151 – Android Live

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun HA, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.com

Instructions

Description Analyze provided Android live acquisition data and answer questions.

Target	Hash (MD5)
SM-F721N_Live.zip	F2F4D387879E2CAF854DB8247C6D421B

Questions

1) What are the user's Google, YouTube, and Instagram account names? (30 points)
2) What is the SSID and location (latitude, longitude coordinates) of the wireless network to which the evidence smartphone is connected? (30 points)
3) Which photos taken with a smartphone have an edited EXIF timestamp? (30 points)
4) Which photos uploaded to Instagram were not taken on the evidence smartphone? (30 points)
5) What smartphone were the photo files found in question 4 taken on? (30 points)

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:	ExiftoolGUI	**Publisher:**	Bogdan Hrastnik
Version:	5.16.0.0		
URL:	https://exiftool.org/forum/index.php?topic=2750.0		

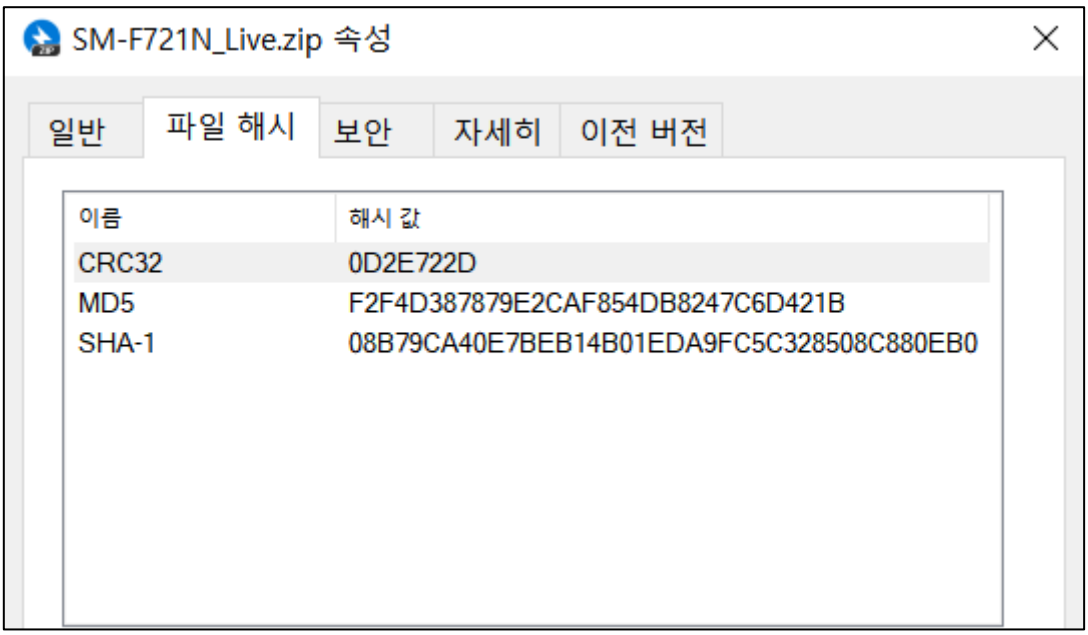
Name:	DB Browser for SQLite	**Publisher:**	sqlitebrowser
Version:	3.12.2		
URL:	https://sqlitebrowser.org/		

Name:	vscode	**Publisher:**	Microsoft
Version:	1.79.2		
URL:	https://code.visualstudio.com/download		

Name:	HashTab	**Publisher:**	Microsoft
Version:	6.0.0		
URL:	https://implbits.com		

Name:	HxD	**Publisher:**	Maël Hörz
Version:	2.5.0.0		
URL:	https://www.mh-nexus.de		

Step-by-step methodology:



