

# 침해 실행 아티팩트



*JK Kim*

*@pr0neer*

*forensic-proof.com*

*proneer@gmail.com*

1. 프리패치
2. 파일시스템 로그
3. 바로가기
4. 점프 목록
5. 레지스트리
6. AV 로그
7. 볼륨 새도 복사본
8. 호환성 아티팩트
9. WoW64
10. 윈도우 문제 보고

# 프리패치

- 프리패치 소개

- 윈도우 프리패칭 (Windows Prefetching)

- ✓ 실행 파일이 사용하는 시스템 자원 정보를 특정 파일에 저장 ➔ 프리패치 파일
- ✓ 윈도우 부팅 시 프리패치 파일을 모두 메모리에 로드
- ✓ 사용자가 파일을 실행할 경우 미리 저장된 정보를 이용해 초기 실행 속도 향상
- ✓ 윈도우 XP 이후 (2003, Vista, 2008, 7, 8, 10)의 운영체제에서 제공

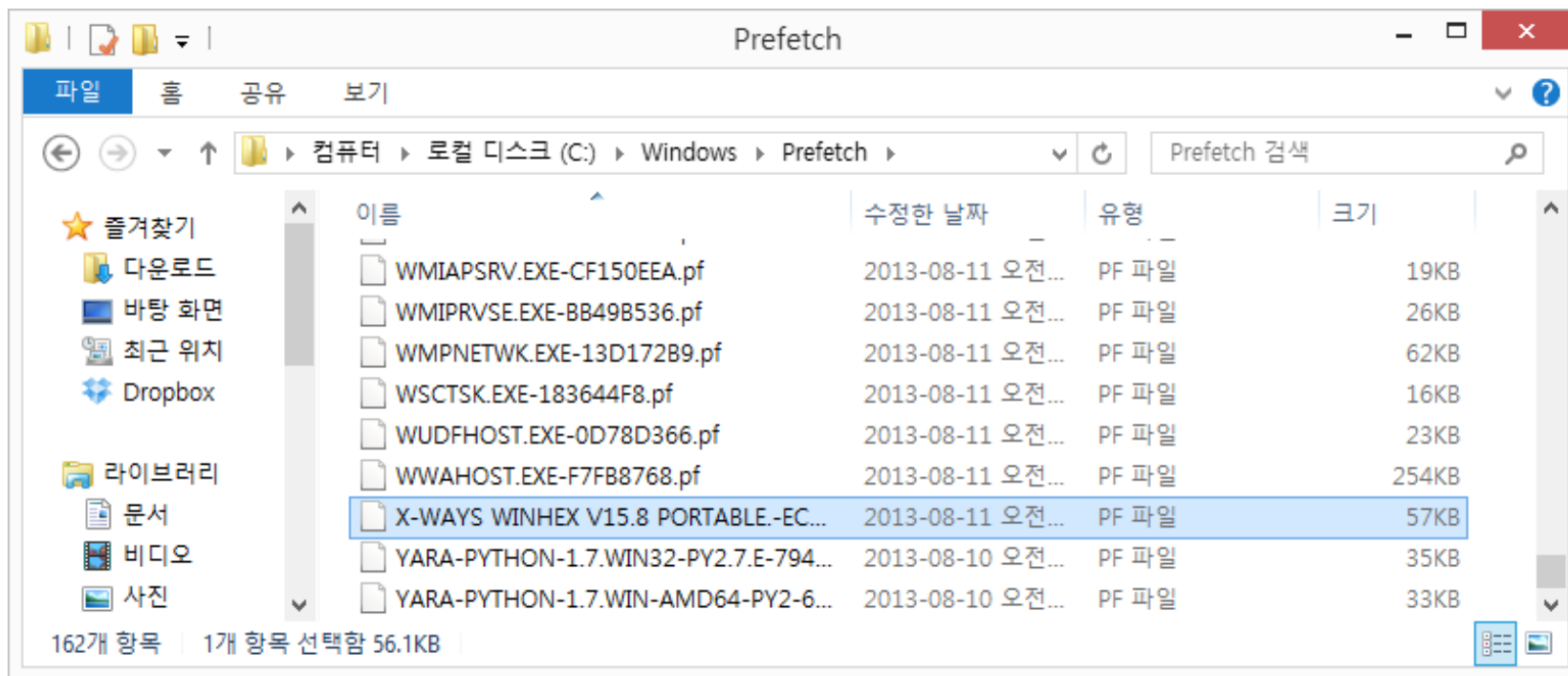
- 프리패칭 유형

- ✓ 부트 프리패칭 (Boot Prefetching) : XP, 2003, Vista 2008, 7
- ✓ 응용프로그램 프리패칭 (Application Prefetching) : XP, Vista, 7, 8, 10

# 프리패치

## ■ 프리패치 파일 경로

### • %SystemRoot%\Prefetch



### • 파일명

✓ 부트 프리패치 : [NTOSBOOT-B00DFAAD.pf](#)

✓ 응용프로그램 프리패치 : [<filename>-<filepath hash>.pf](#)

## ▪ 부트 프리패칭 vs 응용프로그램 프리패칭

### • 부트 프리패칭

- ✓ 부팅과 관련된 파일이 저장장치에 흩어져 있거나 단편화되어 있음 ➔ 부팅 속도 저하
