[제9회디지털범인을찾아라]

Write-Up

작성자	Team A
분석 일자	2024.05.27~2024.06.05
작성 일자	2024.06.05
분석 대상	USB
문서 버전	1.0
작성자 E-mail	dmswjd4315@yonsei.ac.kr

0. 목차

1. 문제

URL	-
문제 내용	문제 내용이 길어 별도첨부에서 확인이 가능하다.
문제 파일	-
문제 유형	system_forensics
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version
FTK Imager	https://www.exterro.com/digital-forensics-software/ftk-imager	4.5.0.3
Registry Viewer	https://www.exterro.com/digital-forensics-software/forensic-toolkit	2.0.0.7
Autopsy	https://www.autopsy.com/download/	4.20.0
	나머지 분석 도구는 별도첨부에 포함	

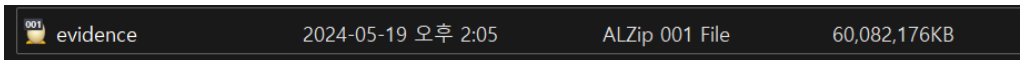
3. 환경

OS
Windows11 64-bit

4. Write-Up

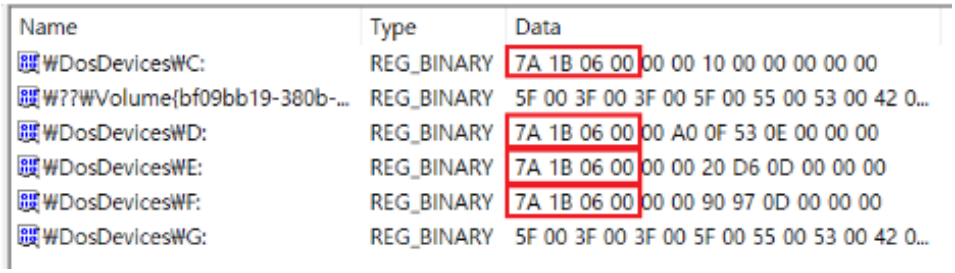
파일명	USB
용량	64GB
SHA256	63580b96bce775e6018661cc4a1b68af2df66b132dc563b4a5126f20efbe704f
Timestamp	2024-05-19 14:43:22

증거 분석 준비



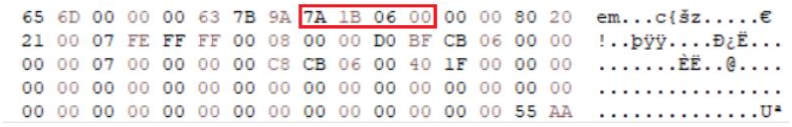
[사진 1] USB 사본 이미지 생성

USB 증거 분석을 위해 FTK Imager 을 이용하여 사본 이미지 파일을 생성하였다. 이때, 사본 이미지 파일은 RAW(.dd) 형식이다.



[사진 2] PC에 연결 되었던 파티션 정보

손상 및 삭제된 파티션을 복구하기 위해 SYSTEM 레지스트리 하이브 파일을 분석하여 파티션 정보를 확인하였다.

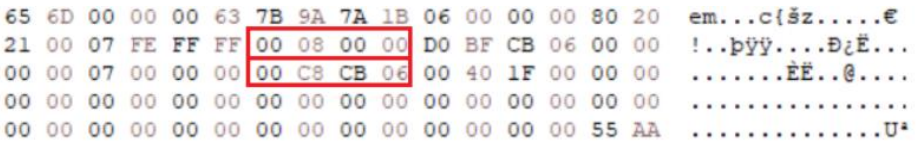


[사진 3] MBR에 기록되어 있는 디스크 시그니처

[사진 2]에서 공통적으로 보이는 **00061B7A**의 값은 MBR에 기록되어 있는 디스크 시그니처 값으로 디스크마다 가지고 있는 고유의 값이다. 이는 MBR offset 0x1B8에 4byte로 기록되어 있는 것을 [사진 3]을 통해 알 수 있다. 현재, [사진 2]에서 C,D,E,F 총 4개의 드라이브 파티션에서 디스크 시그니처 값이 00061B7A로 동일한 것으로 해당 디스크에 **총 4개의 파티션**이 존재하였음을 알 수 있다.

파티션 드라이브 문자	파티션 첫 번째 섹터
C:	Sector 2048
D:	Sector 120162256
E:	Sector 116068352
F:	Sector 114018304

[표 1] 파티션별 첫 번째 섹터 목록



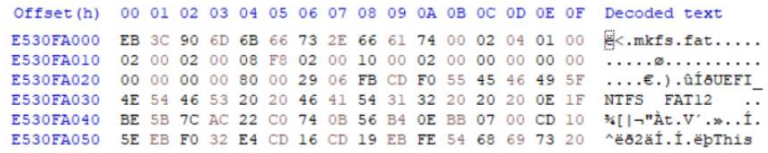
[사진 4] MBR 파티션 테이블에서 확인된 2개의 파티션

[사진 2]에서 확인된 확인된 파티션은 총 4개였지만, MBR 파티션 테이블에서 확인된 파티션은 2개만 확인되었다.

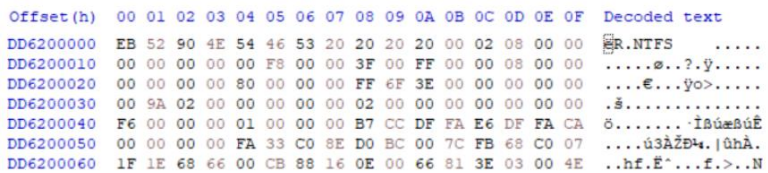
파티션 드라이브 문자	파티션 첫 번째 섹터
C:	Sector 2048
F:	Sector 114018304

[표 2] MBR 파티션 테이블에서 확인된 파티션 정보

[표 1]과 [표 2]의 파티션 수가 차이가 있는 것을 보고 D: 드라이브와 E: 드라이브 파티션은 삭제된 것으로 추정되어 해당 드라이브의 파티션 복구를 진행하였다.



[사진 5] D: 드라이브 파티션 VBR(Volume Boot Record)



[사진 6] E: 드라이브 파티션 VBR(Volume Boot Record)

SYSTEM 레지스트리에서 확인한 D: 드라이브와 E: 드라이브 파티션의 시작 섹터인 위치에 VBR이 온

전히 남아 있어 Total Sector 수를 확인하고 해당 파티션 시작 센터부터 Total Sector만큼 각각을 추출하여 복구를 하였다.

File System Information	
Cluster Size	4,096
Cluster Count	511,487
Free Cluster Count	264,313
Dirty Flag	False
Volume Label	새 볼륨
Volume Serial Number	FADF-CCB7
File System Version	Windows XP (NTFS 3.1)
UTC Timestamps	True

[사진 7] 복구된 E 드라이브 파티션 정보

File System Information	
Cluster Size	2,048
Cluster Count	502
Free Cluster Count	58
Volume Label	UEFI_NTFS
Volume Serial Number	F0CD-FB06
UTC Timestamps	False

[사진 8] 복구된 D 드라이브 파티션 정보

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
D97900000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D97900010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D97900020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D97900030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
D97900040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

[사진 9] 손상되어 있는 F 드라이브 파티션의 VBR

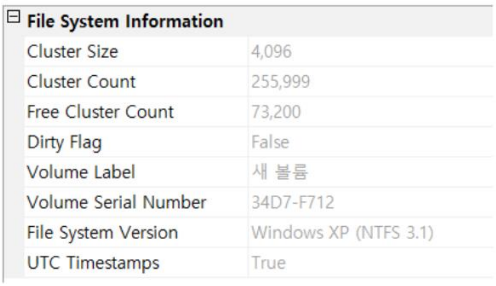
MBR 파티션 테이블에서 확인되었던 F 드라이브 파티션은 삭제되어 있지 않지만, VBR이 손상되어 있어 정상적으로 파일 시스템을 읽어올 수 없었다.

