

202 – Where have you been?

Team Information

Team Name : DogeCoin

Team Member : Dongbin Oh, Donghyun Kim, Donghyun Kim, Yeongwoong Kim

Email Address : dfc-dogecoin@naver.com

Instructions

Description You are an investigator. You got a tip-off that 'Alice' who is required to enter mandatory quarantine in her home went out, after being tested positive for COVID-19. When you investigated 'Alice', she said "I just went out in front of the house for a while". You confirmed that 'Alice' left her smartphone at home and went out wearing a wearable device. For epidemiological investigations, you should analyze the wearable device to check the path of 'Alice'.

Target	Hash (SHA-256)
Alice_Gear_S3.ad1	6a59be484f10a5a8e9baf61b6bf4b39c

Questions

1	Identify the following information of the wearable device. ➤ Device Model Name ➤ SW version ➤ Device OS, Version ➤ Serial Number ➤ Device MAC address ➤ WiFi MAC address	25
2	Identify the following information of connected smartphone. ➤ Device Name ➤ Device OS/Version ➤ SW Version ➤ Samsung Account	25
3	Why did Alice go out?	50

4	Did Alice intentionally leave her smartphone at home? What led you to that conclusion?	50
5	Where did Alice visit on May 22 nd ?	50

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	WEFA	Publisher:	DFRC
Version:	1.53		
URL:	http://forensic.korea.ac.kr/tools.html		

Name:	SQLite DB Browser	Publisher:	Mauricio Piacentini
Version:	3.12.2		
URL:	https://sqlitebrowser.org/		

Name:	Sublime Text3	Publisher:	Sublime HQ Pty Ltd
Version:	Build 3211		
URL:	https://www.sublimetext.com/3		

Step-by-step methodology:

1. Identify the following information of the wearable device.

- Device Model Name : Samsung Gear C
- SW version : R775SKSU2FUD1
- Device OS, Version : Tizen 4.0.0.7
- Serial Number : R5AJ30186D
- Device MAC address : 40:D3:AE:68:AC:EB
- WiFi MAC address : 40:D3:AE:68:AC:EC

문제에서 주어진 파일이름 “Alice_Gear_S3.ad1”을 보아 Gear S3라는 삼성 Tizen OS를 사용하는 smart wearable device를 사용하고 있음을 추정할 수 있다. Tizen OS에서는 아래의 경로에서 문제에서 원하는 Device Model Name과 이하의 정보들을 확인할 수 있다.

- /usr/home/owner/apps_rw/com.samsung.w-manager-service/WearableStatus.xml

/usr/home/owner/apps_rw/com.samsung.w-manager-service /는 Tizen OS의 application을 관리하는 apps_rw 하위에 있는 폴더로서 com.samsung.w-manager-service라는 application을 통해 Host Device와 Wearable Device의 정보를 관리하고 있다.¹

그 중 Wearable device의 정보를 확인할 수 있는 것은 data 폴더 안의 WearableStatus.xml로 아래와 같이 문제에서 필요로 하는 정보를 모두 얻을 수 있다.

```
<?xml version="1.0" encoding="UTF-8"?>
<DeviceStatus>
  <device>
    <deviceID>40:D3:AE:68:AC:EB</deviceID>
    <deviceName>Samsung Gear C</deviceName>
    <devicePlatform>Tizen</devicePlatform>
    <devicePlatformVersion>4.0.0.7</devicePlatformVersion>
    <deviceType>GearC</deviceType>
    <modelNumber>SM-R775S</modelNumber>
    <swVersion>R775SKSU2FUD1</swVersion>
    <salesCode>SK0</salesCode>
    <countryCode>KR</countryCode>
    <serialNumber>R5AJ30186D</serialNumber>
    <MCC>450</MCC>
    <MNC>05</MNC>
    <connectivity>
      <peerID>SAMSUNG_ACCESSORY_40:D3:AE:68:AC:EB</peerID>
      <btAddress>40:D3:AE:68:AC:EB</btAddress>
      <wifiAddress>40:D3:AE:68:AC:EC</wifiAddress>
    </connectivity>
  </device>
</DeviceStatus>
```

[그림 1] WearableStatus.xml 내부 데이터

파일 이름으로 예상했던 기기 종류는 예상했던 바와 다르게 Samsung Gear C임을 확인할 수 있으며, 문제에서 요구하는 Device MAC address의 경우, PeerID에서 사용하는 MAC address를 참고하였을 때, btAddress(블루투스 MAC address)를 Device MAC address로 사용하고 있음을 확인할 수 있다.

¹ Odom, Nicole R., et al. "Forensic inspection of sensitive user data and artifacts from smartwatch wearable devices." *Journal of forensic sciences* 64.6 (2019): 1673-1686.

2. Identify the following information of connected smartphone.

- Device Name : Galaxy S7 Edge
- Device OS/Version : Android 8.0.0
- SW Version : R16NW.G935LKLJ1
- Samsung Account : dfc.alice@gmail.com

- /usr/home/owner/apps_rw/com.samsung.w-manager-service/HostStatus.xml

1 번 문항과 동일하게 /usr/home/owner/apps_rw/com.samsung.w-manager-service/ 이하에 존재하는 파일에서 Host 와 관련된 정보를 확인할 수 있다. 아래는 관련 내용인 data 폴더 하의 HostStatus.xml 이다. 문제에서 요구하는 Device name 을 포함한 모든 내용을 확인할 수 있다.

```
<?xml version="1.0" encoding="UTF-8"?><DeviceStatus>
<device>
<deviceID>E4:FA:ED:09:08:C0</deviceID>
<deviceName>Galaxy S7 edge</deviceName>
<devicePlatform>android</devicePlatform>
<devicePlatformVersion>8.0.0</devicePlatformVersion>
<deviceType>Host</deviceType>
<modelNumber>SM-G935L</modelNumber>
<swVersion>R16NW.G935LKLJ1</swVersion>
<salesCode>LUC</salesCode>
<countryCode>KR</countryCode>
<MCC>00</MCC>
<MNC>00</MNC>
<SDKVersion>26</SDKVersion>
<Resolution>1080x1920</Resolution>
<connectivity/>
<deviceFeature>
```

[그림 2] HostStatus.xml 내부 데이터

- /usr/dbspace/.CompanionInfo.db

.CompanionInfo.db 에서도 HostStatus.xml 과 같이 Host Device(Companion Device)에 관련된 정보를 확인할 수 있다.² Sqlite 형식으로 되어 있어서 SQLite DB Browser 와 같은 도구가 필요하다. 문제에서 요구한 정보를 확인 가능하다.

² Becirovic, Seila, and Sasa Mrdovic. "Manual IoT Forensics of a Samsung Gear S3 Frontier Smartwatch." *2019 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2019.

	key	value
필터	필터	
1	device_id	E4:FA:ED:09:08:C0
2	device_model_name	Galaxy S7 edge
3	device_model_number	SM-G935L
4	device_platform_type	android
5	device_platform_version	8.0.0
6	device_binary_version	R16NW.G935LKLU3ETJ1
7	device_manufacturer	samsung
8	sales_code	LUC
9	country_code	KR
10	sim_mcc	00
11	sim_mnc	00
12	sim_subscriber_number	unknown

[그림 3] .CompanionInfo.db 내부 데이터

- /usr/dbspace/5001/.account.db

삼성 계정 정보의 경보의 경우 /usr/dbspace/5001/.account.db 에서 확인할 수 있다. 5001 폴더 이하에 있는 것으로보아 주 사용자의 삼성 계정 정보임을 추가로 확인할 수 있다. 해당 내용은 다음과 같다.

테이블:  account			
	_id	user_name	email_address
필터	필터	필터	필터
1	1	dfc.alice@gmail.com	dfc.alice@gmail.com

[그림 4] .account.db 내부 데이터

3. Why did Alice go out?

.wemail.db 라는 이메일 내역을 확인할 수 있는 database 를 확인한 결과 자가격리 구역을 이탈하여 “분노의 질주” 영화를 보러가려한 것을 확인하였다.

/usr/home/owner/apps_rw/com.samsung.wemail/data/dbspace/wemail.db 은 Samsung Gear 에 내장된 기본 mail application 으로 .wemail.db 라는 Sqlite Database Browser 를 통해 아래와 같은 내용을 확인할 수 있다. 시간 순으로 정렬하여 메일의 흐름을 확인할 수 있다.

From: charlie dfc <dfc.charlie@gmail.com>
Date: 5/12/21 1:54 PM (GMT+09:00)
To: dfc.alice@gmail.com
Subject: Re: Where shall we meet?

Dear alice,

How is your health??
Anything you want to eat? Didn't you forget the promise you made to see today?
Where do you want to meet?

from charlie.
Thx. <tag:thisisover-1>

[그림 5] 5/12 : Charlie → Alice 에서 건강 안부 및 약속에 대해 물어봄

2021년 5월 21일 (금) 오후 2:01, dfc.alice <dfc.alice@gmail.com>님이 작성:
Dear, Charlie. ↳ Thank you for Your concern! I'm much better now. ↳ Sorry for not contacting Us On the 11th appointment. ↳ But after all medical tests were done, I was asked to self isolate. ↳ I think it will be difficult to meet for the time being. ↳ thanks. From Alice.

Sent from my Samsung Galaxy Watch

[그림 6] 5/21 : Alice → Charlie 자가 격리 중이며 만나기 힘들다고 전달

Dear Alice,

The exact test results haven't come out yet??
If self-isolation, is there no problem in the examination?
If you only stay at home, isn't it stuffy?

Let's go out to breathe together! How about eating something delicious and spending the day?

[그림 7] 5/21 : Charlie → Alice 아직 Test 결과가 안나왔는지에 대해 물어봄

<tag:cid:ii_koyg2ndc0>

2021년 5월 21일 (금) 오후 5:16, dfc.alice <dfc.alice@gmail.com>님이 작성:

Charlie, I want to go out to get some air, too. But when in self-quarantine, if i leave the house my location will be tracked. It will probably be reported to the disease control authorities. Thx...

Sent from my Samsung Galaxy Watch

[그림 8] 5/21 : Alice → Charlie 자가격리 중 집을 나가면 추적당한다고 함

Alice, Did you receive this guidance?
If you leave your phone at home, its possible!
Then you wont be able to track your location and it will be safe.
Would you like to go to the movies? 'Fast and Furious' is newly released!

[그림 9]

5/22 : Charlie → Alice 핸드폰을 집에 두고 오면 추적 당하지 않는다고 괜찮다고함,
Fast and Furious 영화를 같이 보자고 함

메일에서 언급한 this guidance 는 .wemail.db 상 첨부파일 경로를 확인하여 아래와 같은 파일임을 확인할 수 있음(/usr/home/owner/apps_rw/com.samsung.wemail/data/1/22/image.png)



[그림 10] 메일 첨부 이미지

Alice, The last place I went was sold out.
Try watching it at a nearby movie theater!

see you there 3 PM!

2021년 5월 22일 (토) 오후 1:33, charlie dfc <dfc.charlie@gmail.com>님이 작성:

yep, See you there at 3 o'clock!

2021년 5월 22일 (토) 오전 1:12, dfc.alice <dfc.alice@gmail.com>님이 작성:

Umm... yes! okay. If i leave my cell phone, i think it will be fine. Lets go to the movie~!! Are you going to see it there the last time you saw it??

