104 – Find Secret Documents

Team Information

Team Name : ISEGYE_IDOL

Team Member : Eungchang Lee, Sojeong Kim, Mingyu Seong, Donghyun HA

Email Address : dfc-isegyeidol@googlegroups.com

Instructions

Description As a security manager, you searched Trudy's office on a tip that Trudy tried to divulge confidential data. An unauthorized USB was found and imaged for forensic investigation.

Target	Hash (MD5)
Trudy's_USB.bin	B4C2A2F1F98B8472F3B353012F06CD74

Questions

1) Identify Partition Type, Partition Name, Volume Serial Number, and Size of the USB's partition(s) (20 points)

2) Find all the data Trudy tried to hide and leak and calculate the MD5 hash of the data. (80 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:	Md5Checker	Publisher:	nf_xp
Version:	3.3		
URL:	http://getmd5checker.com/download		

Name:	FTK Imager	Publisher:	AccessData
Version:	4.2.1.4		
URL:	https://accessdata.com/		

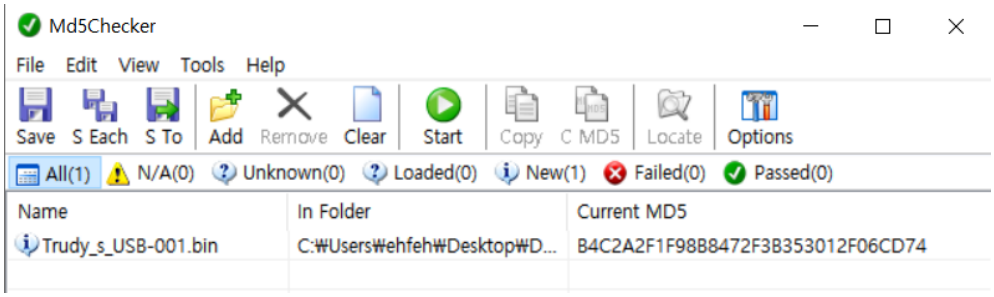
Name:	Winhex	Publisher:	X-ways
Version:	19.0 SR-6		
URL:	https://x-ways.net/winhex/		

Name:	R-STUDIO	Publisher:	R-Tools Technology
Version:	8.3.168003		
URL:	https://www.r-tt.com/		

Name:	Cyberchef	Publisher:	Crown
Version:	9.46.0		
URL:	https://gchq.github.io/CyberChef/		

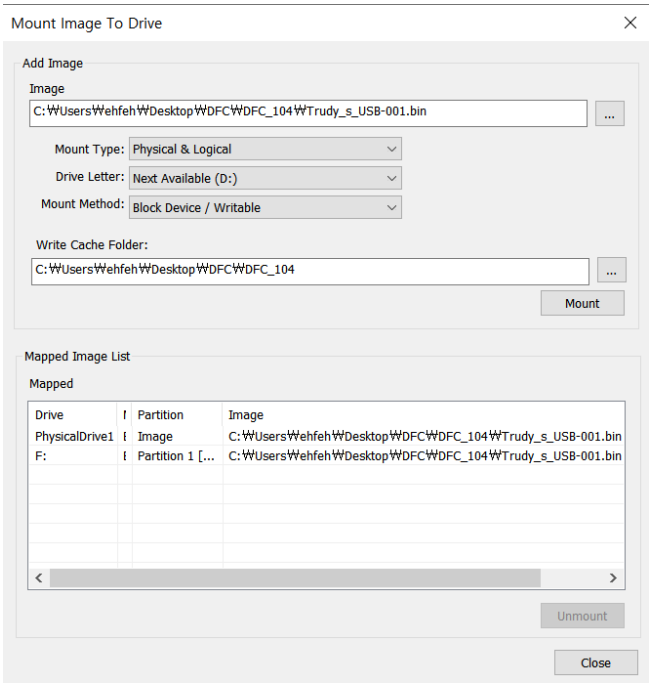
Step-by-step methodology:

1) Identify Partition Type, Partition Name, Volume Serial Number, and Size of the USB's partition(s) (20 points)



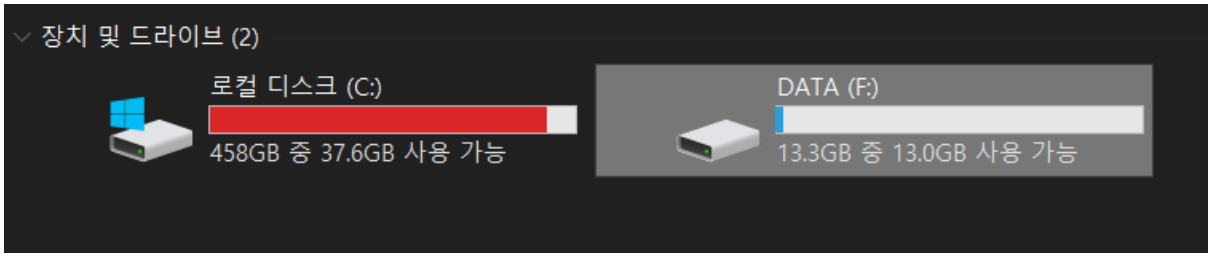
[그림 1]. MD5 check

분석해야 할 target binary 파일의 MD5는 [그림 1]을 통해 다운받기 위한 파일의 MD5와 같음을 확인한다.



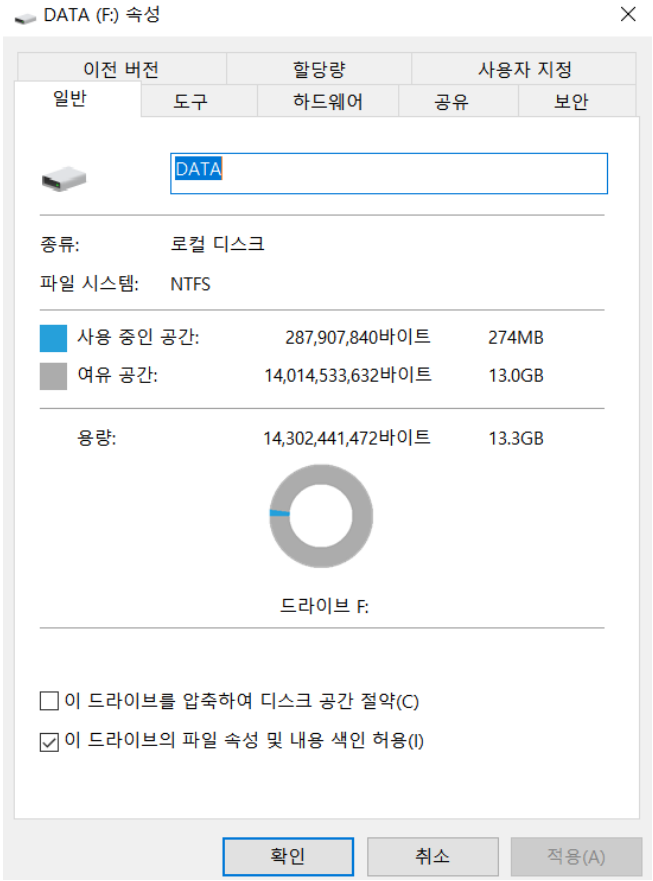
[그림 2]. FTK Imager mount

Partition에 대한 정보를 얻기 위해 FTK Imager를 통해 해당 usb 바이너리 이미지를 F: 로 마운트 작업을 수행했다.



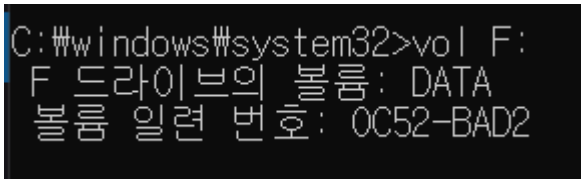
[그림 3]. disk mount check

[그림 3]에서 disk가 정상적으로 마운트 된 것을 확인할 수 있다.