[그림 1] 수집된 증거 파일의 해시 값 확인

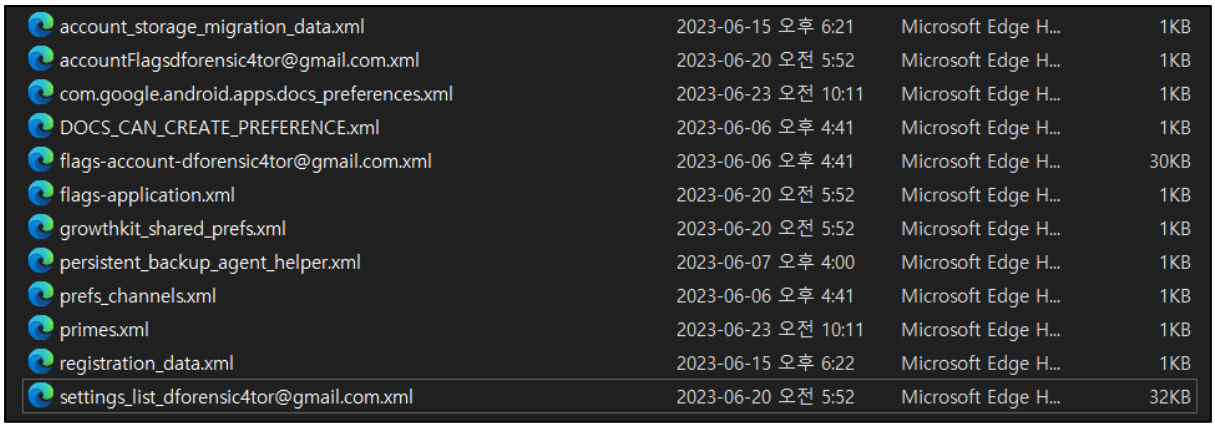
분석에 앞서, 수집된 증거 파일의 해시 값을 산출하여 MD5 해시 값이 일치함을 확인하였습니다.

1) What are the user's Google, YouTube, and Instagram account names? (30 points)

안드로이드 기기 SM-F721N모델에서 사용자의 Google, YouTube, 그리고 Instagram 계정을 찾기 위해서 data 폴더 내 존재하는 관련 파일들을 분석하였습니다.

- **Google 계정정보**

SM-F721N_Live\data\com.google.android.apps.docs\shared_prefs 경로에 존재하는 xml 파일을 통해 바로 확인할 수 있습니다.

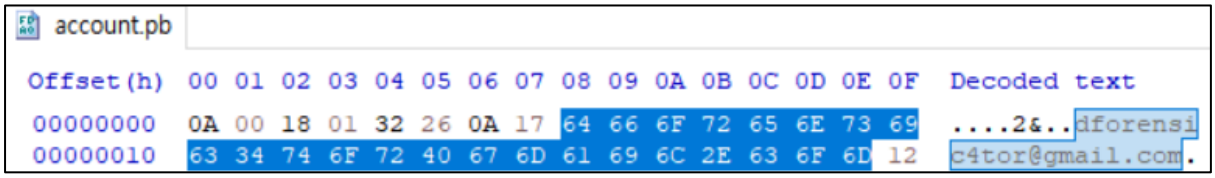


[그림 2] Google account 식별

이를 통해 해당 기기에서 Google을 사용하던 사용자의 Google 계정은 **dforensic4tor@gmail.com**이라는 사실을 확인하였습니다.

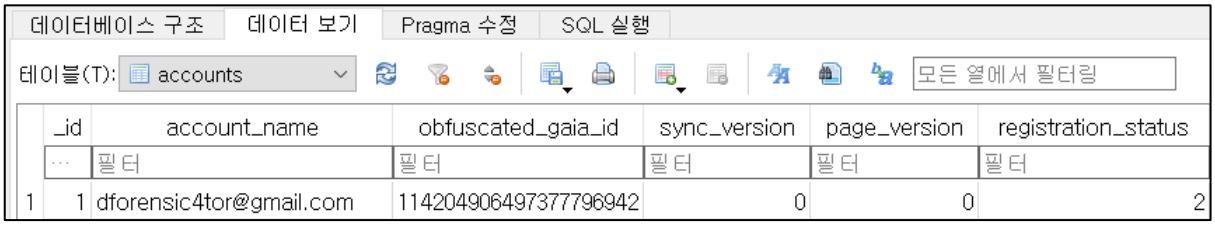
- **Youtube 계정정보**

SM-F721N_Live\data\com.google.android.youtube\files\account\shared 폴더 내에 존재하는 account.pb 파일에서 HxD 도구를 통해 다음과 같이 발견할 수 있었습니다.



[그림 3] account.pb 파일 내 Youtube 계정 식별

또한, SM-F721N_Live\data\com.google.android.youtube\databases 경로에서 accounts.notifications.db 파일을 통해 교차 검증을 수행할 수 있었습니다.