Sent from my Samsung Galaxy Watch

[그림 11]

5/22 : Alice → Charlie 내가 핸드폰을 놓고가면 괜찮을 거 같다며, 저번에 봤던 영화관에서 영화를 보자고 함

5/22 : Charlie → Alice 저번에 보던 영화관에서 표가 매진되어 근처에서 보자고 함

위의 메일 내용을 종합하여 봤을 때, Alice 는 5/12 일 경 부터 자가격리 중이었으며 5/21 일까지 자가격리가 진행되던 와중, 핸드폰을 놓고 가면 추적당하지 않을 수 있다는 Charile 의 말을 듣고 답답함에서 벗어나기 위해 영화를 보러가기 위해 이탈하려한 것을 확인할 수 있음

4. Did Alice intentionally leave her smartphone at home? What led you to that conclusion?

문제의 지문을 통해 집을 나갈 때 스마트폰을 놓고 갔음을 확인할 수 있으며 메일 내역(.wemail.db)를 통해 추적당하지 않기 위함이란 것을 확인할 수 있다. 또한 의도적으로 스마트폰 사용 대신 Wearable device 만 사용하기 위해 “Standalone Mode”로 전환한 것을 runestoneGearLog 를 통해 확인할 수 있다.

먼저 3 번 문항을 통해 추정할 수 있는 영화관에 가기 위해 스마트폰을 놓고 가면 추적 당하지 않을 수 있다는 이메일 내역은 아래와 같다.

2021년 5월 22일 (토) 오후 1:33, charlie dfc <dfc.charlie@gmail.com>님이 작성:

yep, See you there at 3 o'clock!

2021년 5월 22일 (토) 오전 1:12, dfc.alice <dfc.alice@gmail.com>님이 작성:

Umm... yes! okay. If i leave my cell phone, i think it will be fine. Lets go to the movie~!! Are you going to see it there the last time you saw it??

Sent from my Samsung Galaxy Watch

[그림 12] 스마트폰 추적과 관련한 이메일 내역

그러나 위의 내용은 “추적당하지 않을 수 있다”와 관련된 내용이고 실제 Alice 가 스마트폰을 놓고 갔는지 여부는 확인할 수 없다. Alice 가 스마트폰을 놓고 갔는지 여부는 문제에서 주어진 지문을 통해 확인할 수 있다.

Description You are an investigator. You got a tip-off that 'Alice' who is required to enter mandatory quarantine in her home went out, after being tested positive for COVID-19. When you investigated 'Alice', she said "I just went out in front of the house for a while". You confirmed that 'Alice' left her smartphone at home and went out wearing a wearable device. For epidemiological investigations, you should analyze the wearable device to check the path of 'Alice'.³

[그림 13] 스마트폰을 두고 간 것과 관련한 문제 지문

문제의 지문 상 Alice는 외출 시 wearable device를 착용한 채 스마트폰을 두고 갔음을 확인하였다. 추가적으로 문제에서 요구한 “Intentionally”를 만족하기 위해서는 Alice 가 스마트폰을 의도적으로 놓고, wearable device로 필요한 연락 등을 주고 받을 수 있는 조치를 취했는지를 확인하여야 한다.

Wearable device 의 경우, 크게 Connected Mode 와 Standalone Mode 로 구분되어 동작한다. Connected Mode 의 경우 Bluetooth 와 Wifi 를 이용하여 Host Device 와 데이터를 주고 받으며, Standalone Mode 의 경우 Long-Range Cellular 를 이용하여 application 작동에 필요한 데이터를 주고 받게 된다. 상세한 내용은 아래와 같다.³

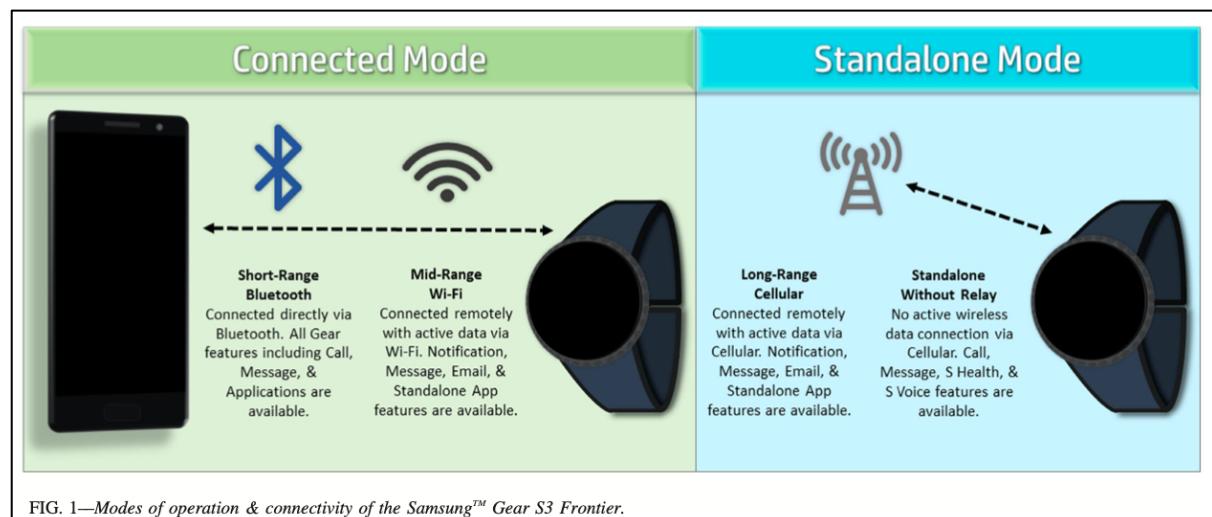


FIG. 1—Modes of operation & connectivity of the Samsung™ Gear S3 Frontier.

[그림 14] Wearable Device 의 모드

즉, Standalone Mode 는 Host Device 가 부재할 수 있는 상황에서 Wearable Device 만 사용하기 위한 기능임을 알 수 있다. 관련된 내용을 파악하기 위해 grep 을 통하여 아래와 같은 내역을 확인할 수 있었다.

³ Odom, Nicole R., et al. "Forensic inspection of sensitive user data and artifacts from smartwatch wearable devices." *Journal of forensic sciences* 64.6 (2019): 1673-1686.

```
(base) sin90@odongbin-ui-MacBookPro 202 % grep -r "standalone mode" .
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/11 18:36:40:359 gear change to standalone mode!
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/12 11:20:37:338 gear change to standalone mode!
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/12 13:18:07:358 gear change to standalone mode!
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/13 13:33:10:378 gear change to standalone mode!
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/13 14:13:37:376 gear change to standalone mode!
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/16 20:55:02:373 gear change to standalone mode!
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/17 09:37:26:338 gear change to standalone mode!
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/21 23:48:52:382 gear change to standalone mode!
./usr/home/owner/apps_rw/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/22 13:28:42:420 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/11 18:36:40:359 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/12 11:20:37:338 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/12 13:18:07:358 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/13 13:33:10:378 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/13 14:13:37:376 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/16 20:55:02:373 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/17 09:37:26:338 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/21 23:48:52:382 gear change to standalone mode!
./usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~:2021/05/22 13:28:42:420 gear change to standalone mode!
```

[그림 15] Standalone Mode 전환 로그

/usr/apps/com.samsung.runestone-gear/data/runestoneGearLog 의 실제 내용을 확인해본 결과 Charile 와 메일을 주고 받은 시간 근방에 Standalone mode 로 전환한 것을 확인하였다.

```
2021/05/22 13:15:00:168 get_cpu_usage alarm triggered started
2021/05/22 13:28:42:309 on_service_connection_terminated = [0]
2021/05/22 13:28:42:309 change_to_standalone_mode, m_mode value[1]
2021/05/22 13:28:42:326 Mode changed, new mode is [1], previous mode is [2]
2021/05/22 13:28:42:420 gear change to standalone mode!
2021/05/22 13:28:42:421 gps location stop
2021/05/22 13:28:42:432 add one alarm success, id 22 [Caller log_collector_cpu_usage_collector_start_collecting]
2021/05/22 13:28:43:440 add one alarm success, id 23 [Caller __start_collecting]
2021/05/22 13:28:43:440 location collector add alarm common
2021/05/22 13:28:44:636 CommutingTimeEventMonitor::setupAlarms
2021/05/22 13:35:00:148 enter pedometer api callback
2021/05/22 13:36:39:249 location_collector_start_lm
2021/05/22 13:36:39:255 get_cpu_usage alarm triggered started
```

[그림 16] Standalone Mode 유지 로그

추가적으로 이 Standalone Mode 는 수면시간이 될 때까지 유지되었음을 아래 로그를 통해 확인하였다.

```
2021/05/22 23:54:54:205 wear status update to[0]
2021/05/22 23:55:17:140 current is not Companion mode, can not sync the real sleep time stat data to mobile
2021/05/22 23:55:17:195 CommutingTimeEventMonitor::setupAlarms
2021/05/22 23:55:17:200 Received event:event.com.samsung.runestone-gear.analysis_sleep_time_event
2021/05/22 23:55:17:200 Sleep_Time_Event_Monitor::setupEventSchedule start
2021/05/22 23:55:17:235 deleteAlarmForSleepCheck.
```

[그림 17] 외출 관련 Standalone Mode 전환 로그

이를 통해 의도적으로 외출 시 Wearable device 만 사용하기 위해 Standalone Mode로 변경하였음을 확인할 수 있다.

5. Where did Alice visit on May 22nd?

- 14 시 경 : 집 -> 목동 CGV (by GPS, Gear Browser 검색 내역)
- 17 시 30 분 경 : 까치산역 (by WIFI 검색 내역, Navermaps 검색 내역)
- 21 시 30 분 경 : 당산역 까치방앗간 근처 (by WIFI 검색, Navermaps 검색 내역)
- 23 시 15 분 경 : 당산역 근처 (by WIFI 검색)

일련의 문항 풀이를 통해, 특히 메일과 관련된 아티팩트를 확인하여 아래와 같이 Alice 는 5/22 에 영화관에 가기 위해 자가격리를 이탈한 것을 추정할 수 있다.

mail_time	mail_title	mail_body	mail_preview
필터	필터	필터	필터
2021-05-11 23:18:56	Where shall we ...	Dear alice,	Dear alice, How ...
2021-05-12 13:54:50	Re: Where shall ...	Dear alice,	Dear alice, How ...
2021-05-21 15:56:06	Re: Where shall ...	Dear Alice,	Dear Alice, The e...
2021-05-21 23:57:55	Re: Where shall ...	Alice, Did you receive this guidance?If you leave your phone at home, its possible!	Alice, Did you re...
2021-05-22 13:33:53	Re: Where shall ...	yep, See you there at 3 o'clock:2021년 5월 22일 (토) 오전 1:12, dfc.alice ,dfc.alice@gmail.com,님이 작성:	yep, See you the...
2021-05-22 14:05:16	Re: Where shall ...	Alice, The last place I went was sold out. Try watching it at a nearby movie theater!	Alice, The last pl...

