc1d0ca335bbcfc11c6263720ab8145ffc637954a7733afc7b23e8c6

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

Network capture
network/dfrws_police.pcap
1837ee390e060079fab1e17cafff88a1837610ef951153ddcb7cd85ad478228e

We are provided with a diagram of the drug lab.



1 Analysis

In this chapter I will show what interesting clues I managed to find

1.1 Jessie Pinkman's phone.

Jessies phone was retrieved by the police from the drug lab. It is a Samsung galaxy s6 edge device. With a quick google we can find the specs of the smartphone.

Also known as Samsung Galaxy S6 edge G925

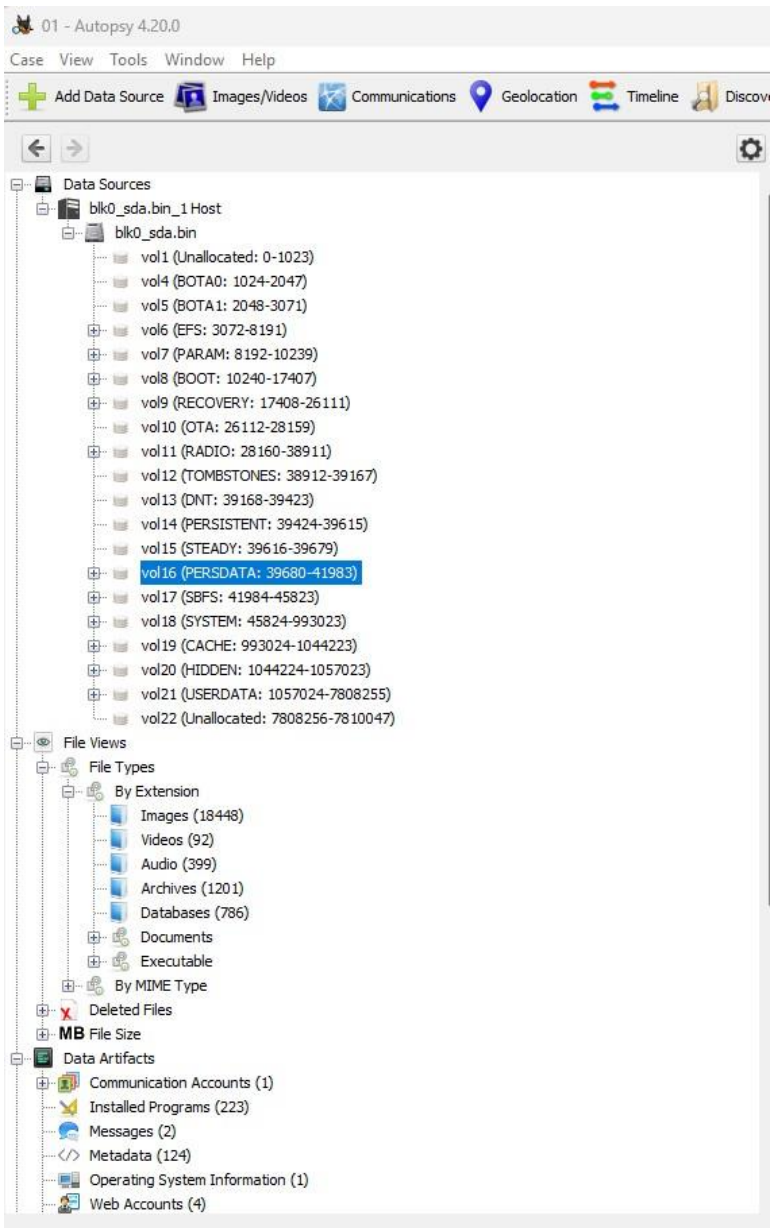
Versions: G925P (Sprint), G925R (US Cellular), G925V (Verizon), G925W8 (Canada)

NETWORK	Technology	GSM / CDMA / HSPA / EVDO / LTE EXPAND ▼
LAUNCH	Announced	2015, March. Released 2015, April
	Status	Discontinued
BODY	Dimensions	142 x 70.1 x 7.1 mm (5.59 x 2.76 x 0.28 in)
	Weight	132 g (4.66 oz)
	Build	Glass front (Gorilla Glass 4), glass back (Gorilla Glass 4), aluminum frame
	SIM	Nano-SIM
DISPLAY	Type	Super AMOLED
	Size	5.1 inches, 71.7 cm^2 (~72.0% screen-to-body ratio)
	Resolution	1440 x 2560 pixels, 16:9 ratio (~576 ppi density)
	Protection	Corning Gorilla Glass 4
PLATFORM	OS	Android 5.0.2 (Lollipop), upgradable to 5.1 (Lollipop), TouchWiz UI
	Chipset	Exynos 7420 Octa (14 nm)
	CPU	Octa-core (4x2.1 GHz Cortex-A57 & 4x1.5 GHz Cortex-A53)
	GPU	Mali-T760MP8
MEMORY	Card slot	No
	Internal	32GB 3GB RAM, 64GB 3GB RAM, 128GB 3GB RAM
		UFS 2.0
MAIN CAMERA	Single	16 MP, f/1.9, 28mm (wide), 1/2.6", 1.12µm, AF, OIS
	Features	LED flash, auto-HDR, panorama
	Video	4K@30fps, 1080p@30/60fps, 720p@120fps, HDR, stereo sound rec., OIS, gyro-EIS
SELFIE CAMERA	Single	5 MP, f/1.9, 22mm (wide)
	Features	Dual video call, Auto-HDR
	Video	1440p@30fps
SOUND	Loudspeaker	Yes
	3.5mm jack	Yes
		24-bit/192kHz audio
COMMS	WLAN	Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot
	Bluetooth	4.1, A2DP, LE, aptX
	Positioning	GPS, GLONASS
	NFC	Yes
	Infrared port	Yes
	Radio	No
	USB	microUSB 2.0, OTG
FEATURES	Sensors	Fingerprint (front-mounted), accelerometer, gyro, proximity, compass, barometer, heart rate, SpO2
		ANT+
		S-Voice natural language commands and dictation

The phone's data is provided as a compressed file. Once unzipped we have 3 disk images we can look through.

Name	Date modified	Type	Size
blk0_sda.bin	5/17/2018 10:05 PM	BIN File	31,240,192 ...
blk16_sdb.bin	5/17/2018 10:05 PM	BIN File	4,096 KB
blk32_sdc.bin	5/17/2018 10:05 PM	BIN File	4,096 KB

I used Autopsy 4.2.0 to open the bin file and enumerate data inside. The most significant out of the 3 is **blk0-sda.bin** because it contains Jessie Pinkman's phone data, screenshots, voice messages, videos and photos taken by NEST camera and Arlo Pro.



The disk had 21 partitions with various information inside.

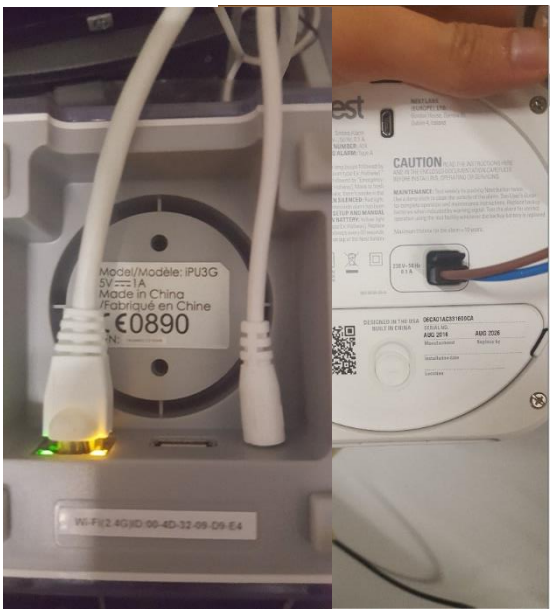
VOL1	Unallocated
VOL4	BOTA0
VOL5	BOTA1
VOL6	EFS
VOL7	PARAM
VOL8	BOOT
VOL9	RECOVERY
VOL10	OTA
VOL11	RADIO
VOL12	TOMBSTONES
VOL13	DNT
VOL14	PERSISTENT
VOL15	STEADY
VOL16	PERSDATA
VOL17	SBFS
VOL18	SYSTEM
VOL19	CACHE
VOL20	HIDDEN
VOL21	USERDATA
VOL22	UNALLOCATED

Information about Jessies phone is in VOL21: USERDATA

I found interesting pictures taken by Jessie on his phone in Vol21/media/0/DCIM/CAMERA

Photographs of Arlo base station.

