[DFRWS 2021 – Samsung Smartphone] Write-Up

작성자	윤지원, 김서영
분석 일자	2024.06.01–2024.06.09
작성 일자	2024.06.07-2024.06.09
분석 대상	3_Samsung GSM_SM-G973F_DS Galaxy S10.zip
문서 버전	1.0
작성자 E-mail	yoonjw0827@gmail.com

0. 목차

1. 문제

URL	DFRWS 2021 Challenge - DFRWS
문제 내용	Based on information obtained from the forensic analysis of the previous evidence, it was possible to identify an individual of interest who was arrested in Geneva on of April 20th, 2021 at 18:30 while trying to board a plane using a ticket bought with a stolen CC. Geneva Airport Police seized his phone and extracted a Full Filesystem copy on April 21st, 2021, which is available here. Preliminary analysis of the smartphone highlighted encoded SMS exchanges which might be of particular interest
문제 파일	-
문제 유형	Mobile forensics
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version
FTK Imager	https://www.exterro.com/digital-forensics-software/ftk-imager	4.7.1.2
Aleapp	abrignoni/ALEAPP: Android Logs Events And Protobuf Parser (github.com)	3.1.9

3. 환경

OS
Windows 11 64-bit

4. Write-Up

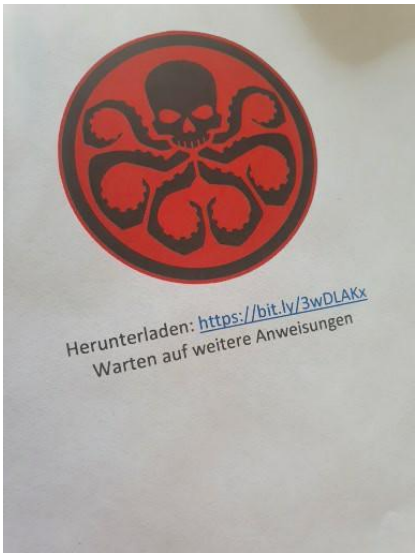
파일명	3_Samsung GSM_SM-G973F_DS Galaxy S10.zip
용량	14.2GB
SHA256	54877505f1b4eb26c4cb6b43fd6338424660c207e678b773044a4a79d6e374b7
Timestamp	2024-06-01 01:35:14

문제 배경은 2021 년 4 월 20 일 18 시 30 분에 신용카드가 도난당했고, 이를 이용하여 구입한 항공권을 통해 비행기에 탑승하려는 자를 2021 년 4 월 21 일에 체포했다는 내용이다.

압축해제를 하니 Dump 라는 형태의 폴더가 나타났고, data 폴더를 발견하여 이곳에 주요 내용이 있을 것 같다는 생각이 들어 보다 자세하게 살펴보았다.

Dump₩data₩media₩0 경로에는 주로 각종 앱들과 사진 그리고 음성 파일들이 존재하였다. 우선 음성 파일들의 경우 알람 소리였기에 주요하게 살펴보지 않고, 앱들도 일반적인 노트 앱이어서 이상한 점을 발견할 수 없었다. 그러나 사진들은 주목할 필요성이 있어 보였다.

사진들은 총 3 개의 폴더에서 발견되었는데, DCIM 과 Download, 그리고 Pictures 폴더였다. 그런데 이 폴더들에 있는 대부분은 동일한 사진들이 중복되어 저장된 것 같았다. 따라서 그나마 유의미해 보이는 사진들 몇 개를 살펴보았다.



[사진 1] Dump₩data₩media₩0₩Pictures₩.thumbnails₩22.jpg

우선 [사진 1]의 경우, 로고와 함께 사이트 주소가 적혀 있다. DCIM 폴더에도 저장되어 있는 사진인데, 이 사이트가 무언가를 의미하는 것 같아서 검색해보았으나 아무것도 발견하지 못했다.

