DFRWS 2018 Challenge

Team Name	AIForensics (AIForensics@gmail.com)
Team Members	Inhwan Cha (Samsun SDS)
	Aran Park (LIG Nex1)

Contents

1 Introduction

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

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

- **Device Level Analysis:**
  Developing methods and tools to forensically process digital traces generated by IoT devices, including on mobile devices.
- **Network Level Analysis:**
  Developing methods and tools to forensically process digital traces generated by IoT devices on networks.
- **Correlation and Analysis:**
  Developing methods and supporting tools that combine information from various data sources and automatically compute, visualize, or otherwise expose patterns of potential interest.
- **Evaluating and Expressing Conclusions:**
  Formally evaluating and expressing the probability or likelihood ratio that the prime suspect committed the offense, versus some unknown person did.

1.1 Case scenario

This case scenario is that Jessie Pinkman의 an illegal drug lab was invaded and unsuccessfully set on fire. Police interrogate two of Jessie Pinkman's known associates: D. Pandana and S. Varga. Because, Pandana and Verga admit having access to the drug lab's WiFi network but deny any involvement in the raid. There are 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) in the durg lab, and an Amazon Echo and a WinkHub are also present. So, the digital forensic specialist observes the cases presented using IoT devices.

2 Report summary

2.1 Illegal drug lab IoT integration network

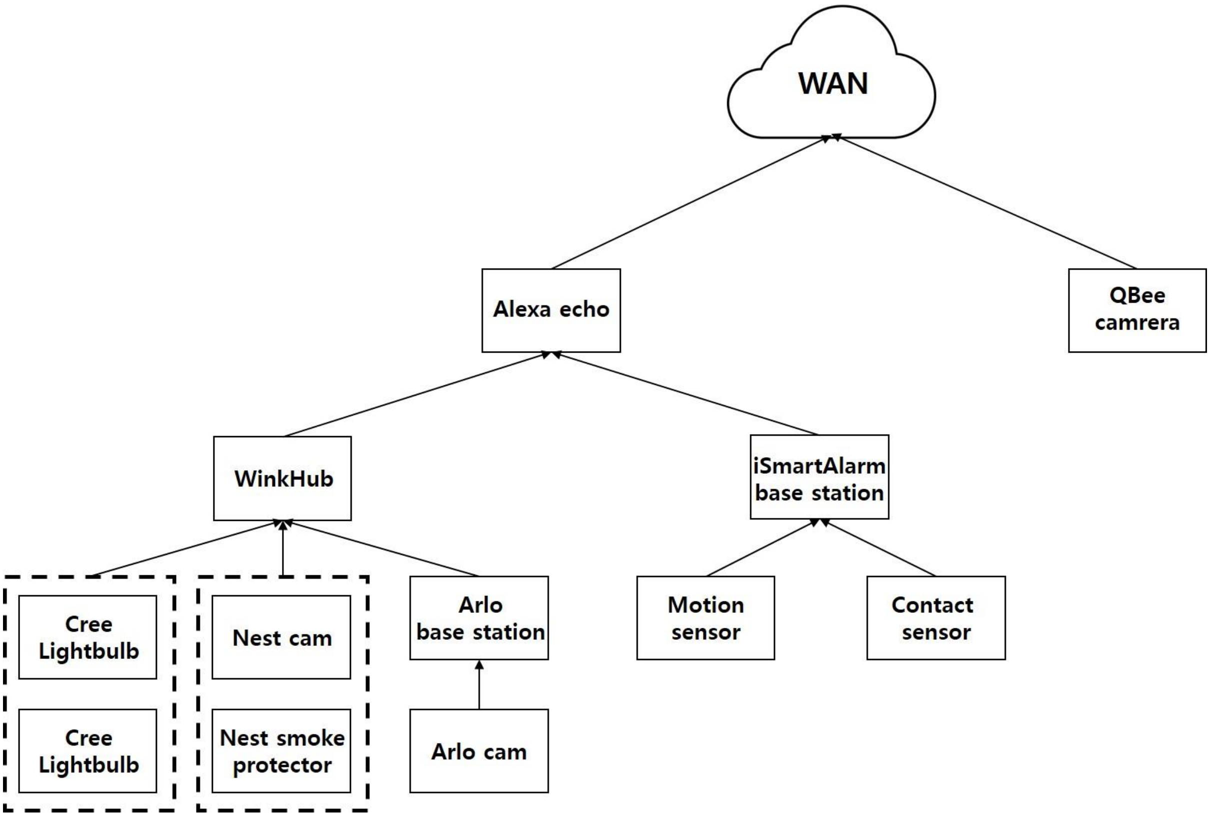


Figure 1 Drug lab's IoT device network

2.2 Analysis result

2.2.1 Drug lab was raided at 2018-05-17T10:34:36+02:00 by pandadodu

Drug lab was raided by a user of the pandadodu account at 2018-05-17T10:34:36+02:00 and has the following grounds:

1) When JPinkman is staying in the drug lab, the alarm mode of the drug lab's alarm mode was changed into DISARM.
2) When the alarm mode is DISARM and the door has been opened, the siren has occurred.
3) Continuous detection of motion and noise for approximately 1 minute.

Based on the above evidence, the pandadodu is a person involved in the raid of the drug lab with a probability of about 60%.

Meanwhile, it is possible that the pandadodu is D.Pandana, a person who has a relationship with JPinkman. The reasons for this is as follows:

1) The fact that the podadu is registered as a member of the drug lab in iSmartAlarm.
2) Because of its characteristics, iSmartAlarm member registration requires communication with a super user(Jpinkman).
3) The privacy mode of QBee camera should physically control QBee camera or use security vulnerabilities in the same network as Qbee camera.

If QBee Camera's conversion to Privacy mode is related to the attack, and it is not done by physically, pandadodu is possibliy D.Pandana or S.Verga. because D.Pandana and S.Verga can communicate with JPinkman and access its internal network. Especially because of the similarity of name between 'D.Pandana' and 'pandadodu', There's a more possibility that pandadodu is D.Pandana.

2.2.2 Possibility of Third Person's Participation in Crime

An analysis of this case suggests that a third person may have joined the crime with pandadodu. The facts identified during the analysis are as follows.

1) At 2018-05-17T09:39:42+02:00 ~ 2018-05-17T09:40:37+02:00 two persons, excluding JPMAN, stayed in the drug lab.
2) At 2018-05-17T10:09:52+02:00 to 2018-05-17T10:33:37+02:00 an unidentified person stayed in the drag lab.
3) An unidentified person was seen attempting to contact the Nest Smoke Protector in a image left in Arlo application cache.

Although this analysis could not clarify the association of a third person to an event, it is not possible to confirm that a third person is not related to the event. In particular, it is possible that the person in contact with the Nest Smoke protector is involved in the incident.

2.2.3 QBee camera was disabled by **Privacy mode**

QBee camera is unavailable due to Privacy mode. The reasons for this are as follows:

1) The network packet analysis showed that the QBee camera was communicating normally.
2) After the incident, traces of using the QBee camera application were found, and the main activity of the application was the word PRIVATE.

After analyzing the network package of QBee camera, we found that API commands from QBee camera use HTTP protocol. This means that another person located in the internal network can do API commands to QBee camera by stealing the credentials of a user with complete user authentication.

QBee camera can be configured in Privacy mode by using physical buttons and APIs.

If the physical button of QBee camera is not set to Private mode, it is possible that a person with access to the internal network stole JPinkman's authentication information and switched to Privacy mode using QBee camera config API.

3 Analysis detail

3.1 Samsung Galaxy Edge S6 (JPinkman's mobile)

Through on-site identification and statements, Jessie Pinkman is using the various IoT devices to protect the illegal drug lab. The various IoT devices can be controlled by mobile device applications, and their activities are recorded in the Sqlite database on the device. When the fire alarm occurred in the illegal drug lab, we acquired the IoT application and cloud data recorded on the Samsung Galaxy Edge S6 for collect the activities that occurred inside the illegal drug lab and analyzed. We also checked whether there was any contact with JPinkman, D.Pandana, S.Verga or any other person before the incident occurred..

Artifact collection and analysis were performed in the following categories.

- Samsung Galaxy Edge S6 Device information
- Analysis of communication between JPinkman and others
  - SMS/MMS events
  - Contacts/Call log
  - Email trace
  - Web browser usage
  - Application installation using Google playstore
  - SNS Application usage
- Media data on Samsung Galaxy Edge S6
- Analysis Samsung Galaxy Edge S6 events at the day of fire alarm(2018-05-17)
  - The events on IoT Device's Application

According to the analysis of above category, confirmed the following facts.

- There are traces of two WiFi connections on the Samsung Galaxy Edge S6.
- JPinkman did't communicate with others on or before the fire alarm had occurred.
- Screen shots and pictures of IoT equipment information exist inside the camera.
- On the day of fire alarm(2018-05-17),
  - There were two people in the Drug lab.
  - The iSmartAlarm account called 'pandadodu' changed the alarm mode to DISARM in the Drug lab.
  - A number of motions and noises were detected.
  - The QBee camera did not close when police spotted it.

3.1.1 The information of Samsung Galaxy Edge S6 device

Using the following artifacts, we have confirmed the basic information of the Samsung Galaxy Edge S6.

Table 1 Artifacts list for mobile device basic information

Artifact path	Artifact category	Hash(SHA1)	Description
/data/misc/wifi/wpa_supplicant.conf	Basic information	8b5214f38fb4d536f6a05331ae2ab4e10bfbedba	Device basic information
/data/misc/wifi/wpa_supplicant.conf	Network information	8b5214f38fb4d536f6a05331ae2ab4e10bfbedba	Connected Wifi network information
/efs/wifi/.mac.info	Network information	54d10c87ad4868961459f7c6371ba23cae330b9f	Wifi adapter MAC address
/efs/bluetooth/bt_addr	Network information	a95a58845979d61939ac79cea0105ba4e51b31f3	Bluetooth Name, MAC address
/data/misc/bluedroid/bt_config.conf	Network information	72c64bcaf30693681e7f060e821c35458b44c19f	Bluetooth MAC address
/data/property/persist.sys.locale	Settings information	5a7bd4149d0d34d3ec86181cdab1cb8dd3f441d7	Timezone set on device
/data/property/persist.sys.timezone	Settings information	2150d066fad6ecdac0bc1d1befc928411fabf6b1	Locale set on device
/data/system/SimCard.dat	Simcard information	60acacd67102279c0475894b847600a3579ed8b8	Sim card information
/system/build.prop	Software(build) information	5235343636def2786e20e329641fc16a13ad23a4	Software(Build) properties

By analyzing each artifact analysis, we found the basic information of Samsung Galaxy Edge S6 device. Using the information, we confirmed that Samsung Galaxy Edge S6 has connected to "Cthulhuuuu's iPhone" and "ESC-IoT".

Table 2 The basic information of Samsung Galaxy Edge S6

Category		Data
Device name		zeroltexx
Manufacturer		samsung
Model_name		SM-G925F
Serial number		0b1502000b8ae1c0
Timezone		Europe/Zurich
Locale		en-US
wifi	Connected wifi 1 SSID	Cthulhuuuu's iPhone

	Connected wifi 2 SSID	ESC-IoT
	MAC address	AC:5F:3E:73:E3:78
Bluetooth	Name	Galaxy S6 edge
	MAC address	D8:C4:E9:7C:2E:F8
Sim card	Country	Italy
	Operator	Italy TIM
	Serial number	89390100002217635543
	Phone number	3662158453
	Change time	2018-05-15T12:52:44+02:00
Software(Build)	Android version	6.0.1
	Build number	MMB29K.G925FXXU4DPIL

3.1.2 Analysis of JPinkman's conversation with others

In order to confirm the existence of a relationship with JPinkman's drug lab raid, we checked the communication history betweenJPinkman and another person. To analyze the JPinkman's conversation history, the following communication categories were defined to collect and analyze artifacts.

SMS/MMS event

Table 3 SMS/MMS event

Artifact path	Hash(SHA1)
/data/data/com.android.providers.telephony/databases/mmssms.db	8b5214f38fb4d536f6a05331ae2ab4e10bfbedba
/data/data/com.android.providers.telephony/databases/mmssms.db-wal	5de1f9a876b68c442dd2878b975b31b3d9c929ae

Contacts/Call log

Table 4 Contacts/Call log file path

Artifact path	Hash(SHA1)
/data/data/com.android.providers.contacts/databases/contacts2.db	17e366b57f3de8cc4087a99601997d9124a10384
/data/data/com.android.providers.contacts/databases/contacts2.db-wal	acfbc026ed8fc27cb010210e920a01ac744a2317

Call log

Table 5 Call log file path

Artifact path	Hash(SHA1)
/data/data/com.android.providers.telephony/databases/telephony.db	56a319fe3de33e5434c0776d4a68b509eddfcb57

Email

Table 6 Email usage

Artifact path	Hash(SHA1)
/data/data/com.google.android.gm/databases/mailstore.jpinkman2018@gmail.com.db	5b8afed9a16beba35967b3f0e908979c98dadc1a
/data/data/com.google.android.gm/databases/mailstore.jpinkman2018@gmail.com.db-wal	9f73f2faaa556a49df12777d05533de5fdf6ddd4

Web browser usage

Table 7 Web browser usage

Artifact path	Hash(SHA1)
/data/data/com.android.chrome/app_chrome/Default/History	7691ba7beb83deb9b3307c30ef5dc68597bf5fad

Application installation and search history on Google Playstore

Table 8 The trace of application installation and Google Playstore search history

Artifact path	Hash(SHA1)
/data/data/com.android.vending/databases/library.db	0225f710751f9dfe52666cb94c6ee2bfe5b001e3
/data/data/com.android.vending/databases/package_verification.db	f0554689353e4e21a798416a555f1daabbab74e5
/data/data/com.android.vending/databases/suggestions.db	eecf9aec82086fae7ab589a286c66150e076a512
/data/data/com.android.vending/databases/localappstate.db	f8cc34f17316da3facc9ee8a18000947d735b2f6

SNS application usage event

Table 9 SNS application usage event

Artifact path
/data/system/usagestats/0/daily/*
/data/system/usagestats/0/monthly/*
/data/system/usagestats/0/weekly/*

The result of SMS / MMS analysis, we found one message. The message is irrelevant because it is related to the authentication code.

