Track_the_file

Description

[함께실습] Track_the_file에서 실습하는 문제입니다.

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

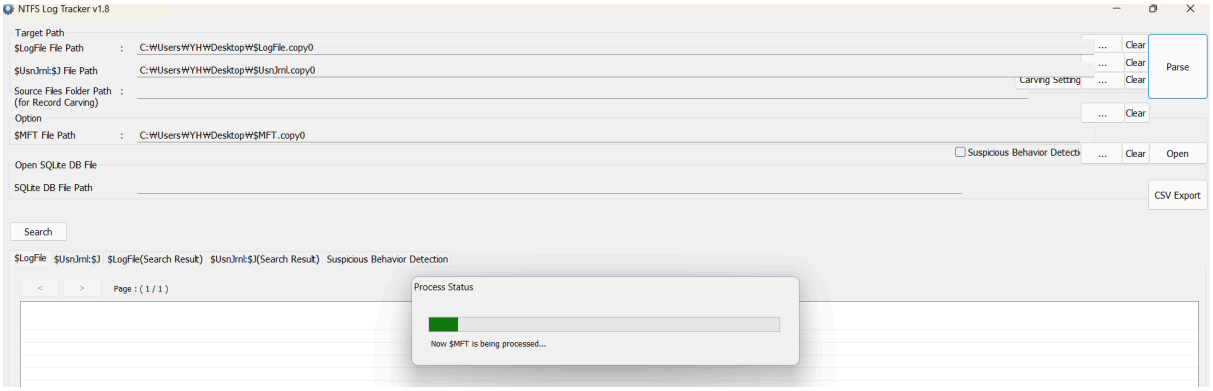
시스템 로그를 분석해 `malware.exe` 파일이 시스템에 복사된 시간을 찾아보세요!

Info

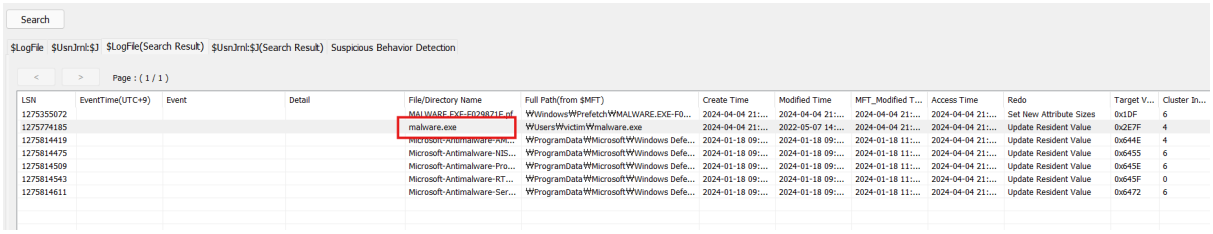
FLAG = `DH{yyyy_MM_dd_hh_mm_ss}yy` , `MM` , `dd` , `hh` , `mm` , `ss` 는 시간을 표현하는 방식으로 각각 연, 월, 일, 시, 분, 초를 나타냅니다. 예를 들어 시간이 `2024-01-02 03:04:05` 라면, FLAG는 `DH{2024_01_02_03_04_05}` 입니다.시간은 UTC+9를 기준으로 합니다.

- 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, FLAG는 `DH{2024_01_02_03_04_05}` 입니다.
- 시간은 UTC+9를 기준으로 합니다.

1. FTK Imager에서 NTFS Log Tracker에 들어갈 내용을 모두 내보내기 한 뒤에 NTFS Log Tracker에서 Parse



2. logfile에서 malware.exe 발견



3. malware가 실행된 시간