DFRWS IoT Forensic Challenge

(2018 - 2019)

Authors

Myungseo Park, Soram Kim, Eunhu Park, Giyoon Kim, Uk Hur, Sehoon Lee, Jongsung Kim

Digital Forensic and Cryptanalysis (DF&C) Laboratory
Kookmin University
http://dfnc.kookmin.ac.kr

<Contents>

<Figure>

<Table>

I. DFRWS Challenge Overview

1. 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 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(Fig. 1). 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 the 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.

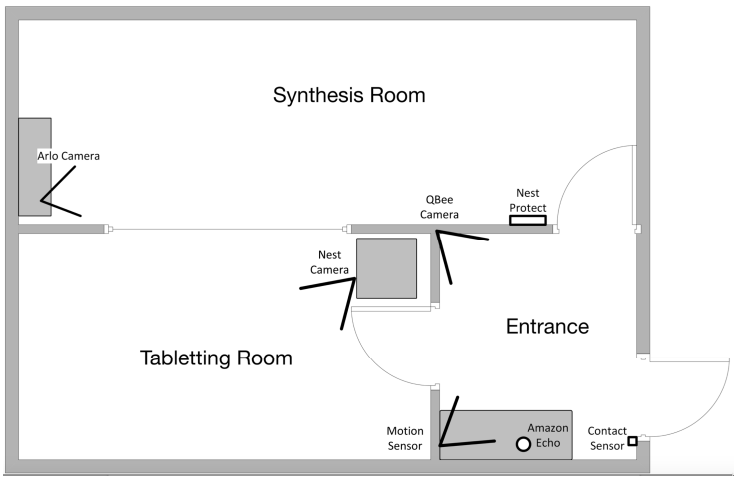

Fig. 1. Diagram of The Illegal Drug Lab.

2. Challenge Dataset

Given data for challenge is as follows:

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

o iSmartAlarm – Diagnostic logs
- File/Folder: ismartalarm/diagnostics/2018-05-17T10_54_28/server_stream
- SHA256: 8033ba6d37ad7f8ba22587ae560c04dba703962ed16ede8c36a55c9553913736

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

o Arlo – Memory image
- File/Folder: arlo/dfrws_arlo.img
- SHA256: 3b957a90a57e5e4485aa78d79c9a04270a2ae93f503165c2a0204de918d7ac70

o Arlo – NVRAM settings
- File/Folder: arlo/nvram.log
- SHA256: f5d680d354a261576dc8601047899b5173dbbad374a868a20b97fbd963dca798

o Arlo – NAND: TAR archive of the folder /tmp/media/nand
- File/Folder: arlo/arlo_nand.tar.gz
- SHA256: 857455859086cd6face6115e72cb1c63d2befe11db92beec52d1f70618c5e421

o Wink Hub – Filesystem TAR archive
- File/Folder: wink/wink.tar.gz
- SHA256: 083e7428dc1d0ca335bbcfc11c6263720ab8145ffc637954a7733afc7b23e8c6

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

o Network capture
- File/Folder: network/dfrws_police.pcap
- SHA256: 1837ee390e060079fab1e17cafff88a1837610ef951153ddcb7cd85ad478228e

3. Challenge Questions

o At what time was the illegal drug lab raided?

o 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?

o How was the QBee camera disabled?

II. Conclusion of Challenge

1. Basic Information

o Analysis Environment

Table 1 Data Analysis Tools

Data	Tool	
Smartphone	Autopsy 4.4.0	
iSmartAlarm	Binwalk 2.1.2	Strings 2.30
Arlo	Binwalk 2.1.2, Volatility 2.6 ReKall 1.7.1	Autopsy 4.4.0 firmware-mod-kit 0.99
Wink Hub	-	
Amazon Echo	-	
Network capture	Wireshark 2.6.3	
Common	010 Editor v6.0.3 Dcode v4.02a	SQlite Expert Personal 3.5.92.2512 Notepad++ v7.5.4

o MAC Address of Devices

Table 2 MAC Address of Devices

Device	MAC Address
Smartphone (Bluetooth)	D8:C4:E9:7C:2E:F8
Smartphone(Wi-Fi)	AC:5F:3E:73:E3:78
Nest Camera	18:B4:30:61:C9:EF
iSmartAlarm	b8:27:eb:5b:6e:10
QBee camera	D8:FB:5E:E1:01:92
Arlo Base Station	08:02:8E:FF:75:4F
Nest Protect	18:B4:30:99:9F:85
Wink Hub	B4:79:A7:25:02:FA
Amazon Alexa	74:75:48:94:23:24

o Network SSID and PSK

```
network={
    priority=0
    scan_ssid=1
    ssid="ESC-IoT"
    psk="esc_iot_2018"
}
```

Fig. 2 Wi-Fi Setting Information

2. Answer to Challenge Question

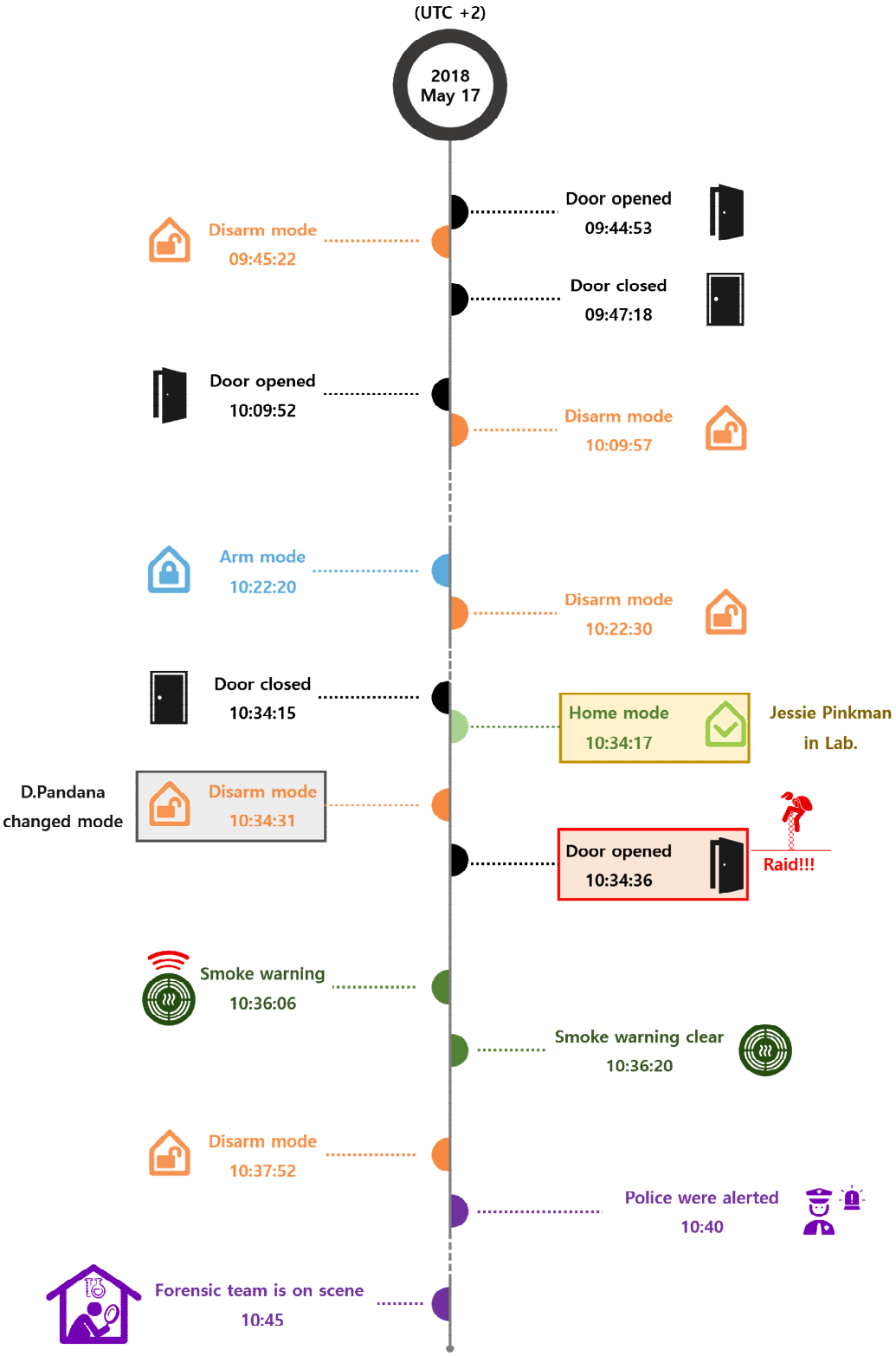

Fig. 3 Timeline on 2018-05-17

Events occurred on 2018-05-17. Fig. 3, a timeline of events, shows events from 10:34 to 10:45 on the day of the crime in chronological order. We used the given data to find out when each event occurred, and the sources for the events are shown in Table 3 below.

Table 3 Timeline and Source of Events

No.	Time (UTC +2)	Event	Source
1	09:44:53 a.m.	Door opened	iSmartAlarm
2	09:45:22 a.m.	Set Disarm mode by The boss(Remote Tag)	iSmartAlarm
3	09:47:18 a.m.	Door closed	iSmartAlarm
4	10:09:52 a.m.	Door opened	iSmartAlarm
5	10:09:57 a.m.	Set Disarm mode by The boss(Remote Tag)	iSmartAlarm
6	10:22:18 a.m.	Set Arm mode by Alexa	Alexa
7	10:22:30 a.m.	Set Disarm mode by The boss(Remote Tag)	iSmartAlarm
8	10:34:15 a.m.	Door closed	iSmartAlarm
9	10:34:17 a.m.	Set Home mode by The boss(Remote Tag)	iSmartAlarm
10	10:34:31 a.m.	Set Disarm mode by D. Pandana	iSmartAlarm
11	10:34:36 a.m.	Door opened	iSmartAlarm
12	10:36:06 a.m.	Smoke warning	NestProtect
13	10:36:20 a.m.	Smoke warning clear	NestProtect
14	10:37:52 a.m.	Set Disarm mode by D. Pandana	iSmartAlarm
15	10:40 a.m.	The police were alerted	Scenario
16	10:45 a.m.	Forensic team is on scene	Scenario

o Source file of No. 6
  - (2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/VOICE/
  - cift_amazon_alexa.db
o Source file of No. 12, 13
  - /USERDATA/data/com.nest.android/cache/cache/cache-1332523362.json(Smartphone)
o Source file of rest event except No. 6, 12, 13, 15, 16
  - /USERDATA/data/iSA.common/databases/iSmartAlarm.DB (Smartphone)
  - Server_stream (iSmartAlarm)

2.1 Summary Answers

Q. At what time was the illegal drug lab raided?
A. 2018/05/17, 10:34:36 a.m. (UTC +2)

Q. Could any of the two friends of Jessie Pinkman have been involved in the raid?
A. Yes, most likely D. Pandana, because he set the control mode of the iSmartAlarm to 'Disarm' mode.

Q. How was the QBee camera disabled?
A. QBee has a known network vulnerability. We have confirmed that the QBee camera in the scenario is a vulnerable version, and we suspect that someone used this vulnerability to disable the camera.

2.2 Details of the Answer

2.2.1 Time That The Illegal Drug lab Was Raided & Who Was Involved In The Raid?

Table 4 shows the key events that were revealed through the iSmartAlarm database analysis on a smartphone. The door was closed at 10:34:15, and the control mode of the iSmartAlarm was set to 'Home' mode by Remote Tag at 10:34:17. This means that Jessie Pinkman was probably in a laboratory at that time.

After that, D. Pandana set the control mode to 'Disarm' mode and immediately opened the door. Therefore, we assume that D. Pandana first set the control mode to 'Disarm' mode to prevent alarms from being triggered by an illegal intrusion. Thus we suspect that D. Pandana participated in the crime.

