[DFC – 2022 - 104] Write-Up

작성자	심주완
분석 일자	2024.05.21
작성 일자	2024.05.22
분석 대상	Tredy_s_USB-001.bin
문서 버전	1
작성자 E-mail	rd002@naver.com

0. 목차

1. 문제

URL	
문제 내용	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. 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)
문제 파일	
문제 유형	Disk 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
OSPMount	https://www.osforensics.com/tools/mount-disk-images.html	3.1.1003
Md5Checker	http://getmd5checker.com/	3.3
Hxd	https://mh-nexus.de/en/hxd/	2.5.0.0
CyberChef	https://gchq.github.io/CyberChef/	10.18.6

3. 환경

OS
Window 11 Home

4. Write-Up

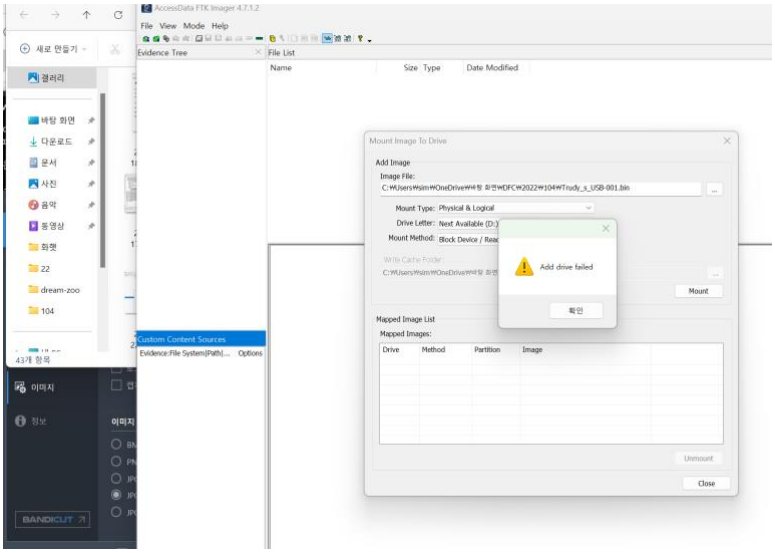
파일명	Trudy_s_USB-001.bin
용량	4GB
SHA256	3ad5c63006931879c6d470649add68fe9def5e6b02d998997a67a7017d37d4d5
Timestamp	2022-06-29 21:59:26

한 문제씩 풀어보자.

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

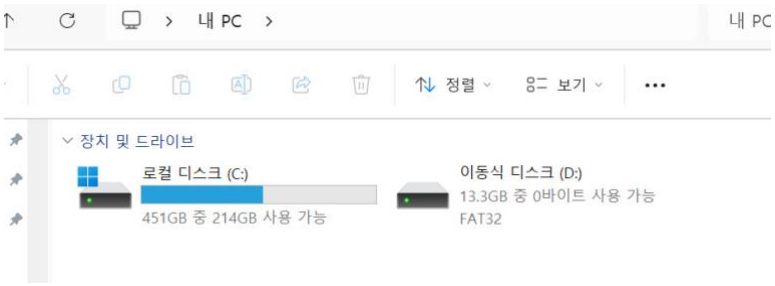
각각에 해당하는 값을 찾아보자.

이를 확인하기 위하여 USB 파일이기 때문에 FTK imager 의 마운팅 기능을 사용했다.



[그림 1] 마운팅 결과(1)

마운팅이 정상적으로 되지 않았다. 아마 로컬적인 문제가 아닌가 싶다. 이렇게 된다면 나오는 모든 결과값을 두 번씩 확인하는 것이 좋다. 다음과 같이 마운팅이 끝난 것을 확인할 수 있다.



[그림 2] 마운팅 결과(2)

속성을 통하여 필요한 정보를 얻어오도록 하자.

