2017 DFRWS IoT Forensic Challenge

Report

Team Name	IoT Insight
Team Members	Philgeun Jin (Yonsei University)
	Namjun Kim (Sejong University)
	Areum Lee (Sejong University)
	Taehong Kim (Somma Inc.)
	Haeni Kim (Kyungil University)

Index

Table Index

Picture Index

1 Report Summary

1.1 Case 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.

1.2 Verification of interrogation statements

The result of verification of Simon's interrogation statements are as follows. To verify Simon's statements we referred to the details shown in [5. Timeline].

Interrogation Question	Statement	Result of Verification	Remarks
Are you living in this home?	Yes, I am living with Betty. She is my wife, Betty Hallym.	O	
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.	X	
Did she have friends or acquaintances in the area?	I don't think so. We just moved here.	O	
Where did you watch the video?	I was in our bedroom	-	Difficult to verify with collected evidence.
Could you remember what time?	Almost 3? I don't know exactly. Maybe around 3pm. I think that's when we got home.	O	
When you was watching video, didn't you hear anything?	She listens to music, so I used headphones. I didn't hear anything	X	
Can you remember what you were watching?	It was a drama from Youtube	O	

[Table 1-1] Result of interrogation statements verification

1.3 Analysis results

1.3.1 What did Simon do until Betty's death?

Simon stated that at 15:01pm, 2017-07-18, he had used Alexa to watch two videos using Bluetooth headset via SmartTV. After watching video "이연걸 vs 이연걸" from 15:03:29, he started watching the second video at 15:07:32 and finished watching at 15:19:37. According to Simon's statement, Betty was found dead when he came out from the room after finishing watching the video. However, according to logs regarding video play on the SmartTV, the total duration of the second video is 50 minutes, but video play starts at 15:07 and ends 12 minutes later. On checking the Bluetooth pairing history in the SmartTV, we could not confirm any trace of connection with the Bluetooth headset. Thus additional investigation is needed regarding this aspect.

1.3.2 Did Simon murder Betty?

Below is a table of deductions we made based on the evidence collected from the crime scene. 7 of them contradict Simon's statements. Based on this, the probability that Betty was murdered by Simon was 87.5%, and the probability that Betty was murdered by a third person was 12.5%. However, since this probability was computed solely based on the collected evidence, it is likely to change when further investigation is proceeded by analyzing additional data which can be collected from the cloud after syncing the IoT devices (SmartThings, Alexa, etc) with cloud services.

#	Deductions
1	According to Simon's statement, he and Betty came home at three o'clock. However, according to Alexa 's voice, it was confirmed that many people' s voice was recorded at 14:45 on the day of the incident. From this evidence, a third person may have been on the scene.
2	We could not confirm that Simon and Betty came home together at 3 o'clock from the collected evidence.
3	We could not check the time when Simon and Betty came home together. However, we were able to confirm that they were both at the scene of the incident through traces of SmartTV and Alexa use.
4	According to Simon's statement, he used a Bluetooth headset to watch Smart TV. However, we did not see any direct connection between the smart TV and the Bluetooth headset.
5	Betty's contacts did not show anything. Through this, it is judged that there is no one with any grudge against her.
6	According to Simon's statement, he used his headphones to watch TV because Betty was listening to music. However, after checking the collected evidence, it appears that the statement is false because the Pandora application is was executed 5 minutes later via Alexa, than when SmartTV was turned on.
7	On the day of the incident, Simon watched the first video (이연걸 vs 이연걸). However, after playing the second video, Alexa recorded the voice of Simon and Betty fighting. Based on the evidence, it is judged that Simon did not watch the second video.
8	After Simon calls for the ambulance, there is a difference of 11 minutes from the actual reporting time. No trace of her husband during that time can be confirmed.

[Table 1-2] Deductions made from the collected evidence

If the IoT devices are synced to the cloud, additional data which can be collected from the day of the crime to prove the presence of a third person in the crime scene are as follows. (We could not collect these data for this challenge as we did not have access to the cloud accounts.)

#	Details
1	In the SmartThings cloud, if we can check for sensor data connected to the main door at 14:45 and it is an activation event, we can determine the existence of a 3rd person at the crime scene.
2	By analyzing the collected evidence, we were able to confirm the events of the two door sensors. If additional event data is collected from the door sensor, entry and exit records at the crime scene can be checked.
3	If it is true that Simon and Betty arrived home at around 15pm, the SmartThings cloud would have collected data related to the motion sensor, and if there is motion detection data before 15pm, it can be determined that a 3rd person was in the house before their arrival.
4	As a result of analyzing the network packet among the collected evidence, we were able to confirm the MAC address (90: da: 6a: 02: 87: b6) of IP Camera manufacturer (FOCUS H & S Co., Ltd.). If additional data related to IP camera is collected, we will be able to clearly determine the access of a 3rd person, and the reason for Betty's death.

[Table 1-3] Possible scenarios

When the probability of Betty being murdered by Simon is recalculated after applying these results, the result shows that there is 59% chance that she was murdered by Simon.

1.4 Additional Comments

On analyzing the collected evidence from the crime scene, some of them were not in accordance with Simon's statements. Also, there were clear limitations to verifying Simon's statements based solely on the collected evidence. For further analysis in the future, more accurate analysis can be expected if more IoT device (the devices in the crime scene) data are collected from the synced cloud. From the network packets, we could not identify any information which could have direct effect on the case analysis due to the difference in the time of the crime and the time of collection of evidence. However, we were able to list the name of devices which were installed at the crime scene.

2 Introduction

2.1 Aim

Our aim was to analyze the collected data from a home containing several IoT devices, and determine the possibility that the husband(Simon) murdered his wife(Betty).

2.2 Analysis Targets

Evidence	SHA1
Smart TV Raspberry Pi	9ac0de76eca7958bfed1bd5909bbf766409af180
Samsung Note 2 (Betty)	cd494cf3097d8482100ce26dc8e35f0d87b67198
Samsung Note 2 (Simon)	fc28e415ee740531df86a2b227c4f514e9ed40ba
Google OnHub Diagnostic report	20eb4825eaf6c303beadd090868110fb2de37066
Amazon Echo Cloud Data	d1d126f47b565926dcc80fe6a4e7094f0281cb47
MDS (Acme, Inc.) Smarthome Network Dump	6ab6c522b070cde292a18645a19929998e009293

[Table 2-1] Analysis Targets

3 Analysis Results

3.1 Smart TV Raspberry Pi

Device	Details	
Smart TV Raspberry Pi	File size	14.59GB
	File name	E001SmartTVMMC
	Operating system	OSMC
	IP addr (Ethernet)	192.168.165.28
	IP addr (WiFi)	192.168.86.25
	Bluetooth MAC address	B8:27:EB:E6:8D:79

[Table 3-1] Smart TV Raspberry Pi analysis target file details

Simon stated that he arrived home at around 3pm on 7th July 2017, and used a Bluetooth headset to watch TV, after which he found her on the ground when he came into the living room.
The following were identified to determine whether Simon's statement was true :

- List of names, and play times of the videos watched on the Smart TV
- MAC address of Bluetooth devices connected to the Smart TV

On identifying the above, we concluded that the evidence of smart TV use did not match Simon's statement.

