205 – Wake up from hibernation

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 result of the search and seizure of the suspect's house related to the company's information leak, a USB formatted with the FAT file system was found. The files on the USB were wiped and the contents could not be recovered.

The given file is the hiberfil.sys file obtained from the company Laptop used by the suspect. Analyze the file to identify the file that the suspect appears to have copied to the USB.

Target	Hash (MD5)
hiberfil.zip	FCCC42376AB6A3C4720E9C2FDA14B82E

Questions

1. What files are suspected of being copied to the USB by the suspect? What is the basis for that judgment? (100 points)
2. What is the manufacturer, model, and serial number of the USB used by the suspect? (100 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:	HxD	**Publisher:**	Maël Hörz
Version:	2.5.0.0 (x86-64)		
URL:	https://mh-nexus.de/en/hxd/		

Name:	Bulk Extractor	**Publisher:**	Maël Hörz
Version:	1.5.5		
URL:	https://mh-nexus.de/en/hxd/		

Name:	Hibr2Bin	**Publisher:**	Comae Toolkit
Version:	3.0		
URL:	https://github.com/comaeio/Hibr2Bin		

Name:	Recall	**Publisher:**	Google
Version:	1.7.1		
URL:	http://www.rekall-forensic.com/		

Step-by-step methodology:

1. What files are suspected of being copied to the USB by the suspect? What is the basis for that judgment?

Windows는 hiberfil.sys 파일을 효율적으로 관리하기 위해 휘발성 메모리 데이터를 압축해 저장한다.[1] 따라서 hiberfil.sys 파일을 분석하기 위하여 압축 해제 도구 Hibr2Bin[2]을 실행했고, 압축 해제된 메모리 데이터(uncompressed.bin)가 생성됐다.

```
>Hibr2Bin.exe /PLATFORM X64 /MAJOR 10 /MINOR 0 /INPUT hiberfil.sys /OUTPUT uncompressed.bin
```

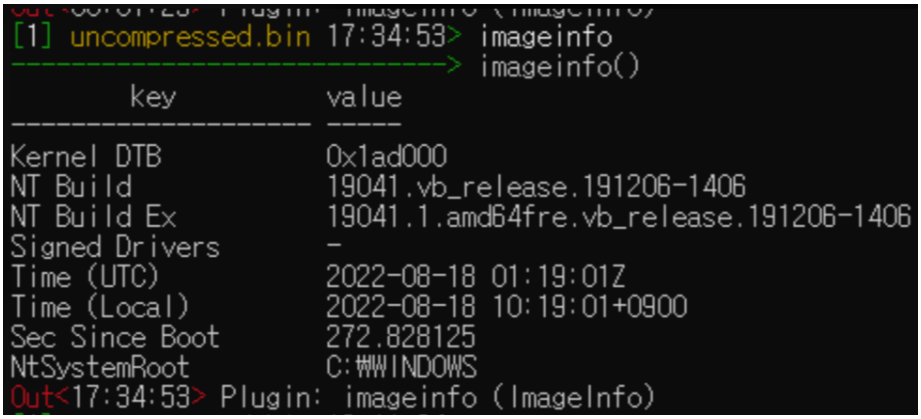
[그림 1] Hibr2Bin.exe Command (cmd.exe)

[그림 2] Hibr2Bin.exe Result (cmd.exe)

메모리 분석 도구인 Rekall을 사용해 확인한 결과, imageinfo 플러그인으로 컴퓨터 운영체제 버전은 Win10x64_19041이고, 컴퓨터 종료 시각은 2022-08-18 10:19:01임을 발견했다.

[1] Windows 10 내의 hiberfil.sys 파일에 대한 포렌식 활용 방안.pdf

[2] Comae Hibernation File Decompressor (SANDMAN project)



[그림 3] Rekall imageinfo plugin (cmd.exe)

운영체제는 필요한 드라이버를 로드 시 Pool Memory 공간을 할당하여 해당 드라이버를 나타내는 4 Bytes 문자인 Pool Tag를 작성한다.[3] 만약 Windows10 운영체제의 NTFS 파일시스템에서 FAT 파일시스템 관련 Pool Tag가 발견된다면, FAT 파일시스템으로 포맷된 외부 저장 장치가 연결되었음을 증명할 수 있다.