[그림 18] 메일 관련 DB

본 문항을 풀이하기 위해서 1) 실제로 메일에서 확인한 봄과 같이 영화관에 간 것인지, 2) 추가적인 방문지가 있는 것은 아닌지에 대해 초점을 맞추어 문제를 풀이하고자 한다.

본격적인 문제를 풀이하기 이전에 5/22에 Alice 가 실제로 사용한 Application 를 확인하기 위해 아래와 같이 /usr/home/owner/applications/dbspace/.context-app-history.db 를 살펴보았다.

rowId	AppId	Duration	AudioJack	BSSID	UTC	LocalTime
필터	필터	필터	필터	필터	필터	필터
168	com.fin10.tizen.gearbrowser	0	0		2021-05-22 04:39:55	2021-05-22 13:39:55
169	com.fin10.tizen.gearbrowser	46	0		2021-05-22 04:40:08	2021-05-22 13:40:08
170	com.fin10.tizen.gearbrowser	0	0		2021-05-22 04:40:59	2021-05-22 13:40:59
171	com.fin10.tizen.gearbrowser	0	0		2021-05-22 04:43:01	2021-05-22 13:43:01
172	com.fin10.tizen.gearbrowser	0	0		2021-05-22 04:45:17	2021-05-22 13:45:17
173	GjEbuFc12C.NaverMap	166	0		2021-05-22 04:46:04	2021-05-22 13:46:04
174	com.fin10.tizen.gearbrowser	89	0		2021-05-22 04:51:12	2021-05-22 13:51:12
175	com.samsung.wemail	15	0		2021-05-22 05:03:14	2021-05-22 14:03:14
176	com.samsung.wemail	16	0		2021-05-22 05:03:30	2021-05-22 14:03:30
177	com.samsung.tizen.bixby-voice	0	0		2021-05-22 05:03:46	2021-05-22 14:03:46
178	com.samsung.wemail	3	0		2021-05-22 05:03:52	2021-05-22 14:03:52
179	com.samsung.wemail	0	0		2021-05-22 05:09:03	2021-05-22 14:09:03
180	GjEbuFc12C.NaverMap	141	0		2021-05-22 05:09:17	2021-05-22 14:09:17
181	GjEbuFc12C.NaverMap	6	0		2021-05-22 05:11:40	2021-05-22 14:11:40
182	GjEbuFc12C.NaverMap	10	0		2021-05-22 05:14:22	2021-05-22 14:14:22
183	com.samsung.clocksetting	33	0		2021-05-22 05:14:35	2021-05-22 14:14:35
184	GjEbuFc12C.NaverMap	1	0		2021-05-22 05:15:28	2021-05-22 14:15:28
185	GjEbuFc12C.NaverMap	3	0		2021-05-22 05:17:06	2021-05-22 14:17:06
186	com.fin10.tizen.gearbrowser	5	0		2021-05-22 05:17:15	2021-05-22 14:17:15
187	com.fin10.tizen.gearbrowser	164	0		2021-05-22 05:17:21	2021-05-22 14:17:21
188	GjEbuFc12C.NaverMap	3	0		2021-05-22 05:20:13	2021-05-22 14:20:13
189	GjEbuFc12C.NaverMap	1	0		2021-05-22 05:20:20	2021-05-22 14:20:20
190	GjEbuFc12C.NaverMap	6	0		2021-05-22 05:23:07	2021-05-22 14:23:07

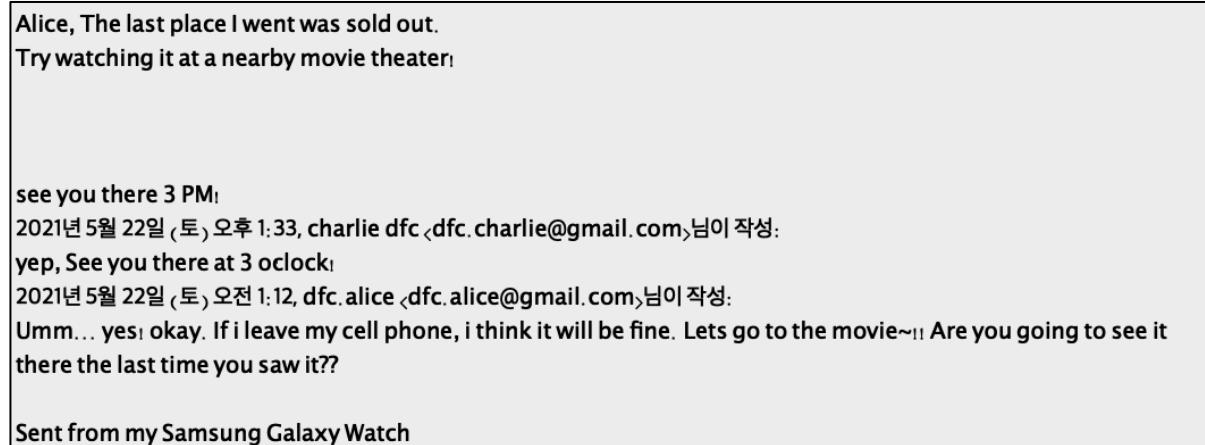
[그림 19] 어플리케이션 사용 History DB

5/22에 사용한 Application 은 Navermap, gearbrowser, wemail, bixby-voice, clocksetting임을 확인할 수 있다. 추가적으로 앱 실행과 관련된 /usr/data/performance/launch_hist.0 를 통해서도 관련 기록들을 확인할 수 있다. .context-app-history.db 에서는 확인할 수 없었던 .wemail-send 와 같은 시간을 추가적으로 확인할 수 있다. 위의 Application 이 남기는 3rd Party application 과 더불어 기기에서 남기는 WIFI 및 GPS Log 를 기반으로 Alice 가 방문한 장소를 확인해보도록 하겠다.

2021/05/22 01:05:50 +09:00 L RE com.samsung.wemail 163 594 1 5 3325 11659
2021/05/22 01:06:48 +09:00 L IN com.samsung.wemail-send 150 1249 5 0 1301 0
2021/05/22 01:12:14 +09:00 L IN com.samsung.w-clock-viewer 166 788 11 0 942 0
2021/05/22 03:44:05 +09:00 F FR wemail 25125
2021/05/22 13:36:51 +09:00 L IN com.fin10.tizen.gearbrowser 165 3127 1 0 3127 0
2021/05/22 13:38:51 +09:00 L RE com.samsung.wemail 121 1004 1 6 3325 9883
2021/05/22 13:39:06 +09:00 L RE com.fin10.tizen.gearbrowser 131 435 1 1 3127 435
2021/05/22 13:39:52 +09:00 F FR wemail 25125
2021/05/22 13:40:08 +09:00 L IN com.fin10.tizen.gearbrowser 166 1914 2 1 2520 435
2021/05/22 13:43:00 +09:00 L IN com.fin10.tizen.gearbrowser 167 1782 3 1 2274 435
2021/05/22 13:45:17 +09:00 L IN com.fin10.tizen.gearbrowser 172 1719 4 1 2135 435
2021/05/22 13:46:04 +09:00 L IN GjEbuFc12C.NaverMap 167 3013 3 1 3226 507
2021/05/22 13:51:12 +09:00 L IN com.fin10.tizen.gearbrowser 133 3548 5 1 2418 435
2021/05/22 13:53:34 +09:00 L IN com.samsung.wemail-send 86 1742 6 0 1375 0
2021/05/22 14:03:14 +09:00 L RE com.samsung.wemail 92 637 1 7 3325 8562
2021/05/22 14:03:30 +09:00 L RE com.samsung.wemail 102 481 1 8 3325 7552
2021/05/22 14:03:46 +09:00 L IN com.samsung.tizen.bixby-voice 102 1448 1 0 1448 0
2021/05/22 14:04:07 +09:00 F FR wemail 25125
2021/05/22 14:09:13 +09:00 F FR wemail 25125
2021/05/22 14:09:17 +09:00 L IN GjEbuFc12C.NaverMap 115 3278 4 1 3239 507
2021/05/22 14:14:35 +09:00 L RE com.samsung.clocksetting 152 917 1 16 4112 805
2021/05/22 14:15:28 +09:00 L RE GjEbuFc12C.NaverMap 168 483 4 2 3239 495
2021/05/22 14:17:15 +09:00 L IN com.fin10.tizen.gearbrowser 149 3523 6 1 2602 435
2021/05/22 14:20:13 +09:00 L RE GjEbuFc12C.NaverMap 103 1126 4 3 3239 705
2021/05/22 14:24:13 +09:00 L RE com.samsung.clocksetting 114 638 1 17 4112 795
2021/05/22 14:24:18 +09:00 L IN com.samsung.clocksetting.display 109 1596 1 0 1596 0
2021/05/22 14:24:39 +09:00 L IN com.samsung.clocksetting.style 101 1391 4 0 1123 0
2021/05/22 14:24:41 +09:00 L IN com.samsung.w-clock-viewer 90 1194 12 0 963 0
2021/05/22 14:24:47 +09:00 L RE GjEbuFc12C.NaverMap 94 509 4 4 3239 656
2021/05/22 14:44:46 +09:00 L RE GjEbuFc12C.NaverMap 143 423 4 5 3239 609
2021/05/22 17:32:33 +09:00 L IN com.samsung.clocksetting 200 868 2 17 2490 795
2021/05/22 17:32:38 +09:00 L IN com.samsung.clocksetting.connections 191 1304 13 0 1131 0
2021/05/22 17:32:40 +09:00 L IN com.samsung.bluetooth 184 1365 6 0 1717 0
2021/05/22 17:33:37 +09:00 L IN GjEbuFc12C.NaverMap 172 3971 5 5 3385 609

[그림 20] 어플리케이션 사용 History Log

- Alice는 실제로 영화관에 갔는가



[그림 21] 영화 시청 및 자가격리 이탈 관련 이메일

기 확보한 이메일 내역을 통해 5/22 15 시 근방에 Alice 는 charile 와 영화를 보기 위해 자가격리를 이탈하려고 했음을 알 수 있다. 이를 검증하기 위해 타임라인 상 15 시 이전에 사용한 ‘NaverMap’, ‘gearbrowser’의 로그를 집중적으로 확인하였다.

