

Forensic Study - 5

Windows Theory (2)

2017.11.7

KUICS

2014210009 주어진

목차

1. Windows Disk Format (NTFS)

2. GPT / MBR

3. Windows Cache

4. Windows Event Log

Windows Disk Format (NTFS)

이전에, 파일 시스템이란 무엇인가?

-> 파일 시스템(file system, 문화어: 파일체계)은 컴퓨터에서 파일이나 자료를 쉽게 발견 및 접근할 수 있도록 보관 또는 조직하는 체제를 가리키는 말이다.

디스크, DB, Transaction 파일 시스템등이 있으며, 지금 다룰 것은 Disk File System

참조 : https://ko.wikipedia.org/wiki/%ED%8C%8C%EC%9D%BC_%EC%8B%9C%EC%8A%A4%ED%85%9C

관련 프로그램 : <http://www.disk-editor.org/>

Windows Disk Format (NTFS)

Disk File System의 종류

- FAT
- **NTFS**
- ext3
- ext4

... 그 외 여러 파일 시스템이 존재.

Windows Disk Format (NTFS)

NTFS?

Windows ME까지는 주로 FAT32를 사용했으나,
XP 이후에서는 NTFS를 사용하게 되었다.

Windows 자체적으로 32GB이상의 파티션을 FAT32으로 포맷하지 못하게 막아놓았고 (NTFS 강요, 사실 다른 유틸리티로는 포맷 가능)

지금 사용하는 Windows가 탑재된 파티션은 99%이상이 NTFS이다.

Windows Disk Format (NTFS)

NTFS?



VBR : Boot Sector, Additional Boot code

MFT : 매우 복잡하므로 설명 생략, 이 부분만으로 1학기 스터디가 가능 (참고 : <http://www.ntfs.com/ntfs-mft.htm>)

Data Area : 실제로 Data가 쓰이는 부분

Windows Disk Format (NTFS)

NTFS?

VBR은 고정된 크기가 아닌 클러스터 (섹터 여러 개를 하나로 묶은 것을 말함. 512byte 섹터 8개를 클러스터 단위라 하면 클러스터 하나의 크기는 4KB) 크기에 의존

일반적으로는 VBR Size = Cluster Size

VBR 첫 번째 섹터는 부트 섹터이다.

VBR이 섹터 1개 크기와 같을 경우는 VBR자체가 부트 섹터이나,
VBR 크기가 1KB이상이 될 경우 나머지 섹터는 Addition Boot Code를 저장하거나 NT Loader를 빠르게 로드하기 위한 인덱싱으로 사용.

Windows Disk Format (NTFS)

NTFS?

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
0X0000:	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00	.R.NTFS
0X0010:	00	00	00	00	00	F8	00	00	3F	00	FF	00	3F	00	00	00?...?...
0X002:	00	00	00	00	80	00	80	00	EB	ED	E1	04	00	00	00	00
0X00:	00	00	0C	00	00	00	00	00	DE	1E	4E	00	00	00	00	00	...N.....
0X0:	F6	00	00	00	01	00	00	00	7E	7C	A2	44	9C	A2	44	58	...D...DX
0X:	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	B8	C0	07
0:	8E	D8	E8	16	00	B8	00	0D	8E	C0	33	DB	C6	06	0E	00	..
:	10	E8	53	00	68	00	0D	68	6A	02	CB	8A	16	24	00	B4	

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	
0x00	Jmp Boot Code				OEM Name							Bytes Per Sector		Sector Per Cluster	Reserved Sec Cnt		
0x10	Unused				Media	Unused											
0x20	Unused								Total Sector								
0x30	Start of MFT								Start of MFTMirr								
0x40	Unused				Unused				Serial Number								
0x50	Unused																

0X0160:	C3	A0	F8	01	E8	09	00	A0	FB	01	E8	03	00	FB	EB	FE
0X0170:	F4	01	0F	F0	AC	30	00	74	00	54	0E	BB	07	00	CD	10<.t.....
0X0180:	MFT Entry Size			0D	0A	41	Index Record Size			73	6B	20	72	65	61	64A disk read
0X0190:				72	6F	72				63	75	72	72	65	64	00	error occurred.

