

## 8) 관련 워게임 풀이

### 1. Find the USB

1

LEVEL 1

## Find the USB

forensics

466 155 2024.10.02. 09:22:21

문제 파일 받기

문제 정보 풀이 11 난이도 투표 11 질문 최근 풀이 0

### 문제 설명

#### Description

[함께실습] Find the USB에서 실습하는 문제입니다.

드림이의 컴퓨터에 누군가가 USB 저장장치를 연결했다가 해제한 것 같아요.

사건이 발생한 시간은 2024년 4월이라고 합니다.

Windows 레지스트리를 분석해 연결된 USB 정보를 찾아낼 수 있을까요?

```
DRIVERS
DRIVERS.LOG1
DRIVERS.LOG2
DRIVERS{53b39e70-18c4-11ea-a811-53b39e70-18c4-11ea-a811}
DRIVERS{53b39e70-18c4-11ea-a811}
ELAM
ELAM.LOG1
ELAM.LOG2
ELAM{53b39eac-18c4-11ea-a811-53b39eac-18c4-11ea-a811}
ELAM{53b39eac-18c4-11ea-a811-53b39eac-18c4-11ea-a811}
Journal
RegBack
SAM
SAM.LOG1
SAM.LOG2
SECURITY
SECURITY.LOG1
SECURITY.LOG2
SOFTWARE
SOFTWARE.LOG1
SOFTWARE.LOG2
SYSTEM
SYSTEM.LOG1
SYSTEM.LOG2
systemprofile
TxF
configmanager2.dll
Configuration
ConfigureExpandedStorage.dll
conhost.exe
```

이름	수정된 날짜	유형	크기
SYSTEM	2024-04-04 오후 9:39	파일	11.520KB

문제 디스크 이미지에서 FTK Imager을 사용해, SYSTEM 하이브만 추출해냈다.

Registry Explorer v2.1.0

File Tools Options Bookmarks (36/0) View Help

Registry hives (1) Available bookmarks (36/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
C:\Users\W82104\Download...	0	17	2024-04-04 12:39:46
ROOT	0	1	2019-12-07 09:15:07
ActivationBroker	0	1	2019-12-07 09:15:07
ControlSet001	0	5	2019-12-07 09:15:07
Control	12	124	2024-04-04 12:40:01
Enum	21	15	2024-04-04 12:08:49
ACPI	0	15	2024-01-17 01:59:18
ACPI_HAL	0	1	2024-01-17 01:59:18
BTH	0	3	2024-01-17 01:59:23
DISPLAY	0	1	2024-01-17 01:59:23
HDAUDIO	0	1	2024-01-17 01:59:22
HID	0	2	2024-01-17 01:59:22
HTREE	0	1	2024-01-17 01:59:16
PCI	0	15	2024-01-17 01:59:19
PCIDE	0	1	2024-01-17 01:59:19
ROOT	0	14	2024-01-17 01:59:22
SCSI	0	2	2024-01-17 01:59:21
STORAGE	0	1	2024-01-17 01:59:21
SWD	0	5	2024-04-04 12:08:50
USB	9	9	2024-04-04 12:08:49
USBSTOR	0	1	2024-04-04 12:08:49
UsbVpn_GenericS...	0	1	2024-04-04 12:08:49
C:\Windows	12	2	2024-04-04 12:08:46
Hardware Profiles	0	2	2024-04-04 12:39:46
Palkee	0	8	2019-12-07 09:15:07
Services	0	71	2024-04-04 12:40:04
DriverDatabase	6	4	2024-04-04 12:38:50
HardwareConfig	2	1	2024-04-04 12:39:46
Input	0	2	2019-12-07 09:15:07
Keyboard Layout	0	2	2019-12-07 14:57:16
Mouse	0	1	2019-12-07 09:15:07
MountedDevices	5	0	2024-04-04 12:08:50
ResourceManager	0	1	2019-12-07 09:15:07
ResourcePartitions	0	2	2019-12-07 09:15:07

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Is Deleted	Data Record Realized
DeviceDesc	RegSz	0-disk.inf\usb_desc%\Disk drive	FF-FF-FF-FF	
Capabilties	RegDword	16		
Address	RegDword	0		
ContainerID	RegSz	{4f60445-d8c7-3f0b-bc7a-8a2d9d7a77a}	FF-FF-FF-FF-FF-FF	
HardwareID	RegMultiSz	USBSTOR\WdGeneric_Flash_Pak_..._6.07 USBSTOR\W...	FF-FF-FF-FF	
CompartID	RegMultiSz	USBSTOR\WdGeneric_Flash_Pak_...	FF-FF-FF-FF-FF-FF	
ClassID	RegSz	{435a9b7-v325-110a-b611-00002b310318}	FF-FF-FF-FF-FF-FF	
Service	RegSz	disk	A4-00	
Driver	RegSz	{435a9b7-v325-110a-b611-00002b310318}\Wd001	FF-FF-FF-FF	
Help	RegSz	0-disk.inf\Superman\Structure%\Standard disk drive	FF-FF-FF-FF-FF-FF	
FriendlyName	RegSz	Generic Flash Disk USB Device		
ConfigFlags	RegDword	0		

그리고, 추출한 하이브를 Register Explorer를 활용해,  
ControlSet001\Enum\USBSTOR 해당 경로를 들어가니, 2024-04 날짜로 기록된 USB 디바이스 기록 하나를 발견할 수 있었다.

