

Write-up: study_checker (DreamHack Forensics Challenge)

<https://dreamhack.io/wargame/challenges/1329>

1. Challenge Info

2. Problem Description

3. Provided Files

4. Tools Used

5. Analysis Steps

5.1 디스크 이미지 마운트

5.2 Prefetch 확인

5.3 게임 실행 파일 식별

5.4. 플래그 실패

5.5 정확한 프로그램 이름 확인

5.6 최종 정보 정리

6. Flag

1. Challenge Info

- **Challenge Name:** study_checker
- **Category:** Forensics
- **Difficulty Level:** Level 1
- **Platform:** DreamHack Wargame
- **Objective:**

드림이의 컴퓨터에서 먼저 실행된 게임 프로그램과 나중에 실행된 게임 프로그램의 이름 및 각각의 최초·최종 실행 시각(Unix Timestamp) 을 분석하여 플래그를 완성하라.

플래그 형식: DH{A_B_C_D}

- A: 먼저 실행된 게임 프로그램의 이름 (경로 및 확장자 제외)
- B: A의 최초 실행 시각 (Unix Timestamp)
- C: 나중에 실행된 게임 프로그램의 이름 (경로 및 확장자 제외)
- D: C의 최종 실행 시각 (Unix Timestamp)

2. Problem 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!"

- 제공된 디스크 이미지: `DiskImage03.vmdk`

3. Provided Files

- `DiskImage03.vmdk` (Windows 시스템의 디스크 이미지 파일, VMDK 포맷)

4. Tools Used

| Tool | Version |
|-----------------|-----------|
| FTK Imager | v4.7.8.31 |
| WinPrefetchView | v1.37 |

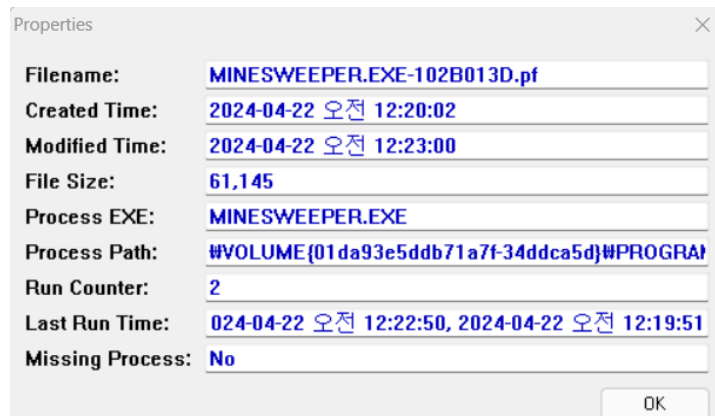
5. Analysis Steps

5.1 디스크 이미지 마운트

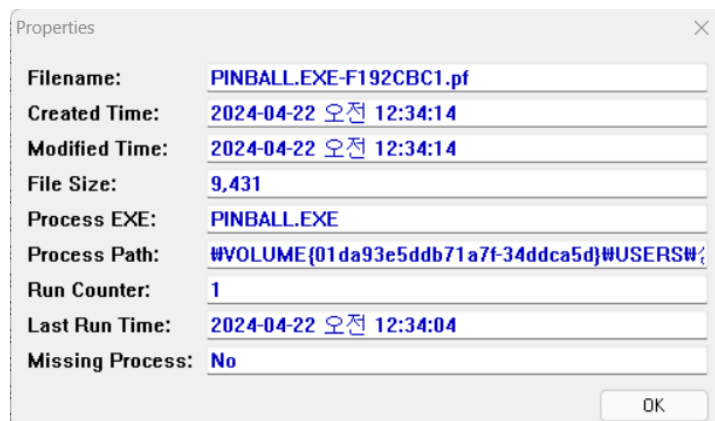
- 도구: FTK Imager
- 제공된 `DiskImage03.vmdk` 파일을 FTK Imager로 열기
- Prefetch 폴더 추출
 - 경로: `C:\Windows\Prefetch`

| | | | |
|--------------|-----------------|--------------|-----------------------|
| Temp | 176 (1 KB) | Directory | 2024-04-21 오후 3:14:19 |
| AppReadiness | 48 (1 KB) | Directory | 2024-04-21 오후 3:40:55 |
| Prefetch | 56 (1 KB) | Directory | 2024-04-21 오후 3:40:55 |
| write.exe | 11,264 (11 ...) | Regular File | 2019-12-06 오후 9:29:00 |
| mib.bin | 43,131 (43 ...) | Regular File | 2019-12-07 오전 9:08:58 |