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
DD60FFE00  EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00  ëR.NTFS     .....
DD60FFE10  00 00 00 00 00 F8 00 00 3F 00 FF 00 00 C8 CB 06  .....ø..?.ÿ..ÈË.
DD60FFE20  00 00 00 00 80 00 80 00 FF 3F 1F 00 00 00 00 00  ....€.€.ÿ?......
DD60FFE30  55 4D 01 00 00 00 00 00 02 00 00 00 00 00 00 00  UM..............
DD60FFE40  F6 00 00 00 01 00 00 00 12 F7 D7 34 27 D8 34 E8  ö........÷×4'Ø4è
DD60FFE50  00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  ....ú3ÀŽÐ¼.|ûhÀ.
DD60FFE60  1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E  ..hf.Ë^...f.>..N
```

[사진 10] F 드라이브 파티션의 마지막 센터에서 찾은 VBR 복사본

파일 시스템에는 VBR 손상을 대비하기 위하여 VBR 복사본이 저장되어 있기 때문에 **해당 VBR 복사본을 찾아 파티션 첫 번째 섹터에 붙여 넣어 복구**할 수 있었다.

F: 파티션의 VBR은 해당 파티션의 마지막 섹터 위치에서 찾을 수 있었으며 이를 F: 파티션의 첫번째 섹터 위치로 복사하여 복구하여 복구한 후 F: 파티션 부분을 추출하였다.



[사진 11] F: 파티션 파일시스템 정보

Image File	Partition_D.001
MD5	b8fa81be883b4131ba143db76eace43a
SHA1	6600eb4080275b7074208469baaeb58680701867

[표 3] D: 드라이브 파티션 복구 이미지 파일 해시 값

Image File	Partition_E.001
MD5	b3d555543ddf99908e4e2f21ac57e566
SHA1	30c84d670a0234122d0b2cf256babe143eb5aa45

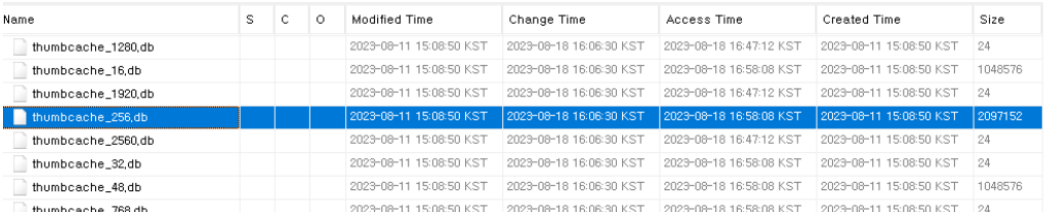
[표 4] E: 드라이브 파티션 복구 이미지 파일 해시 값

Image File	Partition_F.001
MD5	a5020ea5e60745c2ea1f5f3f64f8e3c1
SHA1	ef7a4aeada809dcadeb396c65ff95e562014d70e

[표 5] F: 드라이브 파티션 복구 이미지 파일 해시 값

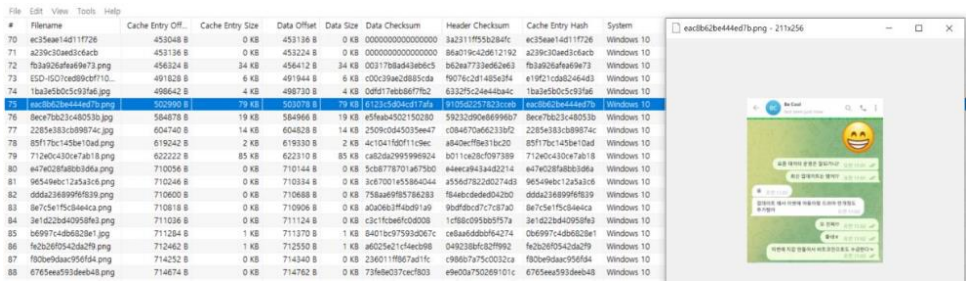
HashCalc를 이용하여 각 드라이브의 파티션 복구 이미지 파일 해시값을 추출하였다.

증거 분석



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size
thumbcache_1280.db				2023-08-11 15:08:50 KST	2023-08-18 16:06:30 KST	2023-08-18 16:47:12 KST	2023-08-11 15:08:50 KST	24
thumbcache_16.db				2023-08-11 15:08:50 KST	2023-08-18 16:06:30 KST	2023-08-18 16:58:08 KST	2023-08-11 15:08:50 KST	1048576
thumbcache_1920.db				2023-08-11 15:08:50 KST	2023-08-18 16:06:30 KST	2023-08-18 16:47:12 KST	2023-08-11 15:08:50 KST	24
thumbcache_256.db				2023-08-11 15:08:50 KST	2023-08-18 16:06:30 KST	2023-08-18 16:58:08 KST	2023-08-11 15:08:50 KST	2097152
thumbcache_2560.db				2023-08-11 15:08:50 KST	2023-08-18 16:06:30 KST	2023-08-18 16:47:12 KST	2023-08-11 15:08:50 KST	24
thumbcache_32.db				2023-08-11 15:08:50 KST	2023-08-18 16:06:30 KST	2023-08-18 16:58:08 KST	2023-08-11 15:08:50 KST	24
thumbcache_48.db				2023-08-11 15:08:50 KST	2023-08-18 16:06:30 KST	2023-08-18 16:58:08 KST	2023-08-11 15:08:50 KST	1048576
thumbcache_768.db				2023-08-11 15:08:50 KST	2023-08-18 16:06:30 KST	2023-08-18 16:58:08 KST	2023-08-11 15:08:50 KST	24

[사진 12] Thumbcache_256



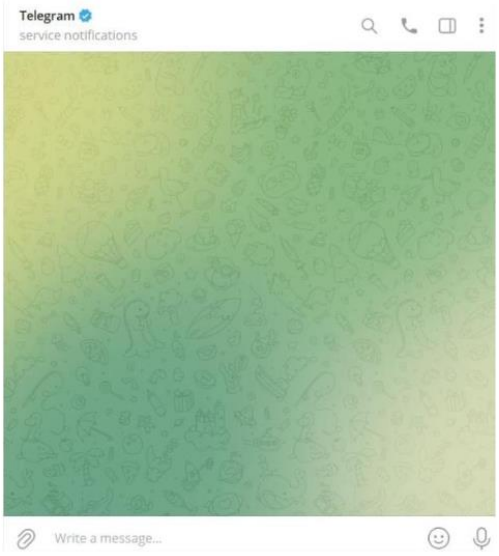
[사진 13] Thumbcache_256.db에서 확인한 문자내역 이미지

증거를 분석하기 위해 C: 드라이브를 분석해보았다.

