Dreamhack-Find the USB(level1)

문제

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?

Info

- FLAG = `DH{VID_PID_DeviceSerialNumber}`
- 예를 들어 `VID` 가 `1111` , `PID` 가 `2222` , 그리고 `DeviceSerialNumber` 가 `AAAABBBB` 이면 플래그는 `DH{1111_2222_AAAABBBB}` 입니다.

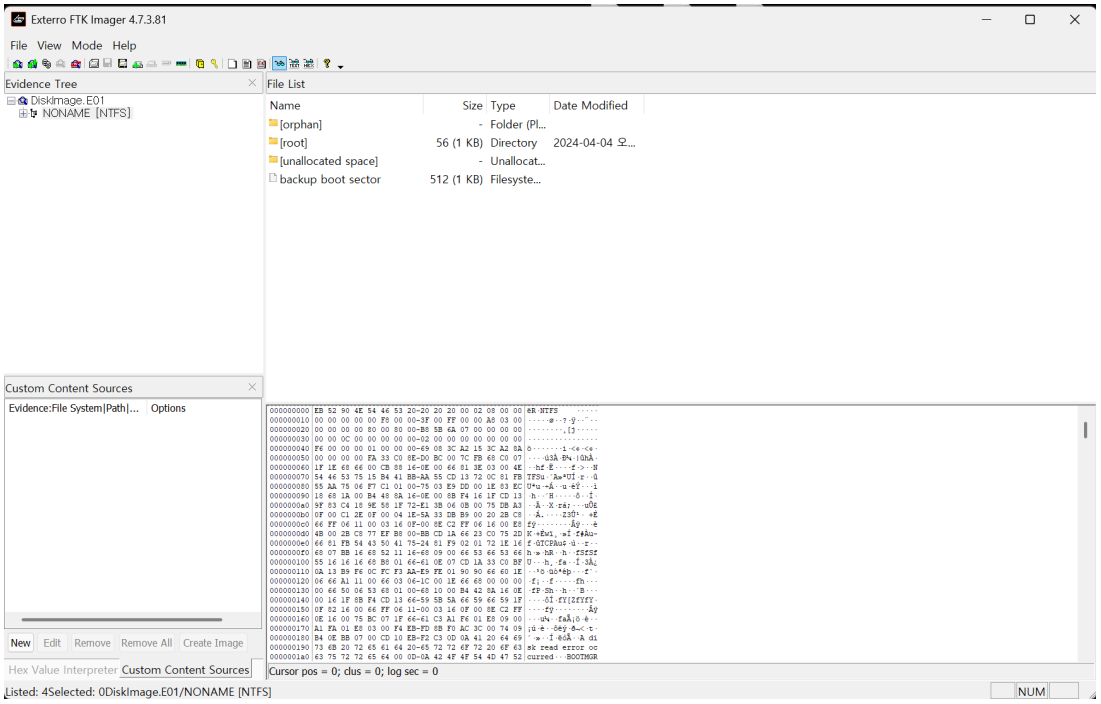
풀이

1. 문제 파악

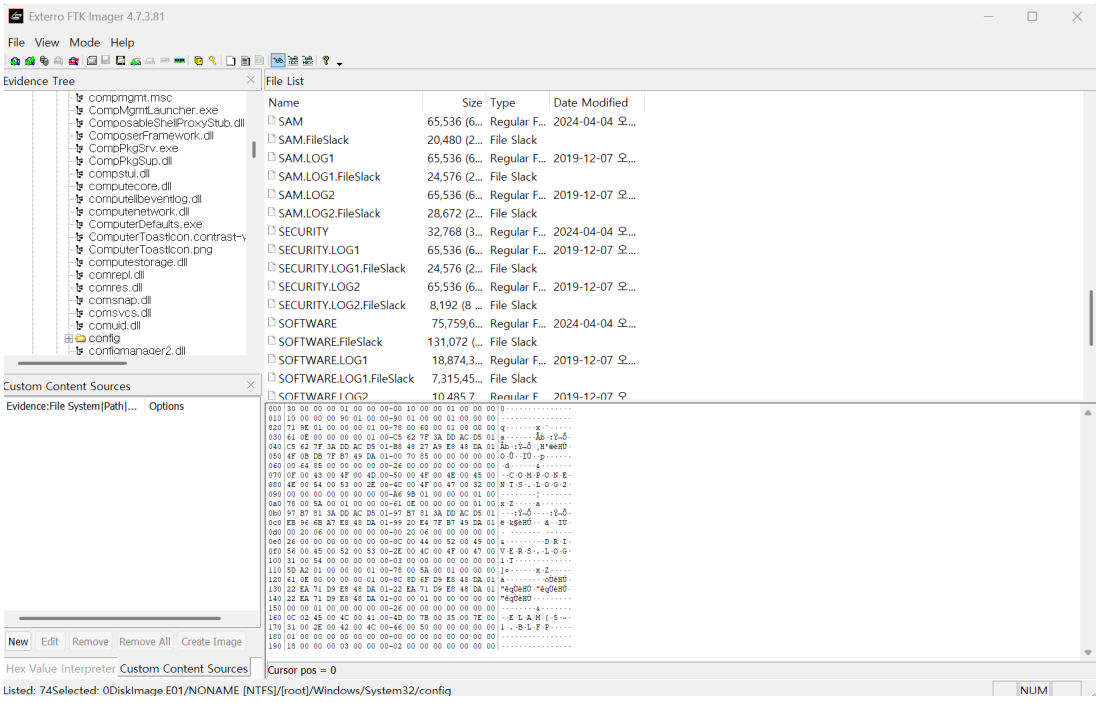
문제 설명을 보면 windows 레지스트리 분석으로 답을 찾아가는 것 같다

레지스트리 분석을 위해 문제 파일인 E01에서 필요한 파일을 추출해 준다.