Table 10 Result of SMS/MMS analysis

Datetime(Sent)	SMS/MMS message content
2018-05-15T15:00:55+02:00	Your verification code is 3723

Result of checking the history of Contacts and Call log, the contact and call history stored in Samsung Galaxy Edge S6 do not exist.

The Samsung Galaxy Edge S6 uses the Gmail application to send email. We checked the traces of Gmail usage and found that most of the messages were emails related to device settings and consisted of notifications from someIoT devices. As a result, there is no e-mail that JPinkman contacted others.

Table 11 Result of Gmail usage

Datetime(Sent)	Sender	Title
2018-04-17T10:45:37+02:00	PayPal <paypal@mail.paypal.com>	Your account still needs a payment method...
2018-04-17T14:23:02+02:00	SKYLAB <notifications@nest.com>	Camera removed from your account
2018-04-17T14:33:15+02:00	support@nest.com <support@nest.com>	Re: Order complete but subscription doesn't attached. [ref:_00D40MIt9._5001W1H71CH:ref]
2018-04-17T15:48:19+02:00	Nest <notifications@nest.com>	Welcome to your free Nest Aware trial.
2018-04-17T22:03:27+02:00	Nest <news@nest-email.com>	Passt Nest Protect gut auf dich auf?
2018-04-19T19:35:30+02:00	Nest <news@nest-email.com>	Make this Earth Day matter.
2018-04-20T22:56:22+02:00	Amazon Echo <store_news@amazon.com>	What's new with Alexa?
2018-04-23T15:36:51+02:00	<no-reply@spotify.com>	Du hast Dein Spotify-Abonnement gekündigt.
2018-04-24T17:49:44+02:00	Nest <news@nest-email.com>	Bestens im Bilde mit der neuen Kamera?
2018-04-25T11:07:21+02:00	iSmartAlarm <no-reply@support.ismartalarm.com>	Your iSmartAlarm System Skylab has been triggered
2018-04-25T11:09:08+02:00	iSmartAlarm <no-reply@support.ismartalarm.com>	Your iSmartAlarm System Skylab has been triggered
2018-04-25T11:10:36+02:00	iSmartAlarm <no-reply@support.ismartalarm.com>	Your iSmartAlarm System Skylab has been triggered
2018-04-25T11:31:10+02:00	<alerts@arlo.com>	Arlo Has Just Detected Motion
2018-04-27T13:11:33+02:00	<alerts@arlo.com>	Arlo Has Just Detected

		Motion
2018-04-27T13:12:06+02:00	<alerts@arlo.com>	Arlo Has Just Detected Motion
2018-04-27T13:12:26+02:00	<alerts@arlo.com>	Arlo Has Just Detected Motion
2018-04-27T13:12:44+02:00	<alerts@arlo.com>	Arlo Has Just Detected Motion
2018-04-27T13:14:28+02:00	<alerts@arlo.com>	Arlo Has Just Detected Motion
2018-04-27T13:25:08+02:00	SuperLab <notifications@nest.com>	Deine Kamera ist offline.
2018-04-27T20:27:03+02:00	Amazon Echo <store_news@amazon.com>	What's new with Alexa?
2018-05-01T15:10:49+02:00	Nest <news@nest-email.com>	The Nest Temperature Sensor is here.
2018-05-01T17:18:32+02:00	Spotify <hello@spotify.com>	Konzerte in der Nähe von Ecublens: Gogol Bordello, Iron Maiden und mehr
2018-05-02T10:56:48+02:00	SuperLab <notifications@nest.com>	Deine Kamera ist offline.
2018-05-04T09:48:40+02:00	<alerts@arlo.com>	Arlo Has Just Detected Motion
2018-05-04T09:50:40+02:00	<alerts@arlo.com>	Arlo Has Just Detected Motion
2018-05-04T21:02:27+02:00	Amazon Echo <store_news@amazon.com>	What's new with Alexa?
2018-05-04T23:27:54+02:00	Nest <news@nest-email.com>	Willkommensgruß von Nest
2018-05-09T14:35:47+02:00	<alerts@arlo.com>	[INVALID_DATA]
2018-05-09T18:12:49+02:00	PayPal <paypal@mail.paypal.com>	Save $10 on $50 DSW gift cards today
2018-05-10T21:32:27+02:00	Nest Home Report <account@nest.com>	Nest April Home Report for SuperLab
2018-05-11T14:13:01+02:00	PayPal <paypal@mail.paypal.com>	Make the gift of money special
2018-05-11T22:23:08+02:00	Amazon Echo <store_news@amazon.com>	What's new with Alexa?
2018-05-12T03:09:45+02:00	Google <privacy-noreply@policies.google.com>	Miglioramenti ai controlli e alle norme sulla privacy
2018-05-14T11:18:14+02:00	SuperLab <notifications@nest.com>	Camera removed from your account
2018-05-14T11:24:48+02:00	Nest <notifications@nest.com>	Welcome to your free Nest Aware trial.
2018-05-15T10:34:32+02:00	Amazon <account-update@amazon.com>	Amazon.com Password Assistance
2018-05-15T10:35:42+02:00	Amazon <account-update@amazon.com>	Revision to Your Amazon.com Account
2018-05-15T11:45:32+02:00	Google <no-reply@accounts.google.com>	Jessie, telefono Samsung Galaxy S6 Edge non sono

		installate le app Google più recenti
2018-05-15T11:45:32+02:00	Google <no-reply@accounts.google.com>	Avviso di sicurezza
2018-05-15T12:52:05+02:00	Samsung account <SA.noreply@samsung-mail.com>	Benvenuti nei servizi Samsung.

The Samsung Galaxy Edge S6 uses Google chrome as its web browser. Therefore, we checked the access history of web site through Google chrome, and analyzed the type of web sites, search history and file download history.

As a result of checking the web site access trace through Google chrome, there are traces of accessing general homepage such as Alexa homepage and Nest homepage, traces of accessingWifi wireless router management page, and there was a trace connected to the Gmail homepage. There was one search through Google. After searching using the search term "Alexa", I checked the trace of downloading the Amazon alexa echo APK file from 'http://www.apkpure.com website'.

As a result, there is no direct evidence related to this case through the verification of access to Google chrome and no specificity was found.

Table 12 Access traces to Google chrome

Datetime	Title
2018-03-16T12:12:06+02:00	Inbox – jpinkman2018@gmail.com
2018-03-16T12:12:06+02:00	Inbox – jpinkman2018@gmail.com
2018-03-27T10:26:48+02:00	Amazon Alexa
2018-03-27T10:26:48+02:00	Amazon Anmelden
2018-03-27T10:26:48+02:00	Amazon Anmelden
2018-03-27T10:31:59+02:00	Amazon Alexa
2018-03-27T10:31:59+02:00	Amazon Alexa
2018-03-27T10:31:59+02:00	Amazon Alexa
2018-03-27T10:32:10+02:00	Amazon.com: Online Shopping for Electronics, Apparel, Computers, Books, DVDs & more
2018-03-27T10:34:32+02:00	Accedi - Google Account
2018-03-27T10:34:47+02:00	Inbox – jpinkman2018@gmail.com
2018-03-27T10:55:39+02:00	Spotify Web Player
2018-03-27T10:55:39+02:00	Spotify Web Player
2018-03-27T10:55:39+02:00	Spotify Web Player
2018-03-27T12:03:36+02:00	Inbox by Gmail
2018-03-27T12:03:36+02:00	Inbox by Gmail

2018-04-09T20:57:31+02:00	Accedi
2018-04-09T20:57:31+02:00	Accedi
2018-04-09T20:57:41+02:00	kettu
2018-04-17T11:18:27+02:00	iptables interface - Cerca con Google
2018-04-17T11:33:04+02:00	WiFi Pineapple
2018-04-17T14:07:12+02:00	Page Not Found
2018-04-17T14:16:24+02:00	Nest Store
2018-04-23T13:16:15+02:00	Online regex tester and debugger: PHP, PCRE, Python, Golang and JavaScript
2018-04-23T13:16:15+02:00	Online regex tester and debugger: PHP, PCRE, Python, Golang and JavaScript
2018-04-26T09:44:01+02:00	Install Elasticsearch with Docker | Elasticsearch Reference [6.2] | Elastic
2018-04-26T11:19:26+02:00	MoodleUnil: Login al sito
2018-04-26T11:19:26+02:00	MoodleUnil: Login al sito
2018-04-26T16:13:56+02:00	Not available
2018-05-09T14:29:22+02:00	Nest | Crea una casa connessa
2018-05-09T14:29:22+02:00	Nest | Crea una casa connessa
2018-05-09T14:29:22+02:00	Nest | Crea una casa connessa
2018-05-09T14:29:22+02:00	Nest | Crea una casa connessa
2018-05-09T14:33:42+02:00	Arlo Smart Home Security Cameras | Home Monitoring | Arlo by NETGEAR
2018-05-09T14:33:42+02:00	Arlo Smart Home Security Cameras | Home Monitoring | Arlo by NETGEAR
2018-05-15T10:32:48+02:00	Amazon Alexa
2018-05-15T10:34:44+02:00	Inbox – jpinkman2018@gmail.com
2018-05-15T10:34:44+02:00	Inbox – jpinkman2018@gmail.com
2018-05-15T10:34:44+02:00	Inbox – jpinkman2018@gmail.com
2018-05-15T10:34:44+02:00	Inbox – jpinkman2018@gmail.com
2018-05-15T10:34:44+02:00	Inbox – jpinkman2018@gmail.com
2018-05-15T10:35:48+02:00	Amazon Alexa
2018-05-15T11:16:01+02:00	Pi-Pinapple
2018-05-15T11:16:01+02:00	Pi-Pinapple
2018-05-15T13:15:41+02:00	android apk - Google-Suche
2018-05-15T13:15:48+02:00	Download APP APK Android App Online - Free Pure APK Downloader
2018-05-15T13:15:50+02:00	Search - APKPure Android App Store
2018-05-15T13:15:55+02:00	Alexa search results | APKPure.com
2018-05-15T13:15:58+02:00	Amazon Alexa APK Download - Free Music & Audio APP for Android | APKPure.com
2018-05-15T13:16:00+02:00	Download Amazon Alexa 2.2.208186.0 APK | APKPure.com

To check the trail of installing the SNS application, we checked the SNS application installation trace and search history on the Google Playstore of Samsung Galaxy Edge S6. After checking the search history on Google Playstore and SNS application installation trail, there were total 6 search records and all the queries were related to IoT applications. We also confirmed that a total of 5 SNS applications were installed on the Samsung Galaxy Edge S6.

Table 13 Google Playstore search history

Datetime	Search string
2018-05-15T13:08:34+02:00	iSmartAlarmwink
2018-05-15T13:08:39+02:00	wink
2018-05-15T13:09:03+02:00	nest
2018-05-15T13:09:43+02:00	arlo
2018-05-15T13:11:07+02:00	qbeez2
2018-05-15T13:11:10+02:00	qbee

Table 14 SNS Applications installed on Samsung Galaxy Edge S6

Datetime	Installed application
2018-05-15T13:56:59+02:00	Instagram (com.instagram.android)
2018-05-15T14:08:59+02:00	Hangouts (com.google.android.talk)
2018-05-15T14:12:18+02:00	Skype (com.skype.raider)
2018-05-15T14:16:33+02:00	Facebook (com.facebook.katana)
2018-05-15T14:24:15+02:00	WhatsApp (com.whatsapp)

After reviewing the applications used in the Samsung Galaxy Edge S6, there was not history of SNS application usage mentioned in Table 14.

As a result of the analysis of the above artifacts, there was no trace of conversation between Jessie Pinkman and another person, and I could not confirm any specific facts related to this case.

3.1.3 Media Data in Samsung Galaxy Edge S6

We collected and analyzed the following media artifacts to identify the media data in the Samsung Galaxy Edge S6.

Table 15 Media Artifacts path

Name	Artifact path
Camera	/data/media/0/DCIM/Camera/*
Screenshots	/data/media/0/DCIM/Screenshots/*
Voice Recorder	/data/media/0/Voice Recorder/*

3.1.3.1 Camera/Screenshots

After analyzing media data such as cameras and screenshots, we found information about the various IoT instruments installed in the Drug lab.

Table 16 IoT devices installed in Drug lab information

Device name	Serial number	MAC address
Arlo Base Station	4RD37B75A1EC9	08028EFF754F
Wink Hub	161700117WZD1	B479A72502FA
Nest Smoke alarm	06CA01AC331600CA	N/A
iPU3G(iSmartAlarm CubeOne)	N/A	004D3209D9E4
PIR3G(iSmartAlarm montion sensor)	141605015143012	N/A
Nest cam A0005	N/A	18B43061C9EF
QBee camera	416B4067717	D8FB5EE10192

3.1.3.2 Voice Recorder

In the voice recording file in Voice Recorder folder contains the voice "So today we are now at the London museum of natural history with my family and we have just finished looking at the Johns and if they're really pretty and I like them". The create time of the voice file is 2018-01-27T18:01:57+02:00, so it is not related to this case.