- ✓ 프리패처에 의해 시스템 부팅 시 최대 120초 까지 모니터링
- ✓ 부팅 시 사용하는 파일을 모니터링한 후 결과를 파일에 저장
- ✓ 프리패칭된 파일을 이용하여 부팅 속도 향상

### • 응용프로그램 프리패칭

- ✓ 응용프로그램 초기 실행 시 캐시 관리자가 처음 10초를 모니터링
- ✓ 10초 동안 사용한 파일을 모니터링한 후 결과를 파일로 저장
- ✓ 프리패칭된 응용프로그램 다시 실행 시, 프리패치 파일을 이용해 초기 실행 속도 향상
- ✓ 파일 개수는 최대 128개로 제한 ➔ 한계치를 넘으면 사용되지 않는 파일부터 자동 삭제

## ■ 프리패치 포렌식

### • 프리패치 파일에서 획득 가능한 정보

- ✓ 응용프로그램 이름
- ✓ 응용프로그램 실행 횟수
- ✓ 응용프로그램 마지막 실행 시각 (FILETIME, 64-Bit Timestamp)
- ✓ 참조 목록 (실행 시 필요한 DLL, SDB, NLS, INI 등의 경로)
- ✓ 파일 시스템 시간 정보 (생성, 수정, 접근 시간)을 이용한 통합 분석



### • 프리패치 활용

- ✓ 악성코드가 실행될 경우, 프리패치 파일 자동 생성
- ✓ 부트 프리패치 파일을 이용해, 부팅 시 로드되는 악성코드 탐지 가능
- ✓ 참조 목록을 통해, 로드한 라이브러리, 파일 목록 확인 가능

# 프리패치

## ■ 프리패치 활용 → 부트 프리패치

- V3 진단명 – Win-Trojan/Agent.166912.BN(5c7f361de004a7a342895beb9f1e0b89)

이름	수정한 날짜	유형	크기
 NTOSBOOT-B00DFAAD_01.pf	2013-03-11 오후 1:22	PF 파일	827KB
 NTOSBOOT-B00DFAAD_02.pf	2013-03-11 오후 3:49	PF 파일	884KB