[그림 4]. disk property

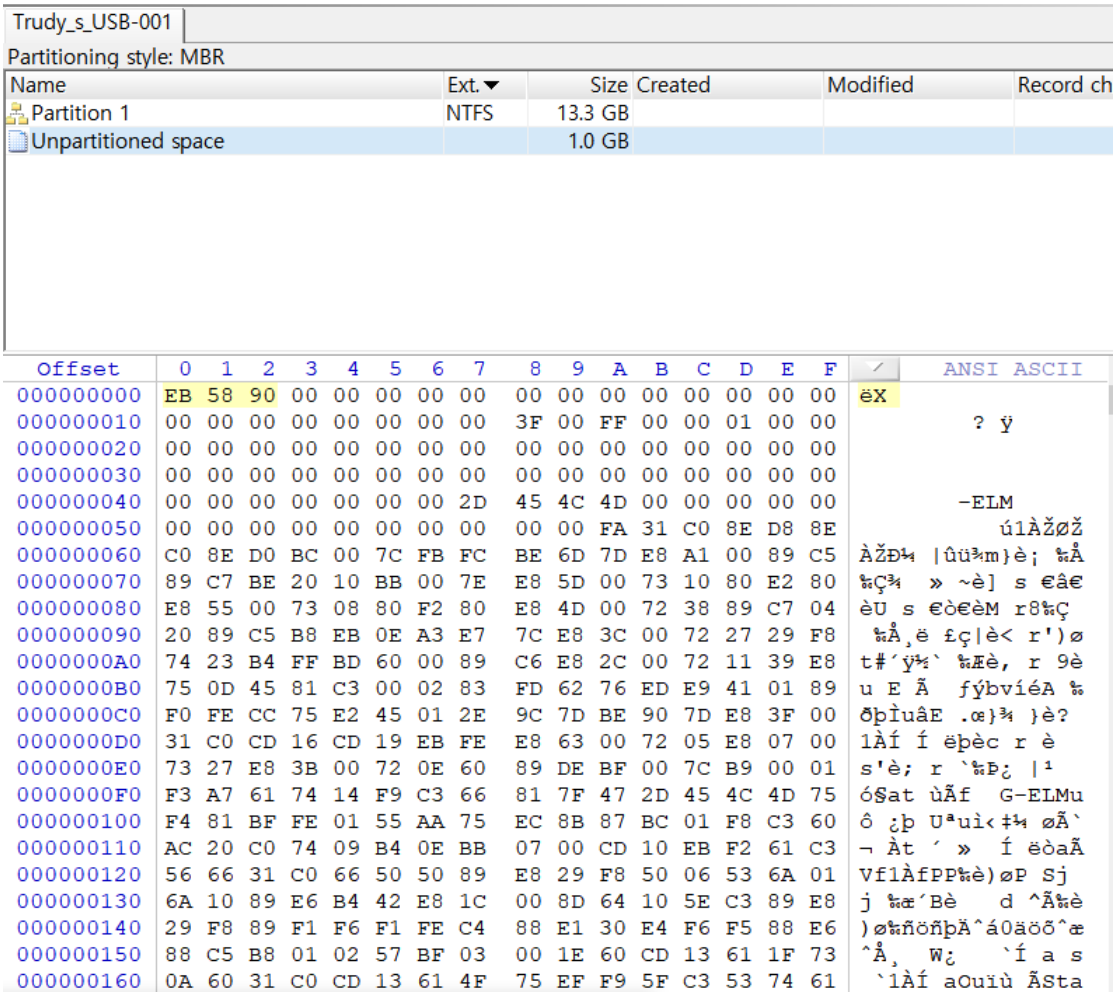
디스크 속성을 살펴보면, 해당 USB의 partition type은 NTFS, partition Name은 DATA, 그리고 USB partition의 size는 14,302,441,472byte(13.3GB)로 확인되었다.



[그림 5]. disk property

마운트 후 cmd창에서 vol F: 로 드라이브의 볼륨이름은 DATA로 확인되었고, Volume Serial Number는 0C52-BAD2로 판단되었다.

교차검증을 위해 winhex 도구를 사용했다.



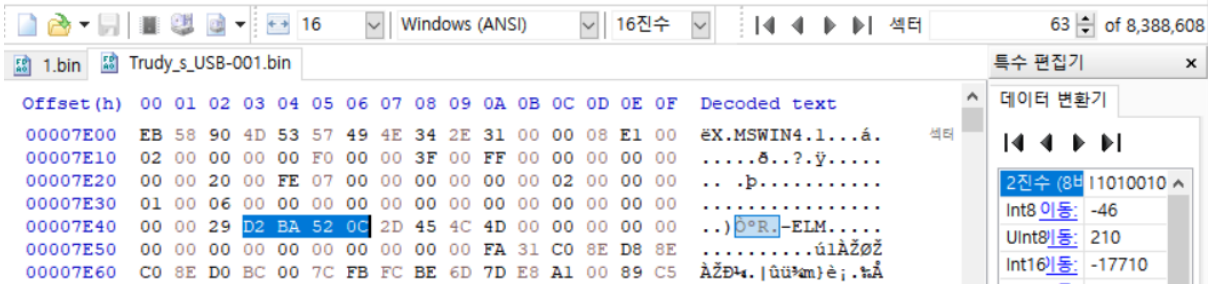
[그림 6]. winhex partition 확인

winhex로 usb image를 open하고 'Interpret Image file as disk' 기능으로 살펴보면 partition 1은 NTFS로 확인되었고, 나머지 하나 unpartitioned space가 확인되었다. 또한, partition의 size는 13.3GB와 1.0GB로 나눠져 있음을 알 수 있다.

Name	Ext.	Size	Created	Modified	Record changed	A 1st sector
Partition 1	NTFS	13.3 GB				2,097,408
Unpartitioned space		1.0 GB				0

[그림 7]. 섹터 위치 확인

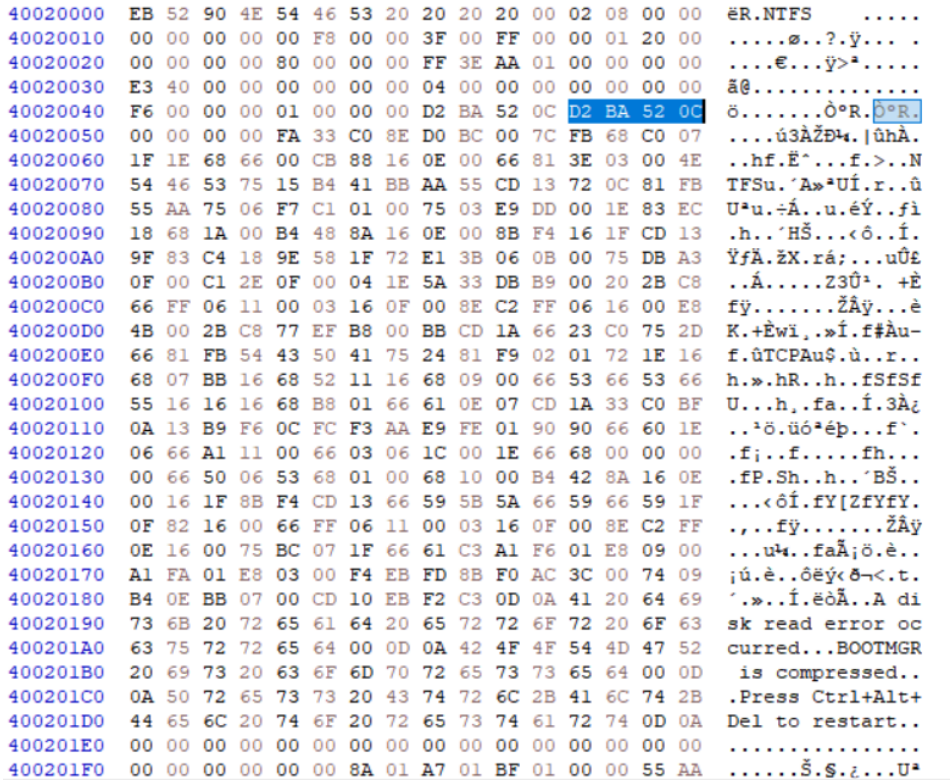
NTFS인 partition 1의 섹터가 2,097,408부터 시작하고 unpartitioned space는 0부터 시작하기 때문에 63번째 섹터에 존재하는 VBR(Boot Sector)를 살펴보았다.



[그림 8]. 63번째 섹터

63번째 섹터에서 MSWIN4.1이라는 OEM을 발견할 수 있었고, 0x43~0x46위치에 Volume Serial Number을 확인할 수 있는 것으로 보아 unpartitioned space의 partition type은 FAT32로 판단된다.