Windows Disk Format (NTFS)

NTFS?

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F
0000000000	EB	52	90	4E	54	46	53	20	20	20	20	00	02	08	00	00
0000000010	00	00	00	00	00	F8	00	00	3F	00	FF	00	00	A8	4A	00
0000000020	00	00	00	00	80	00	80	00	50	32	1E	2C	00	00	00	00
0000000030	00	00	0C	00	00	00	00	00	02	00	00	00	00	00	00	00
0000000040	F6	00	00	00	01	00	00	00	4A	9E	3E	38	C9	3E	38	60
0000000050	00	00	00	00	FA	33	C0	8E	D0	BC	00	7C	FB	68	C0	07
0000000060	1F	1E	68	66	00	CB	88	16	0E	00	66	81	3E	03	00	4E
0000000070	54	46	53	75	15	B4	41	BB	AA	55	CD	13	72	0C	81	FB
0000000080	55	AA	75	06	F7	C1	01	00	75	03	E9	DD	00	1E	83	EC
0000000090	18	68	1A	00	B4	48	8A	16	0E	00	8B	F4	16	1F	CD	13
00000000A0	9F	83	C4	18	9E	58	1F	72	E1	3B	06	0B	00	75	DB	A3
00000000B0	0F	00	C1	2E	0F	00	04	1E	5A	33	DB	B9	00	20	2B	C8
00000000C0	66	FF	06	11	00	03	16	0F	00	8E	C2	FF	06	16	00	E8
00000000D0	4B	00	2B	C8	77	EF	B8	00	BB	CD	1A	66	23	C0	75	2D
00000000E0	66	81	FB	54	43	50	41	75	24	81	F9	02	01	72	1E	16
00000000F0	68	07	BB	16	68	52	11	16	68	09	00	66	53	66	53	66
0000000100	55	16	16	16	68	B8	01	66	61	0E	07	CD	1A	33	C0	BF
0000000110	0A	13	B9	F6	0C	FC	F3	AA	E9	FE	01	90	90	66	60	1E
0000000120	06	66	A1	11	00	66	03	06	1C	00	1E	66	68	00	00	00
0000000130	00	66	50	06	53	68	01	00	68	10	00	B4	42	8A	16	0E
0000000140	00	16	1F	8B	F4	CD	13	66	59	5B	5A	66	59	66	59	1F
0000000150	0F	82	16	00	66	FF	06	11	00	03	16	0F	00	8E	C2	FF
0000000160	0E	16	00	75	BC	07	1F	66	61	C3	A1	F6	01	E8	09	00
0000000170	A1	FA	01	E8	03	00	F4	EB	FD	8B	F0	AC	3C	00	74	09
0000000180	B4	0E	BB	07	00	CD	10	EB	F2	C3	0D	0A	41	20	64	69
0000000190	73	6B	20	72	65	61	64	20	65	72	72	6F	72	20	6F	63
00000001A0	63	75	72	72	65	64	00	0D	0A	42	4F	4F	54	4D	47	52
00000001B0	20	69	73	20	63	6F	6D	70	72	65	73	73	65	64	00	0D
00000001C0	0A	50	72	65	73	73	20	43	74	72	6C	2B	41	6C	74	2B
00000001D0	44	65	6C	20	74	6F	20	72	65	73	74	61	72	74	0D	0A
00000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001F0	00	00	00	00	00	00	8A	01	A7	01	BF	01	00	00	55	AA

ëR.NTFS
.....ø...?.ÿ..."J.
.....€..P2.,.....
.....
ö.....Jž>8É>8`
.....û3ÄZB4..|ûhÄ.
..hf.Ë"...f.>...N
TFSu."A»"UÍ.r..û
U"u.+Ä..u.éÿ..fì
..h..."HŠ....<ö...î.
ÿfÄ.žX.rá;...uûB
..Ä.....Z3Û". +Ë
fÿ.....ŽÄÿ...ë
K.+Ëwi..»î.f#Äu-
f.ûTCPAu\$.ù..r..
h.»hR..h..fSfSf
U...h..fa..î.3Ä;
...'ö.ûö"ép...f`.
..f;..f.....fh...
..fP.Sh..h.."BŠ..
...<öî.fÿ[Zfÿfÿ.
...fÿ.....ŽÄÿ
...u4..faÄ;ö.ë..
;ü.ë..öëÿ<ö-<.t.
".»..î.ëöÄ..A di
sk read error oc
curred...BOOTMGR
is compressed..
..Press Ctrl+Alt+
Del to restart..
.....
.....Š.S.¿...U"

Windows Disk Format (NTFS)

NTFS? (Unused는 왜 있는 것일까?)

