

# study\_checker

## 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!

## 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 1712209876이라면 FLAG는 DH{aaa\_1712154549\_bbb\_1712209876}입니다.

## 사용한 도구



FTK Imager, WinprefetchView

### 1. Prefetch파일 추출

게임 프로그램의 실행 시각을 알아야한다는 FLAG 조건을 통해 prefetch파일에 단서가 있을 것이라고 생각해 FTK Imager를 사용해 prefetch파일을 추출하였다.

경로: `C:\Windows\prefetch`

### 2. WinPrefetchView로 확인

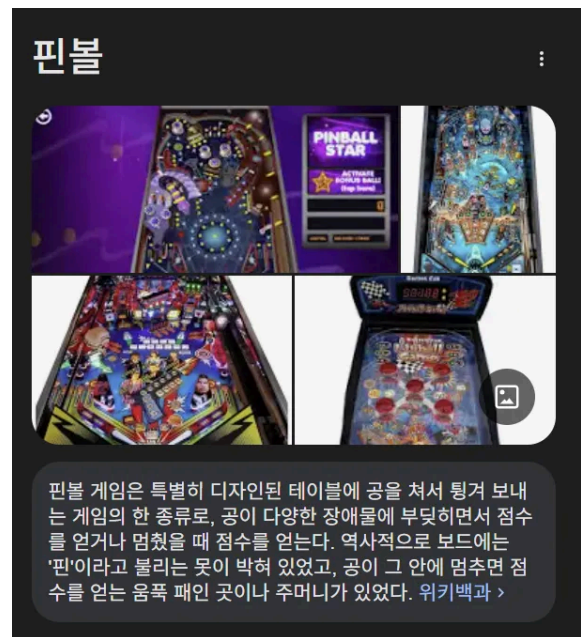
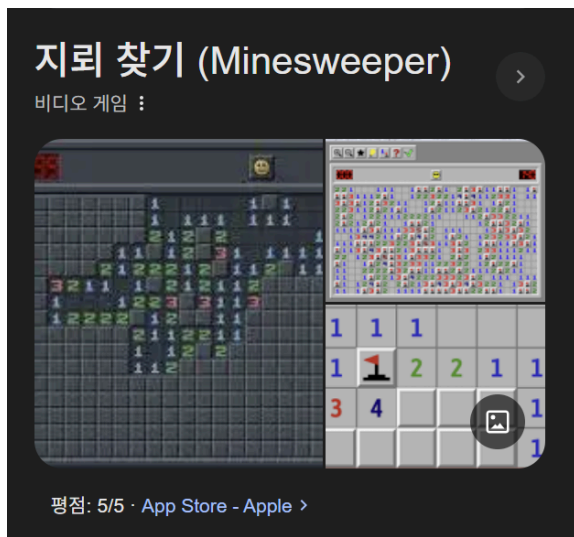
 GAMEBAR.EXE-02FF3E66.pf	2024-04-22 오전 12:20:07	2024-04-22 오전 12:20:07	22,934
 GAMEBARPRESENCEWRITER.EXE-5ADEE7C2.pf	2024-04-22 오전 12:19:54	2024-04-22 오전 12:22:56	3,764

처음 Prefetch파일을 확인했을때 제목에 GAME이 들어가고 연속으로 실행된 파일이 두개가 존재해 이 두 파일의 실행값으로 FLAG를 시도했으나 정답이 아니었다.

이후 모든 프리패치 파일을 다 확인해보았다.

