

Write-up: Find the USB (DreamHack Forensics Challenge)

<https://dreamhack.io/wargame/challenges/1324>

[1. Challenge Info](#)

[2. Problem Description](#)

[3. Provided Files](#)

[4. Tools Used](#)

[5. Analysis Steps](#)

[5.1 디스크 이미지 마운트](#)

[5.2 레지스트리에서 USB 정보 탐색](#)

[5.3 최종 정보 정리](#)

[6. Flag](#)

1. Challenge Info

- **Challenge Name:** Find the USB
- **Category:** Forensics
- **Difficulty Level:** Level 1
- **Platform:** DreamHack Wargame
- **Objective:**

드림이의 컴퓨터에 누군가 연결한 USB 저장장치의 VID, PID, DeviceSerialNumber를 찾아서 플래그를 완성하라.

플래그 형식: DH{VID_PID_DeviceSerialNumber}

2. Problem Description

"드림이의 컴퓨터에 누군가가 USB 저장장치를 연결했다가 해제한 것 같아요.
사건이 발생한 시간은 2024년 4월이라고 합니다.
Windows 레지스트리를 분석해 연결된 USB 정보를 찾아낼 수 있을까요?"

- 제공된 디스크 이미지: `DiskImage.E01`
- 이 파일은 `Autoruns`, `Track_the_file` 문제와 동일

3. Provided Files

- `DiskImage.E01` (Windows 시스템의 디스크 이미지 파일, E01 포맷)

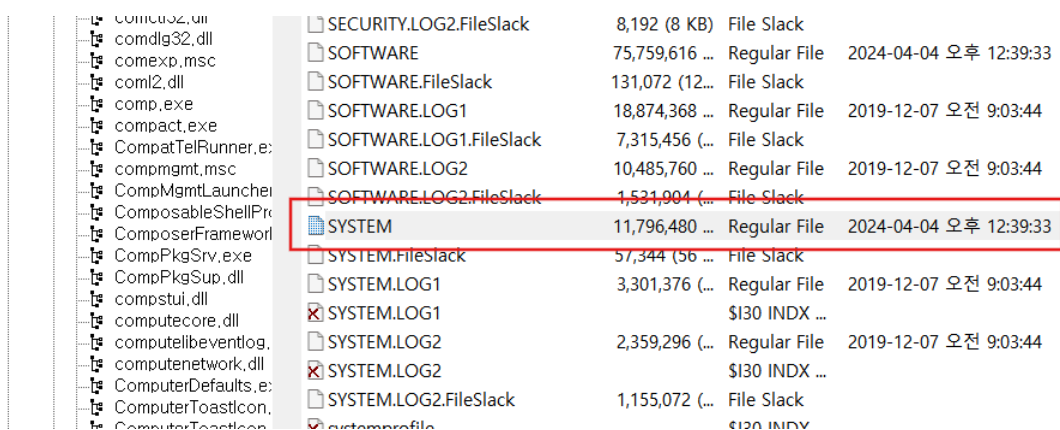
4. Tools Used

Tool	Version
FTK Imager	v4.7.8.31
Registry Explorer	v2.1.0

5. Analysis Steps

5.1 디스크 이미지 마운트

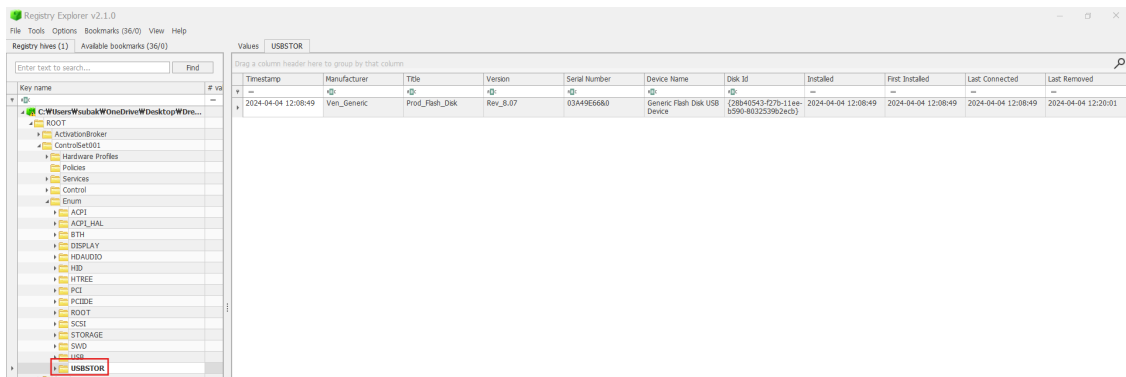
- 도구: FTK Imager
- 제공된 **DiskImage.E01** 파일을 FTK Imager로 열기
- SYSTEM 레지스트리 하이브 파일 추출
 - 경로: **C:\Windows\System32\config\SYSTEM**