일단, Autopsy를 이용하여 Thumbcache_000.db가 어느 위치에 존재하는지 찾아본 결과 **C:₩Users₩human₩AppData₩local₩Microsoft₩Windows₩Explorer**에 존재하는 것을 알 수 있었다. 그 후 해당 경로 안에 있는 Thumbcache_000.db를 Thumbcache_Viewer를 이용하여 썸네일 이미지를 확인해본 결과 **Thumbcache_256.db** 파일에 있는 여러 썸네일 중 **'Be cool'**이라는 이름의 사용자와 문자를 주고 받은 이미지가 **총 3개**가 존재한다는 것을 볼 수 있었다.

텔레그램 대화 내용 스크린샷 원본 파일
F:₩Framework64₩v4.0.30319₩ASP.NETWebAdminFiles₩Images₩be_cool_1_1.png
F:₩Framework64₩v4.0.30319₩ASP.NETWebAdminFiles₩Images₩be_cool_2_2.jpg
F:₩Framework64₩v4.0.30319₩ASP.NETWebAdminFiles₩Images₩be_cool_3_3.jpg

[표 6] Thumbcache_256.db에서 확인한 문자내역 이미지



[사진 14] 텔레그램 메시지 인터페이스

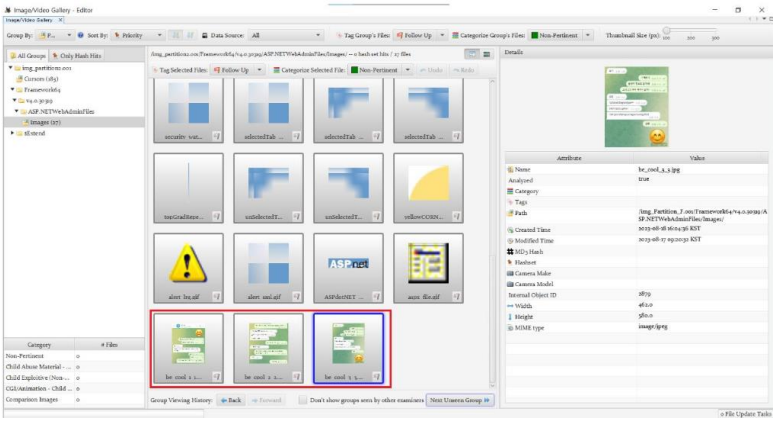
해당 이미지가 [사진 14]의 이미지와 동일한 것을 보아 해당 문제는 텔레그램 메시지를 통해 이루어진 것을 알 수 있다.

[사진 15] thumbcache_256.db 파일에서 확인한 문자내역 스크린샷

해당 문자 내역을 보니 A씨는 비트코인 지갑을 만들어 금전적인 수익을 받는 것으로 보이며 **'Be cool'**이라는 사람에게 A씨의 가상화폐 지갑주소가 담긴 압축파일을 암호화하여 전송한 것 같아 보인다.

[사진 15]를 보면 A씨가 운영자 정보를 **'Be cool'** 사용자에게 요구하자 운영자 정보를 평문이 아닌 ~==, ~= 형태로 **Base64 인코딩**하여 알려준 것으로 보인다.

Thumbcache_256.db에 기록된 썸네일 이미지는 원본 이미지를 작은 이미지로 만들어 저장하기 때문에 썸네일 이미지는 선명하지 않다. 그래서 운영자 정보가 기록된 Base64 인코딩 문자열을 정확히 확인하기 힘들어 원본 이미지 파일을 찾아 분석해보기로 하였다.



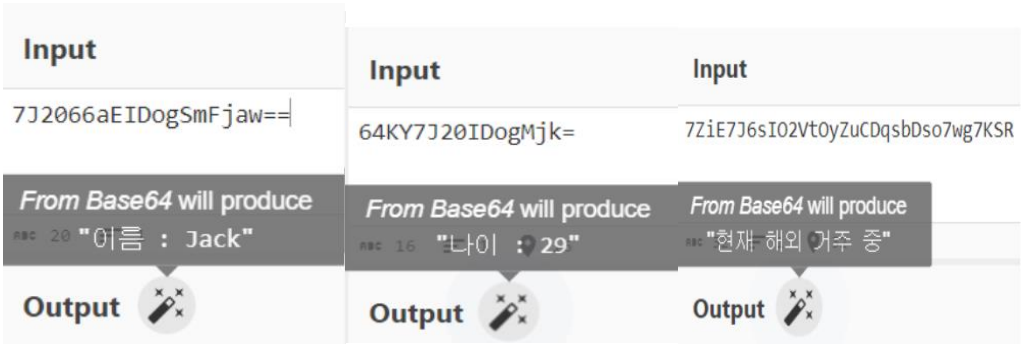
[사진 16] F: 파티션에서 찾은 Telegram 대화 내용 스크린샷 원본 이미지 파일

텔레그램 메시지 대화 내용 스크린샷 원본 이미지 파일은 VBR이 손상되었던 F: 드라이브 파티션에 존재하였다.

[사진 17] 운영자 정보가 있는 Telegram 대화 이미지(be_cool_3_3.jpg)

Thumbcahce_256.db에서 추출한 이미지에서는 base64 문자열을 정확히 확인할 수 없었지만 원본 이미지 파일에서는 정확하게 확인이 가능하다.

따라서, 해당 base64 문자열을 CyberChef(https://gchq.github.io/CyberChef/)를 사용하여 평문으로 복호화를 시도해보기로 하였다.

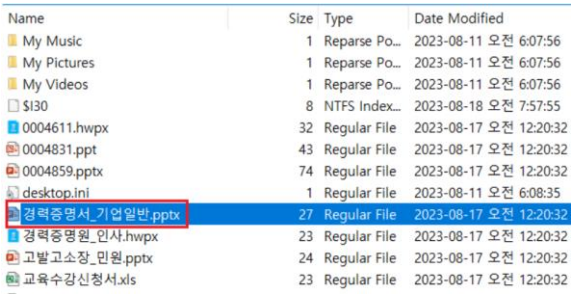


[사진 18] 운영자 정보가 있는 Base64 인코딩 문자 복호화 결과

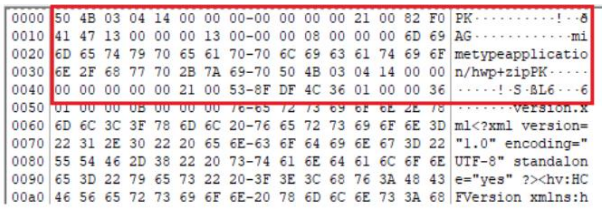
Base64 복호화 결과, 해외 불법 스트리밍 사이트 서버 운영자의 이름, 나이, 거주 정보를 알 수 있었다.

이름	Jack
나이	29
특이사항	현재 해외 거주 중

[표 7] 텔레그램 대화 내역에서 확인한 해외 서버 운영자 정보

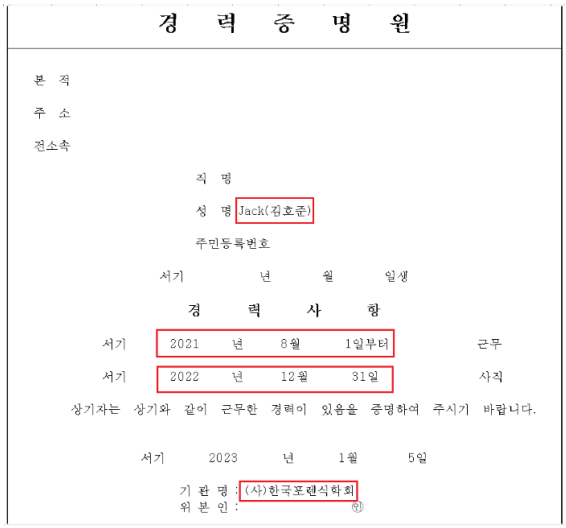


[사진 19] 경력증명서_기업일반.pptx 파일의 확장자 확인



[사진 20] 경력증명서_기업일반 파일의 헤더 시그니처 확인

C:₩Users₩human₩Documents 디렉터리에 있는 "경력증명서_기업일반.pptx" 파일은 확장자가 pptx로 되어있는데 [사진 20]을 보면 해당 파일의 헤더가 hwpx 파일이다. 따라서, "경력증명서_기업일반.pptx" **파일의 확장자명을 .hwp로 변경**하여 한컴오피스 Viewer로 열어 보았다.



경 력 증 명 원

본 적
주 소
점소속
직 명
성 명 Jack(김호준)
주민등록번호
서기 년 월 일생

경 력 사 항

서기 2021 년 8월 1일부터 근무
서기 2022 년 12월 31일 사직

상기자는 상기와 같이 근무한 경력이 있음을 증명하여 주시기 바랍니다.

서기 2023 년 1월 5일

기 관 명 : (사)한국포렌식학회
위 본 인 : ㊞

[사진 21] "경력증명서_기업일반.pptx" 파일 내부 내용

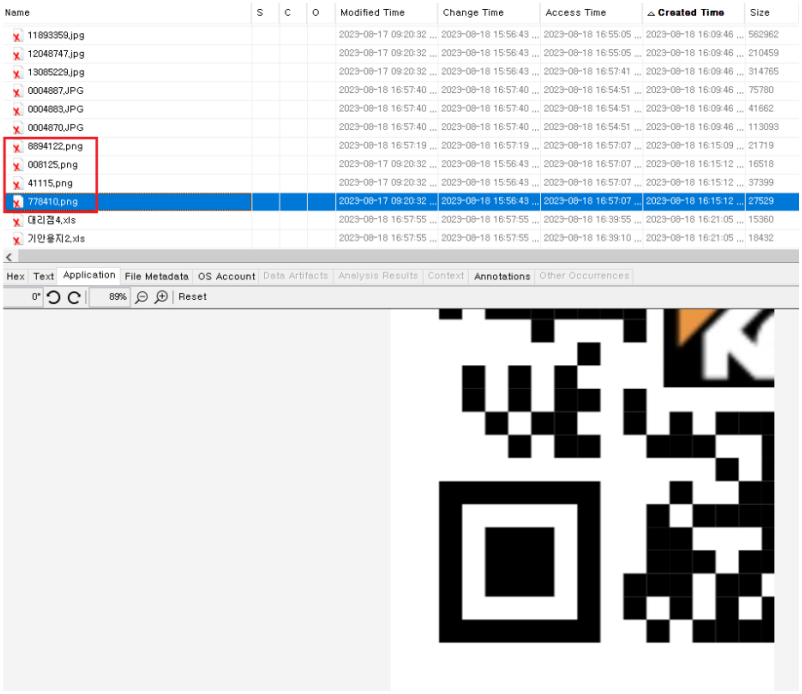
[사진 21]을 통해 내부 내용이 (사)한국포렌식학회 기관의 경력증명서로 확인되었다.

성명은 'Jack(김호준)'으로 [사진 18]의 'Be Cool'과의 텔레그램 메시지 대화 내역에서 'Be Cool'이 알려준 해외 불법 스트리밍 사이트 운영자의 이름인 **Jack과 일치하는 것으로 동일인물로 추정**된다.

해외 불법 스트리밍 사이트 운영자로 추정되는 'Jack'의 **한국 이름은 '김호준'**으로 확인되었으며 'Jack(김호준)'은 **2021년 8월 1일부터 2022년 12월 31일**까지 (사)한국포렌식학회 기관에서 근무를 하였던 것을 확인하였다.

영어이름(한국이름)	Jack(김호준)
나이	29
주거 정보	현재 해외 거주 중
근무 경력	2021년 8월 1일 ~ 2022년 12월 31일 기관: (사)한국포렌식학회

[표 8] 확인된 해외 불법 스트리밍 사이트 운영자 정보



