Find The USB

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?

Info
FLAG = DH{VID_PID_DeviceSerialNumber}
예를 들어 VID가 1111, PID가 2222, 그리고 DeviceSerialNumber가 AAAABBBB이면 플래그는 DH{1111_2222_AAAABBBB} 입니다.

사용한 도구

FTK Imager, Registry Explorer

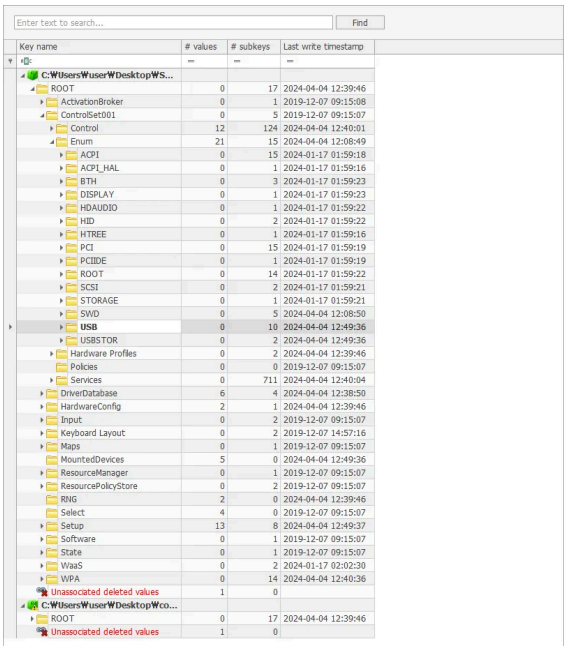
1. FTK Imager 에서 hive파일 정보 추출

   경로: C:Windows\System32\config

Name	Size	Type	Date Modified
SAM	65,536 (6...	Regular F...	2024-04-04 오...
SAM.FileSlack	20,480 (2...	File Slack	
SAM.LOG1	65,536 (6...	Regular F...	2019-12-07 오...
SAM.LOG1.FileSlack	24,576 (2...	File Slack	
SAM.LOG2	65,536 (6...	Regular F...	2019-12-07 오...
SAM.LOG2.FileSlack	28,672 (2...	File Slack	
SECURITY	32,768 (3...	Regular F...	2024-04-04 오...
SECURITY.LOG1	65,536 (6...	Regular F...	2019-12-07 오...
SECURITY.LOG1.FileSlack	24,576 (2...	File Slack	
SECURITY.LOG2	65,536 (6...	Regular F...	2019-12-07 오...
SECURITY.LOG2.FileSlack	8,192 (8 ...	File Slack	
SOFTWARE	75,759,6...	Regular F...	2024-04-04 오...
SOFTWARE.FileSlack	131,072 (...	File Slack	
SOFTWARE.LOG1	18,874,3...	Regular F...	2019-12-07 오...
SOFTWARE.LOG1.FileSlack	7,315,45...	File Slack	
SOFTWARE.LOG2	10,485,7...	Regular F...	2019-12-07 오...
SOFTWARE.LOG2.FileSlack	1,531,90...	File Slack	
SYSTEM	11,796,4...	Regular F...	2024-04-04 오...
SYSTEM.FileSlack	57,344 (5...	File Slack	
SYSTEM.LOG1	3,301,37...	Regular F...	2019-12-07 오...
SYSTEM.LOG1		$I30 IND...	
SYSTEM.LOG2	2,359,29...	Regular F...	2019-12-07 오...
SYSTEM.LOG2		$I30 IND...	
SYSTEM.LOG2.FileSlack	1,155,07...	File Slack	
systemprofile		$I30 IND...	

