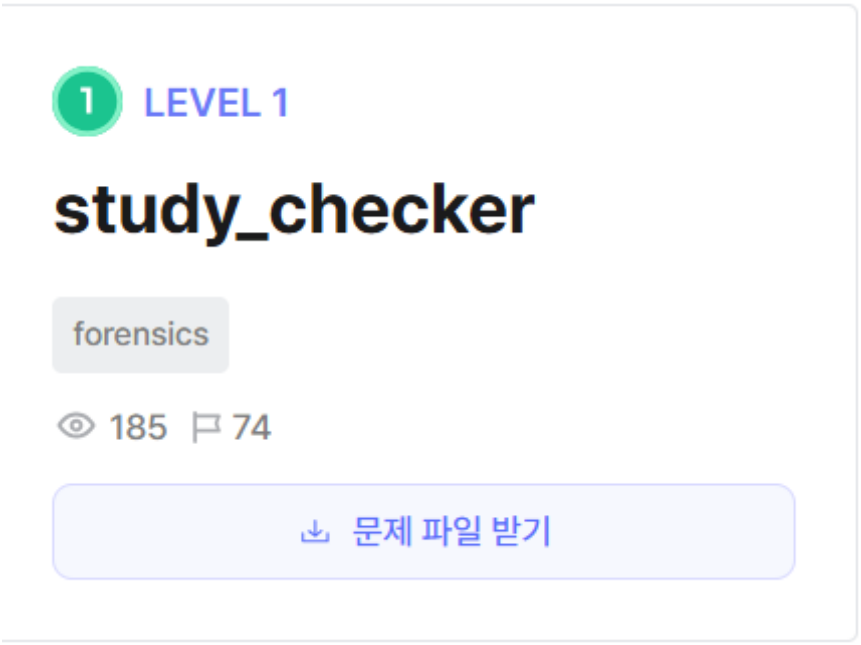
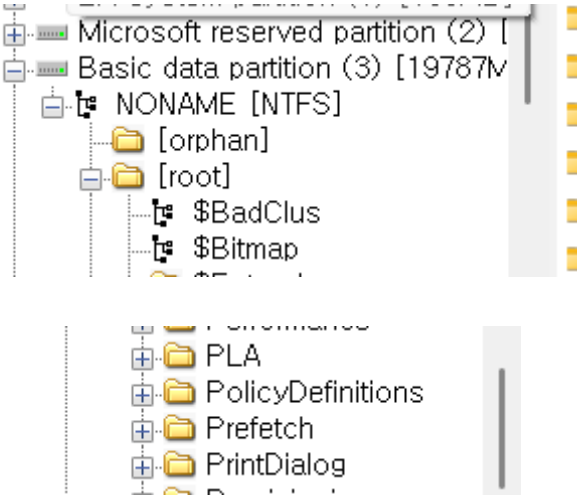
# Dreamhack-study_checker




일단 캐시를 통해서 응용프로그램들의 실행 흔적을 분석해야 하기 때문에

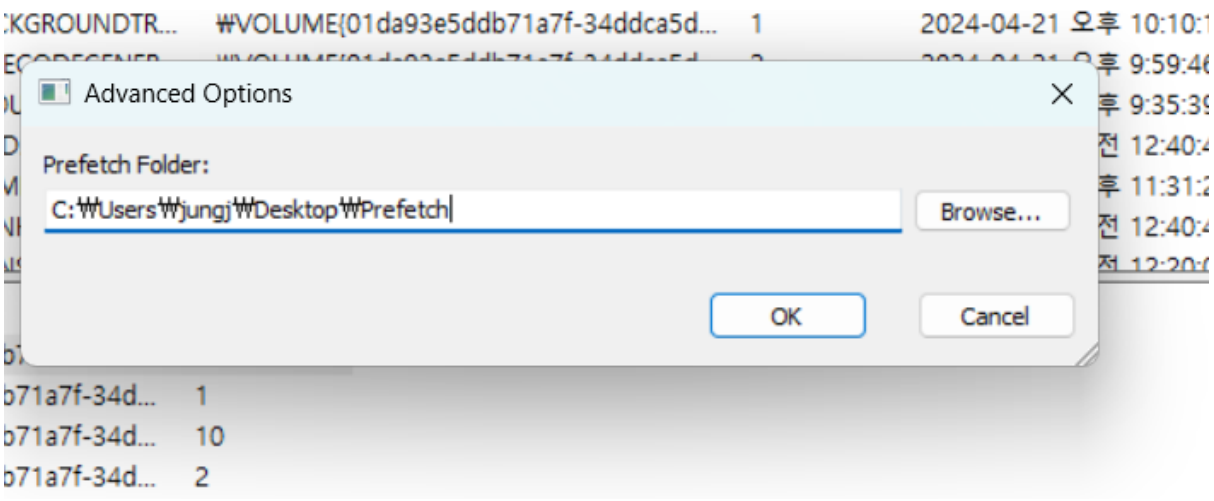
일단 ftk로 열어서 prefetch 파일을 추출해야한다.