Table 4 Key Event Summary

Time (UTC +2)	Event	Operator	Sensor
10:34:15 a.m.	Door closed	-	Contact sensor
10:34:17 a.m.	Set 'Home' mode	TheBoss (Remote Tag)	-
10:34:31 a.m.	Set 'Disarm' mode	pandadodu	-
10:34:36 a.m.	Door opened	-	Contact sensor

2.2.2 How Was the QBee Cameras Disabled?

The QBee camera (version 4.16.4) has a vulnerability in that it accepts unencrypted network traffic from clients (such as the QBee Camera application through 1.0.5 for Android and the Swisscom Home application up to 10.7.2 for Android), which results in

an attacker being able to reuse cookies to bypass authentication and disable the camera (CVE-2018-16225)[1].

The QBee camera in the laboratory is version 4.16.4(Fig. 4).

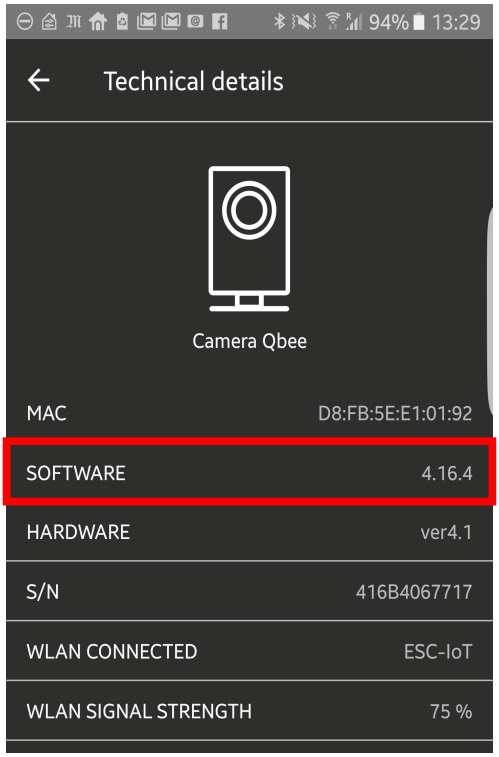

Fig. 4 QBee Camera Software Version

We checked the Network capture file to find that cookie is unencrypted(Fig. 5).

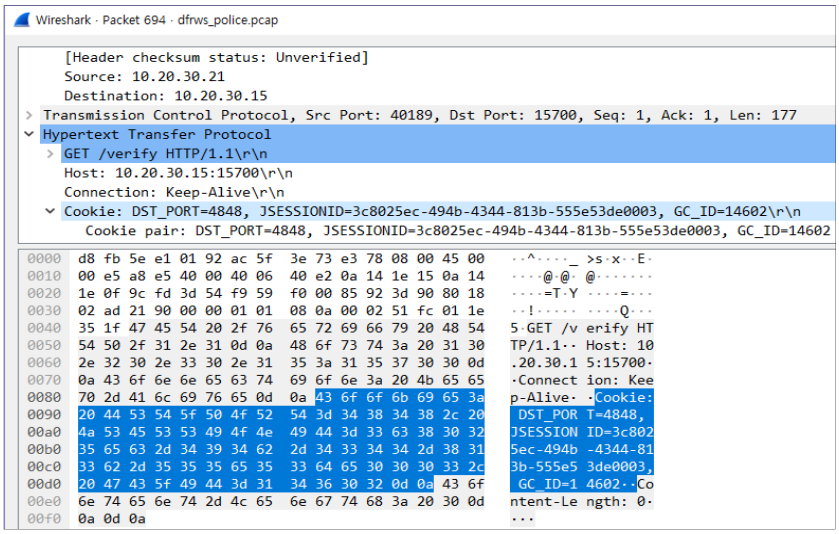

Fig. 5 QBee Camera Network Packet

1) https://nvd.nist.gov/vuln/detail/CVE-2018-16225

So the attacker used that vulnerability to disable the QBee camera. It is possible to enable the privacy mode, so that Live image and all other camera functions are not available through the Swisscom Home app, as well as disabling the functionality of the physical button to toggle the privacy mode. We also found a thumbnail file in the smartphone that indicates that the QBee camera was changed to private mode on 2018-05-17 (Fig. 6).

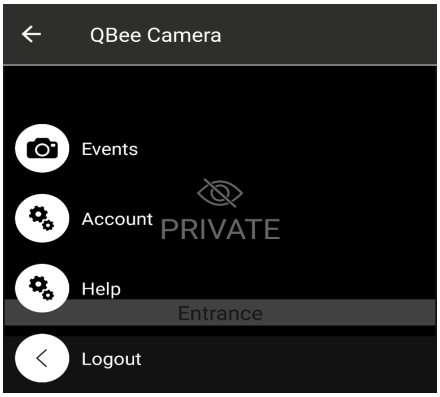

Fig. 6. Thumbnail of QBee Camera

III. Data Analysis

1. Jessie Pinkman's Galaxy S6 edge

1.1 Introduction

The physical image of the Samsung Galaxy device includes many partitions such as SYSTEM, BOOT, RECOVERY, and USERDATA. Most of the data associated with this incident were found in a USERDATA partition that contained user-installed applications and data.

The time zone of the smartphone is set to Europe/Zurich (UTC+2 due to summer time) and found on the following path:

o Time zone: USERDATA/property/persist.sys.timezone (Fig. 7)

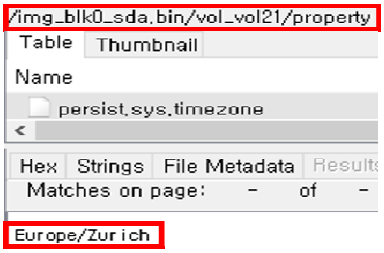

Fig. 7 A Time Zone of The Smartphone

Details of the device name, model, Google account, and other information for the smartphone are shown in Table 5.

Table 5 Details of Smartphone Device

Device Information	Contents
Device Name	Galaxy S6 edge
Model	SM-G925F
OS Version	Android 6.0.1
Phone Number	(+41)0792245315
Google Account	jpinkman2018@gmail.com
Wi-Fi MAC address	AC:5F:3E:73:E3:78
Bluetooth MAC address	D8:C4:E9:7C:2E:F8
Time-zone	Europe/Zurich (UTC+2)

1.2 Challenge Data

Application data for each IoT device can be found on a smartphone. The path where the application data of each IoT device is stored is as follows:

Table 6 IoT Application Data Path

Device Name	Path
Arlo	USERDATA/data/com.netgear.android
Amazon Echo	USERDATA/data/com.amazon.dee.app
Wink Hub	USERDATA/data/com.quirky.android.wink.wink
Nest Protect/Camera	USERDATA/data/com.nest.android
iSmartAlarm	USERDATA/data/iSA.common
QBee Camera	USERDATA/data/com.vestiacom.qbeecamera

The smartphone contains information about the various IoT devices used by Jessie Pinkman. In particular, we found a picture of the IoT device in the camera folder and the screenshot folder. Fig. 8 is a photograph including the information about the IoT device in the *USERDATA/media/0/DCIM/camera*.


20180410_091924.jpg


20180410_092015.jpg


20180410_092029.jpg


20180410_092059.jpg


20180410_092120.jpg


20180410_114908.jpg


20180425_181209.jpg

Fig. 8 Photos with Information about IoT Devices

We identified the MAC address or serial number included in the picture for the IoT device (Table 7).

Table 7 MAC Address or Serial Number of IoT Device

Device Name	File Name	MAC Address or Serial Number
Arlo Base Station	USERDATA/media/0/DCIM/camera/20180326_164922	MAC : 08:02:8E:FF:75:4F
Wink Hub	USERDATA/media/0/DCIM/camera/20180410_091838	MAC : B4:79:A7:25:02:FA
Nest Protect	USERDATA/media/0/DCIM/camera/20180410_091924	S/N : 06CA01AC331600CA
iSmartAlarm PIR3G Motion Sensor	USERDATA/media/0/DCIM/camera/20180410_092059	S/N : 141605015143012
iSmartAlarm iPU3G CubeOne™	USERDATA/media/0/DCIM/camera/20180410_092015	MAC : 00:4D:32:09:D9:E4
Nest Cam	USERDATA/media/0/DCIM/camera/20180410_092120	MAC : 18:B4:30:61:C9:EF
QBee Camera	USERDATA/media/0/DCIM/ScreenShots/ScreenShot_20180502-132904	MAC : D8:FB:5E:E1:01:92 S/N : 416B4067717

In addition to information about the IoT devices, there were pictures that seemed to reflect attempts to debug the Arlo base station and the iSmartAlarm CubeOne™.

1.2.1 Web Browser

In the path *USERDATA/data/com.android.chrome*, we found data from the Chrome browser, such as web page history, login data, and the cookies stored in database files. Most of the web page visits were to the home pages of IoT device manufacturers. A suspicious point is that Jessie Pinkman visited the IP address of a URL named WiFi Pineapple. WiFi Pineapple is a hacking tool for scanning Wi-Fi packets. The port on the address matches port 1471, which is the default port of the actual product. Table 8 is a list of sites in order of numbers of visits.

Table 8 Web Browser History

URL	Title	Visit Time (UTC +2)	Visit Count
https://inbox.google.com/	Inbox - jpinkman2018@gmail.com	2018-05-15 AM 10:34:44	11
https://inbox.google.com/?pli=1	Inbox - jpinkman2018@gmail.com	2018-03-27 AM 10:34:47	10
http://172.16.42.1:1471/	WiFi Pineapple	2018-04-17 AM 11:33:04	5
http://nest.com/	Nest | Crea una casa connessa	2018-05-09 PM 2:29:22	5
https://arlo.netgear.com/	Arlo Smart Home Security Cameras | Home Monitoring | Arlo by NETGEAR	2018-05-09 PM 2:33:42	5
https://mail.google.com/mail/	Inbox - jpinkman2018@gmail.com	2018-05-15 AM 10:34:44	5
https://store.nest.com/ch/fr/account/subscriptions/3a592060-26d1-11e8-83b6-0e2d565eed46	Nest Store	2018-04-17 PM 2:16:24	5
http://10.20.30.1/	Pi-Pinapple	2018-05-15 AM 11:16:01	4
http://10.20.30.1/accounts/login/?next=/	Pi-Pinapple	2018-05-15 AM 11:16:01	4
http://alexa.amazon.com/	Amazon Alexa	2018-05-15 AM 10:32:48	4
http://nest.com/it/	Nest | Crea una casa connessa	2018-05-09 PM 2:29:22	4
https://nest.com/	Nest | Crea una casa connessa	2018-05-09 PM 2:29:22	4
http://alexa.amazon.com/spa/index.html	Amazon Alexa	2018-03-27 AM 10:31:59	3
http://gmail.com/	Inbox - jpinkman2018@gmail.com	2018-05-15 AM 10:34:44	3
https://gmail.com/	Inbox - jpinkman2018@gmail.com	2018-05-15 AM 10:34:44	3
https://www.google.com/gmail/	Inbox - jpinkman2018@gmail.com	2018-05-15 AM 10:34:44	3

1.2.2 Recovery Log

After analyzing the image files, we could not identify basic data such as contacts, messages, and the call log data. Instead, we found Telegram, Snapchat, and WhatsApp messenger data. However, even though there were media files in the Messenger data folder, chat data did not exist. The IoT device, only had log data from about three days before the incident. As a result, we suspected that someone had intentionally removed data related to the incident. To determine the cause of the deletion, we analyzed the file *last_log* in the folder TWRP (Team Win Recovery Project)[2], which is a custom recovery mode. In the log data, we found that there was a trace of the USERDATA partition erase command, except for the media path, as shown in Fig. 9.

```
Running Recovery Commands
I:command is: 'wipe'
I:value is: 'data'
Wiping data without wiping /data/media ...
I:skipped '/data/lost+found'
I:skipped '/data/media'
I:Unable to unlink '/data/system/gps/.lhd.lock'
I:Unable to unlink '/data/system/gps/.gpsd.lock'
I:Unable to unlink '/data/system/gps/.gps.interface.pipe.to_gpsd'
I:Unable to unlink '/data/system/gps/.flp.interface.pipe.to_gpsd'
I:Unable to unlink '/data/system/gps/.pipe.gpsd_to_lhd.to_server'
I:Unable to unlink '/data/system/gps/.pipe.gpsd_to_lhd.to_client'
I:Unable to unlink '/data/system/gps/.gps.interface.pipe.to_jni'
I:Unable to unlink '/data/system/gps/lto2.dat'
I:Unable to unlink '/data/system/gps/ltoStatus.txt'
I:Unable to unlink '/data/system/gps/gldata.sto'
I:Unable to unlink '/data/system/gps/alt.dat'
I:Unable to unlink '/data/system/procstats/state-2018-05-15-10-28-06.bin'
I:Unable to unlink '/data/system/procstats/state-2018-05-08-21-00-54.bin'
I:Unable to unlink '/data/system/procstats/state-2018-05-09-00-00-56.bin'
I:Unable to unlink '/data/system/procstats/state-2018-05-09-03-13-49.bin'
I:Unable to unlink '/data/system/procstats/state-2018-05-09-06-22-46.bin'
I:Unable to unlink '/data/system/procstats/state-2018-05-09-09-31-01.bin'
I:Unable to unlink '/data/system/procstats/state-2018-05-09-12-32-51.bin'
I:Unable to unlink '/data/system/procstats/state-2018-05-09-14-02-23.bin'
I:Unable to unlink '/data/system/procstats/state-2018-05-14-11-02-16.bin'
```

Fig. 9 Deletion Traces in Log Data

The log file contains the path and names of the files that were removed from the USERDATA partition. Also, the file *USERDATA/system/procstats/state-YYYY-MM-DD¯hh¯mm-ss.bin* with time information still existed until 2018-05-15. This observation indicates that data wiping occurred after 2018-5-15.