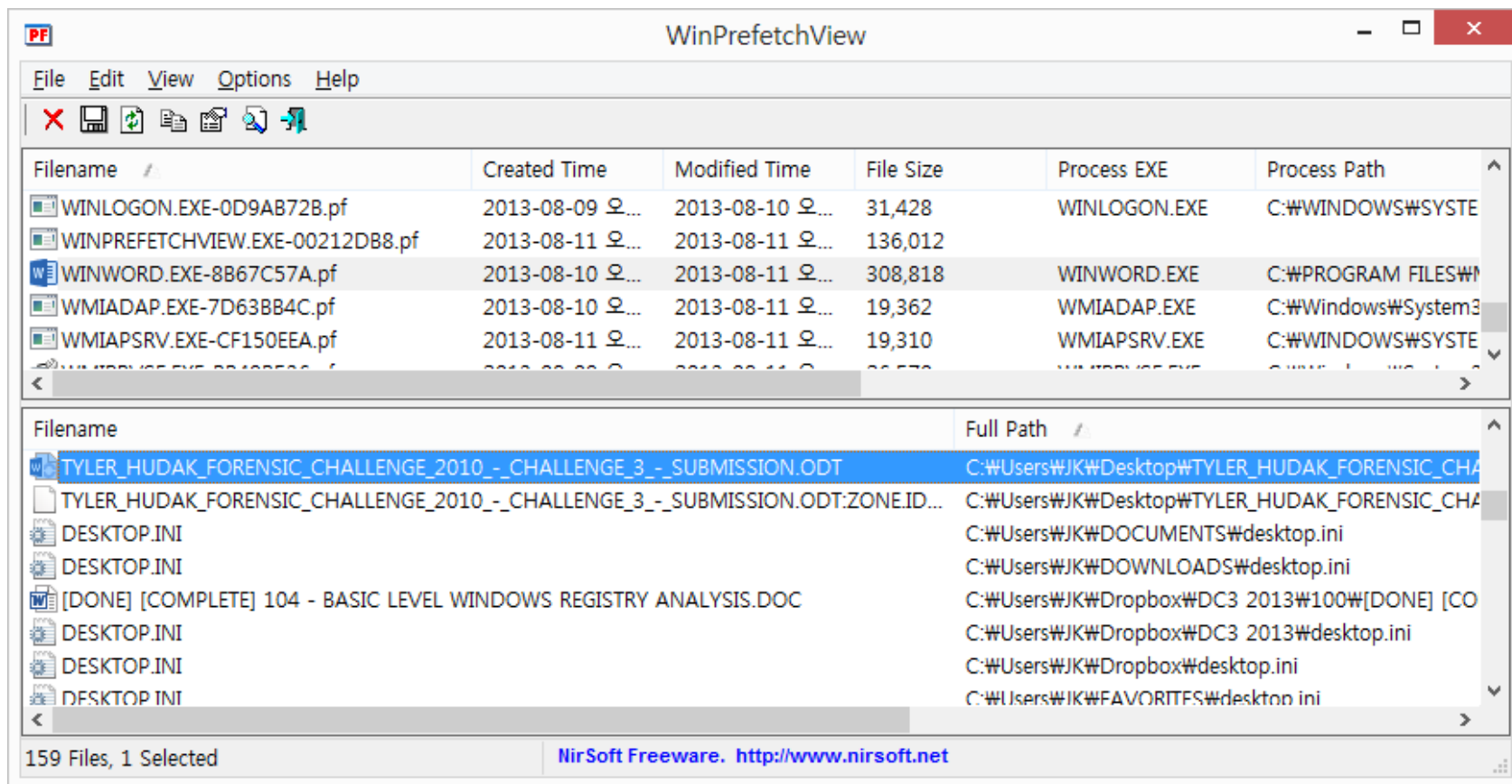
1	NTOSBOOT-B00DFAAD_01.pf	NTOSBOOT-B00DFAAD_02.pf
378		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\COMPMGMT.MSC
400		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\CYSWSS.DLL
401		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DAVCLNT.DLL
406		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DESKTOP.INI
408		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DHCPSPIDLL
509		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DRIVERS\CACHE\XXX.SCR
566		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\DRIVERS\SERVICE.EXE
655		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LOGMAN.EXE
656		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LOGO.SCR
657		%DEVICE%\HARDDISKVOLUME1\WINDOWS\SYSTEM32\LOGON.SCR



