Forensic Study - 7 Windows Prefetch Analysis

2017.11.29

KUICS

2014210009 주어진

목차

- 1. Pre/Superfetch
- 2. Practice With Tool WinPrefetchView

In chapter 5

Prefetch (Superfetch) 확인 (C:\Windows\Prefetch)

이름	수정한 날짜	유형	크기
ReadyBoot	2017-11-07 오전	파일 폴더	
	2017-11-07 오후	PF 파일	15KB
AGENTCONTROLLER.EXE-5B7DAAA0	2017-11-07 오후	PF파일	7KB
AGENTCONTROLLER.EXE-BAAEFDE1.pf	2017-11-07 오후	PF 파일	7KB
APPLICATIONFRAMEHOST.EXE-0CDE	2017-11-07 오후	PF 파일	16KB
ARP.EXE-6FB78BBE.pf	2017-11-07 오후	PF파일	5KB
ASC.EXE-6403B980.pf	2017-11-07 오후	PF 파일	33KB
ASCDOWNLOAD.EXE-D98A1F98.pf	2017-11-07 오후	PF 파일	10KB
ASCINIT.EXE-0C7A50C4.pf	2017-11-07 오후	PF파일	13KB
ASCTRAY.EXE-7EA6B2F8.pf	2017-11-07 오후	PF 파일	16KB
ASCUPGRADE.EXE-1AA42200.pf	2017-11-07 오후	PF 파일	7KB
ASPNET_REGIIS.EXE-8EBA907A.pf	2017-11-07 오전	PF 파일	9KB
ASPNET_REGIIS.EXE-44BD8A08.pf	2017-11-07 오전	PF 파일	10KB
AUDIODG.EXE-856E5CA0.pf	2017-11-07 오후	PF 파일	9KB
AUPDATE.EXE-5C9333A1.pf	2017-11-07 오후	PF 파일	7KB
AUTOCARE.EXE-696A81A1.pf	2017-11-07 오후	PF 파일	14KB
AUTONTS.EXE-57186174.pf	2017-11-07 오후	PF 파일	16KB
AUTOSWEEP.EXE-FA7AD906.pf	2017-11-07 오후	PF 파일	12KB
AUTOUPDATE.EXE-45BE2B19.pf	2017-11-07 오후	PF파일	15KB
AUTOUPDATE.EXE-50B2B93A.pf	2017-11-07 오후	PF 파일	18KB
AWESOMIUM_PROCESS.EXE-B6F35E	2017-11-07 오후	PF 파일	11KB
BACKGROUNDTASKHOST.EXE-01D5	2017-11-07 오전	PF 파일	21KB
BACKGROUNDTASKHOST.EXE-5EC9A	2017-11-07 오후	PF 파일	21KB

Pre/Superfetch

Pre = 미리, Fetch = 가져오다.

Windows Cache중 하나로, 디스크 속도를 향상시키기 위해 나온 기술.

HDD에서는 어느정도의 효과를 보고 있지만, SSD의 경우 오히려 수명을 갉아먹는 기능이라 꺼두는 것이 일반적이나, 이번 시간에는 켜둡시다.

확장자는 .pf이다.

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters에서

EnablePrefetch (REG DWORD) 값에 따라 어떤 항목이 프리패치되는지 정해진다.

0 = Disable

1 = Application

2 = Boot

3 = 1+2

Pre/Superfetch

그럼 어떠한 정보들이 중요한가..?

- 실행 파일 이름
- 실행 파일의 실행 횟수
- 실행 파일의 마지막 실행 시간
- 프리패치 파일의 생성 시간(최초 실행 시간)
- 실행된 볼륨의 정보
- 실행파일 실행 시 참조하는 파일의 목록

등이 중요하다.

그리고 Prefetch파일은 128개가 넘어가면 가장 오래된 파일부터 삭제된다.