Name	Offset	Value	Copy Value
JMP instruction	000	EB 52 90	EB 52 90
OEM ID	003	NTFS	NTFS
▼ BIOS Parameter Block	011		
Bytes per sector	011	512	512
Sectors per cluster	013	8	8
Reserved sectors	014	0	0
(always zero)	016	00 00 00	00 00 00
(unused)	019	00 00	00 00
Media descriptor	021	248	248
(unused)	022	00 00	00 00
Sectors per track	024	63	63
Number of heads	026	255	255
Hidden sectors	028	4,892,672	4,892,672
(unused)	032	00 00 00 00	00 00 00 00
Signature	036	80 00 80 00	80 00 80 00
Total sectors	040	740,176,464	740,176,464
SMFT cluster number	048	786,432	786,432
SMFTMirr cluster number	056	2	2
Clusters per File Record Se...	064	246	246
Clusters per Index Block	068	1	1
Volume serial number	072	4A 9E 3E 38 C9 3E 38 60	4A 9E 3E 38 C9 3E 38 60
Checksum	080	0	0
Bootstrap code	084	FA 33 C0 8E D0 BC 00 7...	FA 33 C0 8E D0 BC 00 7C FB 68 C0 07 1F 1E 6...
Signature (55 AA)	510	55 AA	55 AA

Bookmarks	
Bookmark	Offset

View	A ASCII	U Unicode	Browse File Entries	Open File			
Offset	00 01 02 03 04 05 06 07	08 09 10 11 12 13 14 15	ASCII				
000000000000	EB 52 90 4E 54 46 53 20	20 20 20 00 02 08 00 00	.R.NTFS ...				
000000000016	00 00 00 00 00 F8 00 00	3F 00 FF 00 00 A8 4A 00	...?...				
000000000032	00 00 00 00 80 00 80 00	50 32 1E 2C 00 00 00 00	...P2,...				
000000000048	00 00 0C 00 00 00 00 00	02 00 00 00 00 00 00 00				
000000000064	F6 00 00 00 01 00 00 00	4A 9E 3E 38 C9 3E 38 60J.>8>				
000000000080	00 00 00 00 FA 33 C0 8E	D0 BC 00 7C FB 68 C0 07	...3.... h..				
000000000096	1F 1E 68 66 00 CB 88 16	0E 00 66 81 3E 03 00 4E	..hf.....f.>.N				
000000000112	54 46 53 75 15 B4 41 BB	AA 55 CD 13 72 0C 81 FB	TFSu..A..U..r...				
000000000128	55 AA 75 06 F7 C1 01 00	75 03 E9 DD 00 1E 83 EC	U.u.....u.....				
000000000144	18 68 1A 00 B4 48 8A 16	0E 00 8B F4 16 1F CD 13	.h...H.....				
000000000160	9F 83 C4 18 9E 58 1F 72	E1 3B 06 0B 00 75 DB A3X.r;...u..				
000000000176	0F 00 C1 2E 0F 00 04 1E	5A 33 DB B9 00 20 2B C8z3... +.				
000000000192	66 FF 06 11 00 03 16 0F	00 8E C2 FF 06 16 00 E8	f.....				
000000000208	4B 00 2B C8 77 EF B8 00	BB CD 1A 66 23 C0 75 2D	K.+w.....f#.u-				
000000000224	66 81 FB 54 43 50 41 75	24 81 F9 02 01 72 1E 16	f..TCPAu\$.r..				
000000000240	68 07 BB 16 68 52 11 16	68 09 00 66 53 66 53 66	h...hR..h..fSfSf				
000000000256	55 16 16 16 68 B8 01 66	61 0E 07 CD 1A 33 C0 BF	U...h..fa....3..				
000000000272	0A 13 B9 F6 0C FC F3 AA	E9 FE 01 90 90 66 60 1Ef`..				
000000000288	06 66 A1 11 00 66 03 06	1C 00 1E 66 68 00 00 00	.f...f.....fh...				
000000000304	00 66 50 06 53 68 01 00	68 10 00 B4 42 8A 16 0E	.fP.Sh..h...B...				
000000000320	00 16 1F 8B F4 CD 13 66	59 5B 5A 66 59 66 59 1FfY[ZfYfY.				
000000000336	0F 82 16 00 66 FF 06 11	00 03 16 0F 00 8E C2 FFf.....				
000000000352	0E 16 00 75 BC 07 1F 66	61 C3 A1 F6 01 E8 09 00	...u...fa.....				
000000000368	A1 FA 01 E8 03 00 F4 EB	FD 8B F0 AC 3C 00 74 09<.t.				
000000000384	B4 0E BB 07 00 CD 10 EB	F2 C3 0D 0A 41 20 64 69A di				
000000000400	73 6B 20 72 65 61 64 20	65 72 72 6F 72 20 6F 63	sk read error oc				
000000000416	63 75 72 72 65 64 00 0D	0A 42 4F 4F 54 4D 47 52	currred...BOOTMGR				
000000000432	20 69 73 20 63 6F 6D 70	72 65 73 73 65 64 00 0D	is compressed..				
000000000448	0A 50 72 65 73 73 20 43	74 72 6C 2B 41 6C 74 2B	.Press Ctrl+Alt+				
000000000464	44 65 6C 20 74 6F 20 72	65 73 74 61 72 74 0D 0A	Del to restart..				
000000000480	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00				
000000000496	00 00 00 00 00 00 8A 01	A7 01 BF 01 00 00 55 AAU.				

