Forensic Study - 7
Windows Prefetch Analysis

2017.11.29

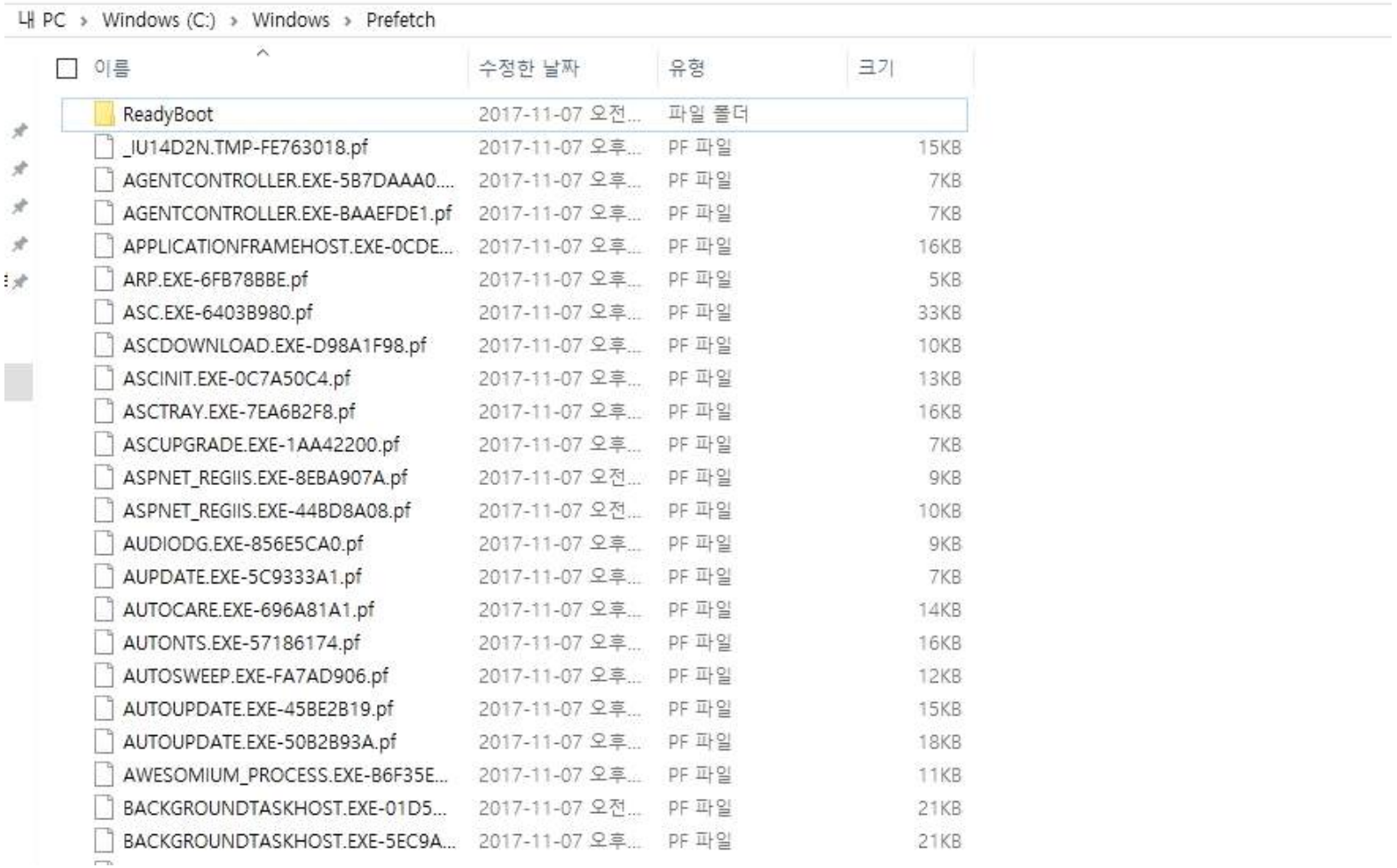
KUICS

2014210009 주어진

목차

In chapter 5

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



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.

Practice With Tool!