NirSoft - WinPrefetchView를 다운로드 합시다.

http://www.nirsoft.net/utils/win_prefetch_view.html

allowed to freely distribute this utility via floppy disk, CD-ROM, Internet, or in any other way, as long as you don't charge anything for this. If you cation!

warranty, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. To see the loss of data or any other reason.

ient, or you found a bug in my utility, you can send a message to nirsofer@yahoo.com

Download WinPrefetchView (32-bit)

Download WinPrefetchView (64-bit)

nguages. In order to change the language of WinPrefetchView, download the appropriate language zip file, extract the 'winprefetchview_lng.ini', ar

Ву	Date	Version
	17/01/2015	1.25
	15/05/2015	WinPrefetchView v1.30
	16/01/2016	1.35
	07/09/2010	1.10
al.de	13/01/2016	1,35
	02/10/0012	1 15

혹시 SysMain (Superfetch) 가 켜져 있는지 확인하고, C:₩Windows₩Prefetch에서 Readyboot와 락이 걸린 파일을 제 외하고 전부 지워준 다음 재부팅합시다. (로그의 양을 줄이기 위해서)

Smart Card	컴퓨터에서 스마트 카드를 액세스할 수 있			사용 안 함	Local Service
🖳 Smart Card Device Enumer	지정한 세션에 액세스할 수 있는 모든 스마			수동(트리	Local System
Smart Card Removal Policy	스마트 카드 제거 시 사용자 데스크톱을 잠			사용 안 함	Local System
SNMP Trap	로컬 또는 원격 SNMP(Simple Network M			사용 안 함	Local Service
🕵 Software Protection	Windows 및 Windows 응용 프로그램의 디			자동(지연	Network Service
Spot Verifier	잠재적인 파일 시스템 손상을 검증합니다.			수동(트리	Local System
SSDP Discovery	UPnP 장치와 같이 SSDP 검색 프로토콜을	실행 중	5	수동	Local Service
State Repository Service	응용 프로그램 모델에 대한 필수 인프라 지	실행 경	\$	수동	Local System
Steam Client Service	Steam Client Service monitors and update			수동	Local System
Still Image Acquisition Eve	정지 이미지 인식 이벤트와 연결된 응용 프			수동	Local System
Storage Service	저장 공간 설정 및 외부 저장 공간 확장에	실행 중	중	수동(트리	Local System
Storage Tiers Management	시스템에 있는 모든 계층화된 저장소 공간			수동	Local System
SynTPEnh Caller Service		실행 경	\$	자동	Local System
SysMain	지속적으로 시스템 성능을 유지하고 향상시킵	니다.	Š	자동	Local System
💫 System Event Notification	시스템 이벤트를 모니터링하고 구독자를	실행 경	중	자동	Local System
🕵 System Events Broker	WinRT 응용 프로그램의 백그라운드 작업	실행 경	Š	자동(트리	Local System
Task Scheduler	사용자가 컴퓨터에서 자동화된 작업을 구	실행 경	8	자동	Local System
TCP/IP NetBIOS Helper	NetBIOS over TCP/IP(NetBT) 서비스 및 Ne	실행 경	<u> </u>	수동(트리	Local Service
Te.Service				수동	Local System
TeamViewer 12	TeamViewer Remote Software	실행 중	\$	자동	Local System
Telephony	로컬 컴퓨터에서 그리고 LAN을 통해 서비	실행 중	\$	수동	Network Service
Themes	사용자 경험 테마 관리를 제공합니다.	실행 경	\$	자동	Local System
Tile Data model server	타일 업데이트를 위한 타일 서버입니다.	실행 경	중	수동	Local System
10%	00	1100	#		

Full Path

1. 일단 켜봅시다.

