DFRWS Forensic Challenge

(IoT Forensic Challenge 2017-2018)

Jaehyung Cho (whwogudsla@kookmin.ac.kr)
Soram Kim (kimsr2040@kookmin.ac.kr)
Serim Kang (ksl5442@kookmin.ac.kr)
Giyoon Kim (gi0412@kookmin.ac.kr)
Jongsung Kim (jskim@kookmin.ac.kr)

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

Contents

I. Introduction

This year's DFRWS Challenge is Internet of Things forensics. The Internet of Things (IoT), generally refer to, network and Internet connected devices used 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-related challenges.

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

- o Evaluating and Expressing Conclusions:
  Formally evaluating and expressing the probability or likelihood ratio that a the husband killed his wife versus some other unknown person.
- o Device Level Analysis:
  Developing methods and tools to forensically process the digital traces generated by IoT devices, including on mobile devices.
- o Network and Cloud Level Analysis:
  Developing methods and tools to forensically process digital traces generated by IoT devices on networks and cloud systems.
- o Correlation and Analysis:
  Developing methods and supporting tools that combine information from various data sources and automatically computing, visualizing, or otherwise exposing patterns of potential interest.

1. Challenge Scenario

A woman (Betty) has been murdered. The murder was called in by Betty's husband (Simon), who claims to have been at home at the time.

1.1 Details of Scenario

- o 15:31 2017-07-17
  Chuncheon Emergency Services receives a phone call from a local apartment building manager. A man that living in the apartment building claims that his wife was attacked inside their apartment. The police responds.

- o 15:40 2017-07-17
  Police arrive on-scene, and find the husband (Simon HALLYM) and apartment manager (KIM Kil Whan) outside the apartment.

The apartment is secured and a woman is found laying on the ground in the living room. She is not breathing and has no pulse. From an initial assessment it appears as though she was stabbed multiple times. Medical services arrive and confirm she is deceased.

o 15:50 2017-07-17

Investigator 1 interrogates the building manager (Mr. KIM) and husband (Mr. HALLYM). The building manager claims Mr. Hallym ran down the stairs screaming for the police.

A search of the apartment reveals the following digital devices:

1) Door sensors at the main door
2) Motion sensor on the shelf
3) Wristband on the floor where the victims' (Betty Hallym) body was found
4) Mobile Phone on the floor where the victims' (Betty Hallym) body was found
5) Amazon Echo device
6) Google OnHub wifi router connected to a SmartThings Hub and an IPTime switch
7) Samsung Smart things hub
8) IPTime Switch OnHub (6) and Modem (ISP)
9) Raspberry Pi connected via HDMI to a TV
10) Bluetooth headphone
11) Door sensor at the bedroom door
12) Husband's (Simon Hallym) mobile phone

1.2 Interrogation of Simon Hallym (15:49 2017-07-17)

1) What is your full name?
   - Simon Hallym

2) What do you do?
   - I am a computer programmer.

3) Are you living in this Home?
   - Yes, I am living with Betty. She is my wife, Betty Hallym.

4) Could you please describe what happened?
   - I was watching a movie. After finishing the movie, I came into the living room and found her on the ground.

5) Do you know someone who would want to hurt your wife?
   - No. No one.

6) Did she have friends or acquaintances in the area?
- I don't think so. We just moved here.

7) Where did you watch the video?
- I was in our bedroom.

8) Could you remember what time?
- Almost 3?, I don't know exactly. Maybe around 3pm. I think that's when we got home.

9) When you was watching video, didn't you hear anything?
- She listens to music, so I used headphones. I didn't hear anything.

10) Can you remember what you were watching?
- It was a drama from Youtube.

11) We found SmartThings sensors around your home. Do you have access to this data?
- Yes, I get it on my phone.

12) May we have permission to access your phone?
- Yes, ok.

13) May we have permission to access your SmartThings data?
- Alright.

14) Can you identify this black Samsung Note II, and Mi step monitor?
- Those are Betty's.

15) Do you know any passwords for the phone?
- No.

16) What are the passwords to your WIFI?
- Home is iot14306, but the guest network is iot14305

1.3 Concept Diagram

Fig. 1-1 is a picture of the crime scene according to the list of digital devices and the interrogation of Simon Hallym. Before the murder happened, Betty was listening to music with Amazon Echo and wearing a band on her wrist. Simon was watching a video on a Smart TV connected via HDMI to a Raspberry Pi, both located in the Bedroom.

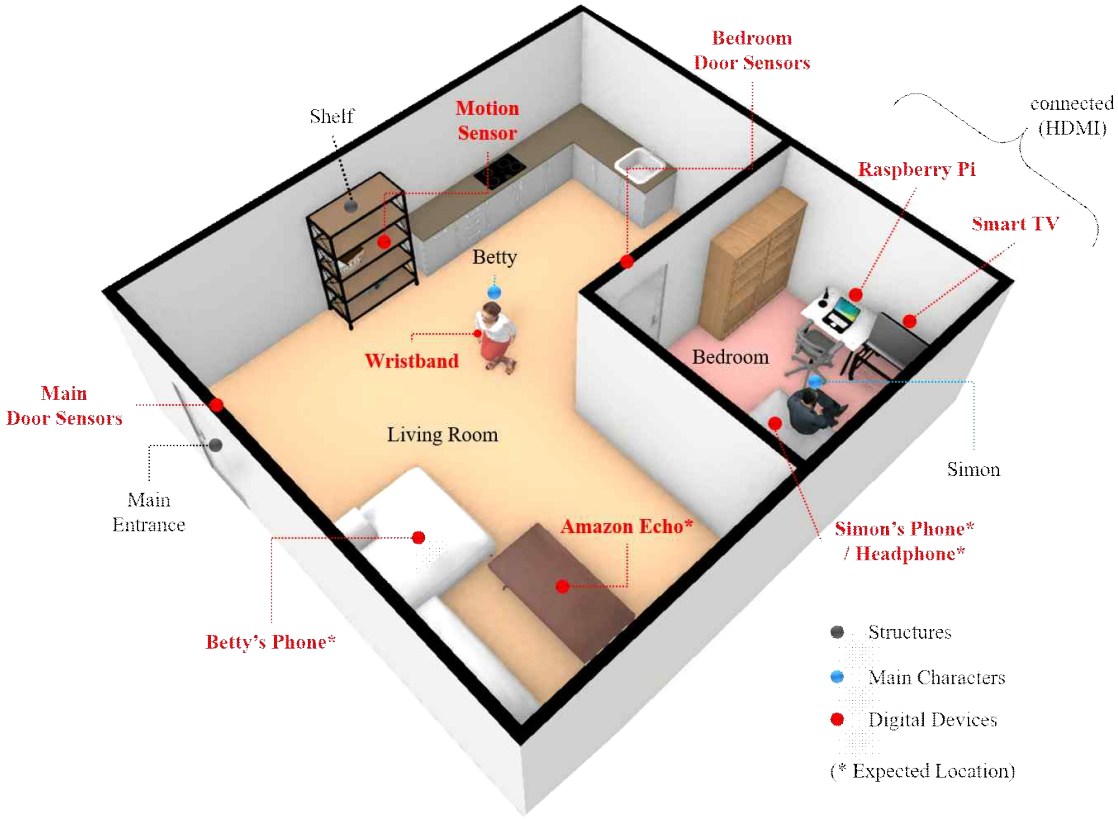


Fig. 1-1. Concept Diagram of Betty & Simon's House

2. Overview of Challenge Data

The given Challenge Data and hash values are as follows:

1) Smart TV Raspberry Pi
- SHA1 : f912e7437025473516c608319b831eeca99f673a
2) Samsung Galaxy Note Ⅱ (Betty)
- SHA1 : cd494cf3097d8482100ce26dc8e35f0d87b67198
3) Samsung Galaxy Note Ⅱ (Simon)
- SHA1 : fc28e415ee740531df86a2b227c4f514e9ed40ba
4) Google OnHub Diagnostic Report
- SHA1 : 20eb4825eaf6c303beadd090868110fb2de37066
5) Amazon Echo Cloud Data
- SHA1 : d1d126f47b565926dcc80fe6a4e7094f0281cb47
6) MDS (Acme, Inc.) Smarthome Network Dump
- SHA1 : 6ab6c522b070cde292a18645a19929998e009293

2.1 Image of Raspberry Pi

The Raspberry Pi is a single board computer developed by the Raspberry Foundation in England. It was originally developed for basic computer science education in schools and developing countries. However, it is currently being used for research and development, experimental environments, and personal computers.

In this scenario, the Raspberry Pi is used as a set-top box. Simon uses the Raspberry Pi connected to the TV via HDMI to watch YouTube. The image file for the Raspberry Pi was extracted using the forensic tool Guymager. Detailed specifications of the Raspberry Pi are as follows (Fig. 1-2, Table 1-1).

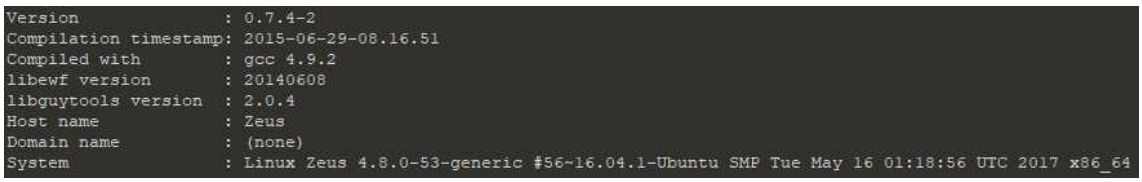


Fig. 1-2. Information from Guymager

Table 1-1. Raspberry Pi Specifications

Linux device	/dev/mmcblk0
Device size	15931539456 (15.9GB)
Format	Linux split dd raw image - file extension is .xxx
Image path and file name	/cases/001/Images/E001-SmartTV/E001SmartTVMMC.xxx
Info path and file name	/cases/001/Images/E001-SmartTV/E001SmartTVMMC.info

The integrity of the acquisition image file is verified with MD5, SHA1, and SHA256.

Table 1-2. Hash Values of Acquisition Image File

MD5	8637bc76b60738088240e6159716eded
SHA1	f912e7437025473516c608319b831eeca99f673a
SHA256	f1adc94eb3e993ca7b8b9cfd1c19e1b622610826281587 97f90c6c97c7c81eda

2.2 Images of Samsung Galaxy Note Ⅱ

The Samsung Galaxy Note Ⅱ is an Android phablet smartphone. The phablet is a class of mobile devices combining or straddling the size format of smartphones and tablets. The following table presents basic information about the Samsung Galaxy Note Ⅱ.

Table 1-3. Galaxy Note Ⅱ (Korean carriers) Specifications

Manufacturer	Samsung
Model	SHV-E250S
First released	26 September 2012
Type	Phablet
Operating system	Android 4.1.1 Jelly Bean ~ 4.4.2 KitKat
CPU	1.6 GHZ quad-core Cortex-A9 & Krait 300 MP4 1.9Ghz
GPU	ARM Mali-400MP4 & Adreno 320
Memory	2GB
Storage	32GB
Removable storage	microSD up to 64GB
Battery	3,100mAh, 11.78wh, 3.8V Li-on
Weight	183g

The given image files were acquired from MD-NEXT (Hancom GMD) and contain 251-byte footer. Encase (Guidance Software) can generally analyzes these files without issues, but FTK Imager (AccessData) shows some errors. When the footer is erased, FTK imager operates normally.

Table 1-4. List of Betty and Simon's Smart phone Image Files

File	Size	Hash (SHA256)
Betty		
SHV-E250L_Physical_20170717_EFS.mdf	20MB	befae2ca8da161dd115ebf29a81611cb7a1879563befdd67919cb6b859845aa3
SHV-E250L_Physical_20170717_CACHE.mdf	1.25GB	efcfab5069175a61a3985392dcd2ba1895d851b33c60ddf4a73f5bd01496cda6
SHV-E250L_Physical_20170717_TOMBSTONES.mdf	256MB	34cc491cc501395871947b98f888c9413d77f3a16eca43a911716ad3a36eeb07
SHV-E250L_Physical_20170717_RADIO.mdf	88MB	0694e0af93ffef502891473833e5d089136062e86c6744a8b6be087c0deff944
SHV-E250L_Physical_20170717_HIDDEN.mdf	560MB	01e9df3c7bd977e67320e9ab6643c696a63258bd62c63a5548304d640f79c277
SHV-E250L_Physical_20170717_SYSTEM.mdf	2.34GB	5c36128d09fdc56500ff4831609904d32a6a62c032e976ecfda77d4b3853a68e
SHV-E250L_Physical_20170717_USERDATA.mdf	24.5GB	1640a9e0ab2d3f235c4d1280fdc1c12b5998648fc942b12012de393d0a74ea65

Simon		
SHV-E250S_Physical_20170718_EFS.mdf	20MB	b5edeacf9433e743c9bf5233868f61a921e2d7ad9a02ff745affdac3c4834955
SHV-E250S_Physical_20170718_CACHE.mdf	1.25GB	260a0c26ba37da4c432864b55011682673848e29a40a0ed58b6fe05c42f8d649
SHV-E250S_Physical_20170718_TOMBSTONES.mdf	256MB	14194c53217e71e118f2245e7364c3ec7b04e9c6bc7a9f1071e1e920b009459b
SHV-E250S_Physical_20170718_RADIO.mdf	88MB	2b61618e80c707db8b7f35881e289175fb618570b547209fa9812ce3a3325317
SHV-E250S_Physical_20170718_HIDDEN.mdf	560MB	12d1ba5aceb78efa65a8b7af1259441ff0be0de3478b8314300920cbc37e25cc
SHV-E250S_Physical_20170718_SYSTEM.mdf	2.34GB	9c53cfa7063eeb08f7666626d5d883dd8283509eeee6d3b0057eecfa20669b17
SHV-E250S_Physical_20170718_USERDATA.mdf	24.5GB	ae38cbb62233cadd82deb0660e8ae70ea7f0fce67630a498fed88daac9160a6f

2.3 Diagnostic Report from Google OnHub

Google OnHub is a residential wireless router product from Google. The two variants are manufactured by TP-Link and ASUS. They differ in prize, size, weight and color but have the same networking technology specs.

Table 1-5. Google OnHub Specifications

Connectivity	AC1900
Wireless Support	IEEE 802.11a/b/g/n/ac
2.4 GHz & 5 GHz Wireless	Dual concurrent 3x3 with Smart Antenna
Wireless Security	WPA2-PSK
WAN Port	1x 10/100/1000 Mbit/s
LAN Port	1x 10/100/1000 Mbit/s
Ethernet Switch	QCA8337 Gigabit sw

There are API methods available for the Google OnHub. The default IP is 192.168.86.1. Let's define /ONHUB_API/ = http://192.168.86.1/api/vi. The given Challenge Data is from '/ONHUB_API/diagnostic-report' which is encoded with protobuf[1].

- /ONHUB_API/status

1) Protocol Buffers. A method of serializing structured data developed by Google.

- /ONHUB_API/diagnostic-report
- /ONHUB_API/welcome-mat
- /ONHUB_API/connected-devices
- /ONHUB_API/wan_configuration
- /ONHUB_API/get-group-configuration
- /ONHUB_API/get-attestation-information
- /ONHUB_API/get-endorsement-information

2.4 Data from Amazon Echo / Alexa Cloud UI

Amazon Echo is a smart speaker developed by Amazon.com. The device is capable of voice interaction, music playback, making to-do lists, setting alarms, streaming podcasts, playing audio books, providing weather, traffic and other real-time information. It can also control several smart devices. In order to operate all these functions, a user must speak the "Wake Word" first; the default word is "Alexa". More available services are listed below.

- Weather from AccuWeather[2)]
- News from iHeartRadio, BBC, NPR and ESPN local radio stations
- Music from Amazon Music, built-in support for the Pandora and Sporify streaming music services, and Apple/Google Play Music
- Support for IFTTT[3)] and Nest thermostats
- Voice-controlled alarms, timers, shopping and to-do lists
- Access Wikipedia articles

Table 1-6 shows the list of evidence files from Amazon Echo. It consists of three file extensions (.png, .json, .wav) and the content type for each file is as follows.

- png : an image file captured from the Amazon website
- json : a file containing request and response body parameters
- wav : a file containing the recorded voice of people who interacted with the Echo

Table 1-6. List of Evidence Files from Amazon Echo

File	Size	Hash(SHA256)
/Alexa screenshot/Home Page/2017-07-17_16h57_34.png	38KB	febebc03df6198e518f947c46d92d03c8576e443957864c5359efbc25d81bfd6
/Alexa screenshot/Home Page/2017-07-17_16h59_15.png	53KB	1245f04c8fb85411c79ec11a0d565984afdc1d06fe6c2d4216e82f1e0d8d6482
/Alexa screenshot/Home Page/2017-07-17_	34KB	2a2221c81302680578b89b515dc7fd51814c7bba

2) American media company that provides commercial weather forecasting services.
3) If This Then That, free web-based service to create chains of simple conditional statements.

16h58_04.png		54f9ec856729b860bfe409b6
/Alexa screenshot/Home Page/2017-07-17_16h59_39.png	41KB	93a66093310608685f25e8781e33922d9e4892670137f821aa8e2c5750e83512
/Alexa screenshot/Home Page/2017-07-17_16h58_24.png	38KB	708dbaff9761a8f18a5c9c9bba7ca1f8ed8075e2e4dbcbbb8a68fa47d78880df
/Alexa screenshot/Home Page/2017-07-17_16h57_20.png	48KB	b7b738e31ac6539a1856c0f728b4c297137f1a4e824a57c708e0c343e2160cef
/Alexa screenshot/Home Page/2017-07-17_16h56_52.png	91KB	923846777ac708ccca59134d34eea2f3fc7ccc514df2c73753192b6471d2f643
/Alexa screenshot/Home Page/2017-07-17_16h57_52.png	50KB	dd9e1f387a5645f48d2f5b4a9bd4878e55e54f1e258197686702dc37c860e84d
/Alexa screenshot/Home Page/2017-07-17_17h00_09.png	62KB	fc1ed00b73e974d9a1e6bd193f92e32548d00b5f769dfa2225be19dc5fbb8199
/Alexa screenshot/Home Page/2017-07-17_17h00_43.png	56KB	ebf4eadb6a9c291d94e6e97412535e3778a6aa6304c20f9acf7b32d210d002d5
/Alexa screenshot/Home Page/2017-07-17_16h59_56.png	53KB	be486369b5d410dfcd1656dde5a483b0dfb190660cefb6a675ce81d35ea571ff
/Alexa screenshot/Home Page/2017-07-17_16h58_43.png	37KB	4bd58d1bb0b3de40c3ba2759fb5b65c1cd29d7529fe9015eb9d8dac895fb9d73
/Alexa screenshot/Now Playing/2017-07-17_17h01_46.png	28KB	fa8d1177ecc40ab1ac94b8cf5c11526c44fa8f3a8260ce8be7b452ea576bda59
/Alexa screenshot/Now Playing/2017-07-17_17h02_09.png	42KB	1ad8297260c8d49815008fdfa2e149f19b91c72c40b433eebe2ab4a52368e7d7
/Alexa screenshot/Music Video and Books/2017-07-17_17h15_47.png	43KB	db73053128875eba7812910a7100dfa055d4141d9205d0281eba88410cf9d96b
/Alexa screenshot/Music Video and Books/2017-07-17_17h13_03.png	48KB	0d72b84d4ffa52b392000c163836ddbc7acfa6908c494fa2ead86a4770602e2a
/Alexa screenshot/Music Video and Books/2017-07-17_17h08_49.png	33KB	df7b5103a954085edacca4b5c2af477559b54312921388209a9bab72dc89966e
/Alexa screenshot/Music Video and Books/2017-07-17_17h18_42.png	32KB	2842324f4b384faebfb519a6ffe8c0b4a6ff1c94be746efda396644b96d5b46b
/Alexa screenshot/Music Video and Books/2017-07-17_17h18_11.png	51KB	2d6b45e082413bab071342aefaa7855994a6d18ee3aec49e4557e3f79c362dc1
/Alexa screenshot/Music Video and Books/2017-07-17_17h16_06.png	43KB	7275db06912d0ba0d09ce8b2b8c025fc47efc52fbccb93bdf5f0850df51865e8
/Alexa screenshot/Music Video and Books/2017-07-17_17h16_38.png	44KB	f21737ad6f3fc221874f7601a05bd472b6d2a06cbc3fe091c3494b69ac30ac60
/Alexa screenshot/Music Video and Books/2017-07-17_17h05_34.png	31KB	2f39e44c377784f8e56e30afcdb3067c21f233e989b8fc02deaf274583a2dc19
/Alexa screenshot/Music Video and Books/2017-07-17_17h14_23.png	47KB	0d178a6816884fe409bb05aa69eb6cecac1a6d2709680c793b23a1648848de9d
/Alexa screenshot/Music Video and Books/2017-07-17_17h15_14.png	47KB	8335ff5ae56f4bd72fcd55e5d149bc4b0c28cbb95bf47932384640ebc05f0700
/Alexa screenshot/Music Video and Books/2017-07-17_17h13_43.png	43KB	51ccd07a908cbf4fe5a4debae78c78e5f5be1e2146a41d644ff45cac22d685a0

/Alexa screenshot/Music Video and Books/ 2017-07-17_17h04_43.png	27KB	3a83a8e0ee1ea00f11730baefd62ad4a6d256674774975768de72ab3cea7ed24
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h13_21.png	44KB	12c0fc3d593f63d8a151885244220023fee11f4574d67a5d21240513679b2726
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h17_35.png	49KB	9342a2dd130e54830dc9d21161cab591ef0fa822536ddb4fc3ede554347b26f2
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h17_54.png	50KB	f81621b781946617383bac7acbc4580d836d8b9e79a00c185bd8dcf73bca8e2f
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h07_00.png	36KB	3a635c758f1b09912100f2881d44eebd49a2d333dcaa40f0eca8b87f3664ad63
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h06_37.png	42KB	d4bb18632887b5187cc2165878ec32de010f05789acbf0e692728895d503565c
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h16_54.png	44KB	1ef8e89d7fa042b0f0e13e0d752e238065a2c817a9af61300fd11a01be1ad64c
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h04_15.png	24KB	2ae1053377568a616a04ed48e34b0d2ea6134fbe35abae910bfedd8e39d2c485
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h07_33.png	34KB	028cdd2ce964f74191bc30eb82cb5d425a9ec9f9ada0123ac1afd0bd06677df8
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h07_55.png	34KB	7ee0cc165bf03c415a3ed4dc1b270618c1623ff0816596b4c3c8266b69bfad09
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h06_10.png	28KB	6a7136c9045f2ad59448a0edf5b4bd3a93da9ebaa691ef327de36e0859aa0363
/Alexa screenshot/Music Video and Books/ Music video and books/2017-07-17_17h03_50.png	42KB	a2f3c06ca29833a8066144dc9f85ce7abb0bb90092a60204a996694da88677d2
/Alexa screenshot/Music Video and Books/ Music video and books/2017-07-17_17h03_29.png	42KB	38361288e7ed4ce1d20c6de33f6c396f6e33e86de02c016424efa260a06b2ed0
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h17_12.png	46KB	67161a5281c19b6982d6bf173a7beba9ffe7694ab80d44e6936d4402ab02fdd6
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h14_45.png	46KB	8fb897a6a6d7cb521b797a24599abd27a614f36c1d5f7b368c715baeee4b52b0
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h08_29.png	32KB	e6a38c1b2b6114c6141e8423a01f5acd1acc8027493de571f14df6037b24a21c
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h05_48.png	25KB	8b72c93e45f4e13b44519a7000f67df5fd263f676ef873314d97cffdd322e1a2
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h09_01.png	33KB	078fbfa710ef2f5d468323601122 43de4b40b73aa3304a2e6547f9b3e6965164
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h10_06.png	45KB	dce76d14b6a42b9257f8cc69c28d274592c151079dc94039844251d191832b36
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h08_14.png	32KB	802e358f1b1de5dbd1f9b04d54402f7509884a9585e8b442862d12bb91e5501a
/Alexa screenshot/Music Video and Books/ 2017-07-17_17h14_05.png	45KB	72305db21f32a796fca870e879d2edf7d3371b7ac471106a37a706da4605aa19