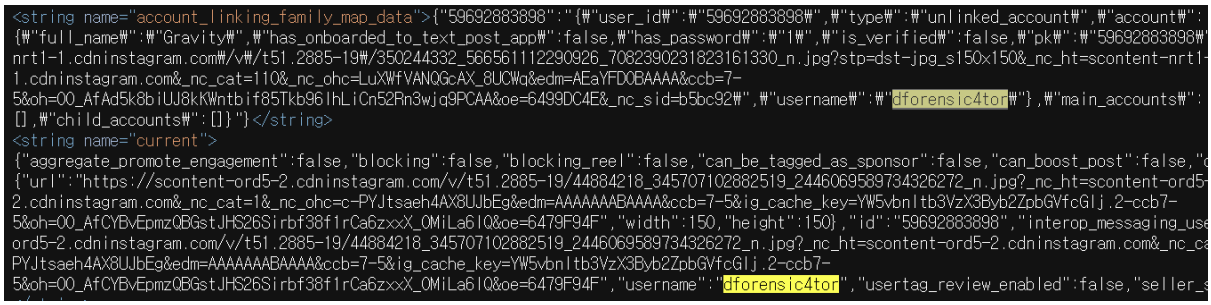


[그림 4] accounts.notifications.db 파일 내 Youtube 계정 식별

이를 통해, 사용자의 Youtube 계정은 Google 계정과 동일하게 **dforensic4tor@gmail.com**임을 확인하였습니다.

- **Instagram 계정**

사용자의 instagram 계정은 SM-F721N_Live\data\com.instagram.android\shared_prefs 폴더 내에 존재하는 com.instagram.android_preferences.xml 파일에서 다음의 그림과 같이 확인하였습니다.



[그림 5] com.instagram.android_preferences.xml 파일 내 사용자 계정 식별

이를 통해 instagram 계정은 **dforensic4tor**임을 확인하였습니다.

따라서 사용자가 증거 디지털 기기에서 사용한 Google, YouTube, Instagram 계정은 다음과 같습니다.

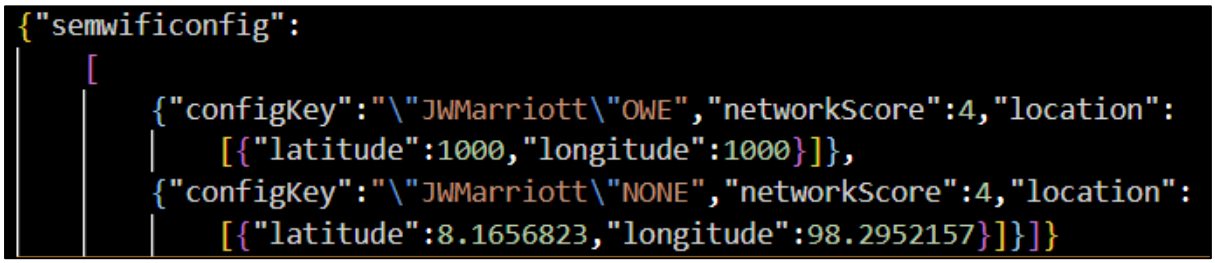
[표 1] user's Google, YouTube, and Instagram account name list

Application	Account name
Google	dforensic4tor@gmail.com
YouTube	dforensic4tor@gmail.com
Instagram	dforensic4tor

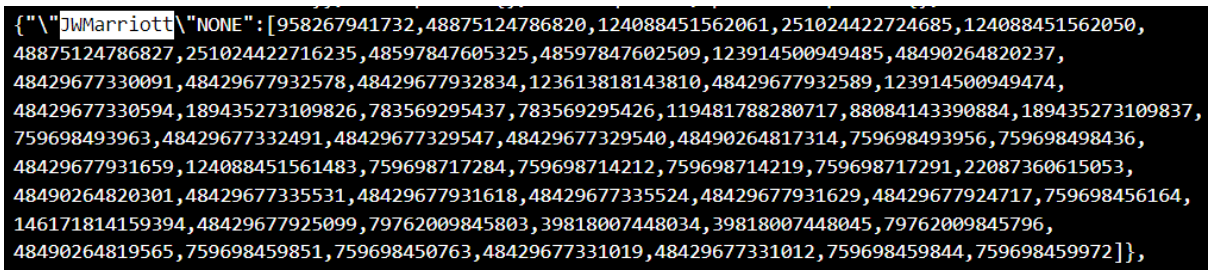
2) What is the SSID and location (latitude, longitude coordinates) of the wireless network to which the evidence smartphone is connected? (30 points)

증거 스마트폰에서 연결되었던 무선 네트워크의 SSID와 위치 정보는 다음의 경로에서 확인할 수 있습니다.

