[DFC 2022 - 402] Write-Up

작성자	윤지원
분석 일자	2024.05.23
작성 일자	2024.05.23
분석 대상	USB.dd
문서 버전	2.0
작성자 E-mail	yoonjw0827@gmail.com

0. 목차

1. 문제 3
2. 분석 도구 3
3. 환경 3
4. Write-Up 4
5. Flag 10
6. 별도 첨부 11
7. Reference 12

1. 문제

URL	-
문제 내용	Description While analyzing the drug suspect's PC, the police found traces of accessing Dropbox through a web browser while the USB was connected. The download history of the web browser is all deleted, so it is not known for sure, but it is suspected that some files were downloaded from Dropbox to USB. Analyze the USB image to find the files that are suspected to have been downloaded from Dropbox and find related files. Questions 1.What file(s) did the suspect download from Dropbox? 2.Find completely deleted files in USB. 3.What is the content of the first file that was completely deleted? (Hint: Person) 4.What is the content of the second file that was completely deleted? (Hint: Appointment)
문제 파일	USB.dd
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	4.7.1.2
NTFS Log Tracker	https://sites.google.com/site/forensicnote/ntfs-log-tracker	1.71
DB Browser(SQLite)	https://sqlitebrowser.org/dl/	3.12.2
HxD	https://mh-nexus.de/en/downloads.php?product=HxD20	2.5

3. 환경

OS
Windows 11 64-bit

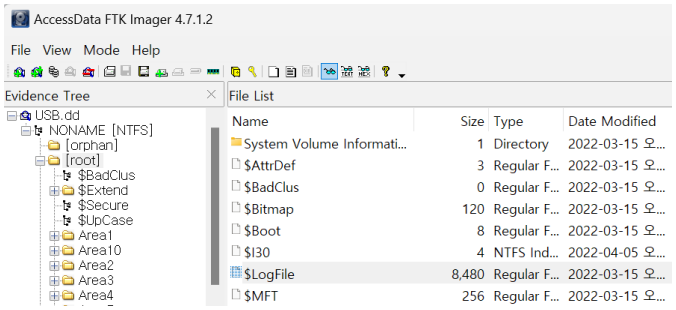
4. Write-Up

파일명	USB.dd
용량	3.72GB
SHA256	a9e6ff0e411ae94cfd542cf2f680b4c602be90adf0872b9ff893d3dcb7ea8ff1
Timestamp	2022-07-29 2:21:08

이 문제를 요약하자면, 마약 용의자의 PC 에서 USB 가 연결된 상태에서 웹브라우저를 통해 드롭박스에 접속한 흔적을 발견하여 다운로드된 것으로 의심되는 파일을 찾는 것이다.

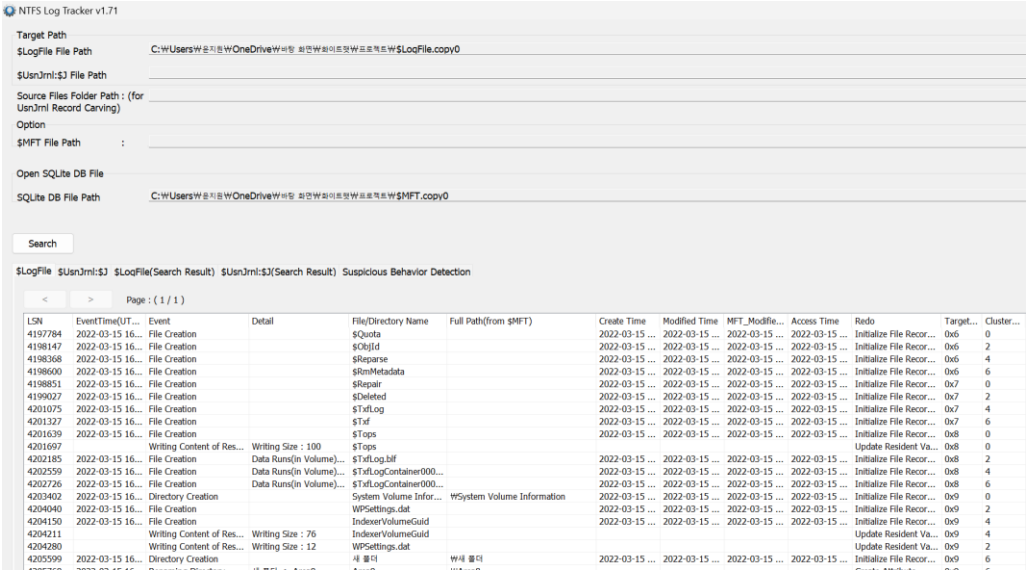
1. 용의자는 dropbox 에서 어떤 파일을 다운로드 받았는가?