GPT / MBR

GPT? MBR?

MBR : Master Boot Record

GPT : EFI에서 사용하는 디스크 형식

MBR은 Disk 해당 섹터에 부팅을 위한 코드를 기록하지만, GPT (GUID Partition Table)의 경우 Core Firmware에 이를 내장. 그래서 MBR Rootkit이 통하지 않는다.

또한 GPT는 BPT (Backup Partition Table)을 디스크 끝 영역에 저장하여 복구에 사용.

GPT / MBR

GPT? MBR?

```
Microsoft DiskPart 버전 10.0.16299.15
```

```
Copyright (C) Microsoft Corporation.  
컴퓨터: DESKTOP-S4RK920
```

```
DISKPART> list disk
```

디스크 ###	상태	크기	사용 가능	Dyn	Gpt
디스크 0	온라인	476 GB	1024 KB		*

```
DISKPART> _
```

GPT / MBR

EFI?

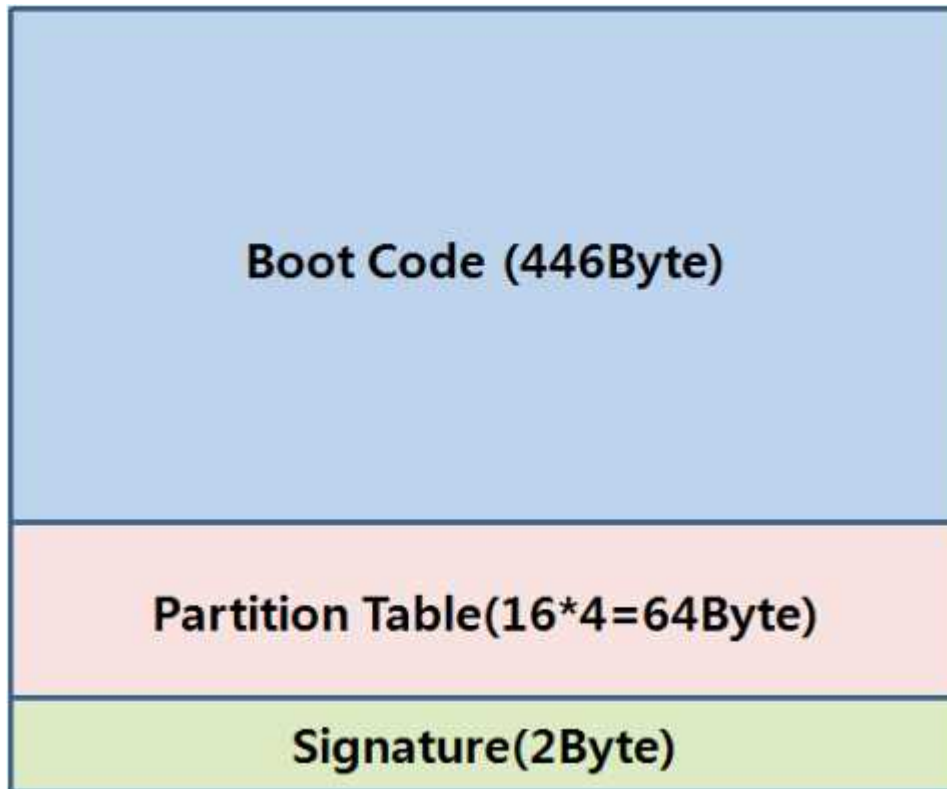
-> 통일 확장 펌웨어 인터페이스(영어: Unified Extensible Firmware Interface, UEFI)는 운영 체제와 플랫폼 펌웨어 사이의 소프트웨어 인터페이스를 정의하는 규격이다. IBM PC 호환기종에서 사용되는 바이오스 인터페이스를 대체할 목적으로 개발되었다.

드라이버 펌웨어, 그래픽스, UEFI 운영체제 로더등등 다양하다.

GPT / MBR

MBR?

MBR : Master Boot Record



GPT / MBR

MBR?

MBR : Master Boot Record

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
														boot Flag	CHS Start
CHS Start		Part Type	End CHS			LBA Start				Size in Sector					

Ex) 00 01

01 00 0B FE BF 7C 3F 00 00 00 FE 25 9C 00

-> 00 : Booting 불가, 00 01 01 : CHS Start, 0B : 파티션 타입, 7C BF FE : CHS End

GPT / MBR

GPT? MBR?