[사진 22] 삭제되어 비할당 영역에 존재한 QR코드 이미지 파일

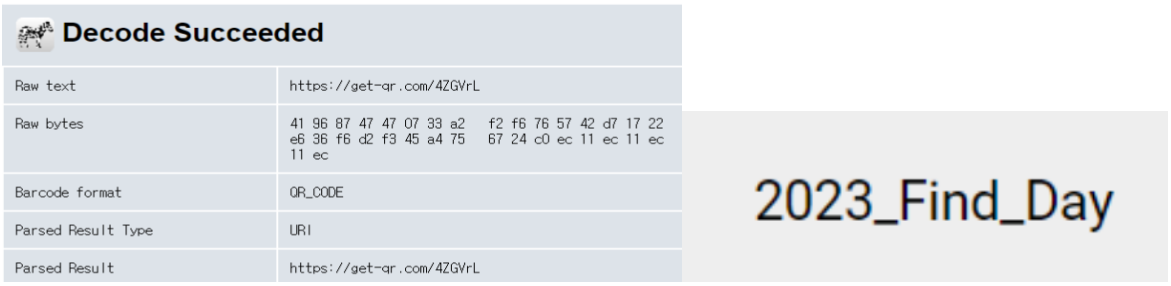
C: 드라이브 파티션에서 삭제된 파일 중 QR코드 이미지가 4분할 되어있는 총 4개의 png 파일을 찾을 수 있었다.

삭제되어 있는 QR코드 이미지 파일
778410.png
41115.png
008125.png
8894122.png

[표 9] 확인된 해외 불법 스트리밍 사이트 운영자 정보

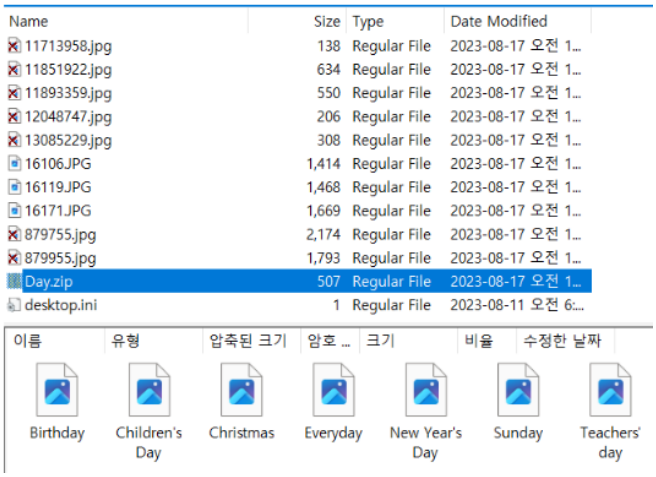
[사진 23] 삭제되어 있던 4개의 QR코드 이미지를 합쳐 복원

삭제되어 있던 4분할 QR코드 이미지를 QR코드 스캔을 위해 4개의 png 파일을 합쳐 스캔을 시도하였다.

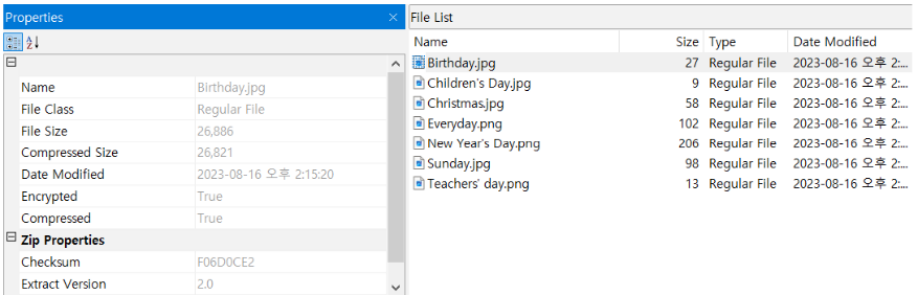


[사진 24] QR 코드 스캔 결과

ZXing Decoder Online(https://zxing.org/w/decode.jspx)에서 해당 QR 코드 이미지 스캔 결과 **"2023_Find_Day"**라는 문자열이 나왔다.



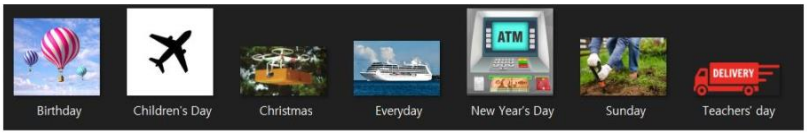
[사진 25] Day.zip 압축파일



[사진 26] 암호화가 되어 있는 Day.zip 파일

Day.zip 파일은 **7개의 이미지 파일을 암호화**하여 압축한 파일로 비밀번호를 통하여 정상적인 압축해제가 가능하다.

C: 드라이브 파티션에서 비할당 영역에 존재했던 QR 코드 이미지로부터 스캔한 결과인 "2023_Find_Day"를 Day.zip 압축 해제시 비밀번호를 입력하니 압축이 정상적으로 해제되었다.



[사진 27] Day.zip 안의 이미지 파일

Day.zip 파일 안을 보았더니 [사진 27]과 같이 7개의 이미지 파일이 존재하였지만 스테가노그래피 또는 안에 숨겨진 내용은 확인되지 않았다.

Source Name	S	C	O	Domain	Text	Program Name	Date Accessed	Data Source
History				google.com	한국포렌식학회	Google Chrome	2023-08-18 16:43:43 KST	Evidence.001
History				google.com	한국포렌식학회	Google Chrome	2023-08-18 16:43:43 KST	Evidence.001
History				google.com	스테가노그래피	Google Chrome	2023-08-18 16:43:56 KST	Evidence.001
History				google.com	스테가노그래피	Google Chrome	2023-08-18 16:43:56 KST	Evidence.001
History				google.com	스테가노그래피	Google Chrome	2023-08-18 16:43:56 KST	Evidence.001
History				google.com	스테가노그래피 기법	Google Chrome	2023-08-18 16:44:31 KST	Evidence.001
History				google.com	스테가노그래피 기법	Google Chrome	2023-08-18 16:44:31 KST	Evidence.001
History				google.com	스테가노그래피 기법	Google Chrome	2023-08-18 16:44:31 KST	Evidence.001
History				google.com	mp3 to wav	Google Chrome	2023-08-18 16:44:57 KST	Evidence.001
History				google.com	mp3 to wav	Google Chrome	2023-08-18 16:44:57 KST	Evidence.001
History				google.com	mp3 to wav	Google Chrome	2023-08-18 16:44:57 KST	Evidence.001
History				google.com	그림파일 bit	Google Chrome	2023-08-18 16:45:33 KST	Evidence.001
History				google.com	그림파일 bit	Google Chrome	2023-08-18 16:45:33 KST	Evidence.001
History				google.com	LSB	Google Chrome	2023-08-18 16:45:46 KST	Evidence.001
History				google.com	LSB	Google Chrome	2023-08-18 16:45:46 KST	Evidence.001
History				google.com	암호화	Google Chrome	2023-08-18 16:47:04 KST	Evidence.001
History				google.com	암호화	Google Chrome	2023-08-18 16:47:04 KST	Evidence.001
History				google.com	암호화	Google Chrome	2023-08-18 16:47:04 KST	Evidence.001
History				google.com	AES 알고리즘	Google Chrome	2023-08-18 16:47:53 KST	Evidence.001
History				google.com	AES 알고리즘	Google Chrome	2023-08-18 16:47:53 KST	Evidence.001
History				google.com	AES 알고리즘	Google Chrome	2023-08-18 16:47:53 KST	Evidence.001