Evidence of Smart TV use which were identified are as follows:

Time	Activity
2017-07-17 15:03:29 ~ 15:07:30	1st video play - Title: 이연걸 vs 이연걸 - URL: plugin://plugin.video.youtube/play/?video_id=ibOskbTPZYE
2017-07-17 15:07:32 ~ 15:19:37	2nd video play - 제목: TOP 15 Korea OST - URL: plugin://plugin.video.youtube/play/?video_id=VKfbVLmkQUs

[Table 3-2] Evidence of Smart TV use

We identified a Smart TV YouTube plugin which was installed on the Smart TV. The video play history from the YouTube plugin was found within the system, and we could further identify information such as last played time, title, play count of the video. File information related to YouTube plugin use history is as shown below:

File Path	SHA1
/home/osmc/.kodi/userdata/Database/MyVideos107.db	317b0f080d450703b0d4f69441291603cc9ddeab

[Table 3-3] Database containing YouTube history

Among the database tables, "files" is the name of the table which contains information related to video play history. Information related to the video ID, play count, and last played time are recorded in this table. Videos played from YouTube and related events are shown below.

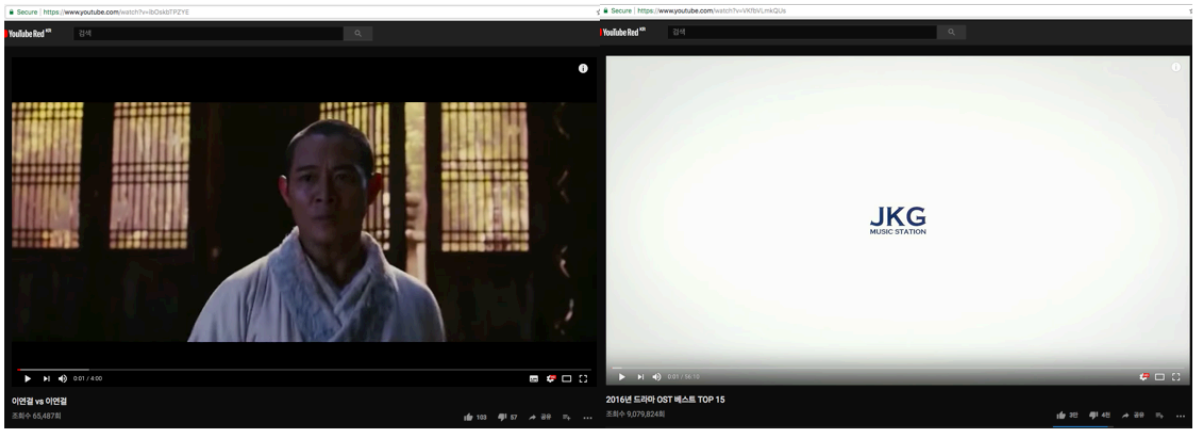
strFilename	playCount	lastPlayed
Filter	Filter	Filter
plugin://plugin.video.youtube/play/?video_id=pF_rqav38Z4	1	2017-07-13 08:43:46
plugin://plugin.video.youtube/play/?video_id=7WX0-O_ENlk	1	2017-07-16 04:54:54
plugin://plugin.video.youtube/play/?video_id=ibOskbTPZYE	1	2017-07-17 02:07:30
plugin://plugin.video.youtube/play/?video_id=VKfbVLmkQUs	NULL	2017-07-17 02:19:37

[Picture 3-1] YouTube video play history

The title of the video corresponding to each video ID could be found through YouTube search. Each time a video is played until the end, the play count increments by 1. Last played time is the time the video play was ended.

VideoId: ibOskbTPZYE

VideoId: VKfbVLmkQUs



[Picture 3-2] YouTube video played on the SmartTV

Last played time was found to be saved in accordance with the operating system's time zone, and the time zone of the system was set as "America/Newyork".

File path	Value	SHA1	Remarks
/etc/timezone	America/New_York	D41D8CD98F00B204E9800998ECF8427E	

[Table 3-4] System time zone

Since the date of the crime was 17 July 2017, Daylight Saving Time had to be applied to the timestamps and converted to Korean Standard Time(KST). The following is the table showing the timestamps converted to KST.

strFileName	playCount	lastPlayed (KST)
plugin://plugin.video.youtube/play/?video_id=pF_rqav38Z4	1	2017-07-13 21:43:46
plugin://plugin.video.youtube/play/?video_id=7WX0-O_ENlk	1	2017-07-17 17:54:54
plugin://plugin.video.youtube/play/?video_id=ibOskbTPZYE	1	2017-07-17 15:07:30
plugin://plugin.video.youtube/play/?video_id=VKfbVLmkQUs		2017-07-17 15:19:37

[Table 3-5] YouTube history after timestamp conversion

Detailed log related to video play can be found in the following file within the system.

File path	SHA1
/home/osmc/.kodi/temp/kodi.log	F8165DDF8B3F28BB7352A2B360B9A66A

[Table 3-6] kodi log file path

The format of the log files is “HH:MM:SS.FFF [LOG_LEVEL]: LOG_MESSAGE”. Some significant logs are as follows.

Timestamp	Details	Remarks
02:03:27.426 T:1938813936	NOTICE: [plugin.video.youtube] Running: YouTube (5.4.0) on Krypton (Kodi-17.3) with Python 2.7.9	
02:03:29.199 T:1958941616	NOTICE: VideoPlayer: Opening: https://r5---sn-i3b7kn76.googlevideo.com/videoplayback?sparams=dur%2Cei%2Cid%2Cinitcwndbps%2Cip%2Cipbits%2Citag%2Clmt%2Cmime%2Cmm%2Cmn%2Cms%2Cmv%2Cpl%2Cratebypass%2Crequiressl%2Csource%2Cexpire&requiressl=yes&mt=1500271293&expire=1500293007&itag=22&lmt=1500105609293231&ei=L1NsWfiEOM684gLE66PQCA&ratebypass=yes&ip=203.253.250.34&pl=24&mime=video%2Fmp4&dur=240.326&mv=m&source=youtube&ms=au&mn=sn-i3b7kn76&mm=31&ipbits=0&key=yt6&id=o-AN36cCxIarsLYxaDaWiaKfYpSDow8FV8NGgXZDzZsE2z&initcwndbps=1697500&signature=D166E73534B5E3738DCCE89031621196647A5899.A4466AA1A2943C7B753FD9A56A10FA0A9EB647B0	1st video play start time
02:07:30.902 T:1518334960	NOTICE: thread end: video_thread	
02:07:30.902 T:1938813936	NOTICE: deleting video codec	1st video play end time
02:07:32.627 T:1938813936	NOTICE: [plugin.video.youtube] Running: YouTube (5.4.0) on Krypton (Kodi-17.3) with Python 2.7.9	2nd video play start time
02:07:33.290 T:1938813936	NOTICE: [plugin.video.youtube] Unable to use mpeg-dash for VKfbVLmkQUs, unable to decipher signature. Attempting fallback play method...	
02:19:37.478 T:1958941616	NOTICE: VideoPlayer: waiting for threads to exit	2nd video play quit
02:19:37.478 T:1958941616	NOTICE: VideoPlayer: finished waiting	