1.json	6KB	8ac0ef2f46e67c25472dbdaf1b95f7412cbd1082e2b631f1c4f66fc75e547cc0
2.json	1KB	123cf0ba5848614bdced4651af7a09d9560c640f58766626ef136620dedf65be
3.json	1KB	a07fb10957ba9ed48b41faaeb0a52e05eb7c357f9d8bec2d132491dd75320d09
4.json	1KB	de19f59694d4aed1f6fe98eb29ee79e9dc32bfbf7ff1e49dab9ab0b7024f171a
5.json	1KB	69863e780ecd2320ca26910c68b083c3cd7ebe6f8f4d775223342a464373dc95
6.json	1KB	e1b28d6b4dac7fb2582bd9eb60802a9f22449d825dcb125ca480b646a6be2070
7.json	0KB	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
8.json	2KB	8300781898f44f25106d132e226ac908b48f1193c6f5da8dabbefde076ec554c
9.json	2KB	dab4e3284f4488559920983018135 9c5ad5128831b3200f4e43483067b8dfee8
10.json	1KB	58b2ffc7da1d819c9e3e3c563f25666e24f25fd4e662039665dfc6b6711c9805
11.json	1KB	7e4c816e48760af9691beb64980e7b0e617eb62f1151fee206f5939c2e6c88aa
12.json	1KB	699bebb40c67ac1066604ef6c6afbe8789dc7c2684373b2ba422892d2184d61d
13.json	4KB	d5b831a0677545ee716e5f9f57f5997bb3e91cb0679a435ab43ffe9f91b9a322
14.json	1KB	60078edfdf88e82804f1e8b8296d3778ef1c828df9869aef1c4be4e8748b2c9a
15.json	1KB	2307dd0255041d4bbf1dc37507bd7bd839bba5ad0e0daa374908a90b6465aa00
16..json	1KB	e52ecc9eefb29e86c6fdd4e42933ce2a4c9b87277037f0ad3e21415bfcd2cf9b
17json	1KB	8bfe470bc059ef0cdd11e931963d5e350c671e6cf57c0fda78c86e20fbbef39f
18.json	1KB	423274025df40524a2cb320dfd2d3338223eed8e6b9fe0077cd0fc1b5bbc0966
1.wav	174KB	22f459e6efc6cc542752c1f3af0adcf68ef0e3e240ee79afc04f8b5dee32b970
2.wav	174KB	22f459e6efc6cc542752c1f3af0adcf68ef0e3e240ee79afc04f8b5dee32b970
3.wav	179KB	a83001dedd1bb87765faf580dee0234126347e4ad9277f2c7e51b6279861780e
4.wav	179KB	a83001dedd1bb87765faf580dee0234126347e4ad9277f2c7e51b6279861780e
5.wav	219KB	c09e0184bd561d2e2565373afd56b2a6350bd0ed

		f759c558da924080bf828de3
6.wav	219KB	c09e0184bd561d2e2565373afd56b2a6350bd0ed f759c558da924080bf828de3
7.wav	232KB	2fbe89e3508b8f029dbfe4f03b5e793bdec8636d4 0a82e0edc20d1355328f9b3
8.wav	182KB	7d66d7102cfdae7b6f792fd71f1fbd152620360bd 241698ba50ac21b61ac4d80
9.wav	212KB	4c7064f32423234a59039ba059f4770838293972 b9e3b016ceb95ea1eb9a336d
10.wav	212KB	4c7064f32423234a59039ba059f4770838293972 b9e3b016ceb95ea1eb9a336d
11.wav	152KB	1b069dadebd5380b814522f47f1021d544da6a17 df293ca11793ed98b7812a78
12.wav	152KB	1b069dadebd5380b814522f47f1021d544da6a17 df293ca11793ed98b7812a78
13.wav	170KB	d79fc71cbb6055dad2d8465e8d7a732bfe44726ad fd758be63a58ee25086c4eb
14.wav	147KB	3168797691c619f91d0bdfb7fce72a9539a152cbc 56aacd21a631f4b9e705458
history first page.png	105KB	ee6d009300947f24dafed6029c193d019f833159c 4d107ea45c6af54c40832d7
history second page.png	116KB	db61c918114ee0bbe816b414868822aebacf82f78 9b1ccc9ee195cf05b2371f7
json and audio api.txt	6KB	9e54ba2a087474bb1ef03b1791df334a02558093 04cabd611d7e3d4411081a6c

2.5 SmartHome Network Traffic Logs

The size of the provided dump file is 15,660,187 bytes. A tcpdump file typically stores dumped data or packet headers delivered to and from the specified NIC (Network Information Center). It is mainly used to check whether the network and ethernet are abnormal. In this scenario, a tcpdump file was obtained to investigate packets from the SmartHome network traffic.

II. Forensic Analysis

1. Forensic Analysis Techniques

In this section, we propose forensic analysis techniques for the Device, Cloud and Network level. Furthermore, important keywords, major file names that must be analyzed and background knowledge will be provided for each device given in the Challenge Data. Table 2-1 shows the list of tools we use for evidence analysis (We have licenses for commercial tools).

Table 2-1. List of Tools Used for Analysis

Tool	Version	Usage
Encase	7.10.05	- Extracting evidence files - Processing image files
SQLite Expert (Personal Edition)	3.5.92.2512	- Viewing SQLite database
010 editor	6.0.3	- Viewing binary files
Wireshark	2.2.7	- Analyzing network packets
NetworkMiner	1.6.1	- Analyzing network packets
AccessData FTK Imager	3.4.3.3	- Verifying file systems
MD-RED Academy	2.0	- Extracting evidence files from smartphones

1.1 Device Level Analysis

1.1.1 Raspberry Pi

We use Encase and FTK Imager for device level analysis of the Raspberry Pi. The partition information for the Raspberry Pi can be found in the 'install.log' file, and the scenario image file consists of two partitions; C and / (Fig. 2-1). The file systems for these partitions are FAT32 (mmcblk0p1) and EXT4 (mmcblk0p2).

```
Thu Jan 1 00:00:07 1970 Starting OSMC installer
Thu Jan 1 00:00:14 1970 Detecting device we are running on
Thu Jan 1 00:00:14 1970 Mounting boot filesystem
Thu Jan 1 00:00:14 1970 Trying to mount to MNT BOOT (/mnt/boot)
Thu Jan 1 00:00:14 1970 Using device->boot: /dev/mmcblk0p1 and FS: fat32
Thu Jan 1 00:00:14 1970 Preseed file found, will attempt to parse
Thu Jan 1 00:00:14 1970 Found a definition for storage: sd
Thu Jan 1 00:00:14 1970 Creating root partition
Thu Jan 1 00:00:14 1970 From a root partition of /dev/mmcblk0p2, I have deduced a base device of /dev/mmcblk0
Thu Jan 1 00:00:14 1970 Determined 255 MB as end of first partition
Thu Jan 1 00:00:14 1970 Calling mkpart for device: /dev/mmcblk0 and fs: ext4 with start 257M and end 100%
Thu Jan 1 00:00:16 1970 Calling fmtpart for partition /dev/mmcblk0p2 and fstype ext4
```

Fig. 2-1. Partition Information for Raspberry Pi (install.log)

Most of the C partition is composed of an overlay[4]. Therefore, we conclude that this partition contains very little information associated with the user's behavior. The / partition is the primary partition that uses Linux as the operating system. Kodi, an application for watching videos on YouTube, was installed in this partition (Fig. 2-2).

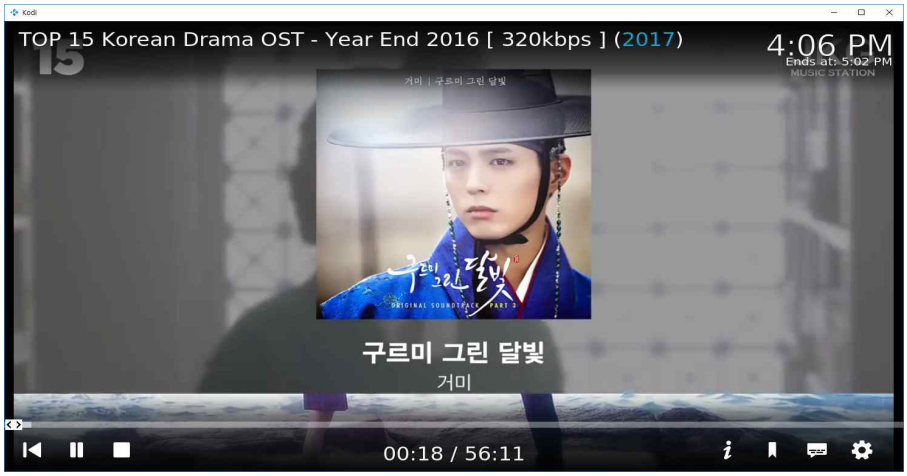


Fig 2-2. Play YouTube with Free Media Player Kodi

The add-ons installed in Kodi for Simon's configuration can be found in /home/osmc/.kodi/addons and /usr/lib/kodi/addons. We need to check the databases or logs generated by Kodi in order to confirm Simon's claim about the time he watched YouTube. Also, we should check which devices are connected to which networks. The network connection information for the Raspberry Pi in the scenario can be found in /var/lib/bluetooth.

1.1.2 Samsung Note Ⅱ

Time zone information is found in the data partition, and the file path is Data/data/property/persist.sys.timezone. The time zones for both Betty and Simon's phones are set to Asia/Seoul (Fig. 2-3). Seoul Time is 9 hours ahead of UTC (UTC +09:00).

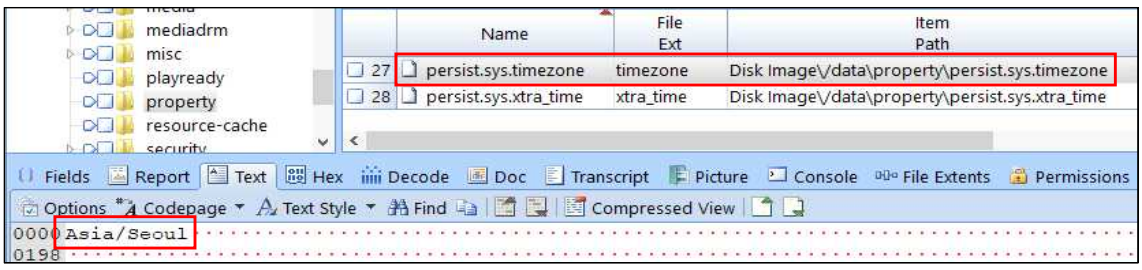


Fig. 2-3. Timezone of Samsung Galaxy Note Ⅱ

4) Technique to reduce the amount of memory used by a program. Use of an overlay allows program sizes to be larger than the computer's main memory.

Bluetooth and Wi-Fi MAC addresses are on the EFS partition. The Bluetooth MAC address is at EFS/bluetooth/bt_addr.

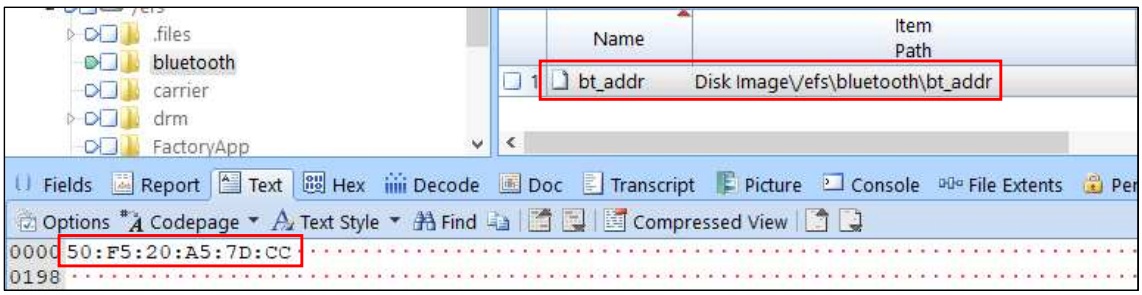


Fig. 2-4. Location of Bluetooth MAC Address in Samsung Galaxy Note Ⅱ

The Wi-Fi MAC address is at EFS/wifi/.mac.info. The MAC address is unique for each device, so it can be used to distinguish devices from the Onhub data or other devices.

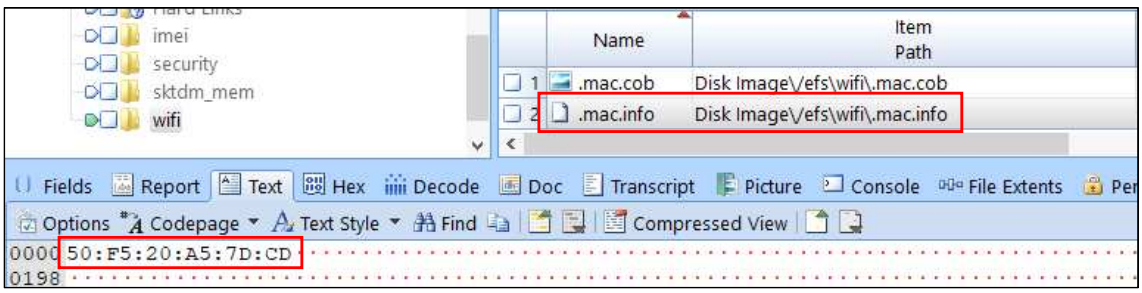


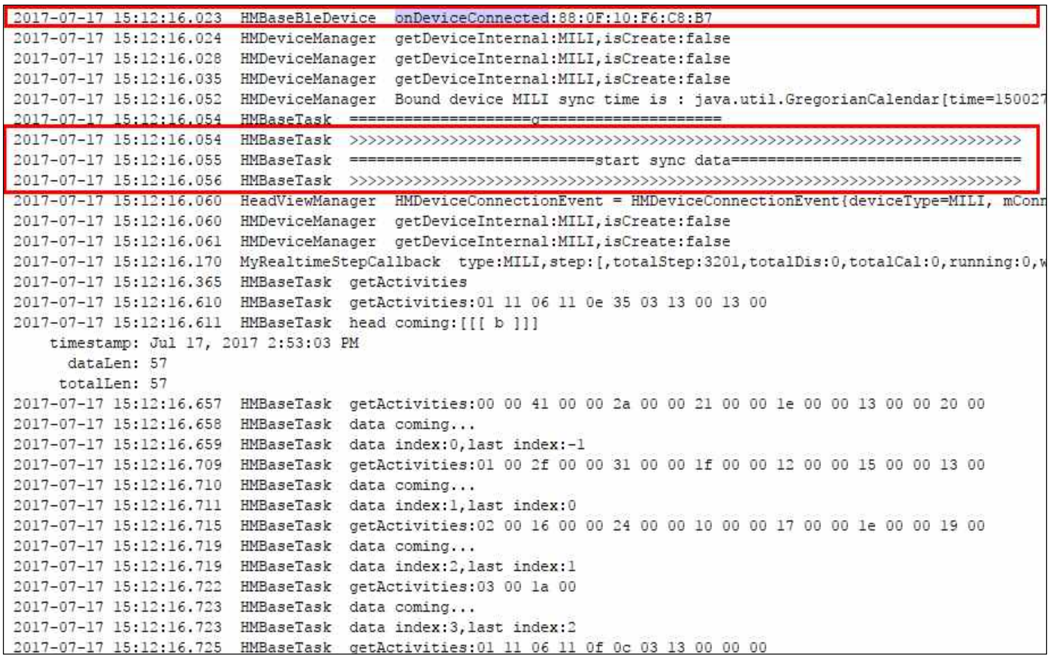
Fig. 2-5. Location of Wi-Fi MAC Address in Samsung Galaxy Note Ⅱ

We extract the 'usage-20170717' file and all databases files. In general, the 'usage-YYYYMMDD' file contains the package names and activities for the corresponding day. Additionally, all txt, log and xml files under the package name in usage-20170717 are extracted.

Database file analysis is focused on web searches and message and email data first. Afterward the rest of database files are checked. All txt, log and xml files changed on the day the event occurred are checked.

1.1.3 Xiaomi Mi Band

The Xiaomi Mi Band is a wearable fitness tracker that can be worn on either hand, ankle or around the neck. It supports a fitness monitor, sleep tracker, smart alarm, unlocking Android device and so on. The only way to check an individual's fitness data is by using the official 'Mi Fit' application developed by Xiaomi. The Mi Band synchronizes with the application via Bluetooth Low Energy (BLE) to view fitness and sleep records. When the connected smartphone is in Bluetooth range of the band, accumulated data in its storage is transmitted to the connected phone (Fig. 2-6).



```
2017-07-17 15:12:16.023  HMBaseBleDevice   onDeviceConnected:88:0F:10:F6:C8:B7
2017-07-17 15:12:16.024  HMDeviceManager   getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:16.028  HMDeviceManager   getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:16.035  HMDeviceManager   getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:16.052  HMDeviceManager   Bound device MILI sync time is : java.util.GregorianCalendar[time=150027
2017-07-17 15:12:16.054  HMBaseTask  ===================g====================
2017-07-17 15:12:16.054  HMBaseTask  >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
2017-07-17 15:12:16.055  HMBaseTask  ==========================start sync data================================
2017-07-17 15:12:16.056  HMBaseTask  >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
2017-07-17 15:12:16.060  HeadViewManager   HMDeviceConnectionEvent = HMDeviceConnectionEvent{deviceType=MILI, mConn
2017-07-17 15:12:16.060  HMDeviceManager   getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:16.061  HMDeviceManager   getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:16.170  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3201,totalDis:0,totalCal:0,running:0,w
2017-07-17 15:12:16.365  HMBaseTask  getActivities
2017-07-17 15:12:16.610  HMBaseTask  getActivities:01 11 06 11 0e 35 03 13 00 13 00
2017-07-17 15:12:16.611  HMBaseTask  head coming:[[[ b ]]]
    timestamp: Jul 17, 2017 2:53:03 PM
      dataLen: 57
     totalLen: 57
2017-07-17 15:12:16.657  HMBaseTask  getActivities:00 00 41 00 00 2a 00 00 21 00 00 1e 00 00 13 00 00 20 00
2017-07-17 15:12:16.658  HMBaseTask  data coming...
2017-07-17 15:12:16.659  HMBaseTask  data index:0,last index:-1
2017-07-17 15:12:16.709  HMBaseTask  getActivities:01 00 2f 00 00 31 00 00 1f 00 00 12 00 00 15 00 00 13 00
2017-07-17 15:12:16.710  HMBaseTask  data coming...
2017-07-17 15:12:16.711  HMBaseTask  data index:1,last index:0
2017-07-17 15:12:16.715  HMBaseTask  getActivities:02 00 16 00 00 24 00 00 10 00 00 17 00 00 1e 00 00 19 00
2017-07-17 15:12:16.719  HMBaseTask  data coming...
2017-07-17 15:12:16.719  HMBaseTask  data index:2,last index:1
2017-07-17 15:12:16.722  HMBaseTask  getActivities:03 00 1a 00
2017-07-17 15:12:16.723  HMBaseTask  data coming...
2017-07-17 15:12:16.723  HMBaseTask  data index:3,last index:2
2017-07-17 15:12:16.725  HMBaseTask  getActivities:01 11 06 11 0f 0c 03 13 00 00 00
```

Fig. 2-6. Synchronizing Log data after the Device is Connected

BLE is a wireless personal area network technology intended to provide reduced power consumption and cost compared to classic Bluetooth. BLE supporting devices use the Advertise/Connection mode to communicate with other devices. In advertising mode, the device transmits packets to all peripheral devices and a phone that receives a message has the choice to either accept or decline.

All current low energy application profiles are based on the generic attribute profile (GATT) and so is the Mi Band. GATT defines the way two BLE devices transfer data using concepts called Services and Characteristics. As the Mi Band is a BLE device, it records GATT-related logs on connected smartphones in txt format. According to the acquired 'mili_log.txt', the process of re-connection is as shown in Table 2-2 when a pre-connected smartphone is in the Mi Band's Bluetooth range.

Table 2-2. The Process of Connection between the Mi Band and a Smartphone

	Log Data	Remark
1	Gatt create:<[32bit]>	Using 32bit address
2	onConnectionStateChange	GATT address, Mi Band MAC address, Change newState 0 → 2
3	Gatt connected:<[32bit]>	-
4	onDeviceConnecting	Mi Band MAC address
5	discoverServices	-
6	onServiceDiscovered	Characteristic list
7	device info	Mi Band ID, firmware version

8	onDeviceConnected	Mi Band MAC address
8	start sync data	Transferring data to connected smartphone
8-1	data coming...	
8-2	BaseSleepInfo	
8-3	stop sync data	
9	onConnectionStateChange	Change newState 2→0
10	Gatt close:<[32bit]>	GATT address

As mentioned above, the data is transmitted to the smartphone when a connection is established (Step 8). Since the log file is recorded on the smartphone, log is created from the perspective of the phone. The GATT address created in Step 1 will be destroyed (Step 10) and some intermediate steps (Step 2~9) are omitted if the device is out of Bluetooth range of the band.

1.2 Cloud Level Analysis

1.2.1 Google OnHub

There are about eight OnHub-related data sets that can be acquired from the server, and we describe the analysis method for the diagnostic-report in this section. Since the report is partially encoded with protobuf, the text is not visible. We used the parsing tool 'onhubdump' in GitHub, which converts the original OnHub diagnostic-report to the JSON file format. Fig. 2-7 shows the objects that included in the result file.

"files", "wanInfo" and "infoJSON" objects in this JSON file contain information about devices that connected to or disconnected from the router. "wanInfo" and "infoJSON" contain information about the devices' and "files" contains the actual log messages. The specific objects to check are as follows.

Fig. 2-7. Json File Parsed with Json Parser Online

o Log Messages in certain Time
 - “files” - “content” with “path” = /var/log/messages.x
o MAC / IP Address
 - “wanInfo”
o Device Name
 - “infoJSON” - “_apState” - “_stations” - (“_dhcpHostname”, “_mdnsNames”)

Generally, log data can be analyzed based on some keywords. The keywords we selected for parsing /var/log/messages are ‘Connected’ and ‘Disconnected’ (Fig. 2-8). The Timestamp , MAC address and Connection State can be obtained and the MAC address coincides with only the first three bytes.

```
2017-07-17T06:11:55.142527+00:00 INFO hostapd[7128]: wlan-5000mhz: STA 109266000026      WPA: received EAPOL-Key fra
2017-07-17T06:11:55.144566+00:00 INFO hostapd[7128]: wlan-5000mhz: STA 109266000026      IEEE 802.11: Connected
2017-07-17T06:11:55.145351+00:00 INFO hostapd[7128]: wlan-5000mhz: IEEE 802.11 AP-STA-CONNECT 109266000026      time
2017-07-17T06:15:21.677574+00:00 INFO hostapd[7128]: wlan-5000mhz: STA 109266000026      IEEE 802.11: Disconnected
2017-07-17T06:15:21.685326+00:00 INFO hostapd[7128]: wlan-5000mhz: STA 109266000026      IEEE 802.11: disassociated
2017-07-17T06:15:22.229716+00:00 NOTICE kernel: [343879.999746] [phy1] FWLOG: [83690328] WAL_DBGID_SECURITY_UCAST_KE
```

Fig. 2-8. Part of the OnHub Log Messages

Fig. 2-9. Contents of "wanInfo"

The contents of "wanInfo" and "infoJSON" are in Fig. 2-9 and Fig. 2-10.

