**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)

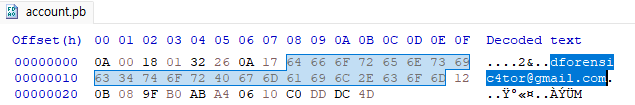
1) SM-F721N\_Live\data\com.google.android.apps.docs\shared\_prefs의 경로에서 flags-account-dforensic4tor@gmail.com이라는 파일 이름을 보고 Google계정을 파악하였다.

텍스트, 스크린샷, 폰트, 번호이(가) 표시된 사진

자동 생성된 설명

**Google account: dforensic4tor@gmail.com**

2) SM-F721N\_Live\data\com.google.android.youtube\files\account\shared의 경로의 account.pb를 HXD로 열었다.



**Youtube account: dforensic4tor@gmail.com**

3) SM-F721N\_Live\data\com.instagram.android\shared\_prefsdml의 경로에서

텍스트, 라인, 스크린샷, 소프트웨어이(가) 표시된 사진

자동 생성된 설명

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)

SM-F721N\_Live\data\_backup\ABR\WIFICONFIG의 경로에서 semconfigurations.json 파일

을 열었다.

텍스트, 스크린샷이(가) 표시된 사진

자동 생성된 설명

\“JWMarriott\”OWE와 \“JWMarriott\”NONE 중 어느 SSID를 사용해야 하는지 알아보기 위해 다른 파일을 열어본다.



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)

SM-F721N\_Live\media\DCIM\Camera

텍스트, 스크린샷, 컵, 커피잔이(가) 표시된 사진

자동 생성된 설명텍스트, 스크린샷, 멀티미디어이(가) 표시된 사진

자동 생성된 설명

대부분의 사진이 왼쪽과 같이 사진의 제목과 찍은 날짜가 동일한데, 20230607\_125642 파일만 동일하지 않다. 그러므로 수정된 파일이라고 판단하였다.

**20230607\_125642.jpg**

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

SM-F721N\_Live\media\Pictures\Instagram

텍스트, 스크린샷, 콜라주이(가) 표시된 사진

자동 생성된 설명

상단의 경로에서 확인할 수 있는 6가지의 사진이다.

텍스트, 스크린샷, 콜라주이(가) 표시된 사진

자동 생성된 설명

혹시나 해서 인스타그램에 직접 검색해보았고, 계정을 찾을 수 있었다.

SM-F721N\_Live\media\DCIM\Camera

텍스트, 스크린샷, 하늘, 구름이(가) 표시된 사진

자동 생성된 설명

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)

EXIF 정보를 나타내는 툴 중 하나인 ExiftoolGUI를 사용하였다.

텍스트, 스크린샷, 소프트웨어, 컴퓨터 아이콘이(가) 표시된 사진

자동 생성된 설명

**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.**