[Table 3-7] Significant kodi log details

Evidence related to Bluetooth pairing could be found in the “/var/lib/bluetooth/cache” folder within the system. When the system and the Bluetooth device are paired in a normal manner, a file is created in the cache folder. The MAC address of the pairing device is used as the filename.

File path	MAC	Vendor	Remarks
/var/lib/bluetooth/B8:27:EB:E6:8D:79/cache/74:C2:46:88:5D:09	74:C2:46:88:5D:09	Amazon Technologies Inc.	Alexa
/var/lib/bluetooth/B8:27:EB:E6:8D:79/cache/88:0F:10:F6:C8:B7	88:0F:10:F6:C8:B7	Huami Information Technology Co.,Ltd.	Mi Fit

[Table 3-8] Bluetooth pairing evidence

From the Bluetooth usage trace, we could identify that 2 devices (Alexa, Mi Fit) were connected to the SmartTV. More importantly, we could not find any trace of a Bluetooth headset being connected to the SmartTV.

3.2 Samsung Note 2 (Betty)

Device	Details	
Samsung Note 2 (Betty)	File size	26.39GB
	File name	SHV-E250L_Physical_20170717_USERDATA
	Operating System	Android 4.4(KitKat)

[Table 3-9] Samsung Note 2 analysis target file details

Simon stated that Betty did not have any friends or acquaintances in the neighborhood. To find out Betty's recent activities and to verify Simon's statement, we looked for the following information:

- Basic system information
- Smartphone contacts
- Use of applications on the day of the crime
- Email
- Recent search word
- Use of Alexa / MiFit

On identifying the above, we could not find any significant digital trace.

To find out the wireless AP and Bluetooth devices to which Betty's phone connected, we analyzed the files in the following table.

File path	SHA1
/misc/bluedroid/bt_config.xml	C21EFDA6BA791EBC1C0F004D0BCA7A0FA4652E50
/misc/wifi/wpa-supplicant.conf	8E01D219390CC6A0716211E49B21F9C0D0527D46

[Table 3-10] Log file containing system information

We identified traces of 3 wireless APs and Bluetooth devices from Betty's cellphone. Judging from this, Betty used her miband(MiFit) and Alexa in sync with her cellphone.

#	MAC	Device name
1	74:c2:46:88:5d:09	Echo-2W5
2	50:f5:20:a5:7d:cc	Simon (SHV-E250S)
3	88:0f:10:f6:c8:b7	MI1A

[Table 3-11] Trace of Bluetooth pairing

#	SSID
1	DFIRE
2	home
3	HOME

[Table 3-12] Trace of wireless internet use

To verify Betty's human relationships, we checked for contacts within the cellphone. The contacts contained only the default group which is setup during reset. Any other data apart from this group was not found. The file path for the contacts is as follows:

File path	SHA1
/data/com.android.providers.contacts/databases/contacts2.db	ED303393177EE8AE86F8654D96BF97D0477EEDBC

[Table 3-13] Contacts file path

The file which contains information about recently used applications can be found in "/system/usagestats/usage-yyyymmdd". Below is the path to the file which contains information about applications used by Betty on the day of the crime (2017-07-17). Nothing peculiar could be found.

File path	SHA1
/system/usagestats/usage-20170717	70C706B3599C45A45006818566DF55E2E5687603

[Table 3-14] Path to file containing information about recently used applications

We could not find any evidence of a separate email application within the system. However, there were evidence of emails received by the google account which was setup during initialization of the device. The following table shows the path to the file wherein the email traces can be found. 2 advertisement emails and 3 general emails were found, and one of the general emails was about miband(MiFit) initial settings.

File path	SHA1
/data/com.google.android.gm/databases/mailstor.betty@gmail.com.db	5EDC1452DE2798D66DB95B3CE17CC49F61F2A9ED

[Table 3-15] Path to file containing email trace

Category	Received time	Sender	Title
Advertisement	n/a	Joyfulfun	Inflatable Water Slide
	n/a	삼성화재DIRECT	삼성다이렉트 운전자보험
General	2017-07-11 21:00:17	"Google 커뮤니티팀" <googlecommunityteam-noreply@google.com>	Hallym님, 새 Google 계정을 최대한 활용해 보세요.
	2017-07-11 23:00:29	"Nest Invitation" <account@nest.com>	Join the Nest home of simon
	2017-07-13 16:45:29	"Xiaomi Corporation" <noreply-account@xiaomi.com>	Activate your Mi Account today

[Table 3-16] Email details

On finding Chrome browser installed on the device, we checked for traces of browser usage. The file related to traces of browser usage is as follows:

File path	SHA1	Remarks
/data/com.android/chrome/app_chrome/Default/History	A1B16C2DE6BBB5ECC24E19C14F93A473083CA70D	Recent search words and downloads list can be found

[Table 3-17] Path to file containing traces of web browser usage

From the traces of browser usage, we could verify that Betty searched for a music album on amazon, on the day of the crime. There were no other significant search words from the day of the crime.

Time	Email title	URL	Visit count
2017-07-12 17:52:38	gmail – Google search	https://www.google.co.kr/search?q=gmail&oq=gmail&aqs=chrome..69i57j0j5j0.2043j0j4&client=ms-android-lgu-kr&sourceid=chrome-mobile&espv=1&ie=UTF-8	1
2017-07-12 17:52:43	N/A	https://www.google.com/gmail/	2
2017-07-12 17:52:43	N/A	https://mail.google.com/mail/	1
2017-07-12 17:52:43	N/A	https://accounts.google.com/ServiceLogin?service=mail&passive=true&continue=https://mail.google.com/mail/&ss=1&scc=1&ltmpl=ecobx&nui=5&	2