FAT 파일 시스템의 Pool Tag 목록은 다음 사진과 같으며, 파일명 버퍼인 "Fatn" Tag를 분석하면 외부 저장 장치로 복사된 파일명을 확인할 수 있다.

Pool Tag	Source Description
Fat	Fat File System allocations
FatB	Fat allocation bitmaps
FatC	Fat Ccbs
FatE	Fat EResources
FatF	Fat Fcbs
FatI	Fat IrpContexts
FatN	Fat Nonpaged Fcbs
FatO	Fat I/O buffer
FatV	Fat Vcb stat bucket
FatW	Fat FAT windowing structure
FatX	Fat IO contexts
Fatf	Fat deferred flush contexts
Fati	Fat IO run descriptor
Fatn	Fat filename buffer
Fatv	Fat events
Fatx	Fat delayed close contexts

[3] Windows 10 내의 hiberfil.sys 파일에 대한 포렌식 활용 방안.pdf

[그림 4] FAT file system – Pool Tag[4]

Hex Editor 프로그램(HxD)로 "Fatn" 검색 서치 결과, FAT 파일시스템의 외부 저장 장치에 존재하였던 총 25건의 파일명을 얻을 수 있었고 결과는 다음 표로 정리한다.

Idx	Fatn filename buffer
1	SYSTEM VOLUME INFORMATION.WOFI
2	INDEXERVOLUMEGUID
3	AUTORUN.INF
4	8_5X11-PORTABLE-CASE-QUICK-START.PDF
5	DESKTOP.INI
6	BCD.LOG
7	\EFI\Microsoft
8	Microsoft
9	\System Volume InformationtaF8F5037
10	System Volume Informationt1923F573B29
11	AadRecoveryPasswordDeleted.l.91EB8B
12	AadRecoveryPasswordDeleteon1.EFB8B
13	ClientRecoveryPasswordRotation
14	\System Volume Information\AadRecoveryPasswordDelete
15	\System Volume Information\WPSettings.dat
16	\System Volume Information\AadRecoveryPasswordDeletell
17	\System Volume Information\ClientRecoveryPasswordRotation
18	Autorun.inf
19	CustomerData.xlsx
20	WPSettings.dat
21	\$RECYCLE.BIN\desktip.ini
22	IndexerVolumeGuid
23	\System Volume Information\IndexerVolumeGuid
24	\EFI\Microsoft\Bootume1
25	\EFI\Microsoft\Boot\BCD.LOG

[표 1] Fatn file buffer list

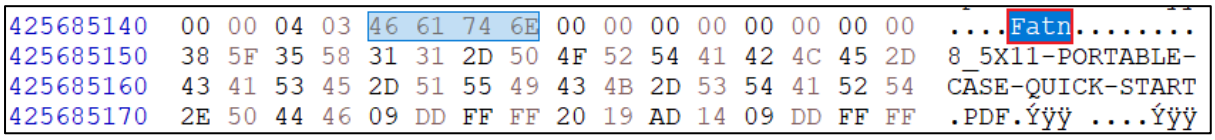
[4] Windows 10 내의 hiberfil.sys 파일에 대한 포렌식 활용 방안.pdf

Fatn filename buffer의 버퍼 크기를 알 수 없어 파일명으로 추정되는 영역을 초과로 추출하여, [표 1]의 파일명이 완전하지 않을 수 있음을 분석 시 감안해야 한다.

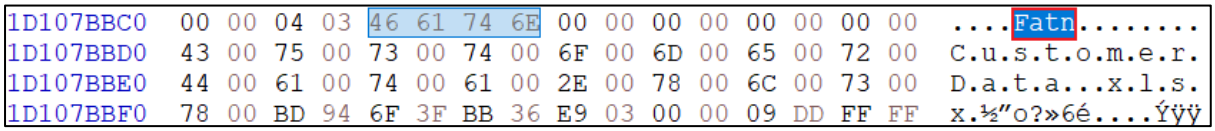
총 25건의 검색 결과에서 시스템 관련 파일을 제외함으로써 최종적으로 용의자가 유출하려던 자료는 pdf 1개와 xlsx 1개이다.