Filename

Created Time	Modified Time	File Size	Process EXE	Process Path	Run 🗸	Last Run Time
2017-11-29 오	2017-11-29 오	3,183	AM_DELTA_PATC	C:\Windows\SOFTWAREDISTRIBUTION\	1	2017-11-29 오후 2:37:30
2017-11-29 오	2017-11-29 오	13,844	APPLICATIONFRA	C:\Windows\System32\APPLICATIONFR	1	2017-11-29 오후 2:36:08
2017-11-29 오	2017-11-29 오	15,651	AUTOUPDATE.EXE	C:\PROGRAM FILES (X86)\lobit\DRIVER	1	2017-11-29 오후 2:38:23
2017-11-29 오	2017-11-29 오	9,342	BACKGROUNDTA	C:\Windows\System32\BACKGROUNDT	1	2017-11-29 오후 2:39:02
2017-11-29 오	2017-11-29 오	13,448	BANDIZIP.EXE	C:\PROGRAM FILES\Bandizip\Bandizip.e	1	2017-11-29 오후 2:35:04
2017-11-29 오	2017-11-29 오	4,267	BSSACTSTATECHE	C:\PROGRAM FILES\BITVISE SSH SERVE	1	2017-11-29 오후 2:34:48
2017-11-29 오	2017-11-29 오	6,638	CCLEANER64.EXE	C:\PROGRAM FILES\Cleaner\CLEANE	1	2017-11-29 오후 2:34:44
2017-11-29 오	2017-11-29 오	25,427	CONSENT.EXE	C:\Windows\System32\consent.exe	1	2017-11-29 오후 2:35:09
2017-11-29 오	2017-11-29 오	2,684	CTFMON.EXE	C:\Windows\System32\ctfmon.exe	1	2017-11-29 오후 2:33:19
2017-11-29 오	2017-11-29 오	6,500	DLLHOST.EXE	C:\Windows\System32\dlhost.exe	1	2017-11-29 오후 2:38:56
2017-11-29 오	2017-11-29 오	5,484	DLLHOST.EXE	C:\Windows\System32\dlhost.exe	1	2017-11-29 오후 2:36:21
2017-11-29 오	2017-11-29 오	5,082	DLLHOST.EXE	C:\Windows\System32\dllhost.exe	1	2017-11-29 오후 2:35:09
2017-11-29 오	2017-11-29 오	3,942	DLLHOST.EXE	C:\Windows\System32\dllhost.exe	1	2017-11-29 오후 2:38:56
2017-11-29 오	2017-11-29 오	21,604	DRIVERBOOSTER	C:#PROGRAM FILES (X86)#IObit#DRIVER	1	2017-11-29 오후 2:39:23
2017-11-29 오	2017-11-29 오	26,202	DSATRAY.EXE	C:\PROGRAM FILES (X86)\INTEL DRIVER	1	2017-11-29 오후 2:34:47
2017-11-29 오	2017-11-29 오	32,309	GOOGLEDRIVESY	C:\PROGRAM FILES (X86)\Google\Drive	1	2017-11-29 오후 2:34:52
2017-11-29 오	2017-11-29 오	4,789	JUSCHED.EXE	C:\PROGRAM FILES (X86)\COMMON FIL	1	2017-11-29 오후 2:34:48
2017-11-29 오	2017-11-29 오	17,104	KAKAOTALK.EXE	C:\PROGRAM FILES (X86)\Kakao\KAKA	1	2017-11-29 오후 2:34:46
2017-11-29 오	2017-11-29 오	15,929	LOGONUI.EXE	C:\Windows\System32\LogonUl.exe	1	2017-11-29 오후 2:33:18
2017-11-29 오	2017-11-29 모	17,518	MPSIGSTUB.EXE	C:\Windows\System32\MPSIGSTUB.EXE	1	2017-11-29 오후 2:37:30
	2017-11-29 Q	2017-11-29 \$ 2017-11-29 \$\text{ 2017-11-29 \$\text{ 2017-11-29 \$\text{	2017-11-29 Q 2017-11-29 Q 3,183 2017-11-29 Q 2017-11-29 Q 13,844 2017-11-29 Q 2017-11-29 Q 15,651 2017-11-29 Q 2017-11-29 Q 9,342 2017-11-29 Q 2017-11-29 Q 13,448 2017-11-29 Q 2017-11-29 Q 4,267 2017-11-29 Q 2017-11-29 Q 6,638 2017-11-29 Q 2017-11-29 Q 25,427 2017-11-29 Q 2017-11-29 Q 2,684 2017-11-29 Q 2017-11-29 Q 5,080 2017-11-29 Q 2017-11-29 Q 5,082 2017-11-29 Q 2017-11-29 Q 3,942 2017-11-29 Q 2017-11-29 Q 21,604 2017-11-29 Q 2017-11-29 Q 26,202 2017-11-29 Q 2017-11-29 Q 32,309 2017-11-29 Q 2017-11-29 Q 4,789 2017-11-29 Q 2017-11-29 Q 17,104 2017-11-29 Q 2017-11-29 Q 15,929	2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 3,183 AM_DELTA_PATC 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 13,844 APPLICATIONFRA 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 15,651 AUTOUPDATE.EXE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 9,342 BACKGROUNDTA 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 13,448 BANDIZIP.EXE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 4,267 BSSACTSTATECHE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 6,638 CCLEANER64.EXE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 25,427 CONSENT.EXE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 26,684 CTFMON.EXE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 6,500 DLLHOST.EXE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 5,484 DLLHOST.EXE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 3,942 DLLHOST.EXE 2017-11-29 \$\omega\$ 2017-11-29 \$\omega\$ 26,202 DSATRAY.EXE 2017-11-29 \$\omega\$	2017-11-29 Q	2017-11-29 Q. 2017-11-29 Q. 13,844 APPLICATIONFRA. C:\(\pi\)Windows\(\pi\)System32\(\pi\)APPLICATIONFR. 1 2017-11-29 Q. 2017-11-29 Q. 15,651 AUTOUPDATE.EXE C:\(\pi\)PROGRAM FILES (X86)\(\pi\)IObit\(\pi\)DRT 1 2017-11-29 Q. 2017-11-29 Q. 9,342 BACKGROUNDTA C:\(\pi\)Windows\(\pi\)System32\(\pi\)BACKGROUNDT 1 2017-11-29 Q. 2017-11-29 Q. 13,448 BANDIZIP.EXE C:\(\pi\)PROGRAM FILES\(\pi\)Bandizip\(\pi\)Ba