Partition Name은 unpartitioned 상태라 확인할 수 없었고, Volume Serial Number는 [그림 7]에서 파란색 음영처리 된 부분을 살펴보면 0C52-BAD2임을 확인할 수 있다.



```
40020000  EB 52 90 4E 54 46 53 20 20 20 20 00 02 08 00 00  ëR.NTFS    .....
40020010  00 00 00 00 00 F8 00 00 3F 00 FF 00 00 01 20 00  .....ø..?.ÿ... .
40020020  00 00 00 00 80 00 00 00 FF 3E AA 01 00 00 00 00  ....€...ÿ>ª.....
40020030  E3 40 00 00 00 00 00 00 04 00 00 00 00 00 00 00  ã@..............
40020040  F6 00 00 00 01 00 00 00 D2 BA 52 0C D2 BA 52 0C  ö.......Ò°R.Ò°R.
40020050  00 00 00 00 FA 33 C0 8E D0 BC 00 7C FB 68 C0 07  ....ú3ÀŽÐ¼.|ûhÀ.
40020060  1F 1E 68 66 00 CB 88 16 0E 00 66 81 3E 03 00 4E  ..hf.Ë^...f.>..N
40020070  54 46 53 75 15 B4 41 BB AA 55 CD 13 72 0C 81 FB  TFSu.´A»ªUÍ.r..û
40020080  55 AA 75 06 F7 C1 01 00 75 03 E9 DD 00 1E 83 EC  Uªu.÷Á..u.éÝ..ƒì
40020090  18 68 1A 00 B4 48 8A 16 0E 00 8B F4 16 1F CD 13  .h..´HŠ...‹ô..Í.
400200A0  9F 83 C4 18 9E 58 1F 72 E1 3B 06 0B 00 75 DB A3  ŸƒÄ.žX.rá;...uÛ£
400200B0  0F 00 C1 2E 0F 00 04 1E 5A 33 DB B9 00 20 2B C8  ..Á.....Z3Û¹. +È
400200C0  66 FF 06 11 00 03 16 0F 00 8E C2 FF 06 16 00 E8  fÿ.......ŽÂÿ...è
400200D0  4B 00 2B C8 77 EF B8 00 BB CD 1A 66 23 C0 75 2D  K.+Èwï¸.»Í.f#Àu-
400200E0  66 81 FB 54 43 50 41 75 24 81 F9 02 01 72 1E 16  f.ûTCPAu$.ù..r..
400200F0  68 07 BB 16 68 52 11 16 68 09 00 66 53 66 53 66  h.».hR..h..fSfSf
40020100  55 16 16 16 68 B8 01 66 61 0E 07 CD 1A 33 C0 BF  U...h¸.fa..Í.3À¿
40020110  0A 13 B9 F6 0C FC F3 AA E9 FE 01 90 90 66 60 1E  ..¹ö.üóªéþ...f`.
40020120  06 66 A1 11 00 66 03 06 1C 00 1E 66 68 00 00 00  .f¡..f.....fh...
40020130  00 66 50 06 53 68 01 00 68 10 00 B4 42 8A 16 0E  .fP.Sh..h..´BŠ..
40020140  00 16 1F 8B F4 CD 13 66 59 5B 5A 66 59 66 59 1F  ...‹ôÍ.fY[ZfYfY.
40020150  0F 82 16 00 66 FF 06 11 00 03 16 0F 00 8E C2 FF  .‚..fÿ.......ŽÂÿ
40020160  0E 16 00 75 BC 07 1F 66 61 C3 A1 F6 01 E8 09 00  ...u¼..faÃ¡ö.è..
40020170  A1 FA 01 E8 03 00 F4 EB FD 8B F0 AC 3C 00 74 09  ¡ú.è..ôëý‹ð¬<.t.
40020180  B4 0E BB 07 00 CD 10 EB F2 C3 0D 0A 41 20 64 69  ´.»..Í.ëòÃ..A di
40020190  73 6B 20 72 65 61 64 20 65 72 72 6F 72 20 6F 63  sk read error oc
400201A0  63 75 72 72 65 64 00 0D 0A 42 4F 4F 54 4D 47 52  curred...BOOTMGR
400201B0  20 69 73 20 63 6F 6D 70 72 65 73 73 65 64 00 0D   is compressed..
400201C0  0A 50 72 65 73 73 20 43 74 72 6C 2B 41 6C 74 2B  .Press Ctrl+Alt+
400201D0  44 65 6C 20 74 6F 20 72 65 73 74 61 72 74 0D 0A  Del to restart..
400201E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
400201F0  00 00 00 00 00 00 8A 01 A7 01 BF 01 00 00 55 AA  ......Š.§.¿...Uª
```

[그림 9]. NTFS VBR

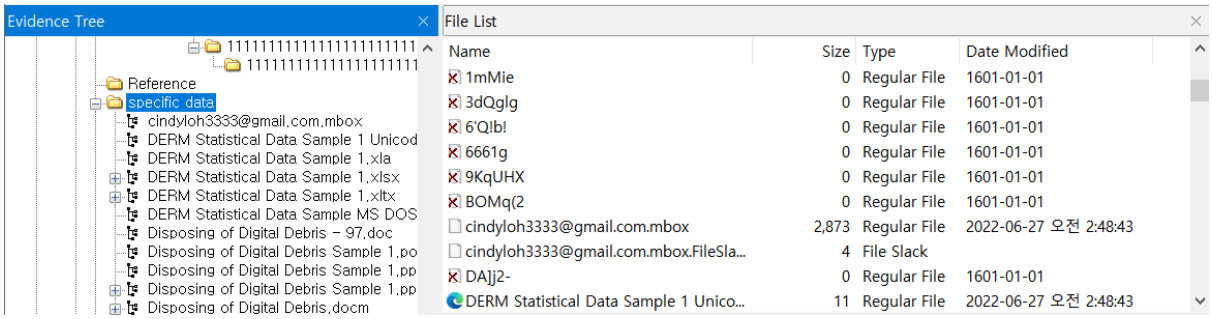
섹터 2097408에 위치하는 partition1의 VBR을 확인해보면, NTFS OEM ID를 확인할 수 있고, volume serial number도 확인이 가능하다.

따라서 확실하게 논리적 디스크 혹은 Partition으로 특정되는 부분을 고려해볼 때, 1번 문제의 **답은** 다음과 같다.

No.	Partition Type	Partition Name	Volume Serial Number	USB's Partition Size
1	NTFS	Partition 1	0C52-BAD2	13.32GB

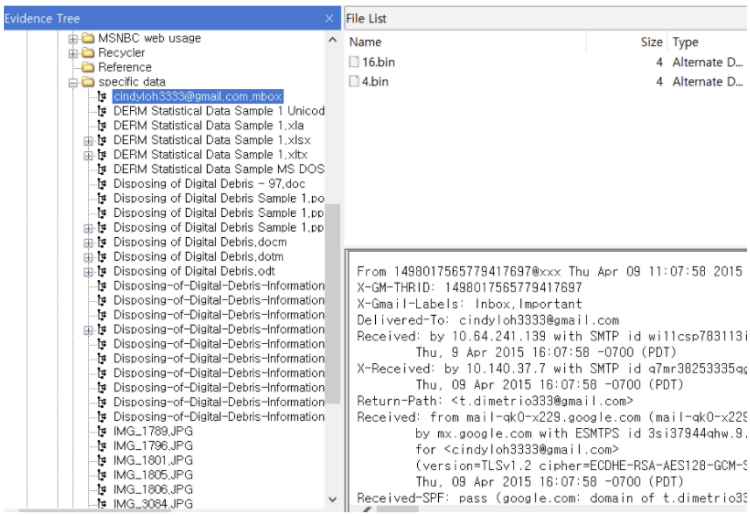
2) Find all the data Trudy tried to hide and leak and calculate the MD5 hash of the data. (80 points)

FTK imager로 파일을 살펴보던 중, 다음 그림과 같이 specific data라는 폴더에 여러 파일들을 확인할 수 있다.