- **8_5X11-PORTABLE-CASE-QUICK-START.PDF**
- **CustermerData.xlsx**

2개의 유출 자료의 "Fatn" 실제 검색 결과는 다음 사진으로 첨부한다.



[그림 5] 메모리 파일(uncompressed.bin) 내 Fatn Tag - pdf (HxD.exe)



[그림 6] 메모리 파일(uncompressed.bin) 내 Fatn Tag – xlsx (HxD.exe)

2. What is the manufacturer, model, and serial number of the USB used by the suspect?

컴퓨터와 연결했던 외부 저장 장치는 레지스트리에 일련의 형식으로 기록되는데, USB의 여러 기록 형식 중에서 다음 형식으로도 기록된다.

- USBSTOR#Disk&Ven_[ven]&Prod_[prod]&Rev_[rev]#[serialnumber]

USBSTOR 하위키 내에서 [ven]은 USB 제조업체, [prod]는 USB 모델명, [rev]는 USB 버전번호, [serialnumber]는 USB 시리얼번호를 의미한다. 따라서 USBSTOR 레지스트리 키를 발견하여 용의자가 사용했던 USB의 정보를 얻고자 한다.

본 분석가는 Hiberfil.sys 파일을 압축 해제한 휘발성 메모리 데이터(uncompressed.bin)에서 Hex Editor(HxD)로 "USBSTOR#Disk&Ven_"을 검색했으며, 검색 결과를 중복 제거하여 다음 표에 정리한다.

Idx	USBSTOR 하위키
1	USBSTOR#Disk&Ven_ADATA&Prod_USB_Flash_Drive&Rev_1100#151261308003001C&0
2	USBSTOR#Disk&Ven_SanDisk&Prod_ExtremePro&Rev_0001#AA0111071502171201 94&0
3	USBSTOR#Disk&Ven_Samsung&Prod_Flash_Drive&Rev_1100#03731170900157 04&0

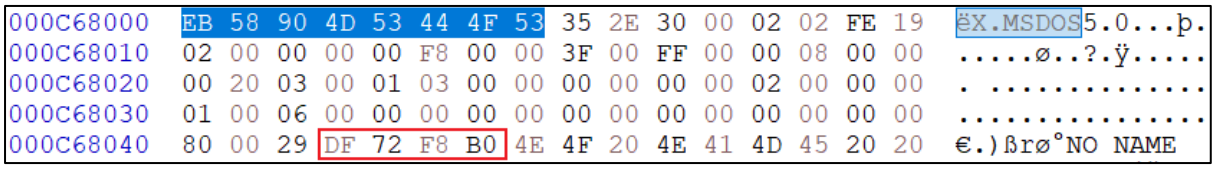
[표 2] USBSTOR 하위키 목록

검색 결과 총 3건의 USB가 발견됐으므로, 어떤 외부 저장 장치가 FAT 파일시스템으로 포맷되었는지 판단할 필요가 있다. 휘발성 메모리 데이터 내에 FAT 파일 시스템이 남아 있는지 확인하기 위해 FAT Reserved Area(예약된 영역) 데이터를 검색한다.

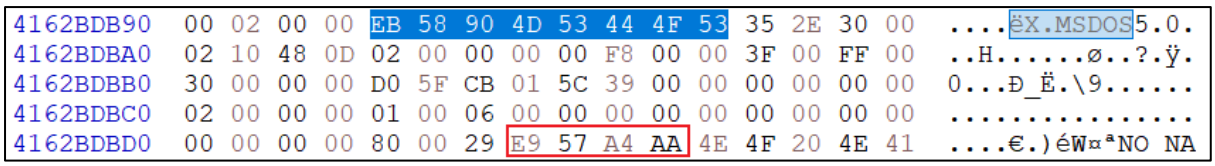
- FAT Reserved Area (Signature) : EB 58 90 4D 53 44 4F 53