Device Path

Index

♦ BANDIZIP.EXE-2D520... 2017-11-29 오... 2017-11-29 오... 13,448

2. 어떤 압축 파일이든 좋으니 압축해제하고 압축 프로그램의 pf를 살펴봅시다.

	2017-11-29 오	2017-11-29 오	4,267	BSSACTSTATECHE	C:\PROGRAM FILES\BITVISE SSH SERVE	1	2017-11-29 오후
CCLEANER64,EXE-DE	2017-11-29 오	2017-11-29 오	6,638	CCLEANER64.EXE	C:\PROGRAM FILES\Cleaner\CLEANE	1	2017-11-29 오후
CONSENT.EXE-1A8D	2017-11-29 오	2017-11-29 오	25,427	CONSENT.EXE	C:\Windows\System32\consent.exe	1	2017-11-29 오후
CTFMON.EXE-437D7	2017-11-29 오	2017-11-29 오	2,684	CTFMON.EXE	C:\Windows\System32\ctfmon.exe	1	2017-11-29 오후
◆ DSATRAY.EXE-B1ACC ◆	2017-11-29 오	2017-11-29 오	26,202	DSATRAY.EXE	C:\PROGRAM FILES (X86)\Intel DRIVER	1	2017-11-29 오후
O GOOGLEDRIVESYNC	2017-11-29 오	2017-11-29 오	32,309	GOOGLEDRIVESY	C:\PROGRAM FILES (X86)\Google\Drive	1	2017-11-29 오후
JUSCHED.EXE-C04F5	2017-11-29 오	2017-11-29 오	4,789	JUSCHED.EXE	C:\PROGRAM FILES (X86)\COMMON FIL	1	2017-11-29 오후
KAKAOTALK.EXE-A97	2017-11-29 오	2017-11-29 오	17,104	KAKAOTALK.EXE	C:\PROGRAM FILES (X86)\Kakao\KAKA	1	2017-11-29 오후
IOGONUI.EXE-D0853	2017-11-29 오	2017-11-29 오	15,929	LOGONUI.EXE	C:\Windows\System32\LogonUI.exe	1	2017-11-29 오후
NVCONTAINER.EXE-F	2017-11-29 오	2017-11-29 오	3,567	NVCONTAINER.EXE	C:\PROGRAM FILES (X86)\NVIDIA CORP	2	2017-11-29 오후
NIVIDIA SHARE EXE-2	2017-11-29 ♀	2017-11-29 ♀	5.650	NIVIDIA SHARE EXE	C:\PROGRAM FILES (X86)\NVIDIA CORP	1	2017-11-29 오호
Filename 🕜	Full Path				Device Path		Index
VERSION.DLL	C:\Windows\Syste	em32₩version.dll			₩VOLUME{01d0025	43e021ff8-383	e 29
VERSIONNO.INI	C:₩PROGRAM FILE	S\Bandizip\VERSIO	INI.ONN		₩VOLUME{01d0025	43e021ff8-383r	e 40
WIN.INI	C:₩Windows₩win.i	ini			#VOLUME{01d0025	43e021ff8-383	e 67
WIN32U.DLL	C:₩Windows₩Syste	em32₩win32u.dll			₩VOLUME{01d0025	43e021ff8-383	e 6
WINDOWS.STORAGE	C:₩Windows₩Syste	em32\WINDOWS.S1	TORAGE.DLL		₩VOLUME{01d0025	43e021ff8-383	e 21
WINDOWSSHELL.MA	C:\Windows\WINI	DOWSSHELL.MANIF	EST		₩VOLUME{01d0025	43e021ff8-383	e 35
	C:\Windows\Syste	em32\winhttp.dll			₩VOLUME{01d0025	43e021ff8-383	e 51
WININET.DLL	C:\Windows\Syste	em32\wininet.dll			₩VOLUME{01d0025	43e021ff8-383	e 32
WINNSI.DLL	C:\Windows\Syste	em32₩winnsi.dll			₩VOLUME{01d0025	43e021ff8-383	e 54
WINPREFETCHVIEW	C:₩Users₩akwke₩I	DOWNLOADS#WINF	PREFETCHVIEW-X64.	ZIP	₩VOLUME{01d0025	43e021ff8-383	e 78
WINPREFETCHVIEW.C	C:₩Users₩akwke₩I	DOWNLOADS#WINE	REFETCHVIEW-X64	WINPREFETCHVIEW.C	HM #VOLUME(01d0025	43e021ff8-383	e 82
WINPREFETCHVIEW,E	C:₩Users₩akwke₩[DOWNLOADS#WINE	REFETCHVIEW-X64	WINPREFETCHVIEW.E	XE #VOLUME{01d0025	43e021ff8-383	e 81
E9		m					15212