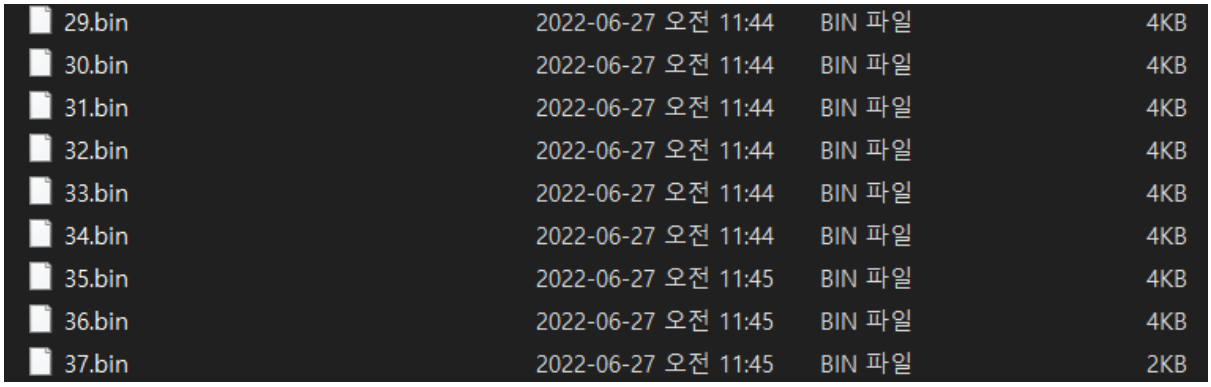


[그림 1]. Specific data 폴더 내 파일

해당 파일들은 다음과 같이, ADS(Alternative Data Stream) 파일을 내포하고 있으며 파일들은 binary file 형태로 존재한다.



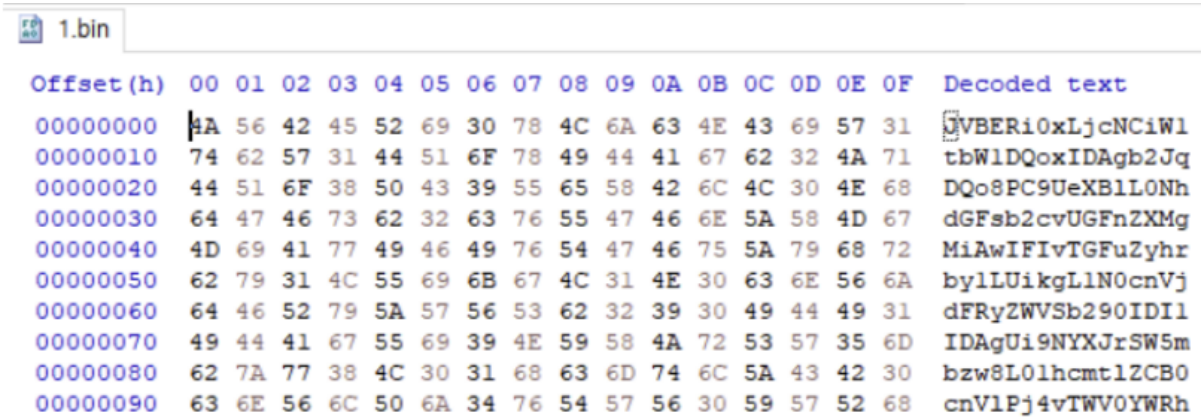
[그림 11]. ADS 파일 확인



29.bin	2022-06-27 오전 11:44	BIN 파일	4KB
30.bin	2022-06-27 오전 11:44	BIN 파일	4KB
31.bin	2022-06-27 오전 11:44	BIN 파일	4KB
32.bin	2022-06-27 오전 11:44	BIN 파일	4KB
33.bin	2022-06-27 오전 11:44	BIN 파일	4KB
34.bin	2022-06-27 오전 11:44	BIN 파일	4KB
35.bin	2022-06-27 오전 11:45	BIN 파일	4KB
36.bin	2022-06-27 오전 11:45	BIN 파일	4KB
37.bin	2022-06-27 오전 11:45	BIN 파일	2KB

[그림 12]. bin 파일 취합

해당 파일들은 1번부터 37번까지 번호가 매겨져 있으며, binary 파일을 특정해보기 위해 1.bin 파일의 헤더 시그니처를 살펴보았다.

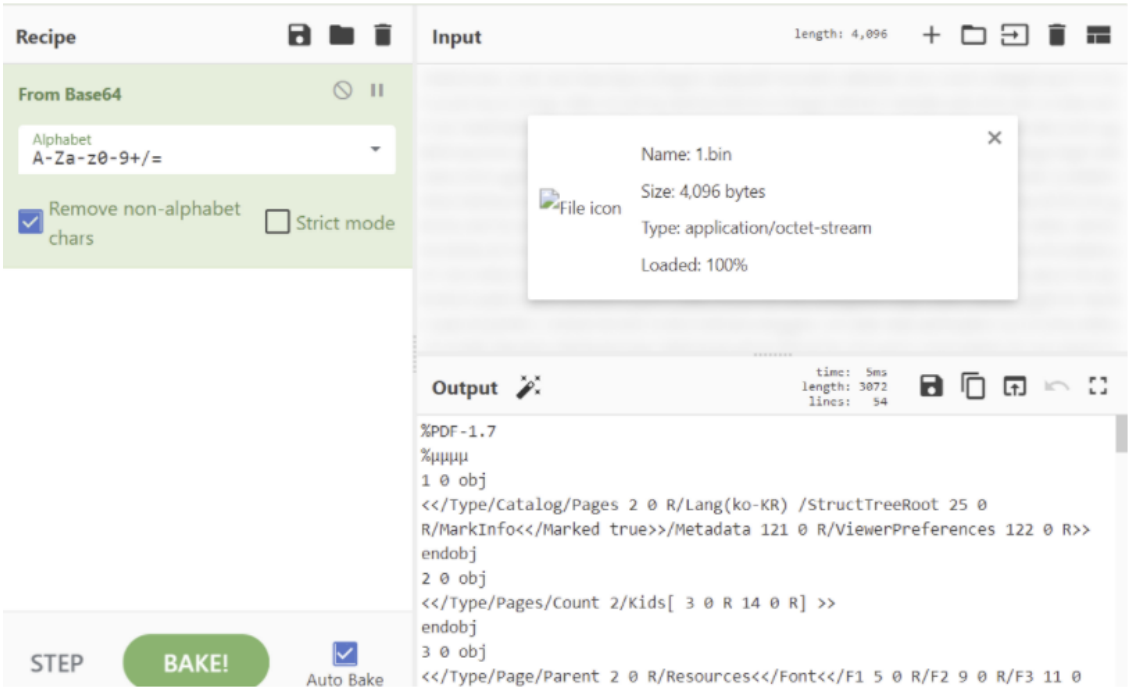


1.bin

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4A	56	42	45	52	69	30	78	4C	6A	63	4E	43	69	57	31	JVBERi0xLjcNCiW1
00000010	74	62	57	31	44	51	6F	78	49	44	41	67	62	32	4A	71	tbW1DQoxIDAgb2Jq
00000020	44	51	6F	38	50	43	39	55	65	58	42	6C	4C	30	4E	68	DQo8PC9UeXBlL0Nh
00000030	64	47	46	73	62	32	63	76	55	47	46	6E	5A	58	4D	67	dGFsb2cvUGFnZXMg
00000040	4D	69	41	77	49	46	49	76	54	47	46	75	5A	79	68	72	MiAwIFIvTGFuZyhr
00000050	62	79	31	4C	55	69	6B	67	4C	31	4E	30	63	6E	56	6A	by1LUikgL1N0cnVj
00000060	64	46	52	79	5A	57	56	53	62	32	39	30	49	44	49	31	dFRyZWVSb290IDI1
00000070	49	44	41	67	55	69	39	4E	59	58	4A	72	53	57	35	6D	IDAgUi9NYXJrSW5m
00000080	62	7A	77	38	4C	30	31	68	63	6D	74	6C	5A	43	42	30	bzw8L01hcmtlZCB0
00000090	63	6E	56	6C	50	6A	34	76	54	57	56	30	59	57	52	68	cnVlPj4vTWV0YWRh

[그림 13]. 1.bin의 hex 값 확인

해당 바이너리 파일은 헤더 시그니처를 특정할 수 없는 값들로 존재했으며, 해당 문제의 키워드가 Anti인것으로 보아 anti-forensic 기법인 암호화가 되어있을 것이라고 판단하였다.