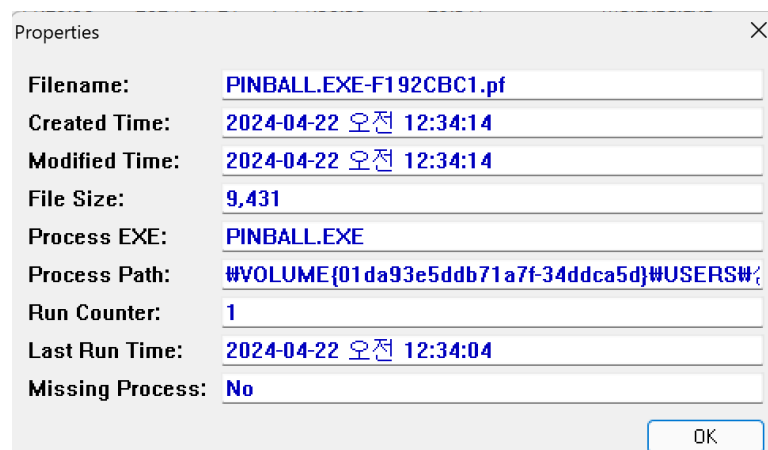
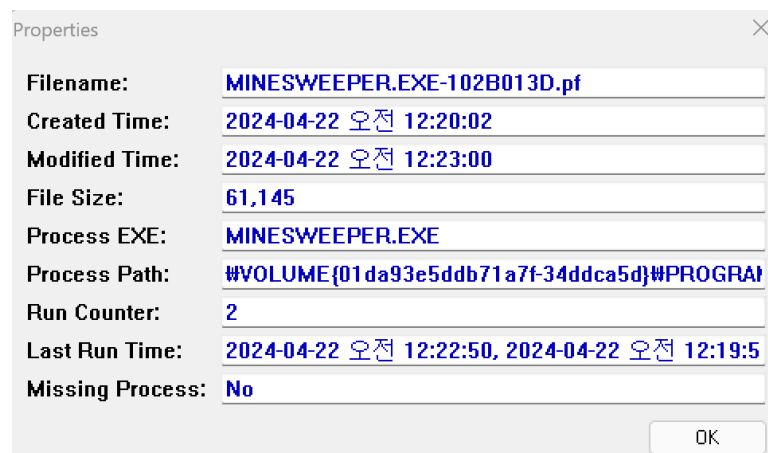
WinPrefetchView				
File Edit View Options Help				
Filename	Created Time	Modified Time	File Size	Process EXE
COREDPUSVR.EXE-035072F5.pf	2024-04-21 오후 11:53:02	2024-04-21 오후 11:53:02	6,349	COREDPUSSVR.EXE
CSRSS.EXE-F3C368CB.pf	2024-04-21 오후 9:40:55	2024-04-21 오후 9:40:55	4,601	CSRSS.EXE
DEFRAG.EXE-3D9E8D72.pf	2024-04-21 오후 9:50:27	2024-04-21 오후 11:43:31	4,215	DEFRAG.EXE
DLLHOST.EXE-15CDDA9C.pf	2024-04-21 오후 9:36:01	2024-04-21 오후 11:52:54	11,428	DLLHOST.EXE
DLLHOST.EXE-3D723117.pf	2024-04-21 오후 9:42:01	2024-04-21 오후 11:59:08	5,483	DLLHOST.EXE
DLLHOST.EXE-4427C062.pf	2024-04-21 오후 9:38:27	2024-04-21 오후 9:38:27	4,946	DLLHOST.EXE
DLLHOST.EXE-4B6CB38A.pf	2024-04-21 오후 9:35:59	2024-04-22 오전 12:33:43	7,764	DLLHOST.EXE
DLLHOST.EXE-4F1B3E7E.pf	2024-04-21 오후 9:35:55	2024-04-21 오후 9:41:28	7,612	DLLHOST.EXE
DLLHOST.EXE-6389524F.pf	2024-04-21 오후 9:39:53	2024-04-21 오후 10:00:32	6,973	DLLHOST.EXE
DLLHOST.EXE-73455075.pf	2024-04-21 오후 11:31:32	2024-04-21 오후 11:31:32	8,735	DLLHOST.EXE
DLLHOST.EXE-960426D8.pf	2024-04-21 오후 9:35:31	2024-04-21 오후 9:38:54	6,402	DLLHOST.EXE
DLLHOST.EXE-A010D183.pf	2024-04-21 오후 11:29:49	2024-04-21 오후 11:29:58	4,167	DLLHOST.EXE
DLLHOST.EXE-ACFEFA21.pf	2024-04-21 오후 9:41:48	2024-04-21 오후 10:00:28	9,577	DLLHOST.EXE
DLLHOST.EXE-C60C3853.pf	2024-04-21 오후 9:35:45	2024-04-21 오후 9:41:41	5,005	DLLHOST.EXE
DLLHOST.EXE-E9BDD978.pf	2024-04-21 오후 9:35:57	2024-04-22 오전 12:22:21	4,447	DLLHOST.EXE
DRVINST.EXE-39D9EAC7.pf	2024-04-21 오후 9:37:12	2024-04-21 오후 11:30:56	8,281	DRVINST.EXE