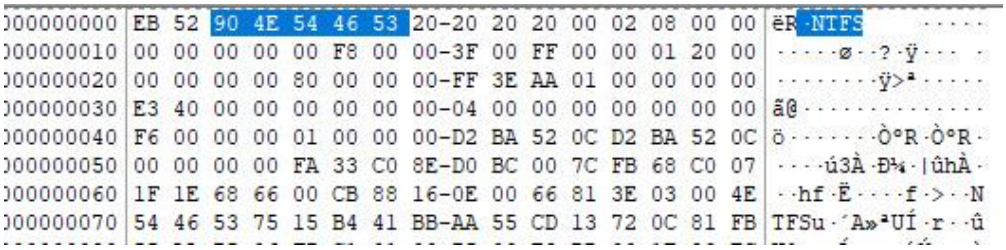
[그림 3] 마운팅 속성값

문제에서 요구하는 파티션 타입, 파티션 용량을 확인할 수 있다. 아까 에러가 났던 것이 신경이 쓰여서 이번엔 마운팅이 아닌 FTK imager를 통하여 문제의 파일을 열어보자.

[그림 4] USB의 Tree

다음과 같이 나타나는 것을 알 수 있었다.

Basic disk 부분을 제외하면 Partition 1 만 남는 것을 확인할 수 있다. 그렇다면 이 Partition 1 이 파티션의 이름일 것이다. 그렇다면 용량은 아까 나온 값을 정답일 것이고, Partition 1 의 시그니처를 조사하여 파일시스템을 다시 한번 확인해 볼 수 있겠다.



[그림 5] Partition 1의 시그니처

시그니처를 확인해 보면 파티션 타입은 NTFS임을 확인할 수 있다. 파티션 타입에 대한 정답을 바

꿔야 할 필요성이 있다.

마지막으로 볼륨은 cmd창에서 vol D: 명령어를 통해서 확인할 수 있을 것이다.

[그림 6] vol D: 명령어 실행 결과

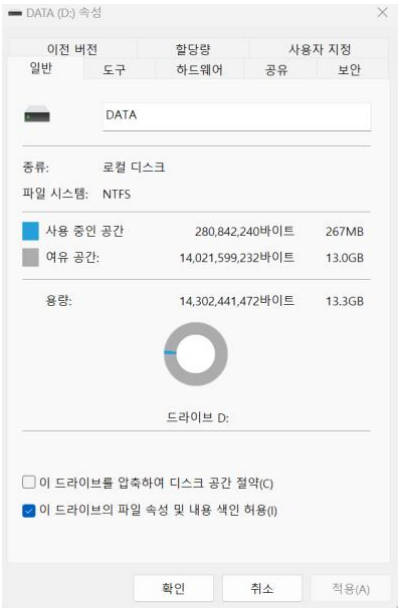
확실히 마운팅이 실패한 것 같다. 안에 파일은 다 보이는데 로컬적인 문제인 것 같다. 다른 Write-Up 을 참고한 사진을 첨부하겠다.

문제를 찾아보니 **Window 11 Home 과 FTK Imager 의 호환 문제였다. 다른 마운팅 툴인 OSPMount 를 사용하여 마운팅을 재시도하였다.**

[그림 7] OSFMount를 사용한 마운팅 결과

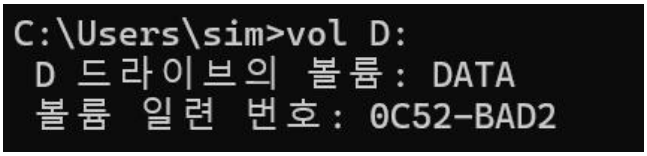
[그림 8] 정상적으로 마운팅 된 모습

드디어 정상적으로 마운팅이 완료되었다.



[그림 9] 정상적 폴더의 속성값

역시나 파티션 타입은 NTFS 가 맞음을 확인할 수 있다. 마지막으로 cmd 창을 이용하여 시리얼 넘버만 구하는 것이 남았다.



