Dreamhack-study_checker (level1)

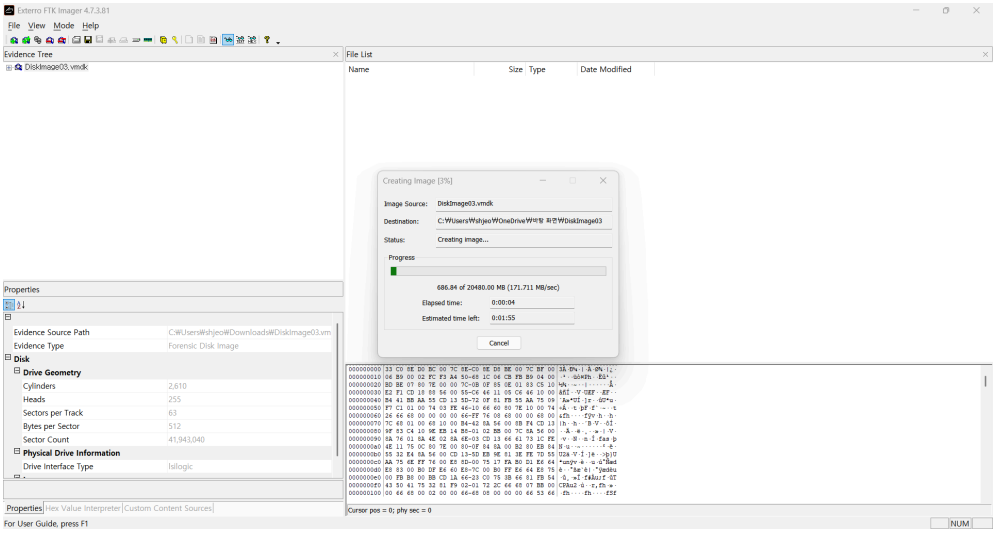
[함께실습] study_checker에서 실습하는 문제입니다.

당신은 드림고등학교의 야간 자율 학습 감독입니다. 어느 날 A 학생이 학습 시간에 컴퓨터를 이용해 몰래 게임을 했다는 제보를 받았습니다.

해당 PC에 대한 디지털 포렌식을 통해 증거를 확보해주세요!

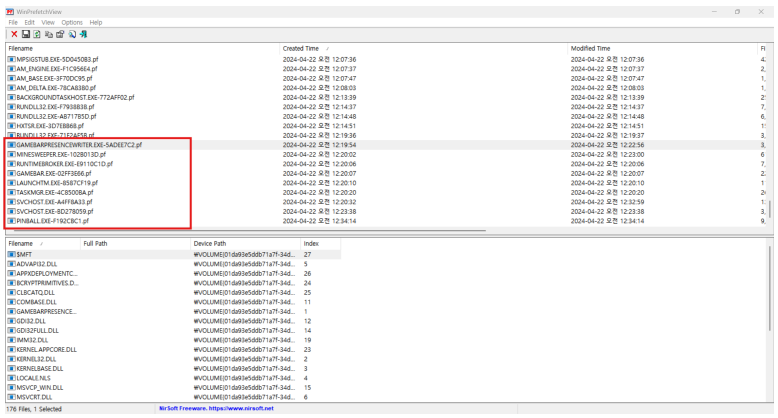
사용 툴 - FTK Imager, WinPrefetchView

1. FTK Imager 를 통해 vmdk 파일 이미징

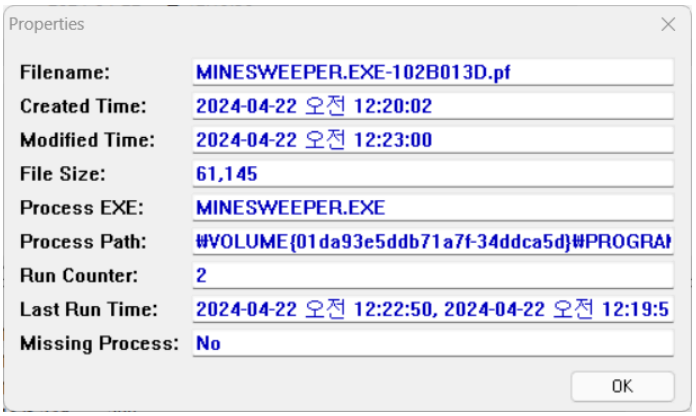


- FTK Imager 를 통해 이미징한 파일로 분석 진행

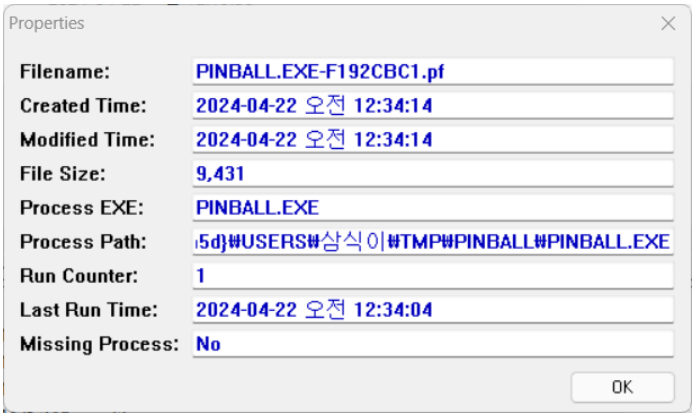
2. FTK Imager 를 통해 Prefetch 파일 추출 후 WinPrefetchView 를 통해 게임 관련 실행 아티팩트 분석
   - 경로 : `C:\Windows\Prefetch`
   - 분석 내용
     - WinPrefetchView 에서 Createtime 정렬 이후 game 검색한 결과 가장 먼저 실행된 게임으로 MINESWEEPER, 가장 마지막으로 실행된 게임으로 PINBALL 을 찾을 수 있었음



