

Dreamhack-Track the file(level1)

[forensics]

Description

드림이는 컴퓨터를 살펴보다가 수상한 점을 발견했습니다. 바로 `malware.exe` 라는 프로그램이 컴퓨터에 생성되어 있다는 것이었어요. 드림이는 누군가가 USB를 연결해 파일을 복사해온 것으로 추측하고 있습니다.

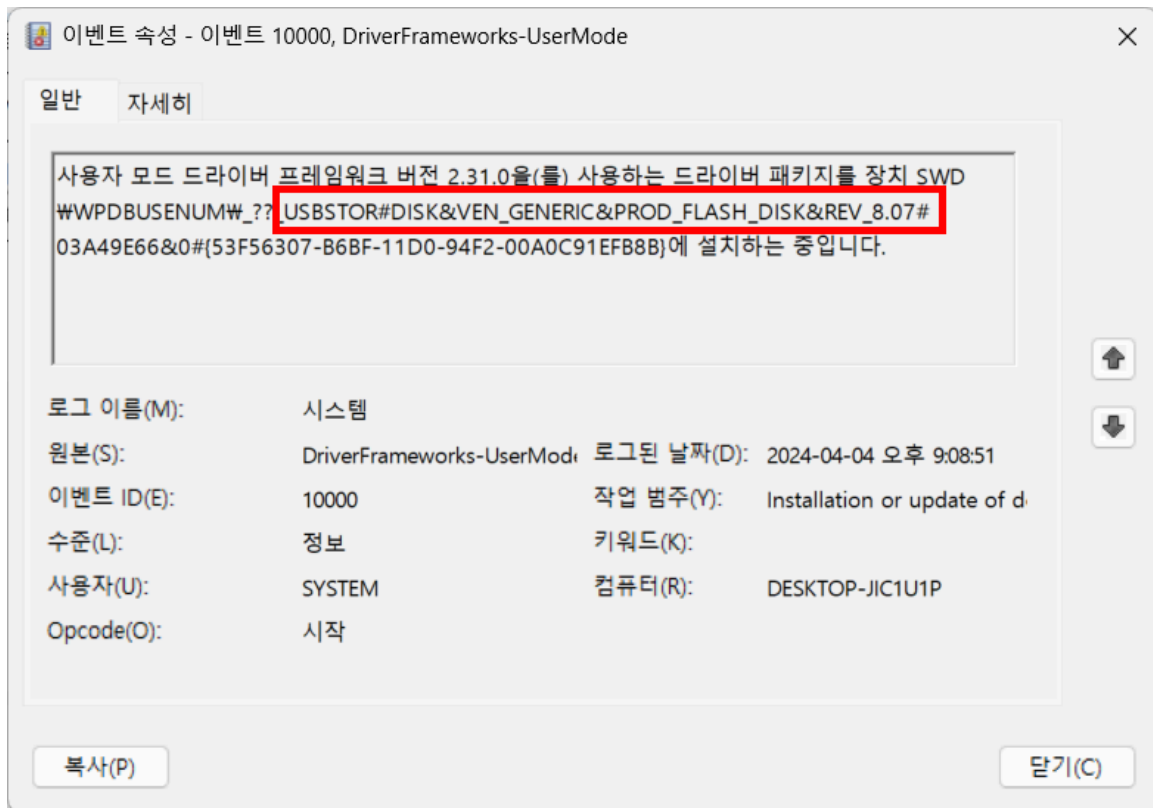
시스템 로그를 분석해 `malware.exe` 파일이 시스템에 복사된 시간을 찾아보세요!
(2024.10.02)