1) Navermap

Navermap 과 관련된 로그는 /usr/home/owner/apps_rw/GjEbuFc12C, /usr/apps/GjEbuFc12C 에서 확인할 수 있다. 두 폴더에 존재하는 파일 내역은 실질적으로 동일하다.

```
(base) sin90@odongbin-ui-MacBookPro GjEbuFc12C % find . -type d | sed -e "s/[^-][^/]*// | /g" -e "s/|\\([^\ ]\\)/|-\\1/" .
+-cache
+-shared
+-data
+-chromium-efl
+-data
+-|-SPP
+-|-GPU Cache
+-|-Local Storage
+-cookie
+-pref
```

[그림 22] chromium-efl 폴더 탐지

폴더 구조를 통해 확인해본 결과 chromium-efl 이라는 폴더를 확인하여 chromium 을 기반으로 동작하고 있음을 추정할 수 있다. 먼저 ./data/.pref 폴더 내에 존재하는 파일을 대상으로 strings 를 통해 아래와 같은 내역을 확인할 수 있다.

```
(base) sin90@odongbin-ui-MacBookPro .pref % cat *
INDX( ?
?{ 779b_e
??[e
|???????;0?|??0?|??0? (06604d1ec2f683059589e1b4887abf64fd290bb8`e
??[e
|???????;0?0???0?0???0?HA (18711aa53eace2feba047b3c30c6767a5
56592e4\`e
??[e
U???0???;0?
U???0?
U???0? (1cf5d73b7a69f181b015d00639f1ccda03300b5be
??[e
0????0???;0?0???0?0???0? (40c3322b3b3d0d946724fe784d3466362
9e1932aae
??[e
0????0???;0?0???0?0???0? (' (51523d3efc0ca031d7abd4a78c94ed0dd22892ff)e
??[e
|????0???;0?|??0?|??0? (a7656b83ce914523e797050707f11d71
81fb3b9de
??[e
0????0???;0??'??0?0???0? (b4267db460d1cf7f96464cba4f1f4a3a29c134eace
??[e
0????0???;0?0???0?0???0? (cc6e82749f20e6317e848fa5487488d
038894e9a^e
??[e
|????0???;0?|??0?|??0? (d0c83205e027210e317ab130f03b9a4331d03b stt_stateready
start-data서울특별시 강서구 화곡동 강서로 57sttofLOCATION37.535024,126.903671,1621674068 sttResult화곡동 347-10 이
RECORD_PPMALLOWRECORD_PPM_REQUEST
```

[그림 23] Strings 를 통한 위치 정보 획득

위에 통해 확인 가능한 GPS 검색 결과는 아래와 같다.



[그림 24] GPS 조회 결과

뿐만 아니라 서울시 화곡동 강서로 57 로 부터 화곡동 347-10 과 관련된 주소를 확인할 수 있었다. 이후에는 cache 를 분석하였다. 기 확인한 chromium-efl 를 통해 cache 는 chrome 기반의 cache 분석 도구를 사용하면 분석 가능할 것이라고 예상할 수 있다. 분석 도구로는 WEFA 를 사용하였다.

필터:	시작	필터 조건:	선택					
캐시	히스토리	쿠키	다운로드 목록	세션	검색정보	로컬파일 열함	임시인터넷파일	타일라인
브라우저	검색정보	디크립트 URL						
Google Chrome	dangsan station	https://openapi.naver.com/v1/search/local.json?query=dangsan station&display=10&start=1&sort=random	https://openapi....	2021-05-22 17:34:29	0	(Cache)		

[그림 25] 당산역 관련 웹 브라우저 캐시

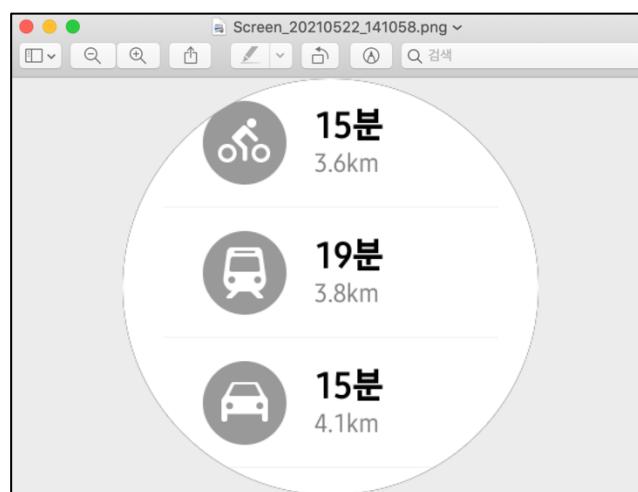
위의 GPS 로그와 유사하게 당산역과 관련된 내역을 확인하였으나 영화관과 관련된 오후 15 시 관련 로그와는 거리가 있음을 확인하였다.

https://naveropenapi.apigw.ntruss.com/map-reversegeocode/v2/gc?coords=126.84575,37.53278&orders=roadaddr,addr&output=json	https://naveropenapi.apigw.ntruss.com/map-reversegeocode/v2/gc?coords=126.84575,37.53278&orders=roadaddr,addr&output=json
http://apis.naver.com/samsung_gear_maps_directions/bicycling_web?lo=ko&st=126.84575,37.53278,na...name=서울특별시 강서구 화곡동 강서로57&destination=126.9018962,37.5341162,na...커피온리 당산역사점...	http://apis.naver.com/samsung_gear_maps_directions/bicycling_web?lo=ko&st=126.84575,37.53278,na...name=서울특별시 강서구 화곡동 강서로57&destination=126.9018962,37.5341162,na...커피온리 당산역사점...
http://apis.naver.com/samsung_gear_directions_walk/walk?&step&o=eco&l=ko&l=126.84575,37.53278,서울특별시 강서구 화곡동 강서로57;126.9018962,37.5341162,na...&msgpad=1621672491245&nd=6yFTColdVPEffs456mWculo=	http://apis.naver.com/samsung_gear_directions_walk/walk?&step&o=eco&l=ko&l=126.84575,37.53278,서울특별시 강서구 화곡동 강서로57&destination=126.9018962,37.5341162,na...&msgpad=1621672491245&nd=6yFTColdVPEffs456mWculo=
http://apis.naver.com/samsung_gearmaps/pubtrans/v2/directions/point-to-point?lang=ko&start=126.84575,37.53278&goal=126.9018962,37.5341162&mainoption=traoptimal&msgpad=1621672491245&nd=6yFTColdVPEffs456mWculo=	http://apis.naver.com/samsung_gearmaps/pubtrans/v2/directions/point-to-point?lang=ko&start=126.84575,37.53278&goal=126.9018962,37.5341162,na...&msgpad=1621672491245&nd=6yFTColdVPEffs456mWculo=
https://apis.naver.com/samsunggearnmaps/pubtrans/v2/directions/point-to-point?lang=ko&start=126.84575,37.53278,서울특별시 강서구 화곡동 강서로57&goal=126.9018962,37.5341162,커피온리 당산역사점&msgp...https://apis.naver.com/samsunggearnmaps/pubtrans/v2/directions/point-to-point?lang=ko&start=126.84575,37.53278,서울특별시 강서구 화곡동 강서로57&goal=126.9018962,37.5341162,커피온리 당산역사점&msgp...	https://apis.naver.com/samsunggearnmaps/pubtrans/v2/directions/point-to-point?lang=ko&start=126.84575,37.53278,서울특별시 강서구 화곡동 강서로57&goal=126.9018962,37.5341162,커피온리 당산역사점&msgp...https://apis.naver.com/samsunggearnmaps/pubtrans/v2/directions/point-to-point?lang=ko&start=126.84575,37.53278,서울특별시 강서구 화곡동 강서로57&goal=126.9018962,37.5341162,커피온리 당산역사점&msgp...

[그림 26] 경로 탐색 관련 로그

당산역 관련 로그는 17 시 35 분경에 까치산역 근처를 출발하여 화곡동 강서로 57를 경유하는 경로로 검색 시도한 것을 확인할 수 있다.

추가적으로, screenshot 을 통해 다음과 같은 검색 기록을 확인할 수 있다. 목표 장소는 검색 장소로 부터 15 분 내외 임을 알 수 있으며, 14 시 10 분에 캡처함을 알수 있다.



[그림 27] 목표 장소 관련 어플리케이션 캡처 파일

2) GearBrowser

NaverMaps 와 사용된 GearBrowser 과 관련된 로그는 /usr/apps/com.fin10.tizen.gearbrowser 와 /usr/home/owner/apps_rw/com.fin10.tizen.gearbrowser 에서 확인할 수 있다. 두 폴더에 존재하는 파일 내역은 실질적으로 동일하다. NaverMaps 분석할 때와 동일한 방법으로 분석을 진행하였다.

(base) sin90@odongbin-ui-MacBookPro com.fin10.tizen.gearbrowser % find . -type d sed -e "s/[^-][^\\/*]*//g" -e "s/ \\([^\]\\)/ -\\1/"
.
-cache
-shared
-data
-chromium-efl
-data
-SPP
-GPU Cache
-IndexedDB
-https://www.google.com_0.indexeddb.leveldb
-databases
-db
-Local Storage
-pref

[그림 28] GearBrowser chromium-efl 폴더 탐지

폴더 구조를 통해 확인해본 결과 chromium-efl 이라는 폴더를 확인하여 chromium 을 기반으로 동작하고 있음을 추정할 수 있다. 먼저 ./data/.pref 폴더 내에 존재하는 파일을 대상으로 strings 를 통해 아래와 같은 내역을 확인할 수 있다.

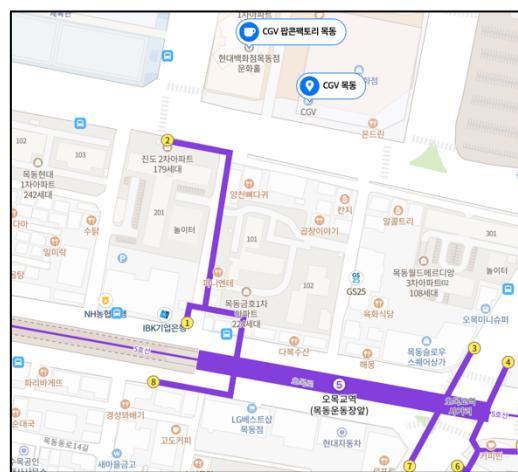
```

(base) sin90@odongbin-ui-MacBookPro .pref % pwd
/Users/sin90/Desktop/DFC_challenge/202/usr/home/owner/apps_rw/com.fin10.tizen.geabrowser/data/.pref
(base) sin90@odongbin-ui-MacBookPro .pref % cat *
pref_key_last_search_keywordTime square Cgvpref_key_search_enginehttps://www.google.com/search?q=pref_key_bookmarks[{"title":"Fast and Furious","url":"http://www.cgv.co.kr/movies/detail-view/show-times.aspx?midx=83115#menu"}]pref_key_last_urlhttps://www.google.com/maps/@37.5257627,126.8743904,15z?gl=kr
(base) sin90@odongbin-ui-MacBookPro .pref %

```

[그림 29] 영화 관련 흔적 및 GPS 정보

Time square CGV 를 검색한 흔적과, 메일 관련 흔적에서 발견하였던 Fast and Furious 와 관련된 흔적과 GPS 좌표를 확인할 수 있다. 해당 GPS 근처에 CGV 하나를 더 발견할 수 있었다.



[그림 30] GPS 정보 조회 결과

이후에는 cache 를 분석하였다. 기 확인한 chromium-efl 를 통해 cache 는 chrome 기반의 cache 분석 도구를 사용하면 분석 가능할 것이라고 예상할 수 있다. 분석 도구로는 WEFA 를 사용하였다.