[그림 14]. 1.bin's hex decodes with base64

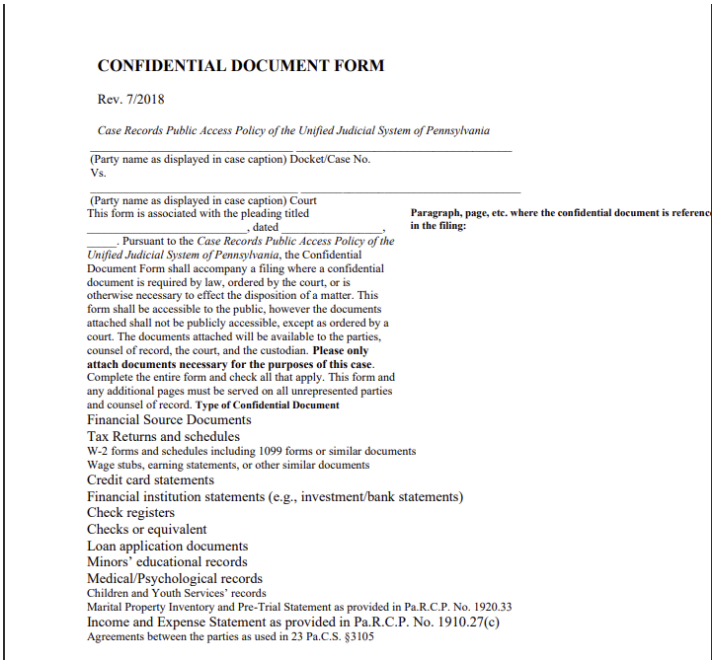
cyberchef를 통해 1.bin 파일을 base64로 디코딩한 결과 pdf 헤더 시그니처가 나왔다. 따라서 해당 바이너리 파일들을 1부터 37까지 concat해서 base64로 디코딩하면 pdf파일이 나올것이라고 판단하였다.

```python
import os
import base64


path_dir = '/Users/eungchanglee/Desktop/binary/'

data = ""
data_byte = ""

for i in range(1,38):
    file = path_dir+str(i)+'.bin'
    with open(file, 'r') as f:
        data += f.read()


f = open('output.bin', 'wb')

data_byte = data.encode('utf-8')

data_b64 = base64.b64decode(data_byte)

f.write(data_b64)

f.close()
```

[그림 15]. split bin files to combine pdf with python script

pdf 파일을 뽑아내기 위해 파이썬 스크립트를 작성하였다. 그 후, 확장자를 .bin에서 .pdf로 바꾸었다.

[그림 16]. pdf 파일 확인1



CONFIDENTIAL DOCUMENT FORM

Rev. 7/2018

Case Records Public Access Policy of the Unified Judicial System of Pennsylvania

(Party name as displayed in case caption) Docket/Case No.
Vs.

(Party name as displayed in case caption) Court
This form is associated with the pleading titled _____, dated _____, _____. Pursuant to the *Case Records Public Access Policy of the Unified Judicial System of Pennsylvania*, the Confidential Document Form shall accompany a filing where a confidential document is required by law, ordered by the court, or is otherwise necessary to effect the disposition of a matter. This form shall be accessible to the public, however the documents attached shall not be publicly accessible, except as ordered by a court. The documents attached will be available to the parties, counsel of record, the court, and the custodian. **Please only attach documents necessary for the purposes of this case.** Complete the entire form and check all that apply. This form and any additional pages must be served on all unrepresented parties and counsel of record. **Type of Confidential Document**

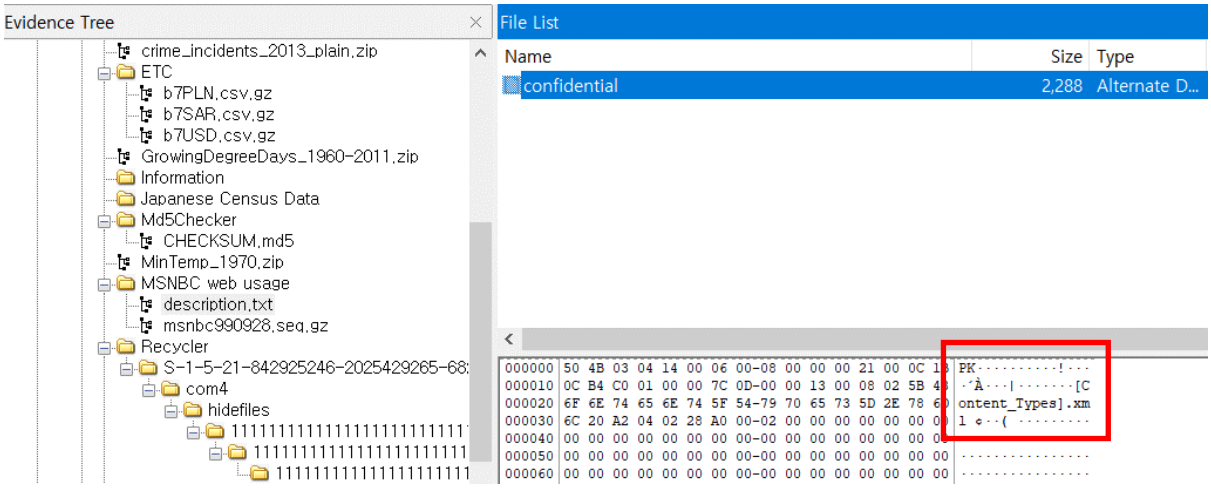
Paragraph, page, etc. where the confidential document is referenc in the filing:

Financial Source Documents
Tax Returns and schedules
W-2 forms and schedules including 1099 forms or similar documents
Wage stubs, earning statements, or other similar documents
Credit card statements
Financial institution statements (e.g., investment/bank statements)
Check registers
Checks or equivalent
Loan application documents
Minors' educational records
Medical/Psychological records
Children and Youth Services' records
Marital Property Inventory and Pre-Trial Statement as provided in Pa.R.C.P. No. 1920.33
Income and Expense Statement as provided in Pa.R.C.P. No. 1910.27(c)
Agreements between the parties as used in 23 Pa.C.S. §3105

[그림 17]. pdf 파일 확인2

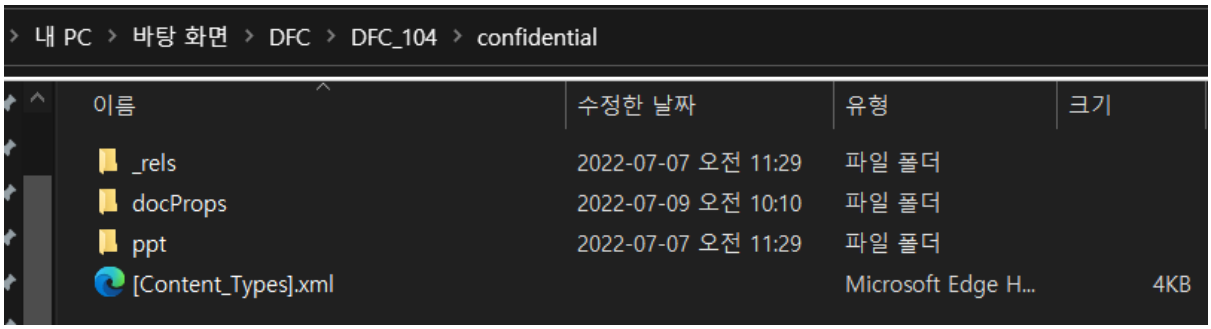
해당 파일은 위 [그림 15], [그림 16]을 통해 확인할 수 있다. DFC 기밀 자료라고 적힌 것을 보아 하니 Trudy가 숨기려고 한 data라고 판단된다.

Data (임의의 파일 명)	MD5
output.pdf	BD871B58D122275C4D0A84B76799E665



[그림 18]. confidential

위 그림을 살펴보면 description.txt 내에 confidential이라는 ADS 파일이 존재한다. 해당 파일의 헤더 시그니처에서 PK와 Content Types.xml을 확인할 수 있기 때문에 ZIP으로 먼저 export해보았다.