# 프리패치

- 프리패치 활용 → 응용프로그램 프리패치

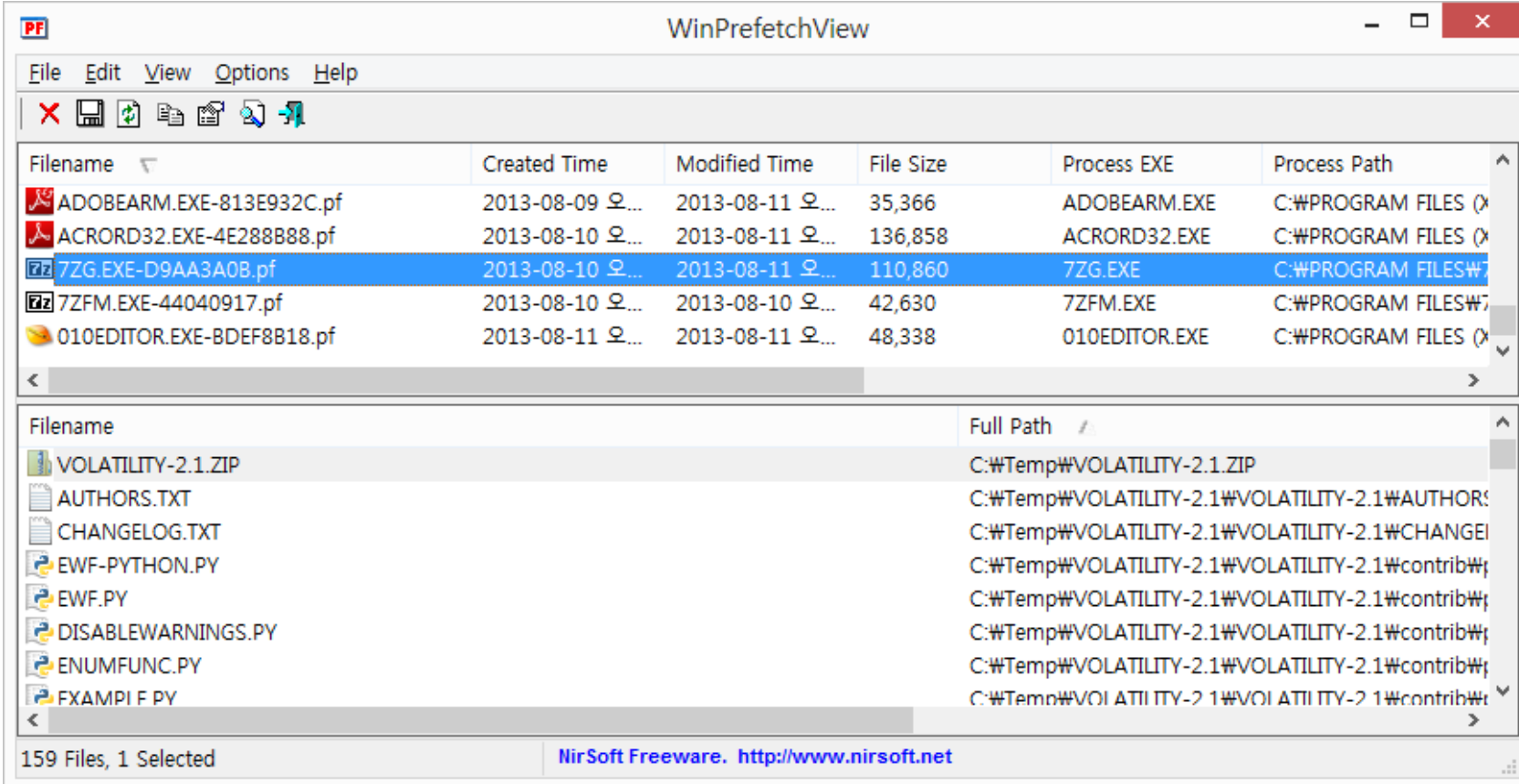
- WINWORD.EXE



# 프리패치

## ■ 프리패치 활용 → 응용프로그램 프리패치

### • 7ZG.EXE



WinPrefetchView

Filename	Created Time	Modified Time	File Size	Process EXE	Process Path
ADOBEARM.EXE-813E932C.pf	2013-08-09 오후 1:11	2013-08-11 오후 1:11	35,366	ADOBEARM.EXE	C:\PROGRAM FILES (X86)\ADOBE\ACROBAT\READER\ADOBEARM.EXE
ACRORD32.EXE-4E288B88.pf	2013-08-10 오후 1:11	2013-08-11 오후 1:11	136,858	ACRORD32.EXE	C:\PROGRAM FILES (X86)\ADOBE\ACROBAT\READER\ACRORD32.EXE
7ZG.EXE-D9AA3A0B.pf	2013-08-10 오후 1:11	2013-08-11 오후 1:11	110,860	7ZG.EXE	C:\PROGRAM FILES (X86)\7-ZIP\7ZG.EXE
7ZFM.EXE-44040917.pf	2013-08-10 오후 1:11	2013-08-10 오후 1:11	42,630	7ZFM.EXE	C:\PROGRAM FILES (X86)\7-ZIP\7ZFM.EXE
010EDITOR.EXE-BDEF8B18.pf	2013-08-11 오후 1:11	2013-08-11 오후 1:11	48,338	010EDITOR.EXE	C:\PROGRAM FILES (X86)\010\010EDITOR.EXE

Filename	Full Path
VOLATILITY-2.1.ZIP	C:\Temp\VOLATILITY-2.1.ZIP
AUTHORS.TXT	C:\Temp\VOLATILITY-2.1\VOLATILITY-2.1\AUTHORS.TXT
CHANGELOG.TXT	C:\Temp\VOLATILITY-2.1\VOLATILITY-2.1\CHANGELOG.TXT
