Write-up: Track_the_file (level1)

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

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

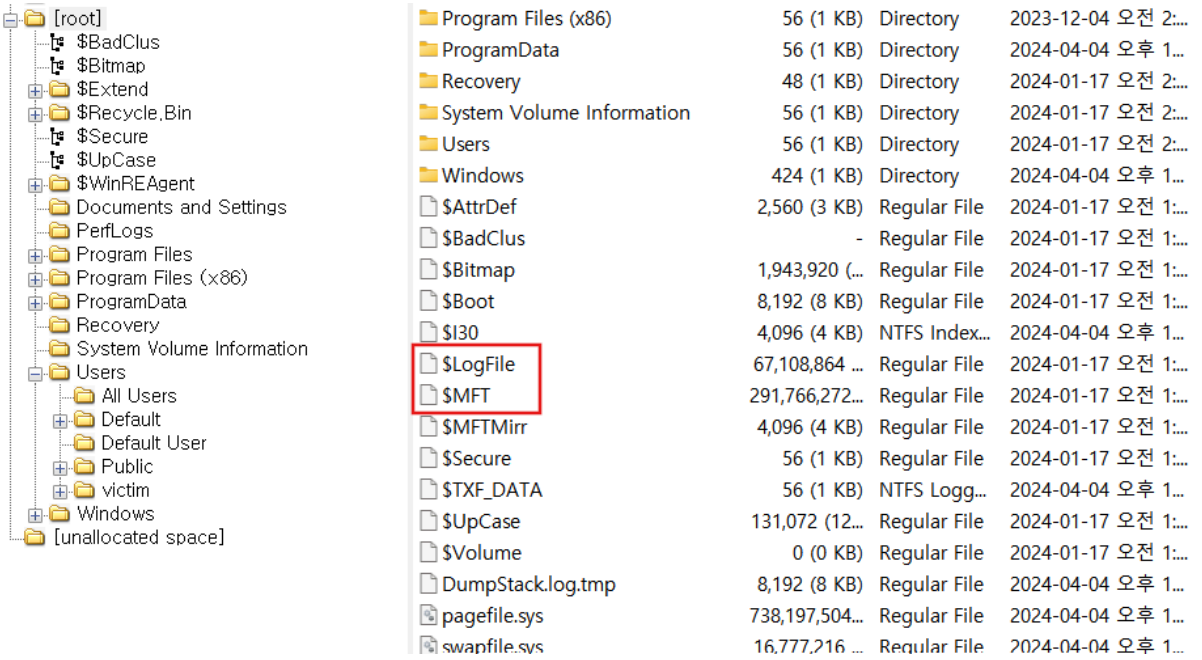
Tool	Version
FTK Imager	v4.7.8.31
NTFS Log Tracker	v1.8

---

5. Analysis Steps

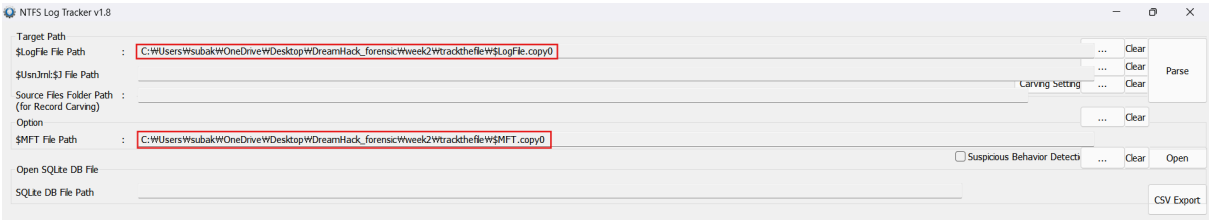
5.1 디스크 이미지 마운트

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

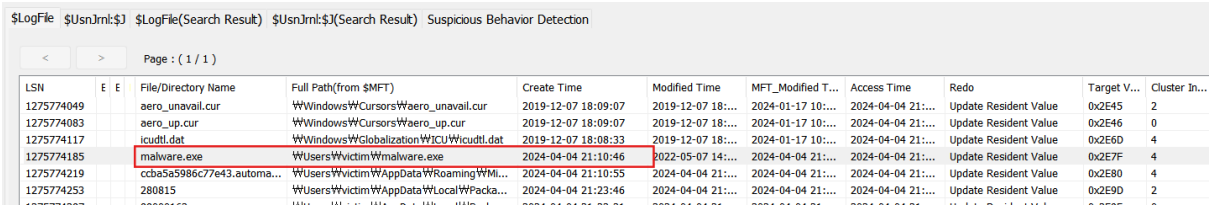


5.2 파일이 시스템에 복사된 시간 확인

- **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 $UsnJrnl:$J $LogFile(Search Result) $UsnJrnl:$J(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:...	2024-01-17 10:...	2024-04-04 21:...	Update Resident Value	0x2E45	2
1275774083			aero_up.cur	₩Windows₩Cursors₩aero_up.cur	2019-12-07 18:09:07	2019-12-07 18:...	2024-01-17 10:...	2024-04-04 21:...	Update Resident Value	0x2E46	0
1275774117			icudtl.dat	₩Windows₩Globalization₩ICU₩icudtl.dat	2019-12-07 18:08:33	2019-12-07 18:...	2024-01-17 10:...	2024-04-04 21:...	Update Resident Value	0x2E6D	4
1275774185			malware.exe	₩Users₩victim₩malware.exe	2024-04-04 21:10:46	2022-05-07 14:...	2024-04-04 21:...	2024-04-04 21:...	Update Resident Value	0x2E7F	4
1275774219			ccba5a5986c77e43.automa...	₩Users₩victim₩AppData₩Roaming₩Mi...	2024-04-04 21:10:55	2024-04-04 21:...	2024-04-04 21:...	2024-04-04 21:...	Update Resident Value	0x2E80	4
1275774253			280815	₩Users₩victim₩AppData₩Local₩Packa...	2024-04-04 21:23:46	2024-04-04 21:...	2024-04-04 21:...	2024-04-04 21:...	Update Resident Value	0x2E9D	2

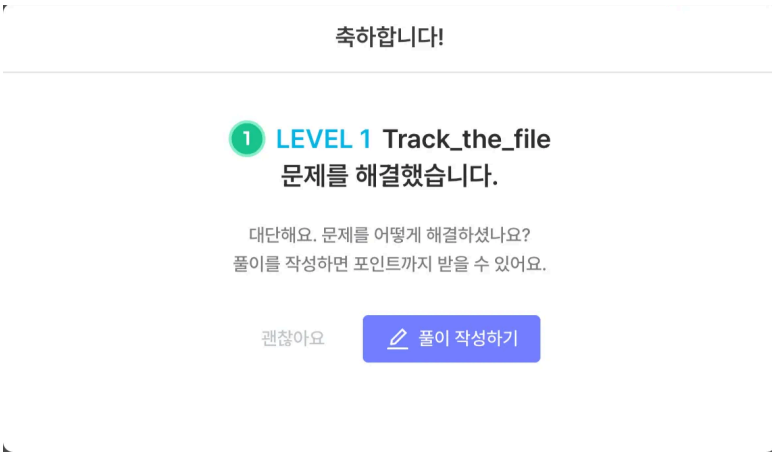
5.3 최종 정보 정리

- **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