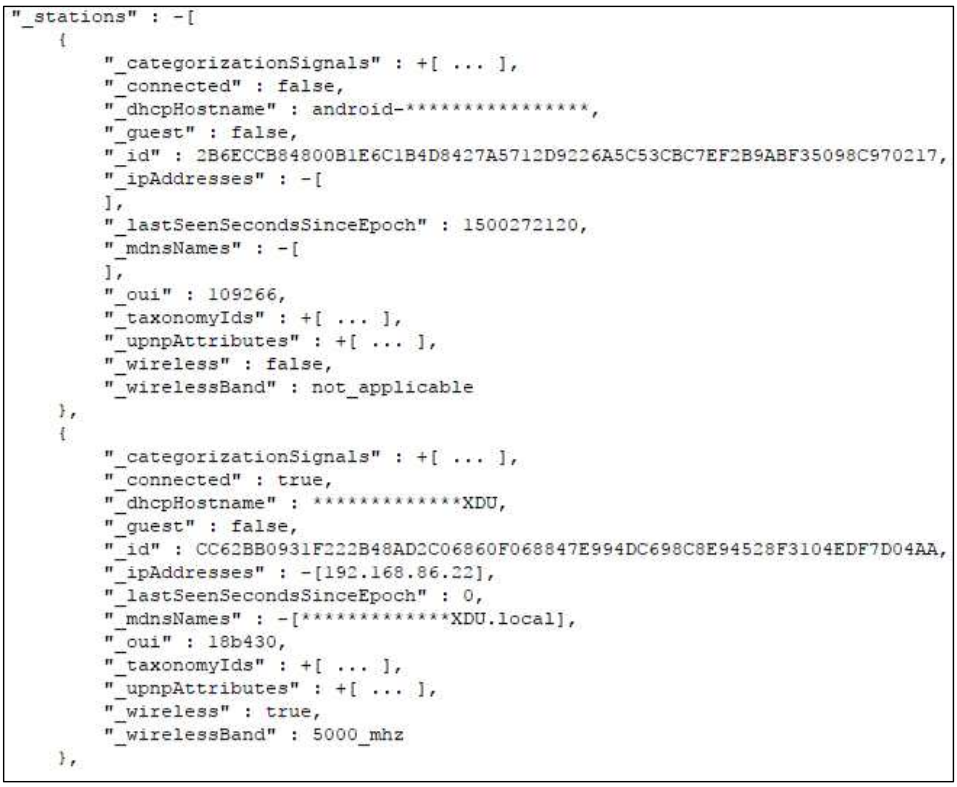


Fig. 2-10. Contents of "infoJSON"

1.2.2 Amazon Echo

As mentioned in Chapter Ⅰ, users can not only manage to-do lists, now playing music and shopping lists but also check their conversation history using the smart speaker Amazon Echo. It is necessary to acquire meaningful user data for forensic investigation and such user data can be obtained from a mobile device or a web server.

The mobile device connected to the Echo stores data in database format. The 'Amazon Alexa' application uses two databases; 'map_data_storage.db' and 'DataStore.db'. One is for logged on user information and the other is for managing to-do/shopping lists.

If the forensic investigator can obtain the user credentials, he or she can access the Amazon web server to acquire user data. The Amazon Echo APIs are not officially open to the public; however, there is an unofficial API list studied at Korea University. Some of these APIs are listed in Table 2-3. JSON-formatted data is returned from these APIs.

Table 2-3. Unofficial API List for Amazon Echo

Category	API
To-do list	https://pitangui.amazon.com/api/todos? type=TASK&size={}
Shopping list	https://pitangui.amazon.com/api/todos? type=SHOPPING_ITEM&size={}
Timer and alarm list	https://pitangui.amazon.com/api/notifications
Music Playing list	https://pitangui.amazon.com/api/media/historical-queue? deviceSerialNumber={}&deviceType={}&size={}&offset=-1
Conversation History	https://pitangui.amazon.com/api/activities? startTime={}&size={}&offset=-1

As most users run applications or SmartHome services through voice commands, 'Conversation History (activities)' is the most important data.

Fig. 2-11 shows a JSON file for one conversation record. 'Summary' is the user's request to the speaker, and 'creationTimestamp' is the time when the request was made. The associated voice file can be obtained with 'utteranceId' and the API 'https://pitangui.amazon.com/api/utterance/audio/data?id={originalAudioId or utteranceId}'.

1.3 Network Level Analysis

Tcpdump can be analyzed with Wireshark. Wireshark is a free and open source software for analyzing network packets. Objectives include network problems, analysis, software and communication protocol development, and training.

```
{
activity: {
_disambiguationId: null,
activityStatus: "SUCCESS",
creationTimestamp: 1500270331742,
description: "{"summary":"wake up","firstUtteranceId":"AB72C64C86AW2:1.0/2017/07/17/05/B0F00715535302W5/45:28::TNIH_2V.0
37537e28de10ZXV/1","firstStreamId":"AB72C64C86AW2:1.0/2017/07/17/05/B0F00715535302W5/45:28::TNIH_2V.0d0117fc-800c-43e5-a
domainAttributes: "{"disambiguated":false,"nBestList":[{"entryType":"Knowledge","mainEntity":{"tkid":"[fake editorial en
card":"false","background":"CustomizeColor"}},"answerText":"Good Morning! I've got some sweet news for you. Today is Nat
scream for ice cream at the same time, things are gonna get noisy!","answered":true,"validForGUI":true,"domains":["[edit
#489694]"],"answerEntities":[{"tkid":"[fake editorial entity]","properties":{"background-color":"#489694","suppress-card
up","spokenAnswerSsml":"<speak><prosody volume=\"x-loud\"><p xmlns:ivona=\"http://www.ivona.com/2009/12/ssml\">Good Morn
might want to pick up some ear plugs. If we all scream for ice cream at the same time, things are gonna get
noisy!<\/p><\/prosody><metadata><promptMetadata><promptId>AnswerSsml<\/promptId><namespace>SmartDJ.MusicQA<\/namespace><
4eaf-93e9-1130c2db01fa<\/variant><condition/><weight>1<\/weight><stageVersion>Adm-20141203_202706-
183<\/stageVersion><promptData><namespace>SmartDJ.MusicQA<\/namespace><overrideId/><prosodyPreRenderHook/><answer>&lt;p
sweet news for you. Today is National Ice Cream Day. But you might want to pick up some ear plugs. If we all scream for
noisy!&lt;/p&gt;<\/answer><promptID>AnswerSsml<\/promptID><\/promptData><\/promptMetadata><\/metadata><\/speak>","search
for you. Today is National Ice Cream Day. But you might want to pick up some ear plugs. If we all scream for ice cream a
noisy!","understood":true,"answerListIntroductionText":"Good Morning! I've got some sweet news for you. Today is Nationa
for ice cream at the same time, things are gonna get noisy!"}]}",
domainType: null,
feedbackAttributes: null,
id: "A32TRBM6QOXJ5H#1500270331742#AB72C64C86AW2#B0F00715535302W5",
intentType: null,
providerInfoDescription: null,
registeredCustomerId: "A32TRBM6QOXJ5H",
sourceActiveUsers: null,
sourceDeviceIds: [
{e
deviceAccountId: null,
deviceType: "AB72C64C86AW2",
serialNumber: "B0F00715535302W5"
}
],
utteranceId: "AB72C64C86AW2:1.0/2017/07/17/05/B0F00715535302W5/45:28::TNIH_2V.0d0117fc-800c-43e5-a052-37537e28de10ZXV",
version: 1
}
}
```


Fig. 2-11. A Json File related to Conversation History

The UI for Wireshark is divided into three parts. 'Packet List( )' shows all captured packets. The columns are number, time, source, destination, protocol, length, and information. The 'Packet Details( )' area analyzes and displays the information for the selected packet. Finally, 'Packet bytes( )' shows the value of the selected packet in binary form.

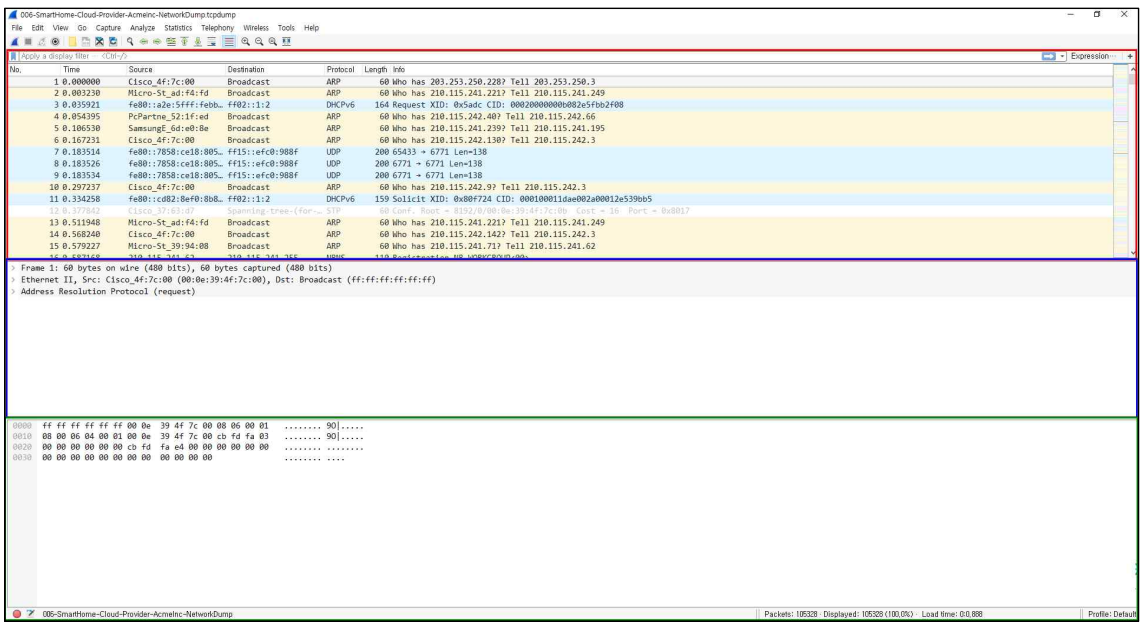


Fig. 2-12. The Wireshark GUI

The provided tcpdump captured the packets from 2017-07-17 18:00:57 to 2017-07-17 18:58:00 in Korea time (UTC+9), capturing a total of 105,328 packets. Wireshark provides various filtering functions. For example, you can filter by the desired MAC or IP address, and also by protocol. Examples of supported commands are shown below.

Table 2-4. Wireshark Instructions

Instruction	Contents
tcp dst port 9999	Packet destination is TCP port 9999
ip src host 192.168.0.1	A packet with a souce IP address of 192.168.0.1
host 192.168.0.1	Packets with a source and destination IP address of 192.168.0.1
not imcp	Exclude the imcp protocol
ethr.addr == B8:27:EB:E6:8D:79	B8: 27: EB: E6: 8D: 79 where the packet is the source or destination
eth.src == B8:27:EB:E6:8D:79	B8: 27: EB: E6: 8D: 79 where the packet is the source
eth.dst == B8:27:EB:E6:8D:79	B8: 27: EB: E6: 8D: 79 where the packet is the destination
ip.addr == 192.168.0.1	192.168.0.1 where the packet is the source or destination
...	...

Wireshark also provides statistics. Using the statistics endpoint feature, you can monitor which devices are using the packets.

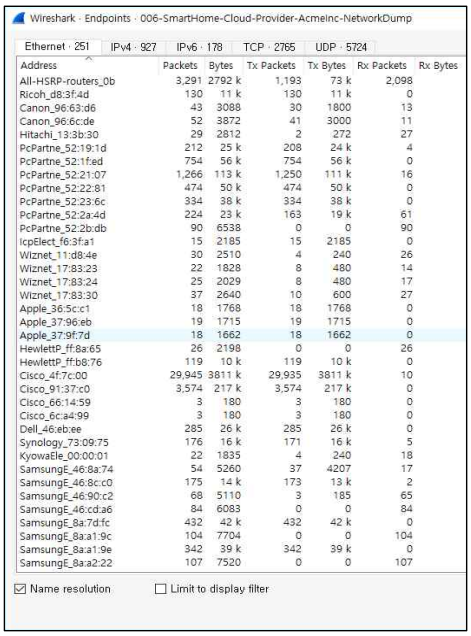


Fig. 2-13. Wireshark Endpoint Feature

2. Acquired Evidence Files

In this subsection, we lists the path and timestamps of the evidence files that should be analyzed in this scenario. Encase and MD-RED are used to extract the files.

2.1 Image of Raspberry Pi

As explained in the device level analysis, we used database files and network information as evidence. All .db files and network information in the Raspberry Pi are as follows.

Table 2-5. All .db Files Raspberry Pi

Path	Filename	Last Modified Time (UTC+09:00)
/home/osmc/.kodi/userdata/Database	ADSP0.db	2017-07-13 17:30:41
/home/osmc/.kodi/userdata/Database	Addons27.db	1970-01-01 09:00:09
/home/osmc/.kodi/userdata/Database	Epg11.db	2017-07-13 17:30:41
/home/osmc/.kodi/userdata/Database	MyMusic60.db	2017-07-13 17:30:40
/home/osmc/.kodi/userdata/Database	MyVideos107.db	2017-07-17 15:19:37
/home/osmc/.kodi/userdata/Database	TV29.db	2017-07-13 17:30:40
/home/osmc/.kodi/userdata/Database	Textures13.db	2017-07-17 15:03:32
/home/osmc/.kodi/userdata/Database	ViewModes6.db	2017-07-13 17:37:03
/usr/lib/arm-linux-gnueablhf/avahi/	Service-types.db	2015-04-14 07:31:34

Table 2-6. Connected Network Information of Raspberry Pi

Full Path	Last Modified Time (UTC+09:00)	Content
/var/lib/bluetooth/B8:27:EB:E6:8D:79	2017-07-16 05:50:14	-
/var/lib/bluetooth/B8:27:EB:E6:8D:79/cache/88:0F:10:F6:C8:B7	2017-07-16 05:44:55	[General] Name=MI1A
/var/lib/bluetooth/B8:27:EB:E6:8D:79/cache/74:C2:46:88:5D:09	2017-07-16 05:50:14	[General] Name=Echo-2WS

2.2 Image of Betty's Samsung Galaxy Note Ⅱ

The following table is a list of evidence files acquired from Betty's smartphone. We extract all database files to investigate traces of application usage and logs that shows the operation of the smart device connected to her phone.

Table 2-7. List of Application Usage Files in Betty's Phone

Partition	File Path
USERDATA	/data\system\usagestats\usage-20170717

Table 2-8. List of Files related to Bluetooth and Wi-Fi in Betty's Phone

Partition	File Path
USERDATA	/data\misc\bluedroid\bt_config.xml
USERDATA	/data\misc\wifi\wpa_supplicant.conf
EFS	/efs\bluetooth\bt_addr
EFS	/efs\wifi\.mac.info

Table 2-9. List of Database Files in Betty's Phone

Partition	File Path
USERDATA	/data/com.amazon.dee.app/app_webview/databases/Databases.db
USERDATA	/data/com.amazon.dee.app/databases/DataStore.db
USERDATA	/data/com.amazon.dee.app/databases/map_data_storage_v2.db
USERDATA	/data/com.android.bluetooth/databases/btopp.db
USERDATA	/data/com.android.browser/databases/browser2.db
USERDATA	/data/com.android.browser/databases/webview.db
USERDATA	/data/com.android.chrome/app_chrome/Default/databases/Databases.db
USERDATA	/data/com.android.chrome/app_chrome/Default/Offline Pages/metadata/OfflinePages.db
USERDATA	/data/com.android.email/databases/EmailProvider.db
USERDATA	/data/com.android.email/databases/EmailProviderBody.db
USERDATA	/data/com.android.providers.calendar/databases/calendar.db
USERDATA	/data/com.android.providers.contacts/databases/contacts2.db
USERDATA	/data/com.android.providers.downloads/databases/downloads.db
USERDATA	/data/com.android.providers.media/databases/external.db
USERDATA	/data/com.android.providers.media/databases/internal.db
USERDATA	/data/com.android.providers.settings/databases/settings.db

USERDATA	/data/com.android.providers.telephony/databases/mmssms.db
USERDATA	/data/com.android.settings/databases/myplace.db
USERDATA	/data/com.android.vending/databases/localappstate.db
USERDATA	/data/com.dropbox.android/databases/evernote_jobs.db
USERDATA	/data/com.dropbox.android/databases/prefs.db
USERDATA	/data/com.dropbox.android/databases/prefs-shared.db
USERDATA	/data/com.google.android.apps.books/databases/books.db
USERDATA	/data/com.google.android.apps.books/databases/google_analytics_v2.db
USERDATA	/data/com.google.android.apps.books/databases/google_analytics_v4.db
USERDATA	/data/com.google.android.apps.books/files/accounts/bettyhallym@gmail.com/books2.db
USERDATA	/data/com.google.android.apps.docs/databases/DocList.db
USERDATA	/data/com.google.android.apps.docs/databases/google_analytics_v2.db
USERDATA	/data/com.google.android.apps.docs/databases/google_analytics_v4.db
USERDATA	/data/com.google.android.apps.maps/databases/gmm_myplaces.db
USERDATA	/data/com.google.android.gm/databases/EmailProvider.db
USERDATA	/data/com.google.android.gm/databases/mailstore.bettyhallym@gmail.com.db
USERDATA	/data/com.google.android.talk/databases/apn.db
USERDATA	/data/com.google.android.talk/databases/babel0.db
USERDATA	/data/com.google.android.talk/databases/babel1.db
USERDATA	/data/com.google.android.talk/databases/google_analytics_v4.db
USERDATA	/data/com.google.android.youtube/databases/downloads.db
USERDATA	/data/com.google.android.youtube/databases/google_analytics.db
USERDATA	/data/com.google.android.youtube/databases/google_conversion_tracking.db
USERDATA	/data/com.sec.android.app.sns3/databases/snsDB.db
USERDATA	/data/com.sec.android.app.sns3/databases/snsFacebookDB.db
USERDATA	/data/com.sec.android.app.sns3/databases/snsFourSquareDB.db
USERDATA	/data/com.sec.android.app.sns3/databases/snsGooglePlusDB.db
USERDATA	/data/com.sec.android.app.sns3/databases/snsInstagramDB.db
USERDATA	/data/com.sec.android.app.sns3/databases/snsLinkedInDB.db
USERDATA	/data/com.sec.android.app.sns3/databases/snsTwitterDB.db
USERDATA	/data/com.xiaomi.hm.health/databases/mistat.db
USERDATA	/data/com.xiaomi.hm.health/databases/sports.db

2.3 Image of Simon's Samsung Galaxy Note Ⅱ

The following tables are the list of evidence files acquired from Simon's smartphone. We extracted all db files, application usage file, and network information files.

Table 2-10. List of Application Usage Files in Simon's Phone

Partition	File Path
USERDATA	/data\system\usagestats\usage-20170717

Table 2-11. List of Files related to Bluetooth and Wi-Fi in Simon's Phone

Partition	File Path
USERDATA	/data\misc\bluedroid\bt_config.xml
USERDATA	/data\misc\wifi\wpa_supplicant.conf
EFS	/efs\bluetooth\bt_addr
EFS	/efs\wifi\.mac.info

Table 2-12. List of Database Files in Simon's Phone

Partition	File Path
USERDATA	/data\data\com.smldm\databases\wssdmdatabase.db
USERDATA	/data\data\com.android.browser\databases\webviewCookiesChromiumPrivate.db
USERDATA	/data\data\com.android.browser\databases\webviewCookiesChromium.db
USERDATA	/data\data\com.android.browser\databases\webview.db
USERDATA	/data\data\com.android.browser\app_icons\WebpageIcons.db
USERDATA	/data\data\com.sec.android.voltesettings\databases\VTErrorTableContent1.db
USERDATA	/data\data\com.sec.android.app.videoplayer\databases\video_remote_file.db
USERDATA	/data\data\com.sec.pcw.device\databases\value.db
USERDATA	/data\data\com.android.providers.userdictionary\databases\user_dict.db
USERDATA	/data\data\com.google.android.gms\databases\upload_queue.db
USERDATA	/data\data\com.google.android.apps.maps\databases\ue3.db
USERDATA	/data\data\com.smartthings.android\databases\ua_preferences.db
USERDATA	/data\data\com.smartthings.android\databases\ua_analytics.db
USERDATA	/data\data\com.vsray.remote.control\databases\ua.db
USERDATA	/data\data\com.hp.android.printservice\databases\tray.db
USERDATA	/data\data\com.google.android.apps.plus\databases\trash.db
USERDATA	/data\data\com.skt.prod.dialer\databases\tphone.db

USERDATA	/data\system\users\0\accounts.db
USERDATA	/data\data\com.sec.android.app.clockpackage\databases\alarm.db
USERDATA	/data\data\com.skt.skaf.OA00199800\databases\aom.db
USERDATA	/data\data\com.google.android.talk\databases\apn.db
USERDATA	/data\data\com.google.android.gms\databases\app_state.db
USERDATA	/data\data\com.android.browser\app_appcache\ApplicationCache.db
USERDATA	/data\data\com.sec.android.app.videoplayer\databases\ThumbnailMgr.db
USERDATA	/data\data\com.sec.android.provider.snote\databases\thumbnaildb.db
USERDATA	/data\data\com.google.android.gms\databases\auto_complete_suggestions.db
USERDATA	/data\data\com.wssyncmldm\databases\wssdmdatabase.db
USERDATA	/data\data\com.android.phone\databases\autoreject.db
USERDATA	/data\data\com.google.android.talk\databases\babel0.db
USERDATA	/data\data\com.skt.skaf.l001mtm091\databases\text_or_url.db
USERDATA	/data\data\com.android.providers.telephony\databases\telephony.db
USERDATA	/data\data\com.skt.tbagplus\databases\tcloud.db
USERDATA	/data\data\com.google.android.talk\databases\babel1.db
USERDATA	/data\data\com.sec.android.provider.badge\databases\badge.db
USERDATA	/data\data\com.google.android.gms\cache\beacon_message_cache.db
USERDATA	/data\data\com.google.android.youtube\databases\bgol_tasks.db
USERDATA	/data\data\com.google.android.apps.books\databases\books.db
USERDATA	/data\data\com.google.android.apps.books\files\accounts\simonhallym@gmail.com\books2.db
USERDATA	/data\data\com.google.android.apps.books\databases\books3.db
USERDATA	/data\data\com.android.browser\databases\browser2.db
USERDATA	/data\data\com.android.bluetooth\databases\btopp.db
USERDATA	/data\data\com.wssnps\databases\wssnpsdb.db
USERDATA	/data\data\com.sec.android.widgetapp.ap.yonhapnews\databases\YonhapNews.db
USERDATA	/data\data\com.google.android.gsf\databases\talk.db
USERDATA	/data\data\com.sec.android.app.sysscope\databases\SysScope.db
USERDATA	/data\data\com.skt.skaf.OA00026910\databases\swdb.db
USERDATA	/data\data\com.android.vending\databases\suggestions.db
USERDATA	/data\data\com.google.android.gsf\databases\subscribedfeeds.db
USERDATA	/data\data\com.android.browser\app_geolocation\CachedGeoposition.db
USERDATA	/data\system\ssrm_secure.db
USERDATA	/data\data\com.sec.android.app.sns3\databases\snsTwitterDB.db

USERDATA	/data\data\com.sec.android.app.sns3\databases\snsLinkedInDB.db
USERDATA	/data\data\com.android.providers.calendar\databases\calendar.db
USERDATA	/data\data\com.google.android.gms\databases\cast.db
USERDATA	/data\data\com.vsray.remote.control\databases\cc.db
USERDATA	/data\data\com.android.browser\databases\autofill.db
USERDATA	/data\data\com.sec.android.daemonapp.ap.yonhapnews\databases\YonhapNewsDaemon.db
USERDATA	/data\data\com.sec.android.app.sns3\databases\snsInstagramDB.db
USERDATA	/data\data\com.sec.android.app.sns3\databases\snsGooglePlusDB.db
USERDATA	/data\data\com.sec.android.app.sns3\databases\snsFourSquareDB.db
USERDATA	/data\data\com.sec.android.app.sns3\databases\snsFacebookDB.db
USERDATA	/data\data\com.sec.android.app.sns3\databases\snsDB.db
USERDATA	/data\data\com.google.android.gms\databases\snet_safe_browsing.db
USERDATA	/data\data\com.google.android.gms\databases\snet_files_info.db
USERDATA	/data\data\com.samsung.android.scloud.sync\databases\smemofiletracker.db
USERDATA	/data\data\com.samsung.android.sm\databases\sm.db
USERDATA	/data\data\com.sec.android.providers.downloads\databases\sisodownloads.db
USERDATA	/data\data\com.android.providers.settings\databases\settings.db
USERDATA	/data\data\com.google.android.talk\databases\concurrent_service_task_store.db
USERDATA	/data\data\com.google.android.gms\databases\config.db
USERDATA	/data\data\com.sec.android.widgetapp.favoriteswidget\databases\senior_favorite.db
USERDATA	/data\data\com.osp.app.signin\databases\samsungaccount.db
USERDATA	/data\system\rut.db
USERDATA	/data\data\com.google.android.gms\databases\rmq.db
USERDATA	/data\data\com.google.android.partnersetup\databases\rlz_data.db
USERDATA	/data\data\com.android.chrome\app_chrome\Default\Offline Pages\request_queue\Request Queue.db
USERDATA	/data\data\com.sec.android.nearby.mediaserver\databases\config.db
USERDATA	/data\data\com.google.android.gms\databases\connectionconfig.db
USERDATA	/data\data\com.android.providers.contacts\databases\contacts2.db
USERDATA	/data\data\com.google.android.gms\databases\reminders.db
USERDATA	/data\data\com.google.android.videos\databases\purchase_store.db
USERDATA	/data\data\com.android.providers.contacts\databases\profile.db
USERDATA	/data\data\com.sec.dsm.system\databases\profile.db
USERDATA	/data\data\com.android.chrome\app_chrome\Default\previews_opt_out.db
USERDATA	/data\data\com.dropbox.android\databases\prefs.db