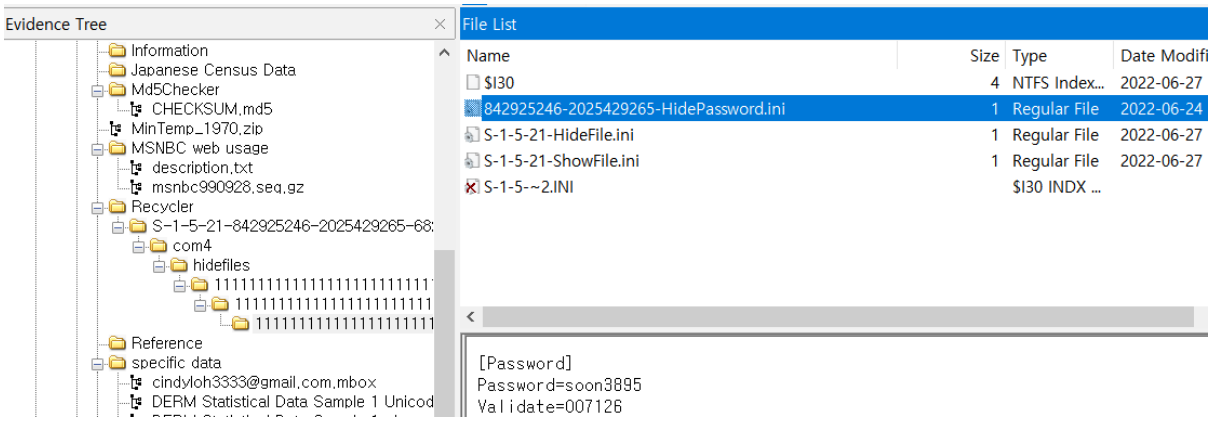
[그림 19]. confidential 파일 확인

해당 파일은 ppt로 판명되었고, 추가적으로 파일을 자세히 살펴보았다.

[그림 20]. thumbnail.jpeg

docProps 폴더에서 thumbnail.jpg를 찾을 수 있었고, 해당 파일을 열어보았더니 앞서 살펴보았던 그림과 비슷한 이미지를 확인할 수 있었다. 해당 파일 역시 Trudy가 숨긴 기밀 데이터로 확인된다.

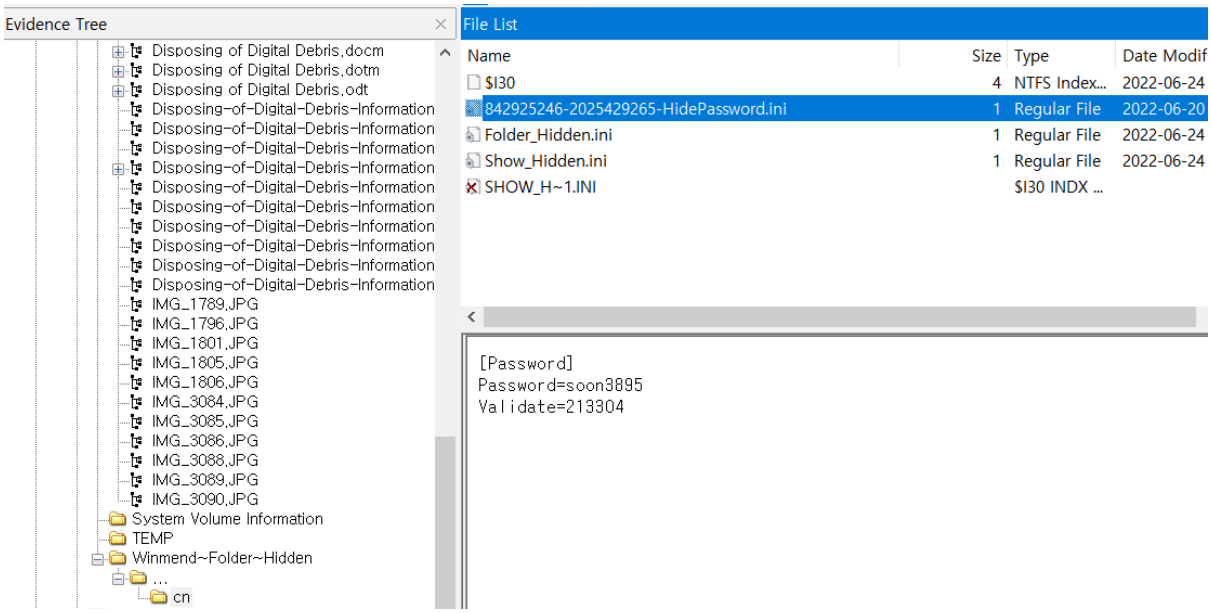
Data	MD5
thumbnail.jpeg	EE1686102FD52A34C71500B3D3D6C6E1



[그림 21]. hidefiles 하위 폴더 내 파일

위의 두 기밀 문서이외에도 hide data를 몇 가지 발견할 수 있다. 842925246-2025429265-HidePassword.ini 파일에서는 Password를 특정할 수 있었다. 해당 파일도 앞선 두 파일들이 2022-06-23 ~ 2022-06-27 내에 생성된 데이터이기 때문에 Trudy가 숨긴 data로 판단하였다.

Data	MD5
842925246-2025429265-HidePassword.ini	7202A337FE2B50A3F19C3775BB9B50DD

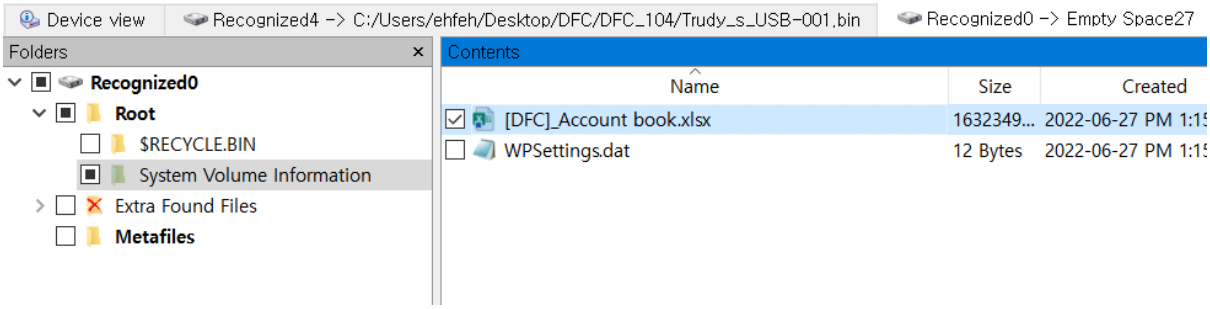


[그림 22]. cn폴더 내 파일

해당 파일은 앞의 파일과 파일 이름은 똑같지만 Validate만 다른 password 정보를 가지고 있다. 다만, 수정 시각은 이 파일이 먼저 앞서므로, Validate는 213304에서 007126으로 변경된 것으로 추정된다.

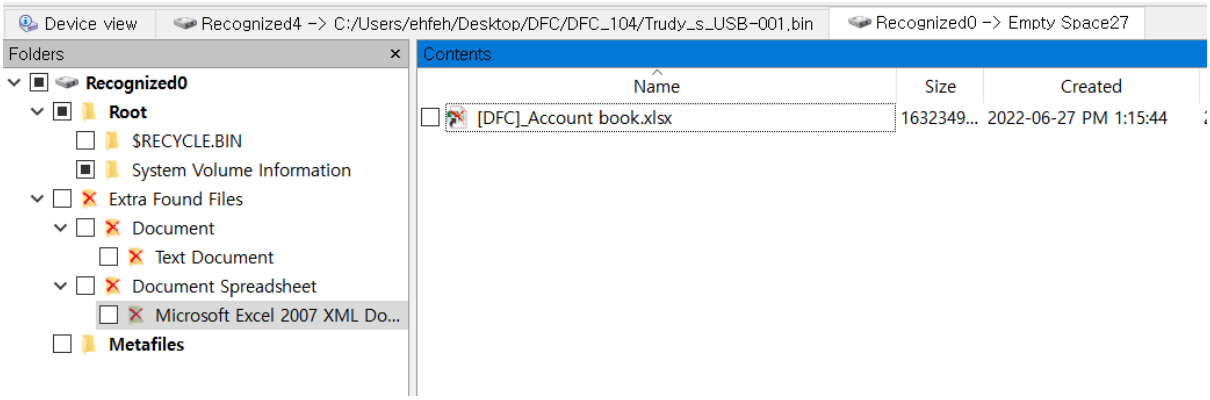
Data	MD5
842925246-2025429265-HidePassword.ini	94BF12428B6CB173DF46C95A48086648

추가적으로 R-Studio를 통해 스캔했던 Recognized partition들에서 삭제된 파일들을 복구해보려고 시도했다.



