Dreamhack-study_checker

문제

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!

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.

풀이

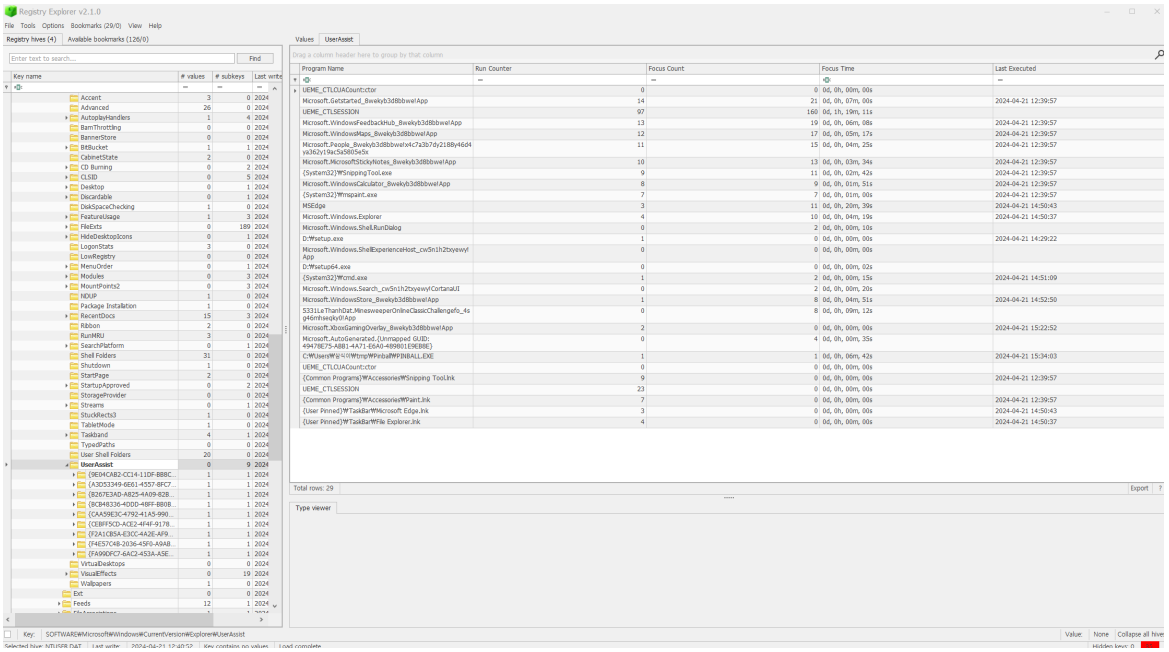
1. 문제 파악

   어떤 게임 프로그램들이 실행됐는지 파악해야한다, 각 게임이 실행된 시각을 분석하여 FLAG 찾기

   DH{최초 실행게임_최초 실행시간_마지막 실행게임_마지막 실행시간}

2. 문제 풀이

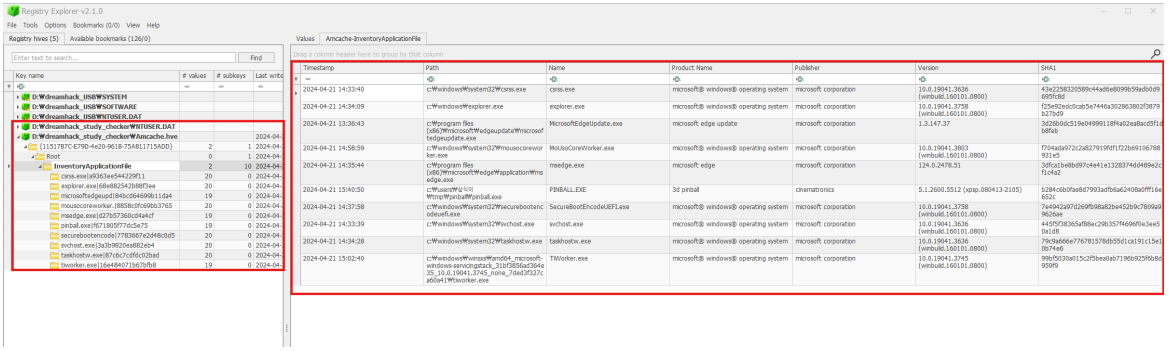
   분석한 파일 : `Amcache.hve` , `NTUSER.DAT`