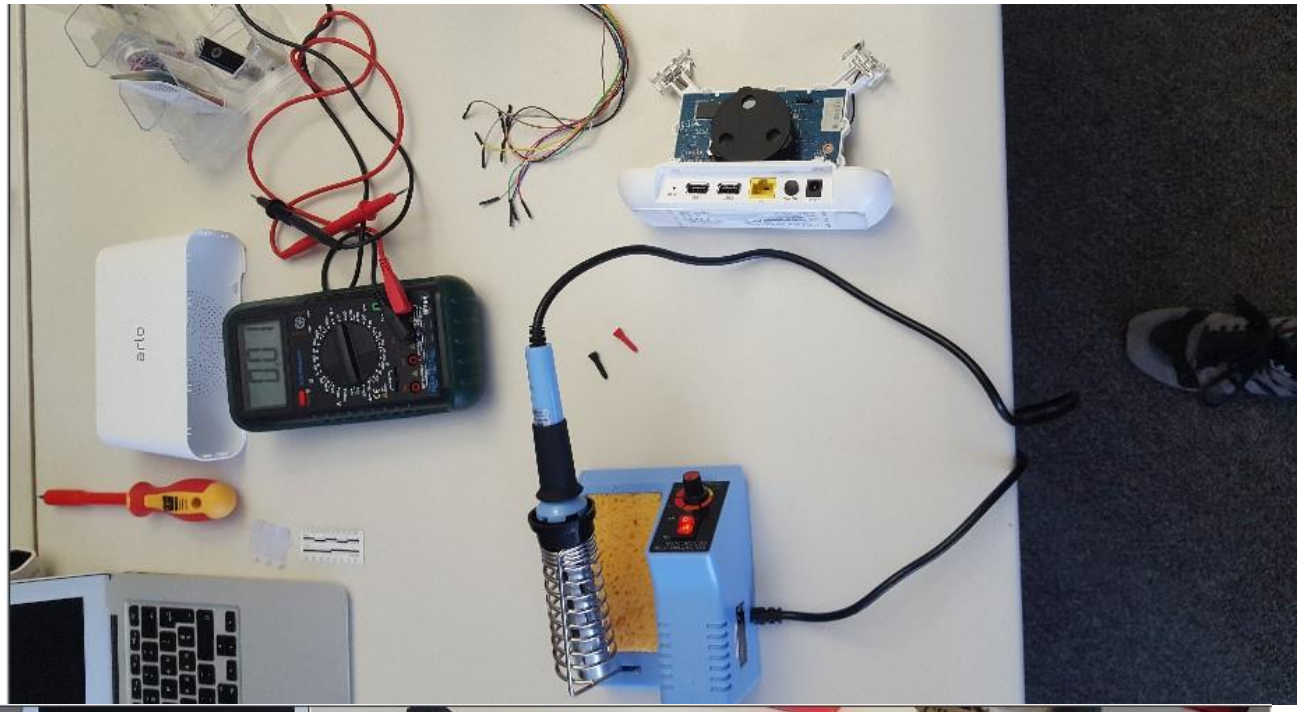
Mac 08028EDD754F

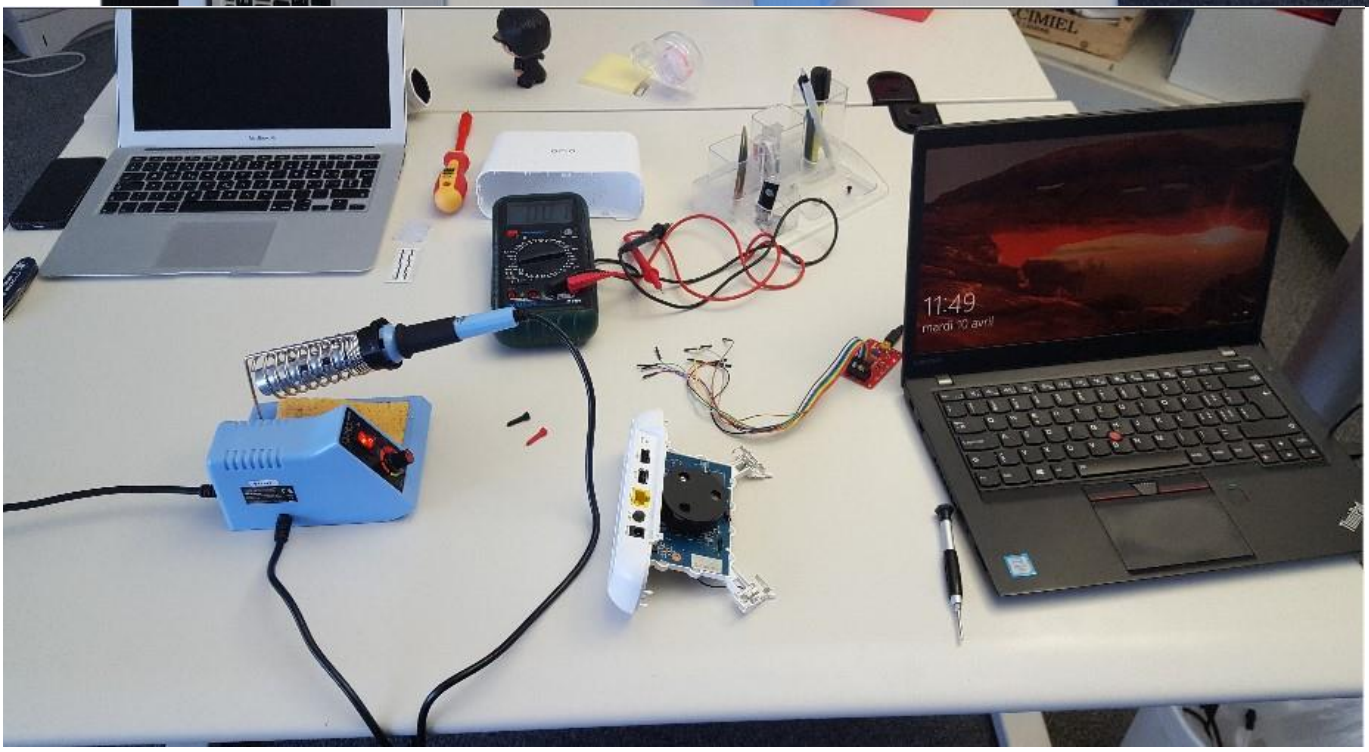

Model/Modèle: IPU3G
Made in China
/Fabriqué en Chine
€0890
CAUTION

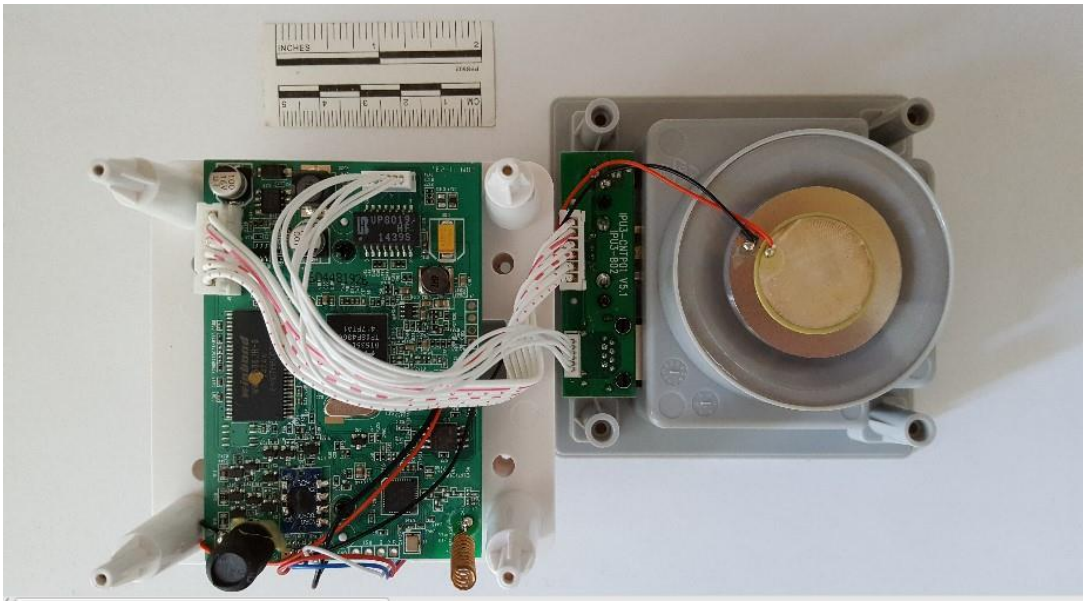

0890
Model/Modèle: PIR3G
Made in China/
Fabriqué en Chine

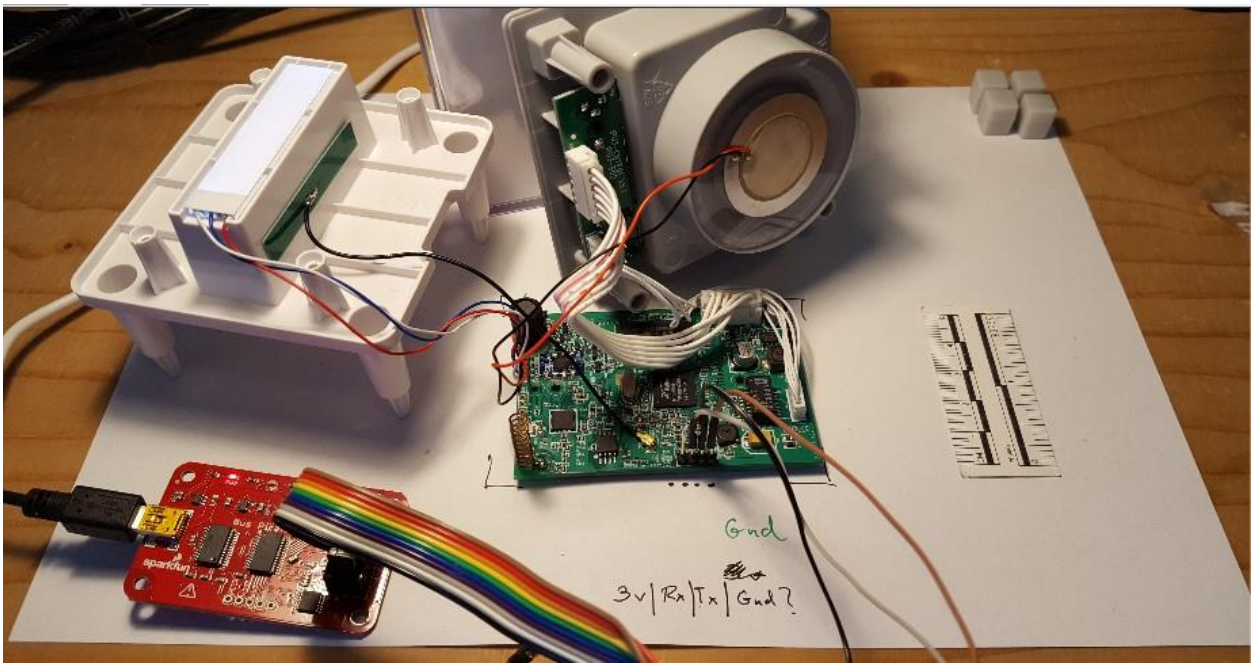

arlo

Assembly of the alarm system in the drug lab.

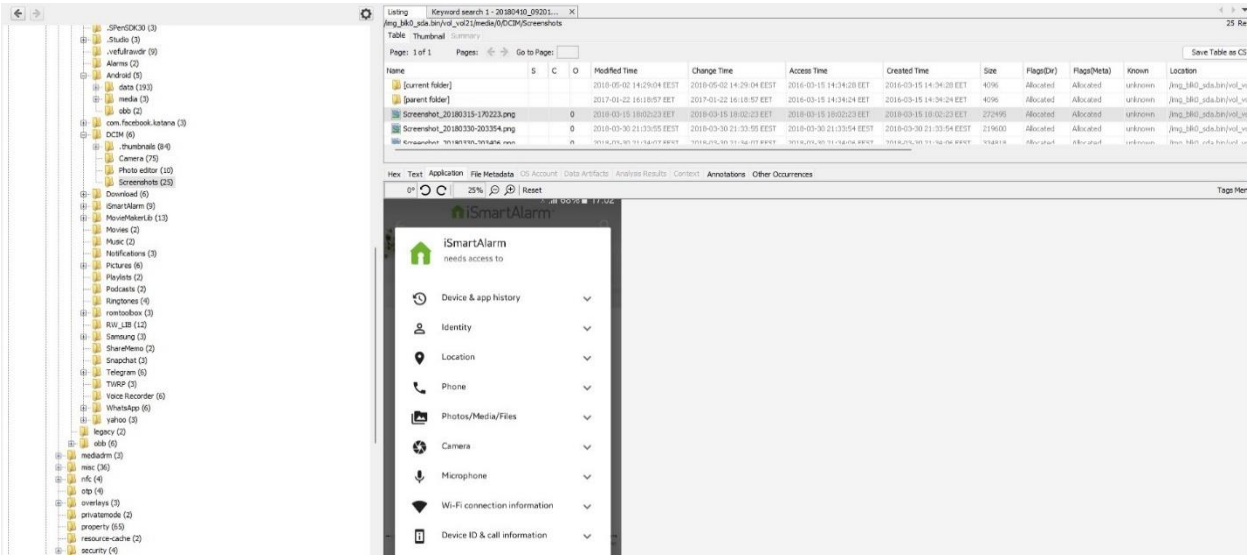


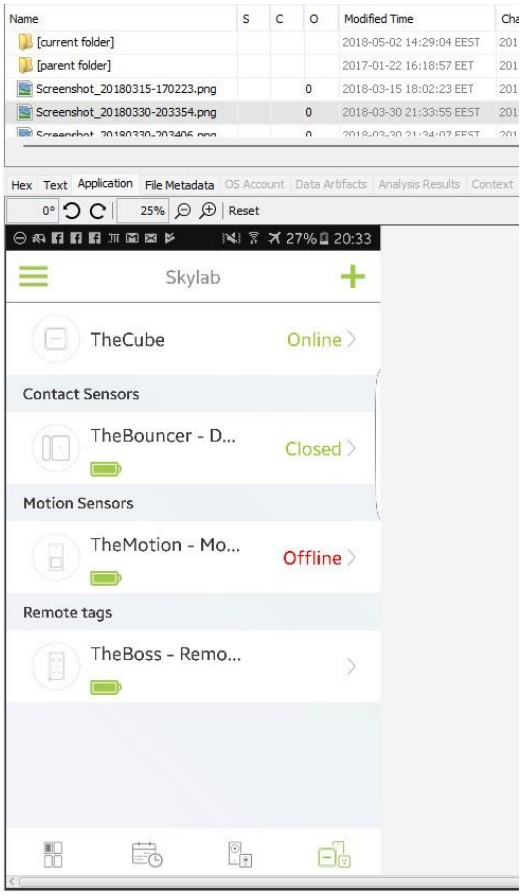

11:49




Gnd
3v | Rx | Tx | Gnd?

