

## 106 – Is there more than meets the eye?

### Team Information

Team Name: ISEGYE\_IDOL

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

Email Address: dfc-isegyeidol@googlegroups.com

### Instructions

**Description** The photos were acquired from Trudy's Mobile's photo gallery, which is suspected of leaking confidential data. Analyze the photos to find clues related to the leak of confidential data.

Target	Hash (MD5)
Trudy_Gallery.ad1	F33C6950FEA57F1DA480592F5AFFEA19

### Questions

1. Find traces related to confidential data leakage and identify the MD5 value of the file Trudy was trying to leak. (50 points)
2. Describe the way Trudy tried to leak the data. (50 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:	Visual Studio Code	Publisher:	Microsoft
Version:	1.71.2		

URL:	<a href="https://code.visualstudio.com/">https://code.visualstudio.com/</a>
------	---

Name:	Python 3.9.9	Publisher:	Python Software Foundation
Version:	3.9.9		
URL:	<a href="https://www.python.org/downloads/">https://www.python.org/downloads/</a>		

Name:	FTK Imager	Publisher:	Python Software Foundation
Version:	3.9.9		
URL:	<a href="https://www.python.org/downloads/">https://www.python.org/downloads/</a>		

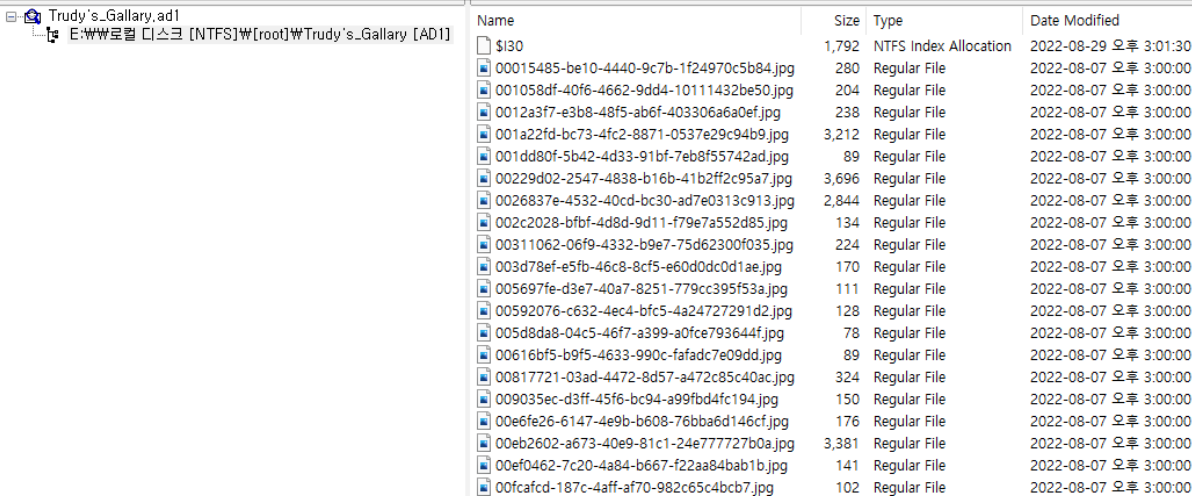
Name:	ExiftoolGUI	Publisher:	Bogdan Hrastrnik
Version:	5.16.0.0		
URL:	<a href="http://u88.n24.queensu.ca/exiftool/forum/">http://u88.n24.queensu.ca/exiftool/forum/</a>		

Name:	Exiftool.exe (cli)	Publisher:	Phil Harvey
Version:	11.9.9.0		
URL:	<a href="https://exiftool.org/">https://exiftool.org/</a>		

## Step-by-step methodology:

1. Find traces related to confidential data leakage and identify the MD5 value of the file Trudy was trying to leak.

FTK Imager을 이용하여 분석 대상파일(Trudy's Gallery.ad1)을 열면, NTFS 파일 시스템에 5,606개의 jpg 파일, 15개의 mp4 파일이 담겨 있다.