- **path : SM-F721N_Live\data_backup\ABR\WIFICONFIG\semconfigurations.json**
- **path : SM-F721N_Live\data_backup\ABR\WIFICONFIG\qtables.json**



[그림 6] semwificonfig.json 파일 내 wifi 구성 및 설정 정보 식별



[그림 7] qtables.json 파일 내 wifi 연결 정보 식별

semwificonfig.json 파일에서 확인 가능한 JWMarriott wifi 중에서 qtables.json 파일에서 연결되었던 확인 가능한 wifi는 OWE(Opportunistic Wireless Encryption)가 아닌 NONE이었습니다.

따라서, 증거 스마트폰에 연결되었던 무선 네트워크의 SSID와 위치 정보는 다음과 같습니다.

[표 2] WiFi SSID and location information which connected with evidence smartphone

SSID	latitude	longitude
JWMarriott	8.1656823	98.2952157

3) Which photos taken with a smartphone have an edited EXIF timestamp? (30 points)

스마트폰으로 촬영된 사진들은 SM-F721N_Live\media\DCIM\Camera 경로에서 확인하였습니다. 사진들은 ExifToolGUI 도구를 통해 EXIF timestamp metadata를 식별하였습니다.

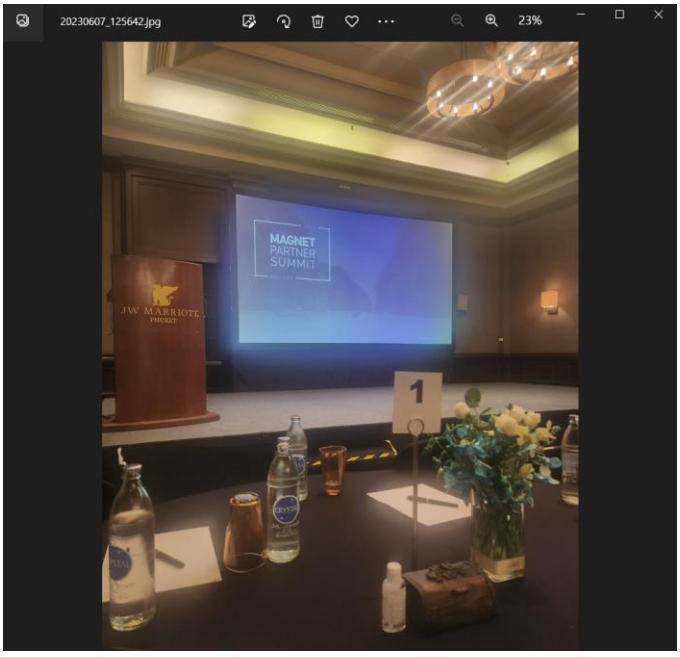
이 중, 단 하나의 사진을 제외하고 ExifIFD의 DateTimeOriginal, CreateDate metadata와 IFD0의 ModifyDate metadata가 모두 일치했습니다.

일치하지 않는 20230607_125642.jpg의 EXIF timestamp metadata는 다음과 같습니다.

[표 3] 20230607_125642.jpg의 EXIF timestamp metadata 정보

Tag Name	Value
IFD0 – ModifyDate	2023.06.06 12:56:00
ExifIFD – DateTimeOriginal	2023.06.06 12:56:00
ExifIFD – CreateDate	2023.06.07 12:56:42

일반적으로 파일의 생성 시각은 변경 시각보다 빠른 경우가 일반적이지만, 해당 케이스는 변경 시각이 생성 시각보다 빠르기 때문에 수정된 EXIF timestamp metadata라고 판단하였습니다. 따라서, 해당 문제의 답은 **20230607_125642.jpg** 로 판단하였습니다.