I found a screenshot of the I smart alarm system.



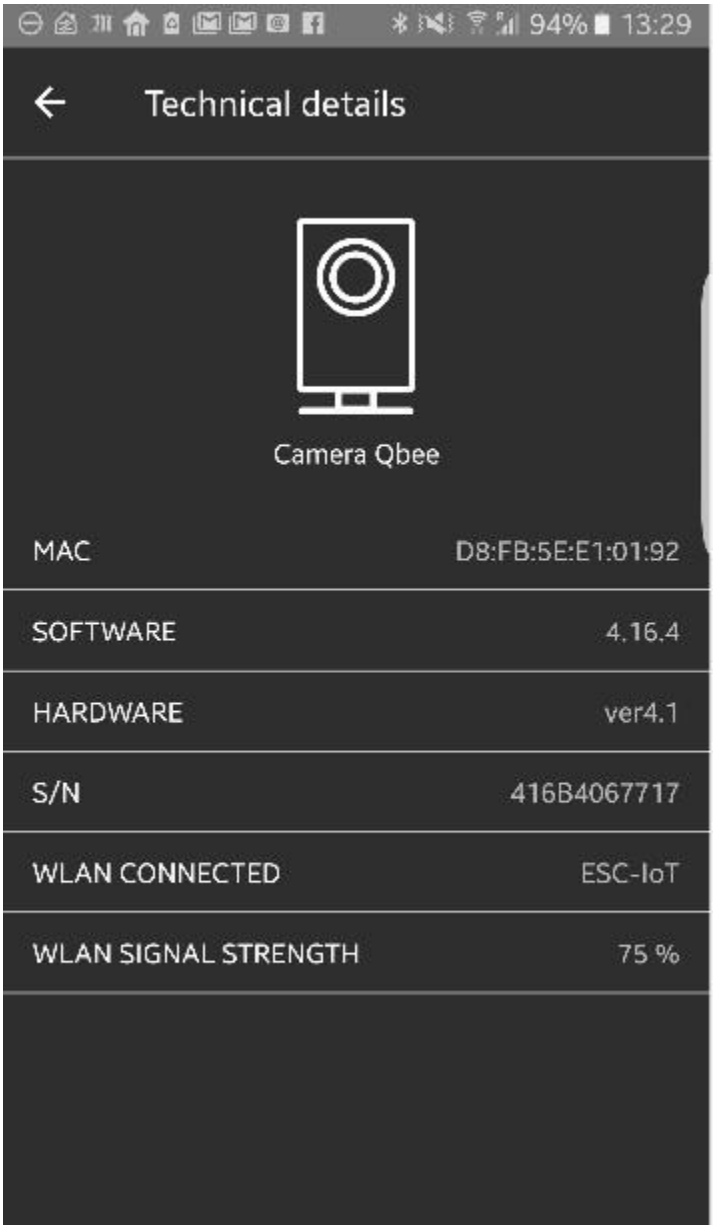


According to the screenshots the alarm system has a:

- station – The cube
- motion sensor – The motion
- contact sensor – The bouncer.

Jessie Pinkman uses a remote tag to arm and disarm the alarm system called The Boss.

Screenshot of Qbee camera technical details



1.1.1 Ismart alarm database

In the Samsung image dump I found a database that shows the activity on the Ismart alarm. I could see which user operated the camera and what actions they took. From this database I can conclude that only 3 accounts had access to the alarm system:

- The boss
- J. Pinkman
- Pandadodu

The boss is a nickname for J Pinkmans phone that he uses to control the Iot devices in the lab remotely. He also has a remote tag that has his name.

Pandadodu is the other user that has access to the alarm system. His account name is very similar to one of Jessies friends D. Pandana. We can assume the account belongs to him due to that.

This database gave us the crucial information that there were only 2 users controlling the alarm system.

Table: TB_IPUDairy

	date	action	IPUID	logType	sensorName	operator	sensorType	sensorID	userID	profileid	profileName
1	1526546272		004D3209D9E4	2		pandadodu				2	DISARM
2	1526546071		004D3209D9E4	2		pandadodu				2	DISARM
3	1526546057		004D3209D9E4	2		TheBoss				1	HOME
4	1526545350		004D3209D9E4	2		TheBoss				2	DISARM
5	1526545342		004D3209D9E4	2		JPinkman				0	ARM
6	1526544597		004D3209D9E4	2		TheBoss				2	DISARM
7	1526543270		004D3209D9E4	2		JPinkman				0	ARM
8	1526543122		004D3209D9E4	2		TheBoss				2	DISARM
9	1526478927		004D3209D9E4	2		JPinkman				0	ARM
10	1526478917		004D3209D9E4	2		JPinkman				2	DISARM
11	1526478911		004D3209D9E4	2		JPinkman				2	DISARM
12	1526478907		004D3209D9E4	2		JPinkman				2	DISARM
13	1526478811		004D3209D9E4	2		JPinkman				0	ARM
14	1526478790		004D3209D9E4	2		JPinkman				1	HOME
15	1526478460		004D3209D9E4	2		TheBoss				2	DISARM
16	1526478453		004D3209D9E4	2		TheBoss				2	DISARM
17	1526478438		004D3209D9E4	2		TheBoss				1	HOME
18	1526478435		004D3209D9E4	2		TheBoss				3	PANIC
19	1526478434		004D3209D9E4	2		TheBoss				3	PANIC
20	1526389527		004D3209D9E4	2		JPinkman				2	DISARM
21	1526389483		004D3209D9E4	2		pandadodu				1	HOME
22	1526389427		004D3209D9E4	2		TheBoss				2	DISARM
23	1526389423		004D3209D9E4	2		pandadodu				3	PANIC
24	1526389416		004D3209D9E4	2		pandadodu				2	DISARM
25	1526389408		004D3209D9E4	2		pandadodu				3	PANIC
26	1526389391		004D3209D9E4	2		pandadodu				3	PANIC
27	1526388095		004D3209D9E4	2		JPinkman				2	DISARM
28	1526387900		004D3209D9E4	2		JPinkman				0	ARM
29	1526377133	2	004D3209D9E4	5							
30	1526376860	1	004D3209D9E4	5							

1 - 30 of 30 Go to: 1

28 row(s), 1 column(s). Sum: 0; Average: 0; Min: 0; Max: 0

1.1.2 Ismart alarm plain text data

In the Samsung dump file, I found an xml file coming from the Ismart alarm that was not encoded. All the data was written in plain text which can lead to serious security problems in the form of man in the middle attacks. The xml file is called ISmartAlarmData.xml.

Listing

/img_blk0_sda.bin/vol_vol21/data/iSA.common/shared_prefs — 8 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2018-05-17 20:38:32 EEST	2018-05-17 20:38:32 EEST	2018-05-15 14:32:23 EEST	2018-05-15 14:32:23 EEST	4096	Allocated	Allocated	unknown	/img_blk0_sda.bin/vol_vol21/c
[parent folder]				2018-05-17 20:58:01 EEST	2018-05-17 20:58:01 EEST	2018-05-15 14:09:51 EEST	2018-05-15 14:09:51 EEST	4096	Allocated	Allocated	unknown	/img_blk0_sda.bin/vol_vol21/c
AD_PAGE_CONTENT.xml			1	2018-05-15 14:32:56 EEST	2018-05-15 14:32:56 EEST	2018-05-15 14:32:56 EEST	2018-05-15 14:32:56 EEST	2081	Allocated	Allocated	unknown	/img_blk0_sda.bin/vol_vol21/c
com.google.android.gcm.xml			1	2018-05-15 14:32:24 EEST	2018-05-15 14:32:24 EEST	2018-05-15 14:32:24 EEST	2018-05-15 14:32:24 EEST	308	Allocated	Allocated	unknown	/img_blk0_sda.bin/vol_vol21/c
iSmartAlermData.xml			1	2018-05-17 20:30:42 EEST	2018-05-17 20:30:42 EEST	2018-05-17 20:30:42 EEST	2018-05-17 20:30:42 EEST	1332	Allocated	Allocated	unknown	/img_blk0_sda.bin/vol_vol21/c
MQTT_Message_Service.xml			1	2018-05-17 20:38:32 EEST	2018-05-17 20:38:32 EEST	2018-05-17 20:38:32 EEST	2018-05-17 20:38:32 EEST	164	Allocated	Allocated	unknown	/img_blk0_sda.bin/vol_vol21/c
MQTT_Message_Service.xml.bak			1	2018-05-17 20:55:35 EEST	2018-05-17 20:55:35 EEST	2018-05-17 20:55:35 EEST	2018-05-17 20:55:35 EEST	1612	Unallocated	Allocated	unknown	/img_blk0_sda.bin/vol_vol21/c
REG_KEY.xml			1	2018-05-15 14:32:24 EEST	2018-05-15 14:32:24 EEST	2018-05-15 14:32:24 EEST	2018-05-15 14:32:24 EEST	226	Allocated	Allocated	unknown	/img_blk0_sda.bin/vol_vol21/c

Data Content

Hex | Text | Application | File Metadata | OS Account | Data Artifacts | Analysis Results | Context | Annotations | Other Occurrences

Strings | Indexed Text | Translation

Page: 1 of 1 Page | Matches on page: - of - Match | 100% | Reset | Text Source: File Text


```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
  <string name="password">esc_iot_2018</string>
  <string name="phoneNum">0792245315</string>
  <string name="monitorShowFrag">fragment3_6_monitoring</string>
  <string name="41-0792245315-uuid">41_079224531575KY4lfi</string>
  <string name="mqtt_client_id">0241_079224531575KY4lfi</string>
  <string name="fragment">fragment3_6_monitoring</string>
  <string name="notification_ID">APA91bHIqXmrhIXxowI2lAb2qAxpHg9BU29rqTNR68L7Odvp3AL_M1y7Mf_UkV64LSUfusoDvuykw92vX0LuglKICa8fWYDXIjk964Cp_8koA2DlMxt14pE</string>
  <string name="0792245315-lasthomeid">149649</string>
  <set name="mqtt_topic_array">
    <string>/ISA/Home/149649/User/200873/Info/#</string>
    <string>/ISA/Home/149649/Info/#</string>
    <string>/ISA/Init/Device/#</string>
  </set>
  <boolean name="isShowFamilyMask" value="true" />
  <string name="UUID">77d30665-d32a-4a64-8526-5dc31b4427a8</string>
  <boolean name="isRemember" value="true" />
  <string name="country">Switzerland</string>
  <string name="countryCode">+41</string>
  <boolean name="isF" value="true" />
  <string name="iSA">fragment5_4_device_cubeone</string>
  <string name="icameraShowFrag">fragment4_0a_camera_main</string>
  <boolean name="showmembermask" value="true" />
</map>
```