3.1.4 On the day of fire alarm(2018-05-17) events

3.1.4.1 Device level analysis

Through the event traces recorded in the IoT application, we confirmed the event that occurred on the day of the fire alarm. The collected artifacts for event confirmation are as follows.

iSmartAlarm

Table 17 iSmartAlarm's artifact files path

Artifact path	Hash(SHA1)
/data/data/iSA.common/databases/iSmartAlarm.DB	8b5214f38fb4d536f6a05331ae2ab4e10bfbedba
/data/app/iSA.comon-1/base.apk	937bf1678a59bcc0a8e952a689a6bedcdb9c71df

Amazon alexa echo

Table 18 Amazon alexa echo's artifact files path

Artifact path	Hash(SHA1)
/data/data/com.amazon.dee.app/databases/RKStorage	f0d2836cc9c309111c08660acb8135ae810eb2e6
/data/data/com.amazon.dee.app/databases/map_data_storage_v2.db	d1cdd333c198ac966186fd663b697a06f678c652
/data/data/com.amazon.dee.app/databases/DataStore.db	c0a89edc06ee861eb60b961a74134b9ae79b366f

WinkHub

Table 19 WinkHub's artifact files path

Artifact path	Hash(SHA1)
/data/data/com.nest.android/databases/cache	cdfa2820b5ffd62085993cd510aeaec58fe2e437
/data/data/com.nest.android/cache/cache/cache-1503821048.json	7455f3734de19f307d3a5433f61b0354aa498775
/data/data/com.nest.android/cache/cache/cache-1332523362.json	48c04e40187c9b5c2e10a2c30c98d3490ce039ed

Nest

Table 20 Nest's artifact files path

Artifact path	Hash(SHA1)
/data/data/com.nest.android/databases/cache	cdfa2820b5ffd62085993cd510aeaec58fe2e437
/data/data/com.nest.android/cache/cache/cache-1332523362.json	48c04e40187c9b5c2e10a2c30c98d3490ce039ed

Arlo

Table 21 Arlo's artifact files path

Artifact path	Hash(SHA1)
/data/data/com.netgear.android/databases/swrve.db	b8f4ed25081b2282e5caa1d006e60f32e2d63d6c

Qbee

Table 22 Qbee's artifact files path

Artifact path	Hash(SHA1)
/data/data/cache/com.vestiacom.qbeecamera /temp-VQBmgZlE4Wjz8vr0KBY37Yup	0924342b5813a9e3827be4c94464cbdd6644a954
/data/data/cache/com.vestiacom.qbeecamera /temp-sNFvHf9ZmWTijIUciAmGbR4W	1a781e6337ddbca80af74219242cf68897a08970

The database in iSmartAlarm stores data about which user set the alarm mode. In addition, information about when a sensor responded is also recorded. After analyzing the contents of iSmartAlarm.DB stored in Samsung Galaxy Edge S6, there were alarm mode settings and contact/motion sensor response history in 2018-05-17 when the fire alarm occured. (The 'action' value of the sensor operation in iSmartAlarm.DB is recorded as a specific integer value, so reverse engineering was performed on iSmartAlarm APK to confirm the meaning of the integer value)

Table 23 Records of iSmartAlarm alarm mode settings

Datetime	User	Mode
2018-05-17T09:45:22+02:00	TheBoss	DISARM
2018-05-17T09:47:50+02:00	Jpinkman	ARM
2018-05-17T10:09:57+02:00	TheBoss	DISARM
2018-05-17T10:22:22+02:00	Jpinkman	ARM
2018-05-17T10:22:30+02:00	TheBoss	DISARM
2018-05-17T10:34:17+02:00	TheBoss	HOME
2018-05-17T10:34:31+02:00	pandadodu	DISARM
2018-05-17T10:37:52+02:00	pandadodu	DISARM

Table 24 iSmartAlarm sensor alarm history

Datetime	SensorID	Action
2018-05-17T09:44:53+02:00	000A8540	Door open
2018-05-17T09:45:22+02:00	004D3209D9E4	Alarm mode change with RC3(DISARM)
2018-05-17T09:47:18+02:00	000A8540	Door close
2018-05-17T10:09:52+02:00	000A8540	Door open
2018-05-17T10:09:55+02:00	0006B4E5	Motion detected
2018-05-17T10:09:57+02:00	004D3209D9E4	Alarm mode change with RC3(DISARM)

2018-05-17T10:22:30+02:00	004D3209D9E4	Alarm mode change with RC3(DISARM)
2018-05-17T10:34:15+02:00	000A8540	Door close
2018-05-17T10:34:17+02:00	004D3209D9E4	Alarm mode change with RC3(HOME)
2018-05-17T10:34:36+02:00	000A8540	Door open
2018-05-17T11:39:50+02:00	000A8540	Door close
2018-05-17T14:52:10+02:00	000A8540	Door open
2018-05-17T14:57:06+02:00	000A8540	Door close
2018-05-17T14:58:03+02:00	000A8540	Door open
2018-05-17T14:58:15+02:00	000A8540	Door close

As a result of checking the above, there is a history that JPinkman and pandadodu users changed the alarm mode in 2018-05-17 when a fire alarm occurred, and the alarm mode has been changed by The Boss, a remote controller of iSmartAlarm.

5 seconds after pandadodu changed the alarm mode to DISARM, Door opening event of the drug lab indicates that the pandadodu is likely to be involved in the intrusion of the drug lab.

Amazon alexa echo records the user's voice command information and response information in the database, along with the display card information that appears on the application’s main activity. In addition, by recording a URL that allows users to download voice commands in MP4 format, the user can determine which user has performed voice commands.

The analysis of Amazon alexa echo database in Samsung Galaxy Edge S6 shows that Jessie Pinkman has been registered with Amazon alexa echo and the total number of events recorded on 2018-05-17 where a fire alarm occurred were 3.

Table 25 Account information for Amazon alexa echo

directed_id	display_name
amzn1.account.AGGMG4DRSURCQ7QT4TCLAINUZT2Q	Jessie Pinkman

Table 26 User voice commands history

Datetime	Card type	Title	User voice command	User voice command audio url
2018-05-17T10:16:09+02:00	SalmonCard	Link Spotify	alexa play led	/api/utterance/audio/data?id=AB72C64C86AW

			zeppelin	2:1.0/2018/05/17/08/B0F00712518400WN/16:07::TNIH_2V.d1cb4dd8-937c-4abf-894b-5840404fa0feZXV/0
2018-05-17T10:22:13+02:00	TextCard	Mode Changed	tell i. smart alarm to arm my system	/api/utterance/audio/data?id=AB72C64C86AW2:1.0/2018/05/17/08/B0F00712518400WN/22:08::TNIH_2V.072f16a3-5c46-45db-99e7-967463fe9020ZXV/1
2018-05-17T10:22:20+02:00	TextCard	Mode Changed	yes	/api/utterance/audio/data?id=AB72C64C86AW2:1.0/2018/05/17/08/B0F00712518400WN/22:18::TNIH_2V.2a142d91-50a8-406d-85f8-5cdac2868f08ZXV/0

Amazon alexa echo in drug lab is linked to iSmartAlarm and WinkHub. so voice command for iSmartAlarm mode change can be performed on Amazon alexa echo.

Of the above data, domain is 'https://alexa.amazon.com/' and user can check voice data if Alexa Echo cloud user authentication is successful. In other words, it is not possible to check voice data through the Device level analysis

WinkHub records events that occur on connected devices. In this case, the IoT devices connected to WinkHub are lightbulb1, lightbulb2, Arlo camera, nest camera, nest smoke protect. In other words, we can analyze the WinkHub database and check the event history of the above IoT device. After analyzing WinkHub's database, we confirmed that 31 events occurred in 2018-05-17 when fire alarm occurred. It consists of 8 events in arlo camera, 21 in nest camera, and 2 events in nest smoke protect.

Table 27 Event records of IoT devices integrated to WinkHub

Datetime	Description
2018-05-17T10:10:11+02:00	Kitchen's camera motion detected
2018-05-17T10:10:45+02:00	Kitchen's camera motion detected
2018-05-17T10:14:05+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:14:12+02:00	Kitchen's camera motion detected

2018-05-17T10:15:00+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:15:56+02:00	Kitchen's camera motion detected
2018-05-17T10:15:58+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:16:59+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:22:36+02:00	SuperLab Tabletting Camera loudness detected
2018-05-17T10:28:50+02:00	Kitchen's camera motion detected
2018-05-17T10:30:20+02:00	Kitchen's camera motion detected
2018-05-17T10:30:30+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:30:50+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:31:48+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:32:50+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:33:15+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:33:37+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:34:44+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T10:35:32+02:00	SuperLab Tabletting Camera loudness detected
2018-05-17T10:35:53+02:00	Kitchen's camera motion detected
2018-05-17T10:36:06+02:00	SuperLab Kitchen Nest Protect (LabSmoker) smoke_detected detected
2018-05-17T10:36:20+02:00	SuperLab Kitchen Nest Protect (LabSmoker) smoke_detected detected
2018-05-17T10:38:52+02:00	Kitchen's camera motion detected
2018-05-17T11:41:54+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T12:03:44+02:00	SuperLab Tabletting Camera capturing_video detected
2018-05-17T12:16:59+02:00	SuperLab Tabletting Camera capturing_video detected
2018-05-17T14:52:30+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T14:56:06+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T15:31:11+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T15:40:21+02:00	SuperLab Tabletting Camera motion detected
2018-05-17T16:27:10+02:00	SuperLab Tabletting Camera motion detected

The Nest database records the information of the connected Nest devices and event log information. As a result of analyzing Nest database, Nest is linked with 'jpinkman2018@gmail.com' account, and connected IoT equipment is Nest camera and Nest smoke protector, and confirmed that two events were recorded on the day of fire alarm.

Table 28 Account information for Nest

User email	User Name
jpinkman2018@gmail.com	jpinkman2018@gmail.com

Table 29 IoT devices list connected with Nest application

Device type	Device name	IP address	Serial number
Smoke protector	LabSmoker	10.20.30.19	06CA01AC331600CA
Camera	Nest Cam	10.20.30.13	18b43061c9ef

Table 30 Smoke detection alarm history

Datetime	Device	Description
2018-05-17T10:36:06+02:00	LabSmoker	protect_smoke_warn
2018-05-17T10:36:20+02:00	LabSmoker	protect_smoke_warn_clear

Arlo stores image data obtained through the camera in the application cache. Saved image files allow analysis of the situation at a given time. after analyzing image data stored in application cache and Arlo database, event data was not present in Arlo database. but there are some image files associated with the raid created between 2018-05-17T09:39:42+02:00 and 2018-05-17T09:40:37+02:00. and the status of the drug lab at that time remains an image. after image file checking, we confirmed that there were three persons staying in the drag lab from 2018-05-17T09:39:42 to 2018-05-17T09:40:37 and that one of the persons seemed to touch the Nest Smoke Protector.

Table 31 Arlo Camera image files stored on cache directory

Image artifact path	HASH(SHA1)
/data/data/com.netgear.android/cache/http/fd6f9b0229627dbc749f065b67e0e72b.0	fd7586639530b209d935d768191fa7a5130c99d0
/data/data/com.netgear.android/cache/http/ab5bcbcbb566f0b349c419c5f8a1ccd5.0	fa7505b9aa1fe3290fd16c2201a103682419a53e
/data/data/com.netgear.android/cache/http/67f43186731b8ca1b0dbf25ec25c5391.0	f535416701419d31f97afd0d6c51bebea549326a
/data/data/com.netgear.android/cache/http/0860f6c5ed0c20de5694f7efd37b94c7.0	f4e0caa009d086cb28ea41d3cfa7c9f9b4ad9464
/data/data/com.netgear.android/cache/http/41593f144685f25ba6494ce186d1ff7a.0	dba7f96dab372c9bd73cd1b6bcfb84dcbd5cb3a1

/data/data/com.netgear.android/cache/http/60a62cffb138cfb578310f8d4fd7b5ed.0	d5b7a58a80ff6ef9bcd5d7a6cc0ae6d1ba44b9c7
/data/data/com.netgear.android/cache/http/b38300b666acf5a7d0f15b1acedb00ff.0	c6b1a8fcefa4d201806aba7d168ca5f5794e905f
/data/data/com.netgear.android/cache/http/92af7d396df2aa692712d3cedc7ce004.0	c0c90dca9fd5c6abe08391b3655075648e9a16a4
/data/data/com.netgear.android/cache/http/417919cda8816ff77ea730dc0038aef3.0	b8d0f2f101cc708a46b1d3703b22aed6999f3897
/data/data/com.netgear.android/cache/http/b1e95faf3a53a051e1a908bd41867c22.0	a67f1a2dc555038f1f9eaac730ec8652e032bea5
/data/data/com.netgear.android/cache/http/ad00d78eeeda8f0aa9f1f945bd65da2790f36f310c13062ca02e24c46ecbf090.0	a3670e0ef13c408e05e17f4f779445628163986a
/data/data/com.netgear.android/cache/http/dc7431626fd7335d0e5f7e8778cdac5b.0	8470674535878910c691400868fbde336c9e9857
/data/data/com.netgear.android/cache/http/969c056279300a23769121089553a78bf8bd518bb9d1803579e764a6100624c5.0	7af42472fe0b6e8c9f52e749e84e3c7db8ce4ee7
/data/data/com.netgear.android/cache/http/7884df1547cf2823c3142e9508eb8c3a.0	6c4ba214d13dff9e354b9d21f128ed8a6cc71c81
/data/data/com.netgear.android/cache/http/83b294d2d624ce46d4a2b14683c0896a.0	58f976dfb7903295d67a10b22f80b72b0fab8c94
/data/data/com.netgear.android/cache/http/983ec6abb50f05e3e68b7495cc704d66.0	4b8707bf7a18a97f65ed74bdb2734c8e44707b49
/data/data/com.netgear.android/cache/http/a52213fe457b9b76431d909d1bce6d7d.0	115d2101a6a4290b4b5d07bd76e3ee87d16ae0a6