Name	Size	Type	Date Modified
\$I30	1,792	NTFS Index Allocation	2022-08-29 오후 3:01:30
00015485-be10-4440-9c7b-1f24970c5b84.jpg	280	Regular File	2022-08-07 오후 3:00:00
001058df-40f6-4662-9dd4-10111432be50.jpg	204	Regular File	2022-08-07 오후 3:00:00
0012a3f7-e3b8-48f5-ab6f-403306a6a0ef.jpg	238	Regular File	2022-08-07 오후 3:00:00
001a22fd-bc73-4fc2-8871-0537e29c94b9.jpg	3,212	Regular File	2022-08-07 오후 3:00:00
001dd80f-5b42-4d33-91bf-7eb8f55742ad.jpg	89	Regular File	2022-08-07 오후 3:00:00
00229d02-2547-4838-b16b-41b2ff2c95a7.jpg	3,696	Regular File	2022-08-07 오후 3:00:00
0026837e-4532-40cd-bc30-ad7e0313c913.jpg	2,844	Regular File	2022-08-07 오후 3:00:00
002c2028-bfbf-4d8d-9d11-f79e7a552d85.jpg	134	Regular File	2022-08-07 오후 3:00:00
00311062-06f9-4332-b9e7-75d62300f035.jpg	224	Regular File	2022-08-07 오후 3:00:00
003d78ef-e5fb-46c8-8cf5-e60d0dc0d1ae.jpg	170	Regular File	2022-08-07 오후 3:00:00
005697fe-d3e7-40a7-8251-779cc395f53a.jpg	111	Regular File	2022-08-07 오후 3:00:00
00592076-c632-4ec4-bfc5-4a24727291d2.jpg	128	Regular File	2022-08-07 오후 3:00:00
005d8da8-04c5-46f7-a399-a0fce793644f.jpg	78	Regular File	2022-08-07 오후 3:00:00
00616bf5-b9f5-4633-990c-fafadc7e09dd.jpg	89	Regular File	2022-08-07 오후 3:00:00
00817721-03ad-4472-8d57-a472c85c40ac.jpg	324	Regular File	2022-08-07 오후 3:00:00
009035ec-d3ff-45f6-bc94-a99fbd4fc194.jpg	150	Regular File	2022-08-07 오후 3:00:00
00e6fe26-6147-4e9b-b608-76bba6d146cf.jpg	176	Regular File	2022-08-07 오후 3:00:00
00eb2602-a673-40e9-81c1-24e777727b0a.jpg	3,381	Regular File	2022-08-07 오후 3:00:00
00ef0462-7c20-4a84-b667-f22aa84bab1b.jpg	141	Regular File	2022-08-07 오후 3:00:00
00fcacfd-187c-4aff-af70-982c65c4bcb7.jpg	102	Regular File	2022-08-07 오후 3:00:00
011740da-c812-420f-b42b-a912676d5456.jpg	108	Regular File	2022-08-07 오후 3:00:00

[그림 1] ad1 이미지 파일 (FTK Imager)

상세 분석을 위해 export 기능을 이용하여 저장되어 있는 모든 파일을 추출한다.

ExiftoolGUI 프로그램으로 파일의 메타데이터를 분석한 결과, 일부 JPG 파일에서

SAMSUNG - EmbeddedVideo Tag가 활성화되어 있음을 발견했다.

EmbeddedVideoType Tag 값이 "MotionPhoto\_Data"인 것으로 미루어 보아, 삼성 모바일 휴대폰으로 모션포토<sup>1</sup> 기능으로 사진 촬영한 것으로 유추된다.

<sup>1</sup> 움직이는 사진이란 의미로 카메라 촬영 버튼을 누르기 약 2초 전의 상황까지 녹화해서 생동감 넘치는 사진을 찍을 때 유용하게 사용되는 기능 (<https://changwoos.tistory.com/365>)

	---- XMP-Container ----
DirectoryItemMime	image/jpeg
DirectoryItemSemantic	Primary
DirectoryItemLength	0
DirectoryItemPadding	59
DirectoryItemMime	video/mp4
DirectoryItemSemantic	MotionPhoto
DirectoryItemLength	4322311
DirectoryItemPadding	0
	---- Samsung ----
TimeStamp	2022:08:29 01:30:15+09:00
EmbeddedVideoType	MotionPhoto_Data
EmbeddedVideoFile	(Binary data 4322255 bytes, use -b option to extract)

[그림 2] JPG 내 SAMSUNG TAG 메타데이터 (ExiftoolGUI.exe)

EmbeddedVideoFile에 저장된 Binary data를 추출하면 모션포토를 획득할 수 있다. 이에 따라 Cli 버전의 exiftool.exe를 이용하여 모션포토 추출 스크립트를 제작했다. 알고리즘은 지정 경로의 모든 파일의 메타데이터를 읽고, EmbeddedVideo가 활성화되어 있다면 EmbeddedVideoFile의 Binary data를 추출해 파일을 생성한다. 생성 파일명은 확장자 포함 원본 파일명으로 설정했다.