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 c
cation !

warranty, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. T
s due to 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)

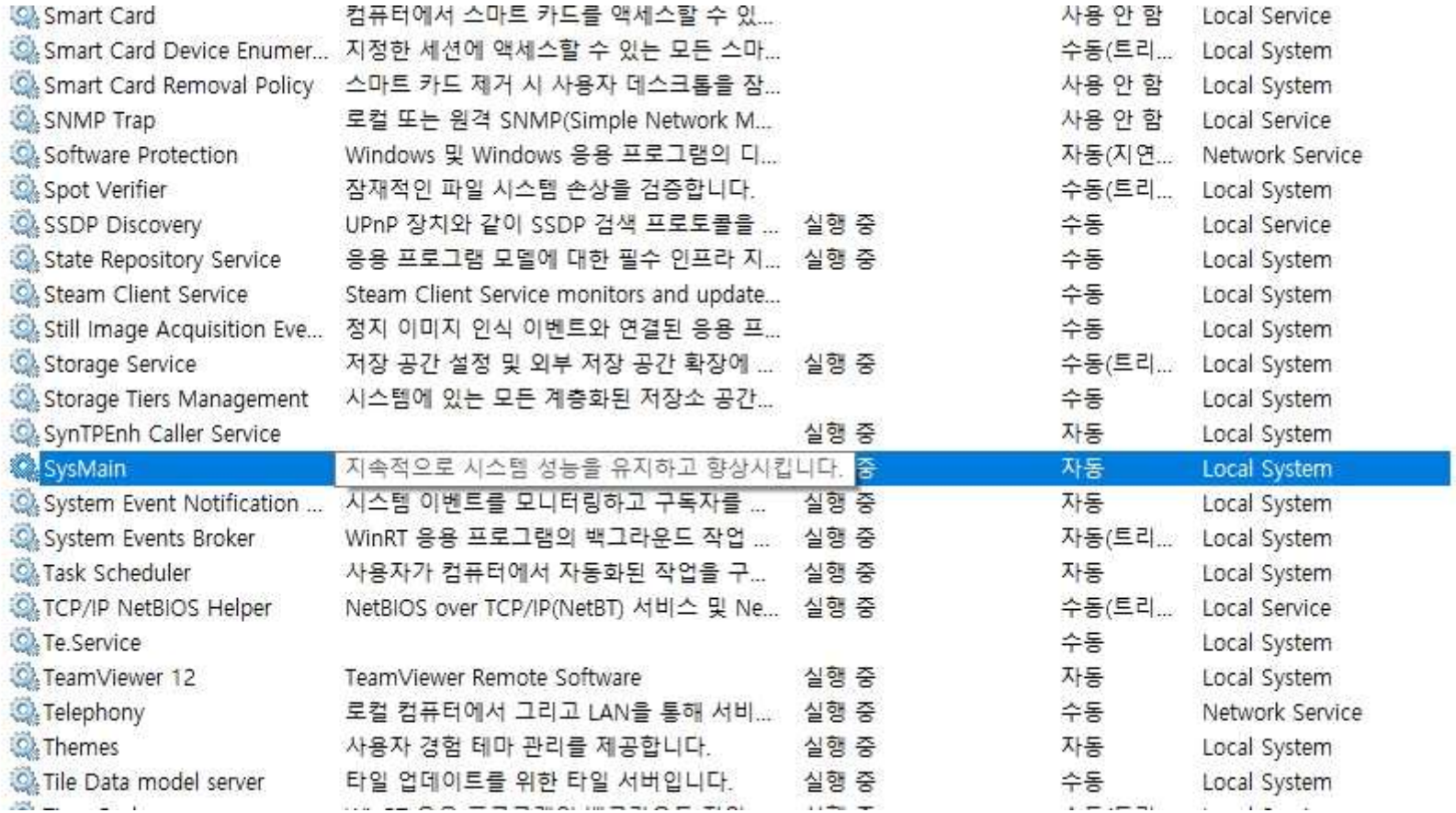
Download WinPrefetchView (64-bit)

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

By	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
	23/12/2013	1.15

Practice With Tool!

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



Practice With Tool!