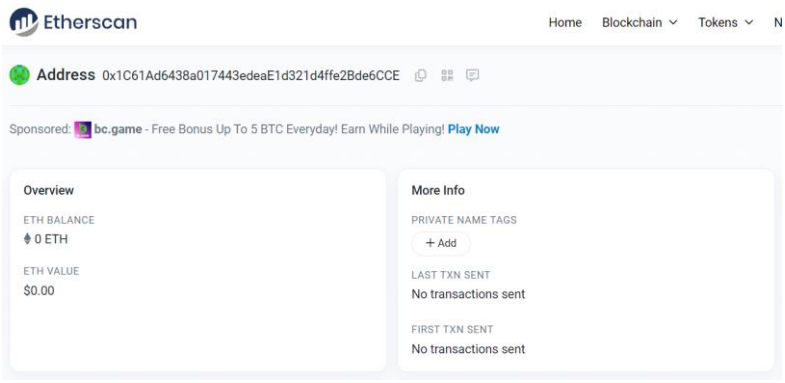
[사진 2] Dump₩data₩media₩0₩DCIM₩Screenshots₩Screenshot_20210418-161954_BRD.jpg

이 사진은 비트코인과 관련된 QR코드를 캡처해 놓은 사진이라고 생각하여, 스캔해보니 **'bitcoincash:qpuv475w4wytd6agujpzfl9muzajf9le45nkefd23y'**라는 비트코인 캐시 주소가 나타났다. 따라서 이를 blockchair(https://blockchair.com/ko)라는 블록체인 탐색기에 넣어보니 [사진 3]과 같은 기록이 나타났다. 사건은 2021년 4월 20일에서 21일사이에 일어났기 때문에 그 전에 발생한 비트코인 기록으로 보인다.

[사진 3] [사진 2]의 비트코인 캐시 주소의 거래 기록

[사진 4] Dump₩data₩media₩0₩Pictures₩1618756982374.jpg

이 QR코드는 스캔하면 **'ethereum:0x1C61Ad6438a017443edeaE1d321d4ffe2Bde6CCE'**라는 메시지가 출력된다. 이는 이더리움 주소로 블록체인 상의 특정 계정을 나타낸다는 것을 알아냈다. 따라서 Etherscan(https://etherscan.io/)라는 블록체인 탐색기에 주소를 넣어본 결과, [사진 5]와 같이 아무것도 발견할 수 없었다.

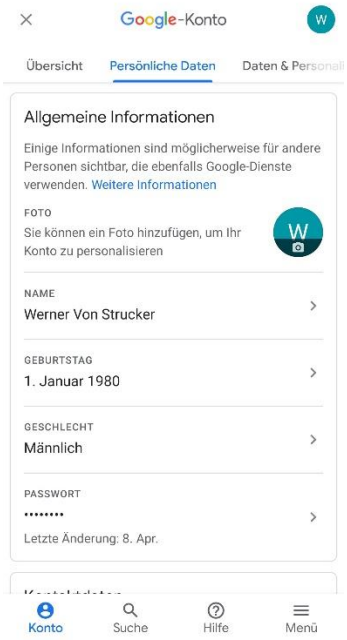


[사진 5] Etherscan에서의 [사진 4] 주소의 거래 기록

마지막으로 찾은 [사진 6]은 범인이 예매한 비행기표의 정보인 것 같다. Genf에서 출발하여 Madrid를 거쳐 New York에 도착하는 비행기표인 것 같다. 따라서 범인은 최종적으로 뉴욕으로 가려 했다는 사실을 알 수 있다.

[사진 6] Dump₩data₩media₩0₩DCIM₩Screenshots₩Screenshot_20210418-174639_Chrome.jpg

이 경로에서는 이 파일들만 발견되었고, 조금 더 둘러보니 Dump₩data₩system_ce₩0₩snapshots 폴더에 더 많고 단서가 될 수 있는 이미지들이 발견되었다.