		btmpl=mobile&emr=1&osid=1#	
2017-07-12 17:52:43	N/A	https://mail.google.com/accounts/SetOSID?authuser=0&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fpli%3D1%26auth%3D6QQMmrjG4qdYUwKAMoKJ8sOo7wz-d-5jtBJCNIm19aucetqEuvSLJ3gTlYlWIwWeyF4mdw.&osidt=ALWU2cszy4uiuuojCI_o682tHZKiRejso4R9TndcmV7t_Npi8xllEgRxtSqC89eb7iyp28nplX_rwWk4L92MmP0wP_IXRy3GIp6L8i-DMmOffREBMaKBR-V5z8jMLh2lDrTn-fRS1wI8#	1
2017-07-12 17:52:43	N/A	https://mail.google.com/mail/?pli=1&auth=6QQMmrjG4qdYUwKAMoKJ8sOo7wz-d-5jtBJCNIm19aucetqEuvSLJ3gTlYlWIwWeyF4mdw.#1	1
2017-07-12 17:52:43	N/A	https://mail.google.com/mail/?pli=1#	1
2017-07-12 17:52:43	N/A	https://mail.google.com/mail/x/1i69dln4su9dj-/?pli=1&f=1#	1
2017-07-12 17:52:44	N/A	https://mail.google.com/mail/mu/#	1
2017-07-12 17:52:44	Gmail	https://mail.google.com/mail/mu/mp/576/#	2
2017-07-12 17:52:56	N/A	https://mail.google.com/mail/mu/mp/576/#cv/priority/%5Esmartlabel_personal/15d31f384ba73407	1
2017-07-12 17:52:51	N/A	https://mail.google.com/mail/mu/mp/576/#tl/priority/%5Esmartlabel_personal	2
2017-07-17 15:07:29	Bach: Complete Organ Works	https://www.amazon.com/Bach-Complete-Organ-Johann-Sebastian/dp/B001R3YJS8	1

[Table 3-18] Traces of web browser use

On checking the download directory from the user memory space("/data/media/0") within the Android system, we found applications related to 'Alexa' and 'Nest' were individually downloaded and installed on the device. Information about the downloaded files is as below:

File path	SHA1
/data/media/0/download/com.amazon.dee.app_2017-07-03.apk	DCCAE17BAEC0E93D3075E48D80F078B9632088DC
/data/media/0/download/com.nest.android-5.0.0.25-500025-minAPI15	EEA3E0F0E435D7F6EC4C267E2ED5746B591B839D

[Table 3-19] List of downloaded files

To find traces of Alexa use, we looked through the following files:

File path	SHA1
/data/com.amazone.dee.app/shared_prefs/service.identity.xml	651CF39D0849EB3F8B7E19AD7777473B26773819
/data/com.amazone.dee.app/databases/map_data_storage_v2.db	F5BC3AA90DDAFBC11C7CD63DF9AA59F05EF4AEDB
/data/com.amazone.dee.app/app_webview/Cache/*	

[Table 3-20] Path to files containing traces of Alexa use

From the service.identity file, we could find additional information about the user's email, name, and unique ID.

Category	Details
email	betty@gmail.com
name	betty
ID	A4C34GWKR5R6R

[Table 3-21] Details in service.identity.xml

"map_data_storage_v2" file is in SQLite format, and its significant tables are as shown below. Versions prior to "map_data_storage_v2" were not encrypted, but recent versions contained encrypted data. For details about decryption, refer to "**Error! Reference source not found. Error! Reference source not found.**".

Table name	Details
account_data	username, user's unique ID, registered device, token information, etc
device_data	Device serial number, device info version, etc

[Table 3-22] Significant tables in map_data_storage_v2

Some significant data from the decrypted database are as follows:

Category	Column name	Details
account_data	com.amazon.dcp.sso.property.devicename	N/A
	com.amazon.dcp.sso.property.account.acctId	N/A
	com.amazon.dcp.sso.property.firstname	N/A
	com.amazon.dcp.sso.property.username	N/A
device_data	serial.number	N/A

[Table 3-23] Important data after decryption

Data which are set up in the cellphone for managing Alexa were found to be empty in Betty's phone. From this we could deduce that Alexa device was managed not through Betty's phone, but through Simon's phone.

We also analyzed cache data for URL and the request headers, corresponding to the APIs sent to the website(alexa.amazon.com or alexa.amazon.com). However, we could not find any significant data. Results for cache file analysis can be found in "betty_alexa_webview_cache_results" excel file attached separately from this document. We extracted only "JSON" files from the request response data and saved them in "{hash of request file}_1.json" format. For example, if a file name is "0e87ed547c7844af_0", the corresponding response file is saved in "0e87ed547c7844af_1.json".

File name
betty_alexa_webview_cache_result
betty_alexa_webview_cache_response_data/*

[Table 3-24] Result file for Alexa cache file analysis

Also, we could not find any trace of sync between the miband(MiFIt) application on Betty's phone, and Betty's miband(MiFit) device.

3.3 Samsung Note 2 (Simon)

Device		Details
Samsung Note 2 (Simon)	File size	26.39GB
	File name	SHV-E250S_Physical_20170718_USERDATA
	Operating System	Android 4.4(KitKat)

[Table 3-25] Samsung Note 2 analysis target file details

To find out Simon's recent activities, we looked for the following information:

- Basic system information
- Smartphone contacts
- Use of applications on the day of the crime
- Recent search word
- Traces of Alexa/SmartThings use

On identifying the above, we could not find any significant digital trace.

To find out the wireless AP and Bluetooth devices to which Simon's phone connected, we analyzed the files in the following table.

File path	SHA1
/misc/bluedroid/bt_config.xml	642B2C48A04F17DEBCA141C87BEC6B2336592457
/misc/wifi/wpa-supplicant.conf	0B7A9C4260631B001E631F7CC8FD865DC8698D64

[Table 3-26] Log file containing system information

Results are in the table below. We identified traces of connection to 9 wireless APs and 4 Bluetooth devices from Simon's cellphone. Among the Bluetooth devices were Alexa, MiBand(MiFit), and Bluetooth headset. Simon might have used the Bluetooth headset after connecting the SmartTV with his cellphone. Further investigation regarding the use of Bluetooth headset is needed.

#	MAC	Device name
1	1c:af:05:9e:19:74	Betty (SHV-E250L)
2	74:c2:46:88:5d:09	Echo-2W5
3	88:0f:10:f6:c8:b7	MI1A
4	b8:ad:3e:01:5b:6a	LG HBS900

[Table 3-27] Traces of Bluetooth pairing

#	SSID
1	T wifi zone_secure
2	T wifi zone
3	U+zone
4	IoTLab_WAN
5	IoTLab
6	neo_house5
7	home
8	setupEBC2
9	HOME

[Table 3-28] Traces of wireless internet use

To verify Simon's human relationships, we checked for contacts within the cellphone. However, we could not collect any contacts information from within the system due to database corruption.

File path	SHA1
/data/com.android.providers.contacts/databases/contacts2.db	7843AB71CF5B2E908025B69E31FCCD61447B9715

[Table 3-29] Path to contacts

The following table shows the file which contains information about applications which were used by Simon on the day of the crime (2017-07-17). Nothing peculiar could be found.