검색정보								
	디코딩 URL	URL	방문시간	제목	방문횟수	타입	크기	파일명
□ Google Chrome	si eoul station	https://www.goo... https://www.goo...	2021-05-10 18:26:04		0	(Cache)		
□ Google Chrome	seoul station	https://www.goo... https://www.goo...	2021-05-10 18:26:23		0	(Cache)		
□ Google Chrome	서울역 서울특별시 용산구	https://www.goo... https://www.goo...	2021-05-10 18:26:44		0	(Cache)		
□ Google Chrome	서울역 서울특별시 용산구	https://www.goo... https://www.goo...	2021-05-10 18:26:45		0	(Cache)		
□ Google Chrome	Time square cgv	https://www.goo... https://www.goo...	2021-05-22 13:37:45		0	(Cache)		
□ Google Chrome	Time square cgv	https://www.goo... https://www.goo...	2021-05-22 13:37:49		0	(Cache)		
□ Google Chrome	Time square Cgv	https://www.goo... https://www.goo...	2021-05-22 13:44:11		0	(Cache)		
□ Google Chrome	m	https://www.goo... https://www.goo...	2021-05-22 13:51:35		0	(Cache)		
□ Google Chrome	MO	https://www.goo... https://www.goo...	2021-05-22 13:51:36		0	(Cache)		
□ Google Chrome	mok	https://www.goo... https://www.goo...	2021-05-22 13:51:37		0	(Cache)		
□ Google Chrome	mokd	https://www.goo... https://www.goo...	2021-05-22 13:51:39		0	(Cache)		
□ Google Chrome	Mokdo	https://www.goo... https://www.goo...	2021-05-22 13:51:40		0	(Cache)		
□ Google Chrome	Mokdon	https://www.goo... https://www.goo...	2021-05-22 13:51:42		0	(Cache)		
□ Google Chrome	Mokdong	https://www.goo... https://www.goo...	2021-05-22 13:51:43		0	(Cache)		
□ Google Chrome	Mokdong	https://www.goo... https://www.goo...	2021-05-22 13:51:45		0	(Cache)		
□ Google Chrome	Mokdong C	https://www.goo... https://www.goo...	2021-05-22 13:51:46		0	(Cache)		
□ Google Chrome	Mokdong [g	https://www.goo... https://www.goo...	2021-05-22 13:51:48		0	(Cache)		
□ Google Chrome	Mokdong ag	https://www.goo... https://www.goo...	2021-05-22 13:51:49		0	(Cache)		
■ Google Chrome	Mokdong	https://www.goo... https://www.goo...	2021-05-22 13:51:56		0	(Cache)		
□ Google Chrome	Mokdong C	https://www.goo... https://www.goo...	2021-05-22 13:51:57		0	(Cache)		
□ Google Chrome	Mokdong cg	https://www.goo... https://www.goo...	2021-05-22 13:51:59		0	(Cache)		
□ Google Chrome	Mokdong cgr	https://www.goo... https://www.goo...	2021-05-22 13:52:00		0	(Cache)		
□ Google Chrome	서울특별시 양천구 목동 목동동으로 CGV 8→ 목동	https://www.goo... https://www.goo...	2021-05-22 13:52:04		0	(Cache)		
□ Google Chrome	서울특별시 양천구 목동 목동동으로 257 CGV 8→ 목동	https://www.goo... https://www.goo...	2021-05-22 14:17:53		0	(Cache)		

[그림 31] GearBrowser 캐시 분석

.pref 의 문자열을 확인한 바와 유사하게 5/22 목동 CGV 와 타임스퀘어 CGV 와 관련된 검색 기록이 존재하는 것을 확인할 수 있었다. 실제 방문한 장소를 확인하기 위해 GPS 기록을 확인할 필요가 있다.

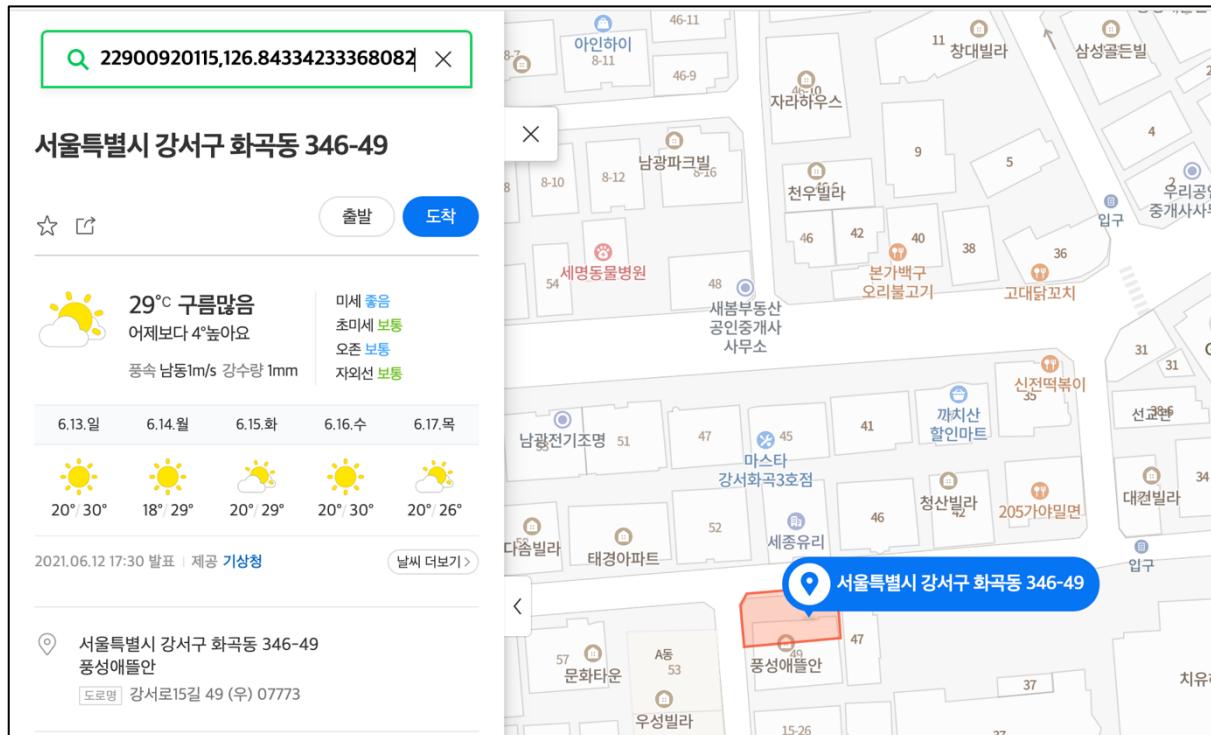
3) GPS Log

Wearable Device 에 기록된 GPS 를 살펴보기 전에 기 분석한 /usr/apps/com.samsung.runestone-gear/data/runestoneGearLog~ 에 기록된 configuration data 를 통해 아래의 정보를 확인할 수 있다.

```
2021/05/13 13:39:00:435 Connection Established(Phone requested)
2021/05/13 13:39:00:679 Received data from mobile:{"data_list":[{"configured_place_list":[{"created_by":"RUNESTONE","latitude":37.532122900920115,"longitude":126.84334233368082,"place_category":"HOME"}, {"created_by":"RUNESTONE","latitude":37.574246317400764,"longitude":126.97290587079918,"place_category":"WORK"}],"mcc":"450","service_status":1,"data_type":"configuration","timestamp":1620880741638}
2021/05/13 13:39:00:680 received configuration data from mobile
2021/05/13 13:39:00:902 service status in mobile config message = [1]
2021/05/13 13:39:00:909 parse_data_from_mobile, m_mode value[2]
```

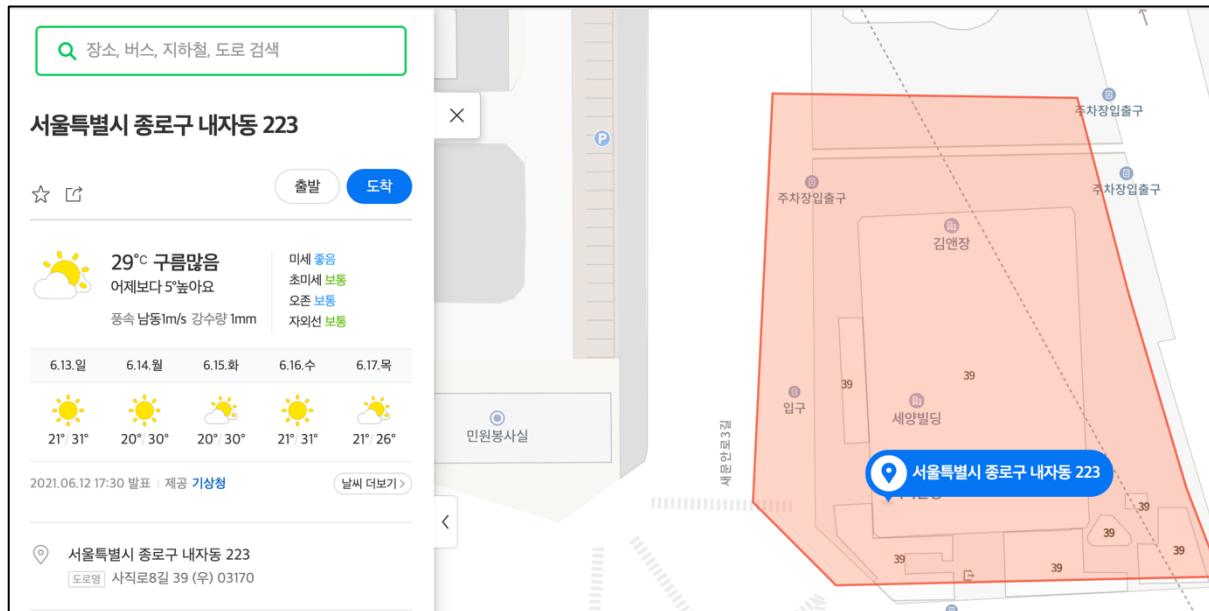
[그림 32] HOME 및 WORK 관련 GPS 정보

동기화된 데이터 상 HOME 으로 기록된 곳은 아래와 같다. 이는 Navermaps 의 .pref 에 기록된 sttResult 화곡동 347-10 과 유사한 GPS 좌표임을 확인할 수 있다.



[그림 33] GPS 정보 조회 결과 (HOME)

동기화된 데이터 상 WORK 으로 기록된 곳은 아래와 같다.