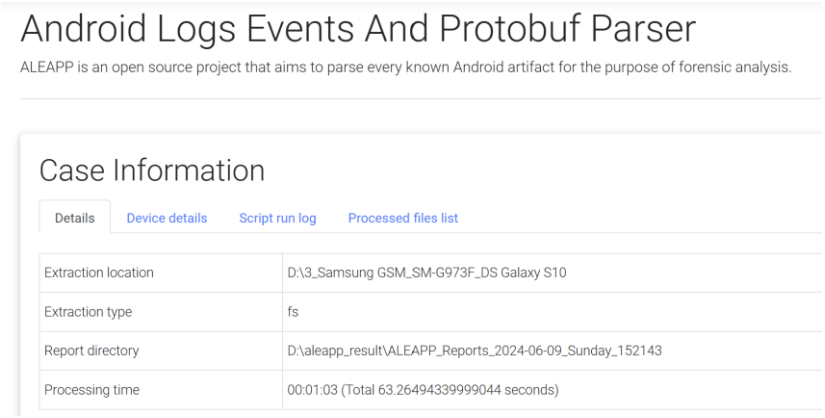
[사진 7] Dump₩data₩system_ce₩0₩snapshots₩141.jpg

이 이미지는 범인의 구글 계정이 캡처된 사진인데, 그의 개인정보를 볼 수 있다. 중요한 단서 중 하나가 될 수 있는 범인의 이름이 **Werner Von Strucker** 라는 것을 알아냈다.

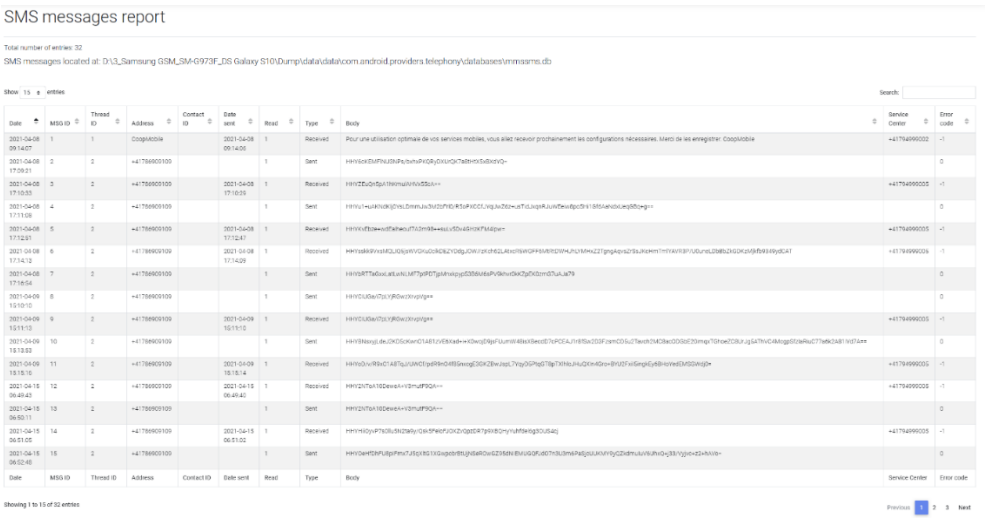
[사진 8] Dump₩data₩system_ce₩0₩snapshots₩154.jpg

[사진 8]의 경우, 처음 보는 이미지라서 살펴보니 노트를 이용하여 무언가를 보호하고자 한 것 같다. 따라서 노트를 의미하는 텍스트 파일을 먼저 찾아보다가 잘 보이지 않아서 무엇일까 고민하다가 아까 Dump₩data₩media₩0 에서 보았던 설치 앱들이 생각났다. 분명 거기에 노트와 관련된 앱들도 많았기 때문에 그들 중 하나에 단서가 있지 않을까 생각했다. 그러나 결국엔 찾지 못했다.