1.2.3 Nest IoT Device Data

We analyzed the data in the *USERDATA/data/com.nest.android* path of the Nest application in smartphone. The registered devices are 'Nest Cam Indoor' and 'Nest Protect'. However, in the case of the Nest Cam Indoor, all of the data is stored in the Cloud, so no data is left in memory. Three photos were found in the cache, but they were created at times not related to the incident. We describe the results of data

2) **https://twrp.me/**

analysis of Nest Protect in this section. Nest Protect works in four modes according to the air conditions and ambient light. Normally, it operates in safe mode which is a green circle, and it operates in early warning mode, represented by a yellow circle, when some smoke is detected. Emergency mode is activated with an alarm when dangerous smoke or carbon monoxide is detected. When the light is turned off, it emits white light and operates as a pathlight. Fig. 10 shows the four modes of Nest Protect.

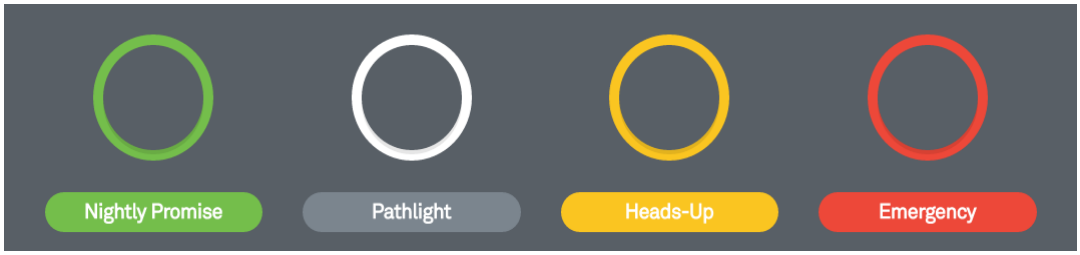

Fig. 10 Four modes of Nest Protect

Nest Protect's specification is as follows (Table 9).

Table 9 Wink Hub Specification

Feature	Summary
Power	230V Connector Three long-life AA Energizer® Ultimate Lithium backup batteries
Features	Voice alarms with custom location Split-Spectrum Sensor Detects carbon monoxide Up to 10-year product lifetime Heads-Up alerts Sound Check Nightly Promise Pathlight Steam Check Self Test Wireless Interconnect Emergency Shut-Off with Nest Learning Thermostat Emergency clip record with Nest Cam Home Report
Nest App Feature	Smoke, Carbon monoxide, Low battery, Sensor failure, App Silence, Safety Check-up, Safety history, What to Do

Sensors	Split-Spectrum Sensor, 450nm and 880 nm wavelength 10-year electrochemical carbon monoxide sensor Heat sensor, ±1°C (±1.8°F) Humidity sensor, ±3%RH Occupancy sensor, 120° field of view to 6 metres (20 feet) Ambient light sensor, 1-100k Lux Dynamic Range
Speaker, siren and light ring	2-watt speaker Siren: 85 dB at 3 metres RGB colour ring with 6 LEDs
Wireless	Working Wi-Fi connection: 802.11b/g/n @ 2.4 GHz Wireless Interconnect: 802.15.4 @ 2.4 GHz Bluetooth Low Energy (BLE)

The operational data of Nest Protect was in *USERDATA/data/com.nest.android/cache/cache/cache-1332523362.json*. In this file, we could check the contents of the app message. Here, we were able to find a smoke_warn message at 10:36 on 17 May. The contents of message are shown in Table 10.

Table 10 Nest Protect Message list

Date	Time (UTC+2)	Message	Location
2018-03-16	12:08:45	protect_power_out_now	Basement, SKYLAB
2018-03-16	14:24:18	protect_power_out_now	Basement, SKYLAB
2018-04-09	09:38:23	protect_power_out_now	Kitchen, LabSmoker, SuperLab
2018-04-27	13:12:16	protect_power_out_now	Kitchen, LabSmoker, SuperLab
2018-04-27	15:59:06	protect_power_out_now	Kitchen, LabSmoker, SuperLab
2018-04-29	10:50:51	protect_power_out_now	Kitchen, LabSmoker, SuperLab
2018-05-02	07:36:45	protect_power_out_now	Kitchen, LabSmoker, SuperLab
2018-05-17	10:36:06	protect_smoke_warn	Kitchen, LabSmoker, SuperLab
2018-05-17	10:36:20	protect_smoke_warn_clear	Kitchen, LabSmoker, SuperLab

We found motion log data in addition to the message contents. The meaning of each log type was confirmed from the source code of the application (Table 11).

Table 11 Type Meaning

Type	Type Meaning	Type	Meaning
0000	INSTALLED	0310	US_FAILURE
0001	MANUALTEST_COMPLETE	0311	PIR_FAILURE
0101	PATHLIGHT	0401	SMOKE_CLEAR
0102	PROMISE	0402	SMOKE_HUSHED
0103	CHECK_IN	0403	SMOKE_HEADS_UP
0201	POWER_OUTAGE	0404	SMOKE_EMERGENCY
0203	DATA_MISSING	0501	CO_CLEAR
0300	BATTERY_OK	0502	CO_HUSHED
0301	BATTERY_LOW	0503	CO_HEADS_UP
0302	BATTERY_NEAR_CRITICAL	0504	CO_EMERGENCY
0303	BATTERY_CRITICAL	0701	STEAM_DETECTED
0304	PRODUCT_EXPIRED	0800	SOUNDCHECK_COMPLETE
0305	SMOKE_SENSOR_FAILURE	0801	SOUNDCHECK_SPEAKER_OK
0306	CO_SENSOR_FAILURE	0802	SOUNDCHECK_SPEAKER_FAILURE
0307	LED_SENSOR_FAILURE	0803	SOUNDCHECK_BUZZER_OK
0308	TEMP_SENSOR_FAILURE	0804	SOUNDCHECK_BUZZER_FAILURE
0309	ALS_FAILURE		

The logs from 7 May, and from 15 May to 17 May are shown in the table below (Table 12).

Table 12 Nest Protect Log

Date	Time (UTC +2)	Type	Type meaning
2018-05-15	03:50:34	0103	CHECK_IN
2018-05-15	07:50:35	0103	CHECK_IN
2018-05-15	11:39:28	0102	PROMISE
2018-05-15	11:50:41	0103	CHECK_IN
2018-05-15	15:15:58	0102	PROMISE
2018-05-15	16:20:38	0103	CHECK_IN
2018-05-15	20:20:40	0103	CHECK_IN
2018-05-16	00:20:40	0103	CHECK_IN
2018-05-16	04:20:42	0103	CHECK_IN
2018-05-16	08:20:43	0103	CHECK_IN

2018-05-16	12:20:44	0103	CHECK_IN
2018-05-16	15:38:52	0001	MANUALTEST_COMPLETE
2018-05-16	15:41:12	0001	MANUALTEST_COMPLETE
2018-05-16	15:52:30	0102	PROMISE
2018-05-16	16:20:46	0103	CHECK_IN
2018-05-16	20:20:46	0103	CHECK_IN
2018-05-17	00:20:48	0103	CHECK_IN
2018-05-17	04:20:49	0103	CHECK_IN
2018-05-17	08:20:50	0103	CHECK_IN
2018-05-17	09:48:05	0102	PROMISE
2018-05-17	10:35:55	0403	SMOKE_HEADS_UP
2018-05-17	10:36:11	0401	SMOKE_CLEAR
2018-05-17	11:41:32	0102	PROMISE
2018-05-17	12:14:23	0102	PROMISE
2018-05-17	12:20:51	0103	CHECK_IN

As shown in the table, the log data also showed a 'SMOKE_HEADS_UP' log at 10:35. The most frequent 'CHECK_IN' logs remained at four hour intervals. The 'PROMISE' log was compared with the contact sensor log of the iSmartAlarm described later and remained a little after the door was closed. Therefore, 'PROMISE' is presumed to be the nightly promise function of Nest Protect, and it seems that the laboratory light was turned off at the time.

1.2.4 QBee

QBee cameras are known to have several vulnerabilities. We have experimented directly with the vulnerability 'CVE-2018-16223'[3], which pertains to the unsecured cryptographic storage of credentials in the QBee camera application. Although QBee camera credentials are encrypted, the encrypted settings are in a format that suggests the use of the generic 'Secure Preferences' library. The next path is one of the paths to the encrypted setting files (Fig. 11). We exploited this vulnerability to decrypt this file.

- USERDATA/data/com.vestiacom.qbeecamera/shared_prefs/com.vestiacom.qbeecamera_preference.xml

3) https://nvd.nist.gov/vuln/detail/CVE-2018-16223

```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="1cESV/QGYZet+LPyrEYC2w">K+B43s/a2fvA5KWoNqLk9A</string>
    <string name="MaItDJveNCVLomdw+J68OsQkEYk/CMUp5qmpa6LMdcw">371blr2jkj9tqloocc360tvujc</string>
    <string name="CV4VN6f609h1Rc+6e4febA">2vyyEswEiwgmDz9OkcAvhA</string>
</map>
```

Fig. 11 com.vestiacom.qbeecamera_preference.xml

In Fig. 11, the key and value pairs are shown in a green square, in which the value is black and the key is purple. To get the encryption key, we first find a value with a length of 26, '371blr2jkj9tqloo360tvujc' in this file and divide it into two equal parts. We name the values Value1 and Value2. We then obtain the cryptographic key through the output obtained by inputting the concatenated values of Value1, Fixed value ("a!k@ES2,g86AX&D8vn2]"), and Value2 in that order (i.e., Value1||Fixed value||Value2) into the hash function SHA256. Here, the fixed value is obtained from the PoC (Proof of concept) code (Fig. 12).

```
key = prefs_key[0:len(prefs_key) // 2]
key += "a!k@ES2,g86AX&D8vn2]"
key += prefs_key[len(prefs_key) // 2:]
print("key: "+key)
# Hash the text to a sha256 fingerprint -> resulting key always 256 bit
key_hash = SHA256.new(data=key.encode('utf-8'))
```

Fig. 12 PoC code of vulnerability in iSmartAlarm

Encrypted data need to be decoded using Base64. The decoded data and the key are used as input parameters into AES-256-ECB. Decrypted data are then obtained. The decryption process is shown in Fig 13.