File path	SHA1
/system/usagestats/usage-20170717	386D50FA65AB07866E5552FA3C6B50C38C786978

[Table 3-30] Path to file containing information about recently used applications

We could not find any trace of a separate email application within the system. However, there were traces of emails received by the google account which was setup during initialization of the device. The following table shows the path to the file wherein the email traces can be found. 8 advertisement emails and 6 general emails were found. Two of the general emails were related to Samsung account initial settings. We deduced that Simon created a Samsung account to use the “smartthings” application.

File path	SHA1
/data/com.google.android.gm/databases/mailstore.simonhallym@gmail.com.db	8AD06028D47D1C394D8072EF6EEB26BEDB9A945D

[Table 3-31] Path to file containing email trace

(Email details in Korean are not translated)

Category	Received time	Sender	Title
Advertisement	n/a	하나투어 항공 - 하나투어 전세계 최저가 항공권 예약	해외항공권 최저가 예약
		삼성화재DIRECT	삼성다이렉트 운전자보험
		삼성화재DIRECT	삼성다이렉트 운전자보험
		하나투어 항공 - 하나투어 전세계 최저가 항공권 예약	해외항공권 최저가 예약
		삼성화재DIRECT	삼성다이렉트 운전자보험
		하나투어 항공 - 하나투어 전세계 최저가 항공권 예약	해외항공권 최저가 예약
		삼성화재DIRECT	삼성다이렉트 운전자보험
		하나투어 항공 - 하나투어 전세계 최저가 항공권 예약	해외항공권 최저가 예약
General	2017-07-11 23:16:30	"삼성계정" <SA.noreply@samsung-mail.com>	삼성서비스 이용을 위하여 삼성계정 Email 인증을 완료해 주세요.
	2017-07-11 23:17:05	"삼성계정" <SA.noreply@samsung-mail.com>	삼성서비스에 오신 것을 환영합니다.
	2017-07-13 16:28:36	"" <pandora@pandora.com>	Welcome to Pandora
	2017-07-14 01:35:25	"Nest" <news@nest-email.com>	Are you cozy yet?
	2017-07-15 05:03:09	"" <Pandora@pandora.com>	Not sure where to start?
	2017-07-16 05:11:06	"" <Pandora@pandora.com>	Take your listening even further

[Table 3-32] Email details

On finding Chrome browser installed on the device, we checked for traces of browser usage. The file related to traces of browser usage is as follows:

File path	SHA1	Remarks
/data/com.android/chrome/app_chrome/Default/History	FFA803D285A3CC6B93644625CB4CD89962123D13	Recent search words and downloads list can be found

[Table 3-33] Path to file containing traces of web browser usage

From the traces of browser usage, we could find 6 traces of Simon accessing the Samsung login page. From this, we deduced that Simon was the one generally in charge of managing SmartThings data.

Time	Email title	URL	Visit count
2017-07-12 13:46:33	Samsung ACCOUNT	https://us.account.samsung.com/accounts/ANDROIDSDK/signIn?locale=en_US&svcParam=eyJzdmNFbmNJViI6ImVhYzcwM...	1
2017-07-12 15:50:25	Samsung ACCOUNT	https://us.account.samsung.com/accounts/ANDROIDSDK/signIn?locale=en_US&svcParam=eyJzdmNFbmNJViI6ljc1NTE1N2Z...	2
2017-07-12 17:46:43	Samsung ACCOUNT	https://us.account.samsung.com/accounts/ANDROIDSDK/signIn?locale=en_US&svcParam=eyJzdmNFbmNJViI6ImQwMmViZDg3Z...	1
2017-07-13 02:35:02	Samsung ACCOUNT	https://us.account.samsung.com/accounts/ANDROIDSDK/signIn?locale=en_US&svcParam=eyJzdmNFbmNJViI6IjJmMTA1OD...	2
2017-07-13 18:13:33	Samsung ACCOUNT	https://us.account.samsung.com/accounts/ANDROIDSDK/signIn?locale=en_US&svcParam=eyJzdmNFbmNJViI6IjgwMzA2NTlkNjI...	1
2017-07-13 18:13:40	Samsung ACCOUNT	https://us.account.samsung.com/accounts/ANDROIDSDK/signIn?locale=en_US&svcParam=eyJzdmNFbmNJViI6IjlkYmZmOTk...	1
2017-07-16 16:38:14	Json – Google search	https://www.google.co.kr/search?q=josn&oq=josn&aqs=chrome..69i57j0l3.1033j0j4&client=ms-android-skt-kr&sourceid=chrome-mobile&ie=UTF-8	1
2017-07-16 16:38:18	JSON - Wikipedia	https://en.m.wikipedia.org/wiki/JSON	1
2017-07-16 16:38:19	Ajax(programming) - wikipedia	https://en.m.wikipedia.org/wiki/Ajax_(programming)	1
2017-07-16 16:38:45	json이란 – Google search	https://www.google.co.kr/search?q=json%EC%9D%B4%EB%9E%80&oq=json%EC%9D%B4%EB%9E%80&aqs=chrome..69i57j0l2.9006j0j4&client=ms-android-skt-kr&sourceid=chrome-mobile&ie=UTF-8	2
2017-07-16 16:38:47	N/A	https://www.google.co.kr/search?q=json%EC%9D%B4%EB%9E%80&oq=json%EC%9D%B4%EB%9E%80&aqs=chrome..69i57j0l2.9006j0j4&client=ms-android-skt-kr&sourceid=chrome-mobile&ie=UTF-8#xxri=0	1
2017-07-16 16:38:47	KS blog	http://killins.egloos.com/m/3013974	2
2017-07-16 16:38:47	KS blog	http://m.egloos.zum.com/killins/v/3013974	1

[Table 3-34] Traces of web browser use

On checking the download directory from the user memory space("/data/media/0") within the Android system, we found applications related to 'Alexa' and 'Nest' were individually downloaded and installed on the device. Information about the downloaded files is as below:

File path	SHA1
/data/media/0/download/com.amazon.dee.app_2017-07-03.apk	DCCAE17BAEC0E93D3075E48D80F078B9632088DC
/data/media/0/download/com.nest.android-5.0.0.25-500025-minAPI15	EEA3E0F0E435D7F6EC4C267E2ED5746B591B839D

[Table 3-35] List of downloaded files

To find traces of Alexa use, we looked through the following files:

File path	SHA1
/data/com.amazone.dee.app/shared_prefs/service.identity.xml	651CF39D0849EB3F8B7E19AD7777473B26773819
/data/com.amazone.dee.app/databases/map_data_storage_v2.db	E537F8E17F8ACB943ED86CFB265B831006FD4C2A
/data/com.amazone.dee.app/app_webview/Cache/*	

[Table 3-36] Path to files containing traces of Alexa use

From the service.identity file, we could find additional information about the user's email, name, and unique ID.