DSMUSERTASK.EXE-853A6893.pf	2024-04-21 오후 9:38:39	2024-04-21 오후 9:41:49	5,949	DSMUSERTASK.EXE
DWM.EXE-314E93C5.pf	2024-04-21 오후 9:41:10	2024-04-21 오후 9:41:10	16,061	DWM.EXE
ELEVATION_SERVICE.EXE-E1E59D04.pf	2024-04-21 오후 10:44:32	2024-04-22 오전 12:22:14	6,416	ELEVATION_SERVI...
FILESYNCCONFIG.EXE-14F4FCAC.pf	2024-04-21 오후 9:57:10	2024-04-21 오후 9:57:10	6,433	FILESYNCCONFIG....
FILESYNCCONFIG.EXE-7D0A5469.pf	2024-04-21 오후 9:56:32	2024-04-21 오후 9:56:32	6,046	FILESYNCCONFIG....
FIRSTLOGONANIM.EXE-FA0BF656.pf	2024-04-21 오후 9:41:11	2024-04-21 오후 9:41:11	13,119	FIRSTLOGONANI...
FONTDRVHOST.EXE-8152304A.pf	2024-04-21 오후 9:41:04	2024-04-21 오후 9:41:04	2,254	FONTDRVHOST.EXE
FSQUIRT.EXE-A8FF1DEB.pf	2024-04-21 오후 9:44:21	2024-04-21 오후 9:44:21	7,491	FSQUIRT.EXE
GAMEBAR.EXE-02FF3E66.pf	2024-04-22 오전 12:20:07	2024-04-22 오전 12:20:07	22,934	GAMEBAR.EXE
GAMEBARPRESENCEWRITER.EXE-5ADEE7C2.pf	2024-04-22 오전 12:19:54	2024-04-22 오전 12:22:56	3,764	GAMEBARPRESEN...
HXTSR.EXE-3D7EBB68.pf	2024-04-22 오전 12:14:51	2024-04-22 오전 12:14:51	15,287	HXTSR.EXE
IDENTITY_HELPER.EXE-51AF345D.pf	2024-04-21 오후 9:45:19	2024-04-22 오전 12:22:31	18,895	IDENTITY_HELPER....
IE4UINIT.EXE-693AF9DC.pf	2024-04-21 오후 9:41:17	2024-04-21 오후 9:41:28	13,996	IE4UINIT.EXE
LAUNCHTM.EXE-8587CF19.pf	2024-04-22 오전 12:20:10	2024-04-22 오전 12:20:10	11,457	LAUNCHTM.EXE
LOCALBRIDGE.EXE-60F55773.pf	2024-04-21 오후 9:59:56	2024-04-21 오후 9:59:56	24,156	LOCALBRIDGE.EXE
LOGONUI.EXE-F639BD7E.pf	2024-04-21 오후 9:40:58	2024-04-22 오전 12:20:09	23,394	LOGONUI.EXE
LPREMOVE.EXE-570BDF7.pf	2024-04-21 오후 9:37:41	2024-04-21 오후 9:37:42	2,266	LPREMOVE.EXE