우선 FTK Imager 로 USB.dd 파일을 열어보았다. [root]에 익숙한 $LogFile 과 $MFT 파일이 존재하는 것을 볼 수 있었다. 이 두 파일을 추출하여 NFTS Log Tracker 에 넣어보았다.



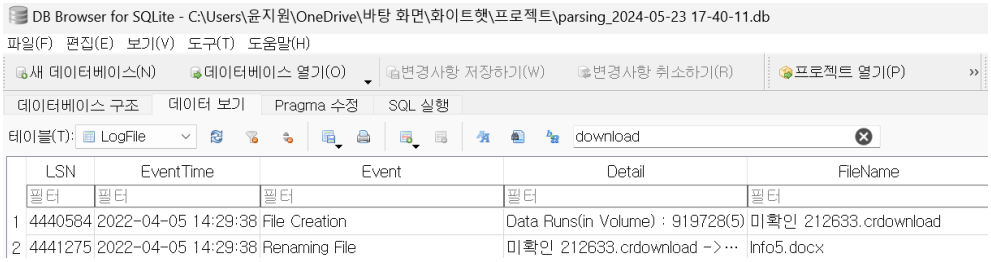
[사진 1] $LogFile과 $MFT 파일이 존재

$UsnJrnl 파일은 없었기 때문에 두 파일로만 파싱을 진행하면 [사진 2]와 같다.



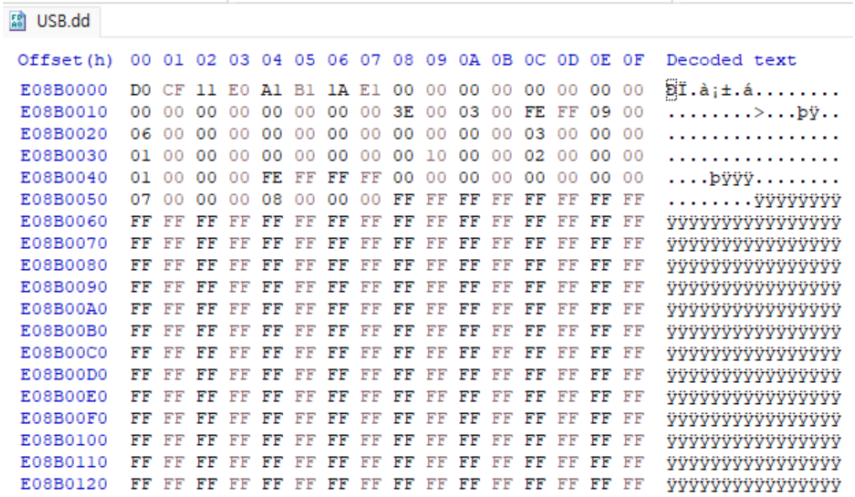
[사진 2] $LogFile과 $MFT 파싱

파싱한 데이터를 데이터베이스 파일로 뽑아냈기 때문에 DB Browser for SQLite 로 분석을 진행하였다. LogFile 테이블에서 다운로드를 한 흔적을 찾기 위해 download 를 검색하니 [사진 3]과 같은 결과가 나왔다. LSN 이 4440584 부분에서 212633.crdownload 라는 파일이 생성된 것을 확인할 수 있었다. Detail 부분을 통해 클러스터 볼륨 919728 에 저장된 것도 알 수 있다.



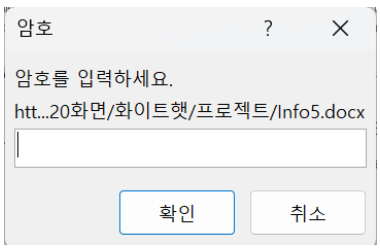
[사진 3] download 검색하여 흔적 확인

저장된 파일을 확인하기 위해 HxD 로 USB.dd 파일을 열어보았다. 클러스터 볼륨 값인 919728 에 8 을 곱한 값인 7357824 로 섹터 이동을 하면 212633.crdownload 파일을 확인할 수 있다는 사실을 알아낸 후 섹터 이동을 진행했다.