[그림 10] vol D: 결과값

1번 문항의 정답을 정리해보면,

Partition Type : NTFS

Partition Name : Partition 1

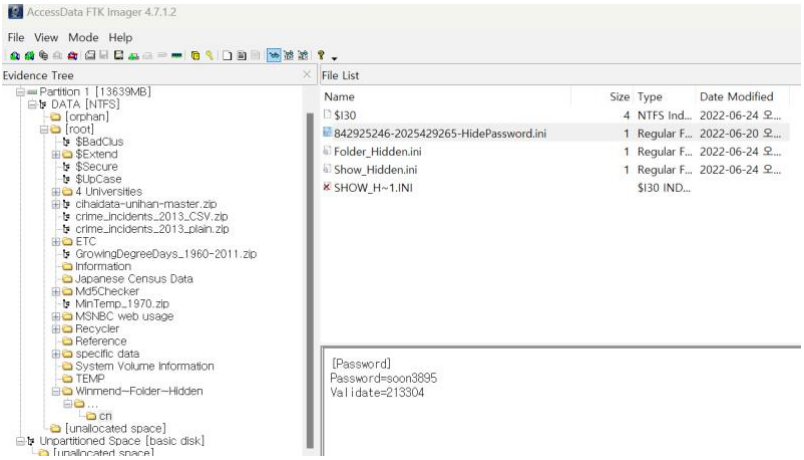
Volume Serial Number : 0C52-BAD2

Size of the USB's partition(s) : 13.3GB

이 될 것이다. 다음 문제로 넘어가자.

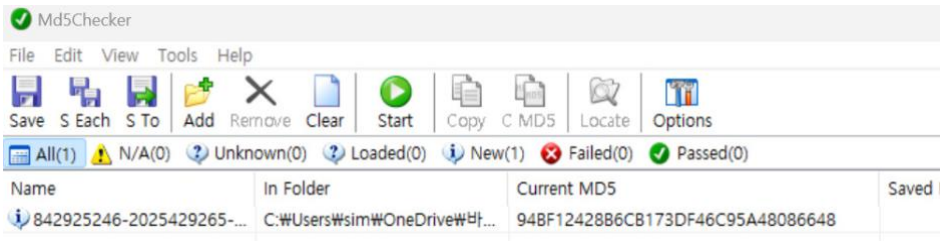
Find all the data Trudy tried to hide and leak and calculate the MD5 hash of the data.

이제 본 문제로 넘어온 것 같다. 먼저 FTK Imager 로 해당 파티션을 조사해보았다. 파일을 쭉 읽어보다가 Winmend~Folder~Hidden 이란 폴더가 수상해서 찾아보던 중 cn 폴더 폴더 안에서 다음과 같은 파일을 발견하였다.



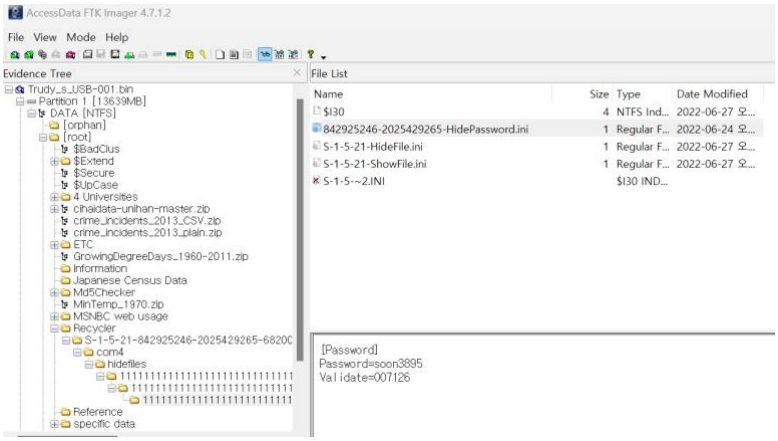
[그림 11] cn 파일 내부

파일의 내용과 시간에 의거하여 해당 파일은 트루디가 숨기려고 한 파일인 것 같다. export 하여 Md5Checker 에서 값을 추출하면 MD5 값을 알 수 있다.