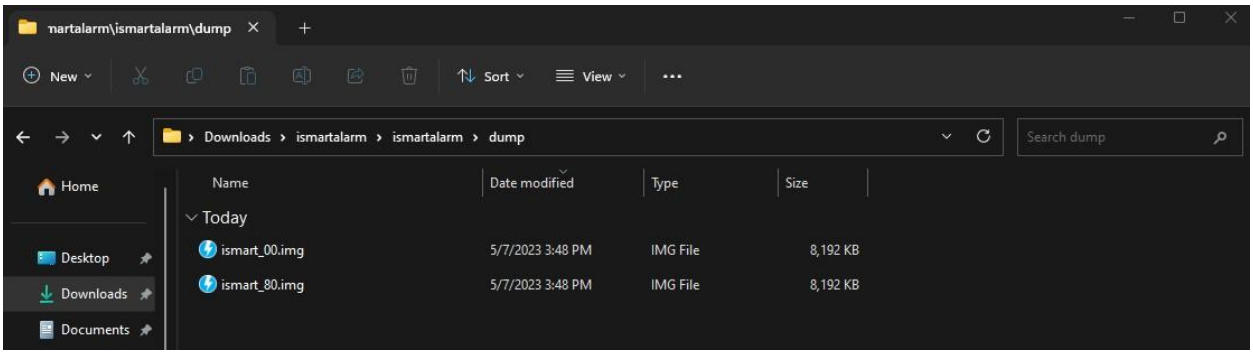

Press the "Print Scrn" on your keyboard to take a screenshot

Wink smart home system

1.2 I smart alarm image and diagnostic logs.

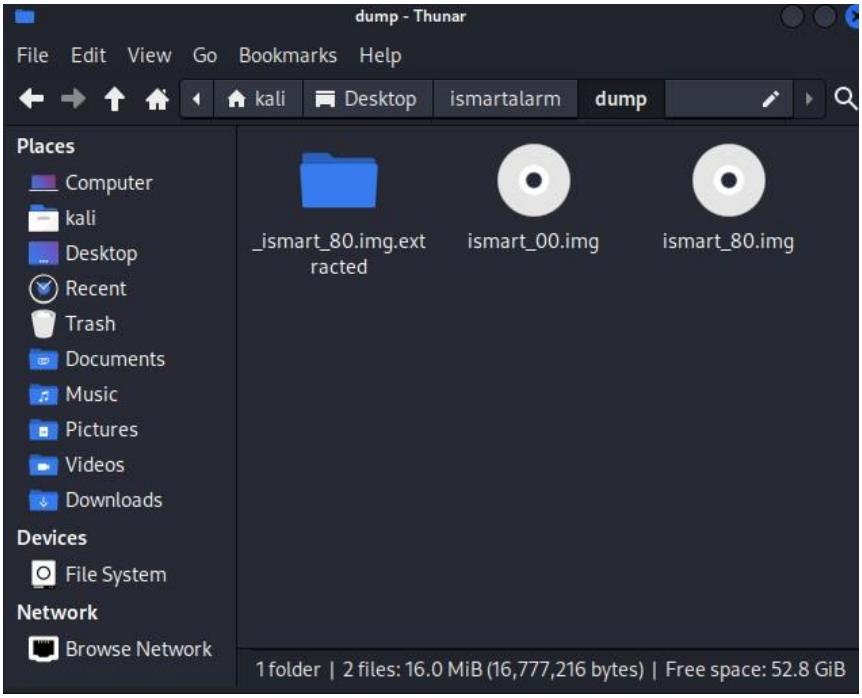
Before I started examining the files I wanted to understand how the ismart alarm works. According to Wikipedia it is an alarm system that is assembled by the user according to his needs. This might include more sensors of various kinds. The alarm system can be operated through a smartphone. It monitors the sensors and in case of unwanted access, it sends notifications to the user's smartphone.

After I was familiar with the arlo alarm system's functions I examined the files.



I used binwalk in Linux to extract the firmware images.

```
┌──(kali㉿kali)-[~/Desktop/ismartalarm/dump]
└─$ binwalk -e -M ismart_80.img

Scan Time:     2023-05-07 12:58:54
Target File:   /home/kali/Desktop/ismartalarm/dump/ismart_80.img
MD5 Checksum:  bbf31212052b73a558fe1d96162a3c09
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
3960          0xF78           uImage header, header size: 64 bytes, header CRC: 0x1A086BAF, created: 2013-04-28 09:57:43, image size: 107
896 bytes, Data Address: 0x80200000, Entry Point: 0x80200000, data CRC: 0x8FDE24EE, OS: Linux, CPU: MIPS, image type: Standalone Program,
 compression type: none, image name: "SPI Flash Image"
2184976       0x215710        U-Boot version string, "U-Boot 1.1.3 (Apr 28 2013 - 17:57:40)"
2185568       0x215960        CRC32 polynomial table, little endian
3145728       0x300000        LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 6126127 bytes


Scan Time:     2023-05-07 12:58:56
Target File:   /home/kali/Desktop/ismartalarm/dump/_ismart_80.img.extracted/300000
MD5 Checksum:  6057e540000d415b0af58e8abd9d856f
Signatures:    411

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
3854388       0x3AD034        Linux kernel version 2.6.21
3855376       0x3AD410        CRC32 polynomial table, little endian
3880880       0x3B37B0        DES SP1, little endian
3881392       0x3B39B0        DES SP2, little endian
3891024       0x3B5F50        CRC32 polynomial table, little endian
3897808       0x3B79D0        SHA256 hash constants, little endian
3903552       0x3B9040        AES Inverse S-Box
3904320       0x3B9340        AES S-Box
3953532       0x3C537C        Unix path: /usr/gnemul/irix/
3955452       0x3C5AFC        Unix path: /usr/lib/libc.so.1
3994328       0x3CF2D8        Unix path: /var/run/udhcpc.pid
4064680       0x3E05A8        Unix path: /etc/Wireless/RT2860STA/RT2860STA.dat
4067836       0x3E11FC        Unix path: /usr/bin/killall
4148167       0x3F4BC7        Neighborly text, "NeighborSolicitsts"
4148191       0x3F4BDF        Neighborly text, "NeighborAdvertisementsmp6OutDestUnreachs"
4148392       0x3F4CA8        Neighborly text, "NeighborSolicitsirects"
4148420       0x3F4CC4        Neighborly text, "NeighborAdvertisementssponses"
4163942       0x3F8966        Copyright string: "Copyright (C) 2004-2005 Intel Corporation <jketreno@linux.intel.com>"
4244704       0x40C4E0        CRC32 polynomial table, little endian
4248176       0x40D270        AES S-Box
4456448       0x440000        LZMA compressed data, properties: 0x5D, dictionary size: 1048576 bytes, uncompressed size: 5938688 bytes


Scan Time:     2023-05-07 12:58:59
Target File:   /home/kali/Desktop/ismartalarm/dump/_ismart_80.img.extracted/_300000.extracted/440000
```



I compared the files, they are identical which indicated that I should explore only one of the files.

```
┌──(kali㉿kali)-[~/Desktop/ismartalarm/dump]
└─$ diff -s ismart_00.img ismart_80.img
Files ismart_00.img and ismart_80.img are identical

┌──(kali㉿kali)-[~/Desktop/ismartalarm/dump]
└─$
```

I used a tool called “ranger” to view the extracted files.

```
kali@kali: ~/Desktop/ismartalarm/dump
File  Actions  Edit  View  Help
kali@kali /home/kali/Desktop/ismartalarm/dump/_ismart_80.img.extracted/_300000.extracted/_440000.extracted/cpio-root/lib
cpio-root        bin        39   ipsec
 0.cpio          dev         1   modules
                 etc         1   ld-uClibc-0.9.28.so
                 etc_ro     13   ld-uClibc.so.0
                 home        0   libc.so
                 lib        37   libc.so.0
                 media       0   libcrypt-0.9.28.so
                 mnt         0   libcrypt.so
                 proc        0   libcrypt.so.0
                 sbin       48   libcrypto.so
                 sys         0   libcrypto.so.0.9.8
                 tmp         0   libcrypto.so.1.0.0
                 usr         4   libcurl.a
                 var         0   libcurl.so
                 init  → 371 K   libcurl.so.4.4.0
                                 libdl-0.9.28.so
                                 libdl.so
                                 libdl.so.0
                                 libembMQTT.so
                                 libiw.so.29
                                 liblogserver.so
                                 libm-0.9.28.so
                                 libm.so
                                 libm.so.0
                                 libnvram-0.9.28.so
                                 libnvram.so
                                 libnvram.so.0
                                 libpaho-mqtt3as.so
                                 libpaho-mqtt3as.so.1
                                 libpaho-mqtt3as.so.1.0
                                 libpthread-0.9.28.so
                                 libpthread.so
                                 libpthread.so.0
                                 libssl.so
                                 libssl.so.0.9.8
drwxr-xr-x 4 kali kali 37 2023-05-07 12:59                371K sum, 52.7G free  6/15  All
```

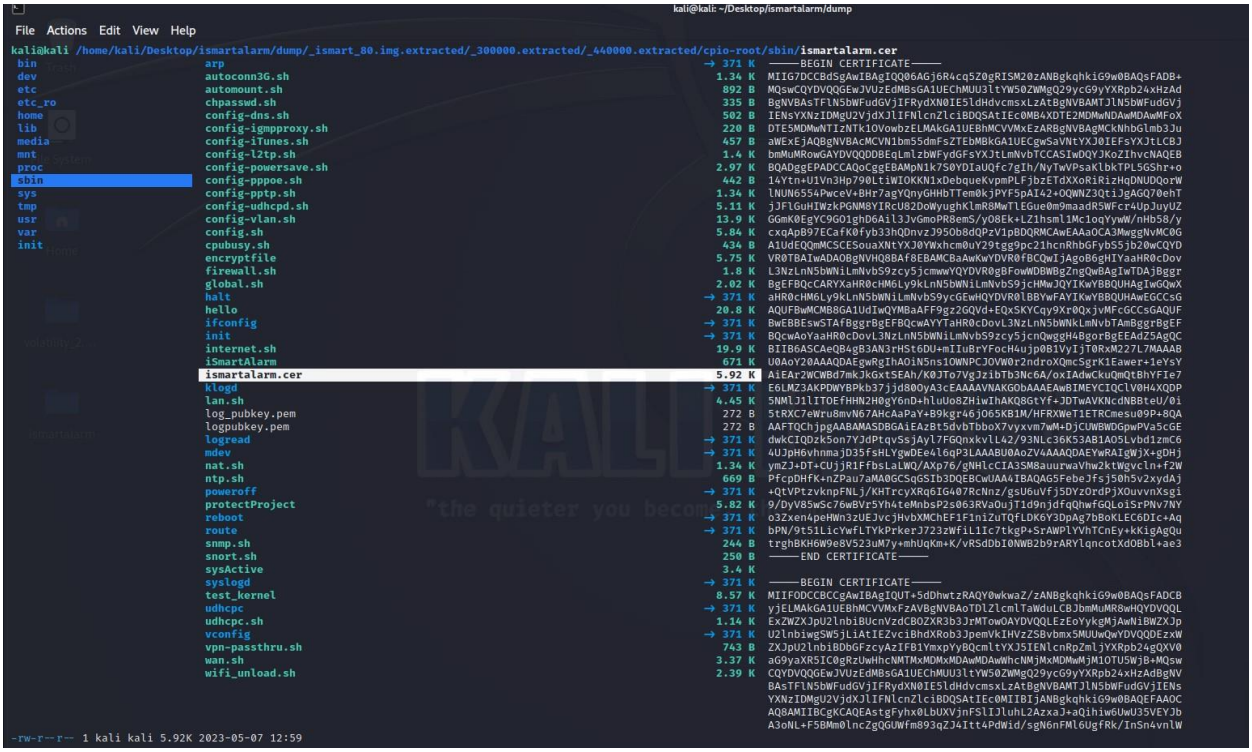
I found the default configuration for the camera

```
kali@kali: ~/Desktop/ismartalarm/dump
File  Actions  Edit  View  Help
kali@kali /h/k/D/ismartalar/dump/_ismart_80.img.extracted/_300000.extracted/_440000.extracted/cpio-root/usr/share/iSmart/default_config
 iSmart        cc1110                88.8 K  #The word of "Default" must not be removed
 udhcpc        default_config         287 B  Default
               IPU                   4.39 K  isFactory=02
                                             Rl=
                                             ipaddr=192.168.1.68
                                             udpcloudip=udpservice.ismartalarm.com
                                             cloudip=api.ismartalarm.com
                                             upgradeip=upgrade.ismartalarm.com
                                             subnetmask=255.255.255.0
                                             ipconfig=1
                                             ipgateway=192.168.1.1
                                             ipddns=202.99.96.68
                                             Conf_Version=1.0.0.1
-rw-r--r-- 1 kali kali 287B 2023-05-07 12:59                    93.5K sum, 52.7G free  2/3  All
```