EWf-PYTHON.PY	C:\Temp\VOLATILITY-2.1\VOLATILITY-2.1\contrib\python\ewf-python.py
EWf.PY	C:\Temp\VOLATILITY-2.1\VOLATILITY-2.1\contrib\python\ewf.py
DISABLEWARNINGS.PY	C:\Temp\VOLATILITY-2.1\VOLATILITY-2.1\contrib\python\disablewarnings.py
ENUMFUNC.PY	C:\Temp\VOLATILITY-2.1\VOLATILITY-2.1\contrib\python\enumfunc.py
FXAMPI F PY	C:\Temp\VOLATILITY-2.1\VOLATILITY-2.1\contrib\python\fxamplif.py

159 Files, 1 Selected      NirSoft Freeware. <http://www.nirsoft.net>

- 프리패치 파일 분석 도구
  - **WinPrefetchView** – Nirsoft
    - ✓ [http://www.nirsoft.net/utils/win\\_prefetch\\_view.html](http://www.nirsoft.net/utils/win_prefetch_view.html)
  - **PrefetchForensics** – Mark Woan
    - ✓ <http://www.woanware.co.uk/forensics/prefetchforensics.html>
  - **APFA(Advanced Prefetch File Analyzer)** – ASH368
    - ✓ <http://www.ash368.com/>
  - **Windows Prefetch Parser** – TZWorks
    - ✓ [https://www.tzworks.net/prototype\\_page.php?proto\\_id=1](https://www.tzworks.net/prototype_page.php?proto_id=1)

## ➔ 실습

- 라이브 시스템의 프리패치 파일 분석하기!!
  - ✓ 정상 프리패치 파일 추출 후 분석
  - ✓ 삭제된 프리패치 파일 카빙 후 분석

# 파일시스템 로그

# 파일시스템 로그

- 파일시스템 로그란?