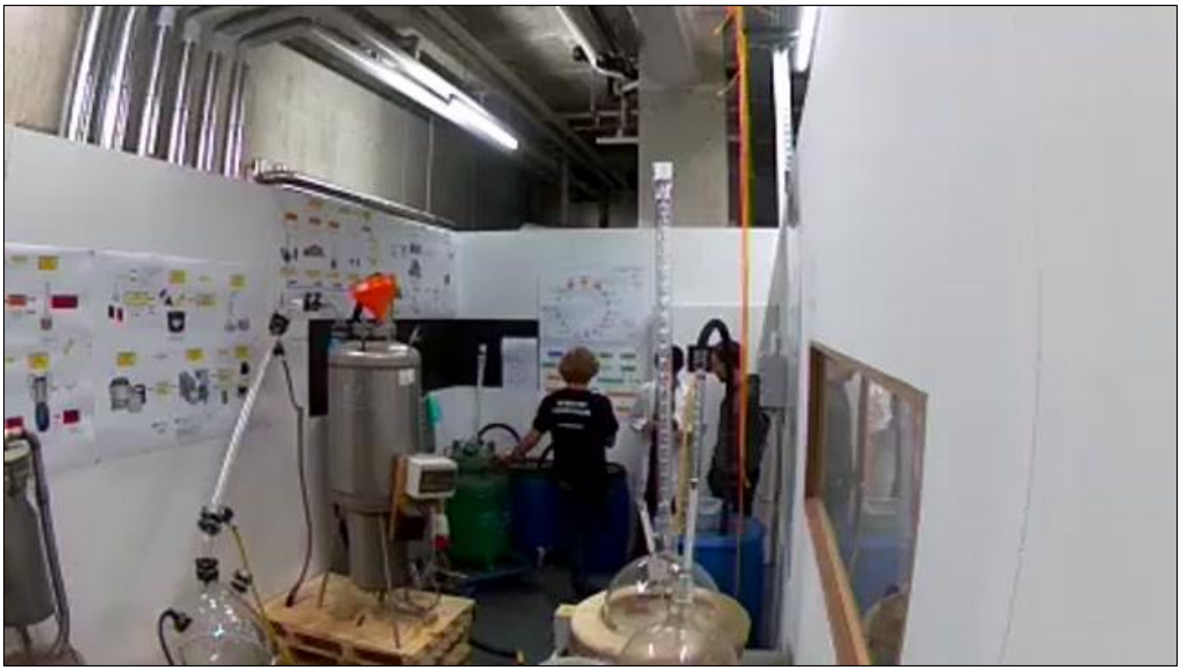


Figure 2 Three persons in drug lab

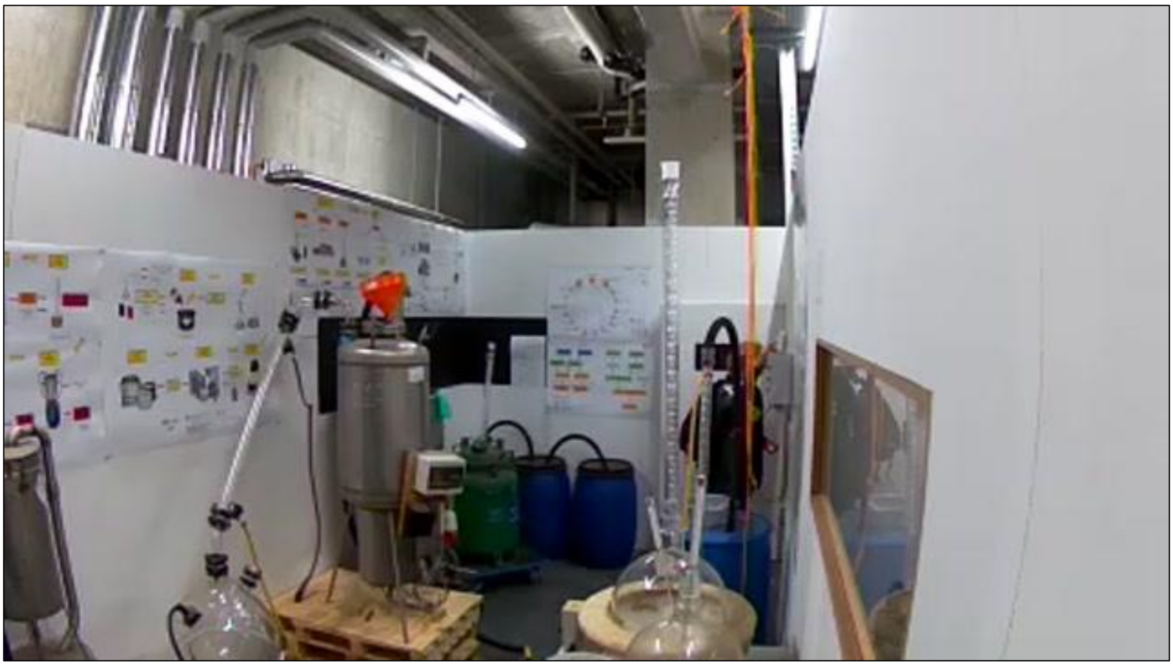


Figure 3 A person who touched Nest smoke protector(1)

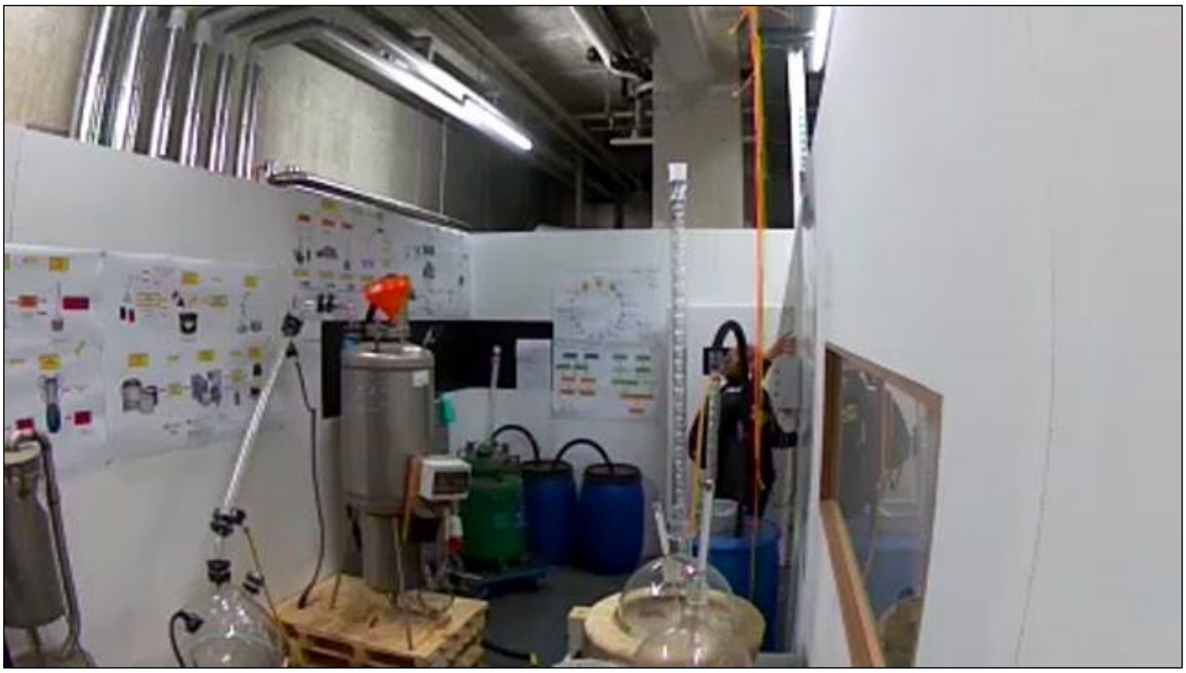


Figure 4 A person who touched Nest smoke protector(2)

There was no event data related to the incident in the QBee camera database. However, in 2018-05-17 when the incident occurred, we noticed the trace of running the QBee camera application on the Samsung Galaxy Edge S6. The artifacts about the execution trace are as follows.

Table 32 Qbee camera application usage history artifacts

Artifacts path	HASH(SHA1)
/data/system/recent_images/57_task_thumbnail.png	98c428fba7e38ec3c8a7d152a9c7c7272e163e5c
/data/system/recent_tasks/57_task.xml	510d780cba4dd5c73d75821753c98f160afefb74

Images stored in the recent_images directory store screens of recently executed applications, and the XML-formatted file in the recent_tasks directory contains timestamp to determine when the application was used. 57_task.xml shows that the QBee camera application was first run at 2018-05-17T15:36:04 and also runs at 2018-05-17T19:35:07. and 57_task_thumbnail.png shows the main activity of the Qbee camera application. The status of the QBee camera shown on the main activity is PRIVATE. This artifact can be used to estimate that the reason why the QBee camera is disabled is because the privacy mode is set in QBee camera.

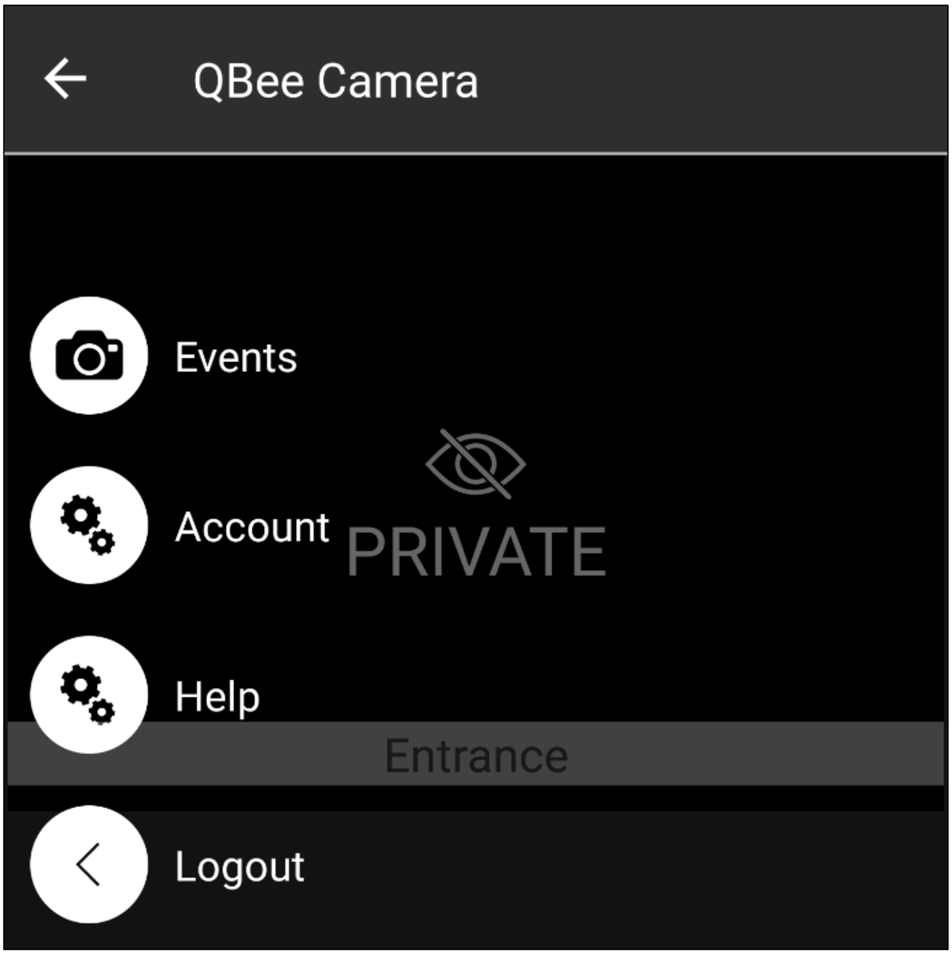


Figure 5 57_task_thumbnail.png

3.1.4.2Cloud analysis

IoT applications typically store user credentials within a device after the user's first successful login for ease of use. Cloud analysis for IoT applications can be performed using authentication information stored on the device for ease of use of IoT applications. In addition, Cloud analysis is also possible by obtaining user credentials from the authentication server through security vulnerabilities or by resetting the authentication information.

The IoT Cloud API can be obtained through data released on the homepage of each IoT device or by reverse engineering of IoT application.

In this case, the devices that have stored the credentials on Samsung Galaxy Edge S6 and were able to access and obtain data through the Cloud API are Amazon alexa echo, WinkHub, QBee camera, and iSmartAlarm.

The following is a Cloud API for checking information on each IoT device and event log.