History				google.com	AES 알고리즘	Google Chrome	2023-08-18 16:47:53 KST	Evidence.001
History				google.com	AES 알고리즘	Google Chrome	2023-08-18 16:47:53 KST	Evidence.001
History				google.com	AES 알고리즘 자바	Google Chrome	2023-08-18 16:48:05 KST	Evidence.001
History				google.com	AES 알고리즘 자바	Google Chrome	2023-08-18 16:48:05 KST	Evidence.001
History				google.com	AES 알고리즘 자바	Google Chrome	2023-08-18 16:48:05 KST	Evidence.001
History				google.com	AES 알고리즘 파이썬	Google Chrome	2023-08-18 16:49:38 KST	Evidence.001

[사진 28] Chrome web browser를 사용한 google 검색 기록

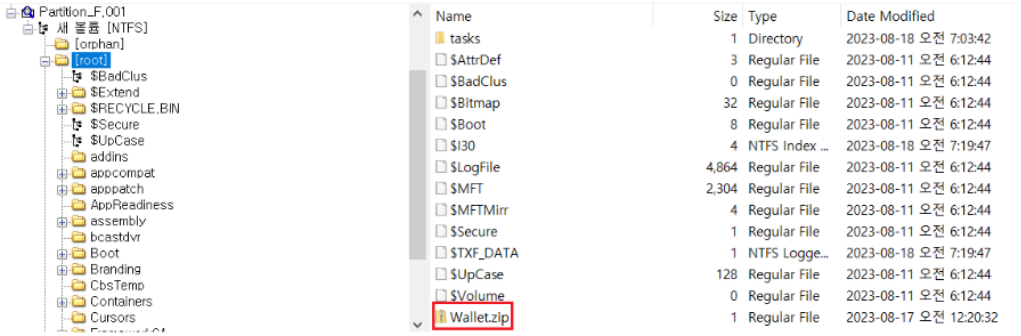
/Users/human/AppData/Local/Google/Chrome/User Data/Default/History 파일에서 확인한 Chrome web browser의 google 검색 기록에는 주로 **"스테가노그래피", "암호화", "AES 알고리즘"** 등과 같이 중요한 정보를 숨기기 위한 안티 포렌식 기법을 검색했던 것으로 확인되었다.

검색 일시	검색어
2023-08-18 16:43:56 KST	스테가노그래피 - Google 검색
2023-08-18 16:45:33 KST	그림파일 bit - Google 검색
2023-08-18 16:47:04 KST	암호화 - Google 검색
2023-08-18 16:47:53 KST	AES 알고리즘 - Google 검색
2023-08-18 16:48:05 KST	AES 알고리즘 자바 - Google 검색
2023-08-18 16:49:28 KST	aes 알고리즘 c 소스 - Google 검색
2023-08-18 16:49:37 KST	AES 알고리즘 파이썬 - Google 검색

[표 10] Google 검색어 주요 목록

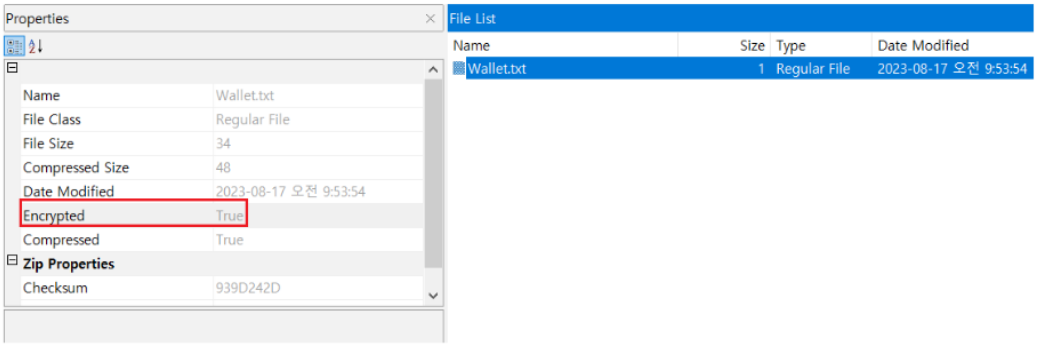
[사진 29] 비트코인 관련 대화 내역(be_cool_2_2.jpg)

F:₩Framework64₩v4.0.30319₩ASP.NETWebAdminFiles₩Images₩be_cool_2_2.jpg파일에서 확인한 대화 내역에서 A씨가 비트코인 지갑을 만들어 **금전적인 수익을 얻고 있다**고 'Be Cool' 에게 알려주고 있으며 'Be Cool'에게 자신의 가상화폐 지갑 주소를 비밀번호를 설정한 압축파일로 전송하여 알려주고 있는 것을 확인할 수 있다.



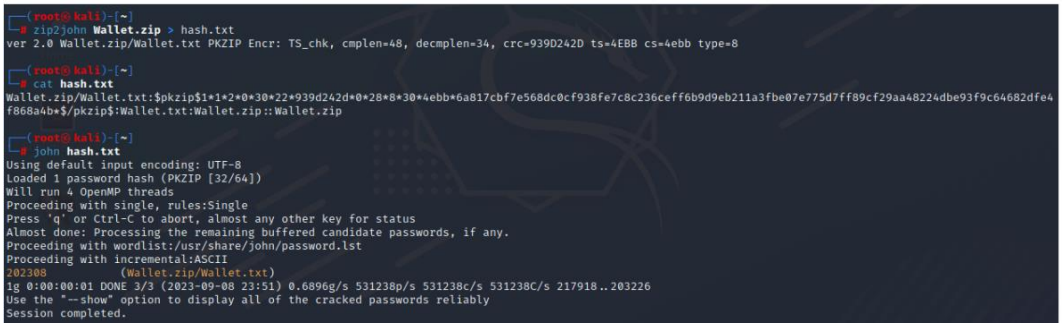
[사진 30] Wallet.zip 파일

'Be cool'에게 가상화폐 지갑주소를 알려주기 위해 생성한 압축파일로 추정되는 **Wallet.zip**을 발견하였다.



[사진 31] Wallet.zip 내부 암호화된 Wallet.txt 파일

Wallet.zip 파일내부 Wallet.txt 파일이 암호화가 설정되어 있어 비밀번호를 통해 Wallet.txt를 열어 볼 수 있다.

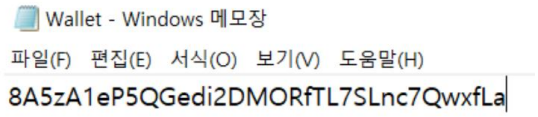


[사진 32] john the ripper 도구를 사용하여 Wallet.zip 파일의 비밀번호 추출

Wallet.zip 파일에 설정되어 있는 비밀번호를 알아내기 위하여 zip2john을 통해 Wallet.zip의 비밀 번호 해시 값을 추출하고 john the ripper 도구를 사용하여 Wallet.zip의 비밀번호를 추출하였다.

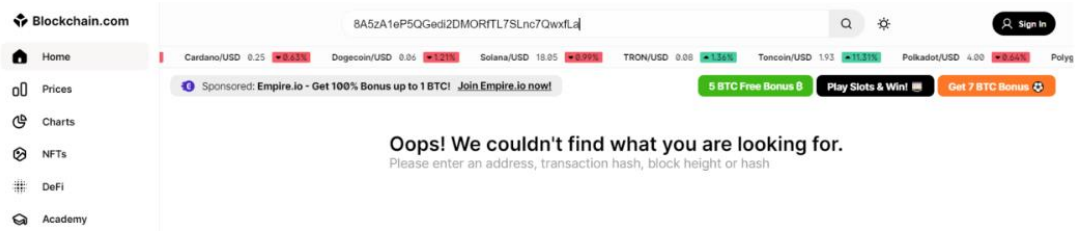
Wallet.zip 파일의 비밀번호
202308

[표 11] john the ripper 도구를 사용하여 Wallet.zip 파일의 비밀번호 추출

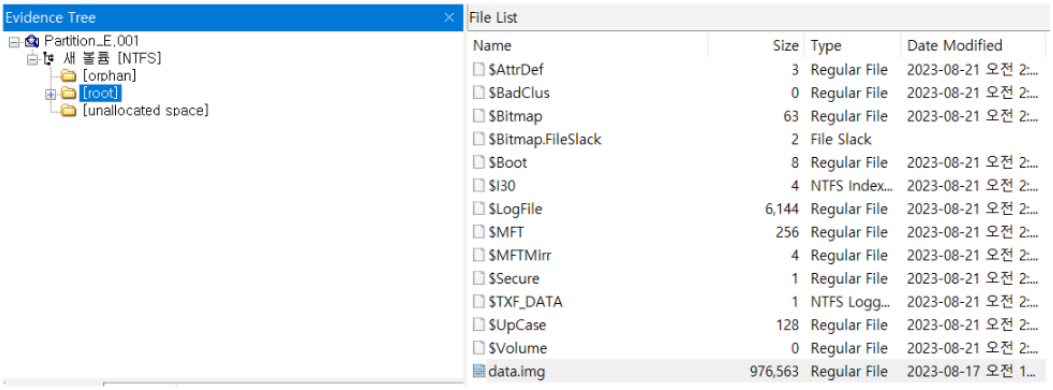


[사진 33] Wallet..txt 파일

Wallet.zip 압축해제 시 비밀번호 **202308**를 입력하니 정상적으로 압축 해제되었으며 내부에 있는 Wallet.txt 파일에는 34 bytes의 "0-9/a-z/A-Z" 범위 임의 값으로 이루어진 가상화폐 지갑주소와 유사한 형태의 문자열이 기록되어 있어 가상화폐를 조회해 보았지만 해당 지갑 주소에 대한 내역은 확인되지 않았다.

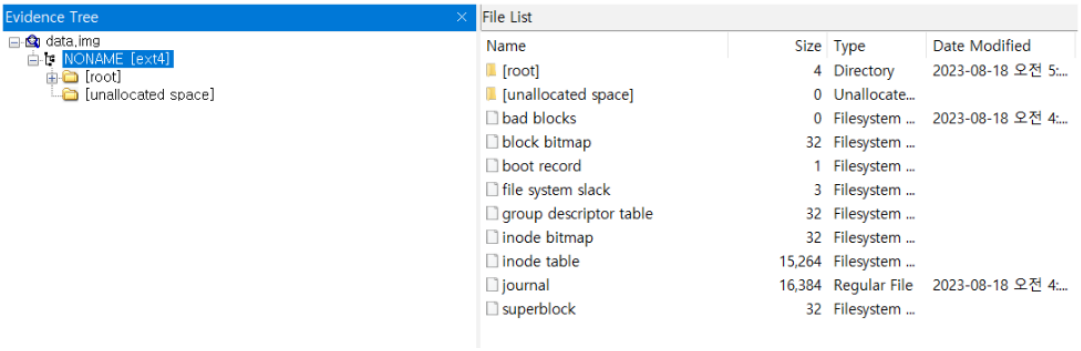


[사진 34] Blockchain Explorer(https://www.blockchain.com/explorer)에서 Wallet.txt에 기록되어 있는 지갑 주소 조회 결과

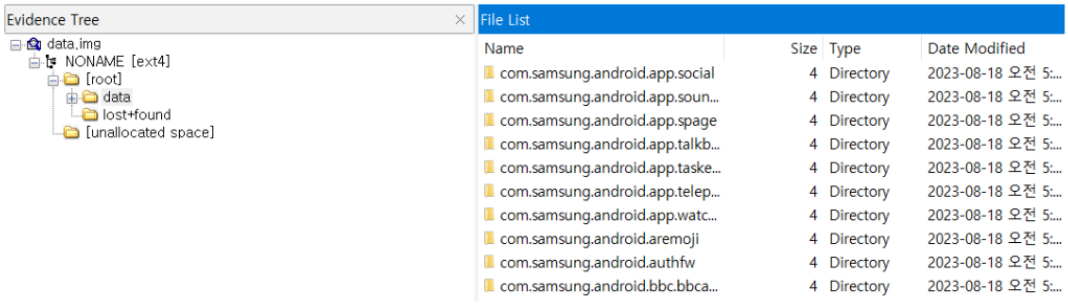


[사진 35] E: 드라이브 파티션에 저장되어 있는 data.img 파일

앞에서 복구했던 E: 드라이브 파티션에는 data.img 파일이 저장되어 있었다.

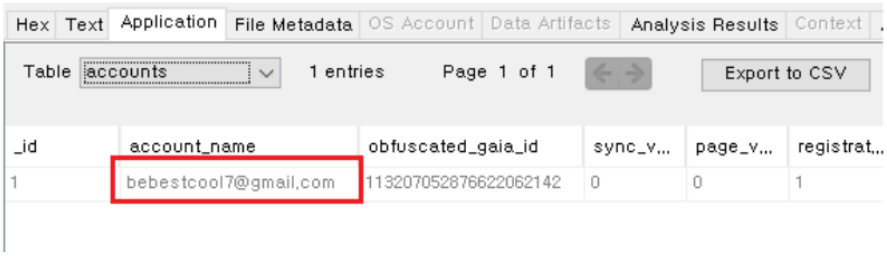


[사진 36] FTK Imager 도구로 열어본 data.img 파일



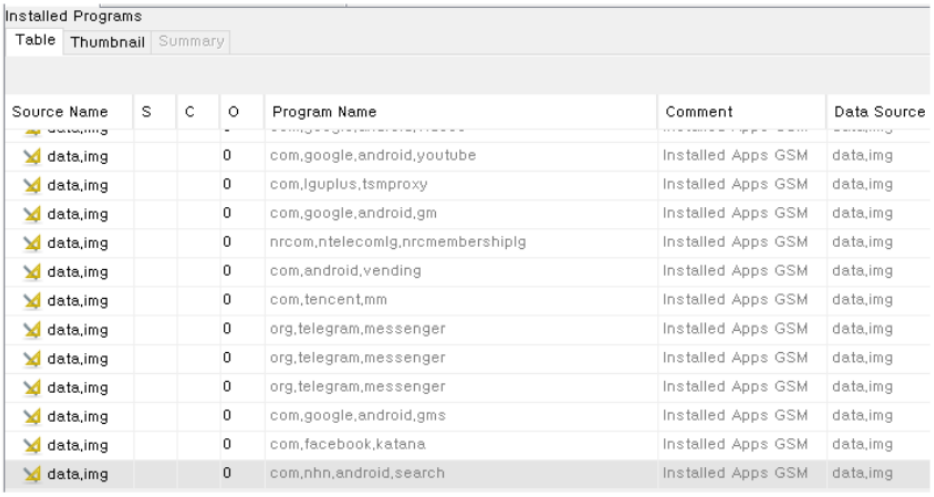
