Dreamhack-Autoruns (level1)

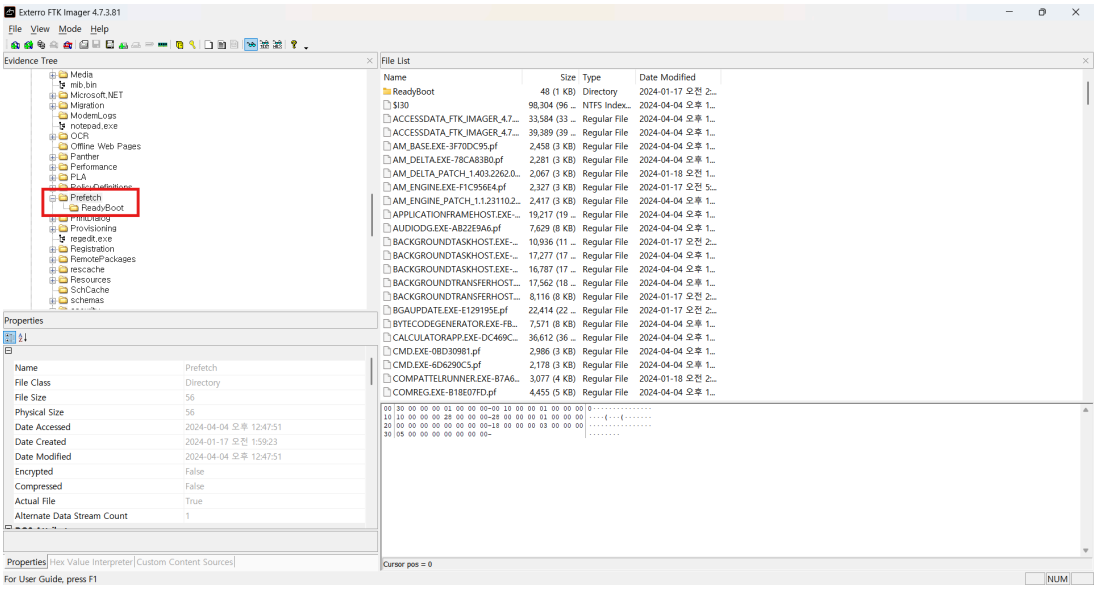
👉 **[함께실습] Autoruns에서 실습하는 문제입니다.**

드림이의 컴퓨터에 누군가가 USB 저장장치를 연결했다가 해제한 후에, 컴퓨터를 재부팅할 때마다 계산기 프로그램이 실행되고 있어요. 도대체 어떻게 된 일일까요?

Windows 레지스트리를 분석해 플래그를 찾아보세요.