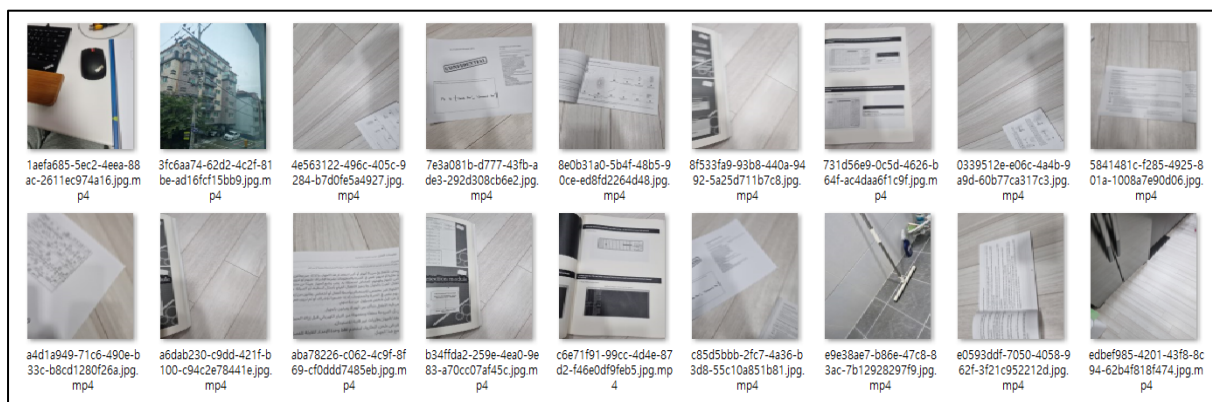
```
from asyncio.windows_events import NULL
import os
import re
import sys
idx=1
for filename in os.listdir("E:/"):
    full_filename = 'E:/' + filename
    stream = os.popen('C:/exiftool.exe -EmbeddedVideoType ' +
full_filename).read()
    if len(stream) == 0:
        print('[' + str(idx) + '] + 'debug: PASS in ' + filename)
        idx+=1
        continue
    regex = re.compile(': (.+)\n')
    Embedded_Video_Type = regex.findall(stream)
    if Embedded_Video_Type[0] == "MotionPhoto_Data":
        os.system('exiftool.exe -EmbeddedVideoFile -b ' + full_filename
+ ' > C:/SJ/DFC2022_106/' + filename + '.mp4');
        print('[' + str(idx) + '] + 'debug: Extract EmbeedebVideoFile in
' + filename)
    else:
        print('[' + str(idx) + '] + 'debug: im not motonphoto_data, **'
+ Embedded_Video_Type[0])
        idx+=1
sys.stdout = open('C:/SJ/DFC2022_106/debug.txt', 'w')
```

[표 1] EmbeddedVideoFile 추출 스크립트

스크립트 실행 결과, 총 18개의 모션 포토가 생성되었고. 다음은 생성된 파일을 정리한 표이다.