[사진 37] Android Samsung 스마트폰 이미지 파일 확인

data.img 파일을 FTK Imager로 열어보니 ext4 파일 시스템 이미지 파일이었으며 내부에는 com.samsung.android~ 와 같은 형식의 디렉터리가 존재하는 것으로 보아 Android Samsung 스마트폰의 이미지 파일로 확인하였다. 하지만 data 디렉터리만 존재하였으며 스마트폰 전체에 대한 이미지 파일은 아닌 것 같다는 생각을 하였다.



[사진 38] accounts.notifications.db 파일에서 확인한 등록된 구글 계정

accounts.notifications.db 파일에서 등록되어 있는 구글 계정 **bebestcool7@gmail.com**을 확인하였다.

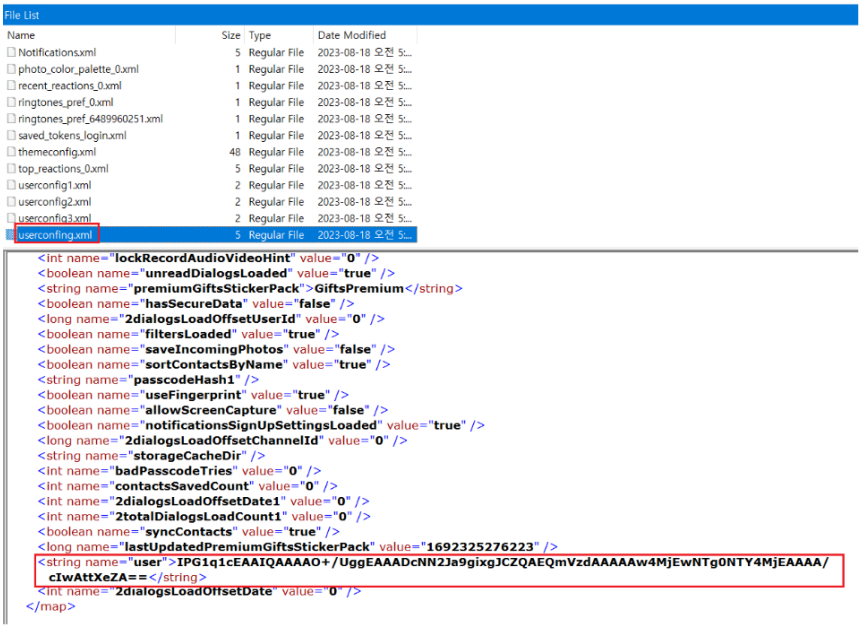


[사진 39] data.img 파일에서 확인한 설치되어 있는 앱 목록

data.img 파일에서 확인한 설치되어 있는 앱 목록 중 메신저 앱으로는 **Telegram, Wechat, Facebook으로 총 3개 앱**이 확인되었다.

설치되어 있는 메신저 앱
org.telegram.messenger (Telegram Messenger)
com.tencent.mm (Wechat)
com.facebook.katana (Facebook)

[표 12] 설치되어 있는 메신저 앱 목록



[사진 40] userconfig.xml 파일에 기록되어 있는 텔레그램 메신저 계정 정보

[사진 41] userconfig.xml <string name="user"> 태그 값 Base64 복호화

태그 안에 있는 값은 Base64 형식으로 인코딩 되어 있어 복호화하여 평문 정보를 확인하였다. 복호화 결과 평문은 **Be, Best, 821058456821**이 확인되었으며 태그에는 First Name과 Last Name 그리고 전화번호가 기록되는 것으로 볼 때 'Be'가 계정의 First Name이며 'Best'가 Last Name으로 유추할 수 있다.

accounts.notifications.db에서 확인한 "bebestcool7@gmail.com" 구글 계정에도 'bebest' 문자열이 포함되어 있는 것으로 **Be Best**를 텔레그램 계정 이름으로도 사용했을 가능성이 있다.

그리고 "821058456821" 값은 앞에 "82" 값이 대한민국 국가 번호인 "+82" 값으로 그 이후 값인 **1058456821**은 전호번호로 유추할 수 있다.

First Name	Be
Last Name	Best
Phone Number	(+82)010-5845-6821

[표 13] 텔리그램 메신저 계정 정보

테이블(T): data

모든 열에서 필터링

	id_only	is_primary	is_super_primary	data_version	data1	data2	data3	data4	data5
	필터	필터	필터	필터	필터	필터	필터	필터	필터
1	0	0	0	0	Be Cool	Be Cool	NULL	NULL	NULL
2	0	0	0	0	555222049	Telegram Profile	메시지 보내기 +821051087648	555222049	NULL
3	0	0	0	0	555222049	Telegram Voice Call	음성 통화 걸기 +821051087648	555222049	NULL
4	0	0	0	0	555222049	Telegram Video Call	영상 통화 걸기 +821051087648	555222049	NULL

[사진 42] contacts2.db 파일의 data 테이블에서 확인한 "Be Cool"

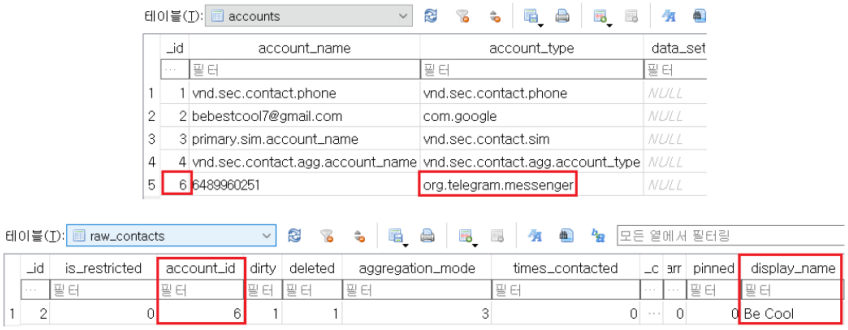
DB Browser for SQLite을 이용하여 contacts2.db 파일은 Samsung 연락처 앱에 기록된 연락처 정보가 저장되는 DB파일로 contacts2.db에는 텔레그램 메신저에 의해 추가된 연락처 정보도 확인할 수 있다.

[사진 42]은 contacts2.db 파일의 data 테이블에서 **'Be Cool' 문자열이 기록**되어 있는 것을 확인 하였다.

[사진 43] be_cool_1_1.png 이미지 파일에서 확인한 텔레그램 메신저 대화 상태 "Be cool"

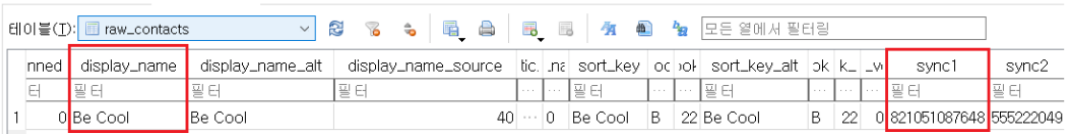
'Be Cool'은 텔레그램 메신저를 사용하여 A씨가 불법 스트리밍 사이트 관련하여 연락을 주고받은 대상이며 해외 불법 스트리밍 사이트 서버 운영자 정보를 알려준 사람이다.

'Be Cool' 이름이 contacts2.db에 기록되어 있는 것으로 보아 data.img이미지 파일을 추출한 대상 스마트폰에서 [사진 43]의 대화가 이루어진 것으로 보이며 해당 스크린샷의 출처로 볼 수 있을 것 같다.



[사진 44] contacts2.db accounts 테이블의 _id 값과 raw_contacts 테이블의 account_id 확인

raw_contacts 테이블에서 org.telegram.messenger의 id 값을 가진 행이 존재하였으며 해당 행의 display_name 칼럼값으로 "Be Cool"이 기록되어 있어 텔레그램 메신저를 통해 연락하였던 'Be Cool'임을 확인하였다.

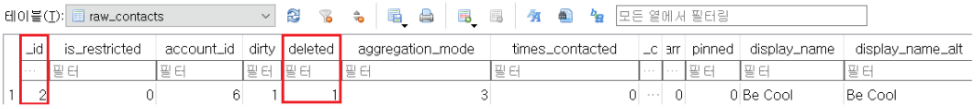


[사진 45] contacts2.db raw_contacts 테이블에서 확인한 'Be Cool'의 전화번호

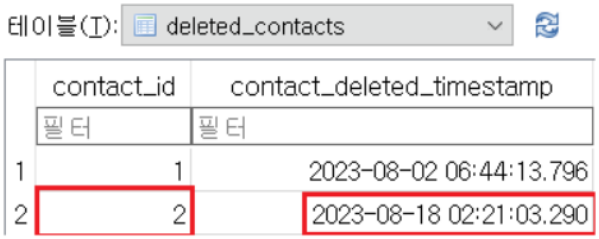