2. 문제 풀이

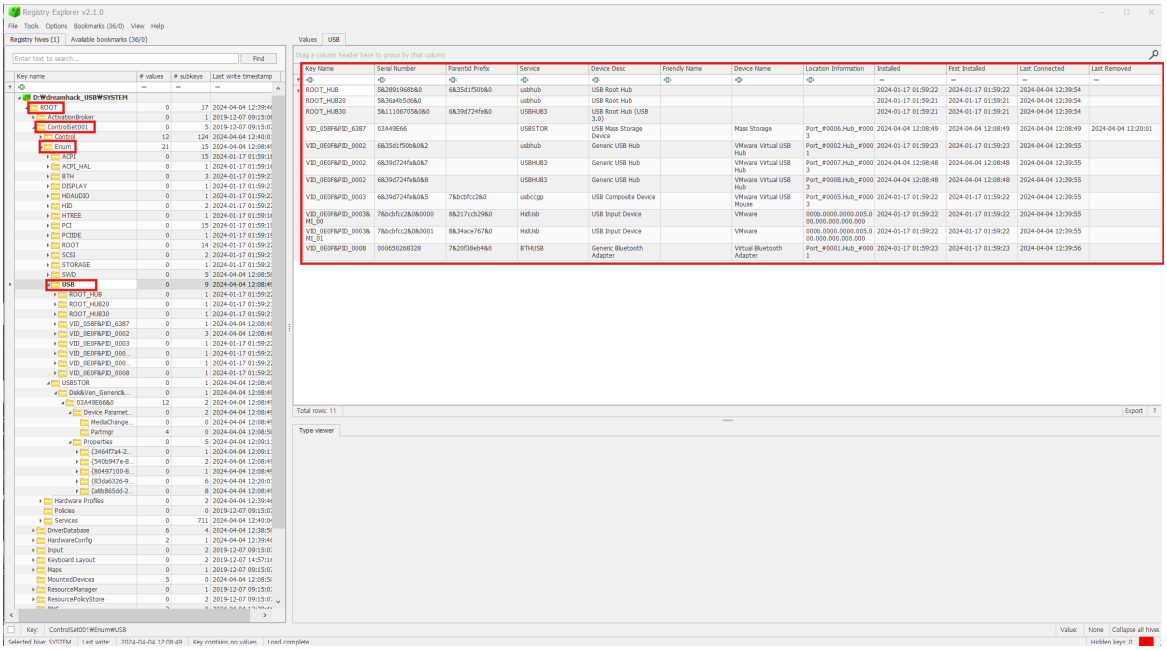


(1) FTK에서 오픈해준다



(2) 경로 : [root]/windows/System32/config

추출한 파일 : SYSTEM



Key Name	Serial Number	Parentid Prefix	Service	Device Desc	Friendly Name	Device Name	Location Information	Installed	First Installed	Last Connected	Last Removed
ROOT_HUB	5&2891968b&0	6&35d1f50b&0	usbhub	USB Root Hub				2024-01-17 01:59:22	2024-01-17 01:59:22	2024-04-04 12:39:54	
ROOT_HUB20	5&36a4b5d6&0		usbhub	USB Root Hub				2024-01-17 01:59:21	2024-01-17 01:59:21	2024-04-04 12:39:54	
ROOT_HUB30	5&11106705&0&0	6&39d724fe&0	USBHUB3	USB Root Hub (USB 3.0)				2024-01-17 01:59:21	2024-01-17 01:59:21	2024-04-04 12:39:54	
VID_058F&PID_6387	03A49E66		USBSTOR	USB Mass Storage Device		Mass Storage	Port_#0006.Hub_#0003	2024-04-04 12:08:49	2024-04-04 12:08:49	2024-04-04 12:08:49	2024-04-04 12:20:01
VID_0E0F&PID_0002	6&35d1f50b&0&2		usbhub	Generic USB Hub		VMware Virtual USB Hub	Port_#0002.Hub_#0001	2024-01-17 01:59:23	2024-01-17 01:59:23	2024-04-04 12:39:55	
VID_0E0F&PID_0002	6&39d724fe&0&7		USBHUB3	Generic USB Hub		VMware Virtual USB Hub	Port_#0007.Hub_#0003	2024-04-04 12:08:48	2024-04-04 12:08:48	2024-04-04 12:39:55	
VID_0E0F&PID_0002	6&39d724fe&0&8		USBHUB3	Generic USB Hub		VMware Virtual USB Hub	Port_#0008.Hub_#0003	2024-04-04 12:08:48	2024-04-04 12:08:48	2024-04-04 12:39:55	