1. 일단 켜봅시다.

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run ...	Last Run Time
AM_DELTA_PATCH_1.257.1086.0.E-3388D410.pf	2017-11-29 오...	2017-11-29 오...	3,183	AM_DELTA_PATC...	C:₩Windows₩SOFTWAREDISTRIBUTION₩...	1	2017-11-29 오후 2:37:30
APPLICATIONFRAMEHOST.EXE-0CDEF718.pf	2017-11-29 오...	2017-11-29 오...	13,844	APPLICATIONFRA...	C:₩Windows₩System32₩APPLICATIONFR...	1	2017-11-29 오후 2:36:08
AUTOUPDATE.EXE-50B2B93A.pf	2017-11-29 오...	2017-11-29 오...	15,651	AUTOUPDATE.EXE	C:₩PROGRAM FILES (X86)₩IObit₩DRIVER...	1	2017-11-29 오후 2:38:23
BACKGROUNDTASKHOST.EXE-5EC9A5AE.pf	2017-11-29 오...	2017-11-29 오...	9,342	BACKGROUNDTA...	C:₩Windows₩System32₩BACKGROUNDT...	1	2017-11-29 오후 2:39:02
BANDIZIP.EXE-2D520967.pf	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
BSSACTSTATECHECK.EXE-A20A8F27.pf	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
CCLEANER64.EXE-DE05DBE1.pf	2017-11-29 오...	2017-11-29 오...	6,638	CCLEANER64.EXE	C:₩PROGRAM FILES₩CCleaner₩CCLEANE...	1	2017-11-29 오후 2:34:44
CONSENT.EXE-1A8D0661.pf	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
CTFMON.EXE-437D7ABA.pf	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
DLLHOST.EXE-22097AD6.pf	2017-11-29 오...	2017-11-29 오...	6,500	DLLHOST.EXE	C:₩Windows₩System32₩dllhost.exe	1	2017-11-29 오후 2:38:56
DLLHOST.EXE-5063609C.pf	2017-11-29 오...	2017-11-29 오...	5,484	DLLHOST.EXE	C:₩Windows₩System32₩dllhost.exe	1	2017-11-29 오후 2:36:21
DLLHOST.EXE-D247D88D.pf	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
DLLHOST.EXE-F5F979B5.pf	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
DRIVERBOOSTER.EXE-75608A78.pf	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
DSATRAY.EXE-B1ACCCEA.pf	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
GOOGLEDRIVESYNC.EXE-726502CB.pf	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
JUSCHED.EXE-C04F5CE5.pf	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
KAKAOTALK.EXE-A9728D75.pf	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
LOGONUI.EXE-D0853078.pf	2017-11-29 오...	2017-11-29 오...	15,929	LOGONUI.EXE	C:₩Windows₩System32₩LogonUI.exe	1	2017-11-29 오후 2:33:18
MPSIGSTUB.EXE-3DA7FE0D.pf	2017-11-29 오...	2017-11-29 오...	17,518	MPSIGSTUB.EXE	C:₩Windows₩System32₩MPSIGSTUB.EXE	1	2017-11-29 오후 2:37:30

Filename	Full Path	Device Path	Index

Practice With Tool!

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

BANDIZIP.EXE-2D520...	2017-11-29 오...	2017-11-29 오...	13,448	BANDIZIP.EXE	C:₩PROGRAM FILES₩Bandizip₩Bandizip.e...	1	2017-11-29 오후
BSSACTSTATECHECK....	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₩CCleaner₩CCLEANE...	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
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
LOGONUI.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
NVIDIA SHARE.EXE-2...	2017-11-29 오...	2017-11-29 오...	5,650	NVIDIA SHARE.EXE	C:₩PROGRAM FILES (X86)₩NVIDIA CORP...	1	2017-11-29 오후