Amazon alexa echo

Table 33 Amazon alexa echo cloud API list

API name	Protocol	Method	API url
History on voice	HTTP(s)	GET	https://pitangui.amazon.com/api/activities?startTime={}&size={}&offset=-1
Accessing to audio data(actual user's voice)	HTTP(s)	GET	https://pitangui.amazon.com/api/utterance/audio/data?id={originalAudioId or utteranceId}

WinkHub

Table 34 WinkHub cloud API list

API name	Protocol	Method	API url
Getting user information	HTTP(s)	GET	https://api.wink.com/users/me
Getting user activities	HTTP(s)	GET	https://api.wink.com/users/me/activities
Getting camera activities	HTTP(s)	GET	https://api.wink.com/cameras/{cameraID}/activities
Getting user wink devices with connected device	HTTP(s)	GET	https://api.wink.com/users/me/wink_devices/
Getting linked service information	HTTP(s)	GET	https://api.wink.com/users/me/linked_services/

Nest

Table 35 Nest cloud API list

API name	Protocol	Method	API url
Getting device information	HTTP(s)	POST	https://home.nest.com/api/0.1/user/9201208/app_launch
Getting clips	HTTP(s)	GET	https://webapi.camera.home.nest.com/api/v1/clips.get_visible_with_quota
Getting camera peroperties	HTTP(s)	GET	https://webapi.camera.home.nest.com/api/v1/cameras.get_owned_and_member_of_with_properties

iSmartAlram

Table 36 iSmartAlarm cloud API list

API name	Protocol	Method	API url
Itegration with alexa	HTTP(s)	POST	https://alexa.ismartalarm.com/api/echo_getconfig
Getting Home user	HTTP(s)	POST	https://api.ismartalarm.com:8443/api/GetHomeUser.htm
Getting Sensor state	HTTP(s)	POST	https://api.ismartalarm.com:8443/api/GetSensorStateEX.htm
Synchronizing user	HTTP(s)	POST	https://api.ismartalarm.com:8443/api/user_sync.htm
Getting control sensor log	HTTP(s)	POST	https://api.ismartalarm.com:8443/api/GetContoSensorLogs
Getting sensor log	HTTP(s)	POST	https://api.ismartalarm.com:8443/api/AppDownloadSensorData.htm

Qbee

Table 37 Qbee camera cloud API list

API name	Protocol	Method	API url
Getting camera information	HTTP(s)	GET	https://hma.vestiacom.com/app/hm/ld?class=camera
Getting camera settings	HTTP(s)	GET	https://hma.vestiacom.com/app/hm/ld/{id}/settings
Getting recoding status	HTTP(s)	GET	https://hma.vestiacom.com/app/hm/ld/recordingStatus
Getting event logs	HTTP(s)	GET	https://hma.vestiacom.com/app/hm/eventPage
Getting last snapshot	HTTP(s)	GET	https://hma.vestiacom.com/app/snapshot/last
Getting user information	HTTP(s)	GET	https://hma.vestiacom.com/app/hm/user

We analyze the event corresponding to 2018-05-17, which is the date of occurrence of the fire alarm among the responses of Cloud API for each device. As a result of the analysis, we confirmed that most of the events are consistent with the information obtained from the device analysis.

After checking the Amazon alexa echo voice command data recorded in the cloud on 2018-05-17, we confirmed 2 unidentified persons that Amazon alexa echo performed voice commands. Table 38 is User voice command history.

Table 38 User voice command history

Device name	User voice command	Pereson
2018-05-17T10:16:09+02:00	alexa play led zeppelin	Person A
2018-05-17T10:22:13+02:00	tell i. smart alarm to arm my system	Person B
2018-05-17T10:22:20+02:00	Yes	Person B

Information of devices connected to WinkHub using WinkHub 's Cloud API and event details recorded at the time of fire alarm are as follows.

Table 39 Linked services list

Linked service id	Service
815083	google now
1044126	arlo
1044132	nest
1044134	amaon_alexa

Table 40 Linked services list

Object id	Object type	Model name	Name
421391	hub	Hub	Wink
1700816	light_bulb	Cree light bulb	Piano
1889042	light_bulb	Cree light bulb	Upstairs
212474	smoke_detector	Protect	SuperLab Kitchen Nest Protect (LabSmoker)
235946	camera	Nest Cam	SuperLab Tabletting Camera
237267	camera	Arlo Pro	Kitchen's camera

Table 41 Event records of IoT devices Integrated into WinkHub

Datetime	Description
2018-05-17T10:10:11+02:00	Kitchen's camera detected motion

2018-05-17T10:10:45+02:00	Kitchen's camera detected motion
2018-05-17T10:14:05+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:14:12+02:00	Kitchen's camera detected motion
2018-05-17T10:15:01+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:15:56+02:00	Kitchen's camera detected motion
2018-05-17T10:15:59+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:17:00+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:22:36+02:00	SuperLab Tabletting Camera detected noise started
2018-05-17T10:28:51+02:00	Kitchen's camera detected motion
2018-05-17T10:30:21+02:00	Kitchen's camera detected motion
2018-05-17T10:30:30+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:30:50+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:31:48+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:32:51+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:33:15+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:33:37+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:34:44+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:35:32+02:00	SuperLab Tabletting Camera detected noise started
2018-05-17T10:35:53+02:00	Kitchen's camera detected motion
2018-05-17T10:36:06+02:00	SuperLab Kitchen Nest Protect (LabSmoker) detected smoke
2018-05-17T10:36:20+02:00	SuperLab Kitchen Nest Protect (LabSmoker) All is well
2018-05-17T10:38:52+02:00	Kitchen's camera detected motion
2018-05-17T11:41:55+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T12:03:45+02:00	SuperLab Tabletting Camera stopped capturing video
2018-05-17T12:17:00+02:00	SuperLab Tabletting Camera started capturing video
2018-05-17T14:52:31+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T14:56:06+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T15:31:11+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T15:40:21+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T16:27:10+02:00	SuperLab Tabletting Camera detected motion

In case of WinkHub, we confirmed that the event information obtained from the Cloud API and the event acquired from the database of the Samsung Galaxy Edge S6 WinkHub application are the same.

The information that can be obtained from the Nest Cloud API is the information of the device connected with the information of the Nest structure. You can also acquire the event history from the connected device and view the video called Nest Clip. Therefore, we confirmed the Nest Clip video, but there were no video clips recorded in 2018-05-17 when the fire alarm occurred.

Table 42 Nest structure and Nest devices linked to Nest structure

Device type	Device name	IP address	Serial number
Nest structure	SuperLab	N/A	D5ADFDD334DA2AA2
Smoke protector	LabSmoker	10.20.30.19	06CA01AC331600CA
Camera	Nest Cam	10.20.30.13	18b43061c9ef

Table 43 Event Records of Nest smoke protector

Datetime	Device	Description
2018-05-17T10:36:06+02:00	LabSmoker	protect_smoke_warn
2018-05-17T10:36:20+02:00	LabSmoker	protect_smoke_warn_clear

Table 44 Nest camera clips list

Datetime	Title	Clip download url
2018-05-30T15:09:46+02:00	N/A	https://clips.dropcam.com/baf574c9fee24b7da8ab68340622893c.mp4
2018-05-30T15:10:34+02:00	Loric	https://clips.dropcam.com/bc6ce1cab6894c6b9922b7e1d40af1db.mp4
2018-05-30T11:42:39+02:00	Dardan	https://clips.dropcam.com/112e871ffe9d4b6caf6f6faa87e3549c.mp4
2018-05-31T10:41:05+02:00	Mariam	https://clips.dropcam.com/af6b3cbedde943789f417b651c5a1ac2.mp4
2018-05-31T08:50:17+02:00	Virginie R	https://clips.dropcam.com/725645080ef54ec5b5daecc105e99209.mp4
2018-05-31T08:52:10+02:00	Virginie R	https://clips.dropcam.com/7e7cbe13c5d0467da0a333d0c027d2b7.mp4

Analysis of SmartAlarm in the cloud, the members registered in the Drug lab were identified as JPinkman and pandadodu, and SmartAlarm was confirmed to be linked with Amazon alexa echo.

Table 45 iSmartAlarm members of drug lab

Nicname	Userid	User name	userright
JPinkman	200873	+41_0792245315	2 (Superuser)
pandadodu	211324	+39_3662158453	1 (Member)

Table 46 iSmartAlarm Integration information

DisarmPasscode	HasEcho
5164	1

We analyzed the cloud about QBee and confirmed the camera information. However, there was no event in 2018-05-17 that occurred on the day of fire alarm.

Table 47 Qbee camera information

lanDeviceId	Model	Name	Owner email
14887	HM Camera	Entrance	jpinkman2018@gmail.com

3.2 iSmartAlarm base station images & diagnosic logs

Diagnostic logs are recorded as binary streams and consist of each record. Each record consists of the Tag data, which means a specific action, and the Value, which means the actual data value. We extracted iSmartAlarm binaries from base station images to write values in Diagnostic log logs using "binwalk" to identify the meaning of Tag data and to develop scripts that can parsing Tag and Value, and reverse engineering them.

The hash of the iSmartAlarm binary writing values in the Diagnostic log is as follows.

Table 48 iSmartAlarm artifacts to analyze

Artifact path	Hash(SHA1)
/diagnostics/2018-05-17T10_54_28 /server_stream	8f9310041c5a705fcb171bd4c4d9a4740e61d014
/dump/ismart_00.img	799f30ffbdfb7d0a436cc0600be9b5d05287feeb
/dump/ismart_80.img	799f30ffbdfb7d0a436cc0600be9b5d05287feeb
/sbin/iSmartAlarm	8b1dac730d84b29f9c84187c6a620c102d5f68db

We confirmed the meaning of the tag written in the diagnostic log by reverse engineering for iSmartAlarm binary.

The following are the Tags that are classified as meaningful to the analysis in this case.

Table 49 Meaningful tag list

Tag	Tag type	Tag description
MODEID	Device status/ARM MODE	Change Alarm (mode id) , Monitoring

		mode id status description
RC3OP	Communication with Remote controller	RC3 Operation description log
ALARMDOOR	Alarm/Door	Door open/close alarm description log
SIRENOP	Setting Monitoring status, Alarm/Siren	Setting siren, Monitoring siren status, Alarm with siren
ALARMPIR	Alarm/Motion sensor(PIR)	Alarm status with motion sensor
AHCR	Setting, Monitoring/AOHOME	Check if rc3 is in home and modify AOHOME list

Table 50 is that based on the tag information in Table 49, information of the time (2018-05-17) when the fire alarm occurred in Diagnostics log among the events recorded in iSmartAlarm.

Table 50 diagnostic log on 2018-05-17

Datetime	Tag	Description
2018-05-17T09:44:53+02:00	ALARMDOOR	Door is open, and send to cloud
2018-05-17T09:45:21+02:00	AHCR	A RC3 change be in home
2018-05-17T09:45:22+02:00	RC3OP	Alarm mode is changed to DISARM by remote tag
2018-05-17T09:45:22+02:00	RC3OP	Alarm mode is changed to DISARM by remote tag
2018-05-17T09:47:18+02:00	ALARMDOOR	Door is closed, and send to cloud
2018-05-17T09:47:50+02:00	MODEID	Alarm mode is changed to ARM by User
2018-05-17T10:09:52+02:00	ALARMDOOR	door is open, and send to cloud
2018-05-17T10:09:55+02:00	ALARMDOOR	door is open, and send to cloud
2018-05-17T10:09:55+02:00	ALARMPIR	Motion sensor(PIR) triggered and send to cloud
2018-05-17T10:09:57+02:00	RC3OP	Alarm mode is changed to DISARM by remote tag
2018-05-17T10:09:57+02:00	RC3OP	Alarm mode is changed to DISARM by remote tag
2018-05-17T10:22:21+02:00	MODEID	Alarm mode is changed to ARM by User
2018-05-17T10:22:23+02:00	AHCR	A RC3 change be out home
2018-05-17T10:22:30+02:00	RC3OP	Alarm mode is changed to DISARM by remote tag
2018-05-17T10:34:15+02:00	ALARMDOOR	Door is closed, and send to cloud
2018-05-17T10:34:17+02:00	RC3OP	Alarm mode is changed to HOME by remote tag
2018-05-17T10:34:17+02:00	RC3OP	Alarm mode is changed to HOME by remote tag
2018-05-17T10:34:31+02:00	MODEID	Alarm mode is changed to DISARM by User
2018-05-17T10:34:36+02:00	ALARMDOOR	Door is open, and send to cloud
2018-05-17T10:34:36+02:00	SIRENOP	Door is open, all the siren need doorbell!!!

As a result of analyzing the event, Most of the events were consistent with data from the iSmartAlarm application database on the Samsung Galaxy Edge S6. However, the additional event identified in the Diagnostic log is the event that the remote controller, TheBoss, is located in the Drug lab, and the siren is activated at the same time the door is opened.

3.3 Arlo Memory Image & NVRAM settings & NAND

Alro Memory Image, NVRAM settings, and NAND not only record basic and setup information for the devices connected to Arlo base station and Arlo base station information but also event log and update log generated from Arlo base station. The details of classifying information identified through Arlo Memory, NVRAM settings and NAND data are as follows.

Table 51 Arlo artifacts to analyze

Artifact path
/media/nand/vzdaemon/conf/*
/media/nand/log-archive/*

Data related directly to this event did not exist through Arlo Memory Image, NVRAM settings, and NAND. Basic information and setup information for Arlo base station and camera that may be of indirect help to this event analysis have been identified.

Table 52 Arlo base station & Arlo camera's basic information

Category	Category detail		Values
Camera	ID		59U17B7BB8B46
	modelID		VMC4030
	MAC address		08028EFDBDCD
	Rule 1	Trigger1	PIR motion active
	Rule 1	Action1	Record video by 59U17B7BB8B46
	Rule 1	Action2	Push notification
	Rule 2.	Trigger1	Audio amplitude
	Rule 2.	Trigger2	PIR motion active
	Rule 2.	Action1	Record video by 59U17B7BB8B46

	Rule 2	Action2	Push notification
Base station	Object version		2.0
	Timezone		CET-1CEST,,M3.5.0,M10.5.0/3
	olsonTimezone		CET-1CEST,,M3.5.0,M10.5.0/3
	IP address		10.20.30.17
	MAC address		B827EB0E3B45

As a result of confirmation, the MAC address of Arlo camera and base station is 08028EFDBCD and B827EB0E3B45 respectively. Camera is connected to Arlo base station. Camera is set up to capture images with an alarm if an action is detected by the motion sensor, and if an audio alarm is detected.

3.4 WinkHub file system

The WinkHub file system stores the network information that the WinkHub connects to, the device information that is connected directly to the WinkHub, and events that occur on the WinkHub device.

Analysis of the WinkHub File system confirmed that no events related directly to this case were identified, but data that could be used indirectly for analysis of this case.