Public key for updating the firmware

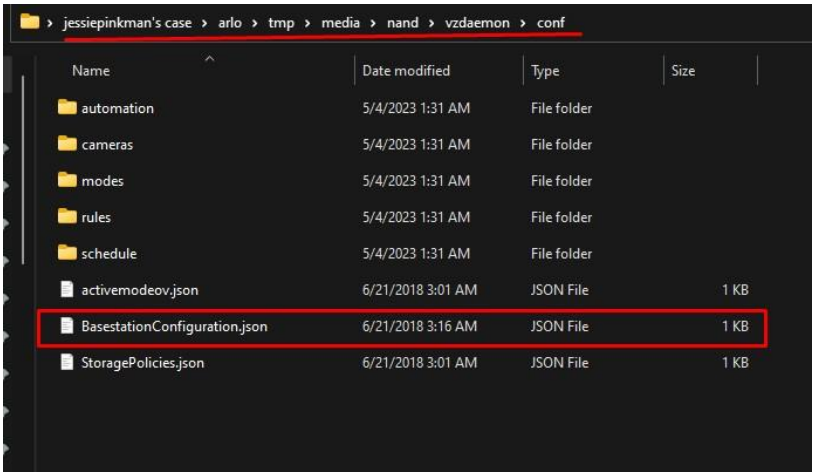
```
kali@kali: ~/Desktop/ismartalarm/dump
File  Actions  Edit  View  Help
kali@kali /hom/kali/Desktop/ismartalarm/dump/_ismart_80.img.extracted/_300000.extracted/_440000.extracted/cpio-root/sbin/log_pubkey.pem
 bin           automount.sh            892 B  -----BEGIN PUBLIC KEY-----
 dev           chpasswd.sh             335 B  MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDIVgZ4JosIeTzvfB58164RU9Ke
 etc           config-dns.sh           502 B  23b4AgfTWOQfiUMvgvzJjcyyfb0pzk6bDmljyK1e0g2XSxkGMtKPbK1I+tY6yEVC
 etc_ro        config-igmpproxy.sh     220 B  di/l8swordnr/O3daiy4AhUq/wCwRRhwgaAyprsUOQNH8v82U3pnpTNxwf+Ux5jb
 home          config-iTunes.sh        457 B  GV9KI5GnFjKax1URXQIDAQAB
 lib           config-l2tp.sh          1.4 K  -----END PUBLIC KEY-----
 media         config-powersave.sh    2.97 K
 mnt           config-pppoe.sh         442 B
 proc          config-pptp.sh         1.34 K
 sbin          config-udhcpd.sh       5.11 K
 sys           config-vlan.sh         13.9 K
 tmp           config.sh              5.84 K
 usr           cpubusy.sh              434 B
 var           encryptfile            5.75 K
 init          firewall.sh             1.8 K
               global.sh              2.02 K
               halt                 -> 371 K
               hello                  20.8 K
               ifconfig             -> 371 K
               init                 -> 371 K
               internet.sh            19.9 K
               iSmartAlarm             671 K
               ismartalarm.cer        5.92 K
               klogd                -> 371 K
               lan.sh                 4.45 K
               log_pubkey.pem          272 B
               logpubkey.pem           272 B
               logread              -> 371 K
               mdev                 -> 371 K
               nat.sh                 1.34 K
               ntp.sh                  669 B
               poweroff             -> 371 K
               protectProject         5.82 K
               reboot               -> 371 K
               route                -> 371 K
-rw-r--r-- 1 kali kali 272B 2023-05-07 12:59                    5.49M sum, 52.7G free  28/48  15%
```

Signing certificates



1.3 arlo pro camera

There are multiple JSON files in the folder of the camera. I used VS code and a web browser to see their contents. I found the base configuration of the camera in VZSAEMON/conf



Conf file opened in Visual Studio code.

```
EXPLORER
OPEN EDITORS 3 unsaved
  BasestationConfi...
  FosIPC_E_app_ve...
  Untitled-1
NO FOLDER OPENED
You have not yet opened a folder.

BasestationConfiguration.json ●   FosIPC_E_app_ver2.x.1.30.bin ●   Untitled-1 ●
C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > BasestationConfiguration.json > apInvalidated
1 {"objVersion":"2.0","autoUpdate":true,"timeZone":"CET-1CEST,M3.5.0,M10.5.0/3","olsonTimeZone":"Europe/Amsterdam","antiFlicker":{"mode":0},
2 "lowBatteryAlert":{"enabled":true},"lowSignalAlert":{"enabled":false},"claimed":true,"mcsEnabled":true,"apIdentifier":{"eth0":"B8:27:EB:0E:3B:45"},
3 "apInvalidated":false,"authTokenType":2,"authToken":"","authTokenV2":"G/+QEd+CJk2nUBIct9y2gscK+sPgGFbUo7o/2BHhY97i9xrP1ONNR6EWakNb23HX","recoveryRebootCount":2}
4
```

I found 3 JSON files called “mode..”. These are the modes the camera can be set in. Depending on the mode it will act differently.

Mode 0 – DISARMED

```
C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > modes > mode0.json > ...
1 {"name":"","id":"mode0","type":"disarmed","rules":[],"objVersion":"1.0","fromAutomationconv":true}
2
```

Mode 1- ARMED

```
C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > modes > mode1.json > ...
1 {"name":"","id":"mode1","type":"armed","rules":["r_mode1_59U17B7BB8B46"],"objVersion":"1.0","fromAutomationconv":true}
2
```

Mode 2 - ALWAYS

```
C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > modes > mode2.json > ...
1 {"name":"Always","id":"mode2","rules":["r_mode2_59U17B7BB8B46"],"objVersion":"1.0","fromAutomationconv":true}
2
C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > modes > mode1.json > ...
1 {"name":"","id":"mode1","type":"armed","rules":["r_mode1_59U17B7BB8B46"],"objVersion":"1.0","fromAutomationconv":true}
2
```

These modes operate under 2 rules that I found.

Rule - mode1_59U17B7BB8B46

```
C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > rules > r_mode1_59U17B7BB8B46.json > id
1 {"id":"r_mode1_59U17B7BB8B46","name":"","protected":true,"objVersion":"1.0","triggers":[{"type":"pirMotionActive",
2 "deviceId":"59U17B7BB8B46","sensitivity":80}],"actions":[{"deviceId":"59U17B7BB8B46","type":"recordVideo","stopCondition":{"type":"triggerEndDetected",
3 "deviceId":"59U17B7BB8B46"}},{"type":"pushNotification"}],"fromAutomationconv":true}
C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > modes > mode2.json > ...
1 {"name":"Always","id":"mode2","rules":["r_mode2_59U17B7BB8B46"],"objVersion":"1.0","fromAutomationconv":true}
2
```

Rule - r_mode2_59U17B7BB8B46

C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > rules > {} r_mode2_59U17B7BB8B46.json > id


```
{"id":"r_mode2_59U17B7BB8B46","name":"","protected":false,"objVersion":"1.0","triggers":[{"type":"audioAmplitude",
"deviceId":"59U17B7BB8B46","sensitivity":3},{"type":"pirMotionActive","deviceId":"59U17B7BB8B46","sensitivity":80}],"actions":[{"deviceId":"59U17B7BB8B46",
"type":"recordVideo","stopCondition":{"type":"triggerEndDetected","deviceId":"59U17B7BB8B46"}},{"type":"pushNotification"}],"fromAutomationconv":true}
```


I also found a schedule for the camera with time indicators in arlo\tmp\media\nand\vzdaemon\conf\schedule

C: > Users > MSI > Desktop > jessiepinkman's case > arlo > tmp > media > nand > vzdaemon > conf > schedule > {} schedule.json > [ ] schedule > {} 10


```
{"active":false,"schedule":[{"modeId":"mode0","startTime":0},{"modeId":"mode1","startTime":28800000},{"modeId":"mode0",
"startTime":61200000},{"modeId":"mode1","startTime":115200000},{"modeId":"mode0","startTime":147600000},{"modeId":"mode1","startTime":201600000},
{"modeId":"mode0","startTime":234000000},{"modeId":"mode1","startTime":288000000},{"modeId":"mode0","startTime":320400000},{"modeId":"mode1","startTime":374400000},
{"modeId":"mode0","startTime":406800000}],"objVersion":"2.0"}
```


I had access to the “nvram” log files of the camera as well. Log parser 2.2 was used to view them but they didn’t contain information that I could use.

```
C:\Program Files (x86)\Log Parser 2.2>"C:\Users\MSI\Desktop\jessiepinkman's case\arlo\nvram.log"
```

nvram.log

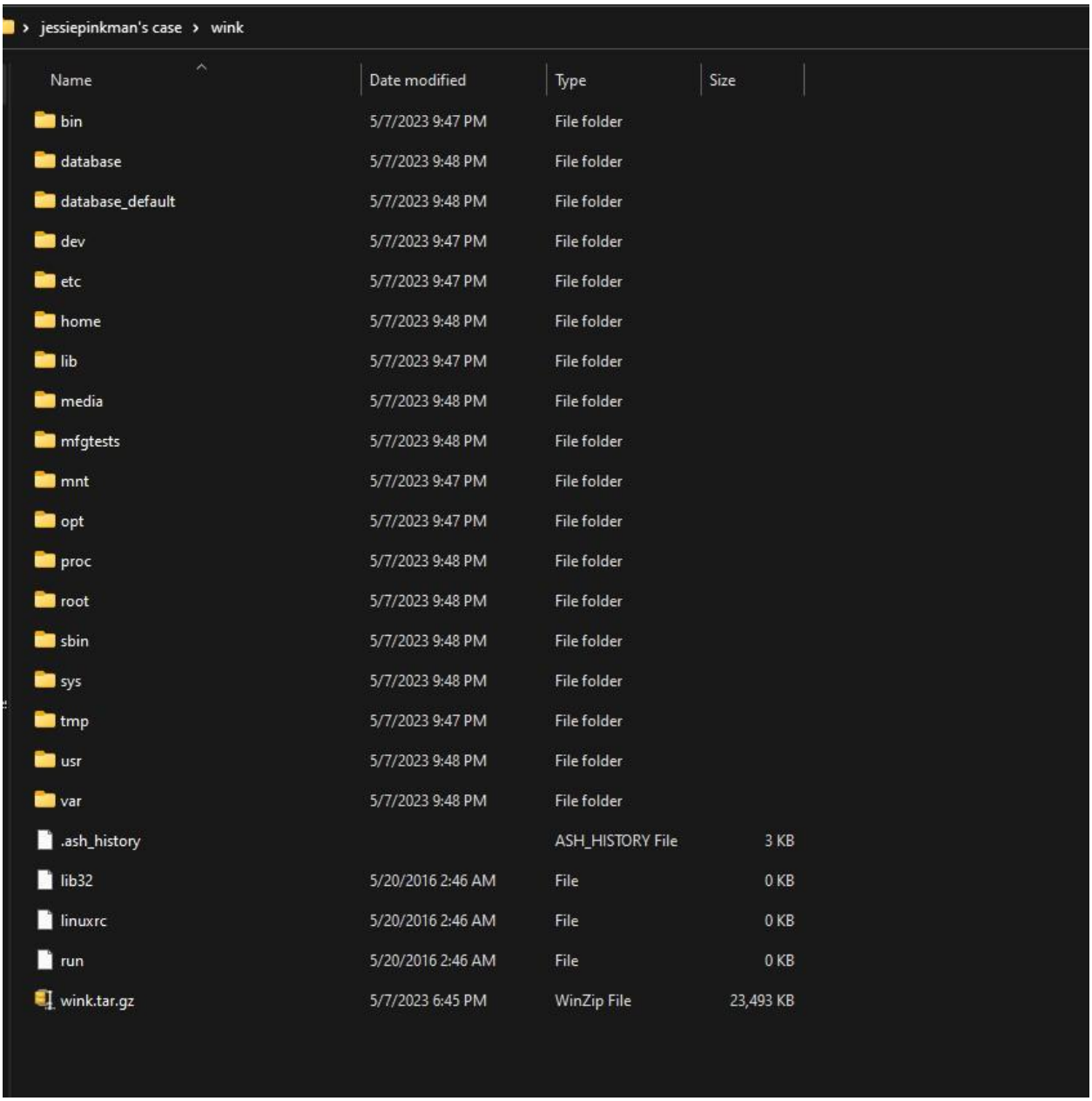
File Edit View


```
nvram show
wl0_scb_activity_time=0
wan2_dns=
wlan_acl_dev24=
wla_temp_wep_length_2=0
wl_radius_port=1812
wlg_wds_mode=1
ap_mode_cur=1
x_broker_port=443
wl1_wme=auto
wlan_acl_dev25=
gui_check_enable=1
connect_event_file=event_file
wan_unit=0
wlan_acl_dev26=
wla_ssid_2=NETGEAR_EXT
wl1_auth=2
wlan_acl_dev27=
wla_ssid_3=
wl0_wmf_bss_enable=0
wan0_primary=1
cur_opmode2=300Mbps
lan2_lease=86400
wan_route=
wlan_acl_dev28=
wla_temp_ssid=
wla_ssid_4=
as_genie=0
wl0_rifs_advert=auto
wl0_mcast_regen_bss_enable=1
x_claimed_url=https://registration.ngxcld.com/registration/status
pppoe2_keepalive=0
wlan_acl_dev29=
wla_region=5
wl_txstreams=0
```