베이직 데이터 파티션-노네임-루트-프리패치 이 경로로 가서 추출하면 된다.




그다음 winprefetchview를 열어서 분석해야 하는데

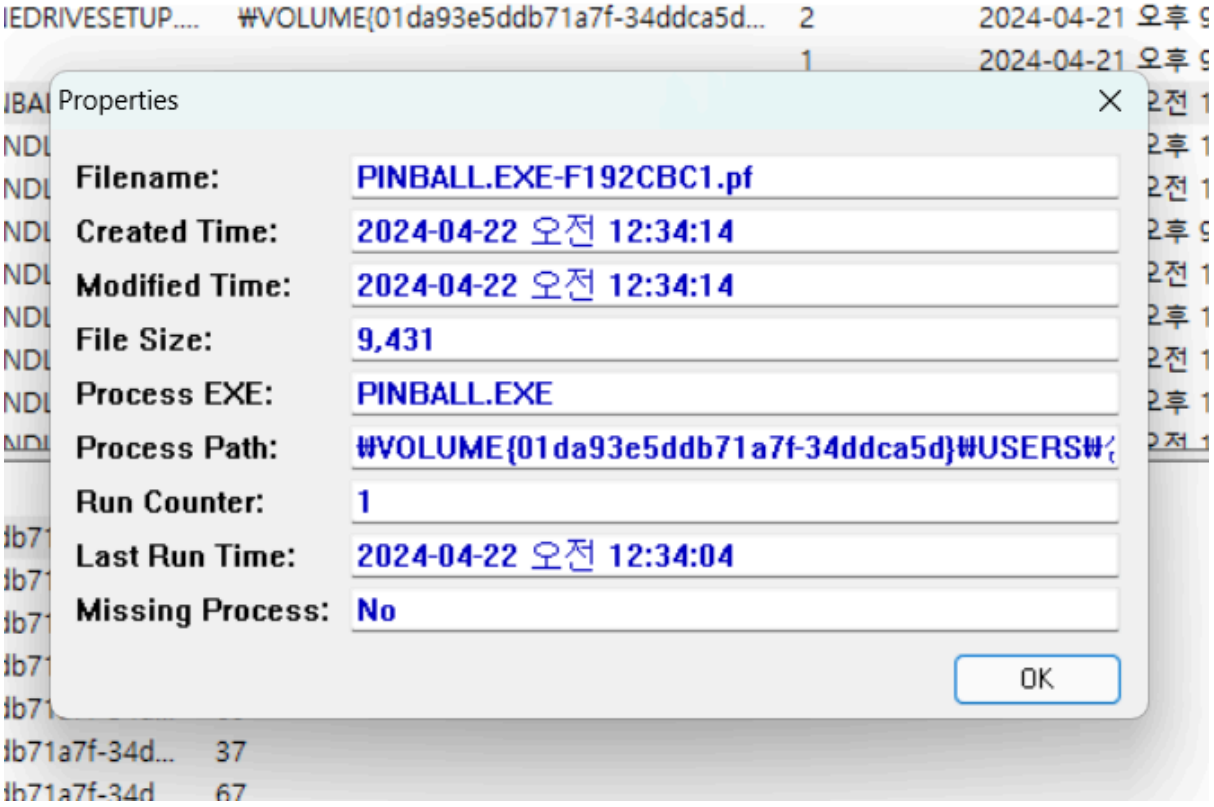
winprefetchview 도구는 기본적으로 현재 실행되고 있는 pc의 프리패치를 보여준다. 그러나 우리는 현재 pc의 프리패치가 아니라 ftk imager로 수집한 프리패치를 분석하기 위해서 상단 Options → Advanced Options 버튼을 클릭해서 경로를 다시 지정해야한다.