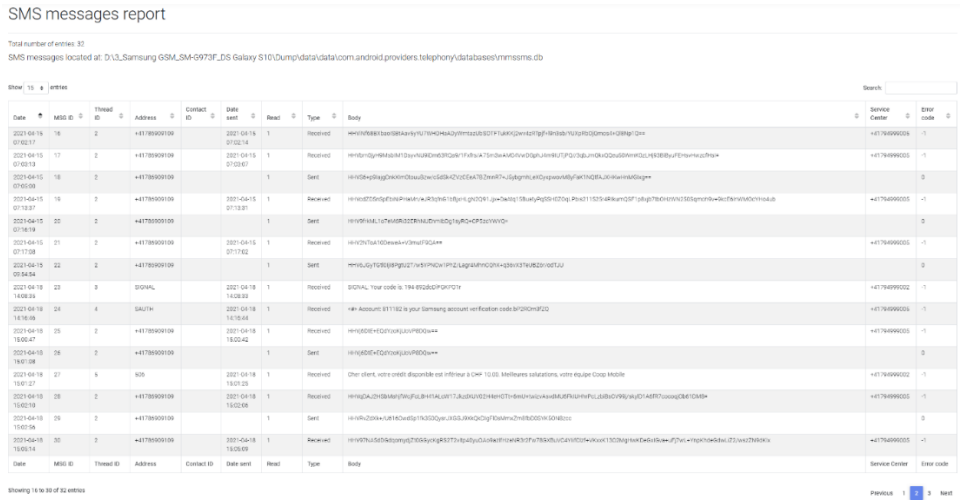
문제에서 제시되어 있는 encrypted SMS messages 를 찾기 위해 ALEAPP 을 사용하여 문제파일의 GalaxyS10 을 분석해보았다.



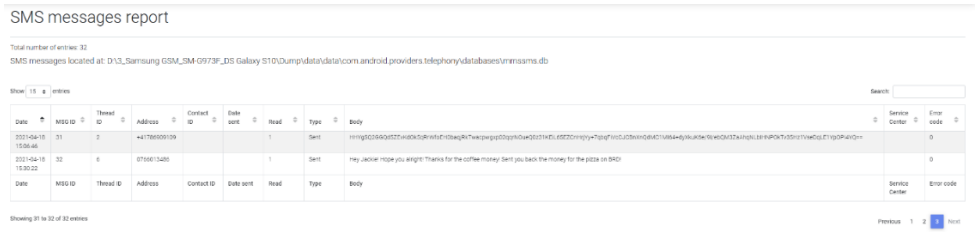
[사진 9] ALEAPP 분석 결과창



[사진 10] ALEAPP 분석 – SMS messages(1)



[사진 11] ALEAPP 분석 – SMS messages(2)



[사진 12] ALEAPP 분석 – SMS messages(3)

3 페이지의 마지막 메시지 제외 다른 메시지들은 내용을 알아볼 수 없었다. 암호화가 적용되어 있는 듯하다.

어떠한 암호화 과정이 적용되었는지 확인하기 위해서는 Android 전문 분석 도구인 Jadx 로 문제 파일을 열어 MainActivity 를 살펴보는 것이 가장 적합하다고 생각했다.

하지만, 문제 풀이자 2 명이 7 일 내내 시도했음에도 jadx 로 열리지 않았다. 또한, jadx 와 비슷한 도구 apktools, Android Studio, Bytecode Viewer, Dex2jar 등 다양한 안드로이드 분석 도구를 사용했음에도 열리지 않고, 분석되지 않았다.

Autopsy, FTK Imager, ALEAPP 와 같은 도구들을 통해 얻을 수 있는 정보는 [사진 12]까지가 전부이다.

문제 파일 zip 을 apk 로 컴파일하는 방법을 떠올렸지만, apk 로 컴파일하는 방법에 대한 지식이 적어 시도 또한 실패했다. 추후에 공부를 더 하여 재시도해보고자 한다.

5. Flag

6. 별도 첨부

7. Reference

- [URL]