Sector 0 (왜 GPT도 MBR을 쓸까?)

Offset	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	ASCII	Unicode
0000000090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0000000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001B0	00	00	00	00	00	00	00	00	E4	A2	22	86	00	00	00	00"
00000001C0	01	00	EE	FE	FF	FF	01	00	00	00	AF	12	9E	3B	00	00;و.....
00000001D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000001F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	55	AAU.

Windows Cache

윈도우에서 저장하는 캐시는 여러 종류가 있는데,

크게는

-> DNS Cache, ARP Cache, Netbios Cache

-> SuperFetch로 생성되는 Process Cache

등이 있다.

Windows Cache

DNS Cache 확인 (ipconfig /displaydns)

```
C:\Users\Wakwke>ipconfig /displaydns

Windows IP 구성

www.gstatic.com
-----
데이터 이름      : www.gstatic.com
데이터 유형      : 1
TTL(Time To Live) : 71
데이터 길이      : 4
섹션             : 응답
(호스트) 레코드   : 172.217.28.3

데이터 이름      : ns1.google.com
데이터 유형      : 1
TTL(Time To Live) : 71
데이터 길이      : 4
섹션             : 추가
(호스트) 레코드   : 216.239.32.10

데이터 이름      : ns2.google.com
데이터 유형      : 1
TTL(Time To Live) : 71
데이터 길이      : 4
섹션             : 추가
(호스트) 레코드   : 216.239.34.10
```