VID_0E0F&PID_0003	6&39d724fe&0&5	7&bcbfcc2&0	usbccgp	USB Composite Device		VMware Virtual USB Mouse	Port_#0005.Hub_#0003	2024-01-17 01:59:22	2024-01-17 01:59:22	2024-04-04 12:39:55	
VID_0E0F&PID_0003&MI_00	7&bcbfcc2&0&0000	8&217ccb29&0	HidUsb	USB Input Device		VMware	000b.0000.0000.005.000.000.000.000	2024-01-17 01:59:22	2024-01-17 01:59:22	2024-04-04 12:39:55	
VID_0E0F&PID_0003&MI_01	7&bcbfcc2&0&0001	8&34ace767&0	HidUsb	USB Input Device		VMware	000b.0000.0000.005.000.000.000.000	2024-01-17 01:59:22	2024-01-17 01:59:22	2024-04-04 12:39:55	
VID_0E0F&PID_0008	000650268328	7&20f38eb4&0	BTHUSB	Generic Bluetooth Adapter		Virtual Bluetooth Adapter	Port_#0001.Hub_#0001	2024-01-17 01:59:23	2024-01-17 01:59:23	2024-04-04 12:39:56	

(3) 경로 : `ROOT/ControlSet001/Enum/USB` / `SYSTEM\ControlSet001\Enum\USBSTOR`

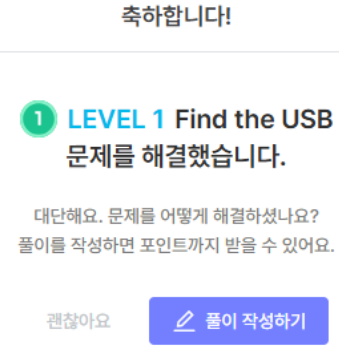
분석 내용 :

Windows 시스템에 연결된 USB 저장장치(USBSTOR) 관련 정보를 기록하는 영역으로, 아래와 같은 내용을 확인할 수 있었다.

[USB가 연결되었다가 연결이 끊어진 한개의 기록 확인]

VID : 058F / PID : 6387 / DeviceSerialNumber : 03A49E66

FLAG : 058F_6387_03A49E66



참고 자료

https://www.igloo.co.kr/security-information/%EC%9C%88%EB%8F%84%EC%9A%B0-%EB%A0%88%EC%A7%80%EC%8A%A4%ED%8A%B8%EB%A6%AC-%EB%B6%84%EC%84%9D%EC%9D%84-%EC%9D%B4%EC%9A%A9%ED%95%9C-%EC%B9%A8%ED%95%B4%EC%82%AC%EA%B3%A0-%EB%B6%84%EC%84%9D-%EA%B8%B0/