BANDIZIP.EXE

C:\PROGRAM FILES\Bandizip\Bandizip.e.. 1

SYSMAIN.SDB

3. 그림판에서 아무 사진이나 열어봅시다. 문서 뷰어도 좋습니다.

MSPAINT.EXE-3E523 2017-11-29 2	2017-11-29 ¥	18,418	MSPAINT.EXE	C:#vvindows#System32#mspaint.exe	2	-	
■ MPSIGSTUB.EXE-3DA 2017-11-29 ♀	2017-11-29 오	17,518	MPSIGSTUB.EXE	C:\Windows\System32\MPSIGSTUB.EXE	1		
III MICROSOFT.PHOTOS 2017-11-29 ♀	2017-11-29 오	53,201	MICROSOFT.PHO	C:\PROGRAM FILES\UNDOWSAPPS\UNDOWSAPPS\UNDOWSAPPS	2	-	
III LOGONUI.EXE-D0853 2017-11-29 ♀	2017-11-29 오	15,929	LOGONULEXE	C:\Windows\System32\LogonUI.exe	1		
KAKAOTALK.EXE-A97 2017-11-29 Ω	2017-11-29 오	17,104	KAKAOTALK.EXE	C:\PROGRAM FILES (X86)\Kakao\KAKA	1	10	
ILISCHED FXE-C04F5 2017-11-29 9	2017-11-29 ♀	4 789	JUSCHED EXE	C:#PROGRAM FILES (X86)#COMMON FIL	1		
Filename	Full Path	2					
CVERSIONS.2.DB	C:₩PROC	RAMDATA#N	IICROSOFT₩Windows₩Cache	es#CVERSIONS.2.DB			
(6AF0698E-D558-4F6E-9B3C-3716689	AF493}.2.V C:₩PROC	RAMDATA#M	IICROSOFT#Windows#Cache	es\{6AF0698E-D558-4F6E-9B3C-3716689AF4	93}.2.VER0	X0000	
(DDF571F2-BE98-426D-8288-1A9A39	03FDA2}.2 C:₩PRO€	RAMDATA#N	IICROSOFT#Windows#Cache	es\{DDF571F2-BE98-426D-8288-1A9A39C3F	DA2}.2.VER	0X000	
CVERSIONS.1.DB	C:₩Users	₩akwke₩AppE	Data\Local\MICROSOFT\Wi	indows\Caches\CVERSIONS.1.DB			
(AFBF9F1A-8EE8-4C77-AF34-C647E37	CA0D9}.1.V C:\Users	₩akwke₩AppE	Data\Local\MICROSOFT\Wi	indows\Caches\AFBF9F1A-8EE8-4C77-AF34	-C647E37C	A0D9	
DESKTOP.INI	C:₩Users	₩akwke₩Desk	top\desktop.ini				
□ DESKTOP.INI	C:\Users	₩akwke₩DOC	UMENTS#desktop.ini				
DESKTOP.INI	C:₩Users	₩akwke₩Musi	c₩desktop.ini				
454D1A8A841A54CE9CCAD93720262	1454.JPG C:\Users	₩akwke₩Pictu	res\454D1A8A841A54CE9C	CAD937202621454JPG			
DESKTOP.INI	C:₩Users	₩akwke₩Pictu	res#desktop.ini				
□ DESKTOP.INI	C:₩Users	₩desktop.ini					
TTS.							

