

Write-up: Track_the_file (level1)

<https://dreamhack.io/wargame/challenges/1325>

[1. Challenge Info](#)

[2. Problem Description](#)

[3. Provided Files](#)

[4. Tools Used](#)

[5. Analysis Steps](#)

[5.1 디스크 이미지 마운트](#)

[5.2 파일이 시스템에 복사된 시간 확인](#)

[5.3 최종 정보 정리](#)

[6. Flag](#)

1. Challenge Info

- **Challenge Name:** Track_the_file
- **Category:** Forensics
- **Difficulty Level:** Level 1
- **Platform:** DreamHack Wargame
- **Objective:**

드림이의 컴퓨터에 누군가 USB를 연결해 malware.exe 파일을 시스템에 복사한 시간을 찾아 플래그를 완성하라.

플래그 형식: **DH{yyyy_MM_dd_hh_mm_ss}**

- yy, MM, dd, hh, mm, ss는 시간을 표현하는 방식으로 각각 연, 월, 일, 시, 분, 초를 나타냄
- 시간은 UTC+9를 기준

2. Problem 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!”

- 제공된 디스크 이미지: `DiskImage.E01`
- 이 파일은 `Find the USB`, `Autoruns` 문제와 동일

3. Provided Files

- `DiskImage.E01` (Windows 시스템의 디스크 이미지 파일, E01 포맷)

4. Tools Used

| Tool | Version |
|------------------|-----------|
| FTK Imager | v4.7.8.31 |
| NTFS Log Tracker | v1.8 |

5. Analysis Steps

5.1 디스크 이미지 마운트

- 도구: FTK Imager
- 제공된 **DiskImage.E01** 파일을 FTK Imager로 열기
- **\$LogFile** , **\$MFT** 추출
 - 경로: **C:**

[root]

\$BadClus

\$Bitmap

\$Extend

\$Recycle.Bin

\$Secure

\$UpCase

\$WinREAgent

Documents and Settings

PerfLogs

Program Files

Program Files (x86)

ProgramData

Recovery

System Volume Information

Users

All Users

Default

Default User

Public

victim

Windows

[unallocated space]

Program Files (x86)