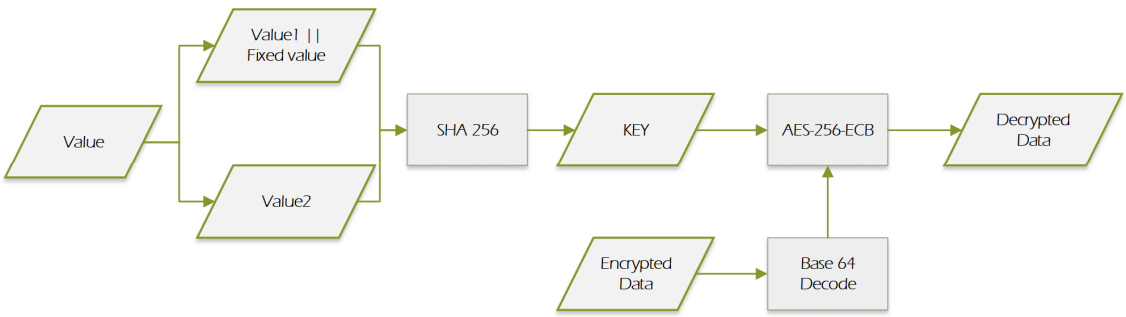

Fig. 13 Decryption Process using the Vulnerability of the QBee Camera

As shown in Fig. 14, decrypted QBee camera setting information was obtained by our own experiments. The user name of the QBee camera is "JPinkman" and the password is "Esc_ioT_2018".

```
"decrypted_settings": [
    {
        "qbeeUser": "JPinkman",
        "qbeePassword": "Esc_iot_2018"
    }
]
```


Fig. 14 Decrypted QBee Settings

2. iSmartAlarm

2.1 Introduction

iSmartAlarm is a self-controlled and self-monitored smart home security system that is controlled by a user's smartphone. The iSmartAlarm smart home system consists of a contact sensor, motion sensor, camera and other devices connected to the CubeOne™.

iSmartAlarm supports the 'Arm', 'Disarm', 'Home' and 'Panic' control modes as shown in Fig. 15. Users can activate all sensors, devices, and cameras in their home using the 'Arm' mode. 'Disarm' mode can disable the system when a user is not concerned about security. 'Home' mode activates all contact sensors but disables motion detectors. Notably, in this scenario, Jessie Pinkman set the control mode of the iSmartAlarm to 'Home' mode in the lab. If intrusion or unauthorized activity is detected in the 'Arm' mode, the control mode is switched to the 'Panic' mode. When in the 'Panic' mode, the system triggers a 110dB siren, sends SMS text messages, pushes notifications, makes automated phone calls, and sends emails to all specified members.

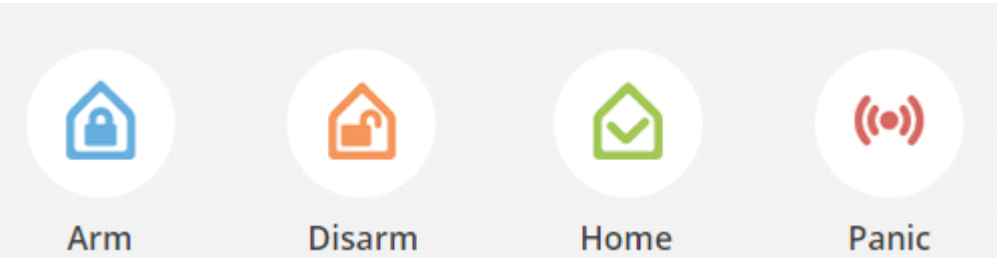

Fig. 15 Control Modes of iSmartAlarm

iSmartAlarm's specification is as follows in Table 13.

Table 13 iSmartAlarm Specification

Feature	Contents
Connection and Expansion	USB port 2.0 10/100 BASE-T Ethernet (RJ-45 connector)
Use with	Products that all iSmartAlarm devices, sensors, and cameras
Dimensions	100mm x 100mm x 105mm

2.2 Data from a Smartphone

2.2.1 Devices connected to iSmartAlarm

We found screen capture images of the iSmartAlarm application on Jessie Pinkman's smartphone (Fig. 16). Fig. 16 shows that the Skylab smart home system consists of "TheBouncer" (= contact sensor), "TheMotion" (= motion sensor), and "TheBoss" (= Remote tags) around "TheCube" (= CubeOne™). Here, the contact sensor is used as a door sensor.

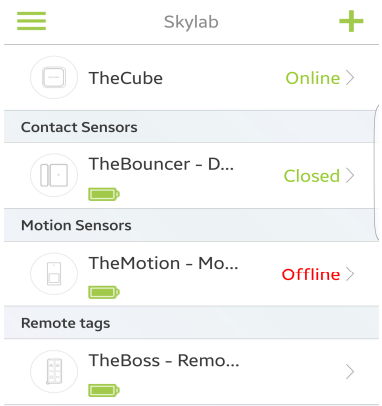

Fig. 16 Capture Image of iSmartAlarm

2.2.2 DB Files

The database of the iSmartAlarm stores information about the behavior of the devices constituting the iSmartAlarm smart home system, and the corresponding database file is located in the following path:

o /data/data/iSA.common/databases/iSmartAlarm.DB

We analyzed the database tables "TB_IPUDairy", "TB_SensorDairy" and "TB_userDairy" and retrieved data including control mode, sensor information and other information for

behavioral analysis. We revealed the acts of the suspect by reconstructing the contents of the three tables.

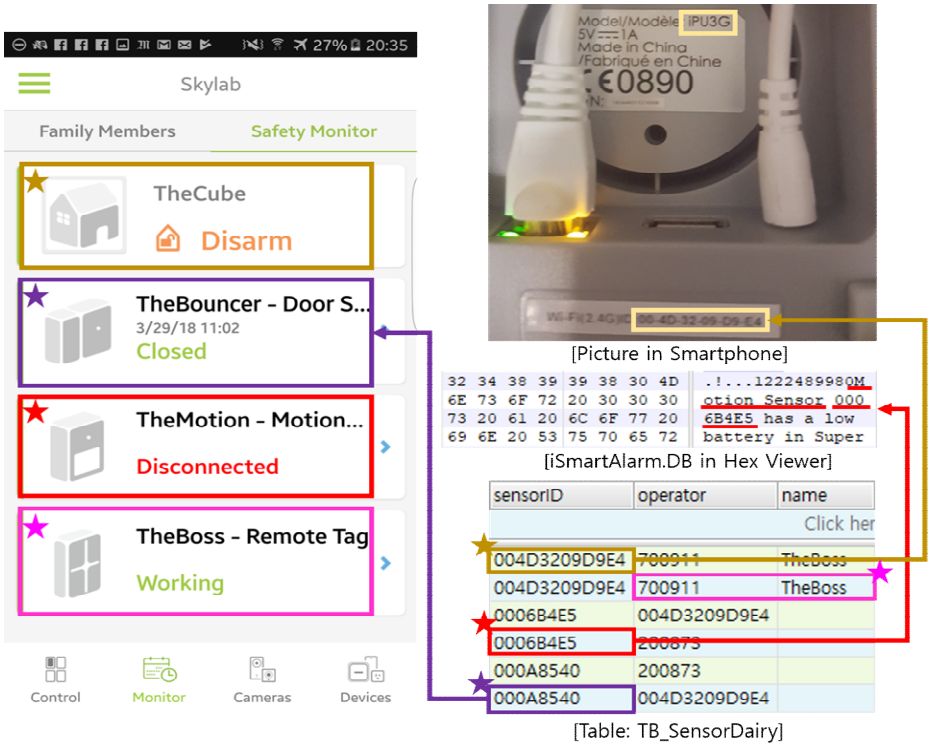

Fig. 17 Identification of sensorID

In TB_SensorDairy, there are many sensorIDs and operators. '004D3209D9E4' matches the MAC address of the picture corresponding to CubeOne™. We found the words 'Motion Sensor 0006B4E5' from iSmartAlarm.DB in the hex viewer. So, '0006B4E5' means motion sensor. Operator '700911' already matched the name 'TheBoss'. Finally, to figure out what '000A8540' was, we compared sensors and operators with device list of the iSmartAlarm app capture from the smartphone. As a result, '000A8540' is a contact sensor. Table 14 summaries the device IDs corresponding to the devices.

Table 14 Device Name & ID

Device	Name	Device ID
CubeOne™	TheCube	004D3209D9E4
Contact Sensor	TheBouncer	000A8540
Motion Sensor	TheMotion	0006B4E5

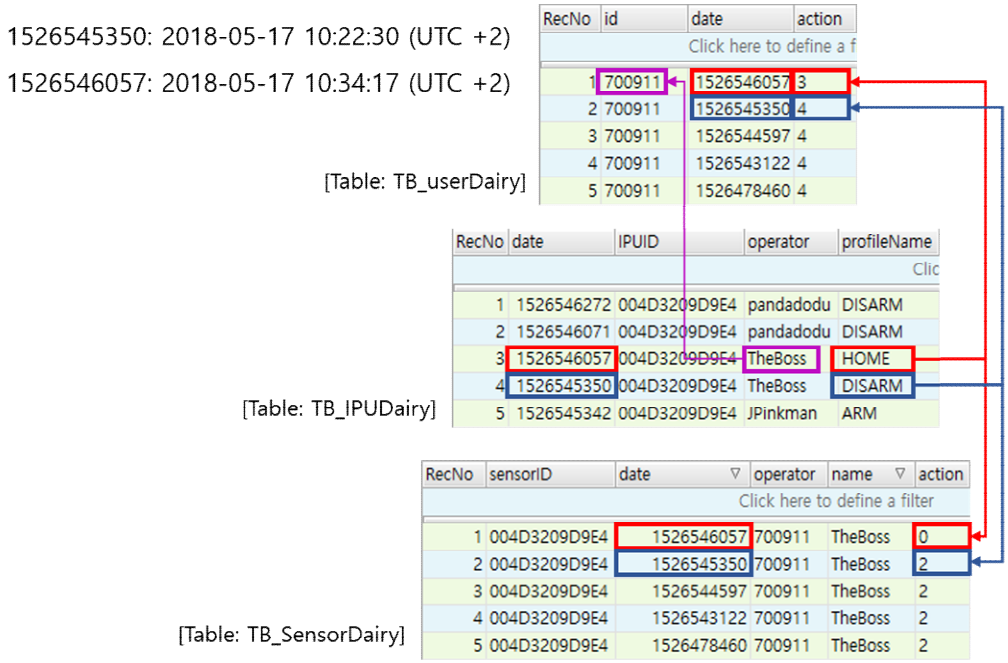

Fig. 18 Identification of Action Meaning

To identify the meanings of these actions, we compared three tables in *iSmartAlarm.DB*. We determined what the action means by comparing values generated at the same time. So actions 3 and 4 in TB_userDairy table mean 'Home' and 'DISARM' respectively. The same goes for TB_SensorDairy table. Identification for all actions except the contact sensor is shown below (Table 15~17).

Table 15 Details of TB_IPUDairy Table

IPU ID : 004D3209D9E4 (CubeOne™)			
Date	Time(UTC +2)	Operator	Mode
2018.5.17	09:45:22	TheBoss	Disarm
	09:47:50	JPinkman	Arm
	10:09:57	TheBoss	Disarm
	10:22:22	JPinkman	Arm
	10:22:30	TheBoss	Disarm
	10:34:17		Home
	10:34:31	Pandadodu	Disarm
	10:34:52		

Table 16 Details of TB_SensorDairy Table (CubeOne™)

Date	Time (UTC +2)	SensorID	Operator	Action Flag	Action meaning
2018.5.17	09:45:22	004D3209D9E4	TheBoss	2	Disarm
	10:09:57	004D3209D9E4	TheBoss	2	Disarm
	10:22:30	004D3209D9E4	TheBoss	2	Disarm
	10:34:17	004D3209D9E4	TheBoss	0	Home
004D3209D9E4: CubeOne™					

Table 17 Action meaning of CubeOne™

Device	Action Flag	Mode
CubeOne™	0	Home
	2	Disarm
	3	Panic
	4	Arm

We used the iSmartAlarm demo, which is produced using sensorlogdata.xml in the iSmartAlarm.apk file, to determine the meaning of the action for the 'contact sensor 000A8540'. Fig. 19 shows how we identified the meaning of the action of the contact sensor. This method is the same as the method of identifying the meaning of action of another device. Tables 18 and 19 show the details of the behavior of the contact sensor and the meanings of the actions.