- 파일시스템의 I/O 혹은 트랜잭션에 대한 로그

- NTFS 파일시스템 로그

- ✓ %SystemDrive%\\$LogFile

- ✓ %SystemDrive%\\$Extend%\\$UsnJrnl:\$J

- 파일시스템 로그의 장점

- ✓ 특정 기간 동안 일어난 상세한 파일시스템 이벤트 분석 가능

- ✓ 삭제된 파일의 흔적 추적 가능

- NTFS \$LogFile

- 트랜잭션 로그 파일

- ✓ 시스템 비정상 동작을 대비하기 위한 트랜잭션 로그
- ✓ 파일 생성, 삭제, 수정, 파일명 변경, 이동 등의 행위 파악 가능

- 트랜잭션 단위의 로그 기록

- ✓ 파일/디렉터리 생성
- ✓ 파일/디렉터리 삭제
- ✓ 파일/디렉터리 변경
- ✓ MFT 레코드 변경

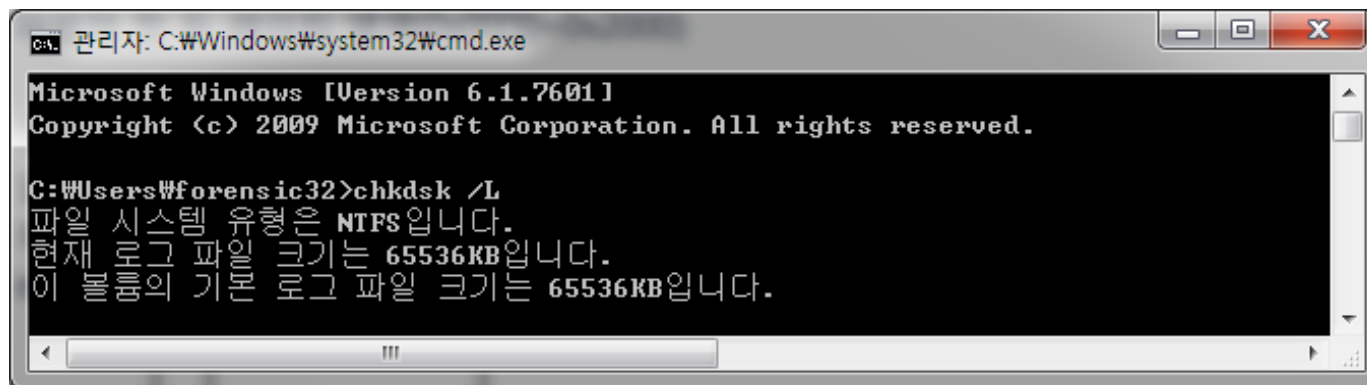
# 파일시스템 로그

## ■ NTFS \$LogFile

### • 로그 설정

- ✓ 일반적으로 64MB 크기
- ✓ PC의 일반적 작업이라면 2~3시간 정도의 로그가 보관
- ✓ 침해사고 준비도 측면에서 용량 증가 필요
- ✓ 크기 설정

```
$> chkdsk /F /L:[size]
```