USERDATA	/data\data\com.dropbox.android\databases\prefs-shared.db
USERDATA	/data\data\com.sec.android.app.samsungapps\databases\ppmt.db
USERDATA	/data\system\container\databases\container.db
USERDATA	/data\data\com.google.android.googlequicksearchbox\app_si\shortcuts_content_store\content_store.db
USERDATA	/data\data\com.google.android.googlequicksearchbox\app_si\now_content_store\content_store.db
USERDATA	/data\data\com.google.android.googlequicksearchbox\app_si\state_dump_event_content_store\content_store.db
USERDATA	/data\data\com.google.android.googlequicksearchbox\app_si\homescreen_shortcut_content_store\content_store.db
USERDATA	/data\data\com.google.android.googlequicksearchbox\app_si\srp_content_store\content_store.db
USERDATA	/data\data\com.google.android.gms\databases\context___ContextManagerNullAccount__.db
USERDATA	/data\data\com.google.android.gms\databases\context_feature_default.db
USERDATA	/data\data\com.google.android.gms\databases\context_simonhallym_gmail.com.db
USERDATA	/data\data\com.samsung.android.providers.context\databases\ContextLog_0.db
USERDATA	/data\data\com.amazon.dee.app\app_webview\databases\Databases.db
USERDATA	/data\data\com.android.browser\app_databases\Databases.db
USERDATA	/data\data\com.amazon.dee.app\databases\DataStore.db
USERDATA	/data\data\com.policydm\databases\policydmdb.db
USERDATA	/data\data\com.google.android.gms\databases\pluscontacts.db
USERDATA	/data\data\com.google.android.gms\databases\plus.db
USERDATA	/data\data\com.google.android.gms\databases\device_connections.db
USERDATA	/data\data\com.google.android.apps.access.wifi.consumer\databases\devices_simonhallym_gmail.com.db
USERDATA	/data\data\com.google.android.gms\databases\playlog.db
USERDATA	/data\data\com.samsung.android.intelligenceservice\databases\Place.db
USERDATA	/data\data\com.sec.android.gallery3d\databases\picasa.db
USERDATA	/data\data\com.skt.prod.phonebook\databases\phonebook.db
USERDATA	/data\data\com.skt.tbagplus\databases\devicesupportinfo.db
USERDATA	/data\data\com.google.android.gms\databases\dg.db
USERDATA	/data\data\com.google.android.gms\databases\dgp.db
USERDATA	/data\data\com.samsung.InputEventApp\databases\diagprovider.db
USERDATA	/data\data\com.google.android.gms\databases\phenotype.db
USERDATA	/data\data\com.android.settings\databases\personalvibration.db

USERDATA	/data\data\com.android.providers.media\databases\person.db
USERDATA	/data\data\com.sec.spp.push\databases\checker.db
USERDATA	/data\data\com.google.android.gms\databases\peoplelog.db
USERDATA	/data\data\com.sec.penup\databases\PenupResponseDB.db
USERDATA	/data\data\com.android.providers.partnerbookmarks\databases\partnerBookmarks.db
USERDATA	/data\data\com.android.vending\databases\package_verification.db
USERDATA	/data\data\com.skt.skaf.OA00026910\databases\oswdata.db
USERDATA	/data\data\com.osp.app.signin\databases\osp.db
USERDATA	/data\data\com.android.providers.telephony\opname.db
USERDATA	/data\data\com.osp.app.signin\databases\openData.db
USERDATA	/data\data\com.android.chrome\app_chrome\Default\Offline Pages\metadata\OfflinePages.db
USERDATA	/data\system\dmappmgr.db
USERDATA	/data\data\com.google.android.apps.docs\databases\DocList.db
USERDATA	/data\data\com.android.providers.telephony\databases\nwk_info.db
USERDATA	/data\data\com.google.android.gms\databases\ns.db
USERDATA	/data\data\com.android.browser\app_webnotification\NotificationPermissions.db
USERDATA	/data\data\com.google.android.gms\databases\DocList.db
USERDATA	/data\data\com.android.providers.downloads\databases\downloads.db
USERDATA	/data\data\com.google.android.gms\databases\downloads.db
USERDATA	/data\data\com.google.android.youtube\databases\downloads.db
USERDATA	/data\system\databases\drmdatabase.db
USERDATA	/data\system\container\databases\ecpp.enterprise.db
USERDATA	/data\data\com.google.android.gms\databases\node.db
USERDATA	/data\data\com.android.email\databases\EmailProvider.db
USERDATA	/data\data\com.google.android.gm\databases\EmailProvider.db
USERDATA	/data\data\com.google.android.gm\databases\EmailProviderBody.db
USERDATA	/data\data\com.google.android.gms\databases\NetworkUsage.db
USERDATA	/data\data\com.android.email\databases\EmailProviderBody.db
USERDATA	/data\system\enterprise.db
USERDATA	/data\data\com.google.android.gms\files\nearby-discovery\nearby_discovery_scan_result_cache.db
USERDATA	/data\data\com.google.android.gms\files\nearby-discovery\nearby_discovery_item_cache.db
USERDATA	/data\data\com.android.settings\databases\mysettings.db
USERDATA	/data\data\com.android.settings\databases\myplace.db
USERDATA	/data\data\com.sec.android.app.music\databases\music_player.db

USERDATA	/data\data\com.android.providers.telephony\databases\mmssms.db
USERDATA	/data\data\com.google.android.gms\databases\metadata.db
USERDATA	/data\data\com.iloen.melon\databases\melonplaylist.db
USERDATA	/data\media\0\melon\db\meloninternal.db
USERDATA	/data\media\0\melon\db\melon.db
USERDATA	/data\data\com.iloen.melon\databases\melon.db
USERDATA	/data\data\com.sktelecom.hoppin.mobile\databases\media.db
USERDATA	/data\data\com.google.android.apps.plus\databases\es0.db
USERDATA	/data\data\com.dropbox.android\databases\evernote_jobs.db
USERDATA	/data\data\com.android.providers.media\databases\external.db
USERDATA	/data\data\com.google.android.gms\databases\matchstickv9.db
USERDATA	/data\data\com.sec.android.SimpleWidget\databases\favoriteapp.db
USERDATA	/data\data\com.sec.android.favoriteappwidget\databases\favoriteapp.db
USERDATA	/data\data\com.android.vending\databases\fetch_suggestions.db
USERDATA	/data\data\com.sec.android.gallery3d\databases\FileInfo.db
USERDATA	/data\data\com.amazon.dee.app\databases\map_data_storage_v2.db
USERDATA	/data\data\com.sec.android.provider.snote\databases\FmFiles.db
USERDATA	/data\data\com.fmm.dm\databases\fmmdm.db
USERDATA	/data\data\com.sec.penup\databases\Friends.db
USERDATA	/data\data\com.google.android.gms\databases\games_79ac6bb4.db
USERDATA	/data\data\com.google.android.gms\databases\gass.db
USERDATA	/data\data\com.google.android.gm\databases\mailstore.simonhallym@gmail.com.db
USERDATA	/data\data\com.sec.android.provider.logsprovider\databases\logs.db
USERDATA	/data\system\locksettings.db
USERDATA	/data\data\com.LocalFota\databases\localfota.db
USERDATA	/data\data\com.tgrape.android.radar\databases\GC.db
USERDATA	/data\data\com.google.android.gms\databases\gcm_registrar.db
USERDATA	/data\data\com.android.browser\app_geolocation\GeolocationPermissions.db
USERDATA	/data\data\com.google.android.apps.maps\databases\gmm_storage.db
USERDATA	/data\data\com.google.android.apps.maps\databases\gmm_sync.db
USERDATA	/data\data\com.google.android.gms\databases\gms.notifications.db
USERDATA	/data\data\com.google.android.gms\databases\google_account_history.db
USERDATA	/data\data\com.google.android.youtube\databases\google_analytics.db
USERDATA	/data\data\com.google.android.gms\databases\google_analytics.db
USERDATA	/data\data\com.google.android.apps.docs\databases\google_analytics_v2.db

USERDATA	/data\data\com.google.android.gm\databases\google_analytics_v2.db
USERDATA	/data\data\com.hp.android.printservice\databases\google_analytics_v4.db
USERDATA	/data\data\com.google.android.apps.magazines\databases\google_analytics_v4.db
USERDATA	/data\data\com.smartthings.android\databases\google_analytics_v4.db
USERDATA	/data\data\com.google.android.apps.books\databases\google_analytics_v4.db
USERDATA	/data\data\com.google.android.apps.access.wifi.consumer\databases\google_analytics_v4.db
USERDATA	/data\data\com.google.android.talk\databases\google_analytics_v4.db
USERDATA	/data\data\com.google.android.gms\databases\google_analytics_v4.db
USERDATA	/data\data\com.google.android.apps.docs\databases\google_analytics_v4.db
USERDATA	/data\data\com.google.android.gms\databases\google_app_measurement.db
USERDATA	/data\data\com.ifttt.ifttt\databases\google_app_measurement.db
USERDATA	/data\data\com.ifttt.ifttt\databases\google_app_measurement_local.db
USERDATA	/data\data\com.google.android.youtube\databases\google_conversion_tracking.db
USERDATA	/data\data\com.google.android.gsf\databases\googlesettings.db
USERDATA	/data\data\com.android.keychain\databases\grants.db
USERDATA	/data\data\com.google.android.gsf\databases\gservices.db
USERDATA	/data\data\com.android.vending\databases\localappstate.db
USERDATA	/data\data\com.samsung.helphub\databases\HelpHub.db
USERDATA	/data\data\com.sec.android.voltesettings\databases\HiddenMenuContentDatabase.db
USERDATA	/data\data\com.samsung.android.sm\databases\history.db
USERDATA	/data\data\com.google.android.gms\databases\icing-indexapi-errors.db
USERDATA	/data\data\com.google.android.gms\databases\icing-indexapi.db
USERDATA	/data\data\com.google.android.gms\databases\icing_contacts.db
USERDATA	/data\data\com.google.android.gms\databases\icing_mmssms.db
USERDATA	/data\data\com.android.vending\databases\library.db
USERDATA	/data\data\com.google.android.youtube\databases\identity.db
USERDATA	/data\data\com.ifttt.ifttt\databases\ifttt_grizzly.db
USERDATA	/data\data\com.sec.android.app.FileShareServer\databases\inbound_transfer.db
USERDATA	/data\data\com.sec.android.app.samsungapps\databases\info2.db
USERDATA	/data\data\com.android.providers.media\databases\internal.db
USERDATA	/data\data\com.google.android.gm\databases\internal.simonhallym@gmail.com.db
USERDATA	/data\data\com.google.android.gms\databases\iu.upload.db
USERDATA	/data\data\com.google.android.apps.plus\databases\iu.upload.db
USERDATA	/data\data\com.google.android.gms\databases\keys.db
USERDATA	/data\data\com.samsung.klmsagent\databases\klms.db

USERDATA	/data\data\com.google.android.googlequicksearchbox\databases\launcher.db
USERDATA	/data\data\com.sec.android.app.launcher\databases\launcher.db
USERDATA	/data\data\com.google.android.gms\databases\id_as_screens.db

2.4 Diagnostic Report from Google OnHub

The original OnHub diagnostic report file needs to be parsed since some part of the report is encoded. We use the parsing tool for OnHub diagnostic reports on GitHub. After parsing the report, we can see the contents saved as various file paths and commands. Table 2-13 shows a list of file path and commands in OnHub diagnostic report.

Table 2-13. List of File Paths and Commands in OnHub

File Path
/etc/lsb-release
/etc/resolv.conf
/proc/net/arp
/proc/slabinfo
/sys/firmware/log
/tmp/debug-log
/var/log/boot.log
/var/log/net.log
/var/log/net.1.log
/var/log/update_engine/update_engine.19700101-000009
/var/log/webservd/2017-07-17.log
/var/log/webservd/2017-07-16.log
/var/lib/ap/monitor/wan_idle_usage
/var/log/messages
/var/log/messages.1
/mnt/stateful_partition/var/log/messages.3
/mnt/stateful_partition/var/log/messages.1
/mnt/stateful_partition/var/log/messages.4
/mnt/stateful_partition/var/log/messages.2
/mnt/stateful_partition/var/log
/mnt/stateful_partition/var/log/update_engine/update_engine.19700101-000009
/mnt/stateful_partition/var/log/update_engine

Commands
/bin/ifconfig
/usr/sbin/iw dev wlan-2400mhz station dump
/usr/sbin/iw dev wlan-5000mhz station dump
/usr/sbin/iw dev guest-2400mhz station dump
/usr/sbin/iw dev guest-5000mhz station dump
/usr/sbin/iw dev
/sbin/brctl showstp br-lan
/sbin/brctl showmacs br-lan
/usr/sbin/ethtool –s wan0
/usr/sbin/ethtool –s lan0
/bin/route –n
/bin/ps auxwwf
/sbin/tc –s qdisc show dev wan0
/bin/cat /dev/ecm/ecm_db
/usr/sbin/iw dev mesh-5000mhz mpath dump
/usr/sbin/iw dev mesh-5000mhz mpp dump
/usr/sbin/iw dev mesh-5000mhz station dump
/usr/sbin/swconfig dev switch0 show

First, there are log messages in /var/log/messages or /var/log/message.* (* is a number starting from 1) (Fig. 2-14). Second, there is a list of MAC addresses for devices connected to OnHub (Fig. 2-15).

```
/var/log/messages
2017-07-17T06:56:17.403219+00:00 INFO ap-pipe-reader[19767]: main.go:52: Error reading from input: EOF
2017-07-17T06:56:17.417506+00:00 WARNING kernel: [346334.177538] init: ap-debug-log main process (19766) t
2017-07-17T06:56:17.417581+00:00 WARNING kernel: [346334.177740] init: ap-debug-log main process ended, re
2017-07-17T06:56:17.892187+00:00 INFO periodic_scheduler[14543]: cleanup_logs: job completed
2017-07-17T06:56:25.619774+00:00 INFO periodic_scheduler[14580]: cros-machine-id-regen: running /usr/sbin/
2017-07-17T06:56:25.692066+00:00 NOTICE cros-machine-id-regen[14594]: Not regenerating since we did so 111
2017-07-17T06:56:25.697916+00:00 INFO periodic_scheduler[14595]: cros-machine-id-regen: job completed
2017-07-17T06:56:44.627598+00:00 INFO kernel: [346361.395472] wlan-5000mhz: dropped frame to 109266000026
2017-07-17T06:56:44.627691+00:00 INFO kernel: [346361.395561] wlan-2400mhz: dropped frame to 109266000026
2017-07-17T06:56:44.633724+00:00 INFO ap-monitor[1281]: [INFO:ssdp_plugin.cc(43)] Found 0 SSDP services
2017-07-17T06:56:44.639286+00:00 INFO kernel: [346361.399601] wlan-5000mhz: dropped frame to b827eb000028
2017-07-17T06:56:44.639357+00:00 INFO kernel: [346361.399688] wlan-2400mhz: dropped frame to b827eb000028
2017-07-17T06:56:44.639388+00:00 INFO kernel: [346361.401522] wlan-5000mhz: dropped frame to 50f520000027
```

Fig. 2-14. Logs in /var/log/messages

```
enable_prioritized_device: false
disable_lan: false
wan_interface: "wan0"
dhcp_lease {
  mac_address: "2016d8000001"
  ip_address: "192.168.86.29"
}
dhcp_lease {
  mac_address: "109266000002"
  ip_address: "192.168.86.28"
}
dhcp_lease {
  mac_address: "d052a8000003"
  ip_address: "192.168.86.27"
}
dhcp_lease {
  mac_address: "b827eb000004"
  ip_address: "192.168.86.25"
}
dhcp_lease {
  mac_address: "50f520000005"
  ip_address: "192.168.86.26"
}
dhcp_lease {
  mac_address: "1caf05000006"
  ip_address: "192.168.86.24"
}
dhcp_lease {
  mac_address: "18b430000007"
  ip_address: "192.168.86.22"
}
dhcp_lease {
  mac_address: "a002dc000008"
  ip_address: "192.168.86.21"
}
wan_ipv4_address: "192.168.165.9"
upstream_name_server: "210.115.225.11"
enable_group_setup_network: false
disable_wireless_lan: false
enable_station_mode: false
wan_ipv4_gateway: "192.168.165.1"
is_channel_149_allowed: true
lan_link_local_ipv6_address: "fe80::6c51:9ff:fe3e:6cf8"
```


Fig. 2-15. List of MAC address in OnHub

2.5 Data from Amazon Echo / Alexa Cloud UI

Same as listed in the 'Overview of Challenge Data' (Chapter Ⅱ).

2.6 SmartHome Network Traffic Logs

Same as listed in the 'Overview of Challenge Data' (Chapter Ⅱ).

III. Digital Investigation

1. Results of Digital Investigation

In this section, we perform digital forensic investigation of the files extracted in Chapter Ⅱ. The analysis results described focuses on the files associated with this scenario.

1.1 Image of Raspberry Pi

1.1.1 Information about watching YouTube

In the Raspberry Pi image file, database files are organized by SQLite format. We used the SQLite Expert application for database analysis. The information about Simon's videos is stored in 'MyVideos107.db' file.

Fig. 3-1. YouTube Information in 'MyVideos107.db'

RecNo	idFile	idPath	strFilename	playCount	lastPlayed	dateAdded
Click here to define a filter						
1	1	1	plugin://plugin.video.youtube/play/?video_id=pF_rqav38Z4	1	2017-07-13 08:43:46	(null)
2	2	1	plugin://plugin.video.youtube/play/?video_id=7WX0-O_ENlk	1	2017-07-16 04:54:54	(null)
3	3	1	plugin://plugin.video.youtube/play/?video_id=ibOskbTPZYE	1	2017-07-17 02:07:30	(null)
4	4	1	plugin://plugin.video.youtube/play/?video_id=VKfbVLmkQUs	(null)	2017-07-17 02:19:37	(null)

'strFilename' column indicates the video URL. The play time for each video is 6 min 34 sec, 'None' for the second video, 4 min, 56 min 10 sec. The second video was denied in South Korea. However, it is not directly related to this scenario because 'lastPlayed' time is 2017-07-16 17:54:54 (UTC+9). The videos viewed close to the time of the scenario are 3 and 4.

The 'playCount' column shows how many times a video was watched. According to our experimental results, 1 means that the entire video was viewed, and (null) means that the video was interrupted. The running time of the fourth video is 56:10; So Simon did not watch the video until the end.

1.1.2 Bluetooth information

The Raspberry Pi is connected to two devices via Bluetooth. The filename is the MAC address and contains the name of the devices.

Table 3-1. Connected Network Information for Raspberry Pi

Bluetooth MAC address	Last Modified Time (UTC+09:00)	Content
88:0F:10:F6:C8:B7	2017-07-16 05:44:55	[General] Name=MI1A
74:C2:46:88:5D:09	2017-07-16 05:50:14	[General] Name=Echo-2WS

1.2 Image of Betty's Samsung Note Ⅱ

1.2.1 Remote-connected Devices

As shown in Fig. 3-2, the elements under the 'Local' tag indicates information about Betty's phone. Those under the 'Remote' tag can be classified based on the Bluetooth MAC address and we can obtain the names of all devices connected to the local device via Bluetooth. Table 3-2 displays the analysis results for 'bt_config.xml'.

Fig. 3-2. Contents of 'bt_config.xml'

Table 3-2. Device Information in 'bt_config.xml'

	Bluetooth MAC address	Name / Device Group	Time (UTC+9)
Local	1c:af:05:9e:19:74	Betty (SHV-E250L)	-
		Smartphone	
Remote	50:f5:20:a5:7d:cc	Simon (SHV-E250S)	2017.07.13 16:38:59
		Smartphone	
	88:0f:10:f6:c8:b7	MI1A	2017.07.13 17:10:46
		Smart band	
	74:c2:46:88:5d:09	Echo-2W5	-
		Smart speaker	

1.2.2 Connected Wi-Fi Information

Betty's smartphone has connected to three networks and the information for these networks is stored in 'wpa_supplicant.conf'. The SSID[5] and PSK (Pre-shared key) for the networks are listed in Table 3-3. The remaining information can be found in Fig. 3-3. Among the SSIDs

```
network={
    ssid="DFIRE"
    psk="D4nc3W1thDr4g0ns."
    key_mgmt=WPA-PSK
    priority=1
    frequency=2452
    autojoin=1
    usable_internet=0
    skip_internet_check=0
}

network={
    ssid="home"
    psk="iot14305"
    key_mgmt=WPA-PSK
    priority=3
    frequency=5745
    autojoin=1
    usable_internet=0
    skip_internet_check=0
}

network={
    ssid="HOME"
    psk="iot14305"
    key_mgmt=WPA-PSK
    priority=4
    frequency=2437
    autojoin=1
    usable_internet=0
    skip_internet_check=0
}
```

Fig. 3-3. Contents of 'wpa_supplicant.conf'

5) Service Set Identifier, serve as "network names" and are typically natural language labels.

Simon mentioned during the interrogation, there is no data about the guest network data on Betty's cell phone and the PSK of 'home' network is iot14305, not iot14306.

Table 3-3. Contents of 'wpa_supplicant.conf'

SSID	PSK
DFIRE	D4nc3W1thDr4g0ns.
home	iot14305
HOME	iot14305

1.2.3 List of Used Applications

'usage-20170717' stores the package names for mobile application and the names of activities activated by the user (Fig. 3-4) on specific date. Table 3-4 shows the analysis results and the application name corresponding with the packages executed on July 17th.

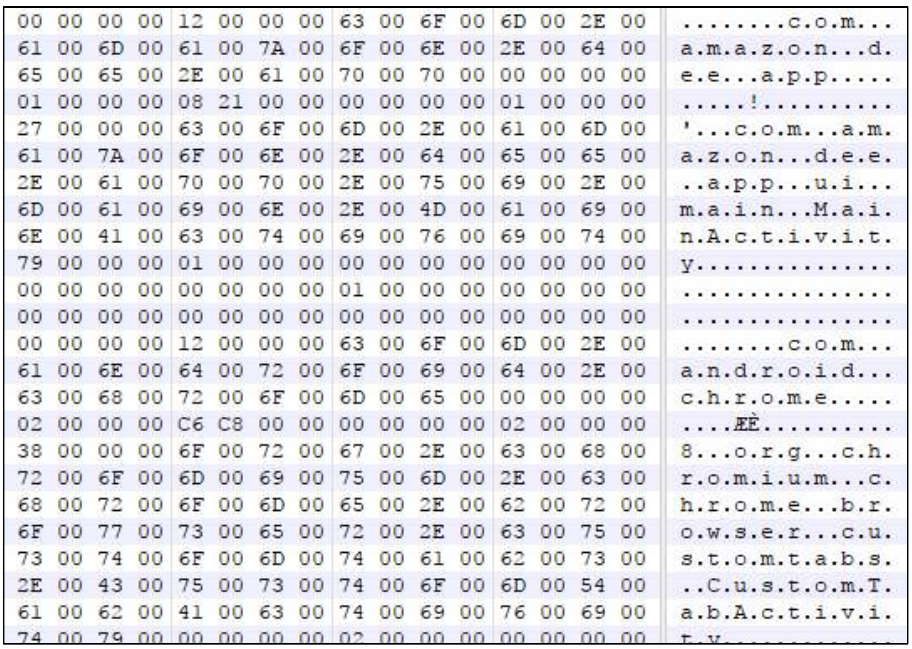


Fig. 3-4. Contents of 'usage-20170717'

Table 3-4. Contents of 'usage-20170717'

Package Name	Application Name
com.google.android.googlequicksearchbox	Google
com.android.mms	SMS
com.amazon.dee.app	Amazon Alexa
com.android.chrome	Google Chrome
com.google.android.gms	Google Play Service
com.sec.android.app.launcher	Samsung TouchWiz Home
com.android.settings	Settings
com.google.android.talk	Hangouts
com.kingoapp.superbattery	Kingo SuperBatery
com.xiaomi.hm.health	Mi Fit

1.2.4 Conversations History using Hangouts

'babel1.db' is a SQLite formatted database file created by the Android application 'Hangouts', which is a communication platform that includes instant messaging, video chat, SMS and VOIP features.