Artifacts collected by WinkHub are as follows:

Table 53 WinkHub artifacts to analyze

Artifact path	Hash(SHA1)
/database-default/db-backup/apron.db	b23e4be3d6dd34b1fcf091dba1ac10d7c96de349
/database-default/db-backup/bd_addr	ac668c86ac009fcba4cd37922c7985991d10247b
/database-default/db-backup/wpa_supplicant.conf	748f60eb52b0d33f00c08cac2b70fe8358dbd038
/tmp/all.log	d7f9712b5969294edeb0a71ae1e0ebe19c3ac97f
/tmp/all.log.1	6cae9c2eae086973203ebe65b05f694eb7b7a069
/tmp/all.log.2	a1aa1a512220896549d551b85db415b6b6b81fc2

Analysis of the above artifacts confirmed that two HA On / Off Light type Cree lightbulbs connected by ZIGBEE are directly connected to WinkHub.

Table 54 Devices connected to WinkHub directly

Interconnect	deviceType	ManufacturerName
ZIGBEE	HA On/Off Light	Cree
ZIGBEE	HA On/Off Light	Cree

Also, the network information of WinkHub can be checked through ‘wpa_supplicant.conf’ and ‘bd_addr’. As a result of checking theses files, there is a trace that WinkHub connected to ESC-IoT network, and the MAC address of Bluetooth adadpter is 00: 21: CC: 09: B7: C9.

Table 55 WinkHub’s network information

Category		Description
Connected wifi	SSID	ESC-IoT
	PSK	esc_iot_2018
Bluetooth	MAC address	00:21:CC:09:B7:C9

3.5 Amazon Echo

The data collected by Amazon Echo includes the user's voice command to Amazon Echo, and Amazon Echo's response to that voice command, as well as shopping history and to-do history.

We analyzed the Amazon Echo data and analyzed the events recorded at the time of the fire alarm (2018-05-17) in this case.

Table 56 Amazon Echo artifacts to analyze

Artifact path	Hash(SHA1)
/(2018-07-01_13.17.01)_CIFT_RESULT/cift_amazon_alexa_TIMELINE.csv	2aa4c211a3fc12c8740a49fb64fc6d959e5a1a9f
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/1840d4712abb8ed67fd2acf76f7c3e1d2b56a11d.json	adaccfbc7e3d4dbe5d310caefe61861e8147baf5
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/ce9240f8f4e8944dfec2ca8f607e451e4d03a474.json	b2266d44904fcfefc25c122042cc89c01db3e9e3
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/082a17905eb233a9863b97ec9f6b5b8970191fbf.json	82b74d65bf1408a7720d246aa586b4174602eb26

/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/690f40fd0a6c6c1a38f32b97b16cec05d1c22cc0.json	4e0a55ed534d8ca7a8b007aa7aca98a2e6f8420f
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/a586bfe14661258f0953aba910cd83519d890bfc.json	9ee0e96cab067b547234364350b8befbfab9430e
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/0305c1b97c035364db7251e540c2cb39b9976091.json	0a0657dbc3e02f25f998fe659b5a170098a944a8
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/VOICE/(2018-05-17T10_16_07+0200)_TEXT(alexa play led zeppelin).wav	445521de048bbdc713a134e35eab9f76febab79c
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/VOICE/(2018-05-17T10_22_08+0200)_TEXT(alexa).wav	2787c47a2de131ae94a6cb9cbef062e014438aca
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/VOICE/(2018-05-17T10_22_08+0200)_TEXT(tell i. smart alarm to arm my system).wav	965acfa172865bbcb256aedf1564f207f61d5117
/(2018-07-01_13.17.01)_CIFT_RESULT/Evidence_Library/AmazonAlexaCloud/VOICE/(2018-05-17T10_22_18+0200)_TEXT(yes).wav	4eac47985d16f07e9a9061626af43363f47c0807

Table 57 User voice command and Amazon Echo's response

Datetime	Description	Notes	Person
2018-05-17T10:16:09+02:00	alexa play led zeppelin	User's command	Person A
2018-05-17T10:16:09+02:00	To play Spotify, link your premium account first using the Alexa App.	Alexa's answer	N/A
2018-05-17T10:22:09+02:00	alexa	User's command	Person B
2018-05-17T10:22:12+02:00	tell i. smart alarm to arm my system	User's command	Person B
2018-05-17T10:22:14+02:00	Your Door is open, Are you sure you want to arm your system?	Alexa's answer	N/A
2018-05-17T10:22:19+02:00	yes	User's command	Person B
2018-05-17T10:22:21+02:00	Your system will set to Arm in 30 seconds.	Alexa's answer	N/A

Analysis of Amazon alexa's voice command data confirmed that two people gave voice commands between 2018-05-17T10:16:09+02:00 and 2018-05-17T10:22:21+02:00. The presence of two persons in the drag lab before the time of the fire alarm, 2018-05-17T10:36:06+02:00, indicates the need for further identification of the two persons in the drag lab and their activities.

3.6 Network packet capture

In this case, we analyze the network packet capture to check the QBee camera disabling method. Analysis of the network packet capture file is performed by establishing the following goals.

- Device identification by internal network IP address
- Analysis of Qbee camera feature
- Analysis of Qbee camera packet
    - Check Qbee camera shutdown
    - Check Qbee camera packet feature
- Suggerst Qbee camera disable method

Table 58 Network packet capture to analyze

Artifact path	Hash(SHA1)
/dfrws_police.pcap	bea1681c40c6b7a9e7835e1060ef2c86a35c7c32

To identify devices by internal network IP address, we confirmed 26 captured IP addresses using Wireshark's Endpoimt statistical function. Of the 26 IP addresses, the private IP address was filtered to identify the internal network IP used in the network of the drug lab. As a result, 8 private IP addresses were confirmed.

Table 59 Private network IP/MAC addresse

IP address	MAC address	Count	Percent
10.20.30.1	B8:27:EB:0E:3B:45	84	1.99%
10.20.30.13	18:B4:30:61:C9:EF	3922	92.74%
10.20.30.15	D8:FB:5E:E1:01:92	113	2.67%
10.20.30.17	08:02:8E:FF:75:4F	14	0.33%
10.20.30.19	18:B4:30:99:9F:85	4	0.09%
10.20.30.21	AC:5F:3E:73:E3:78	125	2.96%

10.20.30.22	B4:79:A7:25:02:FA	11	0.26%
10.20.30.23	74:75:48:96:23:24	32	0.76%

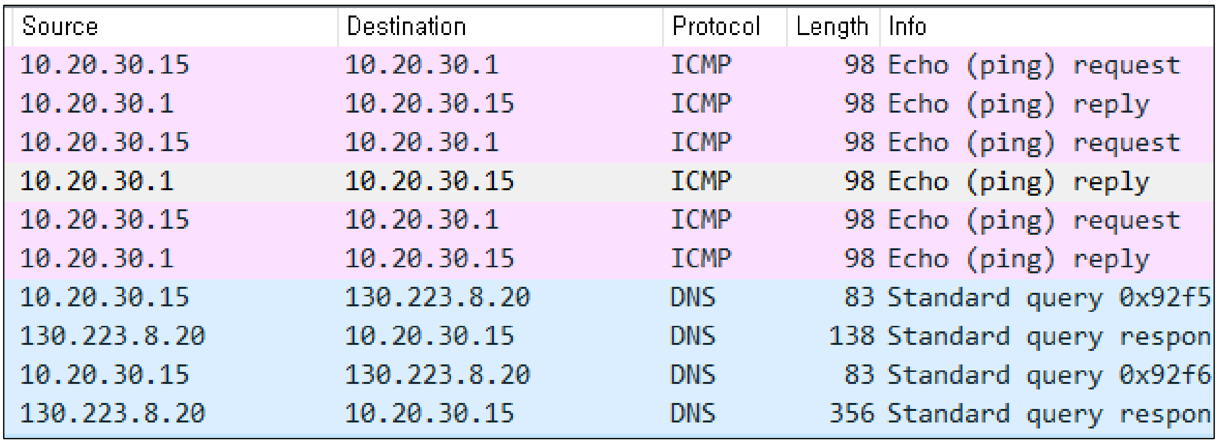
The device corresponding to each IP address can be checked using the vendor information of MAC address and MAC address by IoT device acquired by performing Device level analysis for Samsung Galaxy Edge S6.

Table 60 Devices by IP/MAC address

IP address	MAC address	Device
10.20.30.1	B8:27:EB:0E:3B:45	Drug lab Router
10.20.30.13	18:B4:30:61:C9:EF	Nest cam A0005
10.20.30.15	D8:FB:5E:E1:01:92	QBee camera
10.20.30.17	08:02:8E:FF:75:4F	Arlo base station
10.20.30.19	18:B4:30:99:9F:85	Nest smoke protecter
10.20.30.21	AC:5F:3E:73:E3:78	JPinkman Samsung Galaxy Edge S6
10.20.30.22	B4:79:A7:25:02:FA	WinkHub
10.20.30.23	74:75:48:96:23:24	Amazon alexa echo

According to the above results, QBee camera' IP address is 10.20.30.15 and MAC addressid D8:FB:5E:E1:01:92.

We confirmed the packet of QBee camera to check whether QBee camera works. As a result, the QBee camera was normally communicating with the destination IP. This means that the QBee camera is not shut down.

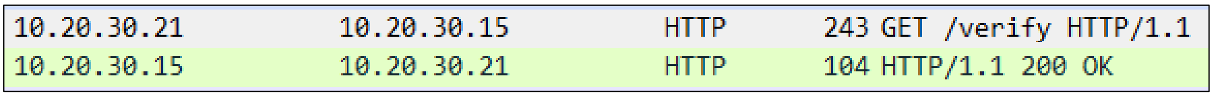


```
Source          Destination     Protocol  Length Info
10.20.30.15     10.20.30.1      ICMP          98 Echo (ping) request
10.20.30.1      10.20.30.15     ICMP          98 Echo (ping) reply
10.20.30.15     10.20.30.1      ICMP          98 Echo (ping) request
10.20.30.1      10.20.30.15     ICMP          98 Echo (ping) reply
10.20.30.15     10.20.30.1      ICMP          98 Echo (ping) request
10.20.30.1      10.20.30.15     ICMP          98 Echo (ping) reply
10.20.30.15     130.223.8.20    DNS           83 Standard query 0x92f5
130.223.8.20    10.20.30.15     DNS          138 Standard query respon
10.20.30.15     130.223.8.20    DNS           83 Standard query 0x92f6
130.223.8.20    10.20.30.15     DNS          356 Standard query respon
```

Figure 6 QBee camera's successful network communication

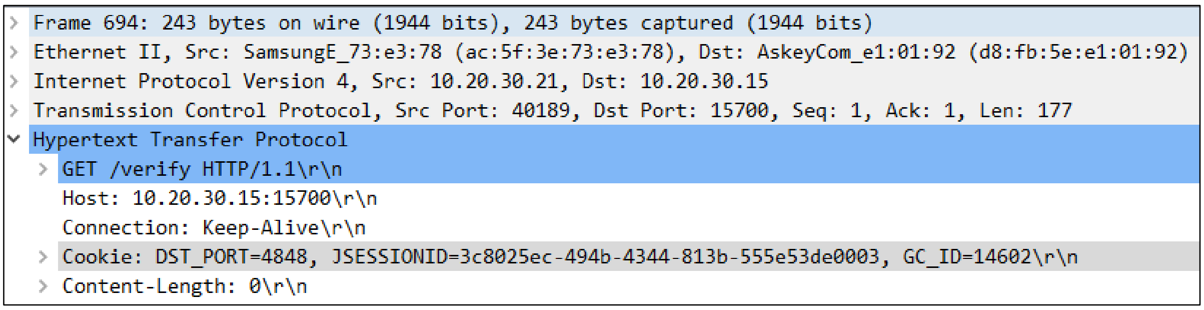
As a result of checking the packet using the API of QBee camera,e confirmed that API command of Qbee camera uses HTTP protocol.

As a result, the credential information of the API user is exposed as plain text to other persons. As a result, another person located on the internal network can sniff packet information between the QBee camera and the API user, and then API commands can be done to the QBee camera using the API user's authentication information.



```
10.20.30.21          10.20.30.15          HTTP       243 GET /verify HTTP/1.1
10.20.30.15          10.20.30.21          HTTP       104 HTTP/1.1 200 OK
```

Figure 7 QBee camera API packets



```
> Frame 694: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
> Ethernet II, Src: SamsungE_73:e3:78 (ac:5f:3e:73:e3:78), Dst: AskeyCom_e1:01:92 (d8:fb:5e:e1:01:92)
> Internet Protocol Version 4, Src: 10.20.30.21, Dst: 10.20.30.15
> Transmission Control Protocol, Src Port: 40189, Dst Port: 15700, Seq: 1, Ack: 1, 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
  > Cookie: DST_PORT=4848, JSESSIONID=3c8025ec-494b-4344-813b-555e53de0003, GC_ID=14602\r\n
  > Content-Length: 0\r\n
```

Figure 8 QBee camera API packet

As a characteristic of QBee camera, there is a privacy mode called privacy mode. If paivacy mode is executed on the QBee camera, the live camera will be stopped. he privacy mode of QBee camera can be set using the QBee camera config API or the Privacy button attached to the top of the QBee camera. However, since the QBee camera config API is designed for use on the internal network, users using the API should be located on the same network as QBee camera.

It is possible that the QBee camera in this case was operating in privacy mode through the results of checking the packet of QBee camera and the characteristics of QBee camera. If QBee camera was not set to Privacy mode through the Privacy mode button, a person who can access the internal network used the QBee camera config API by stealing JPinkman's authentication information, which means switching QBee camera to Private mode.

D.Pandana and S.Verga stated that they had access to the Wifi network of drug lab. Therefore, if QBee camera is not set to Privacy mode through the Privacy mode button, and if no other persons connected to Drug lab's Wifi network except D.Pandana and S.Verga, D.Pandana or S.Verga are the persons who made QBee disable.