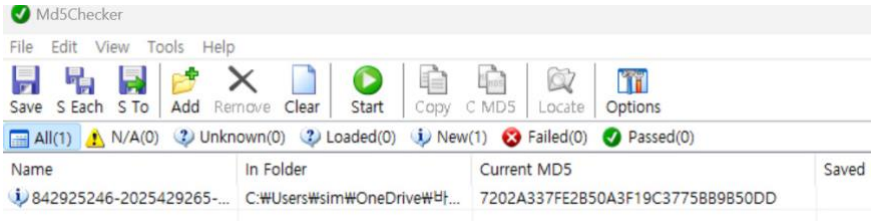
[그림 12] HidePassword.ini 파일 MD5 값

Recycler 폴더를 찾아보던 중에도 폴더 안에서 hidefiles 폴더을 확인할 수 있었다. 이 내용이 수상하여 조사를 하였더니 다음과 같은 파일을 찾을 수 있었다.



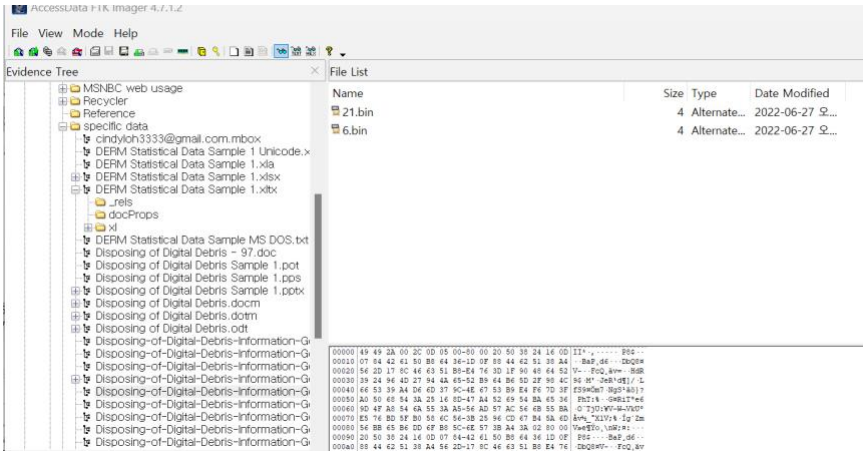
[그림 13] Recycler 폴더 내부

같은 내용의 파일이었지만 다른 파일이었다. 그렇기 때문에 추출되는 MD5가 다를 것이다. 이 파일도 트루디가 숨기려고 한 파일일 것이다. MD5Checker로 파일을 추출하면 MD5 값을 알 수 있다.



[그림 14] HidePassword.ini.copy 파일 MD5값

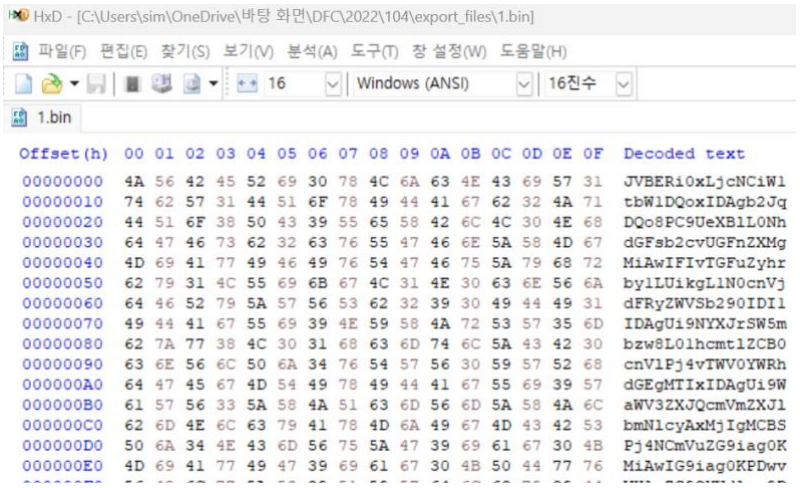
이를 제외하고도 specific data 폴더에서 이상한 파일들을 확인할 수 있었다.