Category	Details
email	simonhallym@gmail.com
name	simonhallym
Id	A32TRBM6QOXJ5H

[Table 3-37] Details in service.identity.xml

The following table shows significant information which were retrieved after decrypting the encrypted data in the "map_data_storage_v2" database. From the decrypted data, we can determine that the Alexa device was mostly managed through Simon's phone.

Category	Column name	Details
account_data	com.amazon.dcp.sso.property.devicename	simon's Android Device
	com.amazon.dcp.sso.property.account.acctId	amzn1.account.AHP3QR64GFO24DGHVS3CXJ7NUIXQ
	com.amazon.dcp.sso.property.firstname	Simon
	com.amazon.dcp.sso.property.username	simon
device_data	serial.number	63fe6859a242470fbfc6345cc1c74342

[Table 3-38] Important data after decryption

We also analyzed cache data for URL and the request headers, corresponding to the APIs sent to the website(alexa.amazon.com or alexa.amazon.com). However, there were no traces from the day of the crime. Results for cache file analysis can be found in "simon_alexa_webview_cache_results" excel file attached separately from this document. We extracted only "JSON" files from the request response data and saved them in "{hash of request file}_1.json" format. For example, if a file name is "0e87ed547c7844af_0", the corresponding response file is saved in "0e87ed547c7844af_1.json".

File name
simon_alexa_webview_cache_result
simon _alexa_webview_cache_response_data/*

[Table 3-39] Result file for Alexa cache file analysis

We checked the following files to find traces of SmartThings use.

File path	SHA1
/data/com.smartthings.android/database/ ua_analytics.db	A22CB22F886290B86FE566483944B32FDAF15FE0
/data/com.smartthings.android/database/ ua_preferences.db	43A225CE386DE177096DD69CC273352A2A357F6F
/data/com.smartthings.android/app_webview/Cache/*	
/data/com.smartthings.android/cache/http/*	

[Table 3-40] File path to traces of SmartThings use

"ua_analytics" database contains information such as event time, whether the application was executed, event ID, etc. However, exact meaning could not be deciphered. Comparison with the data synced to the SmartThings cloud service is required for further understanding.
In the table "ua_preferences.db" was a column ("com.urbanairship.application.metrics.LAST_OPEN") which contained the time the application was last executed. And according to it, the last execution time was day after the day of the crime.

We also analyzed cache data for URL and the request headers, corresponding to the APIs sent to the website(alexa.amazon.com or alexa.amazon.com). However, there were no traces from the day of the crime. Results for cache file analysis can be found in "simon_smartthings_webview_cache_results" file attached separately from this document. We extracted only "JSON" files from the request response data and saved them in "{hash of request file}_1.json" format. For example, if a file name is "0e87ed547c7844af_0", the corresponding response file is saved in "0e87ed547c7844af_1.json".

File name
simon_smartthings_webview_cache_result
simon_ smartthings _webview_cache_response_data/*

[Table 3-41] Results of SmartThings WebView cache file analysis

SmartThings application had traces of HTTP cache data. By analyzing these cache data, we could find traces from the day of the crime. Following is the table of analysis results. We assumed that the Multipurpose Sensor in the SmartThings kit was used as the door sensor. We were able identify two events of deactivation of the Multipurpose Sensor from the day of the crime. Additional data regarding the purpose of sensors connected to SmartThings, installed location of sensors, data synced in the cloud, etc seem to be required.

File name	Time	Details
387fdae596cbe510a84e74f76fb7dd0d_1.json	2017-07-17 15:20:17	{{ device.displayName }} was closed "date": "2017-07-17T06:20:17.681Z"
	2017-07-17 15:53:37	{{ device.displayName }} was closed "date": "2017-07-17T06:53:37.681Z"

[Table 3-42] Results of SmartThings HTTP cache file analysis

Detailed results for cache file analysis can be found in "simon_smartthings_http_cache_results" file attached separately from this document. We extracted only "JSON" files from the request response data and saved them in "{hash of request file}_1.json" format. For example, if a file name is "0e87ed547c7844af_0", the corresponding response file is saved in "0e87ed547c7844af_1.json".

File name
simon_smartthings_http_cache_result
simon_ smartthings_http_cache_response_data/*

[Table 3-43] Result file for SmartThings HTTP cache file analysis

4 Amazon Echo Cloud Data

Category	Details	
Amazon Echo Cloud Data	File size	4.66MB
	File name	005-Amazon-Echo-Alexa-Web-Scrape.zip

[Table 4-1] Amazon Echo cloud data analysis target

The collected Amazon Echo Cloud Data contained voice commands made by the user to Alexa, json data, executed commands, and screenshots of Alexa cloud data. We looked for the following information:

- Connection with IoT devices
- Commands executed by the user

From our observation of the above details, there was a 3rd person in the couple's home on the day of the crime.

We checked the json files of the commands made to Alexa, and ordered them chronologically:

Time	Voice command	File name
2017-07-17 11:57:35	alexa kinda patton a.m. next monday	14.json
2017-07-17 12:07:00	N/A	15.json
2017-07-17 14:31:04	N/A	16.json
2017-07-17 14:45:29	alexa	17.json
2017-07-17 14:45:31	wake up	13.json
2017-07-17 14:45:43	alexa stop	18.json
2017-07-17 15:01:54	alexa	12.json
2017-07-17 15:01:55	turn on tv	11.json
2017-07-17 15:06:03	alexa	10.json
2017-07-17 15:06:06	turn on pandora	9.json
2017-07-17 15:12:39	alexa how could you do this what are the flooding	8.json
2017-07-17 15:12:58	alexa	6.json
2017-07-17 15:13:02	stop	5.json
2017-07-17 15:20:05	alex	4.json
2017-07-17 15:20:07	turn off tv	3.json
2017-07-17 15:20:32	alexa	2.json
2017-07-17 15:20:34	who yes	1.json

[Table 4-2] Alexa voice commands

Simon stated that he came home with Betty around 15pm on the day of the crime. However, an Alexa voice command file from 14:45pm contains the voice of a 3rd person (other than Simon and Betty). Thus, there is high possibility that a 3rd person was at the scene of crime.

The 7th voice command file contains the voice of a male (most probably Simon) getting angry at Betty. And while this is happening, the woman gives a voice command by saying "Alexa, stop." From this, we know that there was an argument between a man and a woman at 15:12pm on the day of the crime. Also, since there was no music in that background, we can deduce that the woman stopped the music before the argument. According to Simon's statement in the interrogation with the investigator, he was watching a video at this time. Moreover, there is evidence that YouTube video was play at this time. Thus, additional interrogation and corresponding statements are required regarding this aspect.

Alexa device's data was synced to the cloud. On analyzing the screenshot files of the synced data, we could find information as shown in the following table. We found screenshots of the voice command made to Alexa, but could not find anything unusual.