[그림 34] GPS 정보 조회 결과 (WORK)

Wearable Device 상 기록된 gps log 는 /usr/data/location/dump_gps.log, /usr/data/location/dump_gps.log.0 에서 확인할 수 있으며 다음과 같은 형식을 가지고 있다.

```
05/22 14:11:17.864 START REMOTE-GPS from [25414/GjEbuFc12C.navermapservice]
05/22 14:11:17.994 Companion-GPS state : POSITION_SEARCHING
05/22 14:11:18.090 add_reference = :1.4587
05/22 14:11:18.101 START REMOTE-WPS from [25414/GjEbuFc12C.navermapservice]
05/22 14:11:18.195 Companion-WPS state : POSITION_SEARCHING
05/22 14:11:18.387 consumer_gps_update_position_cb(3334) companion-gps pos -> FW : [0] error:-103
05/22 14:11:18.395 consumer_wps_update_position_cb(3411) companion-wps pos -> FW : [1621660277] error:-103
05/22 14:11:18.420 consumer_gps_update_position_cb(3334) companion-gps pos -> FW : [0] error:-103
05/22 14:11:18.459 consumer_wps_update_position_cb(3411) companion-wps pos -> FW : [1621660277] error:-103
05/22 14:11:35.206 Companion-WPS state : POSITION_CONNECTED
05/22 14:11:35.212 companion-wps pos -> FW : [0] - [3x.5x2x8x : 1x6.x4x2x4]
05/22 14:11:56.298 nps_set_last_position(226) update NPS last position [1621660317]
05/22 14:11:56.309 companion-wps pos -> FW : [0] - [3x.5x2x8x : 1x6.x4x2x1]
05/22 14:12:36.440 companion-wps pos -> FW : [0] - [3x.5x2x8x : 1x6.x4x2x1]
05/22 14:13:17.289 nps_set_last_position(226) update NPS last position [1621660397]
05/22 14:13:17.298 companion-wps pos -> FW : [0] - [3x.5x2x8x : 1x6.x4x2x3]
05/22 14:13:57.261 companion-wps pos -> FW : [0] - [3x.5x2x8x : 1x6.x4x2x1]
```

[그림 35] GPS 로그 구성

GPS 데이터가 일부 마스킹 되어 있음을 확인할 수 있다. 데이터 분석을 위해 grep 을 이용하여 GPS 로그가 포함된 기록만 아래와 같이 수집하였다.

```
05/18 21:55:05.595 WIFI pos -> FW : [1621342505] - [3x.5x4x6x : 1x6.x7x7x0]
05/18 22:15:03.451 WIFI pos -> FW : [1621343703] - [3x.5x4x6x : 1x6.x7x7x0]
05/18 22:35:06.887 WIFI pos -> FW : [1621344906] - [3x.5x4x5x : 1x6.x7x7x0]
05/18 22:55:06.365 WIFI pos -> FW : [1621346106] - [3x.5x4x6x : 1x6.x7x7x0]
05/18 23:14:59.007 CELL pos -> FW : [1621347299] - [3x.5x4x5x : 1x6.x7x6x0]
05/18 23:35:07.536 GPS pos -> FW : [1621348517] - [3x.5x2x0x : 1x6.x6x1x4]
05/18 23:35:07.683 CELL pos -> FW : [1621348507] - [3x.5x4x5x : 1x6.x7x6x0]
05/18 23:55:03.624 CELL pos -> FW : [1621349703] - [3x.5x4x5x : 1x6.x7x6x0]
05/19 06:14:01.861 WIFI pos -> FW : [1621372441] - [3x.5x5x4x : 1x7.x6x0x0]
05/19 15:34:33.881 CELL pos -> FW : [1621406073] - [3x.5x4x5x : 1x6.x7x6x0]
05/19 15:55:03.669 CELL pos -> FW : [1621407303] - [3x.5x4x5x : 1x6.x7x6x0]
```

[그림 36] GPS 정보 마스킹 확인

전처리 시에 GPS 오차를 고려하기 위해 마스킹된 자리를 기준으로 단계를 나누어 통계를 살펴보았다. 전처리 방법은 다음과 같다.

```

In [7]: x_coord = df[9].apply(lambda x : str(x)[1:-1])

In [8]: y_coord = df[11].apply(lambda x : str(x)[0:-1])

In [9]: x_coord_lv1 = x_coord.apply(lambda x : x[:-2])
y_coord_lv1 = y_coord.apply(lambda x : x[:-2])

In [10]: x_coord_lv2 = x_coord_lv1.apply(lambda x : x[:-2])
y_coord_lv2 = y_coord_lv1.apply(lambda x : x[:-2])

In [11]: ori_coord = x_coord + " : " + y_coord
ori_coord_level1 = x_coord_lv1 + " : " + y_coord_lv1
ori_coord_level2 = x_coord_lv2 + " : " + y_coord_lv2

```

[그림 37] 마스킹 된 영역을 기준으로 전처리

이후 Groupby 를 이용하여 아래와 같이 분석하였다.

05/10	3x.5 : 1x6.x4	2857	2857	2857	2857	2857	2857	2857	2857	2857	2857	2857	2857	2857
	3x.5 : 1x6.x5	5	5	5	5	5	5	5	5	5	5	5	5	5
	3x.5 : 1x6.x6	5	5	5	5	5	5	5	5	5	5	5	5	5
	3x.5 : 1x6.x7	556	556	556	556	556	556	556	556	556	556	556	556	556
05/11	3x.5 : 1x6.x4	5	5	5	5	5	5	5	5	5	5	5	5	5
05/12	3x.5 : 1x6.x4	4	4	4	4	4	4	4	4	4	4	4	4	4
	3x.5 : 1x6.x7	8	8	8	8	8	8	8	8	8	8	8	8	8
05/13	3x.5 : 1x6.x7	4	4	4	4	4	4	4	4	4	4	4	4	4
05/14	3x.5 : 1x6.x5	1	1	1	1	1	1	1	1	1	1	1	1	1
	3x.5 : 1x6.x7	35	35	35	35	35	35	35	35	35	35	35	35	35
	3x.5 : 1x7.x0	1	1	1	1	1	1	1	1	1	1	1	1	1
	3x.5 : 1x7.x1	1	1	1	1	1	1	1	1	1	1	1	1	1
05/15	3x.5 : 1x6.x7	22	22	22	22	22	22	22	22	22	22	22	22	22
05/16	3x.5 : 1x6.x4	5	5	5	5	5	5	5	5	5	5	5	5	5
	3x.5 : 1x6.x7	3	3	3	3	3	3	3	3	3	3	3	3	3
05/17	3x.5 : 1x6.x7	30	30	30	30	30	30	30	30	30	30	30	30	30
05/18	3x.1 : 1x6.x6	1	1	1	1	1	1	1	1	1	1	1	1	1
	3x.5 : 1x6.x6	1	1	1	1	1	1	1	1	1	1	1	1	1
	3x.5 : 1x6.x7	58	58	58	58	58	58	58	58	58	58	58	58	58
05/19	3x.4 : 1x6.x5	1	1	1	1	1	1	1	1	1	1	1	1	1
	3x.5 : 1x6.x7	20	20	20	20	20	20	20	20	20	20	20	20	20
	3x.5 : 1x7.x6	1	1	1	1	1	1	1	1	1	1	1	1	1
05/21	3x.5 : 1x6.x4	688	688	688	688	688	688	688	688	688	688	688	688	688
05/22	3x.5 : 1x6.x0	35	35	35	35	35	35	35	35	35	35	35	35	35
	3x.5 : 1x6.x4	264	264	264	264	264	264	264	264	264	264	264	264	264
	3x.5 : 1x6.x5	299	299	299	299	299	299	299	299	299	299	299	299	299
	3x.5 : 1x6.x6	248	248	248	248	248	248	248	248	248	248	248	248	248
	3x.5 : 1x6.x7	341	341	341	341	341	341	341	341	341	341	341	341	341
	3x.5 : 1x6.x9	1	1	1	1	1	1	1	1	1	1	1	1	1
05/23	3x.5 : 1x6.x4	1	1	1	1	1	1	1	1	1	1	1	1	1

[그림 38] GroupBy 적용

"3x.5 : 1x6.x4" 에서 가장 많은 로그가 존재하고 있음을 확인 가능하며 이는 실제 HOME GPS 좌표에 해당 하는 값이다. 이후 5/22 일에 해당하는 로그만 확인하기 위해 아래와 같이 처리하였다.