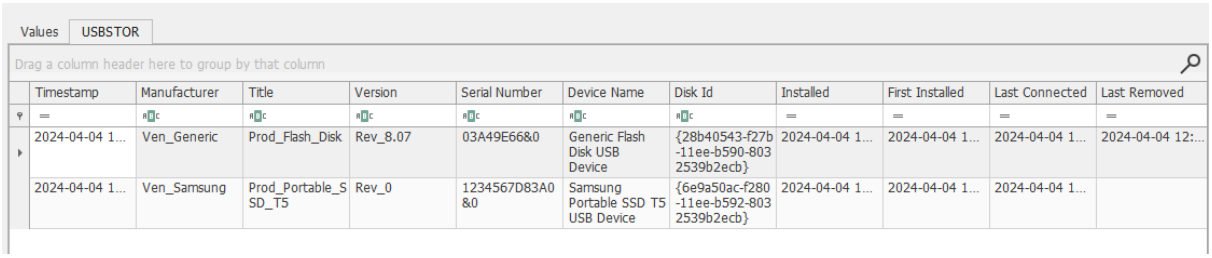
2. Registry Explorer 에서 레지스트리 로드

- 추출한 config 파일에서 SYSTEM 관련 파일 로드



USB 관련 정보 경로 : `ROOT\ControlSet001\Enum\USB` , `ROOT\ControlSet001\Enum\USBSTOR`

3. \USBSTOR에서 시리얼 넘버 확인 가능



Values | USBSTOR

Drag a column header here to group by that column

Timestamp	Manufacturer	Title	Version	Serial Number	Device Name	Disk Id	Installed	First Installed	Last Connected	Last Removed
2024-04-04 1...	Ven_Generic	Prod_Flash_Disk	Rev_8.07	03A49E66&0	Generic Flash Disk USB Device	{28b40543-f27b-11ee-b590-8032539b2ecb}	2024-04-04 1...	2024-04-04 1...	2024-04-04 1...	2024-04-04 12:...
2024-04-04 1...	Ven_Samsung	Prod_Portable_SSD_T5	Rev_0	1234567D83A0&0	Samsung Portable SSD T5 USB Device	{6e9a50ac-f280-11ee-b592-8032539b2ecb}	2024-04-04 1...	2024-04-04 1...	2024-04-04 1...	

Serial Number 확인 가능

두개의 USB중 삭제된 시간이 존재하는 USB가 하나인 걸로 봐서 저 USB가 문제에서 요구되는 USB임을 알 수 있다.

4. \USB에서 해당 시리얼 넘버를 가진 USB의 VID, PID 확인 가능

Drag a column header here to group by that column

Key Name	Serial Number	Parentid Prefix	Service	Device Desc	Friendly Name	Device Name	Location Info...	Installed	First Installed	Last Connect...	Last Removed
ROOT_HUB	5&2891968b&0	6&35d1f50b&0	usbhub	USB Root Hub				2024-01-17 ...	2024-01-17 ...	2024-04-04 ...	
ROOT_HUB20	5&36a4b5d6&0		usbhub	USB Root Hub				2024-01-17 ...	2024-01-17 ...	2024-04-04 ...	
ROOT_HUB30	5&11106705&0&0	6&39d724fe&0	USBHUB3	USB Root Hub (USB 3.0)				2024-01-17 ...	2024-01-17 ...	2024-04-04 ...	
VID_04E8&PID_61F5	1234567D83A0		USBSTOR	USB Mass Storage Device		Portable SSD T5	Port_#0006.Hub_#0003	2024-04-04 ...	2024-04-04 ...	2024-04-04 ...	
VID_058F&PID_6387	03A49E66		USBSTOR	USB Mass Storage Device		Mass Storage	Port_#0006.Hub_#0003	2024-04-04 ...	2024-04-04 ...	2024-04-04 ...	2024-04-04 1...
VID_0E0F&PID_0002	6&35d1f50b&0&2		usbhub	Generic USB Hub		VMware Virtual USB Hub	Port_#0002.Hub_#0001	2024-01-17 ...	2024-01-17 ...	2024-04-04 ...	
VID_0E0F&PID_0002	6&39d724fe&0&7		USBHUB3	Generic USB Hub		VMware Virtual USB Hub	Port_#0007.Hub_#0003	2024-04-04 ...	2024-04-04 ...	2024-04-04 ...	
VID_0E0F&PID_0002	6&39d724fe&0&8		USBHUB3	Generic USB Hub		VMware Virtual USB Hub	Port_#0008.Hub_#0003	2024-04-04 ...	2024-04-04 ...	2024-04-04 ...	
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 ...	2024-01-17 ...	2024-04-04 ...	
VID_0E0F&PID_0003&MI_00	7&bcbfcc2&0&0000	8&217ccb29&0	HidUsb	USB Input Device		VMware	000b.0000.0000.005.000.000.000.000.000	2024-01-17 ...	2024-01-17 ...	2024-04-04 ...	
VID_0E0F&PID_0003&MI_01	7&bcbfcc2&0&0001	8&34ace767&0	HidUsb	USB Input Device		VMware	000b.0000.0000.005.000.000.000.000.000	2024-01-17 ...	2024-01-17 ...	2024-04-04 ...	
VID_0E0F&PID_0008	000650268328	7&20f38eb4&0	BTHUSB	Generic Bluetooth Adapter		Virtual Bluetooth Adapter	Port_#0001.Hub_#0001	2024-01-17 ...	2024-01-17 ...	2024-04-04 ...	