검색 결과, VSN(Volume Serial Number)을 비교 후 결과를 중복 제거하여, 총 3건의

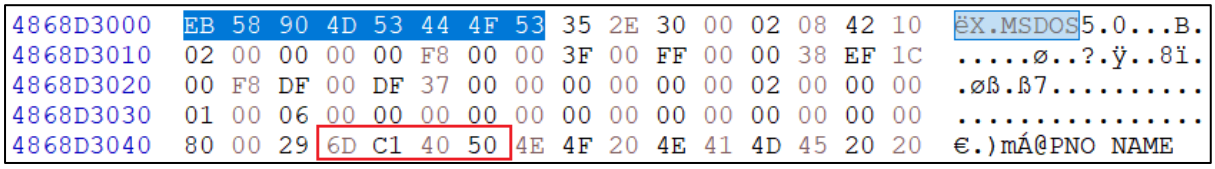
FAT Reserved Area와 예약된 영역 내 VSN이 확인됐다.



[그림 7] FAT file system – VSN B0F872DF (HxD.exe)

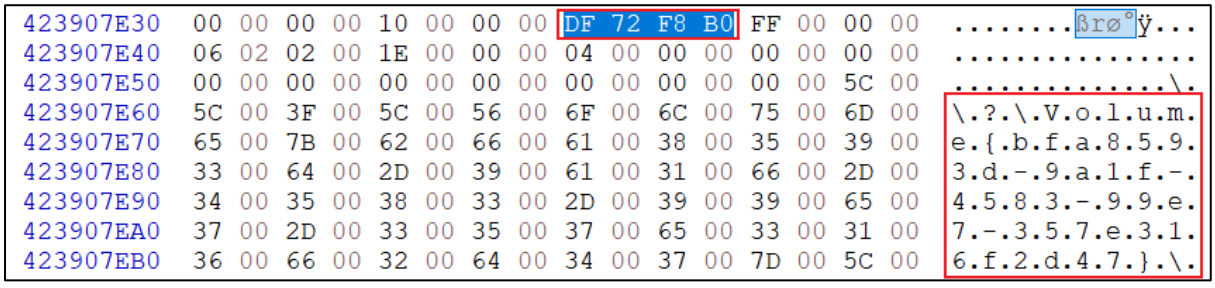


[그림 8] FAT file system – VSN AAA457E9 (HxD.exe)

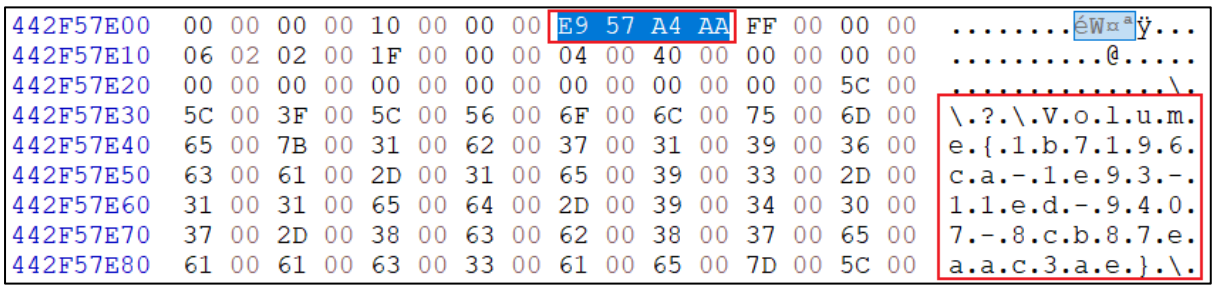


[그림 9] FAT file system – VSN 5040C16D (HxD.exe)

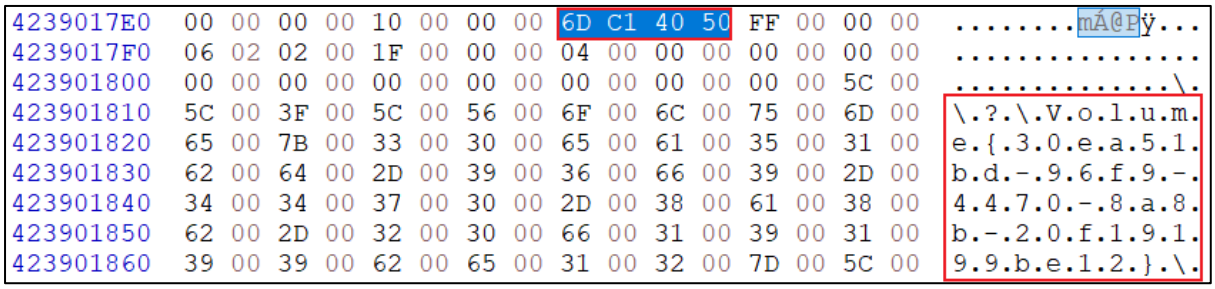
발견한 FAT 파일시스템의 VSN(little endian)을 검색하면, 볼륨의 GUID를 확인할 수 있다.