The 'participants' table shows accounts that participated in Hangouts conversations. According to the acquired file, 'Hallym Betty (registered account)' and 'John Macron (blocked account)' interacted with each other(Table 3-5). The 'chat_id' column is used in the 'messages' table (Table 3-6) to indicate who sent the message.

Table 3-5. Records of 'partitcipants' Table in 'babel1.db'

No.	chat_id	full_name	fallback_name	blocked
1	112549252980293459976	Hallym Betty	bettyhallym@gmail.com	0
2	108778762612058411235	John Macron	John Macron	1

message_id	message_type	conversation_id	author_chat_id	author_gaia_id	text	timestamp
Click here to define a filter						
8V673ca04908V674EEtl-G	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	108778762612058411235	108778762612058411235	;)	1500266348448375
8V673ca04908V67OUALXuX	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	108778762612058411235	108778762612058411235	How are you?	1500266514326967
8V673ca04908V67Z6ecnKP	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	112549252980293459976	112549252980293459976	Hey. Better now ;)	1500266601429983
8V673ca04908V68-Me56LZ	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	108778762612058411235	108778762612058411235	Ugh. Work sucks	1500266832854194
8V673ca04908V68-uwj_VV	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	108778762612058411235	108778762612058411235	I wanna see you later	1500266837370487
8V673ca04908V6GkxrjXoZ	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	112549252980293459976	112549252980293459976	I cant keep doing this	1500271425264235
8V673ca04908V6GoJY0lOf	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	108778762612058411235	108778762612058411235	It's too late now! U promised	1500271452743024
8V673ca04908V6Gp1FJEl1	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	112549252980293459976	112549252980293459976	Evwryone suspectbs	1500271458592671
8V673ca04908V6GrFpsMHr	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	112549252980293459976	112549252980293459976	It feels like they are warching us	1500271476843358
8V673ca04908V6GsIRtvFo	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	108778762612058411235	108778762612058411235	You're just paranoid....	1500271485370253
8V673ca04908V6GvGTG6aF	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	112549252980293459976	112549252980293459976	I cannot take it anymore	1500271509694748
8V673ca04908V6GwIoDOya	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	108778762612058411235	108778762612058411235	...	1500271522025805
8V673ca04908V6Gx8XP7Jq	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	112549252980293459976	112549252980293459976	Its over dont msg me	1500271525061223
8V673ca04908V6Gz03p5kv	(null)	UgzjuBCEJq0DKNmrqB84AaABAagBiLyIDA	108778762612058411235	108778762612058411235	Who the fuck do you think k you are!	1500271540361830

Fig. 3-5. 'message' Table in 'babel1.db'

Fig. 3-5 shows the conversation between Hallym Betty and John Macron which remains in the 'message' Table.

The meaningful columns are 'author_chat_id', 'text' and 'timestamp'. 'author_chat_id' indicates who sent the message and we can get the full name by comparing it with the 'chat_id' in the 'participants' table (Table 3-5). 'timestamp' reveals when the message ('text') was sent and it should be decoded in Unix time. Table 3-6 summarizes all of this information.

Table 3-6. Records of 'messages' Table in 'babel1.db'

No.	author_chat_id	full_name[6)]	timestamp (UTC+09:00)	text
1	108778762612058411235	John Macron	2017-07-17 13:39:08	;)
2	108778762612058411235	John Macron	2017-07-17 13:41:54	How are you?
3	112549252980293459976	Hallym Betty	2017-07-17 13:43:21	Hey. Better now ;)
4	108778762612058411235	John Macron	2017-07-17 13:47:12	Ugh. Work sucks
5	108778762612058411235	John Macron	2017-07-17 13:47:17	I wanna see you later
6	112549252980293459976	Hallym Betty	2017-07-17 15:03:45	I cant keep doing this
7	108778762612058411235	John Macron	2017-07-17 15:04:12	It's too late now! U promised
8	112549252980293459976	Hallym Betty	2017-07-17 15:04:18	Evwryone suspectbs
9	112549252980293459976	Hallym Betty	2017-07-17 15:04:36	It feels like they are warching us
10	108778762612058411235	John Macron	2017-07-17 15:04:45	You're just paranoid....
11	112549252980293459976	Hallym Betty	2017-07-17 15:05:09	I cannot take it anymore
12	108778762612058411235	John Macron	2017-07-17 15:05:22	...
13	112549252980293459976	Hallym Betty	2017-07-17 15:05:25	Its over dont msg me
14	108778762612058411235	John Macron	2017-07-17 15:05:40	Who the fuck do you think k you are!

1.2.5 Xiaomi Mi Band Logs

We checked the Mi Band logs after 15:00 2017-07-17, when Simon insisted that he came home with Betty (Fig. 3-6). At 15:12:07, the previous connection (GATT address – 42ccda00) had been terminated. A New GATT address 4313e070 was created at 15:12:13 and a synchronization process was started. GATT 4313e070 was closed at 16:21:43 after the apartment was searched. Significantly, the total step increased by 31 in 20 seconds (15:13:19~15:13:39) and there were no logs recorded between 15:13:39 and 16:16:59. Detailed analysis result are shown in Table 3-7.

```
2017-07-17 15:01:14.938  HMDeviceManager  destroyDevice:WEIGHT
2017-07-17 15:01:14.951  HMDeviceManager  destroyDevice:SHOES
2017-07-17 15:12:07.950  AbsGattCallback  onConnectionStateChange Gatt:42ccda00,device:88:0F:10:F6:C8:B7,status
2017-07-17 15:12:07.952  HMBaseBleDevice  onDeviceConnecting:88:0F:10:F6:C8:B7
2017-07-17 15:12:07.953  HMHeartRateController  stopManualMeasure
2017-07-17 15:12:07.973  AbsGattCallback  ******Gatt close:<42ccda00>******
2017-07-17 15:12:07.974  AbsGattCallback  ******Gatt clientIf=5******
2017-07-17 15:12:07.980  HeadViewManager  HMDeviceConnectionEvent = HMDeviceConnectionEvent{deviceType=MILI, m
2017-07-17 15:12:07.981  HMDeviceManager  getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:08.042  GattPeripheral  Delay 5 second before reconnect...
2017-07-17 15:12:13.045  AbsGattCallback  connect back...
2017-07-17 15:12:13.052  AbsGattCallback  ******Gatt create:<4313e070>******
2017-07-17 15:12:14.917  AbsGattCallback  onConnectionStateChange Gatt:4313e070,device:88:0F:10:F6:C8:B7,status
2017-07-17 15:12:14.918  AbsGattCallback  ******Gatt connected:<4313e070>******
2017-07-17 15:12:14.918  AbsGattCallback  ******Gatt clientIf=5******
2017-07-17 15:12:14.921  HMBaseBleDevice  onDeviceConnecting:88:0F:10:F6:C8:B7
2017-07-17 15:12:14.922  HMHeartRateController  stopManualMeasure
2017-07-17 15:12:14.926  GattPeripheral  discoverServices return true
2017-07-17 15:12:14.963  AbsGattCallback  onServicesDiscovered Gatt:4313e070,device:88:0F:10:F6:C8:B7,status:0
                                                    ⋮
2017-07-17 15:12:16.023  HMBaseBleDevice  onDeviceConnected:88:0F:10:F6:C8:B7
2017-07-17 15:12:16.024  HMDeviceManager  getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:16.028  HMDeviceManager  getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:16.035  HMDeviceManager  getDeviceInternal:MILI,isCreate:false
2017-07-17 15:12:16.052  HMDeviceManager  Bound device MILI sync time is : java.util.GregorianCalendar[time=1
2017-07-17 15:12:16.054  HMBaseTask  ====================g====================
2017-07-17 15:12:16.054  HMBaseTask  >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
2017-07-17 15:12:16.055  HMBaseTask  ============================start sync data============================
2017-07-17 15:12:16.056  HMBaseTask  >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
2017-07-17 15:12:16.060  HeadViewManager  HMDeviceConnectionEvent = HMDeviceConnectionEvent{deviceType=MILI,
                                                    ⋮
2017-07-17 15:13:19.516  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3211,totalDis:0,totalCal:0,running:
2017-07-17 15:13:19.650  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3212,totalDis:0,totalCal:0,running:
2017-07-17 15:13:20.149  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3213,totalDis:0,totalCal:0,running:
2017-07-17 15:13:20.475  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3214,totalDis:0,totalCal:0,running:
2017-07-17 15:13:21.108  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3215,totalDis:0,totalCal:0,running:
2017-07-17 15:13:21.352  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3216,totalDis:0,totalCal:0,running:
2017-07-17 15:13:21.839  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3217,totalDis:0,totalCal:0,running:
2017-07-17 15:13:22.181  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3218,totalDis:0,totalCal:0,running:
2017-07-17 15:13:29.445  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3228,totalDis:0,totalCal:0,running:
2017-07-17 15:13:30.030  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3229,totalDis:0,totalCal:0,running:
2017-07-17 15:13:30.420  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3230,totalDis:0,totalCal:0,running:
2017-07-17 15:13:30.858  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3231,totalDis:0,totalCal:0,running:
2017-07-17 15:13:31.395  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3232,totalDis:0,totalCal:0,running:
2017-07-17 15:13:31.834  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3233,totalDis:0,totalCal:0,running:
2017-07-17 15:13:32.175  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3234,totalDis:0,totalCal:0,running:
2017-07-17 15:13:32.711  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3235,totalDis:0,totalCal:0,running:
2017-07-17 15:13:33.540  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3236,totalDis:0,totalCal:0,running:
2017-07-17 15:13:35.003  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3237,totalDis:0,totalCal:0,running:
2017-07-17 15:13:35.685  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3238,totalDis:0,totalCal:0,running:
2017-07-17 15:13:36.319  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3239,totalDis:0,totalCal:0,running:
2017-07-17 15:13:37.586  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3240,totalDis:0,totalCal:0,running:
2017-07-17 15:13:38.610  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3241,totalDis:0,totalCal:0,running:
2017-07-17 15:13:39.585  MyRealtimeStepCallback  type:MILI,step:[,totalStep:3242,totalDis:0,totalCal:0,running:
2017-07-17 16:16:59.836  HMActivity  onActivityCreated:HMMiLiSettingActivity
2017-07-17 16:17:00.392  HMDeviceManager  getDeviceInternal:MILI,isCreate:false
2017-07-17 16:17:00.431  HMActivity  onActivityStarted:HMMiLiSettingActivity
                                                    ⋮
2017-07-17 16:20:16.825  MainTabActivity  ================onEnterInBackground================
2017-07-17 16:21:43.302  AbsGattCallback  onConnectionStateChange Gatt:4313e070,device:88:0F:10:F6:C8:B7,status
2017-07-17 16:21:43.305  HMBaseBleDevice  onDeviceConnecting:88:0F:10:F6:C8:B7
2017-07-17 16:21:43.307  AbsGattCallback  ******Gatt close:<4313e070>******
2017-07-17 16:21:43.308  AbsGattCallback  ******Gatt clientIf=5******
```

Fig. 3-6. Contents of 'Mili_log.txt'

6) This column is same as 'full_name' from Table 3-1.

Table 3-7 Analysis Result for Mi Band Log (2017-07-17)

Time	Log Data
15:01:14	destroyDevice
15:12:07	Gatt close : 42ccda00
15:12:13	Gatt create : 4313e070
15:12:14	Gatt connected : 4313e070
15:12:14	onDeviceConnecting : 88:0F:10:F6:C8:B7
15:12:14	onServiceDiscovered
15:12:16	onDeviceConnected : 88:0F:10:F6:C8:B7
15:12:16 ~ 15:12:17	sync data
15:12:17 ~ 15:12:18	getDeviceInternal
15:13:19 ~ 15:13:39	totalStep : 3211 → totalStep : 3242
15:13:39 ~ 16:16:59	-
16:21:43	Gatt close : 4313e070

1.3 Image of Simon's Samsung Note Ⅱ

1.3.1 Remote-connected Devices

'bt_config.xml' contains not only the local device's name and Bluetooth MAC address but also remote devices's that had previously connected to the local device.

Fig. 3-7. Contents of 'bt_config.xml(local device information)'

The “Remote” tag shows the names of all devices and the time they connected to the local device.

Fig. 3-8. bt_config.xml (remote device information)

Four devices were connected to Simon’s phone. Information about the devices is shown in Table 3-8. The time section indicates the time at which the device was first connected.

Table 3-8. Information about Devices Connected to Simon’s Phone

Bluetooth MAC address	Name	Time (UTC+9)	Information
1c:af:05:9e:19:74	Betty(SHV-E250L)	2017.07.13 16:38:53	Smartphone
74:c2:46:88:5d:09	Echo-2W5	2017.07.16 17:35:50	Smart speaker
88:0f:10:f6:c8:b7	MI1A	2017.07.16 17:35:53	Smart band
b8:ad:3e:01:5b:6a	LG HBS900	2017.07.16 17:24:16	Bluetooth earphone

1.3.2 Connected Wi-Fi Information

'wpa_supplicant.conf' contains a list of Wi-Fi APs (Access Point) to which the devicce has connected. If the Wi-Fi AP require a password, that the password information is included.

```
network={
    ssid="T wifi zone_secure"
    key_mgmt=WPA-EAP IEEE8021X
    eap=AKA
    pcsc=""
    priority=1
    autojoin=1
    vendor_spec_ssid=1
    usable_internet=0
    skip_internet_check=0
}

network={
    ssid="T wifi zone"
    key_mgmt=NONE
    autojoin=1
    vendor_spec_ssid=1
    usable_internet=0
    skip_internet_check=0
}

network={
    ssid="U+zone"
    key_mgmt=WPA-EAP IEEE8021X
    eap=PEAP
    identity="iot14305"
    priority=2
```

Fig 3-9. Part of 'wpa_supplicant.conf'

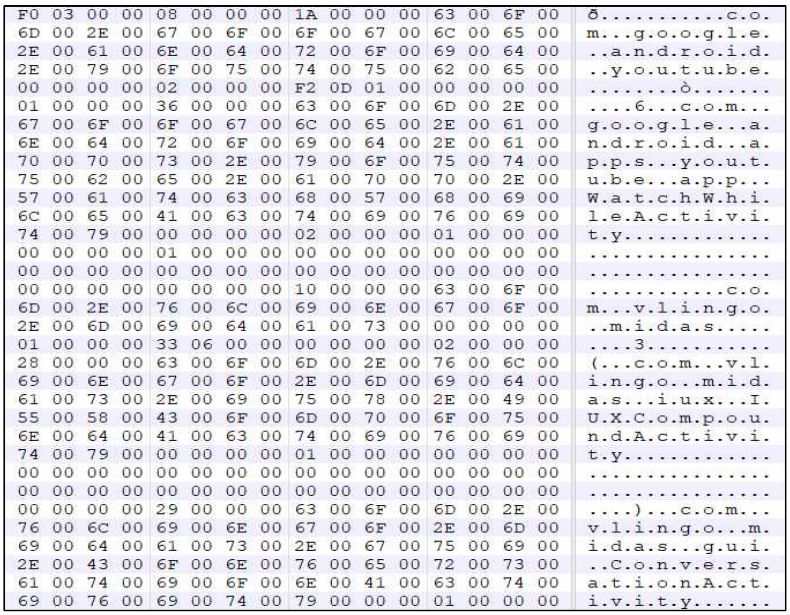
The file contains the SSIDs of nine APs that previously connected to Simon's phone. Simon mentioned the 'home' and 'HOME' networks, but did not mention the others.

Table 3-9. Contents of 'wpa_supplicant.conf' in Simon's Phone

SSID	PSK
T wifi zone_secure	-
T wifi zone	-
U+zone	iot14305
IoTLab_WAN	iot14305
IoTLab	iot14305
neo_house5	neoidm1011
home	iot14305
setupEBC2	bznnyjhxd
HOME	iot14305

1.3.3 List of Used Applications

Fig. 3-10 shows part of the usage-20170717 file. The usage-YYYYMMDD file contains package names and activities used on the corresponding day.



```
F0 03 00 00 08 00 00 00 1A 00 00 00 63 00 6F 00  ð...........c.o.
6D 00 2E 00 67 00 6F 00 6F 00 67 00 6C 00 65 00  m...g.o.o.g.l.e.
2E 00 61 00 6E 00 64 00 72 00 6F 00 69 00 64 00  ..a.n.d.r.o.i.d.
2E 00 79 00 6F 00 75 00 74 00 75 00 62 00 65 00  ..y.o.u.t.u.b.e.
00 00 00 00 02 00 00 00 F2 0D 01 00 00 00 00 00  ........ò.......
01 00 00 00 36 00 00 00 63 00 6F 00 6D 00 2E 00  ....6...c.o.m...
67 00 6F 00 6F 00 67 00 6C 00 65 00 2E 00 61 00  g.o.o.g.l.e...a.
6E 00 64 00 72 00 6F 00 69 00 64 00 2E 00 61 00  n.d.r.o.i.d...a.
70 00 70 00 73 00 2E 00 79 00 6F 00 75 00 74 00  p.p.s...y.o.u.t.
75 00 62 00 65 00 2E 00 61 00 70 00 70 00 2E 00  u.b.e...a.p.p...
57 00 61 00 74 00 63 00 68 00 57 00 68 00 69 00  W.a.t.c.h.W.h.i.
6C 00 65 00 41 00 63 00 74 00 69 00 76 00 69 00  l.e.A.c.t.i.v.i.
74 00 79 00 00 00 00 00 02 00 00 00 01 00 00 00  t.y.............
00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 10 00 00 00 63 00 6F 00  ............c.o.
6D 00 2E 00 76 00 6C 00 69 00 6E 00 67 00 6F 00  m...v.l.i.n.g.o.
2E 00 6D 00 69 00 64 00 61 00 73 00 00 00 00 00  ..m.i.d.a.s.....
01 00 00 00 33 06 00 00 00 00 00 00 02 00 00 00  ....3...........
28 00 00 00 63 00 6F 00 6D 00 2E 00 76 00 6C 00  (...c.o.m...v.l.
69 00 6E 00 67 00 6F 00 2E 00 6D 00 69 00 64 00  i.n.g.o...m.i.d.
61 00 73 00 2E 00 69 00 75 00 78 00 2E 00 49 00  a.s...i.u.x...I.
55 00 58 00 43 00 6F 00 6D 00 70 00 6F 00 75 00  U.X.C.o.m.p.o.u.
6E 00 64 00 41 00 63 00 74 00 69 00 76 00 69 00  n.d.A.c.t.i.v.i.
74 00 79 00 00 00 00 00 01 00 00 00 00 00 00 00  t.y.............
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 29 00 00 00 63 00 6F 00 6D 00 2E 00  ....)...c.o.m...
76 00 6C 00 69 00 6E 00 67 00 6F 00 2E 00 6D 00  v.l.i.n.g.o...m.
69 00 64 00 61 00 73 00 2E 00 67 00 75 00 69 00  i.d.a.s...g.u.i.
2E 00 43 00 6F 00 6E 00 76 00 65 00 72 00 73 00  ..C.o.n.v.e.r.s.
61 00 74 00 69 00 6F 00 6E 00 41 00 63 00 74 00  a.t.i.o.n.A.c.t.
69 00 76 00 69 00 74 00 79 00 00 00 01 00 00 00  i.v.i.t.y.......
```

Fig 3-10. Part of 'usage-20170717'

Eight applications were used on July 17, 2017. Four of the applications, which are marked in blue in Table 3-10 were third party application.

Table 3-10. Package Names and Activities in 'usage-20170717'

Package name	Activity
com.google.android.youtube	com.google.android.apps.youtube.app.WatchWhileActivity
com.vlingo.midas	com.vlingo.midas.iux.IUXCompoundActivity
	com.vlingo.midas.gui.ConversationActivity
com.smartthings.android	com.smartthings.android.main.MainActivity
	com.smartthings.android.main.activity.PrimaryActivity
org.xbmc.kore	org.xbmc.kore.ui.sections.remote.RemoteActivity
com.sec.android.app.launcher	com.android.launcher2.Launcher
com.tgrape.andoid.radar	com.tgrape.android.radar.activity.Loading
	com.tgrape.android.NationSelect
com.android.settings	com.android.settings.Settings$BluetoothSettingsActivity
	con.android.settings.Settings$WifiSettingsActivity
com.android.system.ui	com.android.system.ui.recent.RecentsActivity

The third party application were as follows.

-com.google.android.youtube

Video-sharing application.

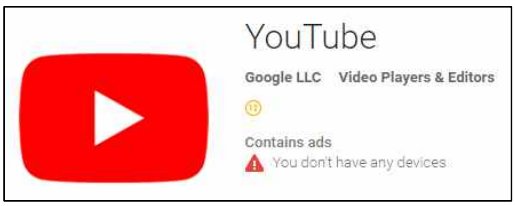


Fig. 3-11. com.google.android.youtube

-com.vlingo.midas

Control phone with voice.

Fig. 3-12. com.vlingo.midas

-com.smartthings.android

Monitoring, controling and securing many connected lights, locks, sensors and other devices in a smart home.

Fig. 3-13. com.smartthings.android

-org.xbmc.kore

Remote for the Kodi media player application.

Fig. 3-14. org.xbmc.kore

com.sec.android.app.launcher, com.tgrape.andoid.radar, com.android.settings, and com.android.system.ui are default packages in the Samsung Galaxy smartphone.

-com.sec.android.app.launcher

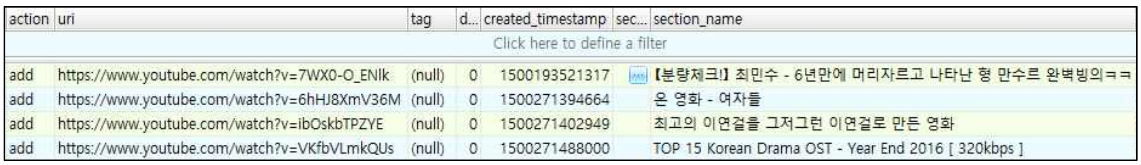
Samsung TouchWiz Home is a default application that provides Home and Apps screens for Samsung Galaxy smartphones.

-com.tgrape.andoid.radar

The S Suggest application helps users discover applications directly from a live widget on the home screen.

1.3.4 YouTube Logs

'icing-indexapi.db' is under com.google.android.gms and is a Google mobile service package. The file contains a list of URLs for YouTube as well as columns for, 'created_timestamp' and section_name. Section_name is the title of the YouTube video while the created_timestamp is the time the video was added to the play list.



action	uri	tag	d...	created_timestamp	sec...	section_name
	Click here to define a filter					
add	https://www.youtube.com/watch?v=7WX0-O_ENlk	(null)	0	1500193521317		【분량체크!】 최민수 - 6년만에 머리자르고 나타난 형 만수르 완벽빙의ㅋㅋ
add	https://www.youtube.com/watch?v=6hHJ8XmV36M	(null)	0	1500271394664		온 영화 - 여자들
add	https://www.youtube.com/watch?v=ibOskbTPZYE	(null)	0	1500271402949		최고의 이연걸을 그저그런 이연걸로 만든 영화
add	https://www.youtube.com/watch?v=VKfbVLmkQUs	(null)	0	1500271488000		TOP 15 Korean Drama OST - Year End 2016 [320kbps]

Fig. 3-15. YouTube Information in 'icing-indexapi.db'

Simon added three videos to his play list on July 17, 2017. In Table 3-11, the Time column shows the time that converted from UTC to Asia/Seoul time zone. It also contains the play time for each video.