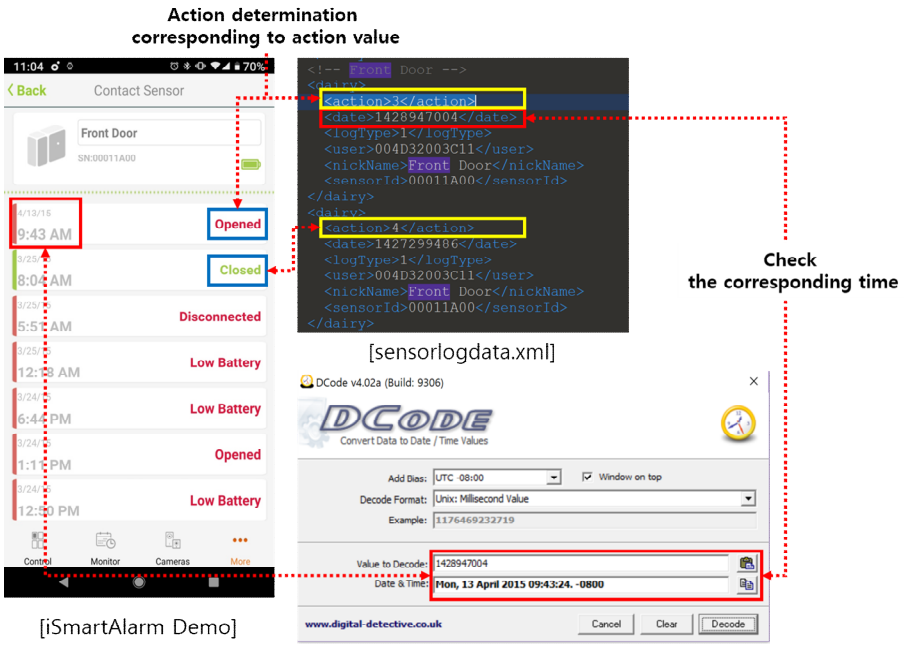

Fig. 19 Identification of Action Meaning (Contact Sensor)

Table 18 Details of TB_SensorDairy Table (Contact Sensor, Motion Sensor)

Date	Time (UTC +2)	Sensor ID	Operator	Action Flag	Action meaning
2018.5.17	09:44:53	000A8540	004D3209D9E4	3	Opened
	09:47:18	000A8540	004D3209D9E4	4	Closed
	10:09:52	000A8540	004D3209D9E4	3	Opened
	10:09:55	0006B4E5	004D3209D9E4	5	Motion Detected
	10:34:15	000A8540	004D3209D9E4	4	Closed
	10:34:36	000A8540	004D3209D9E4	3	Opened
	11:39:50	000A8540	004D3209D9E4	4	Closed
	14:52:10	000A8540	004D3209D9E4	3	Opened
	14:57:06	000A8540	004D3209D9E4	4	Closed
	14:58:03	000A8540	004D3209D9E4	3	Opened
	14:58:15	000A8540	004D3209D9E4	4	Closed
000A8540: Contact Sensor, 0006B4E5: Motion Sensor					

Table 19 Action Meaning of Sensor

Sensor	Action Flag	Mode
Contact Sensor	3	Opened
	4	Closed
Motion Sensor	5	Motion detected

2.3 Challenge Data

2.3.1 Memory dump images

In the given iSmartAlarm data, there are memory dump images named ismart_00.img and ismart_80.img, which appear to be the firmware images of CubeOne™ which constitutes the smart home system. Since the hash values of SHA-256 are the same, the both images can be regarded as identical. We extracted the files from the given memory dump image using binwalk. Table 20 summarizes the results of analyzing the data extracted from the image.

Table 20 Summary of Image Analysis Results

Route	Content
/iSmartAlarm/dump/ismart_00.img/etc_ro/rcS	gateway : 192.168.1.1 ethernet : 192.168.1.68

/iSmartAlarm/dump/ismart_00.img/etc_ro/Wireless/RT2860AP/RT2860_default_vlan	HostName : ralink Login : admin Password : admin0 wan_ip addr : 10.10.10.254 wan_netmask : 255.255.255.0 wan_gateway : 10.10.10.253
/iSmartAlarm/dump/ismart_00.img/etc_ro/Wireless/RT2860AP/RT2860_default_novlan	
/iSmartAlarm/dump/ismart_00.img/sbin/iSmartAlarm.cer	Certificate existence
/sbin/log_pubkey.pem	Public key existence
/sbin/logpubkey.pem	
/usr/share/default_config	ip addr : 192.168.1.68
	subnetmark : 255.255.255.0
	ip gateway : 192.168.1.1
	ip ddns : 202.99.96.68

2.3.2 Diagnostics log

There is Diagnostics log file named ‘server_stream’. It contains the protocol between the server and iSmartAlarm device. We attempted to use Binwalk to identify the format of this file, but did not obtain any useful results. So, we used the string extraction tool, 'Strings', to try to identify meaningful strings in this file. Table 21 summarizes only the relevant information on 2018-05-17, the day of the incident. It shows Sensor ID, Device ID, Alarmdoor[4], SirenOP[5], Message and what mode was used.

Table 21 Diagnostics Log

Time (UTC +2)	Content	
09:44:53	Sensor ID	000A8540
	Contact Sensor	door is open, and send to cloud
	Message	one sensor trigger
09:45:22	Sensor ID	0006B4E5
	Message	- RC3 set IPU to disarm - Disarm, change the LED to white breathe.
09:47:18	Sensor ID	000A8540
	Contact Sensor	door is open, and send to cloud
10:09:57	Sensor ID	000A8540
	Deivce ID	0006B4E5
	Message	- RC3 set IPU to disarm - Disarm, change the LED to white breathe.

4) Alarm for door
5) Siren Operation

10:22:27	Sensor ID	000A9474
	Device ID	0006B4E5
	Message	- RC3 set IPU to disarm - Disarm, change the LED to white breathe.
10:34:15	Sensor ID	000A8540
	Message	- RC3 set IPU to home - Door is closed
10:34:19	Sensor ID	000A9474
	Alarm	- the current alarm sensor is disable in child process.
	Message	Disarm, change the LED to white breathe.
10:34:31	Device ID	004D3209D9E4
	Message	- receive the command to stop all the resend alarm command
10:34:36	Sensor ID	000A8540
	SirenOP	- door is open, all the siren need doorbell!!!
10:37:52	Device ID	004D3209D9E4
	Message	- receive the command to stop all the resend alarm command

3. Arlo Camera

3.1 Introduction

Netgear's Wireless Security Smart Home Camera Arlo system consists of a camera and a base station responsible for data transmission and reception. Users can perform real-time remote monitoring using a smartphone, and if intruders are found, users can set the system to warn or sound alarms.

Table 22 shows the Arlo base station specifications.

Table 22 Arlo Base Station's Specification

Feature	Summary
Interface Port	Fast Ethernet
IP configuration	DHCP
Wireless	2.4 GHz 802.11n
Local Storage	Yes
Siren	Yes
Processor and memory	900MHz ARM Cortex A7 128MB Flash, 128MB RAM
Dimensions	58.6 x 174.5 x 126.5 mm

3.2 Challenge Data

We used data from the Arlo Base Station: Memory image, NVRAM settings and the TAR archive of the folder */tmp/media/nand*. Details of the data analyses are described below.

3.2.1 NVRAM settings.

NVRAM is computer memory that maintains stored information even when not supplied with power. When the computer boots up, the settings in the NVRAM are applied. The values of the settings for the network in the *nvram.log* are shown in Fig. 20

```
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
```

Fig. 20 Contents of nvram.log

3.2.2 /tmp/media/nand Folder

This folder contains the device's log and configuration files in JSON format. A description of the major files is given in Table 23.

Table 23 Description of Major Files in NAND

Path		Description
Directory	File	
~/	eventlog	Event Log with Internet connection, Camera connection, IP&MAC address Check.
	updatelog	Firmware Update Log
~/log-archive	syslog-[number].gz	System Log and Network Log
	xlog-[number].gz	Process Debug Log
~/vzdaemon/conf/	BasestationConfiguration.json	Time zone, Mac address and Token value
	StoragePolicies.json	Storage polices
~/vzdaemon/conf/automation	ActiveAutomations.json	Values of gatewayID, active modes and timestamp
	automation.map	Set type and alarm settings for each mode
	AutomationState.json	Camera audio sensitivity, recording, and alarm settings
~/vzdaemon/conf/camera	59U17B7BB8B46.json	Camera Setting
~/vzdaemon/conf/modes	mode[number].json	Set rules and define type of modes
~/vzdaemon/conf/rules	r_mode[number]_59U17B7BB8B46.json	Action settings based on trigger
* ~ : /tmp/media/nand		

However, no significant data exist because there was no stored log at the estimated time of the crime.

3.2.3 dfrws_arlo.img

This image file is a memory capture of the Arlo base station. Analysis by various tools showed that the file contained NVRAM setting values, network events, certificates and other data. However, no significant data existed.

4. Wink Hub

4.1 Introduction

Wink Hub invented by Wink, allows the connection of diverse smart devices. A user can control them easily, because the vendor provides the “Wink-Smart Home” application (Fig. 21)[6].

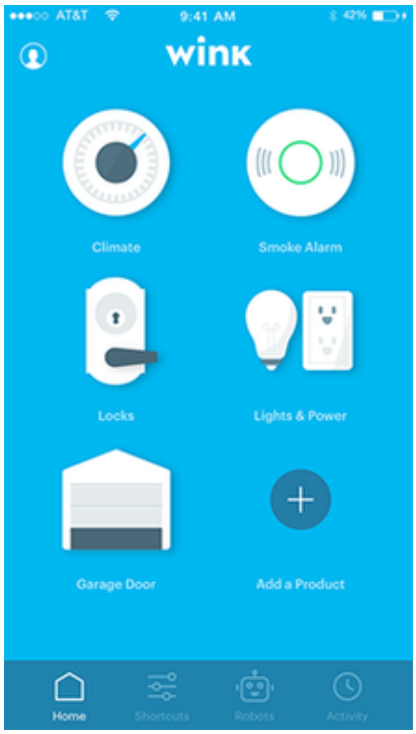

Fig. 21 Wink Hub Application

Wink Hub’s specification is as follows (Table 24).

Table 24 Wink Hub Specification

Feature	Contents
Requirements	Apple® or Android™ smart device. Wi-Fi® network with 2.4 GHz routers running on WPA-PSK, open security, or WEP. (Does not currently support 5 GHz networks)
Supported device types	Z-WAVE®: Door Lock, Door/Window Sensor, Motion Sensor, Tilt Sensor, Light Switch, Light Dimmer, Appliance Module, ZIGBEE®: Light Bulb, Light Switch, Outlet, Door/Window

6) https://www.wink.com/products/wink-hub/

Supported protocols	Bluetooth, Z-Wave® (Security Enabled Z-Wave Plus Device), ZigBee®, Wi-Fi®, Lutron® Clear Connect®, Kidde
Use with	Products that have the "Wink Compatible - Wink Hub Required" seal on packaging
Platform compatibility	Control products from iOS, Apple Watch, Android, and Android Wear. Works with Amazon Alexa. Program recipes with IFTTT.
Dimensions	8" L x 3" W x 8" H

4.2 Challenge Data

Data from Wink Hub is provided as a file system TAR archive. After decompression it produce a Linux directory structure. The FHS (Filesystem Hierarchy Standard)[7] defines the directory structure and contents in the Linux operating system (Table 25).

