

# Write-up: Autoruns (DreamHack Forensics Challenge)

<https://dreamhack.io/wargame/challenges/1323>

---

[1. Challenge Info](#)

[2. Problem Description](#)

[3. Provided Files](#)

[4. Tools Used](#)

[5. Analysis Steps](#)

[5.1 디스크 이미지 마운트](#)

[5.2 레지스트리에서 USB 정보 탐색](#)

[5.3 해시 추출](#)

[5.4 최종 정보 정리](#)

[6. Flag](#)

---

## 1. Challenge Info

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

드림이의 컴퓨터에서 부팅 시 자동으로 실행되는 계산기 프로그램의 원인을 추적하기 위해, 누군가 연결했던 USB 저장장치의 VID, PID, Serial Number를 분석하여 플래그를 완성하라.

플래그 형식: DH{00112233445566778899AABBCCDDEEFF}  
(자동 실행 중인 exe 파일의 MD5 해시값을 플래그로 제출)

---

## 2. Problem Description

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

Windows 레지스트리를 분석해 플래그를 찾아보세요.”

- 제공된 디스크 이미지: `DiskImage.E01`
- 이 파일은 `Find the USB`, `Track_the_file` 문제와 동일

---

## 3. Provided Files

- `DiskImage.E01` (Windows 시스템의 디스크 이미지 파일, E01 포맷)

---

## 4. Tools Used

Tool	Version
FTK Imager	v4.7.8.31
Registry Explorer	v2.1.0
Windows PowerShell	v5.1.26100.4202

## 5. Analysis Steps

### 5.1 디스크 이미지 마운트

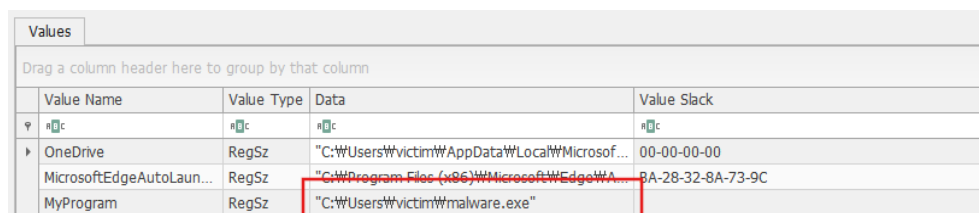
- 도구: FTK Imager
- 제공된 **DiskImage.E01** 파일을 FTK Imager로 열기
- NTUSER.DAT 레지스트리 하이브 파일 추출
  - 경로: **C:\Users\victim\NTUSER.DAT**



Users	SendTo	252 (1 KB)	Reparse Po...	2024-01-17 오전 2:06:28
All Users	Templates	264 (1 KB)	Reparse Po...	2024-01-17 오전 2:06:28
Default	Videos	256 (1 KB)	Directory	2024-04-04 오후 12:03:45
Default User	시작 메뉴	268 (1 KB)	Reparse Po...	2024-01-17 오전 2:06:28
Public	\$I30	8,192 (8 KB)	NTFS Index...	2024-04-04 오후 12:10:46
victim	\$STX DATA	56 (1 KB)	NTFS Logg...	2024-04-04 오후 12:10:46
Windows	malware.exe	26,624 (26 ...)	Regular File	2022-05-07 오전 5:20:18
addins	NTUSER.DAT	1,310,720 (...)	Regular File	2024-04-04 오후 12:39:18
appcompat	NTUSER.DAT.FileSlack	196,608 (19...	File Slack	
appattach				
AppReadiness				

### 5.2 레지스트리에서 USB 정보 탐색

- 도구: Registry Explorer
- 추출한 **NTUSER.DAT** 하이브를 Registry Explorer로 열기
- 경로: **HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run**
- Run 키를 확인해 **C:\Users\victim\malware.exe** 가 부팅할 때 마다 자동 실행되게 설정 되어있는 것을 확인



Value Name	Value Type	Data	Value Slack
OneDrive	RegSz	"C:\Users\victim\AppData\Local\Microsoft...	00-00-00-00
MicrosoftEdgeAutoLaun...	RegSz	"C:\Program Files (x86)\MicrosoftEdgeWA...	BA-28-32-8A-73-9C
MyProgram	RegSz	"C:\Users\victim\malware.exe"	

### 5.3 해시 추출

- 도구: FTK Imager, Windows PowerShell

- 5.2 단계에서 확인한 자동 실행 파일 경로인

`C:\Users\victim\malware.exe` 파일을 FTK Imager를 이용해 추출

Users	SendTo	252 (1 KB)	Reparse Po...	2024-01-17 오전 2:06:28
All Users	Templates	264 (1 KB)	Reparse Po...	2024-01-17 오전 2:06:28
Default	Videos	256 (1 KB)	Directory	2024-04-04 오후 12:03:45
Default User	시작 메뉴	268 (1 KB)	Reparse Po...	2024-01-17 오전 2:06:28
Public	\$I30	8,192 (8 KB)	NTFS Index...	2024-04-04 오후 12:10:46
victim	\$TXF DATA	56 (1 KB)	NTFS Logg...	2024-04-04 오후 12:10:46
Windows	malware.exe	26,624 (26 ...)	Regular File	2022-05-07 오전 5:20:18
addins				
appcompat				

- 추출한 `malware.exe` 에 대해 PowerShell에서 MD5 해시 확인
- 명령어:

```
CertUtil -hashfile malware.exe MD5
```

- `malware.exe`의 MD5 해시: `302021d31f2d0bce01d7afc26bfe2ba2`

```
PS C:\Users\subak\OneDrive\Desktop\DreamHack_forensics\week1\autoruns> CertUtil -hashfile malware.exe MD5
MD5의 malware.exe 해시 :
302021d31f2d0bce01d7afc26bfe2ba2
CertUtil: -hashfile 명령이 성공적으로 완료되었습니다.
```

## 5.4 최종 정보 정리

- MD5 해시: `302021d31f2d0bce01d7afc26bfe2ba2`

## 6. Flag

DH{302021d31f2d0bce01d7afc26bfe2ba2}

축하합니다!

**1 LEVEL 1 Autoruns**  
문제를 해결했습니다.

대단해요. 문제를 어떻게 해결하셨나요?  
풀이를 작성하면 포인트까지 받을 수 있어요.

괜찮아요

 풀이 작성하기