Ln 1, Col 1 100% Unix (LF) UTF-8

1.4 WinkHub

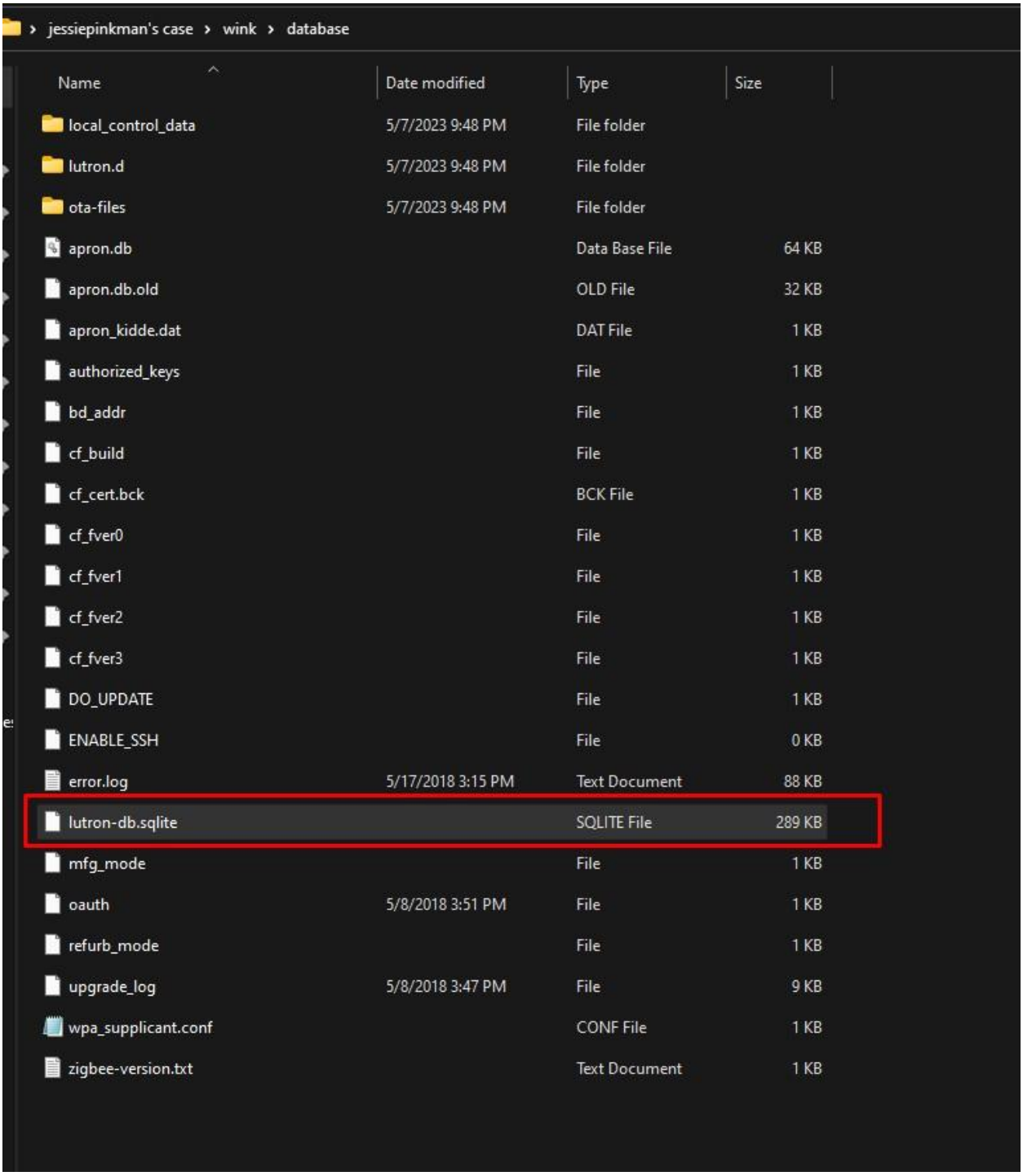
I explored the files of the wink folder.



› jessiepinkman's case › wink

Name	Date modified	Type	Size
bin	5/7/2023 9:47 PM	File folder	
database	5/7/2023 9:48 PM	File folder	
database_default	5/7/2023 9:48 PM	File folder	
dev	5/7/2023 9:47 PM	File folder	
etc	5/7/2023 9:47 PM	File folder	
home	5/7/2023 9:48 PM	File folder	
lib	5/7/2023 9:47 PM	File folder	
media	5/7/2023 9:48 PM	File folder	
mfgtests	5/7/2023 9:48 PM	File folder	
mnt	5/7/2023 9:47 PM	File folder	
opt	5/7/2023 9:47 PM	File folder	
proc	5/7/2023 9:48 PM	File folder	
root	5/7/2023 9:48 PM	File folder	
sbin	5/7/2023 9:48 PM	File folder	
sys	5/7/2023 9:48 PM	File folder	
tmp	5/7/2023 9:47 PM	File folder	
usr	5/7/2023 9:48 PM	File folder	
var	5/7/2023 9:48 PM	File folder	
.ash_history		ASH_HISTORY File	3 KB
lib32	5/20/2016 2:46 AM	File	0 KB
linuxrc	5/20/2016 2:46 AM	File	0 KB
run	5/20/2016 2:46 AM	File	0 KB
wink.tar.gz	5/7/2023 6:45 PM	WinZip File	23,493 KB

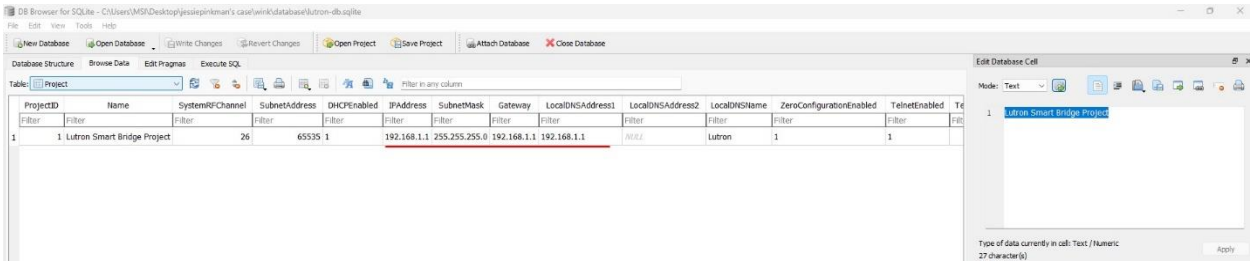
I didn’t find much useful information except for a database file called Lutron.db



jessiepinkman's case › wink › database

Name	Date modified	Type	Size
local_control_data	5/7/2023 9:48 PM	File folder	
lutron.d	5/7/2023 9:48 PM	File folder	
ota-files	5/7/2023 9:48 PM	File folder	
apron.db		Data Base File	64 KB
apron.db.old		OLD File	32 KB
apron_kidde.dat		DAT File	1 KB
authorized_keys		File	1 KB
bd_addr		File	1 KB
cf_build		File	1 KB
cf_cert.bck		BCK File	1 KB
cf_fver0		File	1 KB
cf_fver1		File	1 KB
cf_fver2		File	1 KB
cf_fver3		File	1 KB
DO_UPDATE		File	1 KB
ENABLE_SSH		File	0 KB
error.log	5/17/2018 3:15 PM	Text Document	88 KB
lutron-db.sqlite		SQLITE File	289 KB
mfg_mode		File	1 KB
oauth	5/8/2018 3:51 PM	File	1 KB
refurb_mode		File	1 KB
upgrade_log	5/8/2018 3:47 PM	File	9 KB
wpa_supplicant.conf		CONF File	1 KB
zigbee-version.txt		Text Document	1 KB

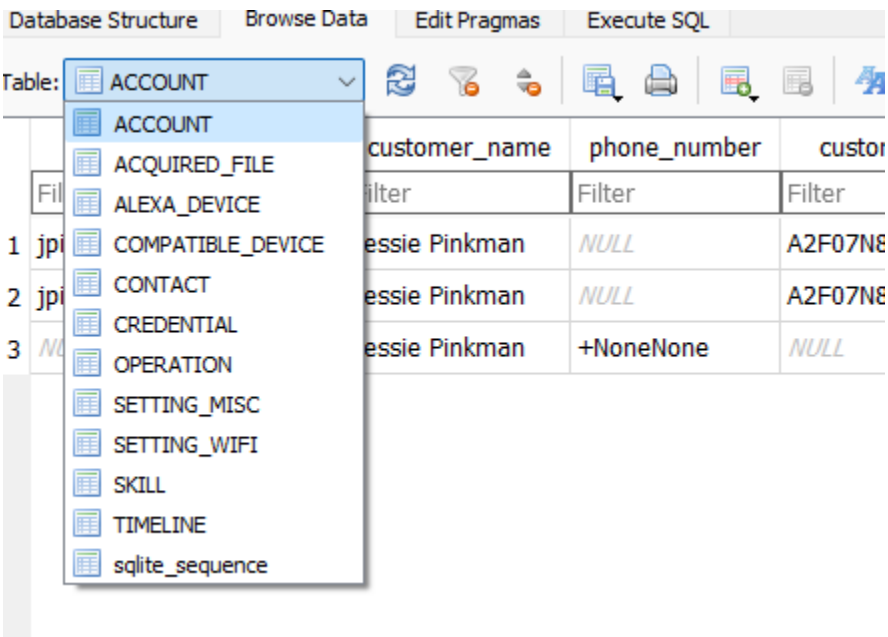
I opened it with DB browser (SQlite) and got an Ip address of the lutron bridge.



