Dreamhack-study_checker(level1)

[forensics]

Description

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! (2024.10.02)

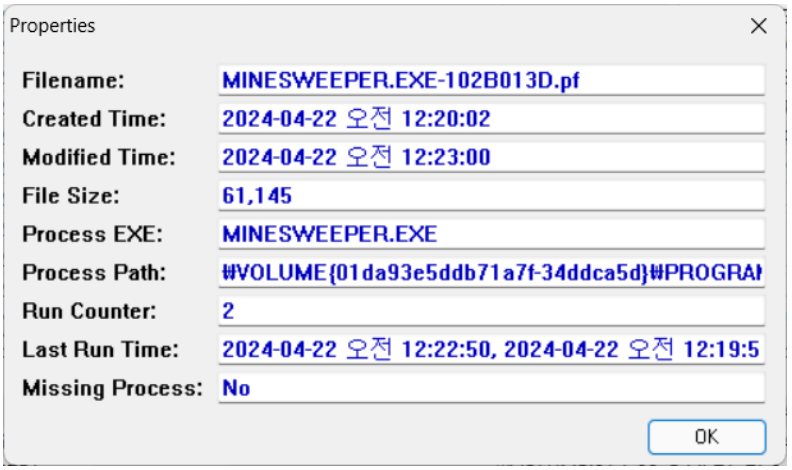
Info

- FLAG = `DH{A_B_C_D}`
  - A: 먼저 실행된 게임 프로그램의 이름 (경로 제외, 확장자 제외)
  - B: A가 처음 실행된 시각 (**Unix Timestamp**, seconds 단위)
  - C: 나중에 실행된 게임 프로그램의 이름 (경로 제외, 확장자 제외)
  - D: C가 마지막으로 실행된 시각 (**Unix Timestamp**, seconds 단위)
- 예를 들어 A가 `aaa`, B가 `1712154549`, C가 `bbb`, 그리고 D가 `1712209876`이라면 FLAG는 `DH{aaa_1712154549_bbb_1712209876}`입니다.

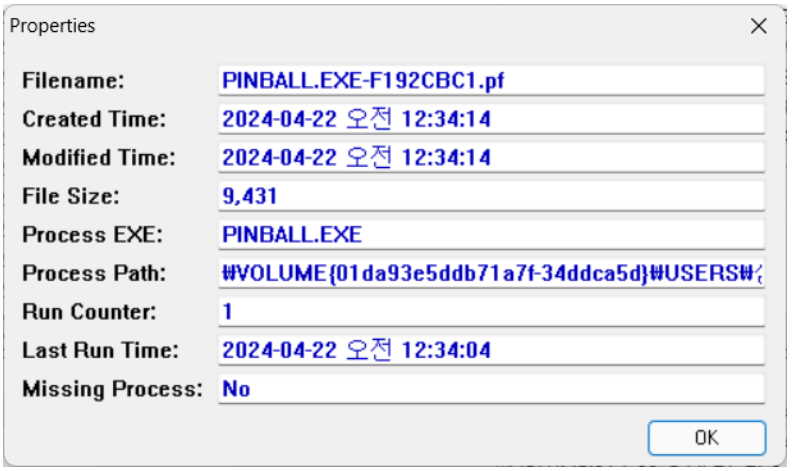
Write up

- 사용 도구: FTK Imager, WinPrefetchView
  1. FTK Imager를 통해 Prefetch 폴더 추출
  2. WinPrefetch를 통해 추출한 Prefetch 폴더 분석
     - 실행된 파일을 분석하여 게임 파일 추출
     - 실행된 시간 = Last Run Time 분석

- **MINESWEEPER.EXE-102B013D.pf**
  - 2024-04-22 00:19:51, 2024-04-22 00:22:50
  - 경로: `\VOLUME{01da93e5ddb71a7f-34ddca5d}\PROGRAM FILES\WINDOWSAPPS\5331LETHANHDAT.MINESWEEPERONLINECLASSICCHALLENGEFO_1.0.5.0_X64__4SG46MHSEQKY0\MINESWEEPER.EXE`



- **PINBALL.EXE-F192CBC1.pf**
  - 2024-04-22 오전 12:34:04
  - 경로: `\VOLUME{01da93e5ddb71a7f-34ddca5d}\USERS\삼식이\TMP\PINBALL\PINBALL.EXE`