Category	Details	Synced account	Installed place	Relevant device	File name
Smart Home Skills	Nest Thermostat	N/A	N/A	N/A	2017-07-17h07_00.png
	SmartThings Outlet (Samsung Connect)				
Devices	Nest Thermostat	N/A	Living Room	N/A	2017-07-17h06_10.png
	SmartThings Outlet	N/A		TV	
Music Services	Amazon Music	simonhallym@gmail.com	N/A	N/A	2017-07-17h10_06.png
	Pandora				

[Table 4-3] Result of Alexa cloud data analysis

5 Timeline

The timeline for the day of the crime, based on the analysis results of the evidence collected from the crime scene, is as follows. We wrote the verifications of the statements in [1.2 Verification of interrogation statements] based on this.

By listing Simon and Betty's actions in chronological order (as shown in the table below), we could find evidences which did not match the statements Simon made during the interrogation. However, we could not find any evidence that clearly pointed at Betty's murderer. Due to this, further investigation is needed regarding the mismatch in Simon's statements and the collected evidences, and the data synced to the cloud is to be collected and analyzed.

Time	Details
2017-07-17 14:33:47	One of the door sensors were deactivated.
2017-07-17 14:45:31	By checking the Alexa voice command traces, we could identify a voice of a 3rd person.
2017-07-17 15:00:00	Simon stated that he and Betty returned home at around 3 pm on the day of the incident.
2017-07-17 15:01:54	We checked the Alexa voice command trace and found that SmartTV was turned on at 15:01pm
2017-07-17 15:03:29	Checking the YouTube plugin and kodi log of SmartTV, We were able to check the first video play at 15:03pm
2017-07-17 15:06:06	We checked the Alexa voice command traces and were able to see that the Pandora application was running at 15:06pm
2017-07-17 15:07:32	Checking the YouTube plugin and kodi log of SmartTV, We were able to check the second video play at 15:07pm.
2017-07-17 15:12:39	We checked the Alexa voice command trace and found that there was a quarrel between a man and a woman at 15:12pm.
2017-07-17 15:20:07	We checked the Alexa voice command trace and found that SmartTV powered off at 15:20pm.
2017-07-17 15:20:34	After checking the Alexa voice command trace, we were able to identify that Simon called the ambulance at 15:20pm.

[Table 5-1] Timeline

6 List of Collected Evidence Files

Category	File path	SHA1
Smart TV	/home/osmc/.kodi/userdata/Database/MyVideos107.db	317b0f080d450703b0d4f69441291603cc9ddeab
	/home/osmc/.kodi/temp/kodi.log	73C3FE2D9E2F63D3BACE2AB3AE796388990E5A80
Betty	/misc/bluedroid/bt_config.xml	C21EFDA6BA791EBC1C0F004D0BCA7A0FA4652E50
	/misc/wifi/wpa-supplicant.conf	8E01D219390CC6A0716211E49B21F9C0D0527D46
	/data/com.android.providers.contacts/databases/contacts2.db	ED303393177EE8AE86F8654D96BF97D0477EEDBC
	/system/usagestats/usage-20170717	70C706B3599C45A45006818566DF55E2E5687603
	/data/com.google.android.gm/databases/mailstor.betty@gmail.com.db	5EDC1452DE2798D66DB95B3CE17CC49F61F2A9ED
	/data/com.android/chrome/app_chrome/Default/History	A1B16C2DE6BBB5ECC24E19C14F93A473083CA70D
	/data/com.amazone.dee.app/shared_prefs/service.identity.xml	651CF39D0849EB3F8B7E19AD7777473B26773819
	/data/com.amazone.dee.app/databases/map_data_storage_v2.db	F5BC3AA90DDAFBC11C7CD63DF9AA59F05EF4AEDB
Simon	/misc/bluedroid/bt_config.xml	C21EFDA6BA791EBC1C0F004D0BCA7A0FA4652E50
	/misc/wifi/wpa-supplicant.conf	8E01D219390CC6A0716211E49B21F9C0D0527D46
	/data/com.android.providers.contacts/databases/contacts2.db	ED303393177EE8AE86F8654D96BF97D0477EEDBC
	/system/usagestats/usage-20170717	70C706B3599C45A45006818566DF55E2E5687603
	/data/com.google.android.gm/databases/mailstor.betty@gmail.com.db	5EDC1452DE2798D66DB95B3CE17CC49F61F2A9ED
	/data/com.android/chrome/app_chrome/Default/History	A1B16C2DE6BBB5ECC24E19C14F93A473083CA70D
	/data/com.amazone.dee.app/shared_prefs/service.identity.xml	651CF39D0849EB3F8B7E19AD7777473B26773819
	/data/com.amazone.dee.app/databases/map_data_storage_v2.db	F5BC3AA90DDAFBC11C7CD63DF9AA59F05EF4AEDB
	/data/com.smartthings.android/database/ua_analytics.db	A22CB22F886290B86FE566483944B32FDAF15FE0
	/data/com.smartthings.android/database/ua_preferences.db	43A225CE386DE177096DD69CC273352A2A357F6F

[Table 6-1] List of collected evidence

7 Appendix

7.1 map_data_storage_v2 decryption

When there is a connection between an Alexa device and an Android device, user information and device information are encrypted and saved in the “map_data_storage_v2” database. By analyzing the Alexa application, we could find out that AES algorithm was used for database encryption, and used CBC mode. The key for decrypting the encrypted data can be found in “/data/data/com.amazon.dee.app/shared_prefs/com.amazon.identity.auth.device.storage.LocalOnlySQLDB.encryption.namespace.xml”. In this XML file is the key with which the database can be decrypted. Use the value of “com.amazon.identity.auth.device.storage.LocalOnlySQLDB.encrypt.key”. The following table shows an example.

key	value
com.amazon.identity.auth.device.storage.LocalOnlySQLDB.encrypt.key	3JKUrmvTArAFAOldfCfzlA==

[Table 7-1] Example of decryption key

Code which can be used to decrypt the encrypted database can be found here:
“https://gist.github.com/bunseok bot/89670a66ca5f0545348ce27791176fe7”

7.1 Android Cache

Android WebView cache format is similar to that of Chrome disk cache file, but they are not exactly same. Android application requests for the “https://m.media-amazon.com/images/G/01/csm/showads.v2.js” file and cache files such as those in the table below are created.

File name	Data
{16 length hash}_0	request URL, request HTTP header
{16 length hash}_1	request URL, response data
{16 length hash}_2	request URL

[Table 7-2] Android WebView cache filename rule and data

HTTP request and header file data are not compressed, and response data in HTTP response are either compressed with gzip algorithm or in raw data form. We found that response data which were compressed with gzip algorithm were mostly json or html data. Traces of recent use can be checked by analyzing HTTP communication data between the application and the server, or the application and device, through android WebView cache files.