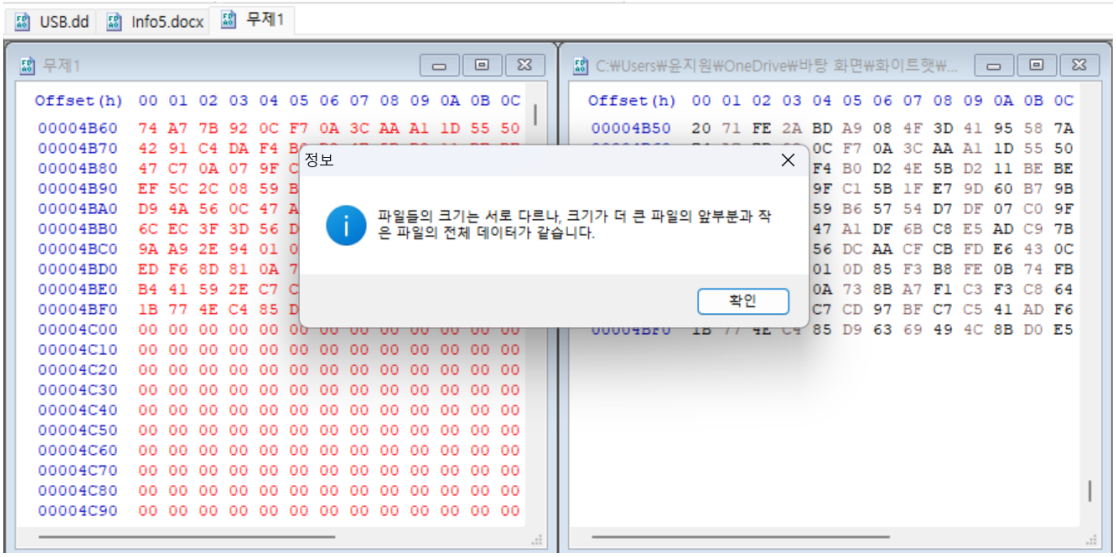
[사진 4] 212633.crdownload 확인

[사진 3]의 2 번째 줄에서 renaming file 이 된 것으로 보아 이 파일은 이름이 info5.docx 로 바뀐 것을 알 수 있다. 또한 이 파일이 OLE 형식으로 되어있기 때문에 docx 파일 암호화가 되어있을 것으로 예상하여 Info5.docx 를 FTK Imager 에서 찾아서 Export 로 추출하였다.



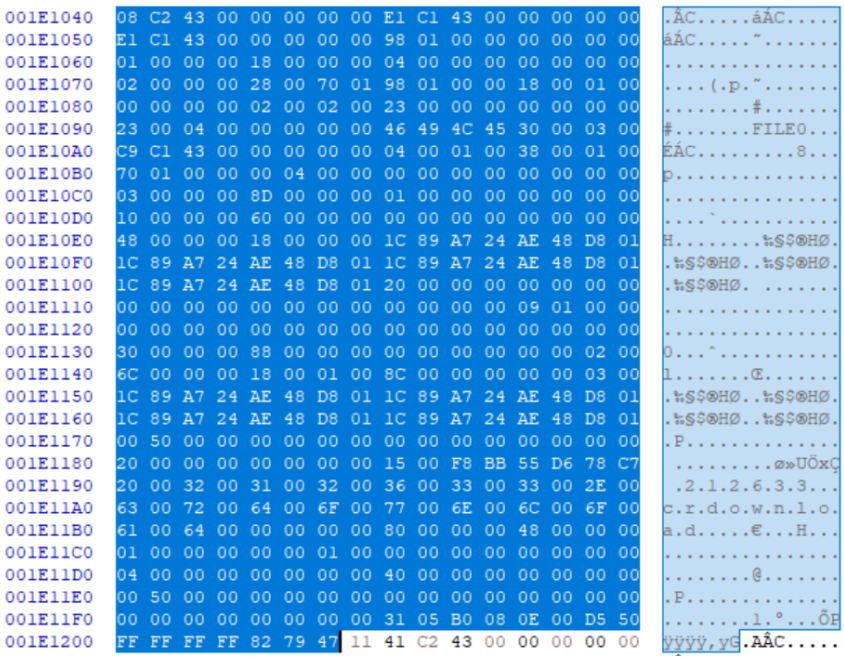
[사진 5] Info5.docx 파일이 암호화되어 있는 모습

[사진 5]와 같이 추출한 파일이 암호화되어 있음을 확인하고 이 Info5.docx 도 HxD 에 넣어보았다. 그런 다음 [사진 4]에서 볼 수 있는 섹터 7357824 인 오프셋 0xE08B000 부터 끝까지 hex 값을 복사하여 새로운 파일을 만들어 붙여넣기 한 후, Info5.docx 와 데이터 비교하면 [사진 6]과 같이 데이터가 같다는 것을 알 수 있다. 이를 통해 212633.crdownload 가 Info5.docx 와 동일하다는 것을 보여준다.