[그림 15] specific data 폴더 내부

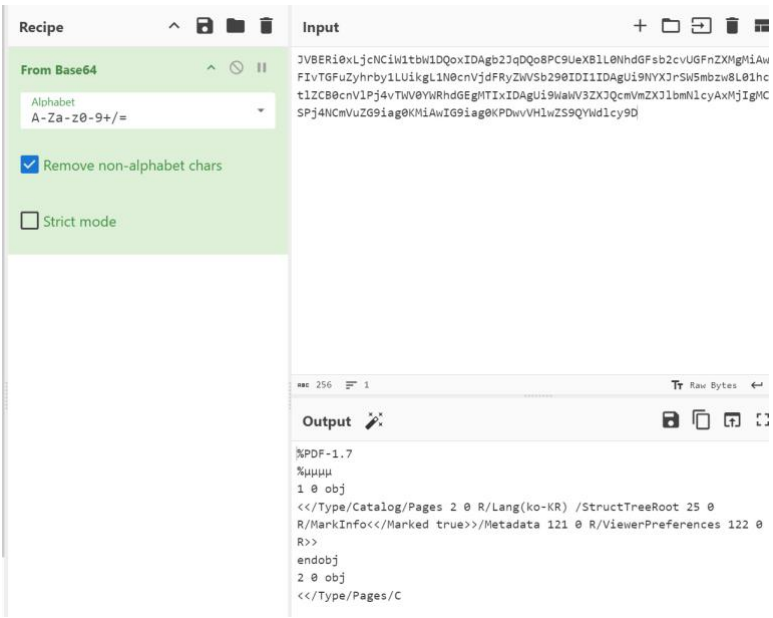
그림 15 와 같이 .bin 확장자의 파일이 폴더 곳곳에 1~37 까지 저장되어 있는 것을 확인하고 이를 추출시켰다.

먼저 파일 형식을 분석하기 위하여 HxD 를 통하여 파일을 분석하였다.



[그림 16] 1.bin HxD 분석

처음 보고 이게 뭐지? 라는 생각이 들었다. 한번도 본적 없는 형식의 시그니처이기 때문이다. 검색을 통해서도 확인할 수 없었다. **그렇다면 이 파일의 시그니처는 난독화가 되어있을 확률이 높다고 추측했다.**



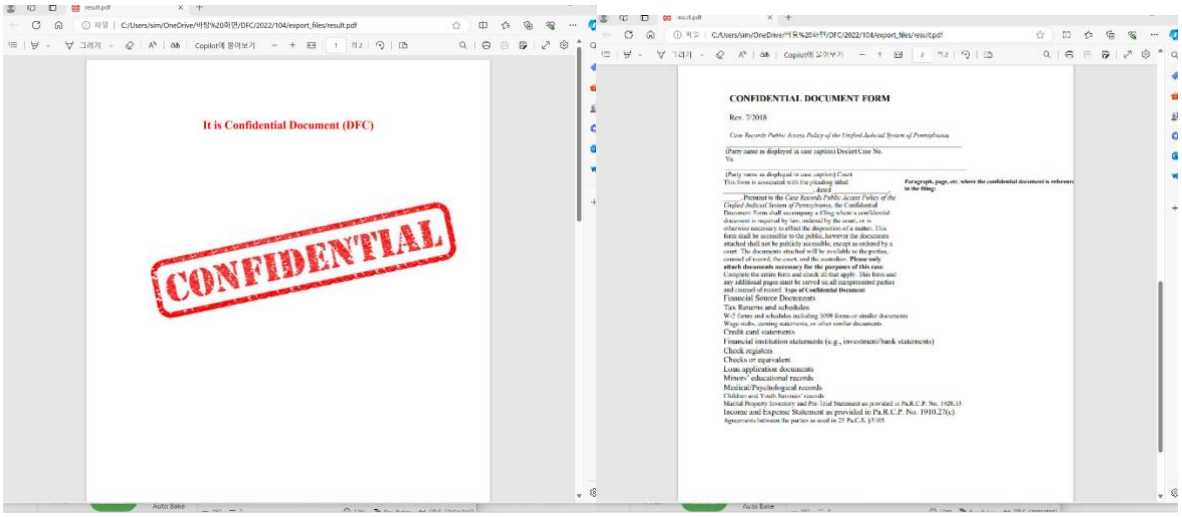
[그림 17] CyberChef를 통한 Base64 복호화

역시나 Base64 를 통하여 암호화되어있는 파일이었다. 그렇다면 복호화된 1~37 파일을 하나로 모으면 하나의 pdf 파일이 될 것이라고 예측할 수 있다.