C:\Windows\apppatch\sysmain.sdb

C-MWindowsWSvetom22Wmenaint ava

2017-11-29 오 2017-11-29 오 24 585

4. USB나 스마트폰을 마운트하여 엑세스해봅시다.

SETUPHOST EXE-AD629B1A of

- SCIOFFIGST.EXE ADUZSUTA.PI	2017-11-23	2017-11-23	24,303	SETURITOST.EXE	C.W. WINDOWS DI WSOULCESWSETOFFIO	Simo 1	2017-11-25 2.33.31		
SKYPE,EXE-270BF55E.pf	2017-11-29 오	2017-11-29 오	16,611	SKYPE.EXE	C:\PROGRAM FILES (X86)\Skype\Phone	e 4	2017-11-29 오후 2:44:32, 2017-11-2		
SMARTSCREEN.EXE-89A7B40A.df	2017-11-29 오	2017-11-29 오	7.675	SMARTSCREEN.EX	XE C:#Windows#Svstem32#SMARTSCREEN	1	2017-11-29 오후 2:51:29		
Filename	Į.	Full Path		Dr	evice Path /				
■ WINHTTP.DLL C:#Windows#System32#winhttp.dll +				₩/v	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#WINHTTP.DLL				
■ WINTRUST.DLL		C:\Windows\System	m32#wintrust.dll	₩	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#WINTRUST.DLL				
		C:\Windows\System	.m32\wkscli.dll	₩V	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#WKSCLI.DLL				
		C:\Windows\System	.m32\wmsgapi.dll	₩v	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#WMSGAPI.DLL				
	DLL C:\Windows\System32\ws2_32.dll			₩z	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#WS2_32.DLL				
		C:\Windows\System	m32#wtsapi32.dll	₩	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#WTSAPI32.DLL				
		C:\Windows\System	m32wmllite.dll	₩٧	VOLUME{01d002543e021ff8-383e9e4a}\WVIN	DOWS#SYST	rem32\xxmllite.dll		
WINDOWSSHELL:MANIFEST		C:#Windows#WIND	DOWSSHELL.MANIFE	EST #\	VOLUME(01d002543e021ff8-383e9e4a)#WIN	DOWS#WIND	DOWSSHELL.MANIFEST		
○ COMCTL32.DLL ○ CO		C:\Windows\WinS	SxS\AMD64_MICROS	SOFT.WINDO #\	VOLUME(01d002543e021ff8-383e9e4a)\WVIN	DOWS#WINS	SXS#AMD64_MICROSOFT.WINDOWS.COM		
T≣ \$MFT				#	VOLUME{01d31b1fdc14dcbb-cedcd368}#\$MF	Ţ			
TT BCD				₩	#VOLUME(01d31b1fdc14dcbb-cedcd368)#BOOT#BCD				
™ BOOT.SDI				#	#VOLUME[01d31b1fdc14dcbb-cedcd368]#BOOT#BOOT.SDI				
BOOTFIX BIN				#	#VOLUME(01d31b1fdc14dcbb-cedcd368)#BOOT#BOOTFIX.BIN				
TE BOOTSECT.EXE				₩	#VOLUME(01d31b1fdc14dcbb-cedcd368)#BOOT#BOOTSECT.EXE				
PER ETECDOOT COM				100	WAYOU UNDOOR 403 his fals a Adabh Andreas BOSWIDOOT WETTERDOOT COM				