- 시도 1 → 실패

MINESWEEPER

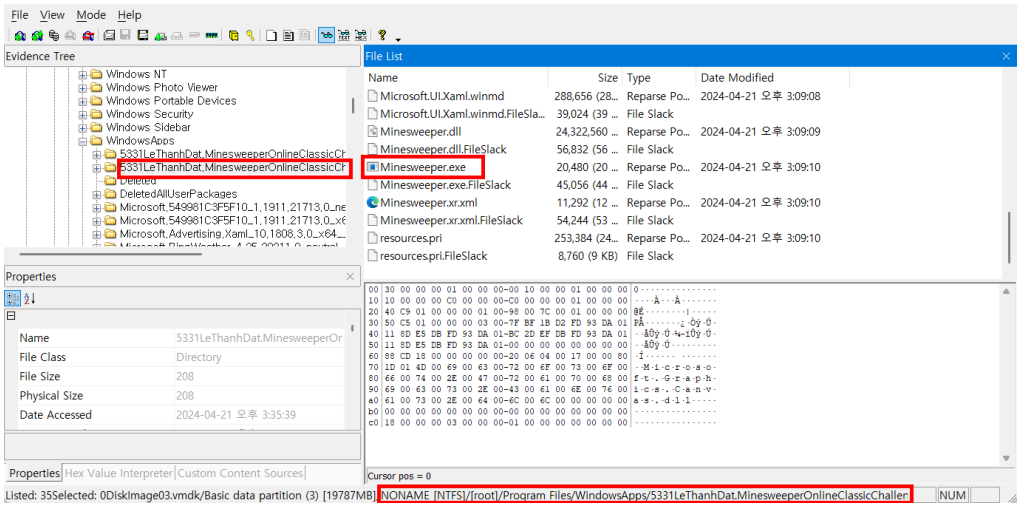
2024-04-22 00:19:51 → 1713712791(Unix Timestamp)

PINBALL

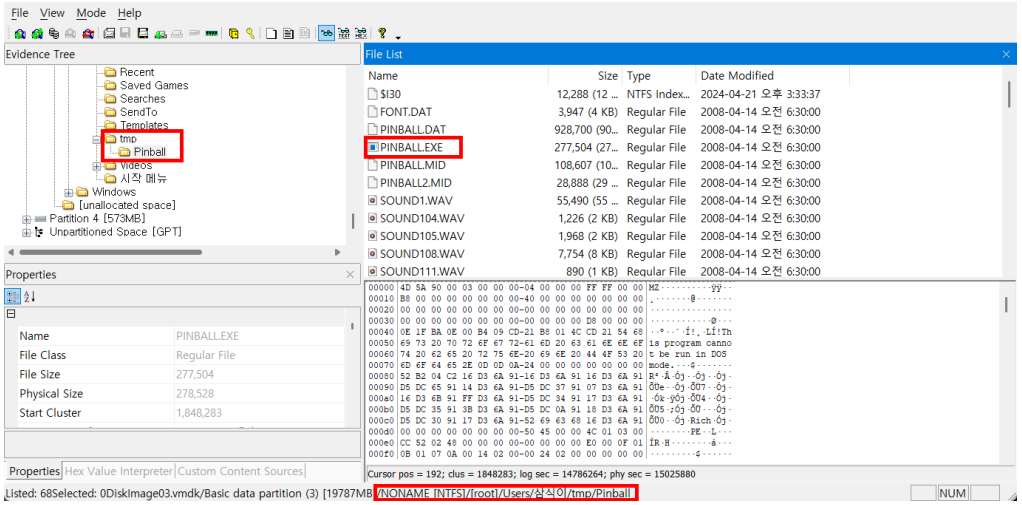
2024-04-22 00:34:04 → 1713713644(Unix Timestamp)

DH{MINESWEEPER_1713712791_PINBALL_1713713644}

- 시도 2 → 성공
  - **대소문자 구분 문제** 때문에 실패한 것 같아서, 해당 경로에 들어가서 파일 이름 확인
  - MINESWEEPER → Minesweeper로 변경



- PINBALL → PINBALL 그대로



Minesweeper

2024-04-22 00:19:51 → 1713712791

PINBALL

2024-04-22 00:34:04 → 1713713644

DH{Minesweeper_1713712791_PINBALL_1713713644}

문제에 대소문자 구분에 대한 힌트가 포함되어 있었다면 풀이 시간을 더 단축할 수 있었을 것 같다.

FLAG

DH{Minesweeper_1713712791_PINBALL_1713713644}