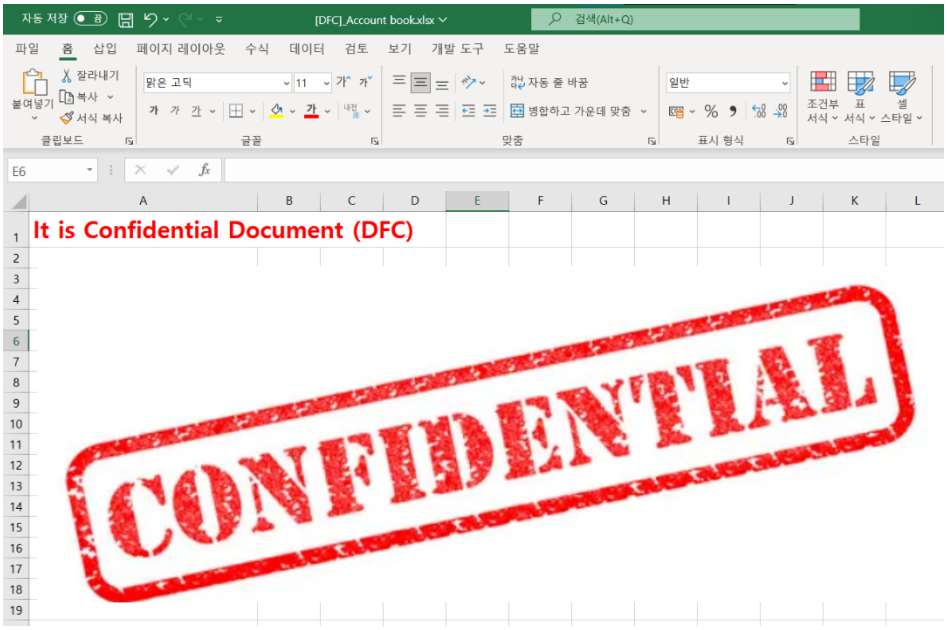
[그림 23]. [DFC]_Account_book 확인1

그 중, Recognized0 파티션에서 [DFC]_Account_book.xlsx라고 적힌 파일을 발견하였다.



[그림 24]. [DFC]_Account_book 확인2

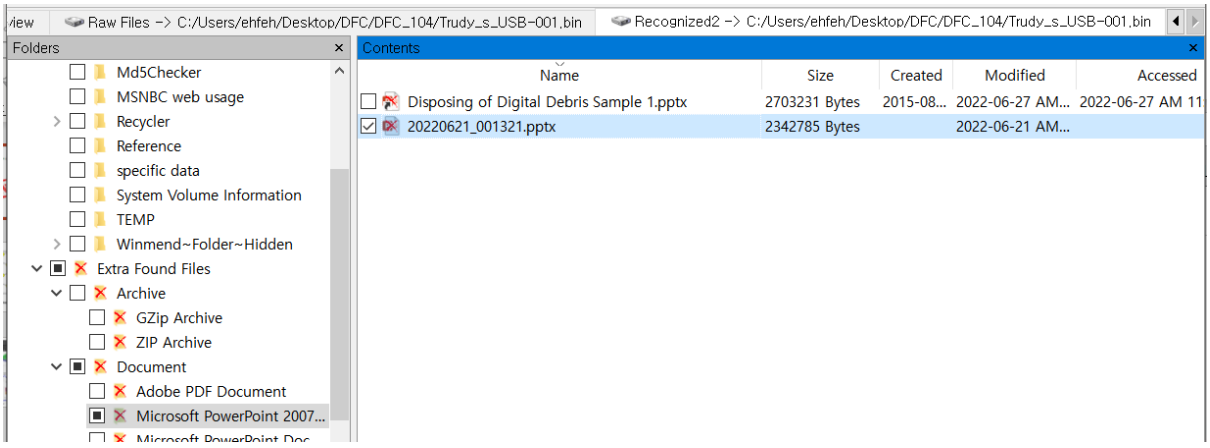
위 두 그림에서 하나는 온전하고, 나머지 하나는 삭제되었지만 동일한 파일을 발견했고, Recover 했다.



[그림 25]. [DFC]_Account_book open

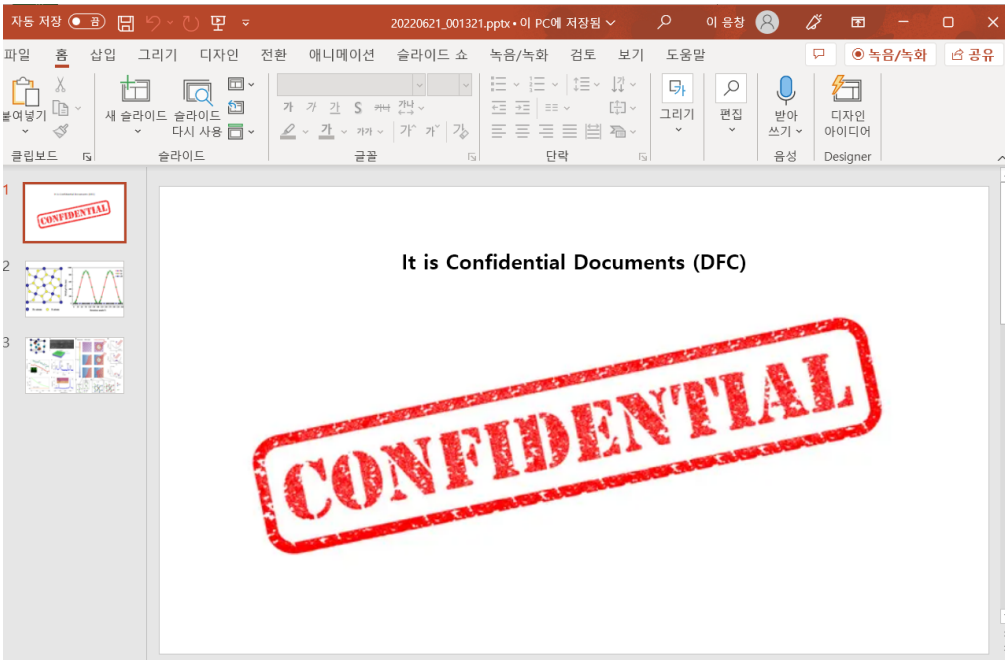
해당 파일을 열어본 결과, 기밀 문서 확인 가능했다. 해당 파일의 MD5는 다음과 같다.

Data	MD5
[DFC]_Account_book.xlsx	0D34B4B17C0C51C8AA79007A97BB4860



[그림 26]. 20220621_001321.pptx

다음으로 Recognized2 partition에서 20220621_001321.pptx를 발견했다.