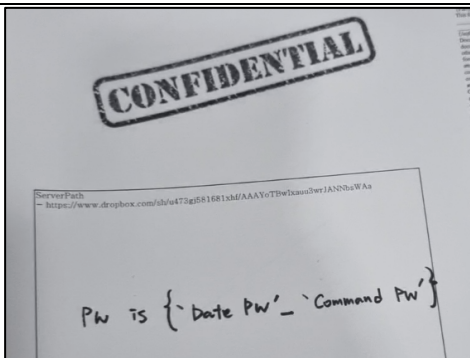
Idx	추출 파일명
1	1aefa685-5ec2-4eea-88ac-2611ec974a16.jpg.mp4
2	3fc6aa74-62d2-4c2f-81be-ad16fcf15bb9.jpg.mp4
3	4e563122-496c-405c-9284-b7d0fe5a4927.jpg.mp4
4	7e3a081b-d777-43fb-ade3-292d308cb6e2.jpg.mp4
5	8e0b31a0-5b4f-48b5-90ce-ed8fd2264d48.jpg.mp4
6	8f533fa9-93b8-440a-9492-5a25d711b7c8.jpg.mp4
7	731d56e9-0c5d-4626-b64f-ac4daa6f1c9f.jpg.mp4
8	0339512e-e06c-4a4b-9a9d-60b77ca317c3.jpg.mp4
9	5841481c-f285-4925-801a-1008a7e90d06.jpg.mp4
10	a4d1a949-71c6-490e-b33c-b8cd1280f26a.jpg.mp4
11	a6dab230-c9dd-421f-b100-c94c2e78441e.jpg.mp4
12	aba78226-c062-4c9f-8f69-cf0ddd7485eb.jpg.mp4
13	b34ffda2-259e-4ea0-9e83-a70cc07af45c.jpg.mp4
14	c6e71f91-99cc-4d4e-87d2-f46e0df9feb5.jpg.mp4
15	c85d5bbb-2fc7-4a36-b3d8-55c10a851b81.jpg.mp4
16	e9e38ae7-b86e-47c8-83ac-7b12928297f9.jpg.mp4
17	e0593ddf-7050-4058-962f-3f21c952212d.jpg.mp4
18	edbef985-4201-43f8-8c94-62b4f818f474.jpg.mp4

[표 2] 추출된 EmbeddedVideoFile 파일 목록

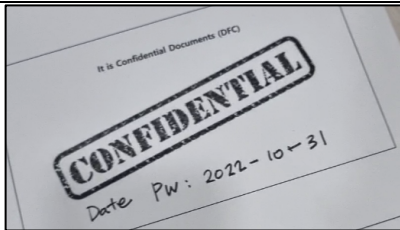


[그림 3] 추출된 EmbeddedVideoFile 파일 목록

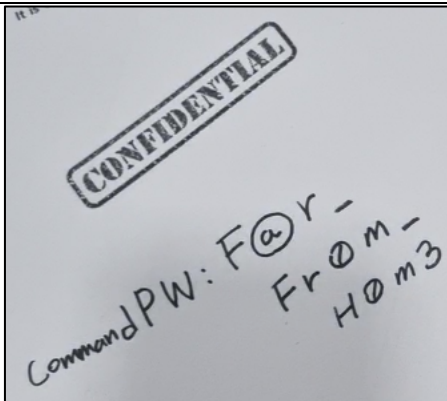
모션 포토(MP4)를 실행하여 총 3건의 “CONFIDENTIAL” 문서를 발견했고, 발견한 주요 내용을 표로 정리한다.

filename	7e3a081b-d777-43fb-ade3-292d308cb6e2.jpg.mp4	
context		
confidential	Pw is {'Date PW'_'Command PW'} <a href="https://www.dropbox.com/sh/u473gj581681xhf/AAAYoTBwIxaau3wrJANNbsWAa">https://www.dropbox.com/sh/u473gj581681xhf/AAAYoTBwIxaau3wrJANNbsWAa</a>	

[표 3] Confidential 첫 번째 문서

filename	8e0b31a0-5b4f-48b5-90ce-ed8fd2264d48.jpg.mp4	
context		
confidential	Date PW : 2022-10-31	

[표 4] Confidential 두 번째 문서

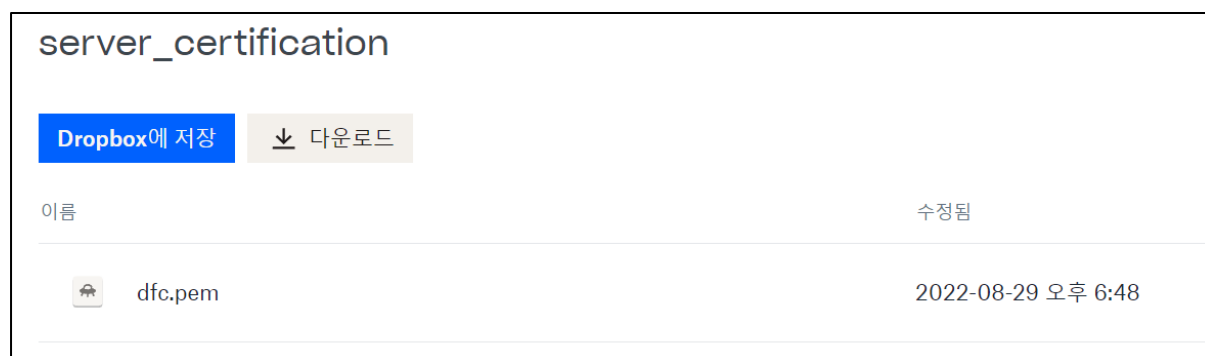
filename	731d56e9-0c5d-4626-b64f-ac4daa6f1c9f.jpg.mp4	
context		
confidential	Command PW: F@r_Fr0m_H0m3	