Filename	Full Path	Device Path	Index
VERSION.DLL	C:₩Windows₩System32₩version.dll	₩VOLUME{01d002543e021ff8-383e...	29
VERSIONNO.INI	C:₩PROGRAM FILES₩Bandizip₩VERSIONNO.INI	₩VOLUME{01d002543e021ff8-383e...	40
WIN.INI	C:₩Windows₩win.ini	₩VOLUME{01d002543e021ff8-383e...	67
WIN32U.DLL	C:₩Windows₩System32₩win32u.dll	₩VOLUME{01d002543e021ff8-383e...	6
WINDOWS.STORAGE....	C:₩Windows₩System32₩WINDOWS.STORAGE.DLL	₩VOLUME{01d002543e021ff8-383e...	21
WINDOWSSHELL.MA...	C:₩Windows₩WINDOWSSHELL.MANIFEST	₩VOLUME{01d002543e021ff8-383e...	35
WINHTTP.DLL	C:₩Windows₩System32₩winhttp.dll	₩VOLUME{01d002543e021ff8-383e...	51
WININET.DLL	C:₩Windows₩System32₩wininet.dll	₩VOLUME{01d002543e021ff8-383e...	32
WINNSI.DLL	C:₩Windows₩System32₩winnsi.dll	₩VOLUME{01d002543e021ff8-383e...	54
WINPREFETCHVIEW-...	C:₩Users₩akwke₩DOWNLOADS₩WINPREFETCHVIEW-X64.ZIP	₩VOLUME{01d002543e021ff8-383e...	78
WINPREFETCHVIEW.C...	C:₩Users₩akwke₩DOWNLOADS₩WINPREFETCHVIEW-X64₩WINPREFETCHVIEW.CHM	₩VOLUME{01d002543e021ff8-383e...	82
WINPREFETCHVIEW.E...	C:₩Users₩akwke₩DOWNLOADS₩WINPREFETCHVIEW-X64₩WINPREFETCHVIEW.EXE	₩VOLUME{01d002543e021ff8-383e...	81

Practice With Tool!

3. 그림판에서 아무 사진이나 열어봅시다. 문서 뷰어도 좋습니다.

MSPAINT.EXE-3E523...	2017-11-29 오...	2017-11-29 오...	18,418	MSPAINT.EXE	C:₩Windows₩System32₩mspaint.exe	2
MPSIGSTUB.EXE-3DA...	2017-11-29 오...	2017-11-29 오...	17,518	MPSIGSTUB.EXE	C:₩Windows₩System32₩MPSIGSTUB.EXE	1
MICROSOFT.PHOTOS...	2017-11-29 오...	2017-11-29 오...	53,201	MICROSOFT.PHO...	C:₩PROGRAM FILES₩WINDOWSAPPS₩MI...	2
LOGONUI.EXE-D0853...	2017-11-29 오...	2017-11-29 오...	15,929	LOGONUI.EXE	C:₩Windows₩System32₩LogonUI.exe	1
KAKAOTALK.EXE-A97...	2017-11-29 오...	2017-11-29 오...	17,104	KAKAOTALK.EXE	C:₩PROGRAM FILES (X86)₩Kakao₩KAKA...	1
IUSCHED.EXE-C04E5...	2017-11-29 오...	2017-11-29 오...	4,789	IUSCHED.EXE	C:₩PROGRAM FILES (X86)₩COMMON FIL...	1

Filename	Full Path
CVERSIONS.2.DB	C:₩PROGRAMDATA₩MICROSOFT₩Windows₩Caches₩CVERSIONS.2.DB
{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.V...	C:₩PROGRAMDATA₩MICROSOFT₩Windows₩Caches₩{6AF0698E-D558-4F6E-9B3C-3716689AF493}.2.VER0X000(
{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2....	C:₩PROGRAMDATA₩MICROSOFT₩Windows₩Caches₩{DDF571F2-BE98-426D-8288-1A9A39C3FDA2}.2.VER0X00(
CVERSIONS.1.DB	C:₩Users₩akwke₩AppData₩Local₩MICROSOFT₩Windows₩Caches₩CVERSIONS.1.DB
{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9}.1.V...	C:₩Users₩akwke₩AppData₩Local₩MICROSOFT₩Windows₩Caches₩{AFBF9F1A-8EE8-4C77-AF34-C647E37CA0D9
DESKTOP.INI	C:₩Users₩akwke₩Desktop₩desktop.ini
DESKTOP.INI	C:₩Users₩akwke₩DOCUMENTS₩desktop.ini
DESKTOP.INI	C:₩Users₩akwke₩Music₩desktop.ini
454D1A8A841A54CE9CCAD937202621454.JPG	C:₩Users₩akwke₩Pictures₩454D1A8A841A54CE9CCAD937202621454.JPG
DESKTOP.INI	C:₩Users₩akwke₩Pictures₩desktop.ini
DESKTOP.INI	C:₩Users₩desktop.ini
SYSMAIN.SDB	C:₩Windows₩apppatch₩sysmain.sdb