ProgramData

Recovery

System Volume Information

Users

Windows

\$AttrDef

\$BadClus

\$Bitmap

\$Boot

\$I30

\$LogFile

\$MFT

\$MFTMirr

\$Secure

\$TXF_DATA

\$UpCase

\$Volume

DumpStack.log.tmp

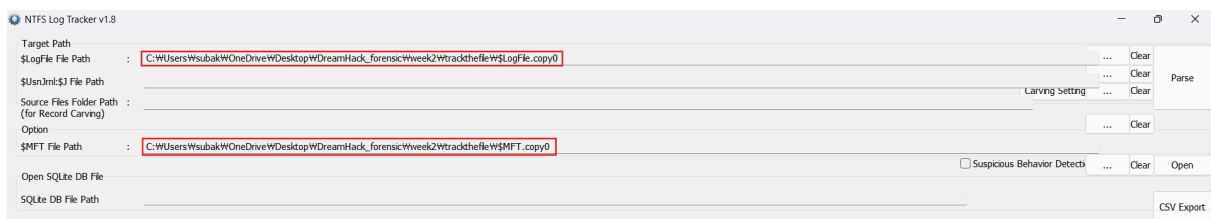
pagefile.sys

swapfile.sys

| | | |
|-----------------|---------------|---------------------|
| 56 (1 KB) | Directory | 2023-12-04 오전 2:... |
| 56 (1 KB) | Directory | 2024-04-04 오후 1:... |
| 48 (1 KB) | Directory | 2024-01-17 오전 2:... |
| 56 (1 KB) | Directory | 2024-01-17 오전 2:... |
| 56 (1 KB) | Directory | 2024-01-17 오전 2:... |
| 424 (1 KB) | Directory | 2024-04-04 오후 1:... |
| 2,560 (3 KB) | Regular File | 2024-01-17 오전 1:... |
| - | Regular File | 2024-01-17 오전 1:... |
| 1,943,920 (...) | Regular File | 2024-01-17 오전 1:... |
| 8,192 (8 KB) | Regular File | 2024-01-17 오전 1:... |
| 4,096 (4 KB) | NTFS Index... | 2024-04-04 오후 1:... |
| 67,108,864 ... | Regular File | 2024-01-17 오전 1:... |
| 291,766,272... | Regular File | 2024-01-17 오전 1:... |
| 4,096 (4 KB) | Regular File | 2024-01-17 오전 1:... |
| 56 (1 KB) | Regular File | 2024-01-17 오전 1:... |
| 56 (1 KB) | NTFS Logg... | 2024-04-04 오후 1:... |
| 131,072 (12... | Regular File | 2024-01-17 오전 1:... |
| 0 (0 KB) | Regular File | 2024-01-17 오전 1:... |
| 8,192 (8 KB) | Regular File | 2024-04-04 오후 1:... |
| 738,197,504... | Regular File | 2024-04-04 오후 1:... |
| 16,777,216 ... | Regular File | 2024-04-04 오후 1:... |

5.2 파일이 시스템에 복사된 시간 확인

- 도구: NTFS Log Tracker
- 추출한 **\$LogFile** , **\$MFT** 파일을 NTFS Log Tracker로 열기



- malware.exe 찾아서 Create Time 확인
 - 파일이 시스템에 복사된 시간: 2024-04-04 21:10:46

| \$LogFile \$UsnJrnl\$ \$LogFile(Search Result) \$UsnJrnl\$(Search Result) Suspicious Behavior Detection | | | | | | | | | | | |
|---|---|---|---------------------------|---|---------------------|---------------------|---------------------|---------------------|-----------------------|-------------|---------------|
| Page : (1 / 1) | | | | | | | | | | | |
| LSN | E | E | File/Directory Name | Full Path(from \$MFT) | Create Time | Modified Time | MFT_Modified T... | Access Time | Redo | Target V... | Cluster In... |
| 1275774049 | | | aero_unavail.cur | \\Windows\\Cursors\\aero_unavail.cur | 2019-12-07 18:09:07 | 2019-12-07 18:09:07 | 2024-01-17 10:00:00 | 2024-04-04 21:00:00 | Update Resident Value | 0x2E45 | 2 |
| 1275774083 | | | aero_up.cur | \\Windows\\Cursors\\aero_up.cur | 2019-12-07 18:09:07 | 2019-12-07 18:09:07 | 2024-01-17 10:00:00 | 2024-04-04 21:00:00 | Update Resident Value | 0x2E46 | 0 |
| 1275774117 | | | icudtl.dat | \\Windows\\Globalization\\WICU\\Wicudtl.dat | 2019-12-07 18:08:33 | 2019-12-07 18:08:33 | 2024-01-17 10:00:00 | 2024-04-04 21:00:00 | Update Resident Value | 0x2E6D | 4 |
| 1275774185 | | | malware.exe | \\Users\\Victim\\malware.exe | 2024-04-04 21:10:46 | 2022-05-07 14:00:00 | 2024-04-04 21:00:00 | 2024-04-04 21:00:00 | Update Resident Value | 0x2E7F | 4 |
| 1275774219 | | | ccba5a5986c77e43.autom... | \\Users\\Victim\\AppData\\Roaming\\WM... | 2024-04-04 21:10:55 | 2024-04-04 21:00:00 | 2024-04-04 21:00:00 | 2024-04-04 21:00:00 | Update Resident Value | 0x2E80 | 4 |
| 1275774253 | | | 280815 | \\Users\\Victim\\AppData\\Local\\Wfacka... | 2024-04-04 21:23:46 | 2024-04-04 21:00:00 | 2024-04-04 21:00:00 | 2024-04-04 21:00:00 | Update Resident Value | 0x2E9D | 2 |

5.3 최종 정보 정리

- 파일이 시스템에 복사된 시간: 2024-04-04 21:10:46

6. Flag

DH{2024_04_04_21_10_46}

축하합니다!

1 LEVEL 1 Track_the_file
문제를 해결했습니다.

대단해요. 문제를 어떻게 해결하셨나요?
풀이를 작성하면 포인트까지 받을 수 있어요.

괜찮아요

풀이 작성하기