raw_contacts 테이블의 sync1 칼럼에 기록되어 있는 값을 통해 **'Be Cool'의 연락처 전화번호**를 확보하였다.

"Be Cool"의 연락처
(+82)010-5108-7648

[표 14] contacts2.db에서 확인한 텔레그램 메신저 'Be Cool'의 연락처



[사진 46] raw_contacts 테이블에서 확인한 텔레그램 메신저 'Be Cool'의 연락처 삭제 여부

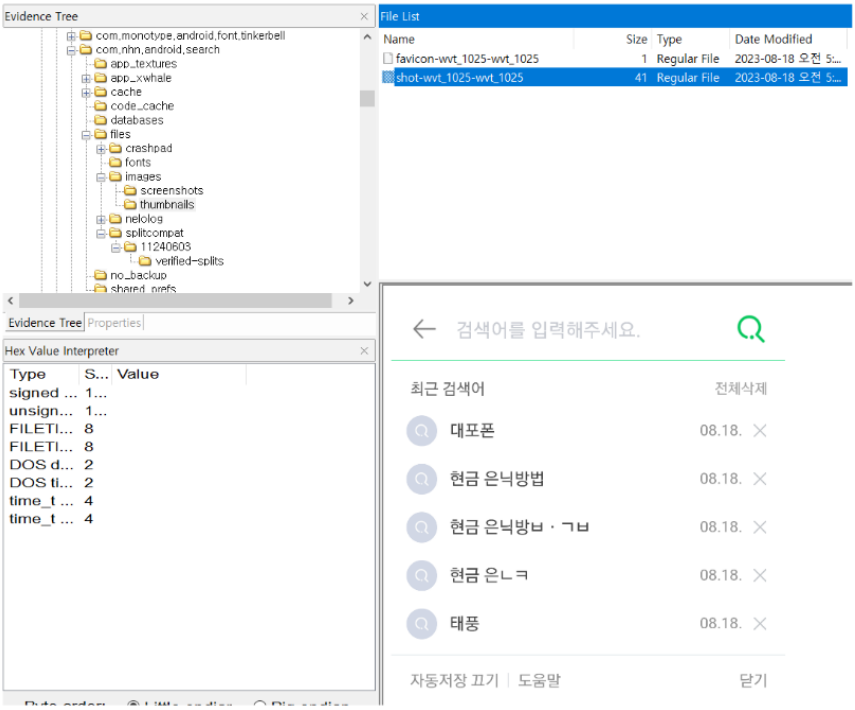


[사진 47] deleted_contacts 테이블에 기록되어 있는 'Be Cool'의 연락처 삭제 시간

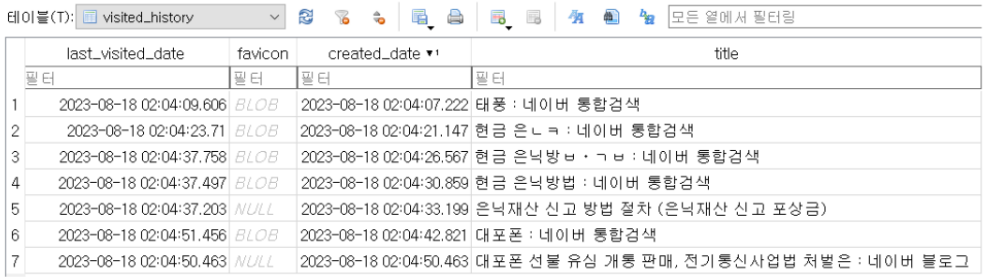
contacts2.db의 raw_contacts 테이블에서 'Be Cool' 행의 deleted 칼럼이 "1"로 **'Be Cool'의 연락처 정보가 삭제되어 있는 것을 확인**하였다. 텔레그램 메신저 'Be Cool'의 연락처 삭제 시점은 deleted_contacts 테이블의 contact_deleted_timestamp 칼럼에 기록되어 있어 확인 가능하였다.

텔레그램 메신저 'Be Cool'의 연락처 삭제 시점
2023-08-18 02:21:03.290 (UTC+0)

[표 15] 'Be Cool' 연락처 삭제 시점



[사진 48] shot-wvt_1025-wvt_1025 파일 네이버 앱 최근 검색어 목록 스크린샷



	last_visited_date	favicon	created_date	title
	필터	필터	필터	필터
1	2023-08-18 02:04:09.606	BLOB	2023-08-18 02:04:07.222	태풍 : 네이버 통합검색
2	2023-08-18 02:04:23.71	BLOB	2023-08-18 02:04:21.147	현금 은ㄴㅋ : 네이버 통합검색
3	2023-08-18 02:04:37.758	BLOB	2023-08-18 02:04:26.567	현금 은닉방ㅂ · ㄱㅂ : 네이버 통합검색
4	2023-08-18 02:04:37.497	BLOB	2023-08-18 02:04:30.859	현금 은닉방법 : 네이버 통합검색
5	2023-08-18 02:04:37.203	NULL	2023-08-18 02:04:33.199	은닉재산 신고 방법 절차 (은닉재산 신고 포상금)
6	2023-08-18 02:04:51.456	BLOB	2023-08-18 02:04:42.821	대포폰 : 네이버 통합검색
7	2023-08-18 02:04:50.463	NULL	2023-08-18 02:04:50.463	대포폰 선불 유심 개통 판매, 전기통신사업법 처벌은 : 네이버 블로그

[사진 49] search.db visited_history 테이블에서 확인한 네이버앱 검색기록

shot-wvt_1025-wvt_1025 파일로 **네이버 앱 검색창의 최근 검색어 목록이 보이는 스크린샷 이미지 파일이 존재**하였다.

해당 스크린샷 이미지에서 확인한 최근 검색어 목록으로는 "대포폰", "현금 은닉방법"등이 있었으며 해당 검색기록은 **search.db 파일에서도 확인**하였다

5. Flag

1. 해당 사건은 어떤 법률을 위반하였으며, 벌칙사항 또한 기재하고 설명하여라.

해당 사건은 불법 스트리밍 사이트를 운영함으로써 저작권이 있는 영상 매체들(방송 프로그램, 영화 등)을 저작재산권자의 허락 없이 업로드하여 불특정 다수에게 제공하는 것으로 **[저작권법] 제 16조 (복제권)** 을 침해한다.

그리고 불법 스트리밍 사이트를 운영하여 저작재산권자 허락 없이 불특정 다수 공중이 수신하거나 접근하게 할 목적으로 무선 또는 유선 통신의 방법에 의하여 송신하거나 이용에 제공하는 것으로 **[저작권법] 제 18조(공중송신권)** 또한 침해하고있다.

A씨는 국내에서 불법 스트리밍 사이트를 개설 및 운영하여 불특정 다수를 대상으로 저작 재산권자의 이용허락없이 영상매체들을 배포, 공중송신, 복제를 함으로서 **[저작권법] 제 16조(복제권)** 및 **[저작권법] 제 18조(공중송신권)**을 침해하며 **[저작권법] 제 136조 제 1항에 의하여 5년 이하의 징역 또는 5천만원 이하의 벌금**에 처한다.

- [저작권법] 제16조(복제권)
저작자는 그의 저작물을 복제할 권리를 가진다.

-[저작권법] 제18조(공중송신권)
저작자는 그의 저작물을 공중송신할 권리를 가진다.

-[저작권법] 제136조(벌칙)
① 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처하거나 이를 병과(병과)할 수 있다.<개정 2011.12.2, 2021.5.18>

1. 저작재산권, 그 밖에 이 법에 따라 보호되는 재산적 권리(제93조에 따른 권리는 제외한다)를 복제, 공연, 공중송신, 전시, 배포, 대여, 2차적저작물 작성의 방법으로 침해한 자

2. 제129조의3제1항에 따른 법원의 명령을 정당한 이유 없이 위반한 자

2. 해외에 접속한 데이터 서버에 대한 정보 및 운영자 정보, 위치 등을 분석하여라.

탤레그램 메신저 대화 내역 스크린샷 이미지 파일로부터 A씨와 'Be Cool' 이름의 상대가 문자를 주고 받은 흔적을 발견 하였으며 "경력증명서_기업일반.pptx" 파일은 hwpx 확장자 문서 파일로 확인되어 해당 문서 파일에서 해외 불법 스트리밍 서버 운영자로 추정되는 사람의 한국 이름과 근무경력사항에 대한 정보를 확인하였다.

