

# Dreamhack-Autoruns (level1)



[함께실습] Autoruns에서 실습하는 문제입니다.

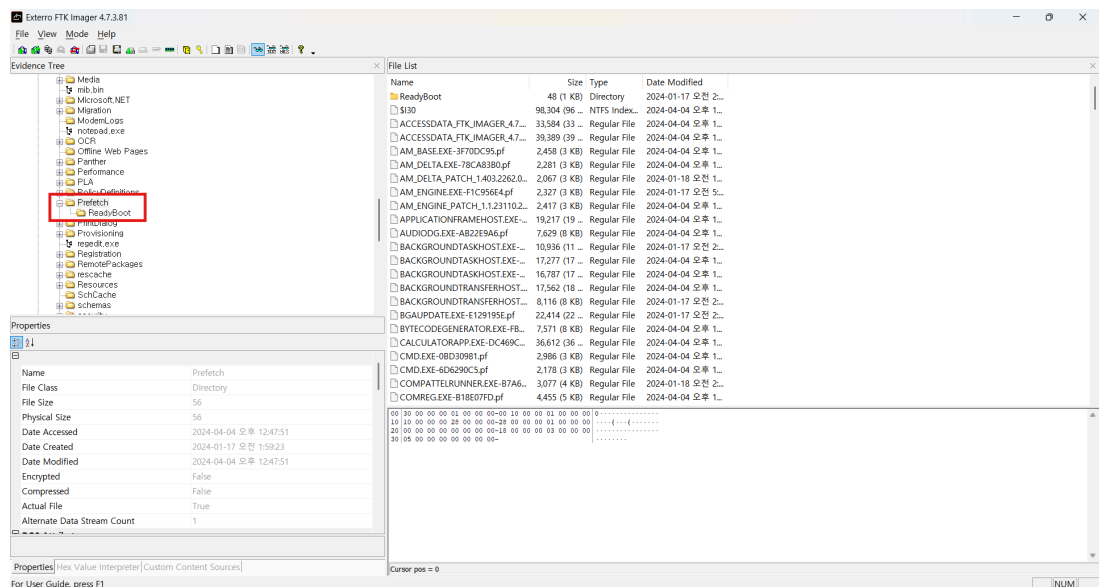
드림이의 컴퓨터에 누군가가 USB 저장장치를 연결했다가 해제한 후에, 컴퓨터를 재부팅할 때마다 계산기 프로그램이 실행되고 있어요. 도대체 어떻게 된 일일까요?

Windows 레지스트리를 분석해 플래그를 찾아보세요.

사용 툴 - FTK Imager, WinPrefetchView

## 1. FTK Imager 를 통해 Prefetch 폴더 추출

- 경로 : `C:\Windows\Prefetch`



## 2. WinPrefechView 를 통해 계산기 흔적 찾기

- 분석 내용 : 다음을 통해, 계산기 실행 시간과 동일하게 MALWARE.EXE 가 실행된 것을 알 수 있음

Filename	Created Time	Modified Time	FI
MICROSOFTEDGE_X64_123.0.2420.1357A807.pf	2024-04-04 오후 9:20:55	2024-04-04 오후 9:20:55	4h
SETUP.EXE-488223A3.pf	2024-04-04 오후 9:21:07	2024-04-04 오후 9:21:07	3,
SVCHOST.EXE-84F3CFD0.pf	2024-04-04 오후 9:22:28	2024-04-04 오후 9:22:28	9,
MICROSOFTEDGE_X64_123.0.2420.090E75EC.pf	2024-04-04 오후 9:22:56	2024-04-04 오후 9:22:56	4h
SETUP.EXE-E1872C82.pf	2024-04-04 오후 9:23:07	2024-04-04 오후 9:23:07	3,
SVCHOST.EXE-D1C4C770.pf	2024-04-04 오후 9:24:01	2024-04-04 오후 9:24:01	4,
USOCIENT.EXE-4ADC1108.pf	2024-04-04 오후 9:24:07	2024-04-04 오후 9:26:48	7,
WINDOWS-KB890830-X64-V5.122.E-C71EBB64.pf	2024-04-04 오후 9:25:35	2024-04-04 오후 9:25:35	2h
WINTIMEBROKER.EXE-1AF29976.pf	2024-04-04 오후 9:26:48	2024-04-04 오후 9:26:48	7,
SVCHOST.EXE-1A7CA621.pf	2024-04-04 오후 9:35:32	2024-04-04 오후 9:40:50	7,
<b>MALWARE.EXE-F029871F.pf</b>	2024-04-04 오후 9:36:12	2024-04-04 오후 9:41:04	1,
<b>CALCULATORAPP.EXE-DC489C54.pf</b>	2024-04-04 오후 9:36:19	2024-04-04 오후 9:41:12	1,
IRONTIMEBROKER.EXE-F5999027.pf	2024-04-04 오후 9:36:22	2024-04-04 오후 9:41:15	1
VMWARETOOLSUPGRADER.EXE-84ED7A5.pf	2024-04-04 오후 9:36:57	2024-04-04 오후 9:37:58	3,
SVCHOST.EXE-9E3372D6.pf	2024-04-04 오후 9:37:05	2024-04-04 오후 9:43:09	4,
SETUP64.EXE-6C6157A8.pf	2024-04-04 오후 9:38:07	2024-04-04 오후 9:38:07	4,
VC_REDIST_X86.EXE-8AD91276.pf	2024-04-04 오후 9:38:11	2024-04-04 오후 9:38:11	1,
VCREDIST_X86.EXE-EAF9B711.pf	2024-04-04 오후 9:38:11	2024-04-04 오후 9:38:12	2-