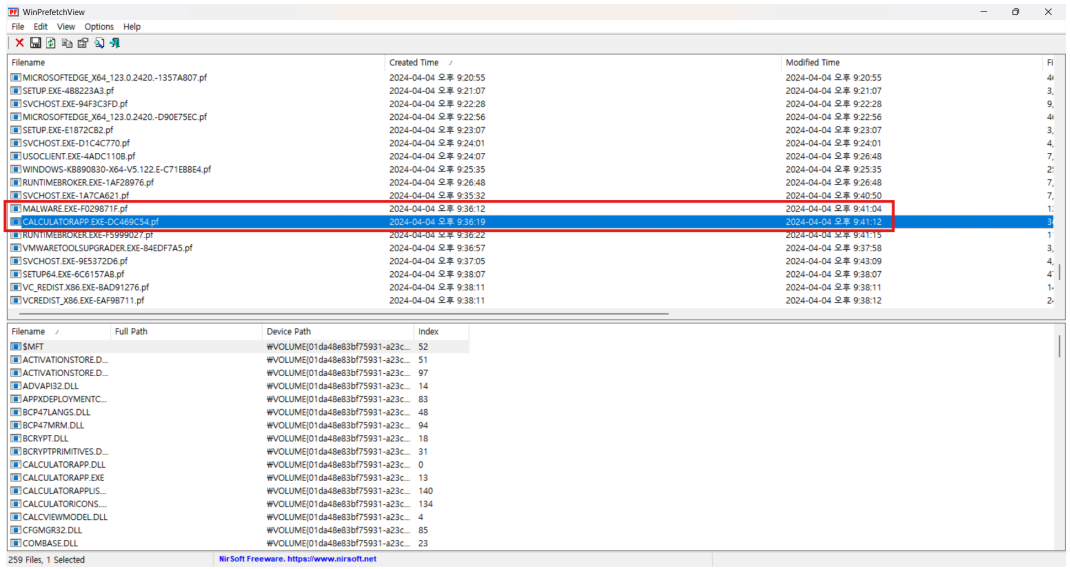
사용 툴 - FTK Imager, WinPrefetchView

1. FTK Imager 를 통해 Prefetch 폴더 추출
   - 경로 : `C:\Windows\Prefetch`

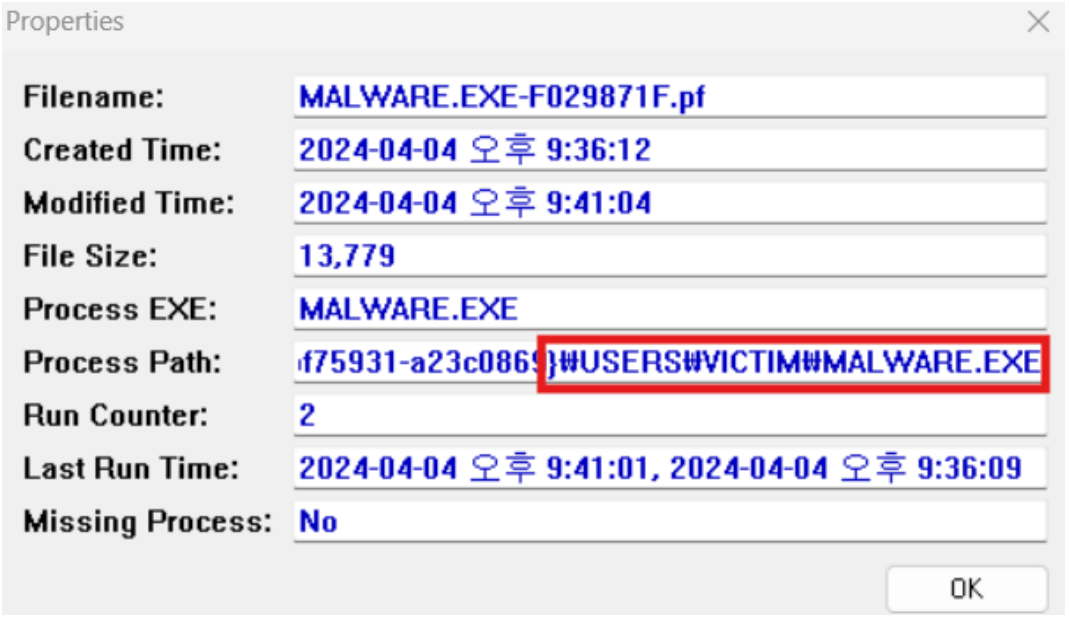


2. WinPrefechView 를 통해 계산기 흔적 찾음

- 분석 내용 : 다음을 통해, 계산기 실행 시간과 동일하게 MALWARE.EXE 가 실행된 것을 알 수 있음

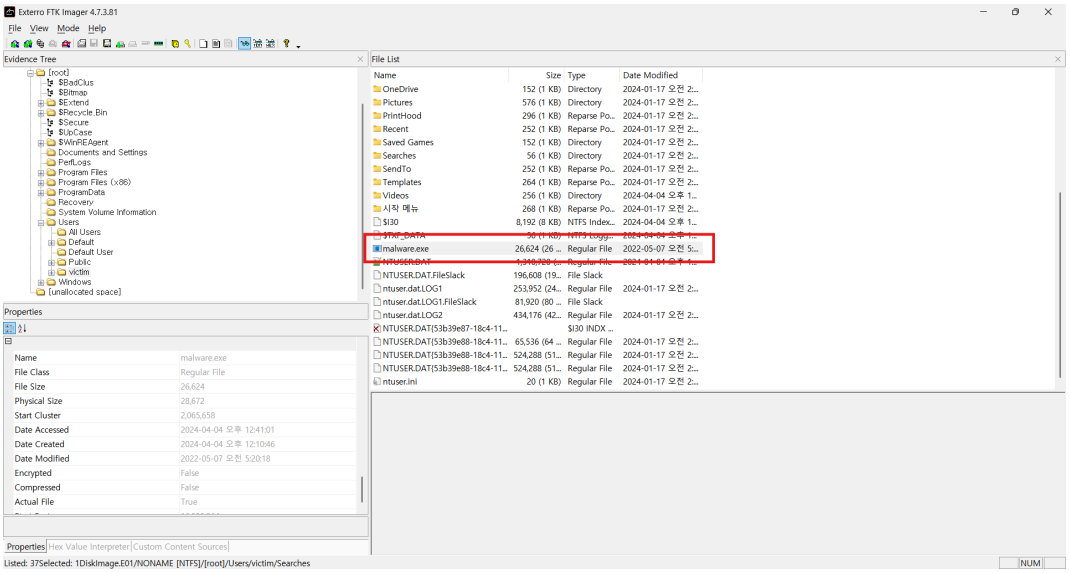


3. WinPrefechView 를 통해 MALWARE.EXE 경로 확인



4. FTK Imager 를 통해 해당 경로에서 해시값 추출

- 경로 : `C:\Users\victim\malware.exe`



MD5 = 302021d31f2d0bce01d7afc26bfe2ba2

👉 DH{302021d31f2d0bce01d7afc26bfe2ba2}