수많은 .pf파일 중 어떤 것이 게임인지 확실하지 않기에 각 파일의 제목을 구글링 하여 두개의 게임을 발견했다.



### 3. 실행시간 찾기

두 프로그램의 실행시각을 확인하였다.



둘 중 먼저 시작된 것은 MINESWEEPER이고 처음 실행 시각은 2024-04-22 오전 12:19:51 이다.

PINBALL 의 마지막 실행시각은 2024-04-22 오전 12:34:04 이다.

두 시각을 Unix Timestamp로 바꾸면 1713712791, 1713713644 가 된다.

\*\*이때 GMT가 아닌 LocalTime으로 해야한다.

#### 4. 정확한 실행파일 제목

플래그 값은 대소문자를 구분하기 때문에 정확한 실행파일의 제목을 알아야 했다.

경로: C:\Program

Files\WindowsApps\5331LeThanhDat.MinesweeperOnlineClassicChallengeo\_1.0.5.0\_x64\_\_4sg46mhseqky()

	Name	Size	Type	Date Modif...
	5331LeThanhDat.MinesweeperOnlineClassicChallen...	56 (1 ...	Direct...	2024-04-2...
	5331LeThanhDat.MinesweeperOnlineClassicChallen...	208 (1 ...	Direct...	2024-04-2...
	Deleted	48 (1 ...	Direct...	2024-04-2...
	DeletedAllUserPackages	56 (1 ...	Direct...	2024-04-2...
	Microsoft.549981C3F5F10_1.1911.21713.0_neutral_~...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.549981C3F5F10_1.1911.21713.0_x64__8we...	192 (1 ...	Direct...	2024-04-2...
	Microsoft.Advertising.Xaml_10.1808.3.0_x64__8weky...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.BingWeather_4.25.20211.0_neutral_split.la...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.BingWeather_4.25.20211.0_neutral_split.sc...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.BingWeather_4.25.20211.0_neutral_~_8we...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.BingWeather_4.25.20211.0_x64__8wekyb3...	200 (1 ...	Direct...	2024-04-2...
	Microsoft.DesktopAppInstaller_1.0.30251.0_neutral_s...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.DesktopAppInstaller_1.0.30251.0_neutral_s...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.DesktopAppInstaller_1.0.30251.0_x64__8w...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.DesktopAppInstaller_2019.125.2243.0_neu...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.GetHelp_10.1706.13331.0_neutral_split.lan...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.GetHelp_10.1706.13331.0_neutral_split.scal...	56 (1 ...	Direct...	2024-04-2...
	Microsoft.GetHelp_10.1706.13331.0_neutral_~_8wek...	56 (1 ...	Direct...	2024-04-2...

Minesweeper.dll	24,322...	Repars...	2024-04-2...
Minesweeper.dll.FileSlack	56,832...	File Sl...	
Minesweeper.exe	20,480...	Repars...	2024-04-2...
Minesweeper.exe.FileSlack	45,056...	File Sl...	
Minesweeper.xr.xml	11,292...	Repars...	2024-04-2...
Minesweeper.xr.xml.FileSlack	54,244...	File Sl...	
resources.pri	253,38...	Repars...	2024-04-2...
resources.pri.FileSlack	8,760 (...	File Sl...	

경로: C:\Users\삼식이\tmp\Pinball

\$I30	12,288...	NTFS I...	2024-04-2...
FONT.DAT	3,947 (...	Regul...	2008-04-1...
PINBALL.DAT	928,70...	Regul...	2008-04-1...
<b>PINBALL.EXE</b>	277,50...	Regul...	2008-04-1...
PINBALL.MID	108,60...	Regul...	2008-04-1...
PINBALL2.MID	28,888...	Regul...	2008-04-1...
SOUND1.WAV	55,490...	Regul...	2008-04-1...
SOUND104.WAV	1,226 (...	Regul...	2008-04-1...

경로에 가서 직접 확인해보니 Minesweeper, PINBALL 로 해야함을 알 수 있었다.