I already had pictures of the bridge taken by Jessie Pinkman's phone and now I got the IP.

1.5 Amazon Echo

The database file contains a lot of useful information. Jessie Pinkman used the amazon echo to control the other IoT devices in the drug lab. I opened the db file with DB browser for SQlite. There are 12 tables in the database and each one gives us clues for completing the investigation.



SKILL table gives us information about the IoT setup of the drug lab. Every device connected to the amazon echo is listed in this table. I can see all the devices I have investigated in there (Arlo camera, Ismart alarm system, Nest camera, Wink hub). If someone with malicious intentions wants to infiltrate the drug lab, his best option is to gain access over the amazon echo since it controls all the other devices.

Table: SKILL

	title	developer_name	account_linked	release_date	short	desc	vendor_id	skill_id
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	Arlo	NULL	True	2017-06-25 12:36:32.000	Access your Arlo cameras with simple voice ...	With the Arlo Skill and Alexa, you can now acces...	MY7L8IYP83Q84	amzn1.ask.skill.8d4d9359-9124-43f9-bb58
2	Nest Camera	NULL	True	2017-06-25 12:36:39.000	Stream your Nest camera video to your Echo Sh...	Nest cameras are designed to help you look after...	M258KP8OWYZDVQ	amzn1.ask.skill.381678d7-278a-4ff5-9071
3	Reuters TV (U.S.)	Thomson Reuters	False	2017-01-13 00:05:02.000	Up-to-date news from Reuters TV.	Reuters Now is your 5 minute news briefing from...	M10DYU5SYWLUEJ	amzn1.ask.skill....
4	Weather	NULL	False	2016-08-02 17:12:29.000	A brief update on today' weather conditions.	As part of your Flash Briefing, Alexa will provide ...	M1JK1NFTW50PO4	amzn1.ask.skill.c86d0fa8-0307-471b-82af
5	Wink	NULL	True	2016-04-20 00:46:31.000	With Amazon Alexa, Wink smart home users can...	Say goodbye to fumbling with the light switch or ...	M262G9N0W7Y1U5	amzn1.ask.skill.013efdab-897c-4dff-9728-
6	iSmartAlarm	NULL	True	2017-05-23 00:18:36.000	iSmartAlarm is the leader in DIY smart home ...	iSmartAlarm is the leader in DIY smart home ...	M3LS6B4DZDHJ46	amzn1.ask.skill.8ccabd3a-a2e5-402a-...

Account table gave me information about the users connected to the amazon echo. This table showed me that Jessie Pinkman is the only user who controls the amazon echo.

Table: ACCOUNT

	customer_email	customer_name	phone_number	customer_id	comms_id	authenticated	source_id
	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	jpinkman2018@gmail.com	Jessie Pinkman	NULL	A2F07N8TDIAK5U	NULL	True	1
2	jpinkman2018@gmail.com	Jessie Pinkman	NULL	A2F07N8TDIAK5U	NULL	NULL	2
3	NULL	Jessie Pinkman	+NoneNone	NULL	NULL	NULL	64

ALEXA_DEVICE table contains information about the amazon echo itself.

Table: ALEXA_DEVICE

	device_account_name	device_family	device_account_id	customer_id	device_serial_number	device_type	sw_version	mac_address	address	postal_code	locale	search_custo
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	This Device	VOX	A0529216353ZKG8WU9M6O	A2F07N8TDIAK5U	515cefc2f44e41dc9b6a4f7d54820900	A2TF17PFR55MTB	130050002	NULL	NULL	NULL	NULL	NULL
2	Jessie's Alexa Apps	MSHOP	AGQS6C6RFOZF	A2F07N8TDIAK5U	6eb18f2fca814f8797c4d970557e435d	A1MPSLFC7L5AFK	130050002	NULL	NULL	NULL	NULL	NULL
3	NULL	NULL	A0529216353ZKG8WU9M6O	NULL	515cefc2f44e41dc9b6a4f7d54820900	A2TF17PFR55MTB	NULL	NULL	NULL	98109	en-us	A2F07N8TDIAK
4	NULL	NULL	AGQS6C6RFOZF	NULL	6eb18f2fca814f8797c4d970557e435d	A1MPSLFC7L5AFK	NULL	NULL	Avenue Forel, Lausanne, VD, CH	1015	en-us	A2F07N8TDIAK

WIFI settings

Table: SETTING_WIFI

	ssid	security_method	pre_shared_key	source_id
	Filter	Filter	Filter	Filter
1	ESC-IoT	WPA_PSK	esc_iot_2018	3

TIMELINE table if very important to the investigation because it gives information about actions that happened in the lab. These actions were taken by J. Pinkman since he is the only user of the amazon echo. I filtered the date to show me only actions that happened on the day of the raid (17.05.2018). There were traces of every day activity – Linking to Spotify , playing led zeppelin. J. Pinkman appears to be the only one using the amazon echo because there aren't any traces of D Pandama and S Varga recorded in its database. There were also events of arming and disarming the alarm.

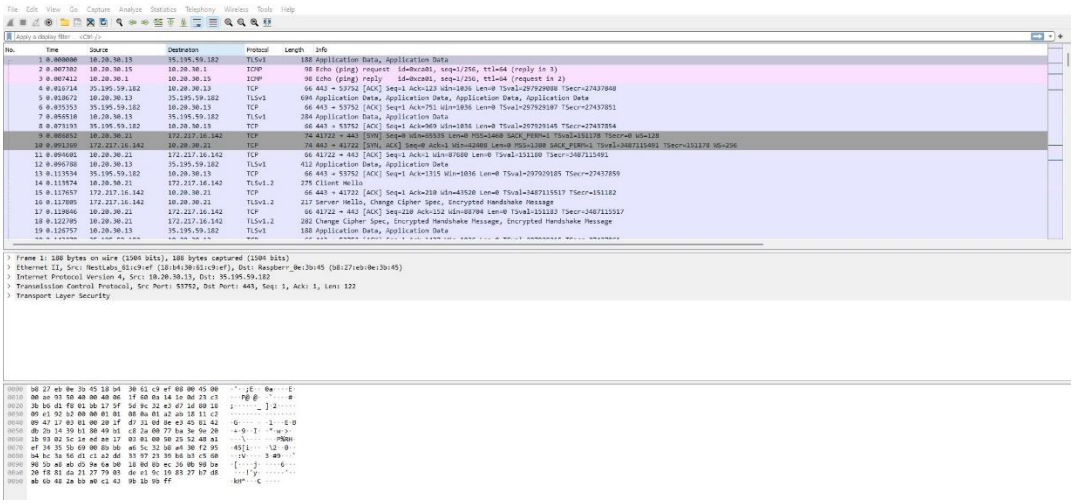
	date	time	timezone	MACB	source	sourcetype	type	user	host	short	desc	version	
	8-05-17	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1	2018-05-17	10:22:20.718	UTC+2	...B	CLOUD	Home	Created	A2F07N8TDIAK5U	B0F00712518400WN	TextCard	Mode Changed (iSmartAlarm)	2	/Users/francesc
2	2018-05-17	10:22:13.528	UTC+2	...B	CLOUD	Home	Created	A2F07N8TDIAK5U	B0F00712518400WN	TextCard	Mode Changed (iSmartAlarm)	2	/Users/francesc
3	2018-05-17	10:16:09.456	UTC+2	...B	CLOUD	Home	Created	A2F07N8TDIAK5U	B0F00712518400WN	SalmonCard	Link Spotify	2	/Users/francesc
4	2018-05-17	10:22:25.439	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History	-	2	/Users/francesc
5	2018-05-17	10:22:20.718	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History	yes	2	/Users/francesc
6	2018-05-17	10:22:13.528	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History	tell i. smart alarm to arm my system	2	/Users/francesc
7	2018-05-17	10:22:09.229	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History	alexa	2	/Users/francesc
8	2018-05-17	10:16:20.470	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History	Unknown	2	/Users/francesc
9	2018-05-17	10:16:09.456	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History	alexa play led zeppelin	2	/Users/francesc
10	2018-05-17	10:22:19.409	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	yes	2	/Users/francesc
11	2018-05-17	10:22:20.720	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	Your system will set to Arm in 30 seconds.	2	/Users/francesc
12	2018-05-17	10:22:12.093	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	tell i. smart alarm to arm my system	2	/Users/francesc
13	2018-05-17	10:22:13.530	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	Your Door is open, Are you sure you want to arm...	2	/Users/francesc
14	2018-05-17	10:22:08.869	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	alexa	2	/Users/francesc
15	2018-05-17	10:16:20.470	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	Unknown	2	/Users/francesc
16	2018-05-17	10:16:08.742	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	alexa play led zeppelin	2	/Users/francesc
17	2018-05-17	10:16:09.458	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	To play Spotify, link your premium account first ...	2	/Users/francesc

The alarm was armed at 10:22 which suggests that Jessie Pinkman left the lab at that time. The action below the marker says that J. Pinkman had 30 seconds to leave the lab before the systems were armed.

11	2018-05-17	10:22:20.720	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	Your system will set to Arm in 30 seconds.	2	/Users/france
12	2018-05-17	10:22:12.093	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	tell i. smart alarm to arm my system	2	/Users/france
13	2018-05-17	10:22:13.530	UTC+2	...B	CLOUD	Activity History	Created	A2F07N8TDIAK5U	B0F00712518400WN	History (Dialog Items)	Your Door is open, Are you sure you want to arm...	2	/Users/france

1.6 Police network traffic extraction

I used Wireshark as my network analyzer to view the network traffic that the police have retrieved from the drug lab. Below is a screenshot of the pcap file opened in wireshark.



Protocol hierarchy

Wireshark · Protocol Hierarchy Statistics · dfrws_police.pcap

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	8335	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	1328	20	9482	1328
Network Time Protocol	0.1	6	0.0	288	40	6	288	40
Dynamic Host Configuration Protocol	0.1	6	0.1	2036	285	6	2036	285
Domain Name System	0.7	28	0.2	3795	531	28	3795	531
Data	0.6	26	0.2	3134	439	26	3134	439
Transmission Control Protocol	96.0	4079	89.7	1475135	206 k	2270	602102	84 k
Transport Layer Security	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	58	3712	520
Data	0.1	6	0.0	558	78	6	558	78
Address Resolution Protocol	0.5	20	0.0	614	86	20	614	86

No display filter.

Close Copy Help

I wanted to see the non-encrypted traffic, so I filtered with “http” parameter and found an interesting communication with the QBEE camera.