Table 3-11. List of YouTube Video Added to Play List

URL	Title	Time (UTC+09:00)	Play Time
https://www.youtube.com/watch?v=7WX0-O_ENlk	【분량체크!】 최민수 - 6년만에 머리자르고 나타난 형 만수르 완벽빙의ㅋㅋ	2017.07.16 17:25:21	
https://www.youtube.com/watch?v=6hHJ8XmV36M	온 영화 - 여자들	2017.07.17 15:03:14	3:34
https://www.youtube.com/watch?v=ibOskbTPZYE	최고의 이연걸을 그저그런 이연걸로 만든 영화	2017.07.17 15:03:22	4:00
https://www.youtube.com/watch?v=VKfbVLmkQUs	TOP 15 Korean Drama OST - Year End 2016 [320kbps]	2017.07.17 15:04:48	56:10

1.4 Diagnostic Report from Google OnHub

This is a list of MAC addresses that had connected to the Google OnHub. Each MAC address and IP address can be used to obtain get information at DHCP[7] host name and MDNS[8] name.

Table 3-12. Information about Devices that were Connected to OnHub

MAC address	IP address	DHCP host name	MDNS name
2016d8000001	192.168.86.29	ademanafe	ademanafe.local
109266000002	192.168.86.28	android-**********	android-**********.local
d052a8000003	192.168.86.27	st-**********	st-**********.local
b827eb000004	192.168.86.25	osmc	osmc.local
50f520000005	192.168.86.26	android-**********	android-**********.local
1caf05000006	192.168.86.24	android-**********	android-**********.local
18b430000007	192.168.86.22	**********XDU	**********XDU.local
a002dc000008	192.168.86.21	-	dp-535302W5.local

/var/log/messages and /var/log/messages.1 are actual log messages from 16 to July 17, 2017. The logs show the connection status of the devices listed in Table 3-12 with timestamp (Table 3-13). Looking at the logs near the time of the incident, Simon and Betty's phones were connected at around 15:00. Additionally, an Android phone that cannot be identified in this scenario was connected at 15:11, and disconnected about four minutes later. Then Simon's phone was disconnected at 15:20.

Table 3-13. Log Messages on Google OnHub

Time(UTC +9)	MAC address	State
2017-07-16 17:14:43	50f520000027	Disconnected
2017-07-16 17:14:43	50f520000027	Connected
2017-07-16 17:18:49	b827eb000028	Connected
2017-07-16 17:57:44	a002dc000020	Disconnected
2017-07-16 19:59:12	50f520000027	Disconnected
2017-07-16 19:59:12	50f520000027	Connected
2017-07-16 20:11:46	a002dc000020	Connected

7) Network management protocol used on TCP/IP networks whereby a DHCP server dynamically assigns an IP address and other network configuration parameters to each device on a network so they can communicate with other IP networks.

8) Host names to IP addresses within small networks that do not include a local name server.

2017-07-17 13:41:26	109266000026	Connected
2017-07-17 13:44:48	109266000026	Disconnected
2017-07-17 14:13:37	a002dc000020	Disconnected
2017-07-17 14:16:13	a002dc000020	Connected
2017-07-17 14:18:44	b827eb000028	Disconnected
2017-07-17 14:21:48	50f520000027	Disconnected
2017-07-17 14:22:12	1caf05000022	Disconnected
2017-07-17 15:00:45	50f520000027	Connected
2017-07-17 15:00:46	1caf05000022	Connected
2017-07-17 15:02:05	b827eb000028	Connected
2017-07-17 15:11:55	109266000026	Connected
2017-07-17 15:15:21	109266000026	Disconnected
2017-07-17 15:20:50	50f520000027	Disconnected
2017-07-17 15:25:21	b827eb000028	Disconnected
2017-07-17 16:21:35	1caf05000022	Disconnected
2017-07-17 16:27:57	2016d800001f	Connected

1.5 Data from Amazon Echo / Alexa Cloud UI

According to Simon Hallym (Betty's husband), Betty was listening to music with the 'Pandora' application installed on Amazon Echo. Json files contains information (the user's requests with the Timestamp, Serial number, etc.) related to Betty's requests for Alexa. Obviously, the source of the JSON file is the voice of a person (or people) which is included in a wav file. The table below shows the content of each JSON file. The last column reveals the wav file name with the voice contents matching the 'summary'.

Table 3-14. Contents of each Json File (In chronological order)

	File Name (JSON)	Contents		File Name (wav)
		createdTimestamp (UTC+09:00)	summary	
1	14.json	2017-07-17 11:57:35	alexa kinda patton a.m. next monday	-
2	15.json	2017-07-17 12:07;00	-	-
3	16..json	2017-07-17 14:31:04	-	-
4	17.json	2017-07-17 14:45:29	alexa	-
5	13.json	2017-07-17 14:45:31	wake up	-
6	18.json	2017-07-17 14:45:43	alexa stop	-

7	12.json	2017-07-17 15:01:54	alexa	11.wav 12.wav
8	11.json	2017-07-17 15:01:55	turn on tv	11.wav 12.wav
9	10.json	2017-07-17 15:06:03	alexa	9.wav 10.wav
10	9.json	2017-07-17 15:06:06	turn on pandora	9.wav 10.wav
11	8.json	2017-07-17 15:12:39	alexa how could you do this what are the flooding	7.wav 8.wav
12	7.json	-	-	-
13	6.json	2017-07-17 15:12:58	alexa	5.wav 6.wav
14	5.json	2017-07-17 15:13:02	stop	5.wav 6.wav
15	4,json	2017-07-17 15:20:05	alexa	3.wav 4.wav
16	3.json	2017-07-17 15:20:07	turn off tv	3.wav 4.wav
17	2.json	2017-07-17 15:20:32	alexa	-
18	1.json	2017-07-17 15:20:34	who yes	-

The fact indicate that:

- o Someone turned on the Smart TV at 15:01 and turned it off at 15:20.
- o Someone turned on the Pandora application at 15:06 and turned it off at 15:13.
- o 1.wav and 2.wav contain the words 'Alexa, call the ambulance' but no corresponding JSON file was created.
- o The 'summary' column in 8.json deviates from the normal request form and the voices of two people are included in the corresponding wav file.

The voice data is also stored on Amazon's server (https://pitangui.amazon.com/) and the given PNG files show user data through Amazon's web interface (screen shots). The user data provided by Amazon and the content of each tab are as follows (Table 3-15):

Table 3-15. Contents of each Tab and Main Screen shot Images

1. Now Playing
- List of songs played with Echo - Which music application was used

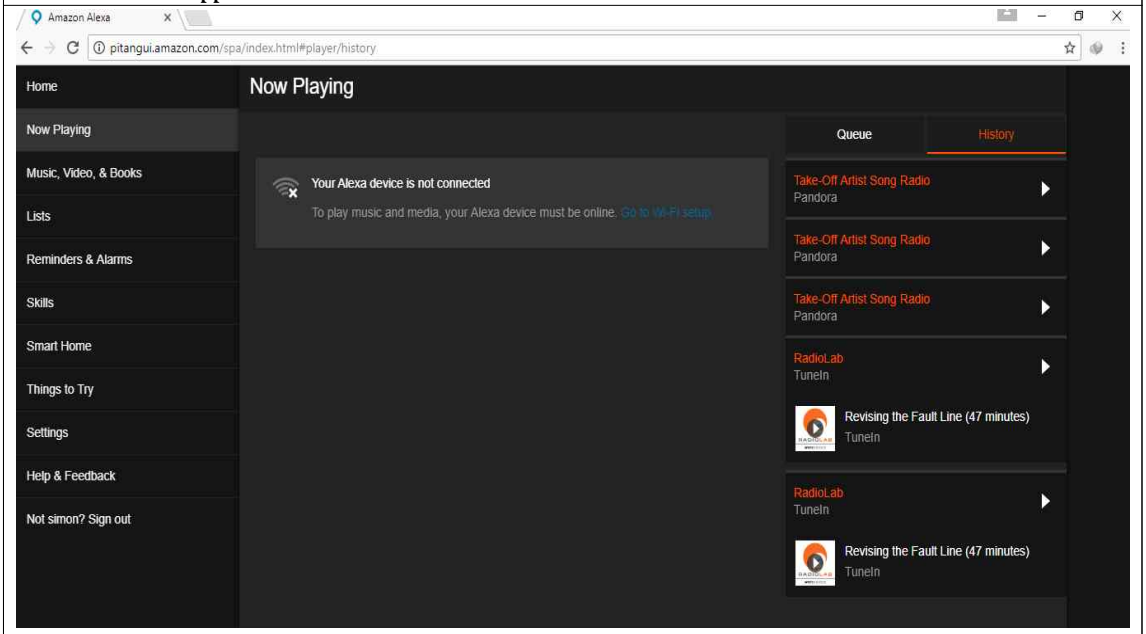


Fig. 3-16. 2017-07-17_17h02_09.png

2. Music, Video & Books
- List of built-in applications related to Music, Video and Books

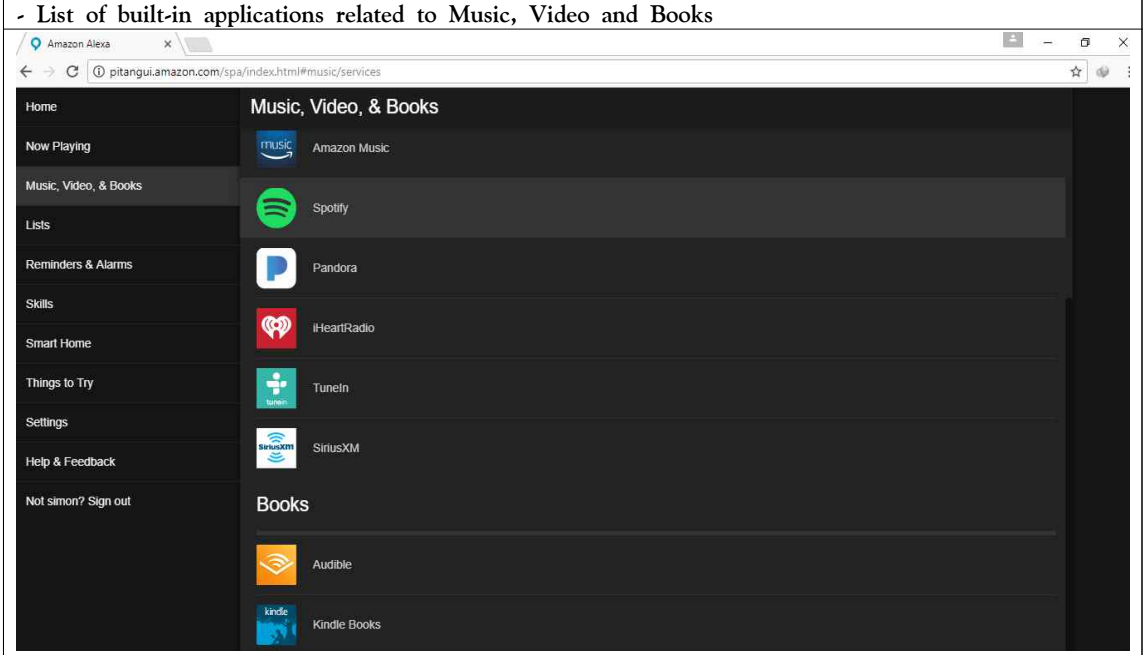


Fig. 3-17. 2017-07-17_17h03_29.png

3. Lists
- User-generated shopping/To-do List

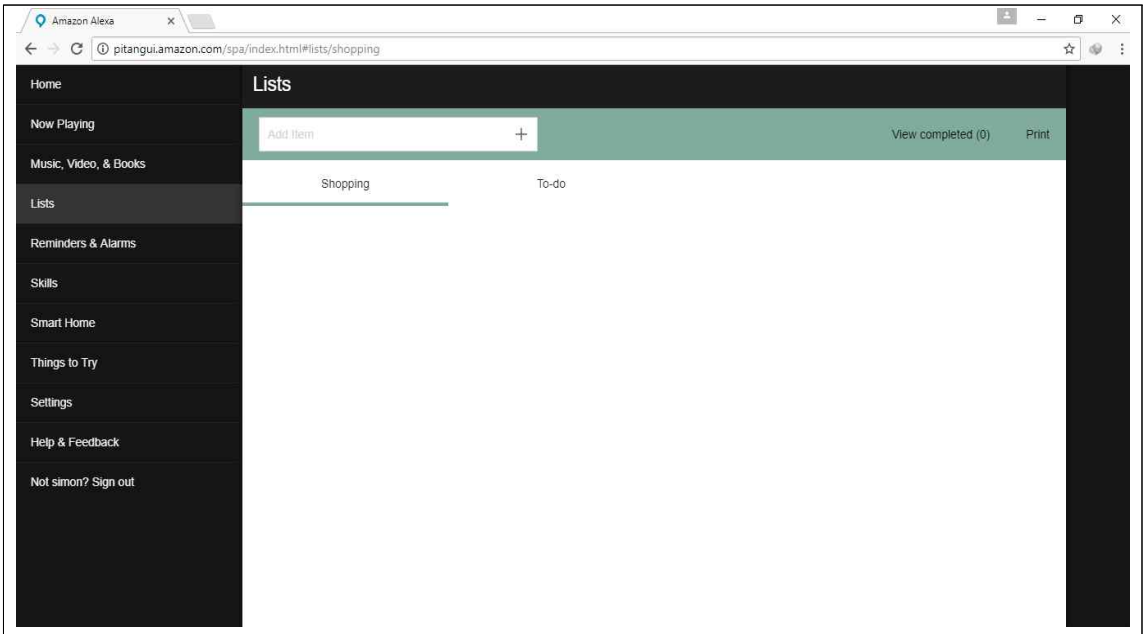


Fig. 3-18. 2017-07-17_17h04_15.png

4. Reminders & Alarms

- Reminders (schedules)
- Alarms
- Timers

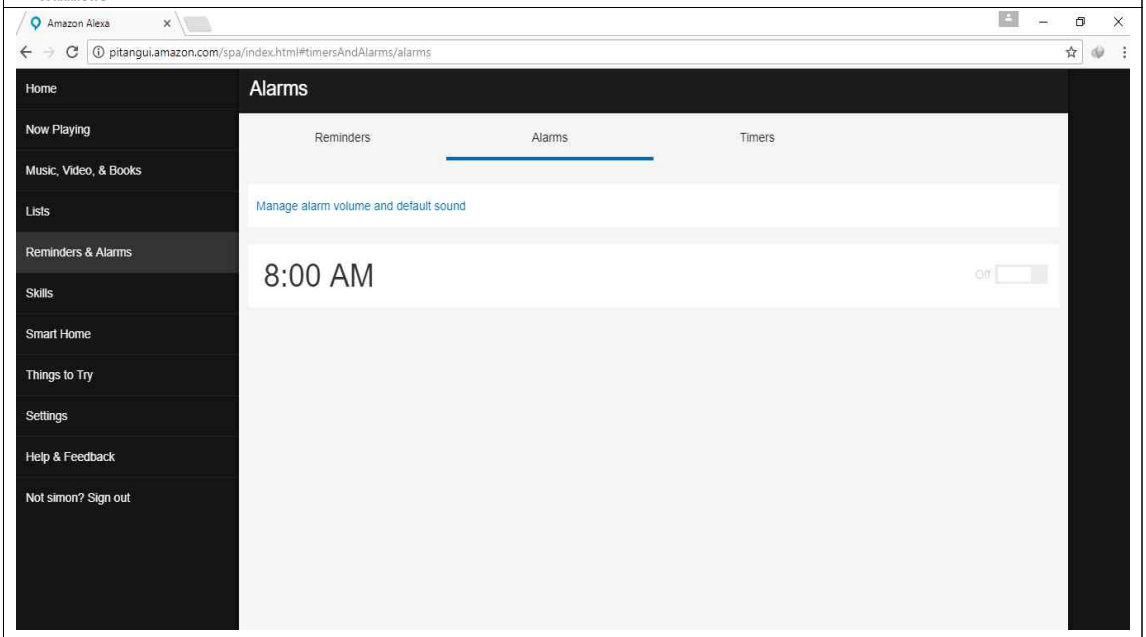


Fig. 3-19. 2017-07-17_17h04_43.png

5. Smart Home

- Connected Smart Devices
- Smart Home Skills

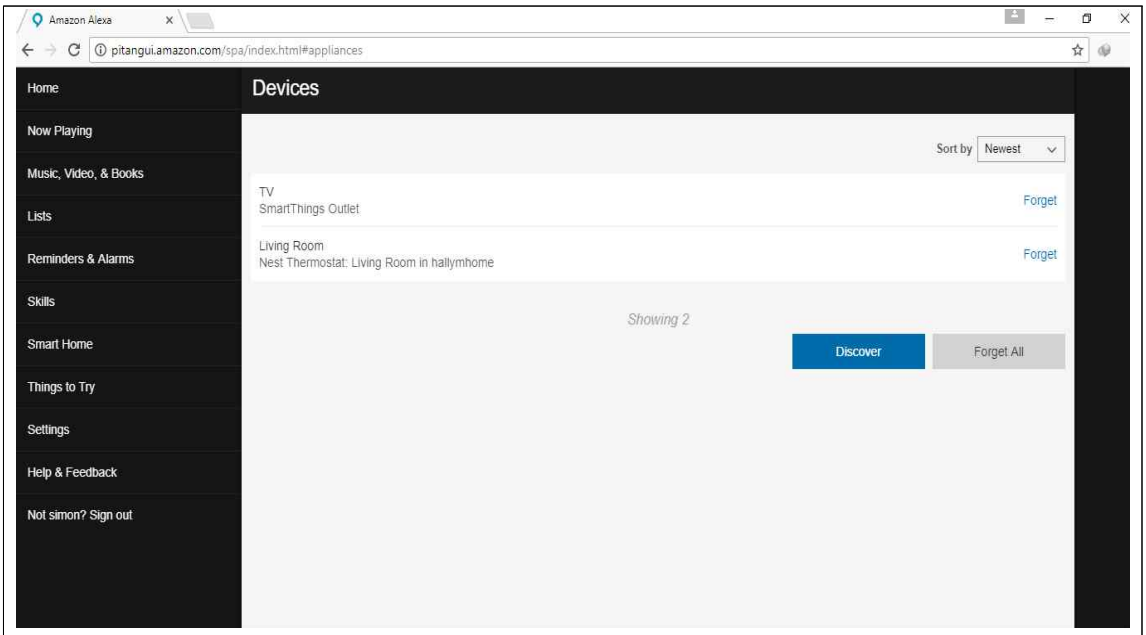


Fig. 3-20. 2017-07-17_17h06_10.png

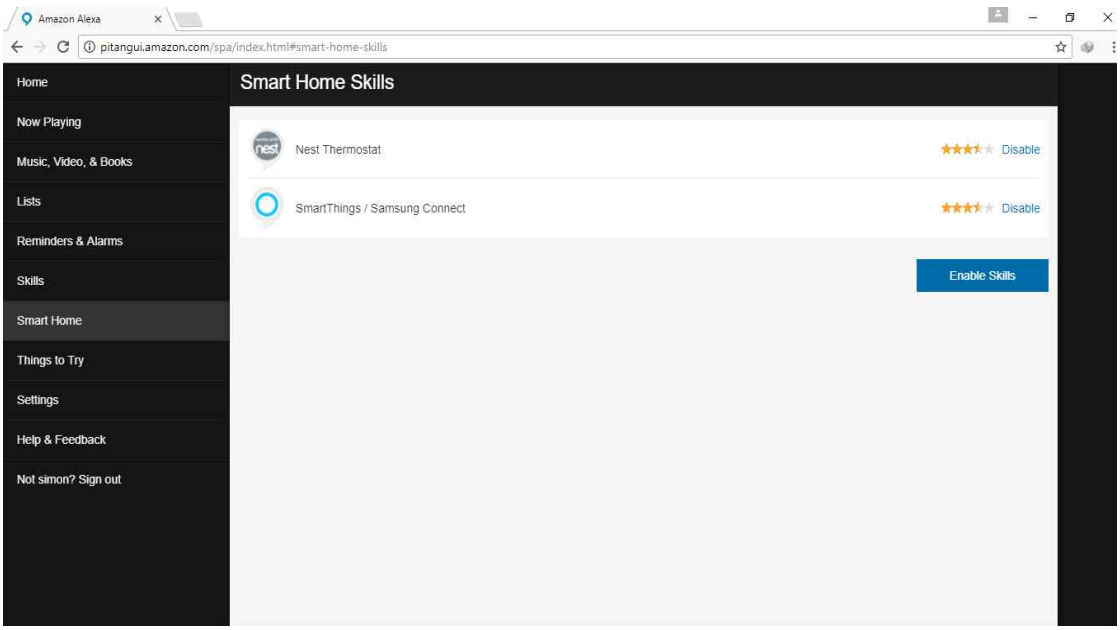


Fig. 3-21. 2017-07-17_17h07_00.png

6. Things to Try

- Commands List

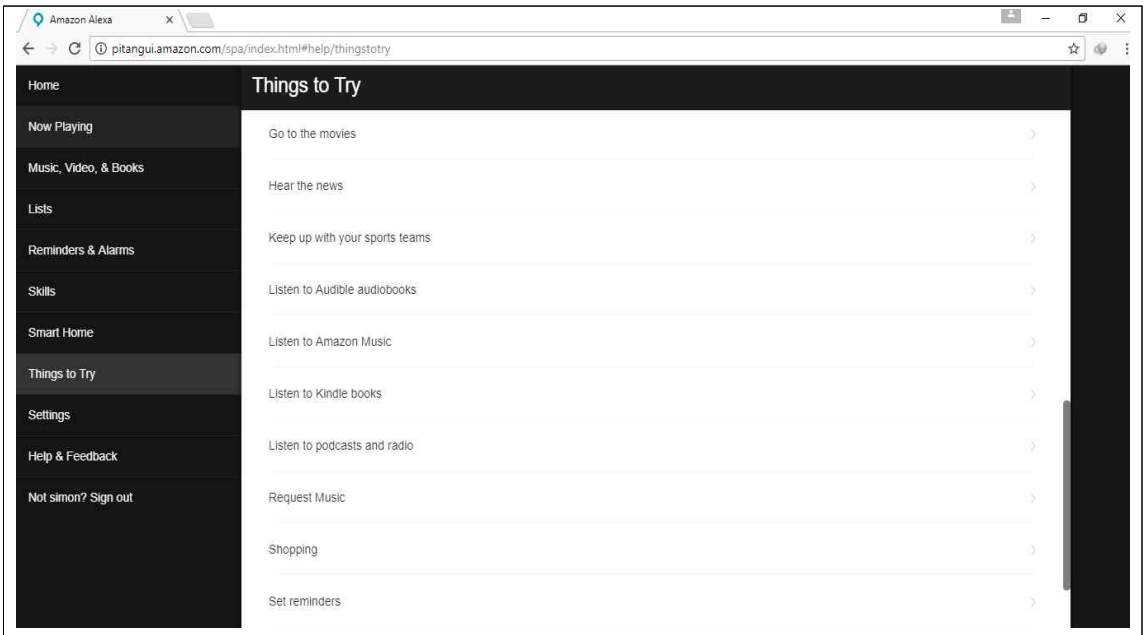


Fig. 3-22 2017-07-17_17h08_14.png

7. Settings

- List of connected smartphones
- Music services with connected accounts
- Conversation history