[사진 6] Info5.docx와 데이터 비교

dropbox에서 다운 받은 파일을 알아내는 것이 목적이기 때문에 다운로드 기록을 살펴보기로 하였고, LSN 기반으로 분석을 진행했다. $LogFile도 HxD에 넣은 다음, volume 919728에 기록된 LSN 4440584를 Hxd에서 검색해보면 [사진 7]과 같이 0x1E1040에서 $MFT와 결합된 구조로 나타난다.



[사진 7] $LogFile에서 LSN 4440584를 검색한 결과

또한 [사진 8]을 통해 LSN 4441836을 확인할 수 있는데, 이는 HostUrl을 통해 dropbox에서의 다운로드 흔적임을 알 수 있다.

```
001E4480  00 00 00 00 00 00 00 00 EC C6 43 00 00 00 00 00  ........ìÆC.....
001E4490  92 C8 43 00 00 00 00 00 00 00 00 00 00 00 00 00  'ÈC.............
001E44A0  00 00 00 00 00 00 00 00 C0 01 00 00 00 00 00 00  ........À.......
001E44B0  01 00 00 00 18 00 00 00 02 00 00 00 00 00 00 00  ................
001E44C0  06 00 05 00 28 00 00 00 28 00 98 01 18 00 01 00  ....(...(.˜.....
001E44D0  50 01 00 00 02 00 02 00 23 00 00 00 00 00 00 00  P.......#.......
001E44E0  23 00 04 00 00 00 00 00 80 00 00 00 98 01 00 00  #.......€...˜...
001E44F0  00 0F 18 00 00 00 04 00 5B 01 00 00 38 00 00 00  ........[...8...
001E4500  5A 00 6F 00 6E 00 65 00 2E 00 49 00 64 00 65 00  Z.o.n.e...I.d.e.
001E4510  6E 00 74 00 69 00 66 00 69 00 65 00 72 00 00 00  n.t.i.f.i.e.r...
001E4520  5B 5A 6F 6E 65 54 72 61 6E 73 66 65 72 5D 0D 0A  [ZoneTransfer]..
001E4530  5A 6F 6E 65 49 64 3D 33 0D 0A 52 65 66 65 72 72  ZoneId=3..Referr
001E4540  65 72 55 72 6C 3D 68 74 74 70 73 3A 2F 2F 77 77  erUrl=https://ww
001E4550  77 2E 64 72 6F 70 62 6F 78 2E 63 6F 6D 2F 0D 0A  w.dropbox.com/..
001E4560  48 6F 73 74 55 72 6C 3D 68 74 74 70 73 3A 2F 2F  HostUrl=https://
001E4570  75 63 62 35 66 33 39 31 36 32 65 30 62 35 66 63  ucb5f39162e0b5fc
001E4580  38 66 64 34 65 36 31 34 36 64 66 66 2E 64 6C 2E  8fd4e6146dff.dl.
001E4590  64 72 6F 70 62 6F 78 75 73 65 72 63 6F 6E 74 65  dropboxuserconte
001E45A0  6E 74 2E 63 6F 6D 2F 63 64 2F 30 2F 67 65 74 2F  nt.com/cd/0/get/
001E45B0  42 6A 62 32 69 54 30 75 45 69 6B 39 43 6A 63 42  Bjb2iT0uEik9CjcB
001E45C0  53 36 76 7A 65 76 58 6B 39 56 57 69 57 6F 30 67  S6vzevXk9VWiWo0g
001E45D0  6C 6A 71 6E 5F 39 75 5F 65 6B 46 44 35 64 74 70  ljqn_9u_ekFD5dtp
001E45E0  79 6A 5A 72 61 65 48 75 56 6A 4E 50 6E 54 5F 4B  yjZraeHuVjNPnT_K
001E45F0  49 61 66 34 5F 4A 51 67 33 5A 41 47 6A 39 D8 50  Iaf4_JQg3ZAGj9ØP
001E4600  6B 35 39 4F 35 75 32 44 36 4F 57 5A 64 67 53 41  k59O5u2D6OWZdgSA
001E4610  42 43 69 6D 74 4B 54 50 42 32 70 48 78 4F 58 31  BCimtKTPB2pHxOX1
001E4620  6D 58 6B 56 74 72 39 68 68 49 43 72 70 64 75 62  mXkVtr9hhICrpdub
001E4630  71 63 6F 67 78 32 68 76 58 58 53 49 62 68 6F 58  qcogx2hvXXSIbhoX
001E4640  4C 52 4A 61 70 6F 62 6B 33 79 52 71 55 7A 50 39  LRJapobk3yRqUzP9
001E4650  30 43 41 67 7A 51 35 4B 6C 7A 51 2D 30 4B 50 75  0CAgzQ5KlzQ-0KPu
001E4660  6D 47 78 5A 2D 46 74 73 73 55 66 41 4C 30 59 54  mGxZ-FtssUfAL0YT
001E4670  67 6B 49 2F 66 69 6C 65 23 0D 0A 00 00 00 00 00  gkI/file#.......
```