Info

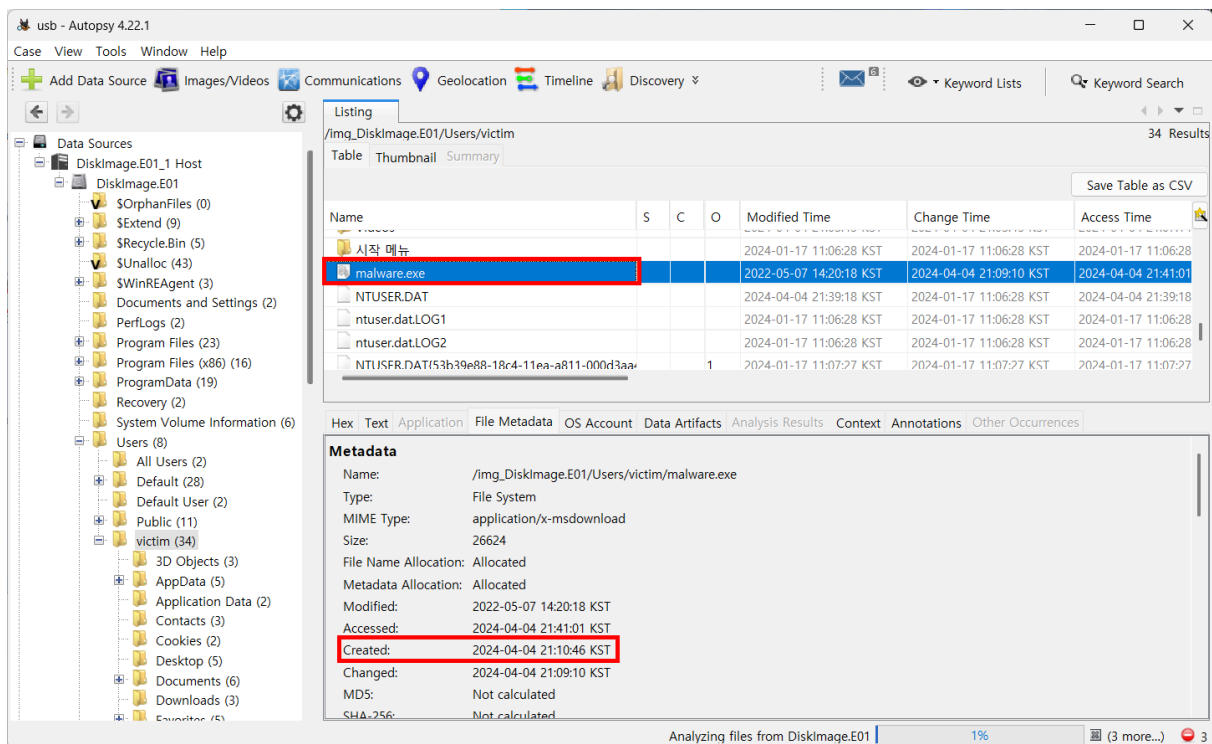
- FLAG = `DH{yyyy_MM_dd_hh_mm_ss}`
- `yy`, `MM`, `dd`, `hh`, `mm`, `ss` 는 시간을 표현하는 방식으로 각각 연, 월, 일, 시, 분, 초를 나타냅니다. 예를 들어 시간이 `2024-01-02 03:04:05` 라면, FLAG 는 `DH{2024_01_02_03_04_05}` 입니다.
- 시간은 UTC+9를 기준으로 합니다.

Write up

- 사용 도구: FTK Imager, 이벤트 뷰어, Autopsy, NTFS Log tracker
- 이벤트 뷰어를 통해 System.evtx 내부의 이벤트 10000, USB 연결 시점 확인 ⇒ 2024-04-04 21:08:51



- Autopsy를 통해 **malware.exe**의 생성 시간 확인 ⇒ **2024-04-04 21:10:46**



- NTFS Log Tracker를 통해 \$LogFile, \$MFT 내부 확인 ⇒ malware.exe 관련 로그 존재
X
 - \$LogFile → 어떤 데이터를 언제, 어디에 쓰는지 기록
- NTFS Log Tracker를 통해 \$UsnJrnl, \$MFT 내부 확인 ⇒ malware.exe 관련 로그 존재
O
 - \$UsnJrnl → 파일이나 디렉터리에 변경 사항이 생길 때 기록
- malware.exe 키워드 검색을 통해 최초 타임스탬프 확인 ⇒ **2024-04-04 21:10:46**
 - malware.exe의 생성 시간과 일치함!

Filter :

\$LogFile \$UsnJrnl:\$J \$LogFile(Search Result) \$UsnJrnl:\$J(Search Result)

< > Page : (1 / 1) Peroid : 2024-04-04 21:10:46 ~ 2024-04-04 21:41:04

TimeStamp	USN	FileName	Full Path(from \$MFT)
2024-04-04 21:10:46	250000240	malware.exe	\\Users\\victim\\malware.exe
2024-04-04 21:10:46	250000328	malware.exe	\\Users\\victim\\malware.exe
2024-04-04 21:10:46	250000416	malware.exe	\\Users\\victim\\malware.exe
2024-04-04 21:10:46	250000504	malware.exe	\\Users\\victim\\malware.exe
2024-04-04 21:10:46	250000592	malware.exe	\\Users\\victim\\malware.exe
2024-04-04 21:36:12	258917752	MALWARE.EXE-F029871F.pf	\\Windows\\Prefetch\\MALWARE.EXE-F029871F.pf
2024-04-04 21:36:12	258917864	MALWARE.EXE-F029871F.pf	\\Windows\\Prefetch\\MALWARE.EXE-F029871F.pf
2024-04-04 21:36:12	258917976	MALWARE.EXE-F029871F.pf	\\Windows\\Prefetch\\MALWARE.EXE-F029871F.pf
2024-04-04 21:40:07	259961776	MALWARE.EXE-F029871F.pf	\\Windows\\Prefetch\\MALWARE.EXE-F029871F.pf
2024-04-04 21:40:07	259961888	MALWARE.EXE-F029871F.pf	\\Windows\\Prefetch\\MALWARE.EXE-F029871F.pf
2024-04-04 21:41:04	260078360	MALWARE.EXE-F029871F.pf	\\Windows\\Prefetch\\MALWARE.EXE-F029871F.pf
2024-04-04 21:41:04	260078472	MALWARE.EXE-F029871F.pf	\\Windows\\Prefetch\\MALWARE.EXE-F029871F.pf

- 즉, malware.exe 파일이 시스템에 복사된 시간은 **2024-04-04 21:10:46**
- FLAG 형식으로는, DH{2024_04_04_21_10_46}

FLAG

DH{2024_04_04_21_10_46}