

문제 10.

10. 2022.11.11. 14:40:41(UTC+9)에 운영체제에 연결됐던 USB Thumb Drive의

① 제조사명 ② 정확한 모델명 ③ Serial Number를 기술하시오.

SYSTEM		0	2022-11-11 14:40:41 KST	SanDisk Corp.	Ultra Flair	04014073e0ba58b4972c65850add184c5bf8090880...	파티션2개복
SYSTEM		0	2022-11-11 14:25:42 KST	VMware, Inc.	Virtual Mouse	6&38eee119&0&5	파티션2개복
SYSTEM		0	2022-11-11 14:25:42 KST	VMware, Inc.	Virtual Mouse	7&2da3d997&0&0000	파티션2개복
SYSTEM		0	2022-11-11 14:25:42 KST	VMware, Inc.	Virtual Mouse	7&2da3d997&0&0001	파티션2개복
SYSTEM		0	2022-11-11 14:25:42 KST	VMware, Inc.	Virtual USB Hub	6&38eee119&0&7	파티션2개복
SYSTEM		0	2022-11-11 14:25:43 KST	VMware, Inc.	Virtual USB Hub	6&38eee119&0&8	파티션2개복

Hex	Text	Application	Source File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Result: 4 of 10 Result USB Device Attached									
Type	Value								Source(s)
Date/Time	2022-11-11 14:40:41 KST								Recent Activity
Device Make	SanDisk Corp.								Recent Activity
Device Model	Ultra Flair								Recent Activity
Device ID	04014073e0ba58b4972c65850add184c5bf8090880ae975a8f6bc1ba03964d220c1a0000000000000000d0bcaaff1c0f1891558107c2a71619								Recent Activity
Source File Path	/img_파티션2개복구_Reimaging_Scenario3.001/vol_vol2/Windows/System32/config/SYSTEM								
Artifact ID	-9223372036854775768								

- Autopsy를 통해 2022.11.11. 14:40:41(UTC+9(KST))에 운영체제에 연결됐던 USB Thumb Drive의 Data Artifacts를 다음과 같이 조회한 결과

Device ID :

'04014073e0ba58b4972c65850add184c5bf8090880ae975a8f6bc1ba03964d220c1a00000000000000000000d0bcaaff1c0f1891558107c2a71619'

로 확인됨.

- 이에 따라 아래와 같이 REGA를 이용하여 다음 항목 확인.

'HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Ultra_USB_3.0&Rev_1.00\04014073e0ba58b4972c65850add184c5bf8090880ae975a8f6bc1ba03964d2'

키 속성

일반	2022-11-11 14:40:41 Fri
최종기록시각 (UTC+09:00)	
속성	
하위키 개수	2
값 개수	12

키 탐색 | 타임라인 아이템

값 이름	값 종류	값 데이터
DeviceDesc	REG_SZ	@disk.inf,%disk_devdesc%;Disk drive
Capabilities	REG_DWORD	00000010
Address	REG_DWORD	00000001
ContainerID	REG_SZ	{3371b070-9941-5dd0-8037-49803e03ff41}
HardwareID	REG_MULTI_SZ	USBSTOR\WDiskSanDisk_Ultra_USB_3.0__1.00 USBSTO...
CompatibleIDs	REG_MULTI_SZ	USBSTOR\WDiskSanDisk_Ultra_USB_3.0__1.00 USBSTO...
ClassGUID	REG_SZ	{4d36e967-e325-11ce-bf1c-08002be10318}
Service	REG_SZ	disk
Driver	REG_SZ	{4d36e967-e325-11ce-bf1c-08002be10318}\W0001
FriendlyName	REG_SZ	@disk.inf,%genmanufacturer%;(Standard disk drives)
ConfigFlags	REG_DWORD	00000000

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Enum\USBSTOR\Disk&Ven_SanDisk&Prod_Ultra_USB_3.0&Rev_1.00\04014073e0ba58b4972c65850add184c5bf8090880ae975a

제조사명	SanDisk Corp.
정확한 모델명	Ultra Flair
Serial Number	04014073e0ba58b4972c65850add184c5bf8090880ae975a8f6b c1ba03964d220c1a000000000000000000000d0bcaaaff1c0f189 1558107c2a71619