4 Timeline analysis

Using the analysis of each device using the Device level analysis and Cloud level analysis methods, the following events were organized in chronological order from the initial event that occurred at 2018-05-17 on the day of the fire alarm to 2018-05-17T10:45+02:00 when the police visited the scene of the incident

Table 61 Timeline for Drug lab case

Datetime	Description
2018-05-17T09:44:53+02:00	Door is opened
2018-05-17T09:45:21+02:00	A RC3[TheBoss] change be in home
2018-05-17T09:45:22+02:00	iSmartAlarm alarm mode is changed into DISARM by [TheBoss]
2018-05-17T09:47:18+02:00	Door is closed
2018-05-17T09:47:50+02:00	iSmartAlarm alarm mode is changed into ARM by [Jpinkman]
2018-05-17T10:09:52+02:00	Door is opened
2018-05-17T10:09:55+02:00	Motion detected
2018-05-17T10:09:55+02:00	Door is opened
2018-05-17T10:09:57+02:00	iSmartAlarm alarm mode is changed into DISARM by [TheBoss]
2018-05-17T10:10:11+02:00	Kitchen's camera detected motion
2018-05-17T10:10:45+02:00	Kitchen's camera detected motion
2018-05-17T10:14:05+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:14:12+02:00	Kitchen's camera detected motion
2018-05-17T10:15:01+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:15:56+02:00	Kitchen's camera detected motion
2018-05-17T10:15:59+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:16:09+02:00	Amazon alaxa echo user void command "alexa play led zeppelin" by [Person A]
2018-05-17T10:16:09+02:00	Amazon alexa echo response "To play Spotify, link your premium account first using the Alexa App."
2018-05-17T10:17:00+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:22:09+02:00	Amazon alexa echo user void command "alexa" by [Person B]
2018-05-17T10:22:12+02:00	Amazon alexa echo user void command "tell i. smart alarm to arm my system" by [Person B]
2018-05-17T10:22:14+02:00	Amazon alexa echo response "Your Door is open, Are you sure you want to arm your system?"
2018-05-17T10:22:19+02:00	Amazon alexa echo user void command "Yes" by [Person B]
2018-05-17T10:22:21+02:00	Amazon alexa echo response "Your system will set to Arm in 30 seconds."

2018-05-17T10:22:22+02:00	**iSmartAlarm alarm mode is changed into ARM by [Jpinkman]**
2018-05-17T10:22:23+02:00	**A RC3[TheBoss] change be out home**
2018-05-17T10:22:30+02:00	iSmartAlarm alarm mode is changed into DISARM by [TheBoss]
2018-05-17T10:22:36+02:00	SuperLab Tabletting Camera detected noise started
2018-05-17T10:28:51+02:00	Kitchen's camera detected motion
2018-05-17T10:30:21+02:00	Kitchen's camera detected motion
2018-05-17T10:30:30+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:30:50+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:31:48+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:32:51+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:33:15+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:33:37+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:34:15+02:00	Door is closed
2018-05-17T10:34:17+02:00	**iSmartAlarm alarm mode is changed into HOME by [TheBoss]**
2018-05-17T10:34:31+02:00	iSmartAlarm alarm mode is changed into DISARM by [pandadodu]
2018-05-17T10:34:36+02:00	Door is open, all the siren need doorbell!!!
2018-05-17T10:34:44+02:00	SuperLab Tabletting Camera detected motion
2018-05-17T10:35:32+02:00	SuperLab Tabletting Camera detected noise started
2018-05-17T10:35:53+02:00	Kitchen's camera detected motion
2018-05-17T10:36:06+02:00	**SuperLab Kitchen Nest Protect (LabSmoker) detected smoke**
2018-05-17T10:36:20+02:00	SuperLab Kitchen Nest Protect (LabSmoker) All is well
2018-05-17T10:37:52+02:00	iSmartAlarm alarm mode is changed into DISARM by [pandadodu]
2018-05-17T10:38:52+02:00	Kitchen's camera detected motion

The above timeline was analyzed to derive the timing and related persons of the drug lab raid, and details of the need for further analysis were identified.

4.1 The time when drug lab is raided and relevant person

The time when the drug lab was raided was 2018-05-17T10:34:36+02:00 and the person involved in the raid is the person using the pandadodu account. events related to this include:

1) At 2018-05-17T10:34:17+02:00 JPinkman changed the alarm mode of the drag lab to HOME mode.
2) At 2018-05-17T10:34:31+02:00 the users of the pandadodu changed the alarm mode of the drag lab to DISARM.

3) At 2018-05-17T10:34:36+02:00 the door of the drag lab opened and siren occurred.
4) Motion and noise were detected from 2018-05-17T10:34:44+02:00 to 2018-05-17T10:35:53+02:00 after the door of the drag lab was opened.
5) A fire alarm was issued at 2018-05-17T10:36:06+02:00.

Based on the above events, the reasons for determining the time of the raid and the relevant person are as follows.

1) When JPinkman was staying in the drag lab, the alarm mode of the drag lab was changed to DISARM
2) When the alarm mode is DISARM and the door has been opened, the siren has occurred.
3) Continuous detection of movement and noise for approximately 1 minute

Based on the above evidence, the person involved in this case is pandadodu, who turned alarm mode HOME into DISARM at 2018-05-17T10:34:31+02:00 and the raid occurred at 2018-05-17T10:34:36+02:00.

4.2 The identity of pandadodu

It is difficult to identify the users of the pandadodu account using only the results of this analysis. However, it is possible to estimate the identity of the pandadodu through facts and evidence data that indirectly help identify the pandadodu.

pandadodu is a person who has a close relationship with JPinkman.

The following is the reasons for estimating the pandadodu as a person with close ties to JPinkman.

1) In iSmartAlarm, pandadodu is registered as a member of the drug lab.
2) Member registration of iSmartAlarm should scan specific QR code that is output to the cell phone of the person with superuser authority.
3) To use the QBee camera remote control vulnerability, which is one of the QBee camera disable reasons, it should be located on the same network as the QBee

camera to control the setting.

D.Pandana and S.Verga are related to pandadodu. The QBee camera has been switched to privacy mode for attack. If this is not the privacy mode via the QBee camera's privacy mode button, one of D.Pandana and S.Verga, who has access to the internal network, is the person associated with the pandadodu account.

If the pandadodu account is one of D.Pandana and S.Verga, the pandadodu account may be D.Pandana due to the similarity of the account name and name.

4.3 Some points requiring further analysis

4.3.1 The identity of pandadodu

This analysis does not provide clear evidence of the actual user of the pandadodu account at the time of the attack. Therefore, additional investigation is needed to identify the actual user of the pandadodu account at the time of the attack.

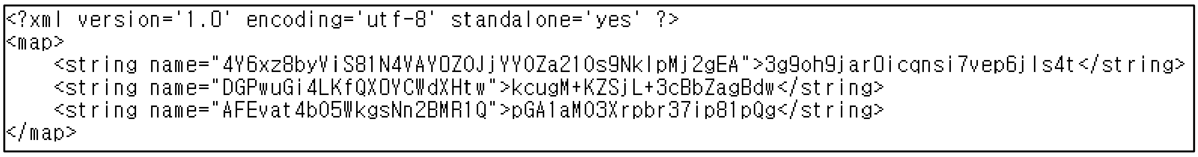
4.3.2 The identity of unidentified persons who stayed in the drug lab prior to the raid

The result of analyzing the voice commands performed by Amazon alexa echo, two people stayed in the drug lab before the raid (2018-05-17T10: 09: 52 + 02: 00-2018-08-05-17T10: 33: 37 + 02: 00). Therefore, it is necessary to investigate the identity of two unidentified persons and to investigate the connection with the raid case.

5 Appendix

5.1 QBee camera account information decryption method

QBee camera application installed on Samsung Galaxy Edge S6 stores encrypted user credential information for user convenience and this credential information is stored in Shared Preference directory as name of "com.vestiacom.qbeecamera_preferences.xml". therefore, It is possible to get credential information as plain text if only a user knows the decryption method.



```
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
    <string name="4Y6xz8byViS81N4VAYOZOJjYYOZa21Os9NklpMj2gEA">3g9oh9jar0icqnsi7vep6jls4t</string>
    <string name="DGPwuGi4LKfQXOYCWdXHtw">kcugM+KZSjL+3cBbZagBdw</string>
    <string name="AFEvat4b05WkgsNn2BMR1Q">pGA1aM03Xrpbr37ip81pQg</string>
</map>
```

Figure 9 Encrypted account information

5.1.1 Secret key generation algorithm

1) Getting a "preference key" in Shared preference directory.
2) Dividing "preference key" into half and put "a!k@ES2,g86AX&D8vn2]" between them.
3) Hashing the "preference key containing "a!k@ES2,g86AX&D8vn2]" value" with SHA256 hash algorithm.

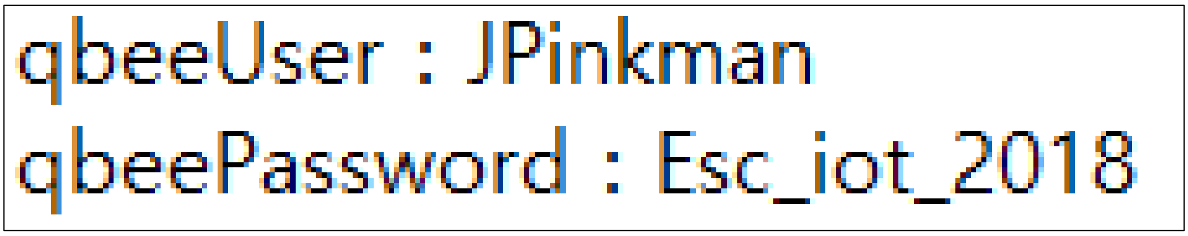
5.1.2 Decryption process

1) Getting secret key from "Secret key generation algorithm".
2) Decoding encrypted string to decrypt with base64 algorithm.
3) Decrypting encrypted string that is decoded base64 algorithm with secret key through AES(ECB mode) algorithm.
4) (Option) remove unnecessary padding within decrypted string.

5.1.3 POC of QBee account decryption

```
import base64
import hashlib

from Crypto.Cipher import AES

class QBeeCrypt():
    def __init__(self, key):
        self.key = key[:len(key)/2]
        self.key = self.key + 'a!k@ES2,g86AX&D8vn2]'
        self.key = self.key + key[len(key)/2:]
        # print self.key
        self.key = hashlib.sha256(self.key.encode('utf-8')).digest()

    @staticmethod
    def _unpad(s):
        return s[:-ord(s[len(s) - 1:])]

    def base64_decode(self, encoded):
        return base64.b64decode(encoded + ('=' * (len(encoded) % 4)))

    def decrypt(self, enc):
        enc = self.base64_decode(enc)
        cipher = AES.new(self.key, AES.MODE_ECB)
        dec = QBeeCrypt._unpad(cipher.decrypt(enc))
        return dec.decode('utf-8')
        # return dec

if __name__ == '__main__':

    qbee_cipher = QBeeCrypt('3g9oh9jar0icqnsi7vep6jls4t')

    print "%s : %s" % (qbee_cipher.decrypt('DGPwuGi4LKfQX0YCWdXHtw'), qbee_cipher.decrypt('kcugM+KZSjL+3cBbZagBdw'))
    print "%s : %s" % (qbee_cipher.decrypt('AFEvat4bO5WkgsNn2BMR1Q'), qbee_cipher.decrypt('pGA1aMO3Xrpbr37ip81pQg'))
```

Figure 10 POC python source code



```
qbeeUser : JPinkman
qbeePassword : Esc_iot_2018
```

Figure 11 Decrypted account information

5.2 Android device artifacts extractor

Android device artifacts extractor is a CLI tool to extract artifact from android physical image and categorizing extracted artifacts.

5.2.1 of Android device artifacts extractor development

1) There are few android device artifacts extractor for now.
2) Deployed Android device artifacts extractors are almost commercial for now.
3) Because of two reasons above, extracting artifacts from android device takes a lot of time.

5.2.2 Objectives of Android device artifacts extractor development

1) It has to have selective collect function according to further analysis objectives.
2) It has to have simple method of add/delete artifact to extract.
3) It has to have categorizing method according to artifact type.

5.2.3 Dependencies

Android device artifact extractor dependent on "**pytsk3**" python module

5.2.4 Command line

```
usage: Analysis android constant from physical image by @aiforensics
        python main.py [-h] -i [image path] [-m   [...]]

optional arguments:
  -h, --help              show this help message and exit
  -i [image path], --image_path [image path]
                          physical image path to analyze
  -m   [ ...], --module_tags   [ ...]
                        extraction/anaysis modules (ex. system/* app/browser/chrome)
```

5.2.5 module tags options

Android device artifacts extractor basically, provides 58 module tags. user can choose not only a module tag to extract relevant artifacts but some module tags whenever user need.

When user want to add or delete some other artifacts that is not provided by Android device artifacts extractor, user just write the artifact path into Android device artifacts extractor's artifacts repository.