C:\\$\\$WINDOWS ~BT\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$\\$1

Practice With Tool! (Advanced)

5. 모든 프로그램을 실행할 때 꼭 NTDLL.DLL이 먼저 로드될까요?

NTDLL.DLL	C:\Windows\System32\ntdll.dll	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#NTDLLE
WUDFHOST.EXE	C:\Windows\System32\WUDFHost.exe	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#WUDFH
KERNEL32.DLL	C:\Windows\System32\kernel32.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#KERNEL:
KERNELBASE.DLL	C:\Windows\System32\KERNELBASE.DLL	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#KERNELI
LOCALE.NLS	C:\Windows\System32\locale.nls	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#LOCALE
RPCRT4.DLL	C:\Windows\System32\rpcrt4.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#RPCRT4
COMBASE.DLL	C:\#Windows\#System32\#combase.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#COMBA
UCRTBASE.DLL	C:\Windows\System32\ucrtbase.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#UCRTBA
BCRYPTPRIMITIVES.DLL	C:\Windows\System32\BCRYPTPRIMITIVES.DLL	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#BCRYPT
SECHOST,DLL	C:\#Windows\#System32\#sechost.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#SECHOS
\$MFT	C:\Windows\System32\sechost.dll	#VOLUME{01d002543e021ff8-383e9e4a}#\$MFT
DEVOBJ.DLL	C:\#Windows\#System32\#devobj.dll	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#DEVOBJ
CFGMGR32.DLL	C:\Windows\System32\cfgmqr32.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#CFGMGI
WUDFPLATFORM.DLL	C:\Windows\System32\WUDFPLATFORM.DLL	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#WUDFPI
ADVAPI32.DLL	C:#Windows#System32#advapi32.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#ADVAPI
MSVCRT.DLL	C:\Windows\System32\msvcrt.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#MSVCR
SSPICLI.DLL	C:\Windows\System32\sspicli.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#SSPICLI.
RPCSS.DLL	C:\Windows\System32\rpcss.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#RPCSS.E
KERNEL.APPCORE.DLL	C:\#Windows\#System32\#KERNEL.APPCORE.DLL	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#KERNEL.
WPDFS.DLL	C:#Windows#System32#DRIVERSTORE#FILEREPOSITORY#WPDFS.INF_AMD64_86B7	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#DRIVERS
USER32.DLL	C:#Windows#System32#user32.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#USER32
WIN32U.DLL	C:\Windows\System32\win32u.dll	#VOLUME{01d002543e021ff8-383e9e4a}#WINDOWS#SYSTEM32#WIN32L
GDI32.DLL	C:#Windows#System32#gdi32.dll	#VOLUME(01d002543e021ff8-383e9e4a)#WINDOWS#SYSTEM32#GDI32.D

Practice With Tool! (Advanced)

5. 모든 프로그램을 실행할 때 꼭 NTDLL.DLL이 먼저 로드될까요?

아닐수도 있습니다만 일반적으로는 NTDLL.DLL이 먼저 로드됩니다. 이를 제대로 알기 위해선 LDR를 참조하면 됩니다. (2주차 스터디에서 언급)

Practice With Tool! (Advanced)

6. NTOSBOOT-BOODFAAD.PF가 존재하지 않는 경우도 있고, 존재하는 경우도 있는데

이는 시스템 부트 프리패치이다.

로드 순서: \$MFT -> CDROM -> NULL, BEEF -> VGA -> ...

감사합니다

과제: 없습니다.

원래 이번주에 VM과 실습하려 했으나, 다음주로 미루게 됐습니다. (5주차와 관련된 실습을 7주차에 하게 됐습니다.)