그렇다면 이를 코드로 구현해보자.

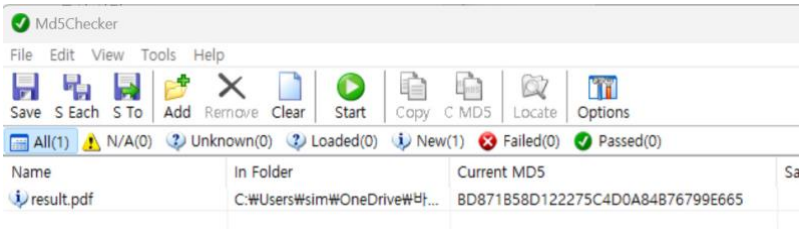
```
import base64

data=""

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

f = open('result.pdf','wb')

data_byte=data.encode('utf-8')
data_base64=base64.b64decode(data_byte)

f.write(data_base64)
f.close()
```

다양한 코드가 나올 수 있겠지만 풀이자는 다음과 같이 코드를 작성하였다. data 변수에 1~37 파일의 내용을 붙히고, 이 내용을 Base64 복호화를 진행하여 하나의 파일을 만드는 형식으로 진행하였다. 코드 실행 결과는 다음과 같았다.



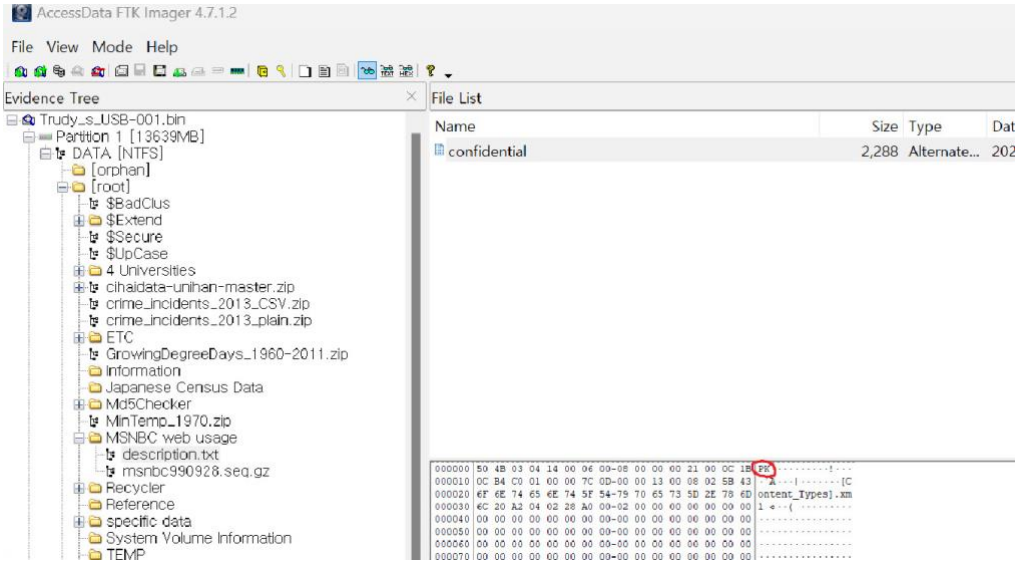
[그림 18, 19] result.pdf 파일 내부

다음과 같은 결과를 얻을 수 있었는데 confidential document 인 것으로 이 폴더 또한 트루디가 난독화하여 숨기려고 한 파일임을 알 수 있다.