The structure of the “{16 length hash}_0” file was similar to that of Chrome disk cache file. However, we could not do a perfect analysis because the rest of the file structure was not clear.

The file structure of the “{16 length hash}_0” file is as follows:

Offset	Length	Significance	Example	Remark
0	8	Signature	0x305C72A71B6DFBFC04	
8	4	Unknown	0x4000000	
12	4	URL Length	0x31	Little Endian
16	4	Unknown	0xBADB2C80	
20	4	Reserved	0x00000000	
24	URL Length	URL	https://smartthings.zendesk.com/embeddable/config	

-	4	Data Length	0x1C10	Little Endian
-	Data Length	Data	HTTP Header(GET, ….)	
-	8	Footer	0xD8410D97456FFAF4	
-	8	Unknown	0x010000002495A9C1	

[Table 7-3] Structure of "{16 length hash}_0" file

The file structure of the "{16 length hash}_1" file is as follows:

Offset	Length	Significance	Example	Remark
0	8	Signature	0x305C72A71B6DFBFC04	
8	4	Unknown	0x4000000	
12	4	URL Length	0x31	Little Endian
16	4	Unknown	0xBADB2C80	
20	4	Reserved	0x00000000	
24	URL Length	URL	https://smartthings.zendesk.com/embeddable/config	
0	8	Signature	0x305C72A71B6DFBFC04	
8	4	Unknown	0x4000000	
-	-	Data	HTTP Response Data	
-	8	Footer	0xD8410D97456FFAF4	
-	8	Unknown	0x010000002495A9C1	

[Table 7-4] Structure of "{16 length hash}_1" file

If the application had used the "OkHttp" library (which is a HTTP communication library for android), we could see that HTTP cache file was created. The cache file was in the following form. Its structure was not in binary format, but was comprised of HTTP Request Header and HTTP Response Data.

File name	Data
{32 length hash}_0	request URL, request HTTP header
{32 length hash}_1	Response data

[Table 7-5] Android HTTP cache filename rule and data

Among the collected evidence in this case, SmartThings application HTTP cache file could be found in Simon's mobile application. And as a result of analysis, we could find out that it was possible to analyze the data related to HTTP communication between the application and the device.

Code for Android WebView analysis can be found here:
"https://gist.github.com/bunseokbot/9d9e5cc3fa1b82876e33e66430f 9a387"

Code for HTTP cache analysis can be found here:
"https://gist.github.com/bunseo kbot/9d9e5cc3fa1b82876e33e66430f9a387"

7.2 Alexa API

Below is a list of API which can be sued to check for Alexa cloud data. They can be used to retrieve the exact same data which we acquired by analyzing the Alexa voice command, JSON, screenshot files collected from the murder case.

Category	Division	API	Details
Account	Information	https://alexa.amazon.com/api/household	User information of users registered to the device
Smart Home	Information	https://alexa.amazon.com/api/phoenix	Information about connected smarthome devices and scenes
	Group	https://alexa.amazon.com/api/phoenix/group	Smart Home Group
Device	Network	https://alexa.amazon.com/api/device-wifi-details?deviceSerialNumber=(serial)&deviceType=(type)	Information about network connected to Alexa
	Information	https://alexa.amazon.com/api/devices-v2/device	Alexa information
	Bluetooth	https://alexa.amazon.com/api/bluetooth	Bluetooth connection information
	Preference	https://alexa.amazon.com/api/device-preferences	Device preferences including local time and address
Activities	Audio	https://alexa.amazon.com/api/utterance/audio/data?id=(utteranceId)	Audio file download
	Command	https://alexa.amazon.com/api/activities/(customerid)%23(timestamp)%23(type)%23(serial)	Command information
	List	https://alexa.amazon.com/api/activities?startTime=&size=(size)&offset=1	List of command information (size <= 50)
	Recent	https://alexa.amazon.com/api/media/historical-queue?deviceSerialNumber=(serial)&deviceType=(type)&size=(number history to view)&offset=-1	Music application history
	Card	https://alexa.amazon.com/api/cards?limit=(count)	Activity card list
To-Do	List	https://alexa.amazon.com/api/todos?startTime=&endTime=&completed=&type=(type)&size=(size)	To do list
Music	List	https://alexa.amazon.com/api/np/player?deviceSerialNumber=(serial)&deviceType=(type)	List of music/radio currently playing
Server	Status	https://alexa.amazon.com/api/ping	Alexa server connection status
		https://alexa.amazon.com/api/allowed-providers	List of third-party providers currently being used
		https://alexa.amazon.com/api/bootstrap	Information about currently logged in user
		https://alexa.amazon.com/api/devices-v2/device	List of devices connected to Amazon account
		https://alexa.amazon.com/api/wifi/configs	Wifi information saved in the Amazon server
		https://alexa.amazon.com/api/traffic/settings	Device location
		https://alexa.amazon.com/api/wake-word	List of wake-words
		https://alexa.amazon.com/api/third-party	Third party application names
		https://alexa.amazon.com/api/eon/householdaccounts	Linked Google calendars
		https://alexa.amazon.com/api/notifications	Timer and alarm list
		https://alexa.amazon.com/api/customer-status	User agreement status

[Table 7-6] Alexa API List

7.3 SmartThings API

In this case, evidence related to SmartThings were heavily inclined toward application data remaining in the cellphone. Thus, they were insufficient to verify Simon's statements. If additional data are collected from the synced cloud, new evidence related to verification of Simon's statements and the murder case are likely to be found. Additional data which can be collected are listed below:

Category	API	Details	Remaks
User	https://graph-na04-useast2.api.smartthings.com/login/auth	Login authentication	Login
Location	https://graph-na04-useast2.api.smartthings.com/location/list	list of locations	
	https://graph-na04-useast2.api.smartthings.com/location/show/(locationId)	location information	
Hub	https://graph-na04-useast2.api.smartthings.com/hub/list	list of hubs	
	https://graph-na04-useast2.api.smartthings.com/hub/show/(hubId)	hub information	
	https://graph-na04-useast2.api.smartthings.com/hub/(hubId)/events?source=false	Events from hub	
Device	https://graph-na04-useast2.api.smartthings.com/device/list	list of devices	
	https://graph-na04-useast2.api.smartthings.com/device/show/(deviceId)	Device information	
	https://graph-na04-useast2.api.smartthings.com/device/(deviceId)/events	Event information from device	
	https://graph-na04-useast2.api.smartthings.com/device/states/(deviceId)?attribute=(attribute)	State logging informa tion from device	
Location	https://graph-na04-useast2.api.smartthings.com/location/installedSmartApps/(locationId)	list of SmartApps mapped in location id	SmartAPP
	https://graph-na04-useast2.api.smartthings.com/installedSmartApp/show/(SmartAppId)?deviceId=(deviceId)	SmartApp information	

[표 7-7] SmartThings API List