[사진 8] dropbox에서의 다운로드 흔적

5	4441275	2022-04-05 14:29:38	Renaming File	미확인 212633.crdownload -> Info5.docx	Info5.docx
6	4444553	2022-04-05 14:31:32	File Creation		2_2_5_a.txt

[사진 9] LSN 4441275와 4444553

[사진 9]에서 나타나는 범위 안에 [사진 8]이 들어가있기 때문에 해당 **212633.crdownload**는 dropbox에서 다운로드되었다고 볼 수 있다.

2. 완전히 삭제된 파일을 USB에서 찾아라.

파일을 완전히 삭제했을 때는 파일명의 길이가 원본 파일명과 동일하고, 파일명 자체는 숫자, 문자, 특수문자 조합으로 변경된다는 점을 알 수 있었다. 또한 마지막에 파일 삭제가 일어나면 비정상적인 파일 시간 정보를 가진다는 것도 특징이었다.

[사진 10]을 살펴보면 파일 삭제 기록을 볼 수 있는데, 총 2개의 파일명을 볼 수 있다. 3번과 4번 문제에서도 완전히 삭제된 첫 번째 파일과 두 번째 파일의 내용을 묻고 있는 것으로 보아 이 파일들을 물어보는 것이 맞는 것 같다. 따라서 **2_2_5_a.txt와 2_2_5_b.txt** 파일이 완전히 삭제된 파일이다.

4455267	2022-04-05 14:34:11	Renaming File	2_2_5_b.txt -> `7a}w377k[P
4455580	2022-04-05 14:34:11	Renaming File	`7a}w377k[P -> ZuTeo4zuR`q
4455885	2022-04-05 14:34:11	Renaming File	ZuTeo4zuR`q -> iB(jRcfcrK=
4456200	2022-04-05 14:34:11	Renaming File	iB(jRcfcrK= -> 7pvuDpZg!_Y
4456516	2022-04-05 14:34:11	Renaming File	7pvuDpZg!_Y -> S3vzt70Bi=3
4456821	2022-04-05 14:34:11	Renaming File	S3vzt70Bi=3 -> /}ykHG-bpa!
4457134	2022-04-05 14:34:11	Renaming File	/}ykHG-bpa! -> +w78CQ}-=D1
4457364	2022-04-05 14:34:11	File Deletion	Abnormal Timestamp (1601-01-01 00:00:00)
4458164	2022-04-05 14:34:11	Renaming File	2_2_5_a.txt -> 3bG[Ja{iczA
4459101	2022-04-05 14:34:11	Renaming File	3bG[Ja{iczA -> VF+i1YD}ege
4459721	2022-04-05 14:34:11	Renaming File	VF+i1YD}ege -> YX3XOAFk12Y
4460026	2022-04-05 14:34:11	Renaming File	YX3XOAFk12Y -> UpPsjG97iv!
4460242	2022-04-05 14:34:11	File Deletion	Abnormal Timestamp (1601-01-01 00:00:00)

[사진 10] 파일 삭제 기록

3. 처음에 완전히 삭제된 파일의 내용은 무엇인가? (힌트 : 인물)

테이블(T): LogFile 2_2_5_a.txt

	필터	필터	필터	필터
1	4444553	2022-04-05 14:31:32	File Creation	
2	4444636	2022-04-05 14:31:32	File Deletion	
3	4444792	2022-04-05 14:31:32	File Creation	
4	4444988		Writing Content of Non-Residen…	Data Runs(in Volume) : 919726(1)
5	4445891		Writing Content of Non-Residen…	Data Runs(in Volume) : 919733(1)
6	4446201		Writing Content of Non-Residen…	Data Runs(in Volume) : 919734(1)
7	4446519		Writing Content of Non-Residen…	Data Runs(in Volume) : 919735(1)
8	4447422		Writing Content of Non-Residen…	Data Runs(in Volume) : 919726(1)
9	4448143		Writing Content of Non-Residen…	Data Runs(in Volume) : 919733(1)

