151 – Android Live

Team Information

Team Name _____

Team Member _____

_____

_____

Email Address _____

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:

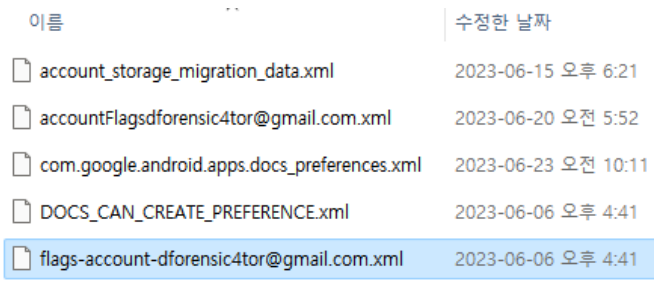
Name:		Publisher:	
Version:			
URL:			

Step-by-step methodology:

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

메모 포함[오전1]: 사용자의 Google, YouTube 그리고 Instagram 계정 이름은 무엇입니까?

1) SM-F721N_Live₩data₩com.google.android.apps.docs₩shared_prefs의 경로에서 flags-account-dforensic4tor@gmail.com이라는 파일 이름을 보고 Google계정을 파악하였다.



Google account: dforensic4tor@gmail.com

2) SM-F721N_Live₩data₩com.google.android.youtube₩files₩account₩shared의 경로의 account.pb를 HXD로 열었다.

account.pb

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   0A 00 18 01 32 26 0A 17 64 66 6F 72 65 6E 73 69  ....2&..dforensi
00000010   63 34 74 6F 72 40 67 6D 61 69 6C 2E 63 6F 6D 12  c4tor@gmail.com.
00000020   0B 08 9F B0 AB A4 06 10 C0 DD DC 4D              ..Ÿ°«¤..ÀÝÜM
```

Youtube account: dforensic4tor@gmail.com

3) SM-F721N_Live₩data₩com.instagram.android₩shared_prefsdml의 경로에서

```
com.instagram.android_preferences.xml
28
29
30
31  j6AZHyiiHu1r5wxStJpjVjSfqNGkoMc&quot;,&quot;username&quot;:&quot;dforensic4tor&quot;,
32  ot;:false,&quot;can_boost_post&quot;:false,&quot;can_create_sponsor_tags&quot;:false,
```

instagram 계정 이름을 찾아내야 하므로 username 키워드를 검색해서 정보를 얻었다.

Instagram account: dforensic4tor

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

메모 포함[오전2]: 증거 스마트폰이 연결된 무선 네트워크의 SSID와 위치(위도, 경도 좌표)는 무엇입니까?

SM-F721N_Live₩data_backup₩ABR₩WIFICONFIG의 경로에서 semconfigurations.json 파일을 열었다.

```
{
  "semwificonfig": [
    {
      "configKey": "\"JWMarriott\"OWE",
      "networkScore": 4,
      "location": [
        {
          "latitude": 1000,
          "longitude": 1000
        }
      ]
    },

    {
      "configKey": "\"JWMarriott\"NONE",
      "networkScore": 4,
      "location": [
        {
          "latitude": 8.1656823,
          "longitude": 98.2952157
        }
      ]
    }
  ]
}
```

₩"JWMarriott₩"OWE와 ₩"JWMarriott₩"NONE 중 어느 SSID를 사용해야 하는지 알아보기 위해

다른 파일을 열어본다.