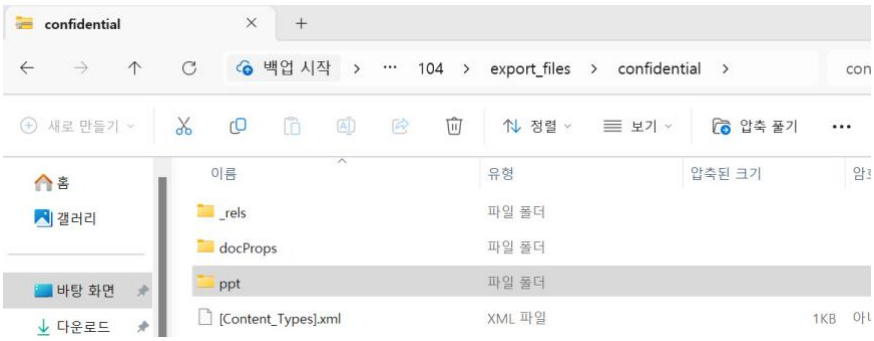
[그림 20] result.pdf MD5 값

마지막 증거는 MSNBC web usage 폴더의 description.txt 파일을 조사할 때 나왔다. confidential 파일을 추출해도 열리지 않아 수상하게 여겨졌다.



[그림 21] MSNBC web usage 폴더 내부

그림 21 을 참고하면 confidnetai 파일의 시그니처를 확인할 수 있는데, 빨간 동그라미 부분인 PK 를 확인할 수 있었다. **이를 통하여 트루디가 확장자를 변경하거나 삭제하여 파일을 은닉한 것을 예측할 수 있다. 그렇다면 .zip 확장자를 넣어서 파일을 확인할 수 있다.**

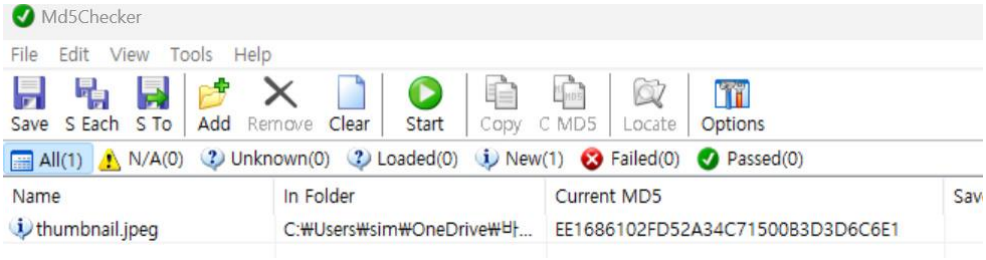


[그림 22] 확장자를 변경하여 열린 confidential 파일

이를 조사중에 docProps 폴더 안에서 thumbnail.jpg 를 확인할 수 있었다.

[그림 23] thumbnail.jpg

thumbnail.jpg 파일의 내용은 아까 result.pdf 에서도 확인할 수 있었던 내용과 일치했다. 이 내용 또한 트루디가 은닉을 시도한 파일일 것이다.



[그림 24] thumbnail.jpeg의 MD5 값

지금까지 구한 모든 파일과 MD5 값을 정리하면 다음과 같다.

HidePasswod.ini.copy - 7202A337FE2B50A3F19C3775BB9B50DD

HidePassword.ini - 94BF12428B6CB173DF46C95A48086648

result.pdf - BD871B58D122275C4D0A84B76799E665

thumbnail.jpeg - EE1686102FD52A34C71500B3D3D6C6E1

5. Flag

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

Partition Type : NTFS

Partition Name : Partition 1

Volume Serial Number : 0C52-BAD2

Size of the USB's partition(s) : 13.3GB

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

HidePasswod.ini.copy - 7202A337FE2B50A3F19C3775BB9B50DD

HidePassword.ini - 94BF12428B6CB173DF46C95A48086648

result.pdf - BD871B58D122275C4D0A84B76799E665

thumbnail.jpeg - EE1686102FD52A34C71500B3D3D6C6E1

6. 별도 첨부

7. Reference

- [URL]