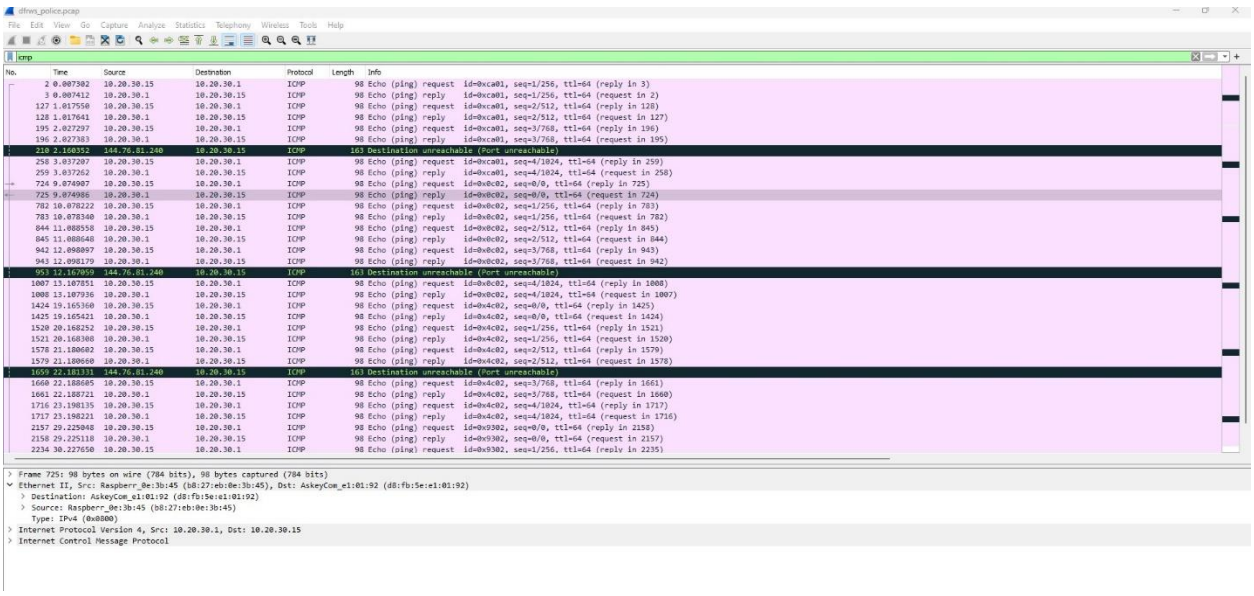
http

No.	Time	Source	Destination	Protocol	Length	Info
694	8.903058	10.20.30.21	10.20.30.15	HTTP	243	GET /verify HTTP/1.1
695	8.906019	10.20.30.15	10.20.30.21	HTTP	104	HTTP/1.1 200 OK
1797	23.901202	10.20.30.21	10.20.30.15	HTTP	243	GET /verify HTTP/1.1
1799	23.904419	10.20.30.15	10.20.30.21	HTTP	104	HTTP/1.1 200 OK
2859	38.906154	10.20.30.21	10.20.30.15	HTTP	243	GET /verify HTTP/1.1
2860	38.912010	10.20.30.15	10.20.30.21	HTTP	104	HTTP/1.1 200 OK
4005	53.903896	10.20.30.21	10.20.30.15	HTTP	243	GET /verify HTTP/1.1
4006	53.907258	10.20.30.15	10.20.30.21	HTTP	104	HTTP/1.1 200 OK

```
> Frame 2859: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
v Ethernet II, Src: SamsungE_73:e3:78 (ac:5f:3e:73:e3:78), Dst: AskeyCom_e1:01:92 (d8:fb:5e:e1:01:92)
  > Destination: AskeyCom_e1:01:92 (d8:fb:5e:e1:01:92)
  > Source: SamsungE_73:e3:78 (ac:5f:3e:73:e3:78)
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 10.20.30.21, Dst: 10.20.30.15
> Transmission Control Protocol, Src Port: 40189, Dst Port: 15700, Seq: 355, Ack: 77, Len: 177
v Hypertext Transfer Protocol
  > GET /verify HTTP/1.1\r\n
    Host: 10.20.30.15:15700\r\n
    Connection: Keep-Alive\r\n
  v Cookie: DST_PORT=4848, JSESSIONID=3c8025ec-494b-4344-813b-555e53de0003, GC_ID=14602\r\n
      Cookie pair: DST_PORT=4848, JSESSIONID=3c8025ec-494b-4344-813b-555e53de0003, GC_ID=14602
  > Content-Length: 0\r\n
    \r\n
    [Full request URI: http://10.20.30.15:15700/verify]
    [HTTP request 3/4]
    [Prev request in frame: 1797]
    [Response in frame: 2860]
    [Next request in frame: 4005]
```

I figured out this device was the qbee camera because I could see the manufacturer which is AskeyCom. It was sending packets containing the session ID and the cookie in plain text. This is a serious security vulnerability that can lead to session hijacking.

I filtered Wireshark to show me the ICMP traffic and I found something bizarre. The Qbee camera was trying to communicate to the raspberry pi in the lab but without success. It was sending multiple ping requests, but the Destination was unreachable.



2.0 Answering questions.

At what time was the illegal drug lab raided?

Time of raid 10:37:52

Amazon echo recorded the last “arming” of the alarm at 10:22 on the day of the raid and Ismart alarm recorded a “disarm” by D Pandana at 10:37:52. I concluded that with the help of epoch converter to show me the time taken from the ISmartAlarm database.

date	action	IPUID	logType	sensorName	operator	sensorType	sensorID	userID	profileid	profileName
Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
1526546272		004D3209D9E4	2		pandadodu				2	DISARM
1526546071		004D3209D9E4	2		pandadodu				2	DISARM

The current Unix epoch time is 1683643689

Convert epoch to human-readable date and vice versa

1526546272 | Timestamp to Human date | [batch convert]

Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **seconds**:
GMT: Thursday, 17 May 2018 8:37:52
Your time zone: четвъртък, 17 май 2018 10:37:52 GMT+02:00 DST
Relative: 5 years ago

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

If YES:

- Which friend?

D Pandana - he was the last person to disarm the Ismart alarm right before the raid happened.

- What is the confidence in such hypothesis?

While we cant confirm with 100% confidence that D Pandana was the friend involved in the raid, he was the last person to disarm the alarm system right before it happened. There is a slight possibility that he might have given his remote tag for the alarm to someone.

My verdict:

80% - D Pandana was involved directly.

20%- D Pandana was involved indirectly.

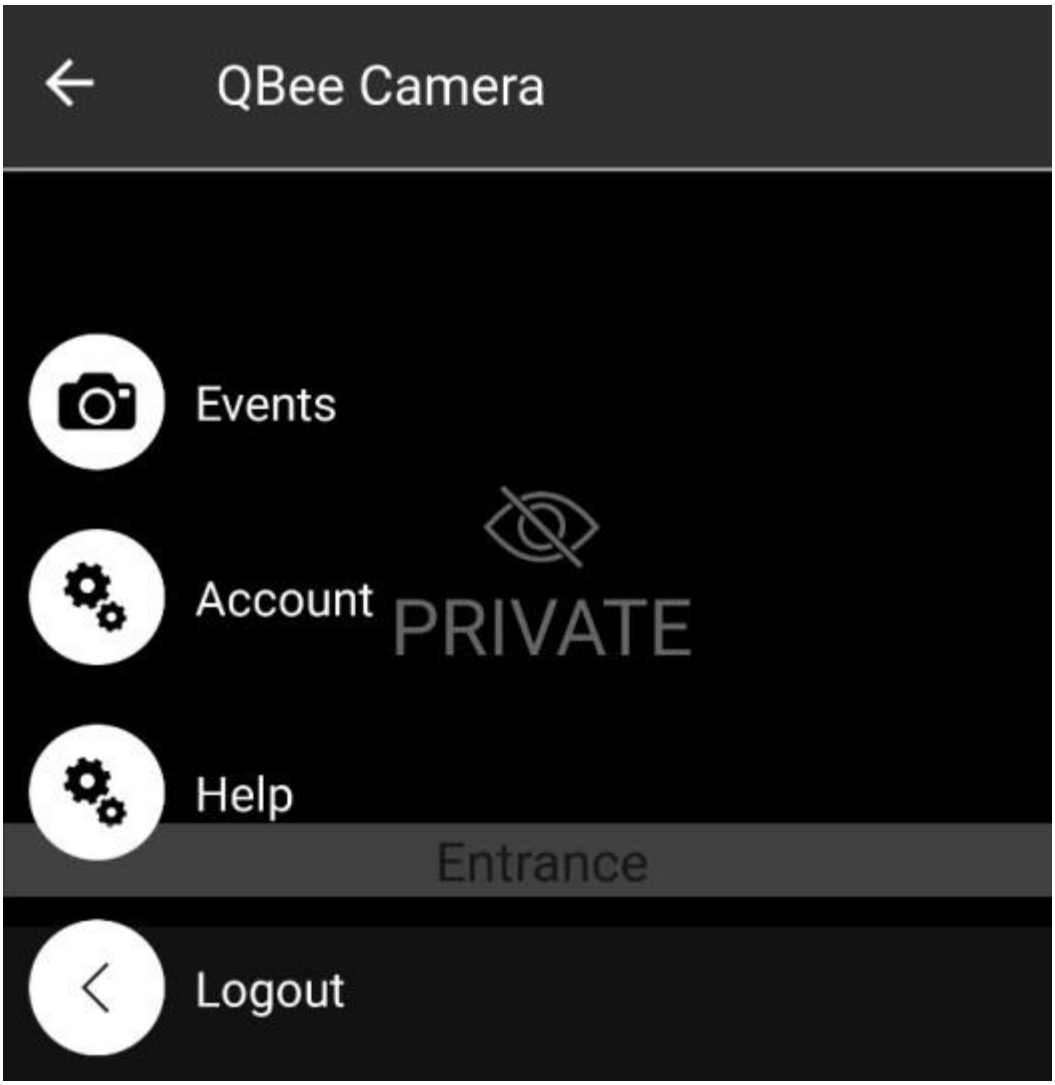
How was the QBee camera disabled?

In the network traffic I found that the qbee camera was sending important information (session id, cookies) in plain text. Anyone that's on the same network can intercept these packets and hijack the

session of the camera, giving him control over it. I found the corresponding CVE of the camera on the internet.

https://blog.francescoservida.ch/2018/09/16/cve-2018-16225-public-disclosure-qbee-camera-vulnerability/

A big clue that makes me think a hacker used this vulnerability is that I found a picture(recent/images) in J Pinkman's phone of the Qbee camera in "private" mode. This is the strongest clue that tells me how the camera was disabled.



Timeline

I have compiled the most useful information using Device and Cloud level analysis about the raid in a timeline. This is the timeline for the day, the raid happened.

2018-05-17 at 10:22:22 iSmartAlarm alarm mode is changed into ARM by J. Pinkman

2018-05-17 at 10:22:23 The Boss change be out home.

2018-05-17 at10:22:30 iSmartAlarm alarm mode is changed into DISARM by The Boss

2018-05-17 at 10:34:15 Door is closed.

2018-05-17 at 10:34:17 iSmartAlarm alarm mode is changed into HOME by The Boss

2018-05-17 at 10:34:31 iSmartAlarm alarm mode is changed into DISARM by pandadodu.

2018-05-17 at 10:34:36 Door is open, all the sirens went off.

2018-05-17 at 10:36:06 Kitchen Nest Protect smoke detector detected smoke.

2018-05-17 at10:37:52 iSmartAlarm alarm mode is changed into DISARM by pandadodu.

From the timeline we can conclude that J Pinkman was not in the lab when it was opened by D Pandama (pandadodu). The alarm was disabled by him and shortly after the smoke detector went off because of the fire set in the lab. From this we can conclude that D Pandama was involved in the raid.

Approach

My first objective was to open every single image file. There were different types of files that could be opened only with specific tools. I started with the biggest file in size – Jessie Pinkman's phone because it was the largest source of information judging by its size. I tried opening it with volatility because it was recommended by my teachers but unfortunately that didn't work. The app was crashing as soon as I started it. I looked for a program that can substitute volatility in google and found autopsy 4.2.0. Once I opened the Samsung image I tried opening the Ismart alarm images. I could do it Windows, so I tried it in Linux. I used binwalk to extract the archived files and then used ranger to be able to browse trough the contents of the folders. The database files were very easy to open and examine since I only had to view them with DB Browser (SQLite). After I gathered enough information from all sources I started piecing it together. There were a lot of screenshots and pictures in the Samsung dump that helped me understand the layout of the security systems in the drug lab. In the end the databases from wink hub and amazon echo were the biggest clues since they give information who opened the lab and when.