Registry Explorer v2.1.0

File Tools Options Bookmarks (36/0) View Help

Registry hives (1) Available bookmarks (36/0)

Enter text to search...

Find

Key name	# values	# subkeys	Last write timestamp
C:\Users\W82104\Download...	0	17	2024-04-04 12:39:46
ROOT	0	1	2019-12-07 09:15:08
ActivationBroker	0	1	2019-12-07 09:15:08
ControlSet001	0	5	2019-12-07 09:15:07
Control	12	124	2024-04-04 12:40:01
Enum	21	15	2024-04-04 12:08:49
ACPI	0	15	2024-01-17 01:59:18
ACPI_HAL	0	1	2024-01-17 01:59:18
BTH	0	3	2024-01-17 01:59:23
DISPLAY	0	1	2024-01-17 01:59:23
HDAUDIO	0	1	2024-01-17 01:59:22
HID	0	2	2024-01-17 01:59:22
HTREE	0	1	2024-01-17 01:59:16
PCI	0	15	2024-01-17 01:59:19
PCIDE	0	1	2024-01-17 01:59:19
ROOT	0	14	2024-01-17 01:59:22
SCSI	0	2	2024-01-17 01:59:21
STORAGE	0	1	2024-01-17 01:59:21
SWD	0	5	2024-04-04 12:08:50
USB	9	9	2024-04-04 12:08:49
ROOT_HUB	0	1	2024-01-17 01:59:22
ROOT_HUB20	0	1	2024-01-17 01:59:21
ROOT_HUB30	0	1	2024-01-17 01:59:21
VID_058F&PID_6387	0	1	2024-04-04 12:08:49
VID_0E0F&PID_0002	0	3	2024-04-04 12:08:48
VID_0E0F&PID_0003	0	1	2024-01-17 01:59:22
6839d724fe&085	13	2	2024-04-04 12:39:55
VID_0E0F&PID_000...	0	1	2024-01-17 01:59:22
VID_0E0F&PID_000...	0	1	2024-01-17 01:59:22
VID_0E0F&PID_000...	0	1	2024-01-17 01:59:22
VID_0E0F&PID_0008	0	1	2024-01-17 01:59:22
USBSTOR	0	1	2024-04-04 12:08:49
Disk&Ven_GenericS...	0	1	2024-04-04 12:08:49
03A49E66	13	2	2024-04-04 12:08:49

Values

Drag a column header here to group by that column

Key Name	Serial Number	ParentId Prefix	Service	Device Desc	Friendly Nam
ROOT_HUB	58289196b8&0	6835d1f50b&0	usbhub	USB Root Hub	
ROOT_HUB20	5836a4b5d6&0		usbhub	USB Root Hub	
ROOT_HUB30	581110670508&0	6839d724fe&0	USBHUB3	USB Root Hub (USB 3.0)	
VID_058F&PID_6387	03A49E66		USBSTOR	USB Mass Storage Device	
VID_0E0F&PID_0002	6835d1f50b&082		usbhub	Generic USB Hub	
VID_0E0F&PID_0002	6839d724fe&087		USBHUB3	Generic USB Hub	
VID_0E0F&PID_0002	6839d724fe&088		USBHUB3	Generic USB Hub	
VID_0E0F&PID_0003	6839d724fe&085	78bcfcfc2&0	usbccpp	USB Composite Device	
VID_0E0F&PID_0003&MI_0	78bcfcfc2&080000	88217ccb29&0	Hidusb	USB Input Device	
VID_0E0F&PID_0003&MI_0	78bcfcfc2&080001	8834ace767&0	Hidusb	USB Input Device	
VID_0E0F&PID_0008	000650268328	7820f38eb4&0	BTHUSB	Generic Bluetooth Adapter	

이번에는 ControlSet001\Enum\USB 경로로 들어가, 해당 2024년 4월 4일에 연결 및 제거된 USB 장치를 찾았다. 그리고 이의 VID, PID, Device Serial Number를 알아내 플래그 값을 얻을 수 있었다.

DH{058F\_6387\_03A49E66}