Table 25 Directory Structure and Contents of Wink Hub

Directory	Description	
/	Primary hierarchy root and root directory of the entire file system hierarchy.	
/bin	Essential command binaries that need to be available in single user mode; for all users, e.g., cat, ls, cp.	
/boot	Boot loader files, e.g., kernels, initrd.	
/dev	Device files, e.g., /dev/null, /dev/disk0, /dev/sda1, /dev/tty, /dev/random.	
/etc	Host-specific system-wide configuration files	
	/etc/opt	Configuration files for add-on packages that are stored in /opt.
	/etc/sgml	Configuration files, such as catalogs, for software that processes SGML.
	/etc/X11	Configuration files for the X Window System, version 11.
	/etc/xml	Configuration files, such as catalogs, for software that processes XML.
/home	Users' home directories, containing saved files, personal settings, etc.	
/lib	Libraries essential for the binaries in /bin and /sbin.	
/lib<qual>	Alternative format essential libraries. Such directories are optional, but if they exist, they have some requirements.	
/media	Mount points for removable media such as CD-ROMs (appeared in FHS-2.3 in 2004).	
/mnt	Temporarily mounted filesystems.	
/opt	Optional application software packages.	
/proc	Virtual filesystem providing process and kernel information as files. In	

7) https://en.wikipedia.org/wiki/Filesystem_Hierarchy_Standard

	Linux, corresponds to a procfs mount. Generally automatically generated and populated by the system, on the fly.	
/root	Home directory for the root user.	
/run	Run-time variable data: Information about the running system since last boot, e.g., currently logged-in users and running daemons. Files under this directory must be either removed or truncated at the beginning of the boot process; but this is not necessary on systems that provide this directory as a temporary filesystem (tmpfs).	
/sbin	Essential system binaries, e.g., fsck, init, route.	
/srv	Site-specific data served by this system, such as data and scripts for web servers, data offered by FTP servers, and repositories for version control systems (appeared in FHS-2.3 in 2004).	
/sys	Contains information about devices, drivers, and some kernel features.	
/tmp	Temporary files (see also /var/tmp). Often not preserved between system reboots, and may be severely size restricted.	
/usr	Secondary hierarchy for read-only user data; contains the majority of (multi-)user utilities and applications.	
	/usr/bin	Non-essential command binaries (not needed in single user mode); for all users.
	/usr/include	Standard include files.
	/usr/lib	Libraries for the binaries in /usr/bin and /usr/sbin.
	/usr/lib<equal>	Alternative format libraries, e.g. /usr/lib32 for 32-bit libraries on a 64-bit machine (optional).
	/usr/local	Tertiary hierarchy for local data, specific to this host. Typically has further subdirectories, e.g., bin, lib, share.
	/usr/sbin	Non-essential system binaries, e.g., daemons for various network-services.
	/usr/share	Architecture-independent (shared) data.
	/usr/src	Source code, e.g., the kernel source code with its header files.
	/usr/X11R6	X Window System, Version 11, Release 6 (up to FHS-2.3, optional).
/var	Variable files—files whose content is expected to continually change during normal operation of the system—such as logs, spool files, and temporary e-mail files.	
	/var/cache	Application cache data. Such data are locally generated as a result of time-consuming I/O or calculation. The application must be able to regenerate or restore the data. The cached files can be deleted without loss of data.

	/var/lib	State information. Persistent data modified by programs as they run, e.g., databases, packaging system metadata, etc.	
	/var/lock	Lock files. Files keeping track of resources currently in use.	
	/var/log	Log files. Various logs.	
	/var/mail	Mailbox files. In some distributions, these files may be located in the deprecated /var/spool/mail.	
	/var/opt	Variable data from add-on packages that are stored in /opt.	
	/var/run	Run-time variable data. This directory contains system information data describing the system since it was booted. In FHS 3.0, /var/run is replaced by /run; a system should either continue to provide a /var/run directory, or provide a symbolic link from /var/run to /run, for backwards compatibility.	
	/var/spool	Spool for tasks waiting to be processed, e.g., print queues and outgoing mail queue.	
		/var/spool/mail	Deprecated location for users' mailboxes.
	/var/tmp	Temporary files to be preserved between reboots.	

Comparing the FHS Directory with the Wink Hub Directory, Wink Hub has all of the same folders except /boot and /srv (Table 26). Additionally, there exists /database, /database_default and /mfgtests folders in Wink Hub. The directories /database, /database_default and /var contain useful data.

Table 26 Comparison Directory Structure

FHS Directory	Wink Hub Directory
/bin	O
/boot	X
/dev	O
/etc	O
/home	O
/lib	O
/lib<qual>	O
/media	O
/mnt	O
/opt	O

/proc	O
/root	O
/run	O
/sbin	O
/srv	X
/sys	O
/tmp	O
/usr	O
/var	O
Additional	/database, /database_default, /mfgtests

Log files, network settings, and DB files were found in Wink Hub (Table 27). Some files are in several places. Useful data are marked in blue at Table 27.

Table 27 Primary File in Wink Hub

File	Route	
bd_addr	/database	/database_default/db_backup
apron.db	/database	/database_default/db_backup
	/database_default	/var/lib/database
apron.db.old	/database	/var/lib/database
	/database_default/db_backup	-
lutron-db.sqlite	/database	/database_default/db_backup
	/database_default	-
wpa_supplicant	/database	/database_default/db_backup
apron-6.db	/run/database	/var/pcmcia/database
	/tmp/database	/var/run/database
	/var/cache/database	/var/spool/database
	/var/log/database	/var/tmp/database
apron-7.db	/run/database	/var/pcmcia/database
	/tmp/database	/var/run/database
	/var/cache/database	/var/spool/database
	/var/log/database	/var/tmp/database
apron-8.db	/run/database	/var/pcmcia/database
	/tmp/database	/var/run/database
	/var/cache/database	/var/spool/database
	/var/log/database	/var/tmp/database
all.log	/run	/var/pcmcia
	/tmp	/var/run
	/var/cache	/var/spool
	/var/log	/var/tmp

all.log.1	/run	/var/pcmcia
	/tmp	/var/run
	/var/cache	/var/spool
	/var/log	/var/tmp
all.log.2	/run	/var/pcmcia
	/tmp	/var/run
	/var/cache	/var/spool
	/var/log	/var/tmp

bt_addr contains the bluetooth MAC address of Wink Hub, that is 00:21:CC:09:B7:B9 (Fig. 22).

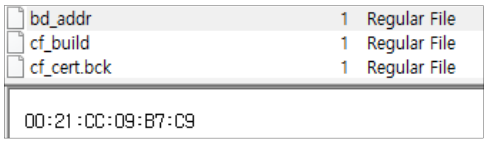

Fig. 22 Bluetooth MAC Address

wpa_supplicant includes Wi-Fi setting information. SSID (Service Set Identifier) is “ESC-IoT” and PSK (Pre-Shared Key) is “esc_iot_2018” (Fig. 23).

```
ctrl_interface=/var/run/wpa_supplicant
update_config=1
ap_scan=1
fast_reauth=1
bgscan=""

network={
    priority=0
    scan_ssid=1
    ssid="ESC-IoT"
    psk="esc_iot_2018"
}
```

Fig. 23 Wi-Fi Setting Information of Wink Hub

all.log and *all.log.** are Wink Hub’s communication log files. Time is recorded as two types (Fig. 24). One is ‘MONTH DAY hh-mm-ss’ and other is the UNIX timestamp type. The former time zone is UTC +0. So we have to +2 at the latter.

```
May 17 08:19:59 flex-dvt user.info monit[1155]: 'ntpd' start on user request
May 17 08:19:59 flex-dvt user.info monit[1155]: Awakened by User defined signal 1
May 17 08:19:59 flex-dvt user.info monit[1155]: monit daemon with PID 1155 awakened
May 17 08:19:59 flex-dvt user.info monit[1155]: 'ntpd' start action done
```

Fig. 24 Wink Hub Log

There are records that “‘ntpd’ start on user request” and “‘ntpd’ start action done”. From this, we can see that some action has taken place. Action records are as follows (Table 28).

Table 28 Action Log

Time (UTC +2)	log
05-17 10:04:36	'ntpd' start action done
05-17 10:09:44	'ntpd' start action done
05-17 10:14:51	'ntpd' start action done
05-17 10:19:59	'ntpd' start action done
05-17 10:25:07	'ntpd' start action done
05-17 10:30:15	'ntpd' start action done
05-17 10:35:22	'ntpd' start action done
05-17 10:40:30	'ntpd' start action done
05-17 10:45:37	'ntpd' start action done
05-17 10:50:45	'ntpd' start action done
05-17 10:55:52	'ntpd' start action done

5. Amazon Echo

5.1 Introduction

Amazon Echo is a smart speaker made by Amazon. It is capable of voice interaction, music playback, alarm settings, weather, and other real-time information. It can also be used as a smart home hub to control multiple smart devices. Users can extend Alexa's capabilities by installing "skills", which are additional functions developed by third-party vendors. The Amazon Echo's specification is shown in Table 29.

Table 29 Amazon Echo Specification

Feature	Contents
Wi-Fi	802.11a/b/g/n Dual-band (2.4GHz and 5GHz)
Alexa Activation	Wake word Action button
Bluetooth	Full support for streaming audio from a device to the Echo and for voice control of mobile devices.
Compatible with Voice Remote for Amazon Echo	Yes
Size	5.9" x 3.5" x 3.5"
Setup Requirements	Needs Wi-Fi connection and compatible control device (Fire OS, Android, iOS, or web portal)

5.2 Challenge Data

Files were extracted using CIFT (Cloud-based IoT Forensic Toolkit) as published in the 2018 Digital Investigation "Digital forensic approaches for Amazon Alexa ecosystem". The challenge data provided includes DB files and CSV files extracted from each table of the DB. The Evidence_Library directory also contains JSON files that contain information about voice command data and a file that records voice commands. Details of each data type will be described below.

5.2.1 JSON files

JSON (Javascript object notation) is an open standard format which uses text to convey data consisting of key-value pairs. All the requests and responses from Echo are returned via JSON. Table 30 shows the contents of an Amazon Echo JSON file.

Table 30 Amazon Echo JSON Data Details


```
"activityItemData":"{\"ttsText\":\"\",\"utteranceId\":\"AB72C64C86AW2:1.0/2018/05/16/13/B0F007125184
00WN/36:10::TNIH_2V.4c169b61-ad88-4c44-94d9-56483e880172ZXV\",\"endOfSpeechTimeInMillis\":0,\"i
sFalseWakeWord\":false,\"asrText\":\"\"}",
                "description":null,
                "feedbackAttributes":null,

"id":"eyJyZWdpc3RlcmVkVXNlcklkIjoiQTJGMDdOOFRESUFLNVUiLCJlbnRyeUlkIjoiMTUyNjQ3Nzc3Mjc2M
SNBQjcyQzYoQzg2QVcyIoIwRjAwNzEyNTE4NDAwV04jMCowIno",
                "itemType":"ASR",
                "registeredUserId":"A2F07N8TDIAK5U",

"sourceDevice":"{\"deviceType\":\"AB72C64C86AW2\",\"deviceSerialNumber\":\"B0F00712518400WN\"}",
                "timestamp":0,

"utteranceId":"AB72C64C86AW2:1.0/2018/05/16/13/B0F00712518400WN/36:10::TNIH_2V.4c169b61-ad88-
4c44-94d9-56483e880172ZXV",
                "version":1
        },
        {
"activityItemData":"{\"ttsText\":\"\",\"intentType\":\"Unknown\",\"slots\":null,\"confidenceValue\":null,\"do
mainType\":\"Unknown\",\"nbestIntentIndex\":0,\"asrText\":\"\"}",
                "description":null,
                "feedbackAttributes":null,

"id":"eyJyZWdpc3RlcmVkVXNlcklkIjoiQTJGMDdOOFRESUFLNVUiLCJlbnRyeUlkIjoiMTUyNjQ3Nzc3Mjc2M
SNBQjcyQzYoQzg2QVcyIoIwRjAwNzEyNTE4NDAwV04jMTUyNjQ3Nzc3Mjc2MioxIno",
                "itemType":"NLU",
                "registeredUserId":"A2F07N8TDIAK5U",

"sourceDevice":"{\"deviceType\":\"AB72C64C86AW2\",\"deviceSerialNumber\":\"B0F00712518400WN\"}",
                "timestamp":1526477772762,

"utteranceId":"AB72C64C86AW2:1.0/2018/05/16/13/B0F00712518400WN/36:10::TNIH_2V.4c169b61-ad88-
4c44-94d9-56483e880172ZXV",
                "version":1
```


We can obtain timestamp, sourceDevices, activityItemData, UUID of the device, and other information through this content.