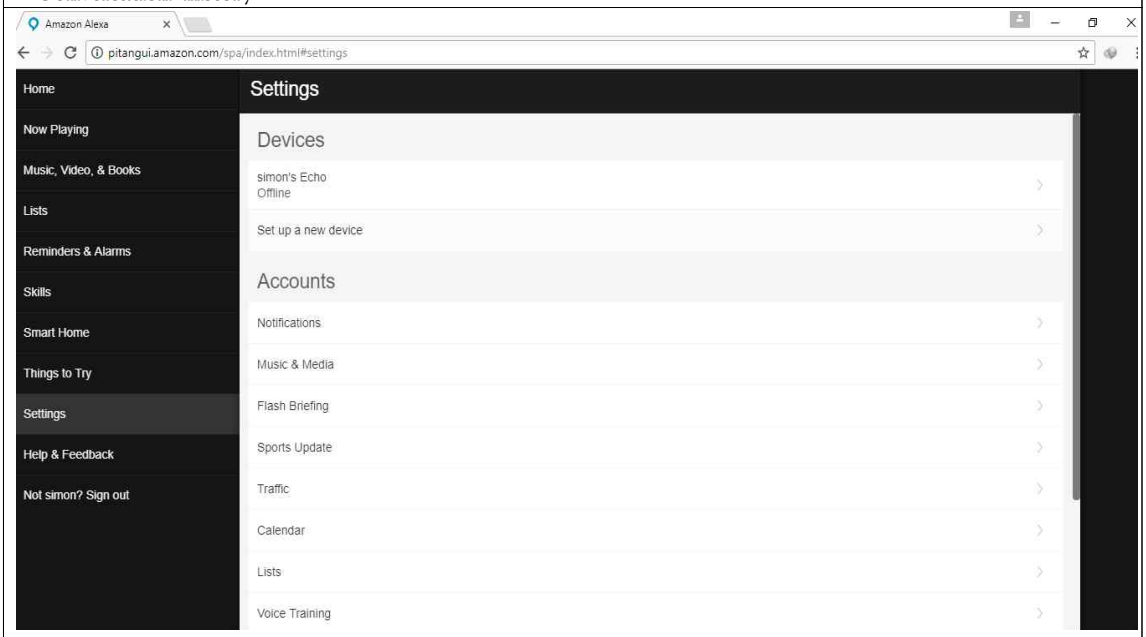


Fig. 3-23. 2017-07-17_17h08_49.png

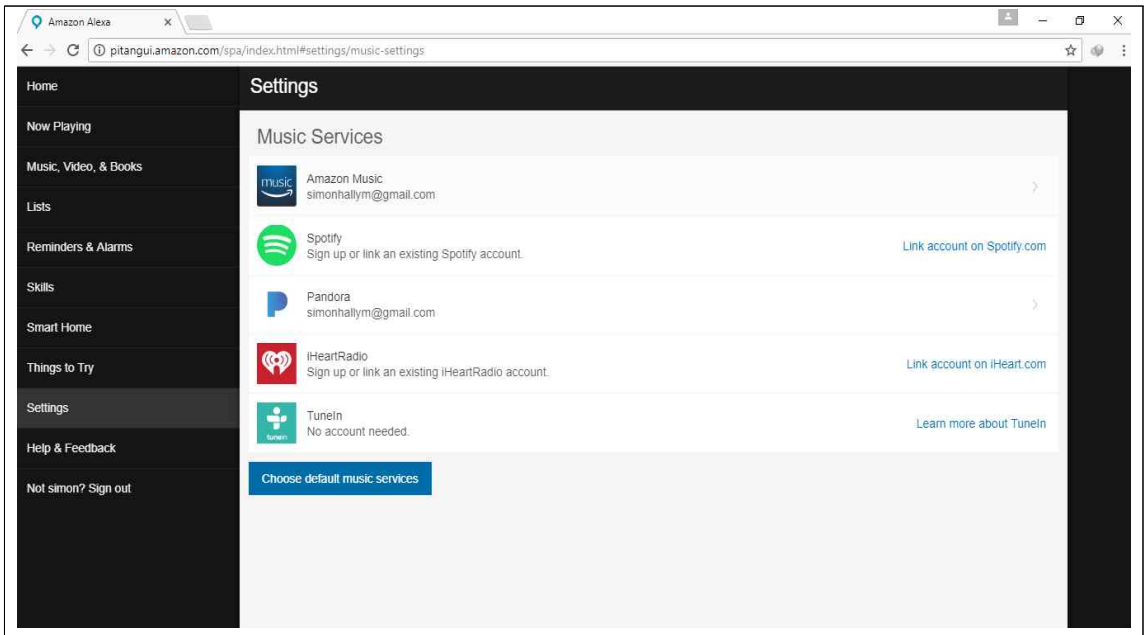


Fig. 3-24. 2017-07-17_17h10_06.png

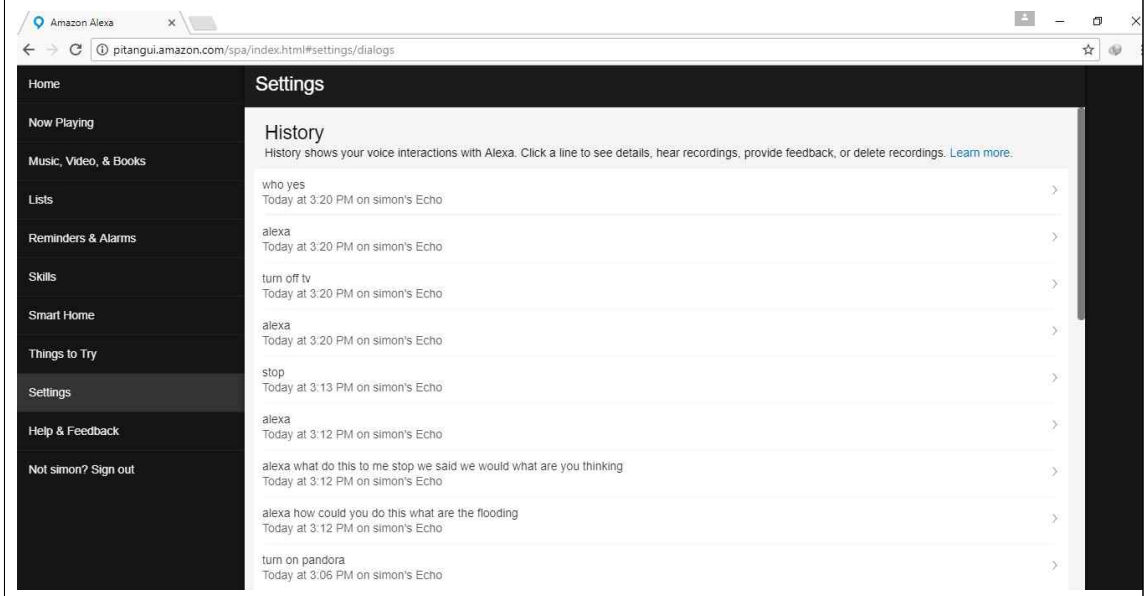


Fig. 3-25. 2017-07-17_17h13_03.png

From searching all the given screen shots, we find that significant data is stored under '5. Smart Home' and '7. Settings' in this case. First, as the Smart TV and Nest Thermostat were connected to the Amazon Echo, they could turn on/off the TV or control the temperature of the living room. Second, Simon's account (simonhallym@gmail.com) was linked with two music applications, one of which was Pandora, the application Betty used before she died. Finally, the conversation history and texts stored on the Echo after 15:00 were corresponded to the WAV/JSON files we mentioned above.

1.6 SmartHome Network Traffic Logs

The NetworkDump file contains records for 1-hour interval from 06:00 PM to 07:58 PM, July 17, 2017. The total number of packets is 105,328, and there are 1,727 sessions. Fig. 3-26 contains the ARP (Address Resolution Protocol) table from Google OnHub, showing 13 IP addresses and the corresponding MAC addresses.

```
/proc/net/arp
192.168.86.28    0x1         0x0         109266000026     *        br-lan
192.168.86.20    0x1         0x0         50f520000027     *        br-lan
192.168.86.25    0x1         0x2         b827eb000028     *        br-lan
192.168.86.26    0x1         0x0         50f520000027     *        br-lan
192.168.1.167    0x1         0x2         2016d800001f     *        br-guest
192.168.86.24    0x1         0x0         1caf05000022     *        br-lan
192.168.86.29    0x1         0x2         2016d800001f     *        br-lan
169.254.3.229    0x1         0x2         2016d800001f     *        br-guest
192.168.86.21    0x1         0x2         a002dc000020     *        br-lan
192.168.86.22    0x1         0x2         18b430000021     *        br-lan
192.168.165.1    0x1         0x2         909f33000025     *        wan0
192.168.87.20    0x1         0x0         2016d800001f     *        br-guest
192.168.86.27    0x1         0x2         d052a8000023     *        br-lan
```

Fig. 3-26. List of IP Addresses in Google OnHub

We attempt to confirm that the IP addresses in OnHub matches the ones in the NetworkDump file. We use the 'ip.addr == xxx.xxx.xxx.xxx' filtering command in WireShark, but nothing matches.

Next, we search for the source names that begin with 'Samsung', since there was a SmartThings[9] Mobile application in Simon's phone. The following table (Table 3-16) shows a list of MAC addresses in the Smart Home network traffic logs. We confirm that these addresses are consistent with those on Simon and Betty's cell phones, but nothing matched up with them.

Table 3-16 List of MAC address Samsung IoT devices in NetworkDump

Source	MAC address
SamsungE_ce:33:c8	00:13:77:ce:33:c8
SamsungE_cc:4c:a0	00:13:77:cc:4c:a0
SamsungE_cb:f8:ca	00:13:77:cb:f8:ca
SamsungE_cb:f8:b7	00:13:77:cb:f8:b7
SamsungE_cb:f8:17	00:13:77:cb:f8:17
SamsungE_c7:86:dd	00:13:77:c7:86:dd
SamsungE_c7:7c:77	00:13:77:c7:7c:77
SamsungE_c0:d4:3f	00:13:77:c0:d4:3f

9) Samsung-owned technology company.

SamsungE_a2:28:8e	50:b7:c3:a2:28:8e
SamsungE_8b:9a:f6	00:13:77:8b:9a:f6
SamsungE_8b:91:1f	00:13:77:8b:91:1f
SamsungE_8a:dd:e8	00:13:77:8a:dd:e8
SamsungE_8a:dd:2b	00:13:77:8a:dd:2b
SamsungE_8a:d9:df	00:13:77:8a:d9:df
SamsungE_8a:a1:9e	00:13:77:8a:a1:9e
SamsungE_8a:7d:fc	00:13:77:8a:7d:fc
SamsungE_7d:38:1d	98:83:89:7d:38:1d
SamsungE_73:67:a2	e8:11:32:73:67:a2
SamsungE_6d:e0:8e	e8:03:9a:6d:e0:8e
SamsungE_69:56:85	e8:03:9a:69:56:85
SamsungE_68:37:e6	e8:03:9a:68:37:e6
SamsungE_62:f3:d6	e8:03:9a:62:f3:d6
SamsungE_62:f3:d2	e8:03:9a:62:f3:d2
SamsungE_62:f3:69	e8:03:9a:62:f3:69
SamsungE_46:90:c2	00:13:77:46:90:c2
SamsungE_46:8c:c0	00:13:77:46:8c:c0
SamsungE_46:8a:74	00:13:77:46:8a:74
SamsungE_3b:b2:9a	98:83:89:3b:b2:9a
SamsungE_3a:34:e3	98:83:89:3a:34:e3
SamsungE_36:18:65	00:24:54:36:18:65
SamsungE_34:06:d6	e8:11:32:34:06:d6
SamsungE_32:41:8a	00:24:54:32:41:8a
SamsungE_32:41:86	00:24:54:32:41:86
SamsungE_32:40:98	00:24:54:32:40:98
SamsungE_30:84:79	00:24:54:30:84:79
SamsungE_27:8c:90	e8:03:9a:27:8c:90

In summary, we cannot find matching MAC/IP addresses that can be sensors in the OnHub-NetworkDump and Mobile-NetworkDump files. Since some of the clues expected based on the available evidence are unavailable, it is difficult to find any association with other data.

2. Correlations between Various Data Sources

2.1 YouTube Watch History in Samsung Galaxy Note Ⅱ and Raspberry Pi

Fig. 3-26 and Fig. 3-27 show the YouTube watch history extracted from Simon's Note Ⅱ and the Raspberry Pi.

seqno	action	uri	tag	d...	created_timestamp	sec...	section_name
		Click here to define a filter					
2	add	https://www.youtube.com/watch?v=7WX0-O_ENlk	(null)	0	1500193521317		【분량제크】 최민수 - 6년만에 머리자르고 나타난 형 만수르 완벽빙의ㅋㅋ
3	add	https://www.youtube.com/watch?v=6hHJ8XmV36M	(null)	0	1500271394664		온 영화 - 여자들
4	add	https://www.youtube.com/watch?v=ibOskbTPZYE	(null)	0	1500271402949		최고의 이연걸을 그저그런 이연걸로 만든 영화
5	add	https://www.youtube.com/watch?v=VKfbVLmkQUs	(null)	0	1500271488000		TOP 15 Korean Drama OST - Year End 2016 [320kbps]

Fig. 3-27. YouTube Information in 'icing-indexapi.db' of Simon's Phone

RecNo	idFile	idPath	strFilename	playCount	lastPlayed	dateAdded
			Click here to define a filter			
1	1	1	plugin://plugin.video.youtube/play/?video_id=pF_rqav38Z4	1	2017-07-13 08:43:46	(null)
2	2	1	plugin://plugin.video.youtube/play/?video_id=7WX0-O_ENlk	1	2017-07-16 04:54:54	(null)
3	3	1	plugin://plugin.video.youtube/play/?video_id=ibOskbTPZYE	1	2017-07-17 02:07:30	(null)
4	4	1	plugin://plugin.video.youtube/play/?video_id=VKfbVLmkQUs	(null)	2017-07-17 02:19:37	(null)

Fig. 3-28. YouTube Information in 'MyVideos107.db' of Raspberry Pi

The following table compares the two database records above the July 17, 2017. There are three video URLs in Simon's phone but only two in the Raspberry Pi since only the videos played by the user are recorded on the Raspberry Pi. In other words, the time recorded on the phone is the time the video was added to the play list and the time on Raspberry Pi is the video finish time. As you can see, the time difference for the second video between Simon's phone and the Raspberry Pi is the same as the 'Play Time' (4 min.). However, this is not the case for the third video, indicating that it was stopped during playback.

Table 3-17. Comparision of YouTube Watch History

No.	URL	Title	Play Time	Time (UTC+09:00)	
				Simon's Phone	Raspberry Pi
1	https://www.youtube.com/watch?v=6hHJ8XmV36M	온 영화 - 여자들	3:34	2017.07.17. 15:03:14	Not recorded
2	https://www.youtube.com/watch?v=ibOskbTPZYE	최고의 이연걸을 그저그런 이연걸로 만든 영화	4:00	2017.07.17. 15:03:22	2017-07-17 15:07:30
3	https://www.youtube.com/watch?v=VKfbVLmkQUs	TOP 15 Korean Drama OST - Year End 2016 [320kbps]	56:10	2017.07.17. 15:04:48	2017-07-17 15:19:37

2.2 MAC Addresses in Samsung Galaxy Note Ⅱ and OnHub

The significant data that can be obtained from the OnHub diagnostic report is the general information and connection status of the devices. Table 3-18 presents the list of MAC addresses extracted from the Google OnHub diagnostic report.

Table 3-18. Information about MAC addresses in OnHub

MAC address	DHCP host name	MDNS name
2016d8000001	ademanafe	ademanafe.local
109266000002	android-**********	android-**********.local
d052a8000003	st-**********	st-**********.local
b827eb000004	osmc	osmc.local
50f520000005	android-**********	android-**********.local
1caf05000006	android-**********	android-**********.local
18b430000007	**********XDU	**********XDU.local
a002dc000008	-	dp-535302W5.local

Additionally, combining the above table with the log messages results in the equivalent of Table 3-19. We can check whether the device is connected or disconnected and the time of occurrence. However, there is a limitation when analyzing OnHub data alone. Since the DHCP/MDNS names simply indicate the device type corresponding to the MAC address, we can not confirm who used the devices, especially for smartphone (Android in this case).

Table 3-19. Part of Log Messages on Google OnHub

Time(UTC +9)	MAC address	Device	State
2017-07-17 14:13:37	a002dc000020	dp-535302W5	Disconnected
2017-07-17 14:16:13	a002dc000020	dp-535302W5	Connected
2017-07-17 14:18:44	b827eb000028	osmc	Disconnected
2017-07-17 14:21:48	50f520000027	android-**********	Disconnected
2017-07-17 14:22:12	1caf05000022	android-**********	Disconnected
2017-07-17 15:00:45	50f520000027	android-**********	Connected
2017-07-17 15:00:46	1caf05000022	android-**********	Connected
2017-07-17 15:02:05	b827eb000028	osmc	Connected

This problem can be solved by associating the report with smart devices. Simon and Betty's phones both contain information for three MAC addresses (Table 3-20).

Table 3-20. Information about MAC addresses in Betty and Simon's phones

Name	MAC address
Betty	1C:AF:05:9E:19:74
Simon	50:F5:20:A5:7D:CD
Kore App	B8:27:Eb:19:72:86

Now we can determine the owner of each devices (mobile and PC) and where the MAC addresses came from (Application). It is also possible to clearly distinguish between important and non-essential data from OnHub. The analysis results after combining information from the smartphone and OnHub are in Table 3-20.

Table 3-21. Result After Combining Information

Time(UTC +9)	MAC address	Device	State
2017-07-17 14:13:37	a002dc000020	dp-535302W5	Disconnected
2017-07-17 14:16:13	a002dc000020	dp-535302W5	Connected
2017-07-17 14:18:44	b827eb000028	Kore App	Disconnected
2017-07-17 14:21:48	50f520000027	Simon's smartphone	Disconnected
2017-07-17 14:22:12	1caf05000022	Betty's smartphone	Disconnected
2017-07-17 15:00:45	50f520000027	Simon's smartphone	Connected
2017-07-17 15:00:46	1caf05000022	Betty's smartphone	Connected
2017-07-17 15:02:05	b827eb000028	Kore App	Connected

3. Timeline

This chapter chronologically summarizes the evidences we extracted earlier. Through the summarization process, we analyze the evidence based on the time Betty died. In Table 3-22, each entry is numbered and divided into time, evidence, and remarks.

Table 3-22. List of Evidences sorted in Chronological Order

*Evidence number
0 : Interrogation
1 : Raspberry Pi
2 : Betty's smartphone
3 : Simon's smartphone
4 : Onhub diagnostic
5 : Amazon Echo
6 : Smarthome tcpdump

No.	Time (UTC+9)	Contents	Evidence number	Remarks
1	2017-07-13 21:43:46	Play YouTube on TV	1	playtime: 335 sec
2	2017-07-16 17:14:43	50f520000027 Disconnected	4	Simon's smartphone disconnected
3	2017-07-16 17:14:43	50f520000027 Connected	4	Simon's smartphone connected
4	2017-07-16 17:18:49	b827eb000028 Connected	4	Raspberry pi connected
5	2017-07-16 17:25:21	YouTube playlist append	3	denied in Korea
6	2017-07-16 17:54:54	Play YouTube on TV	1	denied in Korea
7	2017-07-16 18:44:55	added bluetooth device	1	Name=MI1A
8	2017-07-16 18:50:14	added bluetooth device	1	Name=Echo-2WS
9	2017-07-16 18:57:44	a002dc000020 Disconnected	4	
10	2017-07-16 19:59:12	50f520000027 Disconnected	4	Simon's smartphone disconnected
11	2017-07-16 18:59:12	50f520000027 Connected	4	Simon's smartphone connected
12	2017-07-16 20:11:46	a002dc000020 Connected	4	

13	2017-07-17 11:57:00	-	5	14.wav. Not important
14	2017-07-17 12:07:00	-	5	13.wav. Not important
15	2017-07-17 13:39:08	;)	2	John Macron
16	2017-07-17 13:41:26	109266000026 Connected	4	unknown Android device connected
17	2017-07-17 13:41:54	How are you?	2	John Macron
18	2017-07-17 13:43:21	Hey. Better now ;)	2	Hallym Betty
19	2017-07-17 13:44:48	109266000026 Disconnected	4	unknown Android device disconnected
20	2017-07-17 13:47:12	Ugh. Work sucks	2	John Macron
21	2017-07-17 13:47:17	I wanna see you later	2	John Macron
22	2017-07-17 14:13:37	a002dc000020 Disconnected	4	
23	2017-07-17 14:16:13	a002dc000020 Connected	4	
24	2017-07-17 14:18:44	b827eb000028 Disconnected	4	Raspberry pi disconnected
25	2017-07-17 14:21:48	50f520000027 Disconnected	4	Simon's smartphone disconnected
26	2017-07-17 14:22:12	1caf05000022 Disconnected	4	Betty's smartphone disconnected
27	2017-07-17 15:00:45	50f520000027 Connected	4	Simon's smartphone connected
28	2017-07-17 15:00:46	1caf05000022 Connected	4	Betty's smartphone connected
29	2017-07-17 15:01:00	Alexa turn on TV (Simon)	5	11.wav, 12.wav
30	2017-07-17 15:02:05	b827eb000028 Connected	4	Raspberry pi connected
31	2017-07-17 15:03:14	YouTube playlist append	3	playtime: 214 sec
32	2017-07-17 15:03:22	YouTube playlist append	3	playtime: 240 sec

33	2017-07-17 15:03:45	I cant keep doing this	2	Hallym Betty
34	2017-07-17 15:04:12	It's too late now! U promised	2	John Macron
35	2017-07-17 15:04:18	Evwryone suspectbs	2	Hallym Betty
36	2017-07-17 15:04:36	It feels like they are warching us	2	Hallym Betty
37	2017-07-17 15:04:45	You're just paranoid....	2	John Macron
38	2017-07-17 15:04:48	YouTube playlist append	3	playtime: 3370 sec
39	2017-07-17 15:05:09	I cannot take it anymore	2	Hallym Betty
40	2017-07-17 15:05:22	...	2	John Macron
41	2017-07-17 15:05:25	Its over dont msg me	2	Hallym Betty
42	2017-07-17 15:05:40	Who the fuck do you think k you are!	2	John Macron
43	2017-07-17 15:06:00	Alexa turn on pandora? (Betty)	5	9.wav, 10.wav
44	2017-07-17 15:07:30	Play YouTube on TV	1	playtime: 240 sec
45	2017-07-17 15:11:55	109266000026 Connected	4	unknown Android device connected
46	2017-07-17 15:12:00	Alex stop(Betty) How could you do this what are the thinking (unknown man)	5	8.wav
47	2017-07-17 15:12:16	Miband Connect	2	
48	2017-07-17 15:12:20	Alexa Stop(Betty) what do this to me we said we would what are you thinking (unknown man)	5	7.wav
49	2017-07-17 15:12:59	Alexa. ... Stop (Betty)	5	5.wav, 6.wav
50	2017-07-17 15:15:21	109266000026 Disconnected	4	unknown Android device disconnected
51	2017-07-17 15:19:37	Play YouTube on TV	1	playtime: 3370 sec
52	2017-07-17 15:20:00	Alexa. Turn off TV (Simon)	5	3.wav, 4.wav

53	2017-07-17 15:20:50	50f520000027 Disconnected	4	Simon's smartphone disconnected
54	2017-07-17 15:21:55	Alexa! Call the ambulance	5	1.wav, 2.wav
55	2017-07-17 15:25:21	b827eb000028 Disconnected	4	Raspberry Pi disconnected
56	2017-07-17 15:31:00	Chuncheon Emergency Services received a phone call	0	
57	2017-07-17 15:40:00	Police arrived	0	
58	2017-07-17 15:50:00	Interrogation start	0	
59	2017-07-17 16:21:35	1caf05000022 Disconnected	4	Betty's smartphone disconnected
60	2017-07-17 16:27:57	2016d800001f Connected	4	

IV. Who is the Criminal?

1. Possible Scenarios

In this section, we attempt to guess murderer who killed Betty through the above analysis. Characters in this scenario are as follows.

Table 4-1. Characters in the Scenario

Name	Basic Information
Simon Hallym	Betty's husband. The first eyewitness to the scene of death.
Betty Hallym	Victim of the case.
John Macron	Betty's acquaintance. Traces of fighting with Betty are found.
Kim Kil Whan	Guard in the apartment. Called the emergency center.

1.1 Simon Hallym is the Criminal

Simon is the first witness to the case, but it is difficult to avoid characterizing him as a suspect because he was at the location where Betty was murdered. There are some differences between his testimony in the interviews and the actual evidence analysis, which increases the likelihood that Simon is the murderer. Simon's false testimony is as follows (Table 4-2).

Table 4-2. Simon's False Testimony

Investigator	Simon	Judgment
Could you please describe what happened?	I was watching a movie. After finishing the movie, I came into the living room and found her on the ground.	Simon began to watch the 3370-second video at 2017-07-17 15:07:30, but ended in 2017-07-17 15:19:37.
Do you know someone who would want to hurt your wife?	No. No one.	The argument between Betty and John Macron remains a record in the Hangout application.
Did she have friends or acquaintances in the area?	I don't think so. We just moved here.	Betty had an acquaintance.
Can you remember what you were watching?	It was a drama from YouTube.	The video was drama OST, not drama.

What are the passwords to your WIFI?	Home is iot14306, but the guest network is iot14305	The passwords for all networks are iot14305.

Simon also added a play list for the last YouTube videos he watched on 2017-07-17 15:04:48. This means Simon's alibi cannot be confirmed after this time.