[표 5] Confidential 세 번째 문서

기밀 문서에서 얻은 정보를 취합하여 최종 획득 정보는 다음과 같다.

- Dropbox URL<sup>2</sup>
- PW is {2022-10-31\_F@r\_Fr0m\_H0m3}

획득한 Dropbox URL에 접속하여 Password 입력을 통해 파일을 다운로드한다.



[그림 4] Dropbox URL 접속

최종적으로 Trudy가 유출하고자 했던 파일은 서버 인증키 [dfc.pem] 파일이며, MD5(dfcm.pem) 값은 [6C29C6459759AA2EA28F351E264BECC0]이다.

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA9xbYtIR3VStY9QQD6lyDUJwqOTBTEloZ7oegDGwI0a9CXX
p7m6E2ZvjK2LYWWEIQNI5G+ocb+2S+6XkYdyY9byKU8mD9E3y4hVqk/4v/MJy
MgyqzQx+Dvg/bc1zSRD2Ls6erOuYll7ymVzJ88Ns3p38Cp8srgRv/7k29r74JM+G
kICw3LkeTQhH/wgoCBtDzG3jdS4Dv8j2lgCzgjlfqCYd0D500FPzu9YtC5eom8i0
JqXzdZzPQhF8iy+I3vnfyypz9uB1u6QPvOs86HJr8oWyMvFvZL83+1vs5OIRqzoG
9C75ldCK636liidhV4+EsMwFslr4+3cWYJPLSGQIDAQABAoIBAC4PAU8B8sn96otiQ
wvgt8iGagLqNhyXqOxFTiPdNYZiHyjB2qMyNcuoCZtrLUlDSddJ6e0pvqbRPPgx
CY7imvhQ56U9NqkXh1fJNbv6p+z0SDezV+knQ0o1a8bLnfqXhVdtx42dvQbVls/I
BXKEXmQXaLORTJDSyG9b5YoiUHQOTBjAAZdYbhK6i+kUDK5HgOF93MsMymBx90
2FkKzZ27eBAWE7vxtGy7DWtiCdMO3/j0OKgscF5ILUy5FjPztLyPZdWelp6yIK6
1hdroO/D9k2f5sC+/2Ovm/u6T1767SvyoEckH/2yZsF4zmQ0rmdCrR382egez6L
y2NUIG0CgYEA8ZIASyhcHsKST94+YR1F69cnKnNuH6V9/80GjKxGQ03PGG0aGZge
TstqW4Tk8F5Ce0BRUJ/TYt8jK5d+RXtCee+RbB8tCF+L4Fm3H5iq/Xi+z7P0L3tB4
zNKR7/F5JnpVUTBQY5Qfke39gK0TCSg7VXBgCRhZRoMDgpe/5l6mwNsCgYEAwpQH
fAg2ly0gM1YPKw9F5kylNX33E5UchoE1rJWSMH/vYPg6hvjgtBccXJzIzEaDwt8h
tNh7TYg5Ke56rPGospnN5RY/ZROJofvYhftzcZoeWw70mH19MZux8kczXF6Saccb0
X4v2tw5Pki87UlrepMN4S6+SP+ekLP091E+tmCgYEA7RrYDGGgullhHTYbxdWHD
Q2fOGk1aoFhMRhgS7rzog302L5PBRTc0UTRmowPO5IfzUxC6hmgzHg75b7s+T
GkfMRuPml4curuRisLL3SLpMPKND5RMT2wA1FWTI30hj/uAjPRCaPtNwXR5+eHyY
jotQ1Nw+kYL2qOd7Pircs0CgYBibOUzQ8Ogu8uC9u+ow5M5HncjFR7gqOFDlGh
lu4tHt6exty894hUq8amXk2Q91189p9ONXla/ntd8jnmFGiqDusLfc59vktXPc
ZyUGOr1piZn26CnN0eobWdVcTNfM5bnQL+v7SRDfuCdpMtNt9kMIMEf6NUP1PQ
BkUStQK8gQCsnSmKQ12GguPJ9dWrixAlr1WL5Jsc2yer127hQnFvR2WYING3jP
AQ46coOYnBoDrSIShXrjw2DK8rOGSoO55otdxDBwXTd22Wm7b3XBQmYnzWes33z2S
nKi/R+/DY0yOvABpsRQ2EDPvjN2VjFML62HajOEL27i272WRBXMA==
-----END RSA PRIVATE KEY-----
```

[그림 5] dfc.pem (notepad.exe)

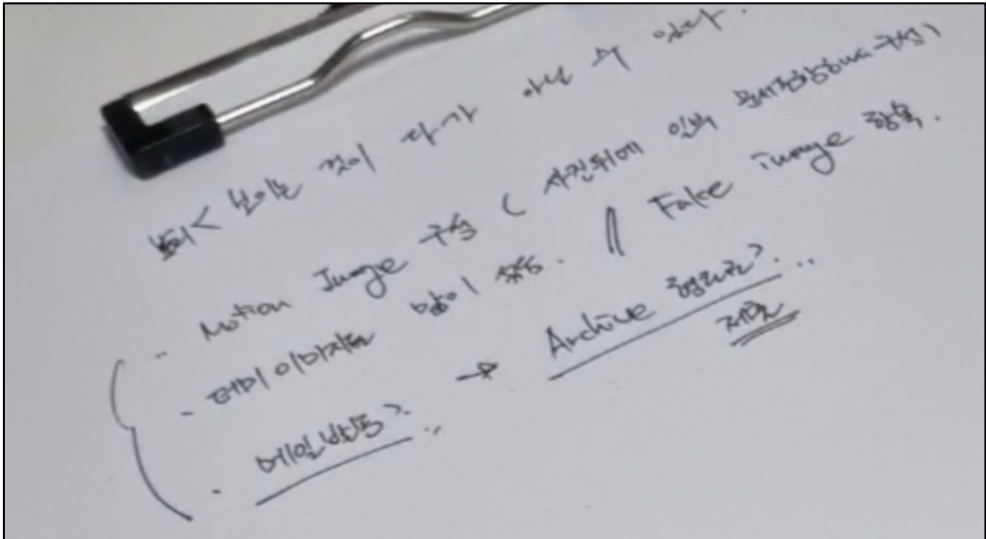
<sup>2</sup> <https://www.dropbox.com/sh/u473qj581681xhf/AAAYoTBwIxaau3wrJANNbsWAa>