- 최초 실행 시간: 1713712791 (오전 12:19:51)



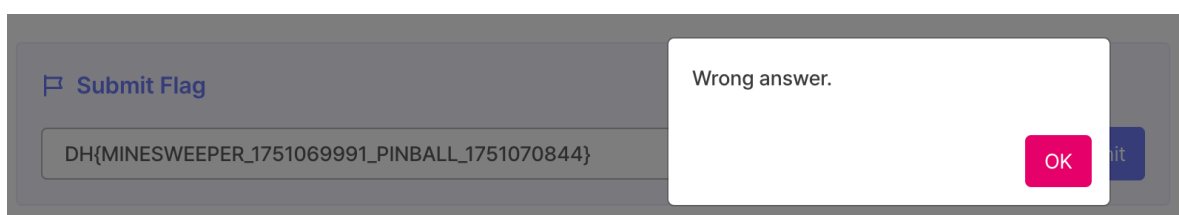
- 나중에 실행된 게임 프로그램
 - 프로그램 이름: PINBALL
 - 최종 실행 시각: 1713713644 (오전 12:34:04)



5.4. 플래그 실패

- 제출:

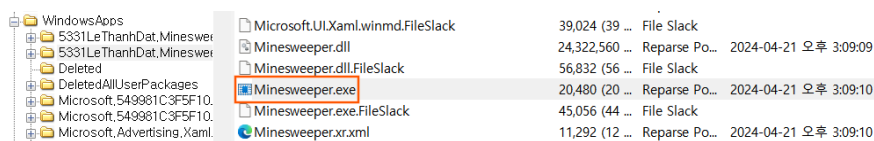
DH{MINESWEEPER_1713712791_PINBALL_1713713644}



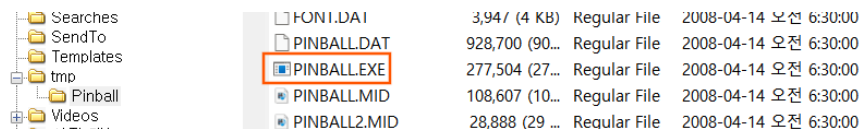
- 결과: Wrong answer

5.5 정확한 프로그램 이름 확인

- 도구: FTK Imager
- 먼저 실행된 게임 프로그램
 - Prefetch 경로 기반으로 정확한 프로그램 이름을 재확인
 - 경로: `C:\Program Files\WindowsApps\5331LeThanhDat.MinesweeperOnlineClassicChallengefo_1.0.5.0_x64__4sg46mhseqky0\MINESWEEPER.EXE`
 - 프로그램 이름: `Minesweeper`



- 나중에 실행된 게임 프로그램
 - Prefetch 경로 기반으로 정확한 프로그램 이름을 재확인
 - 경로: `C:\Users\삼식이\tno\pinball\PINBALL.EXE`
 - 프로그램 이름: `PINBALL`



5.6 최종 정보 정리

- 먼저 실행된 게임 프로그램: `Minesweeper`
- 최초 실행 시간: `1713712791`
- 나중에 실행된 게임 프로그램: `PINBALL`
- 최종 실행 시각: `1713713644`

6. Flag


DH{Minesweeper_1713712791_PINBALL_1713713644}

Congratulations!

1 LEVEL 1 study_checker
You solved this challenge.

Great job! How did you solve this challenge?
Share your writeup to earn points!

No thanks.

 Submit writeup