[그림 10] FAT file system – VSN B0F872DF의 Volume GUID (HxD.exe)



[그림 11] FAT file system – VSN AAA457E9의 Volume GUID (HxD.exe)



```
4239017E0  00 00 00 00 10 00 00 00 6D C1 40 50 FF 00 00 00  ........mÁ@Pÿ...
4239017F0  06 02 02 00 1F 00 00 00 04 00 00 00 00 00 00 00  ................
423901800  00 00 00 00 00 00 00 00 00 00 00 00 00 00 5C 00  ..............\.
423901810  5C 00 3F 00 5C 00 56 00 6F 00 6C 00 75 00 6D 00  \.?.\.V.o.l.u.m.
423901820  65 00 7B 00 33 00 30 00 65 00 61 00 35 00 31 00  e.{.3.0.e.a.5.1.
423901830  62 00 64 00 2D 00 39 00 36 00 66 00 39 00 2D 00  b.d.-.9.6.f.9.-.
423901840  34 00 34 00 37 00 30 00 2D 00 38 00 61 00 38 00  4.4.7.0.-.8.a.8.
423901850  62 00 2D 00 32 00 30 00 66 00 31 00 39 00 31 00  b.-.2.0.f.1.9.1.
423901860  39 00 39 00 62 00 65 00 31 00 32 00 7D 00 5C 00  9.9.b.e.1.2.}.\.
```

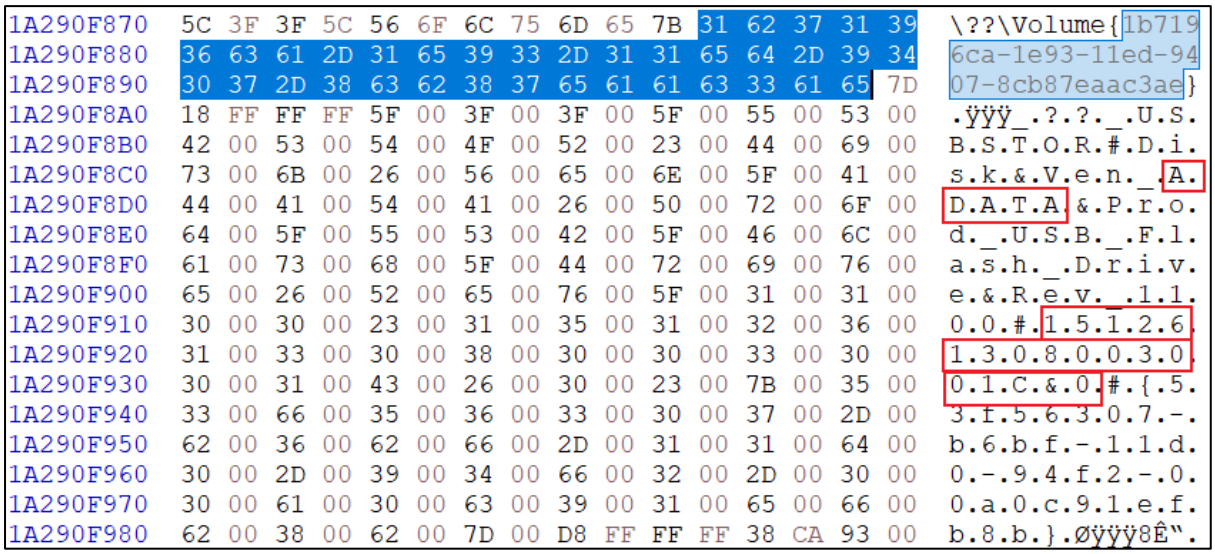
[그림 12] FAT file system – VSN 5040C16D의 Volume GUID (HxD.exe)