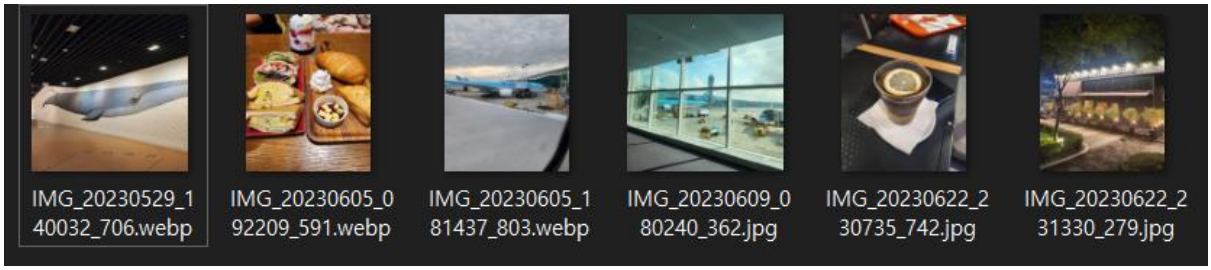


[그림 8] 20230607_125642 파일 확인

4) Which photos uploaded to Instagram were not taken on the evidence smartphone? (30 points)

인스타그램에 업로드 된 사진이 저장되는 아티팩트 경로는 다음과 같습니다.

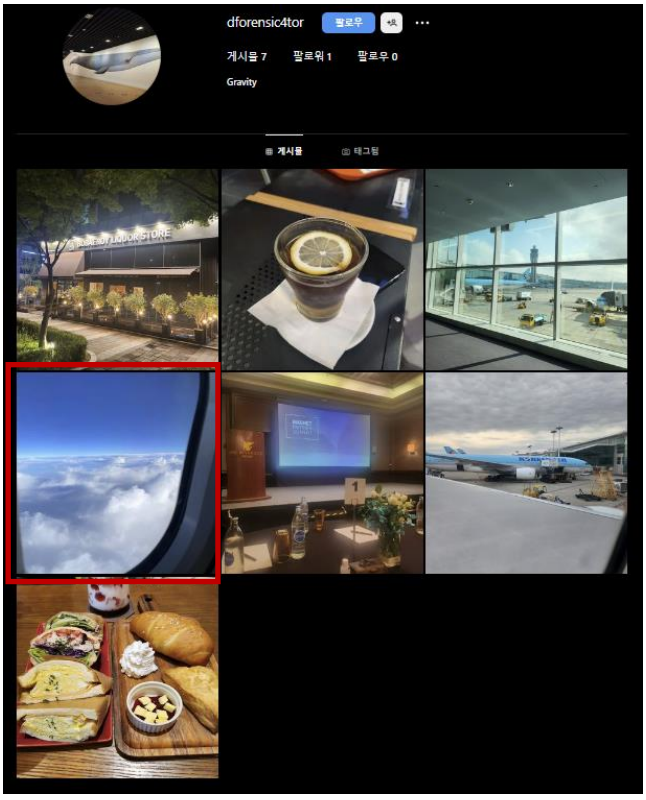
- **path : SM-F721N_Live\media\Pictures\Instagram**



[그림 9] 인스타그램에 업로드 된 사진

하지만, 해당 업로드 사진들에 대한 원본 사진이 저장된 DCIM 폴더에서 exiftoolgui 도구로 살펴보았을 때, 증거 스마트폰 기기 모델인 SM-F721N외 다른 모델을 발견할 수 없었습니다.

따라서, 1번에서 식별한 instagram 계정 정보를 통해 instagram에서 직접 해당 계정 정보를 검색하였고, 그 결과 다른 하나의 사진이 추가적으로 식별되었습니다.



[그림 10] dforensic4tor 계정 내 발견된 추가 업로드 사진

식별된 사진은 **20230609_042440.jpg** 이며, Exiftoolgui로 확인해보았을 때 증거 스마트폰 모델인 SM-F721N에 대한 메타데이터가 존재하지 않음을 확인하였습니다. 따라서 4번 문제의 답으로 판단됩니다.

5) What smartphone were the photo files found in question 4 taken on? (30 points)

Tag name	Value
SceneType	Directly photographed
ExposureMode	Auto
WhiteBalance	Auto
FocalLengthIn35mmForma	26 mm
SceneCaptureType	Standard
LensInfo	1.539999962-6mm f/1.6-2.4
LensMake	Apple
LensModel	iPhone 12 Pro back triple camera 4.2mm f/1.6

[그림 11] 20230609_042440.jpg의 EXIF metadata 정보

해당 그림의 EXIF metadata 내 발견된 LensModel정보에 따라 4번 문항의 답인 20230609_042440.jpg 파일은 **iPhone 12 Pro**로 촬영되었음을 확인하였습니다.