Table 62 Android device artifacts extrator's Module tag list

Module type	Tag	Description
System module	system/*	Extracting all system artifacts
System module	system/basic	Extracting basic info artifacts
System module	system/network	Extracting network artifacts
System module	system/simcard	Extracting simcard artifacts
System module	system/settings/*	Extracting all settings artifacts
System module	system/settings/timezone	Extracting timezone artifacts
System module	system/settings/locale	Extracting locale artifacts
System module	system/accounts	Extracting accounts artifacts
System module	system/packages	Extracting packages artifacts
System module	system/software	Extracting software(build) artifacts
Usage modules	usage/*	Extracting all usage artifacts
Usage modules	usage/network	Extracting network usage artifacts
Usage modules	usage/usagestats	Extracting usage status artifacts
Usage modules	usage/procstats	Extracting process usage status artifacts
Usage modules	usage/batterystats	Extracting battery status artifacts
Usage modules	usage/notifications	Extracting notifications artifacts
Usage modules	usage/recent_activity	Extracing recent activity artifacts
Usage modules	usage/poweron	Extracting device poweron artifacts
Usage modules	usage/poweroff	Extracting device poweron artifacts
App modules	app/*	Extracting all app artifacts
App modules	app/communication/*	Extracting communication app artifacts
App modules	app/communication/contactprovider	Extracting contact provider artifacts
App modules	app/communication/sms	Extracting sms artifacts
App modules	app/communication/facebook	Extracting facebook artifacts
App modules	app/communication/telegram	Extracting telegram artifacts
App modules	app/communication/whatsapp	Extracting whatsapp artifacts
App modules	app/media/*	Extracting all media app artifacts
App modules	app/media/mediaprovider	Extracting media provider artifacts
App modules	app/media/samsungcmhprovider	Extracting samsung cmh provider artifacts
App modules	app/userinteraction/*	Extracting user interaction artifacts
App modules	app/userinteraction/userdictionary	Extracting userdictionary artifacts
App modules	app/iot/*	Extracting all iot app artifacts

App modules	app/iot/echo	Extracting echo artifacts
App modules	app/iot/ismartalarm	Extracting ismartalarm artifacts
App modules	app/iot/nest	Extracting nest artifacts
App modules	app/iot/arlo	Extracting arlo artifacts
App modules	app/iot/qbeecam	Extracting arlo artifacts
App modules	app/iot/wink	Extracting wink artifacts
App modules	app/mail/*	Extracting all mail app artifacts
App modules	app/mail/gmail	Extracting gmail artifacts
App modules	app/store/*	Extracting all store app artifacts
App modules	app/store/playstore	Extracting playstore artifacts
App modules	app/browser/*	Extracting all browser app artifacts
App modules	app/browser/chrome	Extracting chrome artifacts
App modules	app/clouddrive/*	Extracting cloud drive app artifacts
App modules	app/clouddrive/onedrive	Extracting onedrive artifacts
App modules	app/finder/*	Extracting all finder app artifacts
App modules	app/finder/samsungfinder	Extracting samsung finder artifacts
App modules	app/misc/*	Extracting all miscellenous app artifacts
App modules	app/misc/peelsmart	Extracting peelsmart artifacts
App modules	app/map/*	Extracting all map app artifacts
App modules	app/map/swissmapmobile	Extracting swissmapmobile artifacts
Media data modules	'media/*',	Extracting all media data artifacts
Media data modules	media/camera	Extracting camera media data artifacts
Media data modules	media/screenshot	Extracting screenshot media data artifacts
Media data modules	media/download	Extracting download media data artifacts
Media data modules	media/voice_recorder	Extracting void recorder media data artifacts
Media data modules	media/picture	Extracting picture media data artifacts

5.3 IoT Cloud API

5.3.1 Arlo camera Cloud API

Type	Method	URL	Description
Arlo camera	POST	https://arlo.netgear.com/hmsweb/login/v2	AUTHENTICATION
Arlo camera	GET	https://arlo.netgear.com/hmsweb/users/profile	GET PROFILE
Arlo camera	GET	https://arlo.netgear.com/hmsweb/users/session	GET SESSION
Arlo camera	GET	https://arlo.netgear.com/hmsweb/users/friends	GET FRIENDS
Arlo camera	GET	https://arlo.netgear.com/hmsweb/users/locations	GET USER LOCATIONS
Arlo camera	GET	https://arlo.netgear.com/hmsweb/users/serviceLevel/v2	GET SERVICE LEVEL
Arlo camera	GET	https://arlo.netgear.com/hmsweb/users/devices	GET DEVICES
Arlo camera	POST	https://arlo.netgear.com/hmsweb/users/library	GET LIBRARY
Arlo camera	GET	https://arlo.netgear.com/hmsweb/users/library/metadata/v2	GET LIBRARY METADATA
Arlo camera	GET	https://arlo.netgear.com/hmsweb/users/payment/offers	GET PAYMENT OFFERS
Arlo camera	GET	https://arlo.netgear.com/hmsweb/client/subscribe https://arlo.netgear.com/hmsweb/users/devices/notify	EVENT PUBLICATION AND SUBSCRIPTION
Arlo camera	POST	https://arlo.netgear.com/users/devices/notify/DEVICE_ID	ARMING/DISARMING SYSTEM

5.3.2 Nest Cloud API

Type	Method	URL	Description
Camera	GET	https://developer-api.nest.com/devices/cameras/{device_id}/device_id	Nest Cam unique identifier.
Camera	GET	https://developer-api.nest.com/devices/cameras/{device_id}/software_version	Software version.
Camera	GET	https://developer-api.nest.com/devices/cameras/{de	A unique, Nest-generated identifier that represents name, the display

		vice_id}/where_id	name of the device.
Camera	GET	https://developer-api.nest.com/devices/cameras/{device_id}/where_name	The display name of the device. Associated with the Nest Cam where_id. Can be any room name from a list we provide, or a custom name.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/name	Display name of the device; can be any room name from a list we provide, or a custom name.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/name_long	Long display name of the device. Includes a custom (label), created by the user, or via wheres.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/is_online	Device connection status with the Nest service.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/is_streaming	Camera status, either on and actively streaming video, or off.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/is_audio_input_enabled	Camera microphone status, either on and listening, or off. Learn more about Nest Cam audio settings.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_is_online_change	Timestamp that identifies the last change to the online status, in ISO 8601 format.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/is_video_history_enabled	Nest Aware subscription status (subscription active or not).
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/web_url	Web URL (deep link) to the live video stream at home.nest.com.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/app_url	App URL (deep link) to the live video stream in the Nest app.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/is_public_share_enabled	Users can choose to share their video and make it viewable by anyone. When public share is enabled, you can read public_share_url.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/activity_zones	Returns an array of all defined Activity Zones. Activity Zones are used to monitor motion events within user-defined areas of the video stream.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/public_share_url	You can access this URL when a user makes their video stream public.

Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/snapshot_url	Capture an image on demand. Returns the URL of an image captured from the live video stream.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/has_sound	Sound event - sound was detected.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/has_motion	Motion event - motion was detected.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/has_person	Person event - a person was detected.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/start_time	Event start time, in ISO 8601 format.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/end_time	Event end time, in ISO 8601 format.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/urls_expire_time	Timestamp, in ISO 8601 format, that identifies the expiration of these event-related URLs: last_event/web_url last_event/app_url last_event/image_url last_event/animated_image_url Expiration time is calculated as: last_event/start_time + n days (where n = 10 or 30 days, depending on the Nest Aware subscription plan). Requires Nest Aware.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/web_url	Web URL (deep link) to the last sound or motion event at home.nest.com. Used to display the last recorded event, and requires user to be signed in to the account. Requires Nest Aware. If the event URL has expired or the device does not have an active subscription, then this value is not included in the payload.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/app_url	Nest app URL (deep link) to the last sound or motion event. Used to display the last recorded event, and requires user to be signed in to the account. Requires Nest Aware. If the event URL has expired or the device does not have an active subscription, then

			this value is not included in the payload.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/image_url	URL (link) to the image file captured for a sound or motion event. Requires Nest Aware.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/animated_image_url	URL (link) to the gif file captured for a sound or motion event. Requires Nest Aware.
Camera	GET	https://developer-api.nest.com/devices/cameras/device_id/last_event/activity_zone_ids	Identifiers for Activity Zones that detected a motion event. Requires Nest Aware. When used with the activity_zones array, you can get the zone name from these ids. If last_event/has_motion is true = returns the activity zone ids that detected a motion event false = returns an empty array
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/device_id	Nest Protect unique identifier.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/locale	Specifies language and region (or country) preference.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/software_version	Software version.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/structure_id	Structure unique identifier.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/name	Display name of the device; can be any room name from a list we provide, or a custom name.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/name_long	Long display name of the device. Includes a custom (label), created by the user, or via wheres.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/last_connection	Timestamp of the last successful interaction with the Nest service, in ISO 8601 format.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/is_online	Device connection status with the Nest service.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/battery_health	Battery life/health; estimate of remaining battery power level.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/co_alarm_state	Carbon monoxide (CO) alarm status.

Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/smoke_alarm_state	Smoke alarm status.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/is_manual_test_active	State of the manual smoke and CO alarm test.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/last_manual_test_time	Timestamp of the last successful manual smoke and CO alarm test, in ISO 8601 format.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/ui_color_state	Indicates device status by color in the Nest app UI. It is an aggregate condition for battery+smoke+CO states, and reflects the actual color indicators displayed in the Nest app.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/where_id	A unique, Nest-generated identifier that represents name, the display name of the device.
Smoke+ CO Alarm		https://developer-api.nest.com/devices/smoke_co_alarms/device_id/where_name	The display name of the device. Associated with the Nest Protect where_id. Can be any room name from a list we provide, or a custom name.

5.3.3 Wink Cloud API

Type	Method	URL	Description
Wink Hub	PUT	https://api.wink.com/device_type/device_id/desired_state	Desired State and Last Reading
Wink Hub	GET	https://api.wink.com/users/me/wink_devices	Retrieve All Devices of User
Wink Hub	GET	https://api.wink.com/device_type/device_id/users	List shared device users
Wink Hub	POST	https://api.wink.com/device_type/device_id/users	Share a device
Wink Hub	DELETE	https://api.wink.com/device_type/device_id/users/email	Unshare a device
Wink Hub	GET	https://api.wink.com/air_conditioners/device_id	Get Air Conditioner
Wink Hub	GET	https://api.wink.com/binary_switches/device_id	Get Binary Switch
Wink Hub	GET	https://api.wink.com/shades/device_id	Get Blind
Wink Hub	GET	https://api.wink.com/cameras/device_id	Get Camera
Wink	GET	https://api.wink.com/doorbells/device_id	Get Doorbell

Hub			
Wink Hub	GET	https://api.wink.com/eggtrays/{device_id}	Get Egg Minder
Wink Hub	GET	https://api.wink.com/garage_doors/device_id	Get Garage Door
Wink Hub	GET	https://api.wink.com/hubs/device_id	Get Hub
Wink Hub	GET	https://api.wink.com/light_bulb/device_id	Get Light Bulb
Wink Hub	GET	https://api.wink.com/locks/device_id	Get Lock
Wink Hub	GET	https://api.wink.com/cloud_clocks/device_id	List nimbi
Wink Hub	GET	https://api.wink.com/cloud_clocks/cloud_clock_id/alarms	List alarms of nimbus
Wink Hub	POST	https://api.wink.com/cloud_clocks/cloud_clock_id/alarms	Create an alarm
Wink Hub	PUT	https://api.wink.com/alarms/alarm_id	Edit an alarm
Wink Hub	DELETE	https://api.wink.com/alarms/alarm_id	Delete an alarm
Wink Hub	GET	https://api.wink.com/power_strips/device_id	Get Power Strip
Wink Hub	GET	https://api.wink.com/piggy_bank/device_id	Get Piggy Bank
Wink Hub	GET	https://api.wink.com/piggy_banks/{piggy_bank_id}/deposits?since={timestamp}	Get all deposits for Piggy Bank
Wink Hub	POST	https://api.wink.com/piggy_banks/{piggy_bank_id}/deposits?since={timestamp}	Create a deposit or withdrawal
Wink Hub	GET	https://api.wink.com/refrigerators/device_id	Get Refrigerator
Wink Hub	GET	https://api.wink.com/propane_tanks/device_id	Get Refuel
Wink Hub	GET	https://api.wink.com/remotes/device_id	Get Remote
Wink Hub	GET	https://api.wink.com/sensor_pods/device_id	Get Sensor
Wink Hub	GET	https://api.wink.com/sirens/device_id	Get Siren
Wink Hub	GET	https://api.wink.com/smoke_detector/device_id	Get Smoke Alarm
Wink Hub	GET	https://api.wink.com/sprinklers/device_id	Get Sprinklers
Wink Hub	GET	https://api.wink.com/thermostats/device_id	Get Thermostat
Wink Hub	GET	https://api.wink.com/water_heaters/device_id	Get Water Heater
Wink Hub	GET	https://api.wink.com/users/me/groups	Get all groups

Wink Hub	POST	https://api.wink.com/users/me/groups	Create a group
Wink Hub	GET	https://api.wink.com/groups/group_id/	Retrieve a group
Wink Hub	PUT	https://api.wink.com/groups/group_id/	Update group settings
Wink Hub	DELETE	https://api.wink.com/groups/group_id/	Delete a group
Wink Hub	POST	https://api.wink.com/groups/group_id/activate	Set state of group
Wink Hub	GET	https://api.wink.com/users/me/scenes	Get all scenes
Wink Hub	POST	https://api.wink.com/users/me/scenes	Create a scene
Wink Hub	GET	https://api.wink.com/scenes/scene_id/	Retrieve a scene
Wink Hub	PUT	https://api.wink.com/scenes/scene_id/	Update scene settings
Wink Hub	DELETE	https://api.wink.com/scenes/scene_id/	Delete a scene
Wink Hub	POST	https://api.wink.com/scenes/scene_id/activate	Set state of scene
Wink Hub	GET	https://api.wink.com/users/me/robots	Get all robots
Wink Hub	POST	https://api.wink.com/users/me/robots	Create a robot
Wink Hub	GET	https://api.wink.com/robots/robot_id/	Retrieve a robot
Wink Hub	PUT	https://api.wink.com/robots/robot_id/	Update robot settings
Wink Hub	DELETE	https://api.wink.com/robots/robot_id/	Delete a robot
Wink Hub	POST	https://api.wink.com/users	Create user
Wink Hub	PUT	https://api.wink.com/users/user_id	Update current user's profile
Wink Hub	POST	https://api.wink.com/users/user_id/update_password	update password
Wink Hub	GET	https://api.wink.com/users/me/activities	Get user activities