5.2.2 Voice file

As shown in Fig. 25, the voice file name includes the command that the user requested of the Echo and the corresponding time. The name of the file is as follows.

o filename : (YYYY-MM-DDTHH_MM_SS+UTC)_TEXT(user-requested command).wav

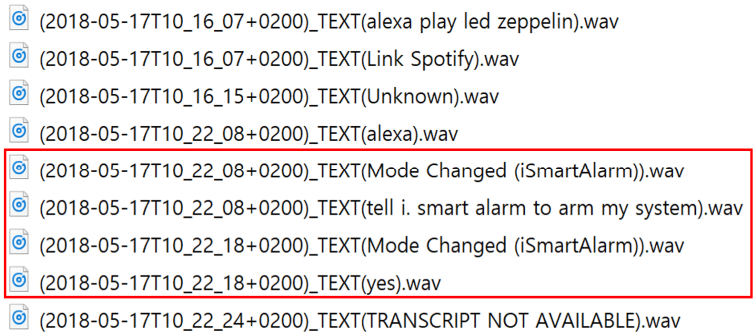

Fig. 25 Amazon Echo Voice Files of Incident Day

We analyzed the time at which the voice file was created and the corresponding command, and it was found that the control mode of iSmartAlarm was changed to 'ARM' mode by Amazon Echo at 10:22:08.

5.2.3 Database

The database contains user accounts, router settings information, Amazon skills, timelines, and other information (Fig. 26). By analyzing it, we were able to find useful forensic information.

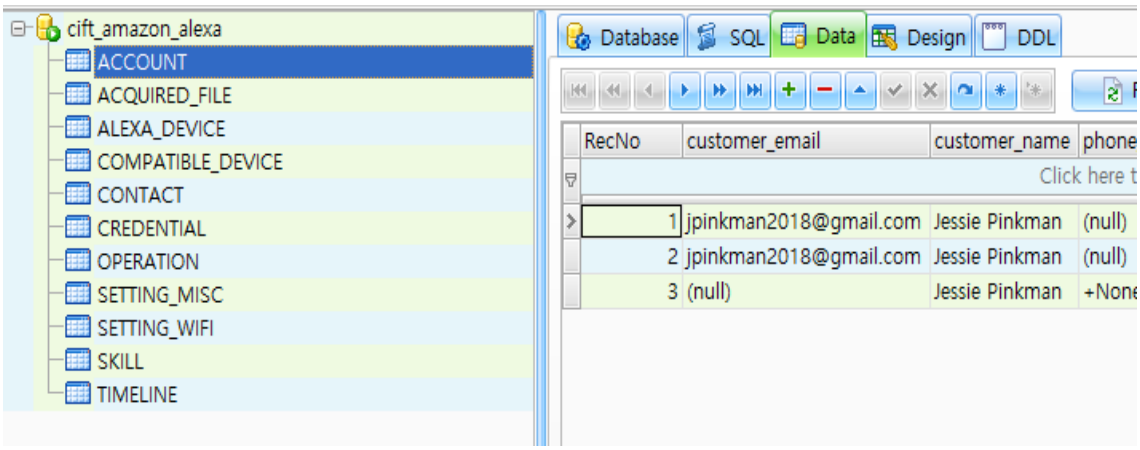

Fig. 26 Contents of Database

The most useful contents of the database are as follows.

o Account
-mail id : jpinkman2018@gmail.com
-customer id : A2F07N8TDIAK5U

o Wi-Fi Setting
-security method : WPA-PSK
-ssid: ESC-IoT
-Password : esc_iot_2018

o Skill
-Arlo, Nest Camera, Wink, iSmartAlarm

o Timeline
-The following table details the voice command timeline.

Table 31 Timeline of Voice Recordings (2018-05-17)

Time (UTC +2)	Sourcetype	Short	Desc	Note
	File Name			
10:16:08	Activity History	History (Dialog Items)	alexa play led zeppelin	User's command
	082a17905eb233a9863b97ec9f6b5b8970191fbf.json			
10:16:09	Home	Salmon Card	Link Spotify	Alexa heard: "alexa play led zeppelin" | Alexa's answer: "To ask Alexa to play Spotify, link your Spotify Premium account. You can also ask Alexa to "Spotify Connect" and control the music directly from your Spotify App."
	1840d4712abb8ed67fd2acf76f7c3e1d2b56a11d.json			
10:16:09	Activity History	History	alexa play led zeppelin	INVALID
	ce9240f8f4e8944dfec2ca8f607e451e4d03a474.json			
10:16:09	Activity History	History (Dialog Items)	To play Spotify, link your premium account first using the Alexa App.	Alexa's answer
	082a17905eb233a9863b97ec9f6b5b8970191fbf.json			

10:16:20	Activity History	History (Dialog Items)	Unknown	User's command
	690f40fd0a6c6c1a38f32b97b16cec05d1c22cc0.json			
10:16:20	Activity History	History	Unknown	SUCCESS
	ce9240f8f4e8944dfec2ca8f607e451e4d03a474.json			
10:22:08	Activity History	History (Dialog Items)	alexa	User's command
	a586bfe14661258f0953aba910cd83519d890bfc.json			
10:22:09	Activity History	History	alexa	SUCCESS
	ce9240f8f4e8944dfec2ca8f607e451e4d03a474.json			
10:22:12	Activity History	History (Dialog Items)	tell i. smart alarm to arm my system	User's command
	0305c1b97c035364db7251e540c2cb39b9976091.json			
10:22:13	Activity History	Text Card	Mode Changed (iSmartAlarm)	Alexa heard: "tell i. smart alarm to arm my system" | Alexa's answer: "Your Door is open, Are you sure you want to arm your system?"
	1840d4712abb8ed67fd2acf76f7c3e1d2b56a11d.json			
10:22:13	Home	History	tell i. smart alarm to arm my system	SUCCESS
	ce9240f8f4e8944dfec2ca8f607e451e4d03a474.json			
10:22:13	Activity History	History (Dialog Items)	Your Door is open, Are you sure you want to arm your system?	Alexa's answer
	0305c1b97c035364db7251e540c2cb39b9976091.json			
10:22:19	Activity History	History (Dialog Items)	yes	User's command
	2b8c27e2807996578e4baa0954d0340e632f3b6d.json			
10:22:20	Activity History	Text Card	Mode Changed (iSmartAlarm)	Alexa heard: "yes" | Alexa's answer: "Your system will set to Arm in 30 seconds."
	1840d4712abb8ed67fd2acf76f7c3e1d2b56a11d.json			
10:22:20	Home	History	yes	SUCCESS
	ce9240f8f4e8944dfec2ca8f607e451e4d03a474.json			
10:22:20	Activity History	History	Your system will set to Arm in 30 seconds.	Alexa's answer
	2b8c27e2807996578e4baa0954d0340e632f3b6d.json			
10:22:25	Activity History	History	-	DISCARDED_NON_DEVICE_ DIRECTED_INTENT
	ce9240f8f4e8944dfec2ca8f607e451e4d03a474.json			

5.2.1 The Amazon Alexa Application in a Smartphone

By analyzing the Alexa application package installed on the smartphone, we confirmed that the user credentials, the user's commands, and Alexa's answers are stored in a DB.

We found that a voice command is stored as text, as shown in Fig. 27. It is stored in the catalystLocalStorage table of the *USERDATA/data/com.amazon.dee.app/database /RKStorage.db*.


```
"descriptiveText":[
   "Your Door is open, Are you sure you want to arm your system?"
],
"giveFeedbackAction":{
   "actionType":"GiveFeedbackAction",
   "mainText":"Thank you! Your feedback helps Alexa understand you better.",
   "musicCustomerId":null,
   "route":"beta-feedback",
   "routeAddOnComponent":null,
   "serviceName":null,
   "subText":"Send more detailed feedback.",
   "subTextRoute":null,
   "thirdPartyAppId":"amzn1.ask.skill.8ccabd3a-a2e5-402a-b281-680ee078cb26",
   "thirdPartyAppName":"iSmartAlarm"
},
"hint":null,
"id":"A2F07N8TDIAK5U#1526545333528#AB72C64C86AW2#B0F00712518400WN",
"nBestOptions":null,
"originIntentType":"ChangeMode",
"playbackAudioAction":{
   "actionType":"PlayAudioAction",
   "mainText":"Alexa heard: \"tell i. smart alarm to arm my system\"",
   "subText":null,
   "subTextRoute":null,
```


Fig. 27 Contents of map_data_storage_v2.db

As shown in Fig. 28, we confirm that user credentials are stored in *USERDATA/data/com.amazon.dee.app/database/map_data_storage_v2.db*.

RecNo	_id	directed_id	display_name
Click here to define a filter			
1	1	amzn1.account.AGGMG4DRSURCQ7QT4TCLAINUZT2Q	Jessie Pinkman

Fig. 28 User Credential in map_data_storage_v2.db

6. Network capture

6.1 Introduction

A given network capture is a packet collected from 2018-05-17 15:36:25 to 15:37:23 (UTC +2). Using NTP (Network Time Protocol), we figured out the timestamps of packets (Fig. 29).

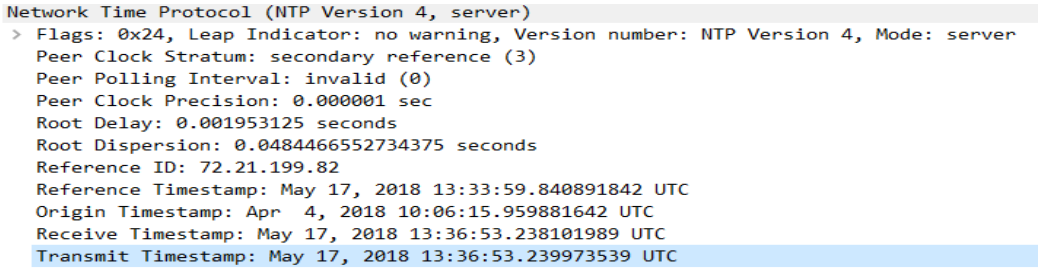

Fig. 29 Timestamp in NTP

6.2 Challenge Data

6.2.1 Packet Analysis

We matched the IP of the MAC addresses of IoT devices. We calculated the communication flow of each smart device. The QBee camera communication packet of the smartphone was found. The main communication details for each device are as shown in Table 32.

Table 32 Summary of Packets Flows

Source IP [Device name]	Destination IP [Device name]	Time (UTC+2)	Protocol
10.20.30.13 [Nest Cam]	35.195.59.182	15:36:25~15:37:23	TLS v1
10.20.30.15 [QBee Camera]	**144.76.81.240**	**15:36:28~15:37:18**	**TCP/UDP**
	10.20.30.21 [Galaxy S6 Edge]	**15:36:34~15:37:19**	**HTTP**
10.20.30.17 [Arlo Base Station]	54.72.123.194	15:36:27~15:37:11	TCP
10.20.30.19 [Nest Protector]	54.152.107.0	15:36:57	TCP
10.20.30.21 [Galaxy S6 Edge]	172.217.16.142	15:36:26	TLS v1.2
	172.217.23.106		
	216.58.205.174		
	172.217.16.142		UDP
	144.76.81.240	15:37:09	TLS v1.2
	31.13.64.35	15:37:12	
	31.13.64.16	15:37:15	
10.20.30.22 [Wink Hub]	34.224.5.65	15:36:45~15:37:15	
10.20.30.23 [Amazon Echo]	23.23.189.37	15:36:27~15:36:39	UDP
	52.46.156.66	15:36:39	TLS v1.2
	23.23.78.17	15:36:55~15:37:22	UDP

6.2.2 QBee Camera Vulnerability

In the companion app, QBee Cam, the default communication mode with the camera is unencrypted text when on a local network (CVE-2018-16225). Packets contain the cookies needed to authorize requests to the camera. As shown in Fig. 30, we confirmed that cookies transmitted from the QBee Camera are unencrypted. Therefore, anyone in the local network is able to eavesdrop on the communication as well as to intercept the cookies.