Filename	Full Path	Device Path	Index
SMFT		WVOLUME{01da48e3b775931-a23c...	52
ACTIVATIONSTORE.D...		WVOLUME{01da48e3b775931-a23c...	51
ACTIVATIONSTORE.D...		WVOLUME{01da48e3b775931-a23c...	97
ADVAPI32.DLL		WVOLUME{01da48e3b775931-a23c...	14
APPXDEPLOYMENTC...		WVOLUME{01da48e3b775931-a23c...	83
BCP47LANGS.DLL		WVOLUME{01da48e3b775931-a23c...	48
BCP47MRM.DLL		WVOLUME{01da48e3b775931-a23c...	94
BCRYPT.DLL		WVOLUME{01da48e3b775931-a23c...	18
BCRYPTPRIMITIVES.D...		WVOLUME{01da48e3b775931-a23c...	31
CALCULATORAPP.DLL		WVOLUME{01da48e3b775931-a23c...	0
CALCULATORAPP.EXE		WVOLUME{01da48e3b775931-a23c...	13
CALCULATORAPPLI...		WVOLUME{01da48e3b775931-a23c...	140
CALCULATORCONSO...		WVOLUME{01da48e3b775931-a23c...	134
CALVIEWMODEL.DLL		WVOLUME{01da48e3b775931-a23c...	4
CFGMR32.DLL		WVOLUME{01da48e3b775931-a23c...	85
COMBASE.DLL		WVOLUME{01da48e3b775931-a23c...	23

### 3. WinPrefechView 를 통해 MALWARE.EXE 경로 확인

**Properties**

**Filename:** MALWARE.EXE-F029871F.pf

**Created Time:** 2024-04-04 오후 9:36:12

**Modified Time:** 2024-04-04 오후 9:41:04

**File Size:** 13,779

**Process EXE:** MALWARE.EXE

**Process Path:** f75931-a23c0865\#USERS#VICTIM#MALWARE.EXE

**Run Counter:** 2

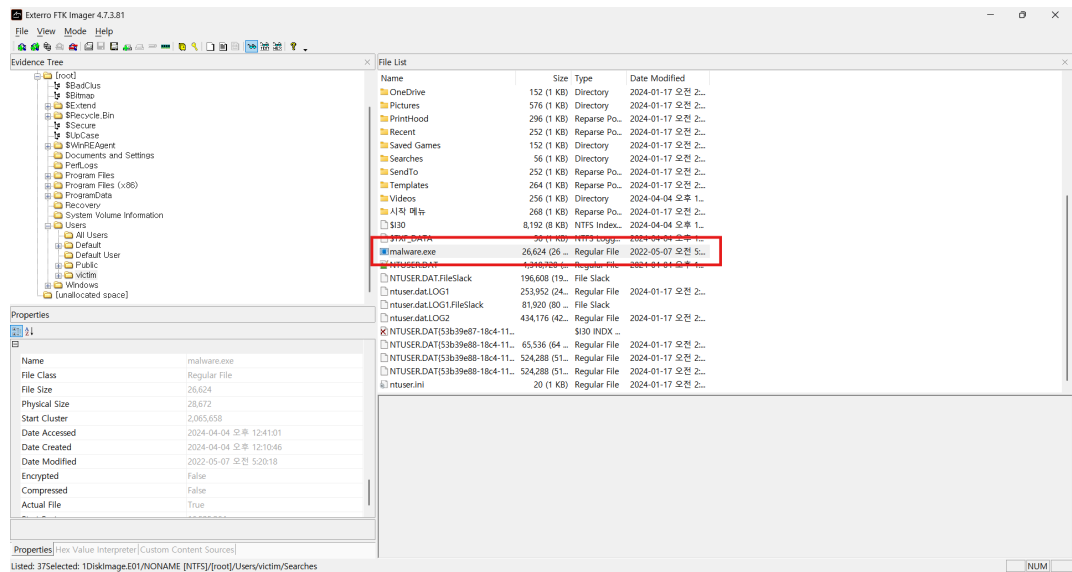
**Last Run Time:** 2024-04-04 오후 9:41:01, 2024-04-04 오후 9:36:09

**Missing Process:** No

OK

### 4. FTK Imager 를 통해 해당 경로에서 해시값 추출

- 경로 : C:\Users\victim\malware.exe



**MD5 = 302021d31f2d0bce01d7afc26bfe2ba2**



**DH{302021d31f2d0bce01d7afc26bfe2ba2}**