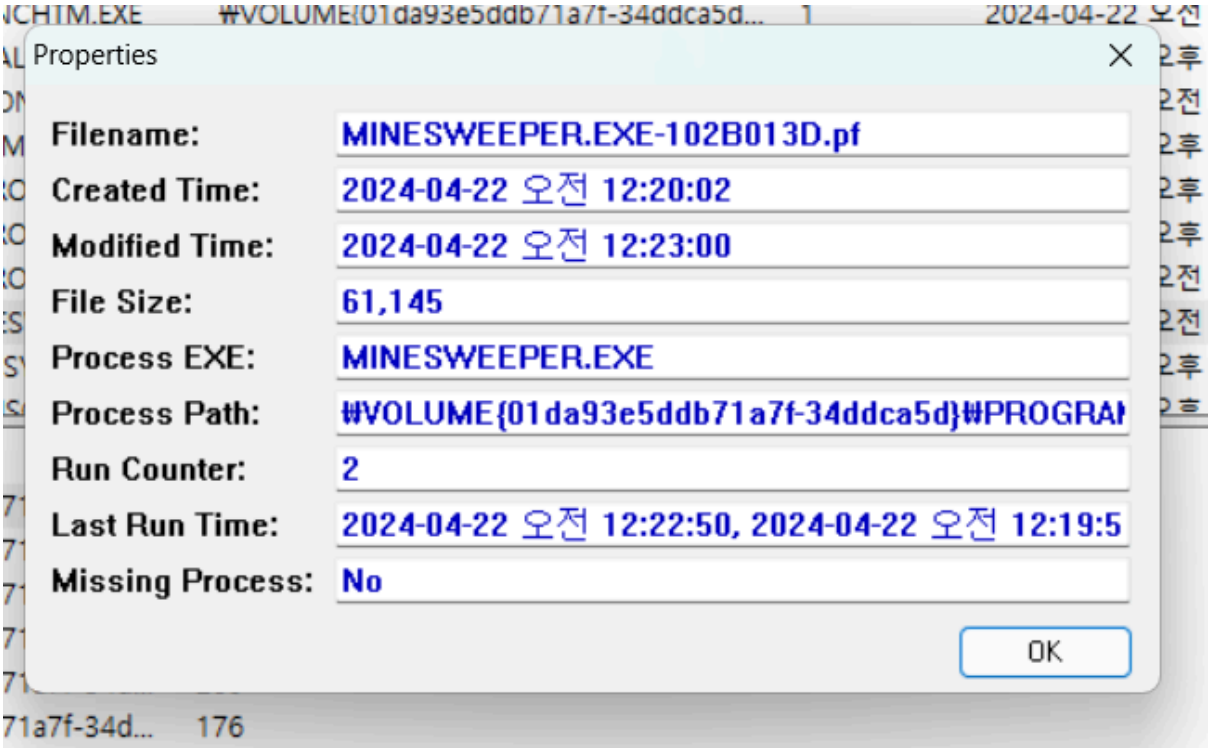

근데 여기서 우리가 찾아야 하는건 게임 프리패치 파일이기 때문에 게임이 들어간 파일을 찾으면 된다.

근데 여기서 게임 이름 자체를 찾아야하기 때문에 검색 기능을 이용을 못하고 일일이 찾아야 한다.

찾다 보면



이렇게 게임 이름이 나온다..핀볼 게임... 이게 첫번째고




두번째가 지뢰찾기 게임이다...

근데 라스트 런타임이 지뢰찾기 게임이 핀볼보다 먼저이므로 먼저 실행된 게임 프로그램 이름은 지뢰찾기 이다.

A: 먼저 실행된 게임 프로그램의 이름 (경로 제외, 확장자 제외) - MINESWEEPER

B: A가 처음 실행된 시각 (Unix Timestamp, seconds 단위) - 1713712791

C: 나중에 실행된 게임 프로그램의 이름 (경로 제외, 확장자 제외) - PINBALL

D: C가 마지막으로 실행된 시각 (Unix Timestamp, seconds 단위) - 1713713644

**FLAG: DH{Minesweeper_1713712791_PINBALL_1713713644}**