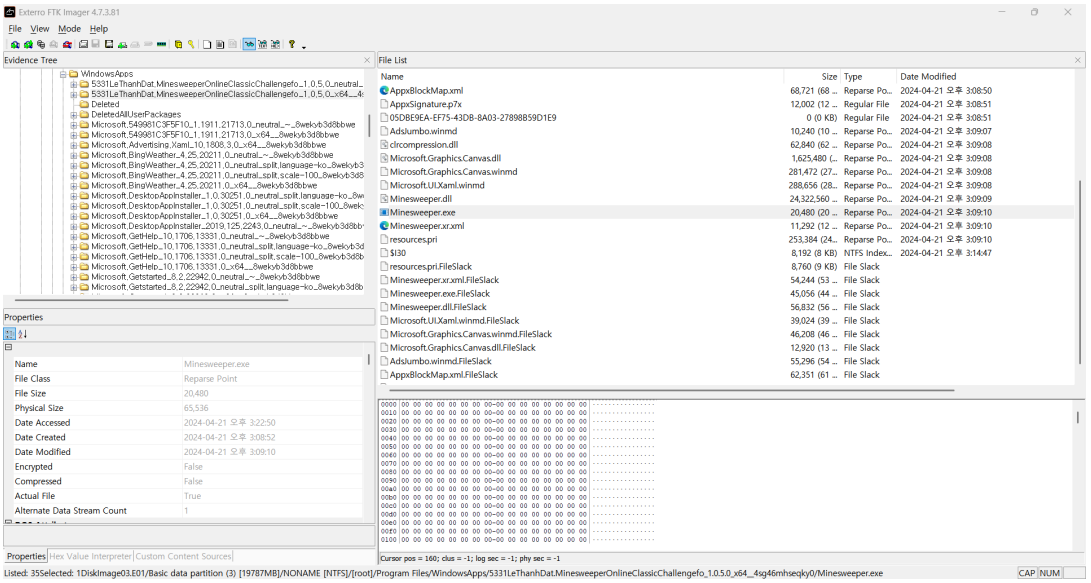
- MINESWEEPER 가 처음 실행된 시각은 2024-04-22 오전 12:19:51 이며, Unix Timestamp 로 변환 시 1713712791 임



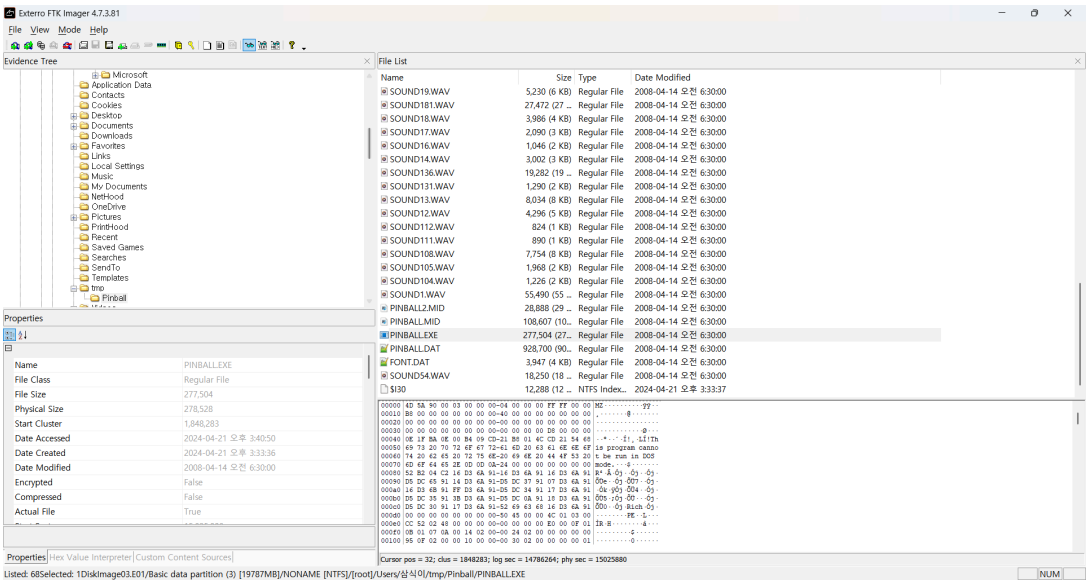
- PINBALL 가 마지막으로 실행된 시각은 2024-04-22 오전 12:34:04 이며, Unix Timestamp 로 변환 시 1713713644 임



3. FTK Imager 를 통해 앞서 확보한 경로를 추적하여 실제 프로그램 이름 확인
   - 가장 먼저 실행된 게임
     - 경로 : `C:\PROGRAM FILES\WINDOWSAPPS\5331LETHANHDAT.MINESWEEPERONLINECLASSICCHALLENGEFO_1.0.5.0_X64__4SG46MHSEQKY0\Minesweeper.EXE`



- 나중에 실행된 게임
  - 경로 : `C:\Users\삼식이\tmp\Pinball\PINBALL.EXE`



👉🏻 DH{Minesweeper_1713712791_PINBALL_1713713644}