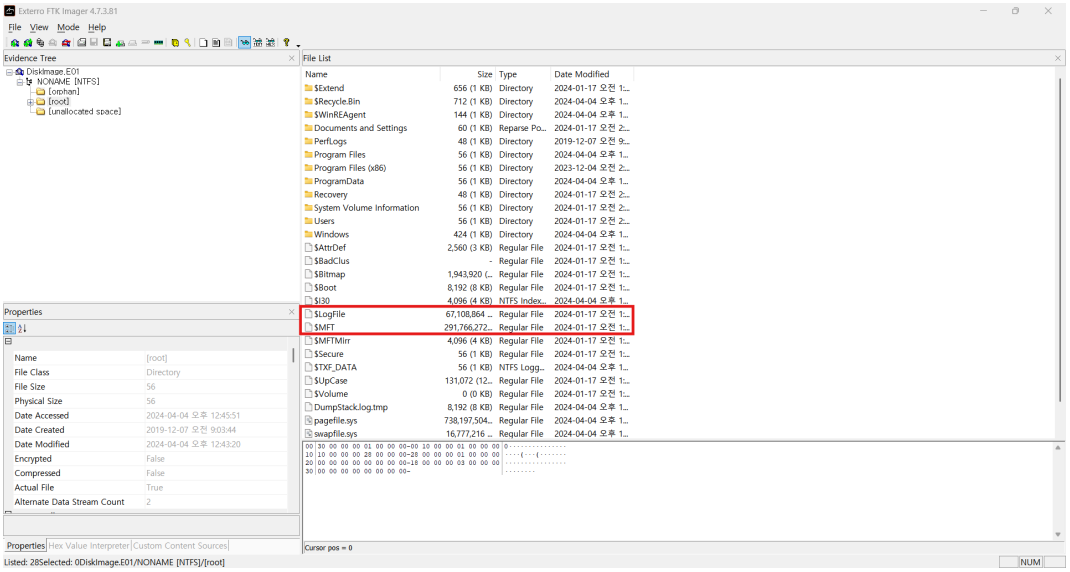
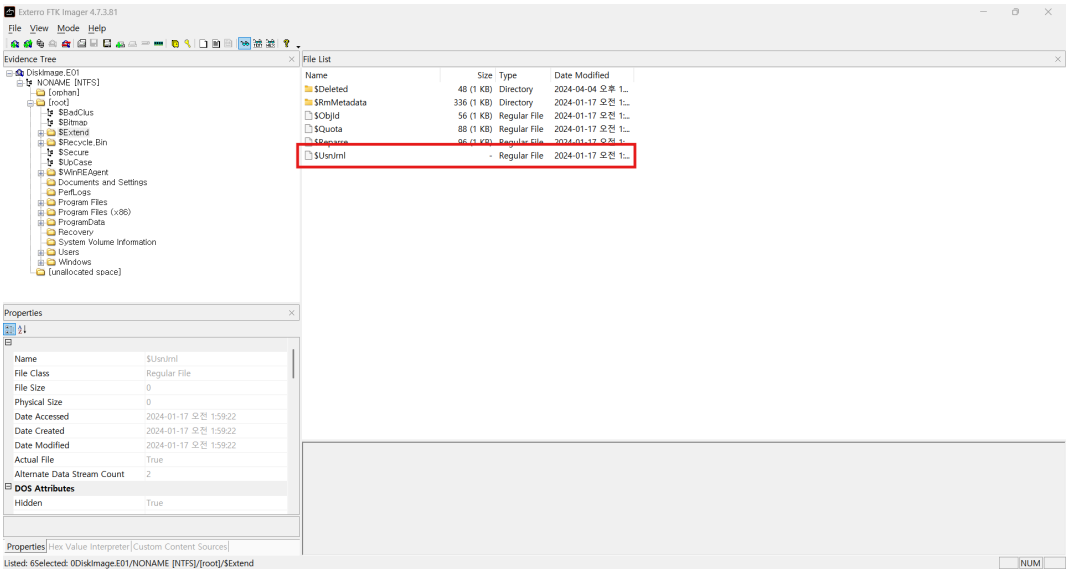
Dreamhack-Track_the_file (level1)

> 👉 **[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!**

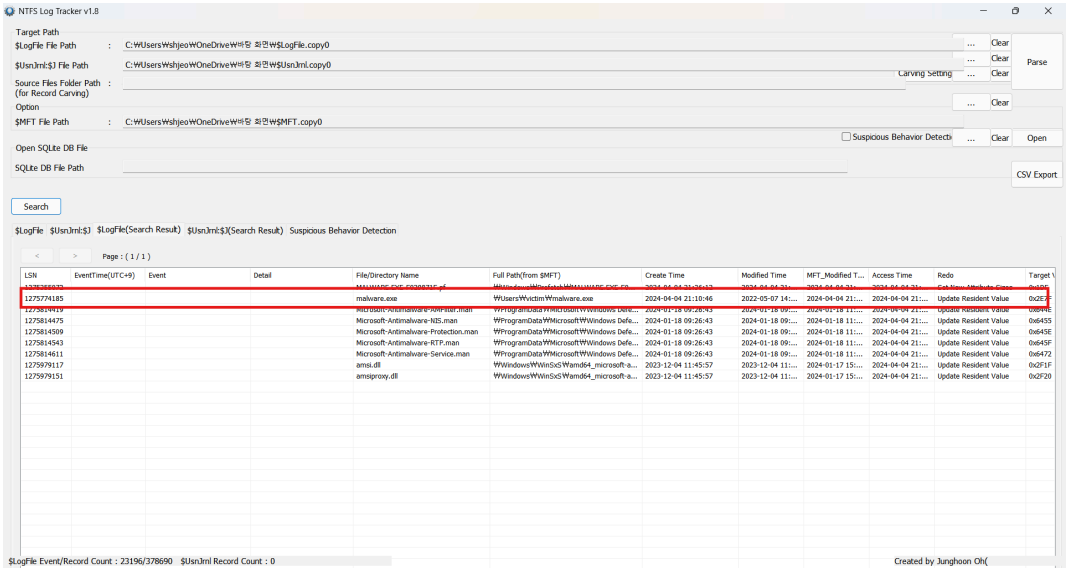
사용 툴 - FTK Imager, NTFS Log Tracker

1. FTK Imager 를 통해 $MFT, $LogFile, $UsnJrnl 파일 추출
   - 경로 : `C:\$MFT` , `C:\$LogFile` , `C:\$Extend\$UsnJrnl`





2. NTFS Log Tracker 를 통해 malware.exe 의 최초 시간 확인
    - 분석 내용 : 2024-04-04 21:10:46 인 것을 확인



👉 DH{2024_04_04_21_10_46}