지금까지 발견한 FAT 파일시스템의 볼륨 정보를 정리하면 다음 표와 같다.

idx	VSN	Volume GUID
1	B0F872DF	₩Volume{bfa8593d-9a1f-4583-99e7-357e316f2d47}
2	AAA457E9	₩Volume{1b7196ca-1e93-11ed-9407-8cb87eaac6ae}
3	5040C16D	₩Volume{30ea51bd-96f9-4470-8a8b-20f19199be12}

[표 3] FAT file system Volume information

최종적으로 3개의 FAT Volume GUID를 검색한 결과, 단 하나의 Volume GUID만 "USBSTOR#"이 발견됐다. 해당 GUID는 [₩Volume{1b7196ca-1e93-11ed-9407-8cb87eaac6ae}]이며, USB는 ADATA 제조업체의 USB이다.



```
1A290F870  5C 3F 3F 5C 56 6F 6C 75 6D 65 7B 31 62 37 31 39  \??\Volume{1b719
1A290F880  36 63 61 2D 31 65 39 33 2D 31 31 65 64 2D 39 34  6ca-1e93-11ed-94
1A290F890  30 37 2D 38 63 62 38 37 65 61 61 63 33 61 65 7D  07-8cb87eaac3ae}
1A290F8A0  18 FF FF FF 5F 00 3F 00 3F 00 5F 00 55 00 53 00  .ÿÿÿ_.?.?._.U.S.
1A290F8B0  42 00 53 00 54 00 4F 00 52 00 23 00 44 00 69 00  B.S.T.O.R.#.D.i.
1A290F8C0  73 00 6B 00 26 00 56 00 65 00 6E 00 5F 00 41 00  s.k.&.V.e.n._.A.
1A290F8D0  44 00 41 00 54 00 41 00 26 00 50 00 72 00 6F 00  D.A.T.A.&.P.r.o.
1A290F8E0  64 00 5F 00 55 00 53 00 42 00 5F 00 46 00 6C 00  d._.U.S.B._.F.l.
1A290F8F0  61 00 73 00 68 00 5F 00 44 00 72 00 69 00 76 00  a.s.h._.D.r.i.v.
1A290F900  65 00 26 00 52 00 65 00 76 00 5F 00 31 00 31 00  e.&.R.e.v._.1.1.
1A290F910  30 00 30 00 23 00 31 00 35 00 31 00 32 00 36 00  0.0.#.1.5.1.2.6.
1A290F920  31 00 33 00 30 00 38 00 30 00 30 00 33 00 30 00  1.3.0.8.0.0.3.0.
1A290F930  30 00 31 00 43 00 26 00 30 00 23 00 7B 00 35 00  0.1.C.&.0.#.{.5.
1A290F940  33 00 66 00 35 00 36 00 33 00 30 00 37 00 2D 00  3.f.5.6.3.0.7.-.
1A290F950  62 00 36 00 62 00 66 00 2D 00 31 00 31 00 64 00  b.6.b.f.-.1.1.d.
1A290F960  30 00 2D 00 39 00 34 00 66 00 32 00 2D 00 30 00  0.-.9.4.f.2.-.0.
1A290F970  30 00 61 00 30 00 63 00 39 00 31 00 65 00 66 00  0.a.0.c.9.1.e.f.
1A290F980  62 00 38 00 62 00 7D 00 D8 FF FF FF 38 CA 93 00  b.8.b.}.Øÿÿÿ8Ê".
```

[그림 12] FAT file system – Volume GUID 검색 (HxD.exe)

[그림 12]에서 USBSTOR 하위키의 제조업체가 ADATA 제품이며 일련번호가 "1512613080003001C"인 것으로 미루어 보아, 앞서 [표 2] USBSTOR 하위키 목록 내 ADATA 제품의 일련번호와 동일하므로 3개의 USB에서 ADATA USB만이 FAT 파일시스템임을 증명한다.

따라서 용의자가 회사 자료를 유출할 때 사용하던 FAT 파일시스템의 USB는 다음과 같은 정보를 지닌다.

- **제조업체 : ADATA**
- **모델명 : USB_Flash_Drive**
- **일련번호 : 151261308003001C**