comctl32.dll	SECURITY.LOG2.FileSlack	8,192 (8 KB)	File Slack	
comdlg32.dll	SOFTWARE	75,759,616 ...	Regular File	2024-04-04 오후 12:39:33
comexp.msc	SOFTWARE.FileSlack	131,072 (12...	File Slack	
coml2.dll	SOFTWARE.LOG1	18,874,368 ...	Regular File	2019-12-07 오전 9:03:44
comp.exe	SOFTWARE.LOG1.FileSlack	7,315,456 (...)	File Slack	
compact.exe	SOFTWARE.LOG2	10,485,760 ...	Regular File	2019-12-07 오전 9:03:44
CompatTelRunner.exe	SOFTWARE.LOG2.FileSlack	1,531,904 (...)	File Slack	
compmgmt.msc	SYSTEM	11,796,480 ...	Regular File	2024-04-04 오후 12:39:33
CompMgmtLauncher.exe	SYSTEM.FileSlack	57,344 (56 ...)	File Slack	
ComposableShellPr...	SYSTEM.LOG1	3,301,376 (...)	Regular File	2019-12-07 오전 9:03:44
ComposerFramework...	SYSTEM.LOG1		\$I30 INDX ...	
CompPkgSrv.exe	SYSTEM.LOG2	2,359,296 (...)	Regular File	2019-12-07 오전 9:03:44
CompPkgSup.dll	SYSTEM.LOG2		\$I30 INDX ...	
compstui.dll	SYSTEM.LOG2.FileSlack	1,155,072 (...)	File Slack	
compute-core.dll	SYSTEM.LOG2		\$I30 INDX ...	
computelibraryeventlog...	SYSTEM.LOG2.FileSlack		File Slack	
computenetwork.dll	SYSTEM.LOG2		\$I30 INDX ...	
ComputerDefaults.e...	SYSTEM.LOG2		\$I30 INDX ...	
ComputerToastscon...	SYSTEM.LOG2		\$I30 INDX ...	
ComputerToastscon...	SYSTEM.LOG2		\$I30 INDX ...	

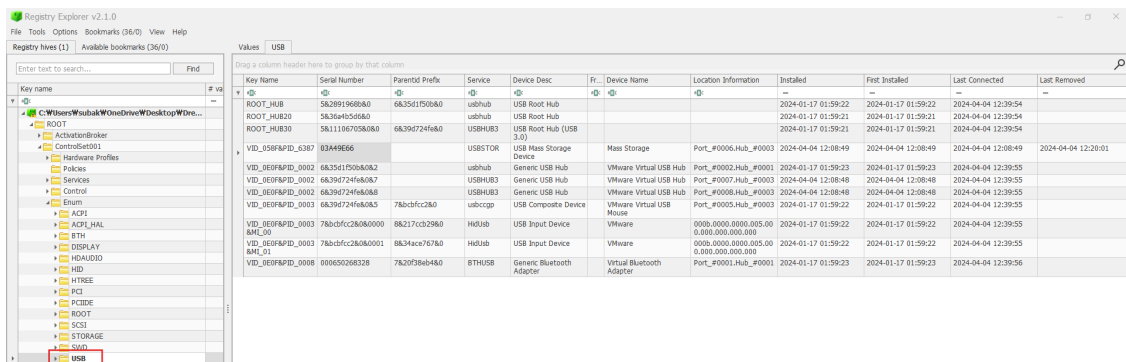
5.2 레지스트리에서 USB 정보 탐색

- 도구: Registry Explorer
- 추출한 **SYSTEM** 하이브를 Registry Explorer로 열기
- 경로: **SYSTEM\ROOT\ControlSet001\Enum\USBSTOR**
- 하위 키에서 Serial Number 확인
 - Serial Number: **03A49E66**



Values USBSTOR					
Drag a column header here to group by that column					
Timestamp	Manufacturer	Title	Version	Serial Number	
2024-04-04 12:08:49	Ven_Generic	Prod_Flash_Disk	Rev_8.07	03A49E66&0	

- 경로: **SYSTEM\CurrentControlSet\Enum\USB**
- 하위 키에서 PID 및 VID 확인
 - **VID: 058F**
 - **PID: 6387**



Values USB					
Drag a column header here to group by that column					
Key Name	Serial Number	Parentid Prefix	Service	Device Desc	
ROOT_HUB	5&2891968b&0	6&35d1f50b&0	usbhub	USB Root Hub	
ROOT_HUB20	5&36a4b5d6&0		usbhub	USB Root Hub	
ROOT_HUB30	5&1110670580&0	6&39d724fe&0	USBHUB3	USB Root Hub (USB 3.0)	
VID_058F&PID_6387	03A49E66		USBSTOR	USB Mass Storage Device	
VID_REFR&PID_0002	6&35d1f50b&0&2		usbhub	Generic USB Hub	

5.3 최종 정보 정리

- VID: 058F
- PID: 6387
- Serial Number: 03A49E66

6. Flag


DH{058F_6387_03A49E66}

축하합니다!

1 LEVEL 1 Find the USB
문제를 해결했습니다.

대단해요. 문제를 어떻게 해결하셨나요?
풀이를 작성하면 포인트까지 받을 수 있어요.

괜찮아요

 풀이 작성하기