Windows Cache

ARP Cache 확인 (arp -a)

```
C:\Users\wakwke>arp -a
```

```
인터페이스: 192.168.28.1 --- 0x4
인터넷 주소      물리적 주소      유형
192.168.28.255    ff-ff-ff-ff-ff-ff  정적
224.0.0.2         01-00-5e-00-00-02  정적
224.0.0.22        01-00-5e-00-00-16  정적
224.0.0.251       01-00-5e-00-00-fb  정적
224.0.0.252       01-00-5e-00-00-fc  정적
239.255.255.250   01-00-5e-7f-ff-fa  정적
```

```
인터페이스: 192.168.0.10 --- 0x9
인터넷 주소      물리적 주소      유형
192.168.0.1       90-9f-33-b0-b5-28  동적
192.168.0.255     ff-ff-ff-ff-ff-ff  정적
224.0.0.2         01-00-5e-00-00-02  정적
224.0.0.22        01-00-5e-00-00-16  정적
224.0.0.251       01-00-5e-00-00-fb  정적
224.0.0.252       01-00-5e-00-00-fc  정적
239.255.255.250   01-00-5e-7f-ff-fa  정적
255.255.255.255   ff-ff-ff-ff-ff-ff  정적
```

```
인터페이스: 192.168.244.1 --- 0xa
인터넷 주소      물리적 주소      유형
192.168.244.255   ff-ff-ff-ff-ff-ff  정적
224.0.0.2         01-00-5e-00-00-02  정적
224.0.0.22        01-00-5e-00-00-16  정적
224.0.0.251       01-00-5e-00-00-fb  정적
224.0.0.252       01-00-5e-00-00-fc  정적
```

Windows Cache

netbios 확인 (nbtstat -c)

```
C:\Users\wakwke>nbtstat -c
```

```
VMware Network Adapter VMnet1:  
노드 IpAddress: [192.168.28.1] 범위 ID: []
```

캐시에 이름 없음

```
VMware Network Adapter VMnet8:  
노드 IpAddress: [192.168.244.1] 범위 ID: []
```

캐시에 이름 없음

```
Bluetooth 네트워크 연결:  
노드 IpAddress: [0.0.0.0] 범위 ID: []
```

캐시에 이름 없음

```
이더넷:  
노드 IpAddress: [0.0.0.0] 범위 ID: []
```

캐시에 이름 없음
























```
Wi-Fi:  
노드 IpAddress: [192.168.0.10] 범위 ID: []
```

캐시에 이름 없음

Windows Cache

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

내 PC > Windows (C:) > Windows > Prefetch

<input type="checkbox"/> 이름	수정한 날짜	유형	크기
 ReadyBoot	2017-11-07 오전...	파일 폴더	
 _JU14D2N.TMP-FE763018.pf	2017-11-07 오후...	PF 파일	15KB
 AGENTCONTROLLER.EXE-5B7DAAA0....	2017-11-07 오후...	PF 파일	7KB
 AGENTCONTROLLER.EXE-BAAEFDE1.pf	2017-11-07 오후...	PF 파일	7KB
 APPLICATIONFRAMEHOST.EXE-0CDE...	2017-11-07 오후...	PF 파일	16KB
 ARP.EXE-6FB788BE.pf	2017-11-07 오후...	PF 파일	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...	PF 파일	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...	PF 파일	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

Windows Event Log

윈도우에서 발생한 이벤트를 저장하는 것.

이 역시 포렌식에 이용된다.

Event Source	Event	Event ID		
		2000	XP & 2003	Vista & Over
Security	Login Success	528	528	4624
	Network Login	540(Type : 3)	540(Type : 3)	4624(Type : 3)
	Login fail	529 ~ 535	529 ~ 535	4625
	Attempt login	Not Logged	552	4648
	Assignment of login access right	576	576	4672
	Create Process	592	592	4688
	Service install	Not Logged	602	4697
	Start Windows	512	512	4608
	Off the Windows	513	513	4609
	Access to network shared object	Not Logged	Not Logged	5140
System	System halt	1074	1074	1074
	Start event log service	6005	6005	6005
	Stop event log service	6006	6006	6006
	Service install	7045	7045	7045
	Service realted	7036	7036	7036
	RDP Connection	682	682	4778
Application	Application error	1000	1000	1000
	Start service	1006	1006	1006
	Add member into group	1525	1525	1525
	Del member in group	1526	1526	1526
	Create shared object	2817,2818	2817,2818	2817,2818
	Change authorization of shared object	3329,3330	3329,3330	3329,3330

Windows Event Log

WinXP까지는

- Remote Logon or access
- Account create or delete
- Service start or end
- Process start
- System halt

정도만 제공했으나, Vista 이후부터는

- Task Scheduler
- RDP Connection

등의 이벤트도 저장해둔다.

감사합니다

과제 : 없습니다.