```
298    "bssidPerSsidList": { "\"JWMarriott\"NONE":
```

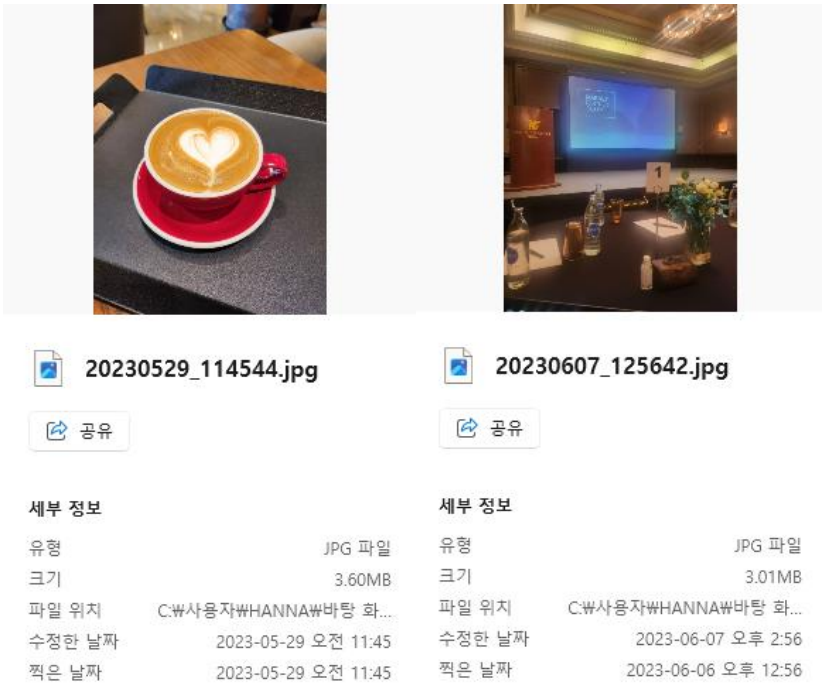
동일한 경로의 qtavels.json 파일에서 ₩"JWMarriott₩"NONE를 발견하였다.

SSID	latitude	longitude
JWMarriott	**8.1656823**	**98.2952157**

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

메모 포함[오전3]: 스마트폰으로 촬영된 사진 중에 편집된 'EXIF 타임스탬프'를 가진 것은 어떤 것입니까?

SM-F721N_Live₩media₩DCIM₩Camera



대부분의 사진이 왼쪽과 같이 사진의 제목과 찍은 날짜가 동일한데, 20230607_125642 파일만 동

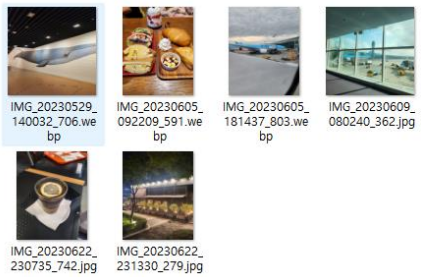
일하지 않다. 그러므로 수정된 파일이라고 판단하였다.

20230607_125642.jpg

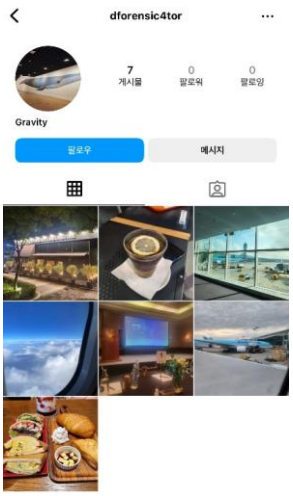
4. Which photos uploaded to Instagram were not taken on the evidence smartphone? (30 points)

메모 포함[오전4]: 인스타그램에 업로드된 사진 중 증거 스마트폰에서 촬영되지 않은 것은 무엇입니까?

SM-F721N_Live₩media₩Pictures₩Instagram



상단의 경로에서 확인할 수 있는 6가지의 사진이다.



혹시나 해서 인스타그램에 직접 검색해보았고, 계정을 찾을 수 있었다.

SM-F721N_Live₩media₩DCIM₩Camera

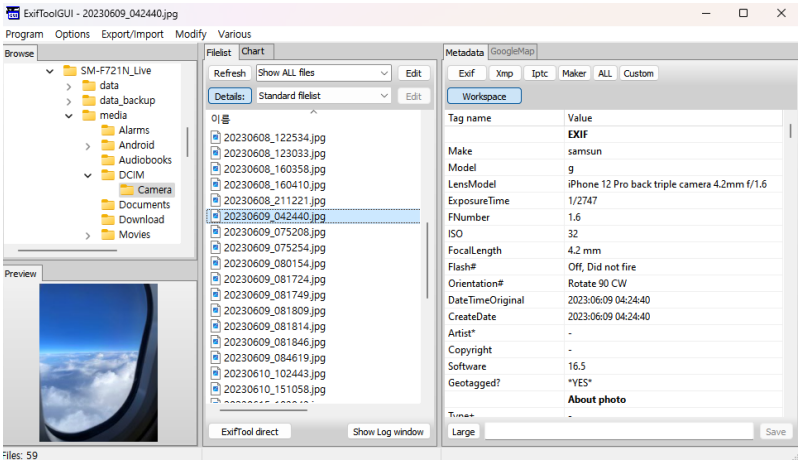
카메라 모델에 SM-F721N(SAMSUNG 갤럭시 Z 플립4)이라고 되어있는 다른 파일들과 다르게 g로 설정되어 있다.

20230609_042440.jpg

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

메모 포함[오전5]: 질문 4에서 발견된 사진 파일은 어떤 스마트폰에서 촬영되었습니까?

EXIF 정보를 나타내는 툴 중 하나인 ExiftoolGUI를 사용하였다.



iPhone 12 Pro back triple camera 4.2mm f/1.6

The deadline for this problem is August 31.

Please do not post your write-up before the deadline for fair competition!

*** Delete this box when submitting your answer.**