```
MD5의 dfc.pem 해시:
6c29c6459759aa2ea28f351e264becc0
CertUtil: -hashfile 명령이 성공적으로 완료되었습니다.
```

[그림 6] Windows CertUtil Command result (cmd.exe)

## 2. Describe the way Trudy tried to leak the data.

앞서 스크립트로 생성한 18개의 모션 포토 중에서 “CONFIDENTIAL” 마크가 기재된 문서 외에 Trudy가 작성한 것으로 추정되는 문서를 찾을 수 있었으며, 주요 정보는 다음 표와 같다.

filename	1aefa685-5ec2-4eea-88ac-2611ec974a16.jpg.mp4
context	
Way	<p style="color: red;">&lt;보이는 것이 다가 아닐 수 있다.&gt;</p> <ul style="list-style-type: none"> <li>- Motion Image 구성 (사진뒤에 일부 문서포함해서 구성)</li> <li>- 더미 이미지를 많이 섞음. // False image 항목</li> <li>- 메일발송? -&gt; Archive 형태로? .. 제출</li> </ul>

[표 6] Trudy의 유출 방법

자필로 작성된 종이 문서에서 “Motion Image” 혹은 “Archive” 등의 단어로부터 실제로 Trudy가 데이터(키 파일)를 유출하기 위해 사용했던 방식과 동일한 것을 알 수 있다. 따라서 위 내용은 Trudy의 데이터 유출 방안으로 볼 수 있다.