In [21]:	df_522 = df[df[0] == '05/22']																																																																																																																																																																																																	
In [31]:	df_522																																																																																																																																																																																																	
Out[31]:	<table border="1"> <thead> <tr> <th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>cord</th><th>cord1</th><th>cord2</th><th>hours</th><th>minutes</th></tr> </thead> <tbody> <tr><td>718</td><td>05/22</td><td>13:47:41.179</td><td>companion-wps</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[0]</td><td>-</td><td>[3x.5x2x8x : 1x6.x4x2x9]</td><td>3x.5x2x8 : 1x6.x4x2x9</td><td>3x.5x2x2 : 1x6.x4x2</td><td>3x.5 : 1x6.x4</td><td>13</td><td>47</td></tr> <tr><td>719</td><td>05/22</td><td>14:10:40.924</td><td>companion-wps</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[0]</td><td>-</td><td>[3x.5x2x8x : 1x6.x4x2x4]</td><td>3x.5x2x8 : 1x6.x4x2x4</td><td>3x.5x2x2 : 1x6.x4x2</td><td>3x.5 : 1x6.x4</td><td>14</td><td>10</td></tr> <tr><td>720</td><td>05/22</td><td>14:11:16.349</td><td>companion-wps</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[0]</td><td>-</td><td>[3x.5x2x8x : 1x6.x4x2x4]</td><td>3x.5x2x8 : 1x6.x4x2x4</td><td>3x.5x2x2 : 1x6.x4x2</td><td>3x.5 : 1x6.x4</td><td>14</td><td>11</td></tr> <tr><td>721</td><td>05/22</td><td>14:11:35.212</td><td>companion-wps</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[0]</td><td>-</td><td>[3x.5x2x8x : 1x6.x4x2x4]</td><td>3x.5x2x8 : 1x6.x4x2x4</td><td>3x.5x2x2 : 1x6.x4x2</td><td>3x.5 : 1x6.x4</td><td>14</td><td>11</td></tr> <tr><td>722</td><td>05/22</td><td>14:11:56.309</td><td>companion-wps</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[0]</td><td>-</td><td>[3x.5x2x8x : 1x6.x4x2x1]</td><td>3x.5x2x8 : 1x6.x4x2x1</td><td>3x.5x2x2 : 1x6.x4x2</td><td>3x.5 : 1x6.x4</td><td>14</td><td>11</td></tr> <tr><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td><td>...</td></tr> <tr><td>1901</td><td>05/22</td><td>22:15:07.642</td><td>GPS</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[1621689307]</td><td>-</td><td>[3x.5x6x1x : 1x6.x0x5x5]</td><td>3x.5x6x1 : 1x6.x0x5x5</td><td>3x.5x6 : 1x6.x0x5</td><td>3x.5 : 1x6.x0</td><td>22</td><td>15</td></tr> <tr><td>1902</td><td>05/22</td><td>22:35:07.640</td><td>GPS</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[1621690507]</td><td>-</td><td>[3x.5x7x7x : 1x6.x0x0x3]</td><td>3x.5x7x7 : 1x6.x0x0x3</td><td>3x.5x7x : 1x6.x0x0</td><td>3x.5 : 1x6.x0</td><td>22</td><td>35</td></tr> <tr><td>1903</td><td>05/22</td><td>22:55:03.500</td><td>GPS</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[1621691703]</td><td>-</td><td>[3x.5x7x8x : 1x6.x0x1x1]</td><td>3x.5x7x8 : 1x6.x0x1x1</td><td>3x.5x7x7 : 1x6.x0x1x1</td><td>3x.5x7 : 1x6.x0x1</td><td>22</td><td>55</td></tr> <tr><td>1904</td><td>05/22</td><td>23:15:03.642</td><td>WIFI</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[1621692903]</td><td>-</td><td>[3x.5x5x7x : 1x6.x0x1x0]</td><td>3x.5x5x7 : 1x6.x0x1x0</td><td>3x.5x5x6 : 1x6.x0x1x0</td><td>3x.5x5 : 1x6.x0</td><td>23</td><td>15</td></tr> <tr><td>1905</td><td>05/22</td><td>23:54:01.507</td><td>WIFI</td><td>pos</td><td>-></td><td>FW</td><td>:</td><td>[1621695241]</td><td>-</td><td>[3x.5x2x6x : 1x6.x4x1x0]</td><td>3x.5x2x6 : 1x6.x4x1x0</td><td>3x.5x2x5 : 1x6.x4x1</td><td>3x.5 : 1x6.x4</td><td>23</td><td>54</td></tr> </tbody> </table>	0	1	2	3	4	5	6	7	8	9	10	11	cord	cord1	cord2	hours	minutes	718	05/22	13:47:41.179	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x9]	3x.5x2x8 : 1x6.x4x2x9	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	13	47	719	05/22	14:10:40.924	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x4]	3x.5x2x8 : 1x6.x4x2x4	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	14	10	720	05/22	14:11:16.349	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x4]	3x.5x2x8 : 1x6.x4x2x4	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	14	11	721	05/22	14:11:35.212	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x4]	3x.5x2x8 : 1x6.x4x2x4	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	14	11	722	05/22	14:11:56.309	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x1]	3x.5x2x8 : 1x6.x4x2x1	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	14	11	1901	05/22	22:15:07.642	GPS	pos	->	FW	:	[1621689307]	-	[3x.5x6x1x : 1x6.x0x5x5]	3x.5x6x1 : 1x6.x0x5x5	3x.5x6 : 1x6.x0x5	3x.5 : 1x6.x0	22	15	1902	05/22	22:35:07.640	GPS	pos	->	FW	:	[1621690507]	-	[3x.5x7x7x : 1x6.x0x0x3]	3x.5x7x7 : 1x6.x0x0x3	3x.5x7x : 1x6.x0x0	3x.5 : 1x6.x0	22	35	1903	05/22	22:55:03.500	GPS	pos	->	FW	:	[1621691703]	-	[3x.5x7x8x : 1x6.x0x1x1]	3x.5x7x8 : 1x6.x0x1x1	3x.5x7x7 : 1x6.x0x1x1	3x.5x7 : 1x6.x0x1	22	55	1904	05/22	23:15:03.642	WIFI	pos	->	FW	:	[1621692903]	-	[3x.5x5x7x : 1x6.x0x1x0]	3x.5x5x7 : 1x6.x0x1x0	3x.5x5x6 : 1x6.x0x1x0	3x.5x5 : 1x6.x0	23	15	1905	05/22	23:54:01.507	WIFI	pos	->	FW	:	[1621695241]	-	[3x.5x2x6x : 1x6.x4x1x0]	3x.5x2x6 : 1x6.x4x1x0	3x.5x2x5 : 1x6.x4x1	3x.5 : 1x6.x4	23	54
0	1	2	3	4	5	6	7	8	9	10	11	cord	cord1	cord2	hours	minutes																																																																																																																																																																																		
718	05/22	13:47:41.179	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x9]	3x.5x2x8 : 1x6.x4x2x9	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	13	47																																																																																																																																																																																			
719	05/22	14:10:40.924	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x4]	3x.5x2x8 : 1x6.x4x2x4	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	14	10																																																																																																																																																																																			
720	05/22	14:11:16.349	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x4]	3x.5x2x8 : 1x6.x4x2x4	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	14	11																																																																																																																																																																																			
721	05/22	14:11:35.212	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x4]	3x.5x2x8 : 1x6.x4x2x4	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	14	11																																																																																																																																																																																			
722	05/22	14:11:56.309	companion-wps	pos	->	FW	:	[0]	-	[3x.5x2x8x : 1x6.x4x2x1]	3x.5x2x8 : 1x6.x4x2x1	3x.5x2x2 : 1x6.x4x2	3x.5 : 1x6.x4	14	11																																																																																																																																																																																			
...																																																																																																																																																																																			
1901	05/22	22:15:07.642	GPS	pos	->	FW	:	[1621689307]	-	[3x.5x6x1x : 1x6.x0x5x5]	3x.5x6x1 : 1x6.x0x5x5	3x.5x6 : 1x6.x0x5	3x.5 : 1x6.x0	22	15																																																																																																																																																																																			
1902	05/22	22:35:07.640	GPS	pos	->	FW	:	[1621690507]	-	[3x.5x7x7x : 1x6.x0x0x3]	3x.5x7x7 : 1x6.x0x0x3	3x.5x7x : 1x6.x0x0	3x.5 : 1x6.x0	22	35																																																																																																																																																																																			
1903	05/22	22:55:03.500	GPS	pos	->	FW	:	[1621691703]	-	[3x.5x7x8x : 1x6.x0x1x1]	3x.5x7x8 : 1x6.x0x1x1	3x.5x7x7 : 1x6.x0x1x1	3x.5x7 : 1x6.x0x1	22	55																																																																																																																																																																																			
1904	05/22	23:15:03.642	WIFI	pos	->	FW	:	[1621692903]	-	[3x.5x5x7x : 1x6.x0x1x0]	3x.5x5x7 : 1x6.x0x1x0	3x.5x5x6 : 1x6.x0x1x0	3x.5x5 : 1x6.x0	23	15																																																																																																																																																																																			
1905	05/22	23:54:01.507	WIFI	pos	->	FW	:	[1621695241]	-	[3x.5x2x6x : 1x6.x4x1x0]	3x.5x2x6 : 1x6.x4x1x0	3x.5x2x5 : 1x6.x4x1	3x.5 : 1x6.x4	23	54																																																																																																																																																																																			

1188 rows x 17 columns

[그림 39] 05/22 일의 로그로 필터링

특히 14 시 이후부터 15 시 이전에 영화관으로 이동했을 거라 추정되는 시간에 companion-gps, companion-wps 와 관련된 로그가 많이 발생한 것을 확인할 수 있다. 분별로 이동 경로를 확인해보면 다음과 같다.

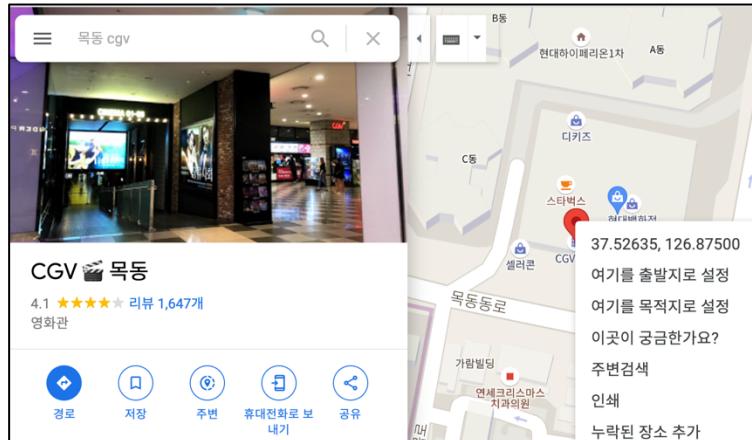
23	3x.5 : 1x6.x4	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
24	3x.5 : 1x6.x4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
25	3x.5 : 1x6.x4	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30
26	3x.5 : 1x6.x4	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
27	3x.5 : 1x6.x4	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
28	3x.5 : 1x6.x4	36	36	36	36	36	36	36	36	36	36	36	36	36	36	36
	3x.5 : 1x6.x5	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24
29	3x.5 : 1x6.x5	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
30	3x.5 : 1x6.x5	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
31	3x.5 : 1x6.x5	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
32	3x.5 : 1x6.x5	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
33	3x.5 : 1x6.x5	35	35	35	35	35	35	35	35	35	35	35	35	35	35	35
	3x.5 : 1x6.x6	25	25	25	25	25	25	25	25	25	25	25	25	25	25	25
34	3x.5 : 1x6.x6	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
35	3x.5 : 1x6.x6	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
36	3x.5 : 1x6.x6	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
37	3x.5 : 1x6.x6	43	43	43	43	43	43	43	43	43	43	43	43	43	43	43
	3x.5 : 1x6.x7	17	17	17	17	17	17	17	17	17	17	17	17	17	17	17
38	3x.5 : 1x6.x7	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
39	3x.5 : 1x6.x7	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
40	3x.5 : 1x6.x7	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
41	3x.5 : 1x6.x7	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
42	3x.5 : 1x6.x7	60	60	60	60	60	60	60	60	60	60	60	60	60	60	60
43	3x.5 : 1x6.x7	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24

[그림 40] 나열된 GPS 정보

41	3x.5x5 : 1x6.x7x0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3x.5x5 : 1x6.x7x1	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	3x.5x5 : 1x6.x7x2	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13	13
	3x.5x5 : 1x6.x7x3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	3x.5x5 : 1x6.x7x4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	3x.5x5 : 1x6.x7x5	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	3x.5x5 : 1x6.x7x6	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	3x.5x5 : 1x6.x7x7	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	3x.5x5 : 1x6.x7x8	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	3x.5x5 : 1x6.x7x9	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	3x.5x6 : 1x6.x7x0	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
	3x.5x6 : 1x6.x7x1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	3x.5x6 : 1x6.x7x2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	3x.5x6 : 1x6.x7x9	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
42	3x.5x6 : 1x6.x7x0	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14	14
	3x.5x6 : 1x6.x7x1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
	3x.5x6 : 1x6.x7x9	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
	3x.5x7 : 1x6.x7x1	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
	3x.5x7 : 1x6.x7x2	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9	9
	3x.5x7 : 1x6.x7x3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3x.5x8 : 1x6.x7x3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	3x.5x8 : 1x6.x7x4	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7	7
	3x.5x8 : 1x6.x7x5	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
	3x.5x9 : 1x6.x7x5	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	3x.5x9 : 1x6.x7x6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6	6
	3x.5x9 : 1x6.x7x7	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
43	3x.5x9 : 1x6.x7x7	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24	24

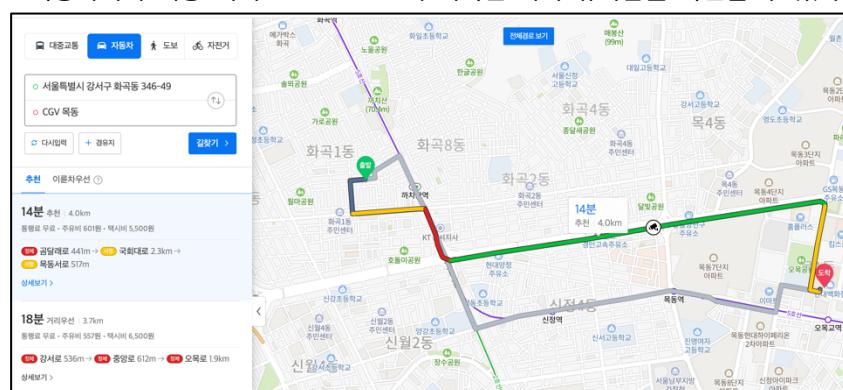
[그림 41] 나열된 GPS 정보

GPS 오차 및 위 검색 기록 및 이메일 로그를 확인한 결과 위 GPS 로그와 가장 관련 높은 곳은 목동 CGV 임을 확인할 수 있다.



[그림 42] GPS 정보에 기반한 영화관 위치

HOME에서 CGV 목동까지의 이동 역시 Screenshot에 기록된 바와 유사함을 확인할 수 있다.