1.2 John Macron is the Criminal

John Macron is a man with some malice toward Betty. After an argument on Hangouts, Betty blocked his account . Then he came to the Hallym house and murdered her. On this basis, there is a record of an unknown android device on OnHub that is believed to be John Macron's. The time when the device disconnected from the home network also corresponds to the estimated time of Betty's death. Crucially, the Amazon Echo recorded the voice of someone other than Simon.

No.	Time (UTC+9)	Contents	Remarks
42	2017-07-17 15:05:40	Who the fuck do you think k you are!	John Macron
45	2017-07-17 15:11:55	109266000026 Connected	unknown android device connected
49	2017-07-17 15:12:59	Alexa. ... Stop (Betty)	5.wav, 6.wav
50	2017-07-17 15:15:21	109266000026 Disconnected	unknown android device disconnected

If Simon's testimony is honestly based on all he knew, John Macron would be the criminal in this scenario.

2. Our Conclusion

We evaluated the probability that husband (Simon Hallym) killed his wife (Betty Hallym) versus some other unknown person (Table 4-3). There is a possibility that Simon and John Macron are accomplices. Simon tried to secure his alibi with television, and tried to hide John Macron's existence by saying no one would harm his wife. Simon is the first suspect in Betty's murder. Thus, it can be assumed that Simon provided John Macron with an environment for murder rather than directly murdering his wife. There is also the possibility that someone else committed the crime since physical evidence may remain on the scene.

Simon made the mistake of confusing the drama OST as a drama because he did not watch the video properly. It can be interpreted that Simon was not watching the video at the time. Therefore, it is very likely that Simon witnessed the scene of the murder, and it is very likely that the unknown android device with the access record at the time of interest belongs to John Macron. The reason we concluded that the unknown android device is John

Macron's is that traces of Kim Kil Whan, who called the emergency center, do not remain on the Google OnHub, and only John Macron is left from among the characters in the scenario.

Table 4-3. Our Conclusion on this Case

Suspect	Probability (%)	Reason
Simon Hallym	10	- There is no reason to give false testimony. - There will be a direct or indirect connection to murder.
John Macron	10	- There is a record of fighting with Betty. - The Amazon echo has a voice of a character other than Simon.
accomplice	80	- As mentioned in Ⅳ.2 Our Conclusion.
Kim Kil Whan	0	- Trace of Kim Kil Whan who called the emergency center do not remain on the Google OnHub. If he was involved in Betty's death, there would be some remaining evidence.

V. Newly Developed Forensic Tools

1. SQLite Databases Extractor

SQLite Databases Extractor is a database extract tool from the EXT4-based device image. It is implemented in Python 2.7 and PyQt5. After extracting all DB files, the tool displays the contents of databases through SQLite3 in real-time. It also provides a function to generate a CSV file that lists the last modified times and MAC addresses of all devices connected through Bluetooth. Finally, files that contain device information (bt_config.xml, wpa_supplicant.conf, usage-YYYYMMDD) can also be extracted.

This program is applicable only to a single file. Therefore, if the device image is split/partitioned, the parts must be combined using 'File-Merge' option. Afterward, putting the merged file (or a single file) into the tool will begin the analysis process described below.

1.1 Analysis Process

First, SQLite Database Extractor finds a Superblock within the EXT4 file system by reading the device image in binary mode. All the necessary information found in this step is used to calculate the Group Descript Table (GDT) and the Inode Table, then the tool saves Inode and data block offsets for all files.

File paths are saved as a list format in Python, and all other information form a dictionary based on Inodes. Data is filtered out if it does not satisfy the pre-set database extension or file path (related to device info.). Unless the file path is corrupted, data blocks of fragmented files are linked in sequence and made into a new file. At this time, information about the database modified time and the MAC addresses of Bluetooth connected devices is processed as a CSV formatted file. The CSV file contains information such as device image name, nickname/alias, file path of the database, and modified times.

1.2 Usage

o File-Merge

To merge split/partitioned files, select the 'File - File-Merge' option on the menu bar. When a new window appears, drag-and-drop the split/partitioned files in it and click the 'Merge' button. The merged file 'File_Merge_Result' is created.

o Extract Databases

Load the device image (EXT4 File System) with 'File – Open File'. The tool starts the analysis process, which takes about 0-2 seconds. After the process is finished, the file names

for the database/device information, and the connected Bluetooth device information are displayed.

Now you can extract and view these files. Use the 'Make_File' toggle button to extract the database file and a file nickname/alias can be assigned. Within a short period (0-5 seconds), database extraction and CSV file generation will be completed. Database contents can be accessed by using the 'DB_VIEW' toggle button from the displayed database list (Exceptions: encrypted file and broken/corrupted files cannot be accessed).

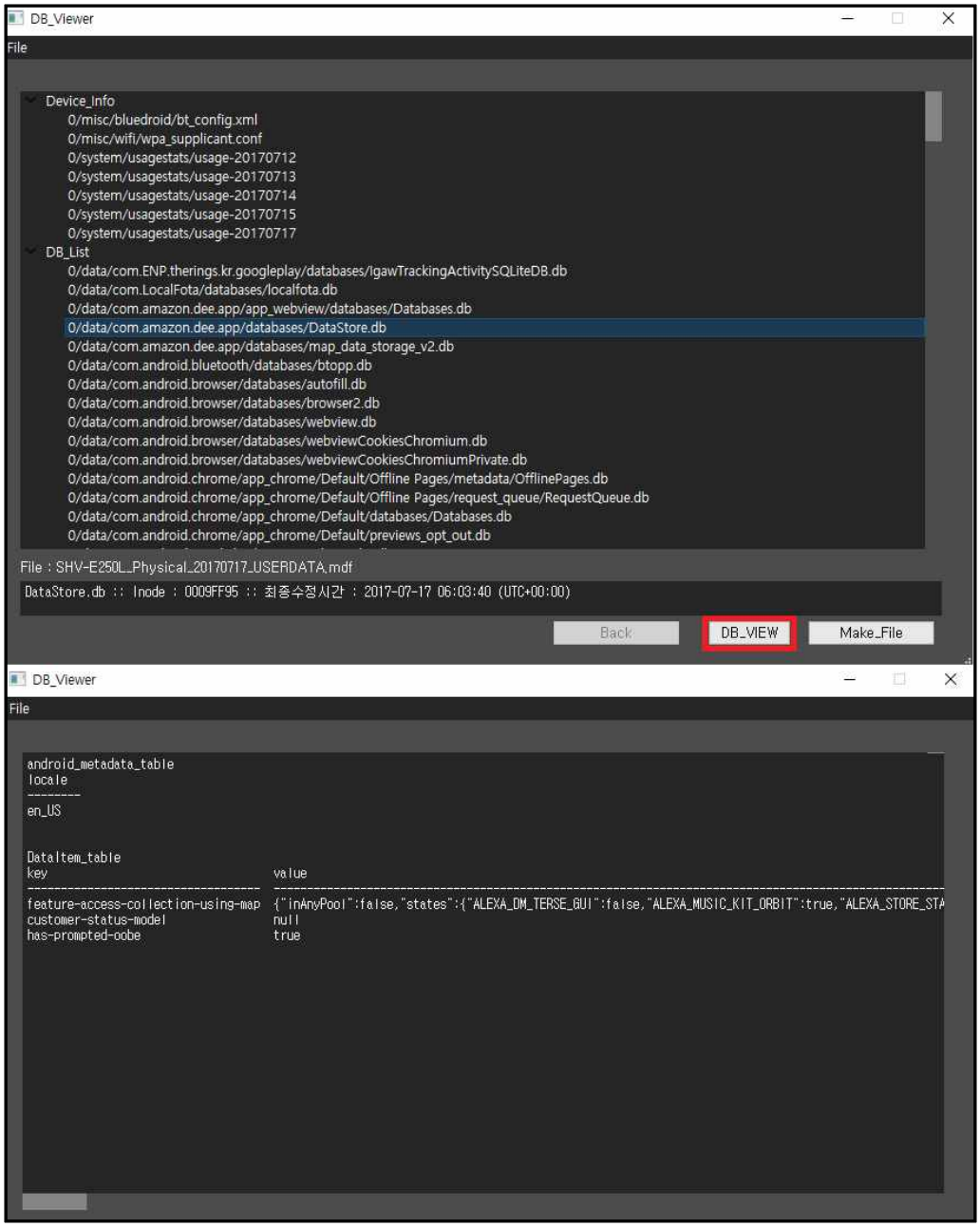


Fig. 5-1 The GUI for SQLite Database Extractor

1.3 How to Interpret the Output File

- o DB_Info and Device_Info folder are created in the same location as the extracted file. The last file is the extracted file.
- o The first line in [imagefilename].csv contains the name of the extracted image file (nickname/alias), extracted time, and extracted Database modified time as UTC+N (N=natural number). The second line displays the latest modified time and file path.
- o Bluetooth.csv lists the MAC addresses of devices with their model names, and the connection times for Bluetooth connected devices. When the device model names and the nickname/aliases obtained with the 'Make_File' toggle function are the same, the MAC address is the device address of the extracted image.

	A	B	C	D	E	F	G	H	I	J	K
1	Database_SHV-E250L_Physical_20170717_USERDATA.mdf(Betty)-2018-02-12 16:32:14	(UTC+00:00)									
2	Modified Time	FileName									
3	2017-07-15 10:23:40	0/data/com.ENP.therings.kr.googleplay/databases/IgawTrackingActivitySQLiteDB.db									
4	2017-07-12 09:16:06	0/data/com.LocalFota/databases/localfota.db									
5	2017-07-13 07:36:27	0/data/com.amazon.dee.app/app_webview/databases/Databases.db									
6	2017-07-17 06:03:40	0/data/com.amazon.dee.app/databases/DataStore.db									
7	2017-07-17 06:03:18	0/data/com.amazon.dee.app/databases/map_data_storage_v2.db									
8	2017-07-12 05:29:49	0/data/com.android.bluetooth/databases/btopp.db									
9	2017-07-12 08:39:53	0/data/com.android.browser/databases/autofill.db									
10	2017-07-12 05:23:31	0/data/com.android.browser/databases/browser2.db									
11	2017-07-12 05:23:31	0/data/com.android.browser/databases/webview.db									
12	2017-07-12 10:22:31	0/data/com.android.browser/databases/webviewCookiesChromium.db									
13	2017-07-12 10:22:31	0/data/com.android.browser/databases/webviewCookiesChromiumPrivate.db									
14	2017-07-13 07:49:57	0/data/com.android.chrome/app_chrome/Default/Offline Pages/metadata/OfflinePages.db									
15	2017-07-13 07:49:56	0/data/com.android.chrome/app_chrome/Default/Offline Pages/request_queue/RequestQueue.db									
16	2017-07-12 08:52:45	0/data/com.android.chrome/app_chrome/Default/databases/Databases.db									
17	2017-07-13 07:49:56	0/data/com.android.chrome/app_chrome/Default/previews_opt_out.db									
18	2017-07-12 05:30:40	0/data/com.android.email/databases/EmailProvider.db									
19	2017-07-12 05:30:40	0/data/com.android.email/databases/EmailProviderBody.db									
20	2017-07-12 05:31:55	0/data/com.android.keychain/databases/grants.db									
21	2017-07-12 09:16:01	0/data/com.android.phone/databases/autoreject.db									
22	2017-07-16 10:17:41	0/data/com.android.providers.calendar/databases/calendar.db									
23	2017-07-12 05:23:12	0/data/com.android.providers.contacts/databases/contacts2.db									

Fig. 5-2. Output File Format for SQLite Database Extractor

2. Google OnHub Log Parser

The Google OnHub Log Parser is a CLI (Command Line) based OnHub Diagnostic Report analysis tool implemented in Python 2.7. It exports the data for connected/disconnected devices in CSV format and the name of the output file can be specified by the user. Furthermore, this file is the input file for Timeline Viewer (Section 4).

2.1 Analysis Process

The tool first decodes a JSON-formatted input file into dictionary format using Python's standard library 'json'. Objects in the input file become keys in the dictionary and the tool uses three objects. The list of objects used is the same as that mentioned in Chapter Ⅱ.

First, the tool makes a list of connected devices. This list consists of several tuples containing MAC address, IP address, dhcphostname and mdnsname. The number of tuples is the same as the number of devices connected to OnHub. A tuple is actually a combination of two datasets. One is the information (MAC, dhcphostname, mdnsname) extracted from the

'infoJSON' object and the other set of data (MAC, IP) is from 'wanInfo'. These constitute one tuple based on the MAC address.

Second, the tool creates another list containing the log messages stored in '/log/messages.x' (x is natural number). The smaller x is, the more recently the log was stored. From the object named 'files', entries containing '/log/messages' in their path are extracted and sorted in chronological order. The extracted data is loaded line by line. If the string 'Connected' or 'Disconnected' is included, the timestamp, MAC and state information are obtained to create one tuple (timestamp, MAC, state).

Finally, the tool exports the generated lists in one CSV file. One list corresponds to one table.

2.2 Usage

First, you should convert the extracted binary form of the diagnostic report into JSON file format. This can be done using onhubdump from Github. Next, enter the following command in cmd.exe to create a result file [output file name].csv.

python OnhubParser.py [JSON file name] [output file name]

- [JSON file name] : JSON-formatted OnHub diagnostic report generated by onhubdump
- [output file name] : specific string used as the name of the result file

2.3 How to Interpret the Output File

The first line shows the analysis time and the time zone information to distinguish the file from the other result files. The rest of the file consists of two tables. The top table shows the connected device information and the second table indicates the connect/disconnect time for the corresponding MAC address.

	A	B	C	D
1	Onhub(Simon's_Home)-2018-02-20 13:03:48	UTC+00:00		
2	MAC	IP	dhcphostname	mdnsname
3	109266000002	192.168.86.28	android-**********	
4	18b430000007	192.168.86.22	**********XDU	**********XDU.local
5	1caf05000006	192.168.86.24	android-**********	
6	2016d8000001	192.168.86.29	ademanafe	ademanafe.local
7	50f520000005	192.168.86.26	android-**********	android-**********-lan.local
8	a002dc000008	192.168.86.21		dp-535302W5.local
9	b827eb000004	192.168.86.25	osmc	osmc.local
10	d052a8000003	192.168.86.27	st-**********	**********.local
11				
12	Time	MAC	State	
13	2017-07-16 08:14:43	50f520000027	Disconnected	
14	2017-07-16 08:14:43	50f520000027	Connected	
15	2017-07-16 08:18:49	b827eb000028	Connected	
16	2017-07-16 09:57:44	a002dc000020	Disconnected	
17	2017-07-16 10:59:12	50f520000027	Disconnected	
18	2017-07-16 10:59:12	50f520000027	Connected	
19	2017-07-16 11:11:46	a002dc000020	Connected	
20	2017-07-17 04:41:26	109266000026	Connected	
21	2017-07-17 04:44:48	109266000026	Disconnected	
22	2017-07-17 05:13:37	a002dc000020	Disconnected	
23	2017-07-17 05:16:13	a002dc000020	Connected	
24	2017-07-17 05:18:44	b827eb000028	Disconnected	
25	2017-07-17 05:21:48	50f520000027	Disconnected	
26	2017-07-17 05:22:12	1caf05000022	Disconnected	
27	2017-07-17 06:00:45	50f520000027	Connected	
28	2017-07-17 06:00:46	1caf05000022	Connected	
29	2017-07-17 06:02:05	b827eb000028	Connected	
30	2017-07-17 06:11:55	109266000026	Connected	
31	2017-07-17 06:15:21	109266000026	Disconnected	
32	2017-07-17 06:20:50	50f520000027	Disconnected	
33	2017-07-17 06:25:21	b827eb000028	Disconnected	
34	2017-07-17 07:21:35	1caf05000022	Disconnected	
35	2017-07-17 07:27:57	2016d800001f	Connected	

Fig. 5-3. Output File Format of Google OnHub Log Parser

3. JSON Parser

The Json Parser is a command line-based tool that extracts specific variables from the scenario's JSON file. Json is a form of name-value pairing, where each value is enclosed in double quotation marks. However, the name value in the provided JSON file is a string not in double quotes. Thus, the tool only extracts the values of the JSON files of the scenario correctly.

The values we focus on in the tool are 'creationTimestamp' and 'summary'. Timestamps are written in Amazon Echo. The summary refers to information the speaker recognizes.

Fig. 5-4. Meaningful Data in the Json File

3.1 Analysis Process

First, the JSON Parser gets the local time to be written to the output file and calculate the time zone information. Then, it verifies whether the target file is a JSON file based on the extension. If the file is a JSON file, the tool extracts the values 'creationTimestamp' and 'summary'.

3.2 Usage

The Json Parser supports file and folder unit extraction. Usage is simple.

python JsonToCsv [arg1] [arg2]

arg1 is the value to select the desired filename. The output filename format is 'Amazon Echo(arg1)-localtime.csv'.

You can put the filename or folder name in the arg2 value. If you enter a file name, it analyzes one file. If you put a folder name, it analyzes all the files in the folder.

3.3 How to Interpret the Output File

The first line shows the analysis time (local time) and the time zone information. The Time columns shows the 'creationTimestamp' in local time. The Filename clearly contains the file name. Finally, the Content columns is the 'summary'. If there is no corresponding value, then 'None' will be written to this column.

	A	B	C
1	Amazon Echo(Simon's_Amazon_Echo)-2018-02-20 13:07:45	UTC+09:00	
2	Time	Filename	Content
3	2017-07-17 15:20:34	1.json	who yes
4	2017-07-17 15:06:03	10.json	alexa
5	2017-07-17 15:01:55	11.json	turn on tv
6	2017-07-17 15:01:54	12.json	alexa
7	2017-07-17 14:45:31	13.json	wake up
8	2017-07-17 11:57:35	14.json	alexa kinda patton a.m. next monday
9	2017-07-17 12:07:00	15.json	
10	2017-07-17 14:31:04	16..json	
11	2017-07-17 14:45:29	17.json	alexa
12	2017-07-17 14:45:43	18.json	alexa stop
13	2017-07-17 15:20:32	2.json	alexa
14	2017-07-17 15:20:07	3.json	turn off tv
15	2017-07-17 15:20:05	4.json	alexa
16	2017-07-17 15:13:02	5.json	stop
17	2017-07-17 15:12:58	6.json	alexa
18	None	7.json	None
19	2017-07-17 15:12:39	8.json	alexa how could you do this what are the flooding
20	2017-07-17 15:06:06	9.json	turn on pandora

Fig. 5-5. Output File Format of Json Parser

4. Timeline Viewer

Timeline Viewer is a visualization tool to show the analysis results of 'SQLite Databases Extractor', 'Google OnHub Log Parser', and 'Json Parser'. Python 2.7 and PyQt4 are used to implement the tool.

4.1 Visualization Process

First, the tool filters files with the csv extension in the user-selected files or directory path. To verify that a filtered file is the correct target file, the tool checks whether the file contains a specific string. If target files exist in the folder, a canvas is constructed by defining the X and Y-axes with the Y-axis labeled 'Devices' and the X-axis labeled 'Time (hours)'. User-specified strings written to the target file are marked on the Y-axis, while integer 0 to 24 are marked on the X-axis. The canvas shows the start and end date contained in the target files and this refers to the period in which all actions (user's request to smart speaker, device connected to router and so on) occurred.

Second, the tool classifies data for the selected date and creates annotations. The results of visualization are as follows.

o Output of SQLite Database Extractor
- An event is shown as a green triangle.
- Annotation shows the file name and time for each event.

o Output of Google OnHub Log Parser
- Connection event is shown as a red circle and disconnection is shown as a black X mark.
- Annotation shows the MAC address, time, and action (Connected or Disconnected).

o Output of Json Parser
- An event is shown as blue star mark.
- Annotation shows the file name, time, and content.

Finally, data corresponding to that day is displayed.

4.2 Usage

The functions of the tool are as follows.
- File analysis
- Directory analysis
- Changing time zone (UTC) change
- Zoom, pan, home button

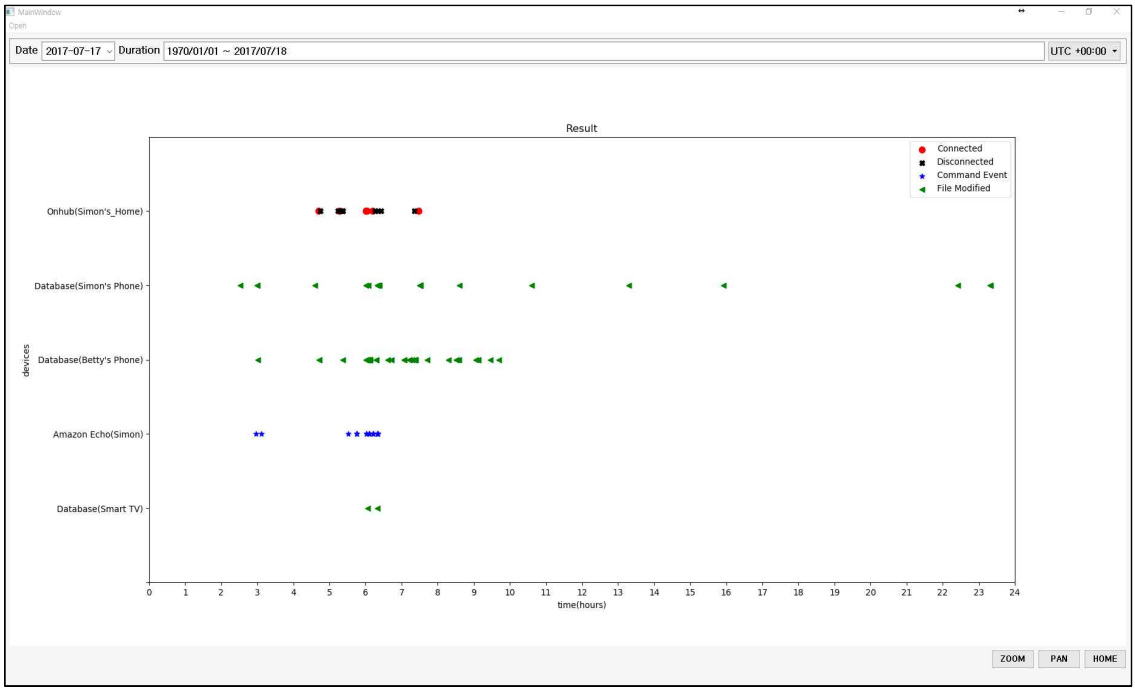


Fig. 5-6. Timeline Viewer

The details of usage are as follows. Choose 'File' or 'Directory' under the 'Open' button on the menu bar. If the duration is displayed normally, select the date you want to see and the corresponding data will be displayed on the canvas. The default time zone is UTC +00:00 but this can be changed for convenience at any time (before or after visualization process).

After all markers are displayed, you can use ZOOM, PAN and HOME button for navigation. ZOOM is for expanding a specific area for a better view. You can use PAN to move the canvas. If you want to undo ZOOM or PAN, click the HOME button. You can mouse-over each marker to view detailed information.

VI. Future Work

Just as Smart Home devices were installed in Hallym's home, the market size of the Smart Home is expected to grow from 24.1 (2016) to 53.45 billion dollars (2022). Not only Samsung, but also Panasonic and Xiaomi's smart devices can be managed using their own smartphone applications. The 'SmartThings Mobile' app from Samsung stores SQLite databases, XML and cache files on the mobile phone. We are planning to study how to obtain device operational information from such files (application data) and find correlations with Smart Home network traffic logs.

VII. Reference

[1] Google OnHub, https://on.google.com/hub/features/

[2] Github, https://github.com/olssonm/google-wifi-api

[3] Wikipedia, https://en.wikipedia.org/wiki/Amazon_Echo

[4] Wikipedia, https://en.wikipedia.org/wiki/Xiaomi_Mi_Band

[5] Xiaomi Mi Band, http://www.mi.com/en/miband/#05

[6] Wikipedia, https://en.wikipedia.org/wiki/Bluetooth_advertising

[7] Introduction to Bluetooth Low Energy, https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt

[8] Github, https://github.com/benmanns/onhub/tree/master/cmd/onhubdump

[9] Hyunji Chung, Jungheum Park, Sangjin Lee, "Digital approaches for Amazon Alexa ecosystem", Digital Investigation, 2017.

[10] Wikipedia, https://en.wikipedia.org/wiki/Google_Hangouts