1) A씨가 'Be Cool'에게 데이터 운영에 대한 부분을 물어보며 이에 'Be Cool'은 불법 스트리밍 서버에 음란물과 드라마 10,000개를 업로드 하였다고 대답하는 것으로 볼 때 'Be Cool' 이름의 텔레그램 사용자는 해외 불법 스트리밍 서버를 관리하는 운영자로 추정된다.

2) A씨가 고객들이 운영자 정보를 요청한다며 운영자 정보를 'Be Cool'에게 요구하자 운영자의 이름, 나이, 거주 정보를 Base64 방식으로 인코딩 하여 A씨에게 알려주고 있었다. 운영자 정보가 담긴 Base64 인코딩 문자 복호화 결과 운영자 이름은 'Jack' 이며 나이는 29살이고 현재 해외 거주 중임을 알 수 있었다.

3) 경력증명서_기업일반.pptx 파일에서 확인한 hwp 형식의 경력증명서에서 텔리그램 메신저 대화 스크린샷에서 확인하였던 해외 불법 스트리밍 서버 운영자 이름으로 추정되는 'Jack'의 한국명 "김호준"과 (사)한국포렌식학회 기관에서 2021년 8월 1일부터 2022년 12월 31일까지 근무한 경력을 확인할 수 있었다.

3. 광고주들과의 금전관계 및 금전 전달 등을 입증할 수 있는 정보를 모두 분석하여라.

텔레그램 메신저 대화 내역 스크린샷 이미지 파일로부터 A씨가 금전적인 수익을 비트 코인 지갑을 통해 받고 있는 흔적 발견하였다.

1) A씨가 비트코인 지갑을 만들어 수금을 하고있다는 언급을 한 것으로 볼 때 A씨는 불법 스트리밍 사이트 운영을 하면서 얻은 광고 수익을 비트코인을 통해 받고 있는것으로 추정할 수 있다.

2) A씨가 'Be Cool'에게 지갑 주소를 알려준다며 주소가 담긴 압축파일을 전달하는 언급이 있었으며 'Be Cool'에게 전달한 압축파일로 추정되는 Wallet.zip 파일을 찾았으며 해당 압축파일의 비밀번호는 "202308"로 확인 하였다. 내부에는 Wallet.txt 파일로 가상화폐 지갑 주소로 추정되는 문자열이 기록되어 있었지만 지갑주소 조회 결과가 없었다.

6. 별도 첨부

문제 내용

문화체육관광부 소속 특별사법경찰관 甲과 문화체육관광부 소속기관인 한국저작권보호원은 불법 영상저작물 유통 사이트 운영 관련 저작권 침해 범죄에 대한 조사과정 중
해외에 데이터 서버 등을 활용하여 불법으로 제작·복제된 방송영상물을 국내에 불법 스트리밍 사이트를 개설하여 불특정 다수를 대상으로 스트리밍 서비스를 제공하는 A가 있다는 첩보를 입수하게 되었다.
이후 대검찰청 사이버수사과 수사관 乙과 함께 수사를 진행하여, 국내 불법 스트리밍 사이트 운영자 A의 실제 운영을 위해 거주한 오피스텔에 대한 압수영장을 발부받았다. 디지털 포렌식을 통해 불법 영상 스트리밍에 직접 사용한 Windows 운영 PC와 모바일 전체 데이터에 대한 이미징 작업을 진행한 후, 증거를 분석하게 되었다.
피압수자 A를 조사하는 과정에서, 국내 개설된 불법 스트리밍 사이트는 불법 영상 스트리밍 서비스를 이용하고자 하는 불특정 다수를 대상으로 불법 도박 및 음란 사이트 링크 등을 홍보할 때 발생하는 광고 수입을 목적으로 운영된 것으로 드러났다.
하지만 피압수자 A는 브로커가 알려준 IP를 통해 해외에 구축된 데이터 서버에 접속하였을 뿐 해외에 서버를 운영하는 운영자에 대한 정보를 전혀 알지 못한다고 진술하고 있다. 또한 불법 도박 사이트 및 음란 사이트 광고 수입에 대한 일체의 범죄사실을 모두 부인하고 있다.

[문제]
압수한 Windows 운영 PC를 디지털 포렌식 수사를 통해 분석하여
1. 해당 사건은 어떤 법률을 위반하였으며, 벌칙사항 또한 기재하고 설명하여라.
2. 해외에 접속한 데이터 서버에 대한 정보 및 운영자 정보, 위치 등을 분석하여라.
3. 광고주들과의 금전관계 및 금전 전달 등을 입증할 수 있는 정보를 모두 분석하여라.

추가 분석도구

도구명	다운로드 링크	Version
HashCalc	https://hashcalc.software.informer.com/download/	2.02
DB Browser for SQLite	https://sqlitebrowser.org/dl/	3.12.2
John The Ripper	https://www.openwall.com/john/	1.9.0
HxD	https://mh-nexus.de/en/hxd/	2.5.0.0
Thumbcache_viewer	https://thumbcacheviewer.github.io/	1.0.3.7
Windows 한컴오피스 Viewer	https://www.hancom.com/main/main.do	9.6.1.10368

7. Reference

- https://zero-min.tistory.com/entry/%EB%A6%AC%EB%88%85%EC%8A%A4Linux-John-the-Ripper-%EB%8B%A4%EC%9A%B4%EC%82%AC%EC%9A%A9%EB%B2%95
- https://velog.io/@yys7517/Android-Android%EC%97%90%EC%84%9C-QR%EC%BD%94%EB%93%9C-%EB%8B%A4%EB%A4%84%EB%B3%B4%EA%B8%B0
- https://seong6496.tistory.com/233
- https://vinssy.tistory.com/entry/John-the-ripper%EB%A5%BC-%EC%9D%B4%EC%9A%A9%ED%95%98%EC%97%AC-%EC%95%95%EC%B6%95-%ED%8C%8C%EC%9D%BC-%EB%B9%84%EB%B0%80%EB%B2%88%ED%98%B8-%EC%95%8C%EC%95%84%EB%82%B4%EA%B8%B0
- https://aquasosal.tistory.com/20