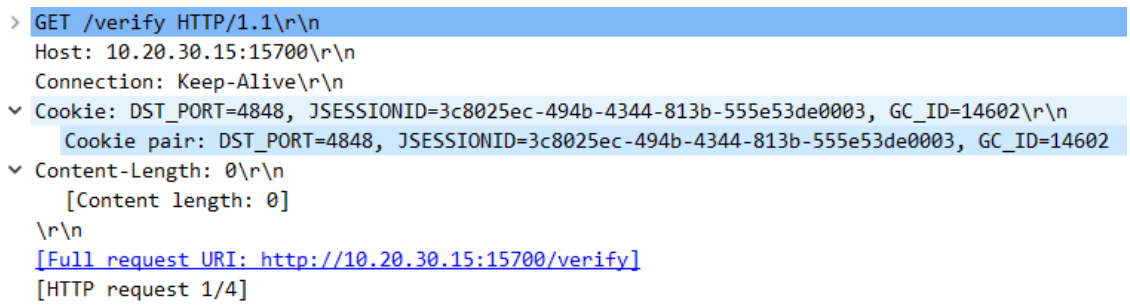

Fig. 30 QBee Camera's Credential in network packet

It is possible to disable the camera and enable the privacy mode. In addition, disabling the functionality of the physical button to toggle the privacy mode is possible.

IV. Forensic Tool

1. Introduction

We developed a visualization tool based on analyzing the data. This tool provides a better insight into the incident by showing the data associated with the event in chronological order.

1.1 Development environment

We developed a visualization tool using the ELK (Elasticsearch, Logstash, Kibana) solution. By injecting the given forensic data into the ELK solution, we can view incident-related events visualized via Kibana (Web browser).

Table 33 details the ELK solution environment.

Table 33 ELK Solution Specification

Feature	Tool
OS (Server)	Ubuntu 18.04.2 LTS
Web Browser (Client)	Chrome 72.0.3626.121
ELK solution	Elasticsearch 6.5.4
	Logstash 6.5.4
	Kibana 6.5.4

2. Description of the Tool

2.1 How to Use

① Access Kibana page

This tool is a web-based dashboard that provides a timeline for the events we find analyzing the given data. The URL information needed to access the tool are as follows.

o URL : http://LocalHost:5601

② Time range setting

After access, choose Dashboard on left side of web page. Then, apply the time interval of the data to be displayed on the dashboard using the time picker on the upper right as shown in Fig. 31. Here, we set the time interval from 2018-05-16 to 2018-05-17, including the time of the incident.

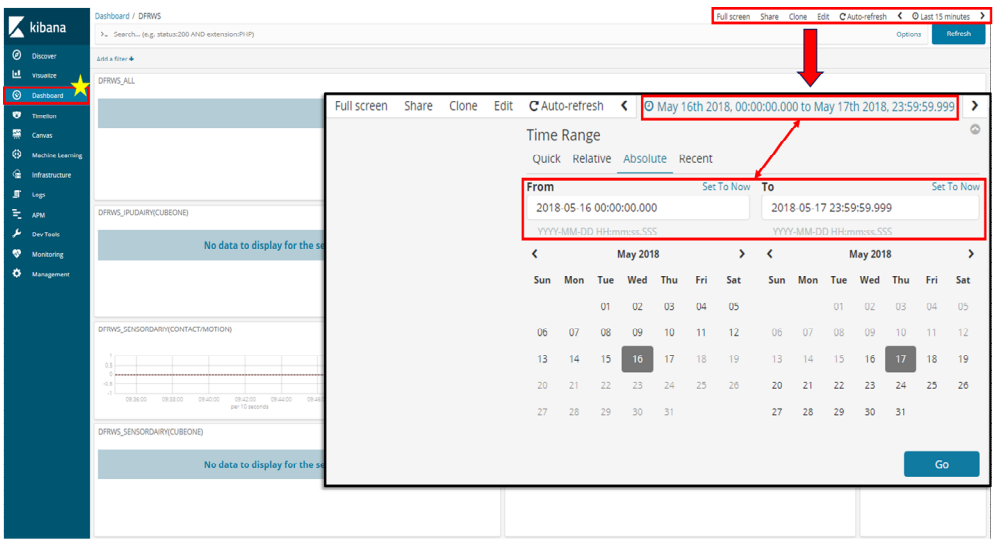

Fig. 31 Set the Time Interval Using the Time Picker

③ Check timeline of data

After completing the time setting, the dashboard shown in Fig. 32 is displayed.

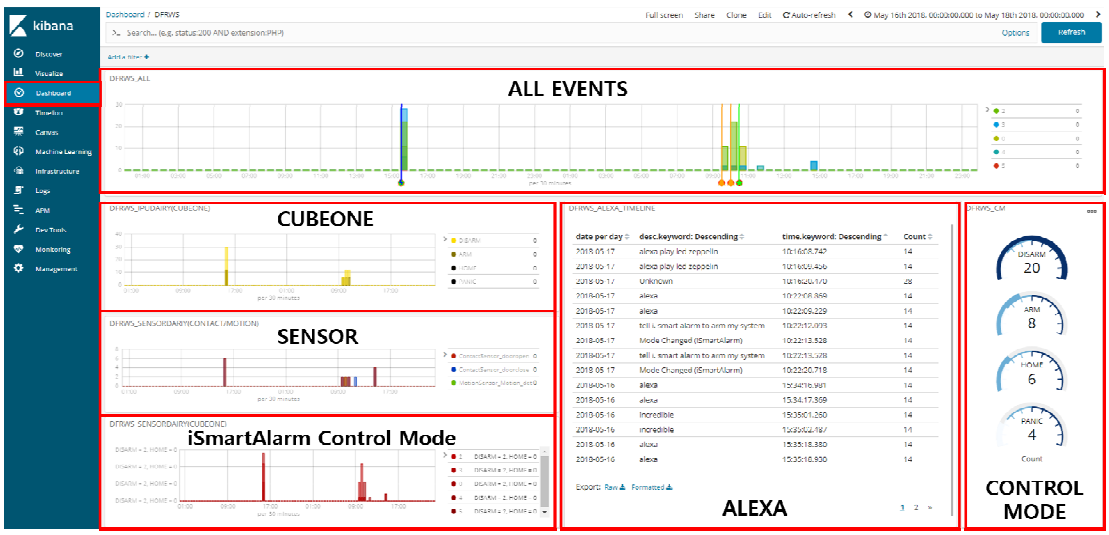

Fig. 32 Dashboard for Incident Timelines

Each item shows the timeline for iSmartAlarm, including CubeOne™, Contact Sensor, Motion Sensor, and Alexa's timeline.

④ Check 'Discover' for details of data

There are detail information of data in Discover as shown in Fig. 33. It can be able to see all of data or chosen data.

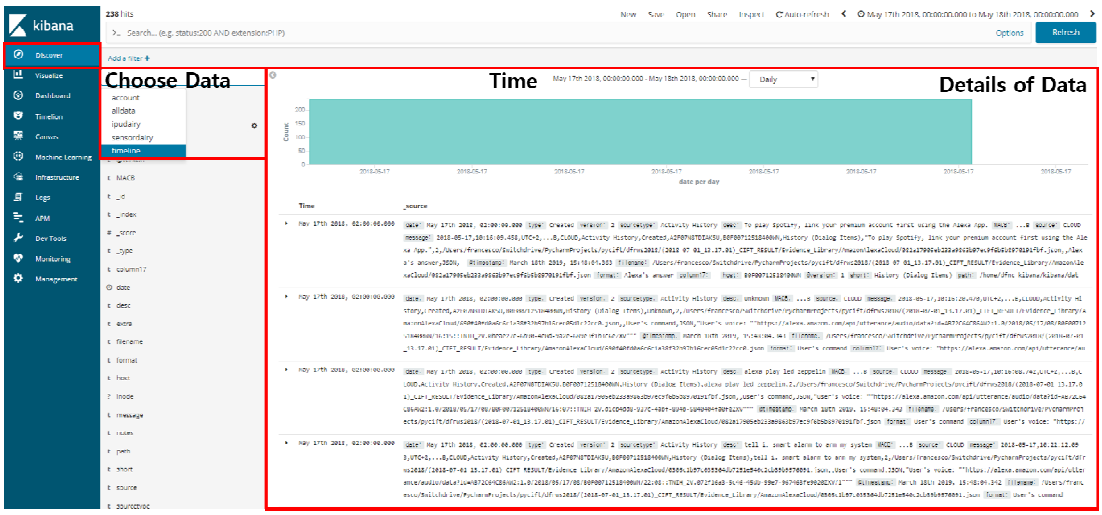

Fig. 33 Discover for Details of Data

2.2 Description of Each Item

Fig. 34 shows the timeline for iSmartAlarm, where the label number is the same as the action number described in Section 2.2.2.

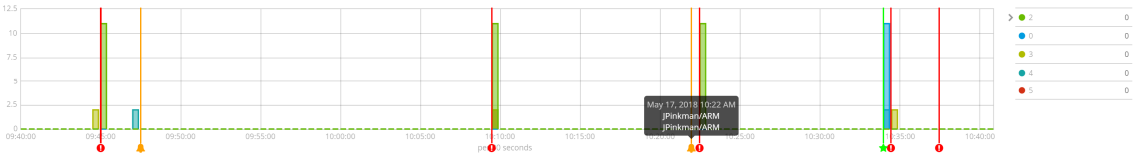

Fig. 34 Timeline for iSmartAlarm

The exclamation circle, bell, star, and bolt icons indicate when the 'DISARM', 'ARM', 'HOME', and 'PANIC' modes are set, respectively. To check the name of the user who changed the control mode setting, move the mouse over the icon. The usage of all timelines is the same, and Fig. 35~38 show the timeline for each device.

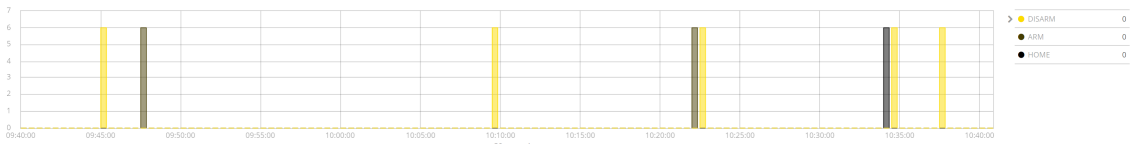

Fig. 35 Timeline for "IPUDariy" Table (CubeOne™)

Fig. 36 Timeline for "SensorDariy" Table (Contact/Motion Sensor)

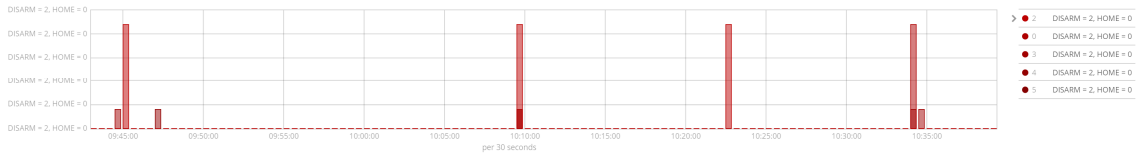

Fig. 37 Timeline for "SensorDariy" Table (iSmartAlarm control mode)

date per day	desc.keyword: Descending	time.keyword: Descending
2018-05-17	alexa play led zeppelin	10:16:08.742
2018-05-17	alexa play led zeppelin	10:16:09.456
2018-05-17	Unknown	10:16:20.470
2018-05-17	alexa	10:22:08.869
2018-05-17	alexa	10:22:09.229
2018-05-17	tell i. smart alarm to arm my system	10:22:12.093
2018-05-17	Mode Changed (iSmartAlarm)	10:22:13.528
2018-05-17	tell i. smart alarm to arm my system	10:22:13.528
2018-05-17	Mode Changed (iSmartAlarm)	10:22:20.718
2018-05-16	alexa	15:34:16.981
2018-05-16	alexa	15:34:17.369
2018-05-16	incredible	15:35:01.260
2018-05-16	incredible	15:35:02.487
2018-05-16	alexa	15:35:18.380
2018-05-16	alexa	15:35:18.930

Fig. 38 Timeline for Alexa