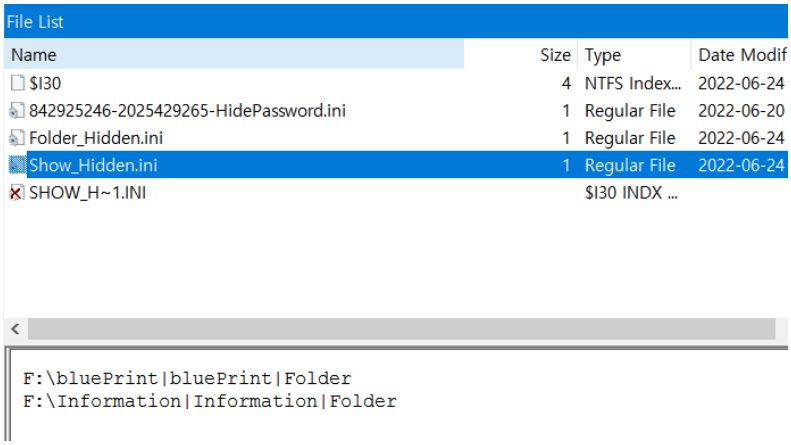


[그림 27]. 20220621_001321.pptx

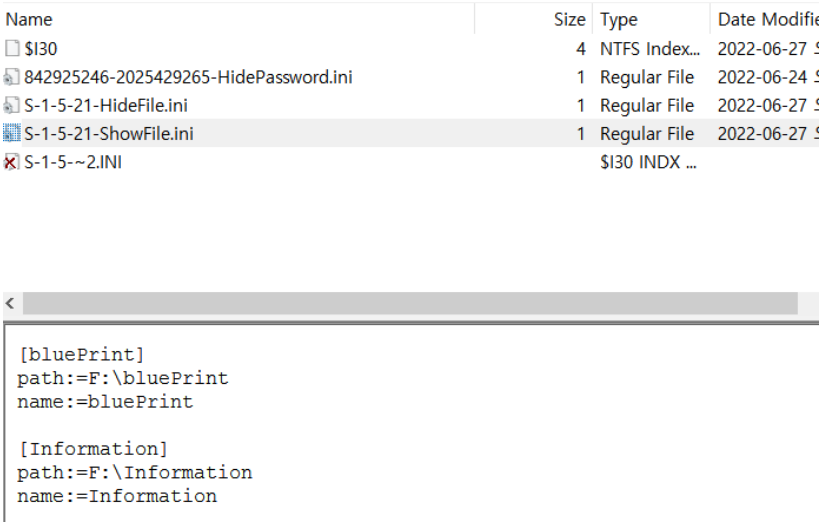
해당 파일 역시 열어본 결과, CONFIDENTIAL 문서 확인이 가능하였다.

해당 파일의 MD5는 다음과 같다.

Data	MD5
20220621_001321.pptx	1E6BE0E73E051F825B5A1B4513ADA234

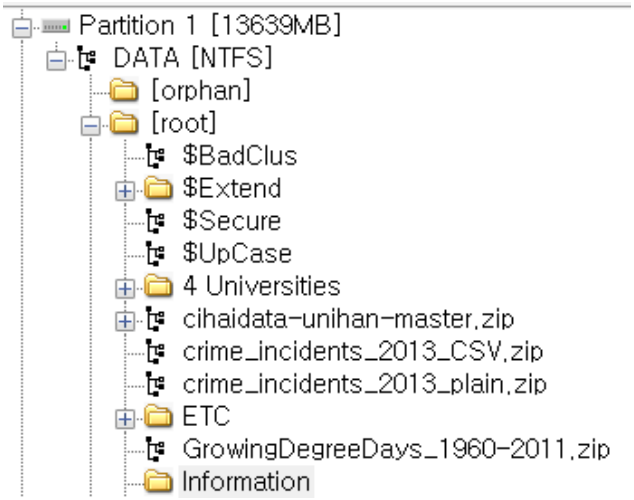


[그림 28]. Show_Hidden.ini

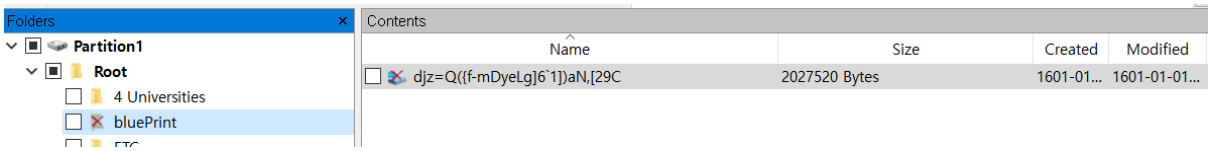


[그림 29]. S-1-5-21-ShowFile.ini

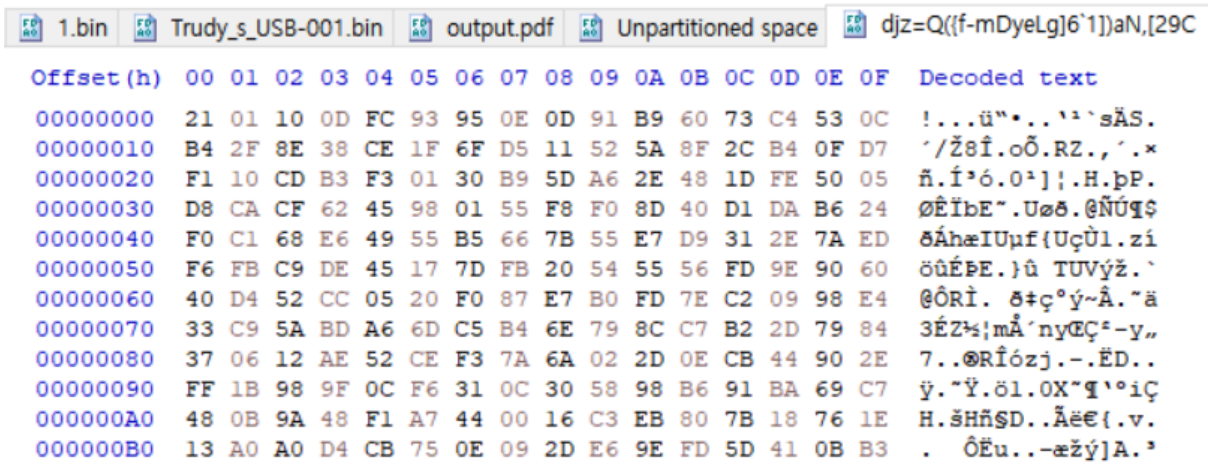
위 두 그림이 bluePrint폴더와 Information폴더를 나타내고 있지만, FTK Imager에는 Information 폴더만 존재하고, bluePrint 폴더는 확인 불가능하다.



[그림 30]. bluePrint 폴더 확인 불가



[그림 31]. bluePrint 폴더 내 파일 확인

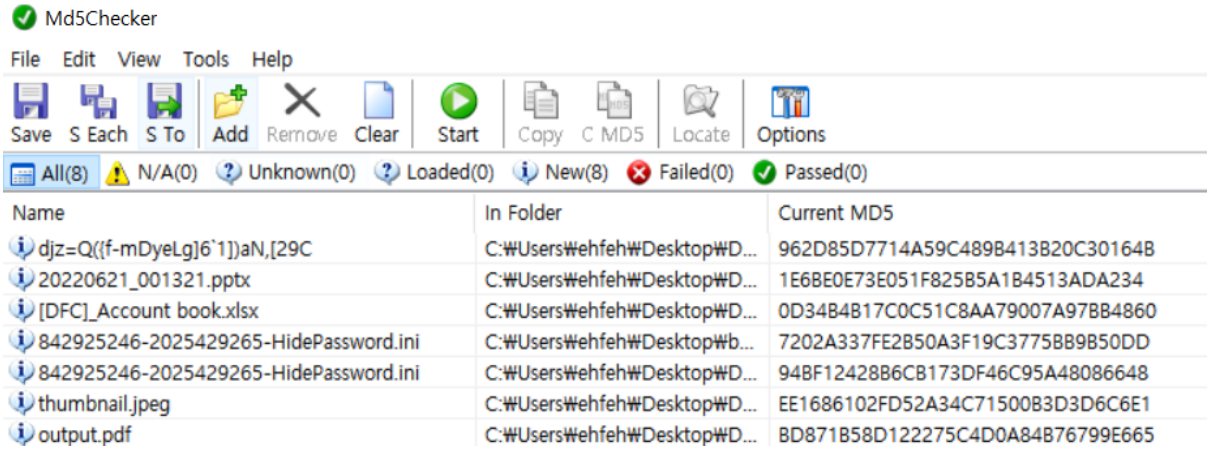


[그림 32]. djz=Q({f-mDyeLg]6`1])aN,[29C 식별 불가

해당 파일은 해독이 불가능하다고 판단되어 수상한 bluePrint 폴더 내 파일 자체의 MD5를 첨부했다.

Data	MD5
djz=Q({f-mDyeLg]6`1])aN,[29C	962D85D7714A59C489B413B20C30164B

전체적으로 Trudy가 숨기거나 유출했을 데이터들을 Md5Checker로 돌린 결과는 다음과 같다.



[그림 33]. MD5 Checker 결과