Dreamhack-Find the USB(level1)

[forensics]

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? (2024.10.02)

Info

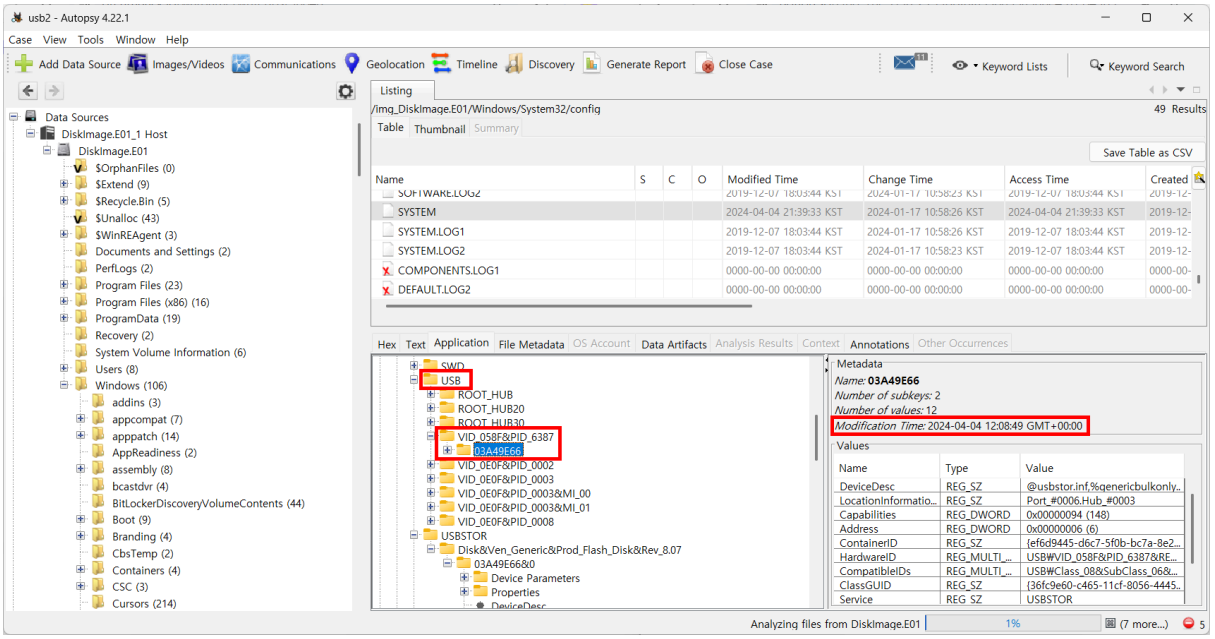
FLAG = `DH{VID_PID_DeviceSerialNumber}` 예를 들어 `VID`가 `1111`, `PID`가 `2222`, 그리고 `DeviceSerialNumber`가 `AAAABBBB`이면 플래그는 `DH{1111_2222_AAAABBBB}` 입니다.

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

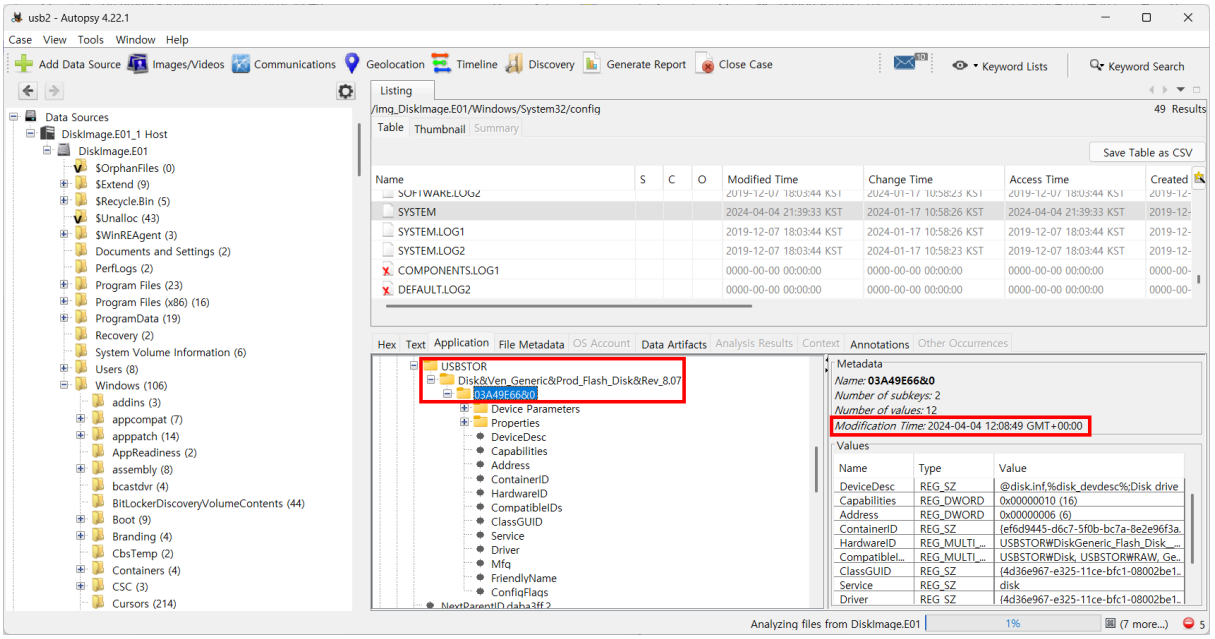
Write up

- 사용 도구: Autopsy
- `DiskImage.E01` 삽입한 뒤, 분석 시작
- 폴더 하위에 있는 각각의 장치별 **수정 시간(Modification Time)을 비교**해서 시간이 일치하는 폴더를 매칭하여 해당 장치의 VID, PID, Serial Number를 확인함

- 상세 경로: `Windows/System32/config/SYSTEM/ControlSet001/Enum/USB`
  - 2024-04-04 12:08:49 UTC



- 상세 경로: `Windows/System32/config/SYSTEM/ControlSet001/Enum/USBSTOR`
  - 2024-04-04 12:08:49 UTC



- **2024-04-04 12:08:49**로 동일한 폴더 확인
- **VID = 058F**
- **PID = 6387**

- **DeviceSerialNumber = 03A49E66**
- FLAG 형식으로는, DH{058F_6387_03A49E66}

FLAG

DH{058F_6387_03A49E66}