[그림 43] 정보에 기반한 경로 비교

- 추가적인 장소에 방문한 기록이 있는지

위의 GPS 로그에 따르면, Alice는 14 시 40 분 경 부터 15 시 전까지 집에서 CGV로 이동했음을 확인하였다. 이후 NaverMaps 상 기록된 ‘당산역’ 관련 로그를 확인하기 위해 추가 분석을 진행하였다. /usr/data/snlp/snlp_dump에는 wifi 연결과 관련된 로그를 확인할 수 있다. 특히 wifi 검색과 관련된 검색된 AP 목록들을 나타내고 있어 이를 통해 현재 장소를 유추할 수 있다. 5/22와 관련되며 장소 유추가 가능한 로그는 아래와 같다.

```
:05-22 20:55:01.619+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] 00:07:89:81:3f:2a [-70] [KT_GiGA_2G_참새방앗간]
:05-22 20:55:01.619+0900 5150 5150 __snlp_get_wifi_list(1714) > [01] d8:0d:17:ff:89:82 [-79] [TP-Link_8982]
:05-22 20:55:05.030+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] 00:07:89:81:3f:2a [-75] [KT_GiGA_2G_참새방앗간]
:05-22 20:55:05.030+0900 5150 5150 __snlp_get_wifi_list(1714) > [01] d8:0d:17:ff:89:82 [-80] [TP-Link_8982]
:05-22 21:15:01.730+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] 00:07:89:81:3f:2a [-63] [KT_GiGA_2G_참새방앗간]
:05-22 21:15:01.730+0900 5150 5150 __snlp_get_wifi_list(1714) > [01] d8:0d:17:ff:89:82 [-81] [TP-Link_8982]
:05-22 21:15:01.730+0900 5150 5150 __snlp_get_wifi_list(1714) > [02] 88:3c:1c:a1:59:1c [-89] [U+Net591D]
:05-22 21:15:01.730+0900 5150 5150 __snlp_get_wifi_list(1714) > [03] b4:a9:4f:88:ad:3b [-91] [U+NetAD3C]
:05-22 21:15:05.523+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] 00:07:89:81:3f:2a [-62] [KT_GiGA_2G_참새방앗간]
:05-22 21:15:05.524+0900 5150 5150 __snlp_get_wifi_list(1714) > [01] d8:0d:17:ff:89:82 [-80] [TP-Link_8982]
:05-22 21:15:05.524+0900 5150 5150 __snlp_get_wifi_list(1714) > [02] 88:3c:1c:a1:59:1c [-91] [U+Net591D]
:05-22 21:15:05.524+0900 5150 5150 __snlp_get_wifi_list(1714) > [03] b4:a9:4f:88:ad:3b [-90] [U+NetAD3C]
:05-22 21:15:05.524+0900 5150 5150 __snlp_get_wifi_list(1714) > [04] 90:9f:33:b3:10:16 [-93] [hyojin]
:05-22 21:34:12.779+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] 00:07:89:81:3f:2a [-52] [KT_GiGA_2G_참새방앗간]
:05-22 21:34:12.779+0900 5150 5150 __snlp_get_wifi_list(1714) > [01] d8:0d:17:ff:89:82 [-74] [TP-Link_8982]
:05-22 21:34:12.780+0900 5150 5150 __snlp_get_wifi_list(1714) > [02] 88:36:6c:63:0c:1e [-93] [gzonetop]
:05-22 21:34:12.780+0900 5150 5150 __snlp_get_wifi_list(1714) > [03] 64:e5:99:82:c9:b4 [-93] [Iptime]
:05-22 21:34:16.037+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] 00:07:89:81:3f:2a [-69] [KT_GiGA_2G_참새방앗간]
```

[그림 44] 참새방앗간 관련 로그

‘참새방앗간’의 로그를 확인할 수 있으며 이는 Navermaps의 .pref 데이터를 통해 확인 가능하다.

```

05-22 17:34:46.595+0900 742 742 __snlp_get_wifi_list(1714) > [00] 12:63:40:15:b2:4e [-37][Galaxy Note10 5G3897]
05-22 17:34:46.595+0900 742 742 __snlp_get_wifi_list(1714) > [01] 0a:5d:dd:d6:d0:70 [-73][KT_GiGA_5G_D06C]
05-22 17:34:46.596+0900 742 742 __snlp_get_wifi_list(1714) > [02] 08:5d:dd:d6:d0:70 [-75][KT_GiGA_2G_D06C]
05-22 17:34:46.596+0900 742 742 __snlp_get_wifi_list(1714) > [03] 42:09:a5:03:9a:c6 [-71][미카도스시_2.4G]
05-22 17:34:46.596+0900 742 742 __snlp_get_wifi_list(1714) > [04] 08:5d:dd:80:26:42 [-73][olleh_WiFi_263E]
05-22 17:34:46.596+0900 742 742 __snlp_get_wifi_list(1714) > [05] 18:c5:01:cd:0e:d6 [-76][U+Net0ED4]
05-22 17:34:46.596+0900 742 742 __snlp_get_wifi_list(1714) > [06] 08:5d:dd:af:62:df [-78][U+Net62E0]
05-22 17:34:46.602+0900 742 742 __snlp_get_wifi_list(1714) > [07] 0a:5d:dd:af:62:df [-78][U+zone]
05-22 17:34:46.602+0900 742 742 __snlp_get_wifi_list(1714) > [08] 00:07:89:39:6b:33 [-78][DON_O-YA]
05-22 17:34:46.602+0900 742 742 __snlp_get_wifi_list(1714) > [09] 16:65:ee:bd:6e:72 [-81][Test]
05-22 17:34:46.602+0900 742 742 __snlp_get_wifi_list(1714) > [10] b4:a9:4f:55:82:91 [-85][KT_GiGA_2G_Wave2_828D]
05-22 17:34:46.602+0900 742 742 __snlp_get_wifi_list(1714) > [11] b4:a9:4f:5d:bc:0e [-85][KT_GiGA_2G_Wave2_BC0A]
05-22 17:34:46.602+0900 742 742 __snlp_get_wifi_list(1714) > [12] 90:9f:33:6a:12:2a [-85][zz978900]
05-22 17:34:46.602+0900 742 742 __snlp_get_wifi_list(1714) > [13] 70:5d:cc:e1:36:b6 [-87][youngdang]
05-22 17:34:46.603+0900 742 742 __snlp_get_wifi_list(1714) > [14] 88:3c:1c:c4:4d:1b [-88][kkachisan_2G]

```

[그림 45] 까치산역 관련 로그

17 시 34 분 근처에는 까치산역 근처를 지나고 있음을 추정할 수 있다. 하지만 Masking 된 GPS 로는 검증을 하기는 부족하다. 이외에도 sinsung tech 와 ministop 등의 WIFI AP 를 확인하였으나, 실 위치는 어디인지 확인하지 못하였다.

```

05-22 22:35:01.711+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] d0:be:2c:22:1c:ff [-68][Sinsung_Tech]
05-22 22:35:01.712+0900 5150 5150 __snlp_get_wifi_list(1714) > [01] 02:d3:a9:94:c0:4b [-88][MINISTOPGUEST]
05-22 22:35:04.839+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] d0:be:2c:22:1c:ff [-61][Sinsung_Tech]
05-22 22:35:04.839+0900 5150 5150 __snlp_get_wifi_list(1714) > [01] 02:d3:a9:94:c0:4b [-88][MINISTOPGUEST]
05-22 22:35:04.839+0900 5150 5150 __snlp_get_wifi_list(1714) > [02] 00:07:89:84:24:1d [-85][KT_GiGA_2G_Wave2_241A]
05-22 22:35:04.839+0900 5150 5150 __snlp_get_wifi_list(1714) > [03] 90:9f:33:d2:98:f2 [-89][iptime]
05-22 22:35:07.827+0900 5150 5150 __snlp_get_wifi_list(1714) > [00] d0:be:2c:22:1c:ff [-62][Sinsung_Tech]
05-22 22:35:07.827+0900 5150 5150 __snlp_get_wifi_list(1714) > [01] 02:d3:a9:94:c0:4b [-81][MINISTOPGUEST]

```

[그림 46] sinsung tech 및 ministop 관련 로그

아래의 로그 역시 당산역 근처로 확인된다 (navermaps 검색어, iibi, 부산포)

```

:05-22 23:15:02.118+0900 5150 5150 __snlp_get_wifi_list(1714) > [13] c8:3a:35:34:2b:d0 [-80][부산포]
:05-22 23:15:02.118+0900 5150 5150 __snlp_get_wifi_list(1714) > [14] 02:06:ac:80:1c:02 [-80][U+zone]
:05-22 23:15:02.118+0900 5150 5150 __snlp_get_wifi_list(1714) > [15] 88:36:6c:1b:7e:0e [-80][SY]
:05-22 23:15:02.118+0900 5150 5150 __snlp_get_wifi_list(1714) > [16] 22:06:ac:80:1c:0e [-82][U+Wifi]
:05-22 23:15:02.118+0900 5150 5150 __snlp_get_wifi_list(1714) > [17] 72:5d:cc:c0:d9:34 [-82][iibi-7F-2,4G]
:05-22 23:15:02.118+0900 5150 5150 __snlp_get_wifi_list(1714) > [18] 72:5d:cc:ce:51:e0 [-83][JHkorea]
:05-22 23:15:02.118+0900 5150 5150 __snlp_get_wifi_list(1714) > [19] 72:5d:cc:ce:3b:b8 [-83][iibi 4F-1]
:05-22 23:15:02.118+0900 5150 5150 __snlp_get_wifi_list(1714) > [20] 00:27:1c:ea:a4:e0 [-84][U+zone]
:05-22 23:15:02.119+0900 5150 5150 __snlp_get_wifi_list(1714) > [21] 88:36:6c:63:3b:fe [-85][iptime]
:05-22 23:15:02.119+0900 5150 5150 __snlp_get_wifi_list(1714) > [22] 1c:ec:72:04:69:32 [-86][KT_GiGA_692F]
:05-22 23:15:02.119+0900 5150 5150 __snlp_get_wifi_list(1714) > [23] 70:5d:cc:8a:17:62 [-86][pharmtaxiptime]
:05-22 23:15:02.119+0900 5150 5150 __snlp_get_wifi_list(1714) > [24] 02:e3:c7:09:0e:ba [-87][T_wifi_zone_secure]
:05-22 23:15:02.119+0900 5150 5150 __snlp_get_wifi_list(1714) > [25] 60:29:d5:11:9e:f4 [-88][KT_GiGA_2G_Wave2_9EF0]
:05-22 23:15:02.119+0900 5150 5150 __snlp_get_wifi_list(1714) > [26] 18:c5:01:df:c6:ca [-88][PHOIBOS_2.4G]
:05-22 23:15:02.119+0900 5150 5150 __snlp_get_wifi_list(1714) > [27] fc:3f:db:76:40:e5 [-89][HP-Print-E5-Officejet]

```

[그림 47] 당산역 관련 로그

관련 내역들을 종합하면 아래와 같다.

- 14시 경 : 집 → 목동 CGV (by GPS, Gear Browser 검색 내역)
- 17시 30분 경 : 까치산역 (by WIFI 검색 내역, Navermaps 검색 내역)
- 21시~21시 30분 경 : 당산역 까치방앗간 근처 (by WIFI 검색, Navermaps 검색 내역)
- 22시 35분 경 : sinsung_tech, ministop 근처 (세부 장소 확인 불가)
- 23시 15분 경 : 당산역 근처 (by WIFI 검색)