Practice With Tool!

4. USB나 스마트폰을 마운트하여 엑세스해봅시다.

SETUPHOST.EXE-AD629B1A.pf	2017-11-29 오...	2017-11-29 오...	24,585	SETUPHOST.EXE	C:₩$WINDOWS.~BT₩Sources₩SETUPHOS...	1	2017-11-29 오후 2:55:31
SKYPE.EXE-270BF55E.pf	2017-11-29 오...	2017-11-29 오...	16,611	SKYPE.EXE	C:₩PROGRAM FILES (X86)₩Skype₩Phone...	4	2017-11-29 오후 2:44:32, 2017-11-2
SMARTSCREEN.EXE-89A7B40A.pf	2017-11-29 오...	2017-11-29 오...	7,675	SMARTSCREEN.EXE	C:₩Windows₩System32₩SMARTSCREEN....	1	2017-11-29 오후 2:51:29

Filename	Full Path	Device Path
WINHTTP.DLL	C:₩Windows₩System32₩winhttp.dll	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩WINHTTP.DLL
WINTRUST.DLL	C:₩Windows₩System32₩wintrust.dll	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩WINTRUST.DLL
WKSCLI.DLL	C:₩Windows₩System32₩wkscli.dll	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩WKSCLI.DLL
WMSGAPI.DLL	C:₩Windows₩System32₩wmsgapi.dll	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩WMSGAPI.DLL
WS2_32.DLL	C:₩Windows₩System32₩ws2_32.dll	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩WS2_32.DLL
WTSAPI32.DLL	C:₩Windows₩System32₩wtsapi32.dll	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩WTSAPI32.DLL
XMLLITE.DLL	C:₩Windows₩System32₩xmllite.dll	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩XMLLITE.DLL
WINDOWSSHELL.MANIFEST	C:₩Windows₩WINDOWSSHELL.MANIFEST	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩WINDOWSSHELL.MANIFEST
COMCTL32.DLL	C:₩Windows₩WinSxS₩AMD64_MICROSOFT.WINDO...	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩WINSXS₩AMD64_MICROSOFT.WINDOWS.COM...
$MFT		₩VOLUME{01d31b1fdc14dcbb-cedcd368}₩$MFT
BCD		₩VOLUME{01d31b1fdc14dcbb-cedcd368}₩BOOT₩BCD
BOOT.SDI		₩VOLUME{01d31b1fdc14dcbb-cedcd368}₩BOOT₩BOOT.SDI
BOOTFIX.BIN		₩VOLUME{01d31b1fdc14dcbb-cedcd368}₩BOOT₩BOOTFIX.BIN
BOOTSECT.EXE		₩VOLUME{01d31b1fdc14dcbb-cedcd368}₩BOOT₩BOOTSECT.EXE
ETFSBOOT.COM		₩VOLUME{01d31b1fdc14dcbb-cedcd368}₩BOOT₩ETFSBOOT.COM

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₩NTDLL.D
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₩KERNEL3
KERNELBASE.DLL	C:₩Windows₩System32₩KERNELBASE.DLL	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩KERNELE
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₩BCRYPTP
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₩cfgmgr32.dll	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩CFGMGF
WUDFPLATFORM.DLL	C:₩Windows₩System32₩WUDFPLATFORM.DLL	₩VOLUME{01d002543e021ff8-383e9e4a}₩WINDOWS₩SYSTEM32₩WUDFPL
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₩MSVCRT
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.D
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₩WIN32U
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.)