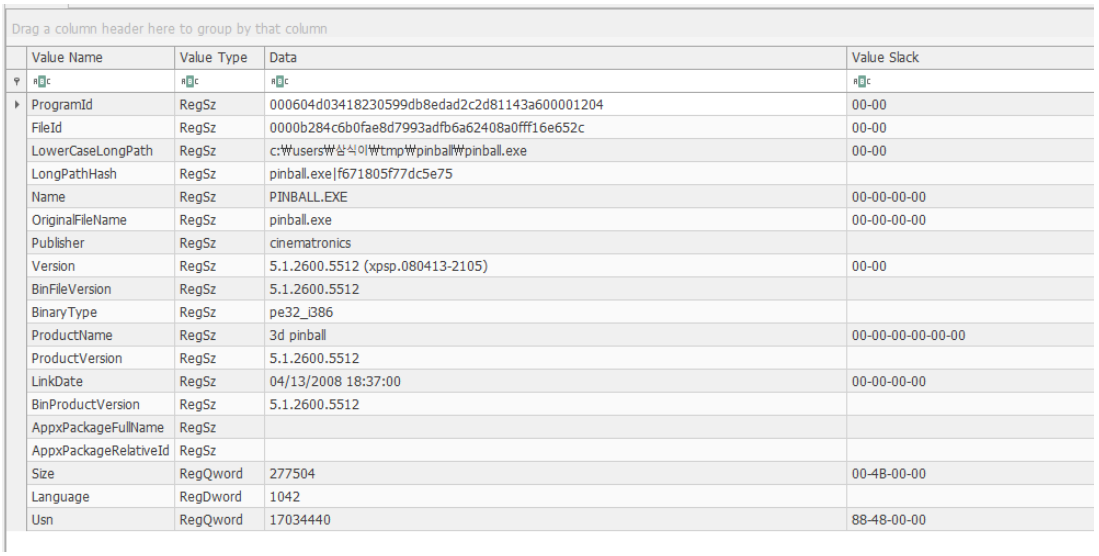


(1) 경로 : SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist

분석 내용 : 사용자 인터페이스를 통해 실행한 프로그램에 대한 정보를 기록하는 레지스트리 위치, 프로그램 이름, 실행 횟수, 포커스 시간, 마지막 실행 시각 등이 기록

[pinball.exe 확인 가능]





Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack
ProgramId	RegSz	000604d03418230599db8edad2c2d81143a600001204	00-00
FileId	RegSz	0000b284c6b0fae8d7993adfb6a62408a0fff16e652c	00-00
LowerCaseLongPath	RegSz	c:₩users₩삼식이₩tmp₩pinball₩pinball.exe	00-00
LongPathHash	RegSz	pinball.exe|f671805f77dc5e75	
Name	RegSz	PINBALL.EXE	00-00-00-00
OriginalFileName	RegSz	pinball.exe	00-00-00-00
Publisher	RegSz	cinematronics	
Version	RegSz	5.1.2600.5512 (xpsp.080413-2105)	00-00
BinFileVersion	RegSz	5.1.2600.5512	
BinaryType	RegSz	pe32_i386	
ProductName	RegSz	3d pinball	00-00-00-00-00-00
ProductVersion	RegSz	5.1.2600.5512	
LinkDate	RegSz	04/13/2008 18:37:00	00-00-00-00
BinProductVersion	RegSz	5.1.2600.5512	
AppxPackageFullName	RegSz		
AppxPackageRelativeId	RegSz		
Size	RegQword	277504	00-4B-00-00
Language	RegDword	1042	
Usn	RegQword	17034440	88-48-00-00

(2) 경로 : `Root\InventoryApplicationFile\pinball.exe|f671805f77dc5e75`

분석 내용 :

항목	값
실행 파일 이름	`pinball.exe`
실행 경로	`C:\Users\삼식이\tmp\pinball\pinball.exe`
Product Name	`3d pinball`
Publisher	`cinematronics`
실행 시각	`2024-04-21 15:40:50`