[사진 11] 2_2_5_a.txt를 LogFile 테이블에서 검색한 결과

[사진 11]과 같이 검색하면 [사진 3]과 같이 클러스터 볼륨이 Detail에 나와있다. 따라서 이를 HxD의 USB.dd에서 검색해보았다. 이 볼륨들 중 하나인 919735에 8을 곱한 섹터 7357880으로 이동한 다음 조금 아래를 살펴보면 [사진 12]와 같이 인물의 정보를 발견할 수 있다.

```
E08B71C0  09 09 09 09 20 20 0D 0A 4E 61 6D 65 20 3A 20 47  ....  ..Name : G
E08B71D0  61 65 6C 0D 0A 48 61 69 72 20 63 6F 6C 6F 72 20  ael..Hair color
E08B71E0  3A 20 47 72 65 65 6E 0D 0A 43 6C 6F 74 68 65 73  : Green..Clothes
E08B71F0  20 3A 20 47 72 61 79 20 70 61 6E 74 73 0D 0A 09   : Gray pants...
```

[사진 12] 발견한 인물 정보

문제의 힌트가 인물이기 때문에 다음 정보가 삭제된 파일의 내용이라고 생각하였다.

Name : Gael

Hair color : Green

Clothes : Gray pants

4. 두 번째로 완전히 삭제된 파일의 내용은 무엇인가? (힌트 : 약속)

3번 문제와 비슷하게 우선 LogFile 테이블에 2_2_5_b.txt부터 검색해보았다. 이 파일은 Resident File이라고 되어 있는데 일단은 이전과 비슷하게 3개의 LSN을 HxD의 USB.dd에서 검색해보았다.

테이블(T): LogFile 2_2_5_b.txt

	LSN	EventTime	Event	
	필터	필터	필터	필터
1	4449501	2022-04-05 14:32:16	File Creation	
2	4449584	2022-04-05 14:32:16	File Deletion	
3	4449732	2022-04-05 14:32:16	File Creation	
4	4449800		Writing Content of Resident File	Writing Size : 69
5	4450760		Writing Content of Resident File	Writing Size : 67
6	4451571		Writing Content of Resident File	Writing Size : 69
7	4452100	2022-04-05 14:33:38	File Creation	
8	4452160		Writing Content of Resident File	Writing Size : 7

[사진 13] 2_2_5_b.txt를 LogFile 테이블에서 검색한 결과

각각의 LSN 를 살펴보면 특별히 보이는 값이 없었다. 그래서 가장 큰 LSN 값과 가장 작은 LSN 값 사이에 정보가 있지 않을까 생각해보았다. 따라서 그 사이를 쭉 보다가 [사진 14]와 같은 값을 발견하였다.

```
001F4AE0  44 61 74 65 20 26 20 54 69 6D 65 20 3A 20 32 30   Date & Time : 20
001F4AF0  32 32 2F 30 36 2F 31 31 20 31 33 3A 30 30 20 7E   22/06/11 13:00 ~
001F4B00  20 31 33 3A 33 30 0D 0A 4C 6F 63 61 74 69 6F 6E    13:30..Location
001F4B10  20 3A 20 31 33 20 73 6F 75 74 68 20 31 31 72 64    : 13 south 11rd
001F4B20  20 53 74 0D 0A 00 00 00 65 E9 43 00 00 00 00 00    St.....eéC.....
```

[사진 14] LSN 4449800과 44451571 사이에서 발견된 정보

날짜와 시간, 위치까지 적혀있는 것으로 보아 문제의 힌트인 약속에 대한 내용이 확실하다. 따라서 정답은 다음과 같다.

Date & Time : 2022/06/11 13:00 ~ 13:30

Location : 13 south 11rd St

5. Flag

1번 : 212633.crdownload

2번 : 2_2_5_a.txt, 2_2_5_b.txt

3번 :

Name : Gael

Hair color : Green

Clothes : Gray pants

4번 :

Date & Time : 2022/06/11 13:00 ~ 13:30

Location : 13 south 11rd St

6. 별도 첨부

7. Reference

- [URL]