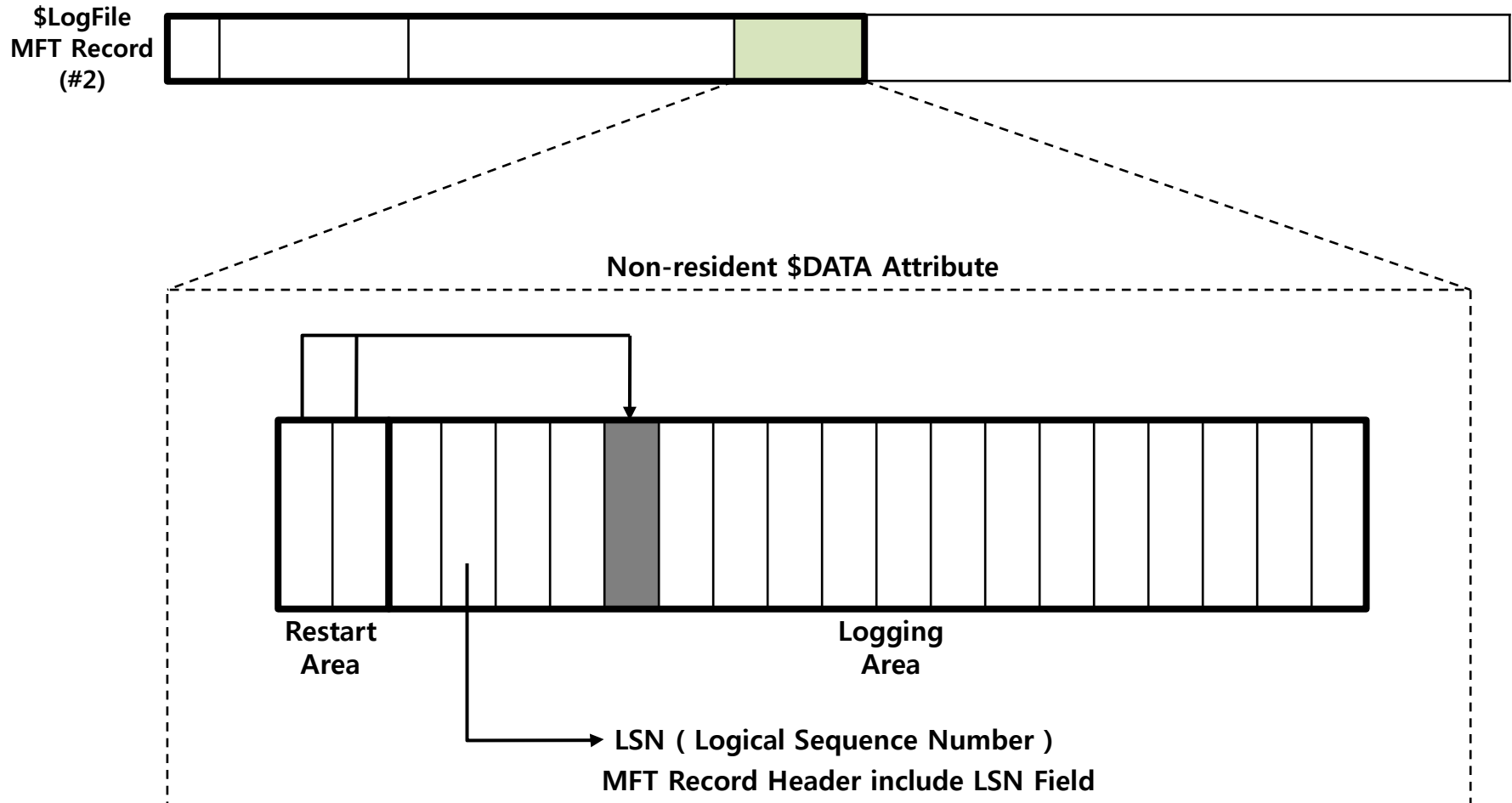


```
관리자: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\forensic32>chkdsk /L
파일 시스템 유형은 NTFS입니다.
현재 로그 파일 크기는 65536KB입니다.
이 볼륨의 기본 로그 파일 크기는 65536KB입니다.
```



## ▪ NTFS \$LogFile



- NTFS \$UsnJrnl (Change Log)

- NTFS 변경 로그

- ✓ 파일이나 디렉터리의 변경 내용 기록
- ✓ 윈도우 7부터 기본 활성화

- 로그에 기록되는 정보

- ✓ 변경된 시간
- ✓ 변경 이유
- ✓ 파일/디렉터리의 이름
- ✓ 파일/디렉터리의 속성
- ✓ 파일/디렉터리의 MFT 레코드 번호
- ✓ 파일의 부모 디렉터리에 대한 파일 참조 주소
- ✓ 보안 ID (Security ID)
- ✓ 레코드의 USN (Update Sequence Number)

- NTFS \$UsnJrnl (Change Log)

- 기록되는 로그의 양

- ✓ 컴퓨터를 계속 사용할 경우, 보통 1~2일의 로그 저장
- ✓ 하루 8시간 정도 사용할 경우, 보통 4~5일의 로그 저장
- ✓ 신속한 대응이나 로그의 백업 필요
- ✓ 크기 확인

```
$> fsutil usn queryjournal <VolumePath>
```

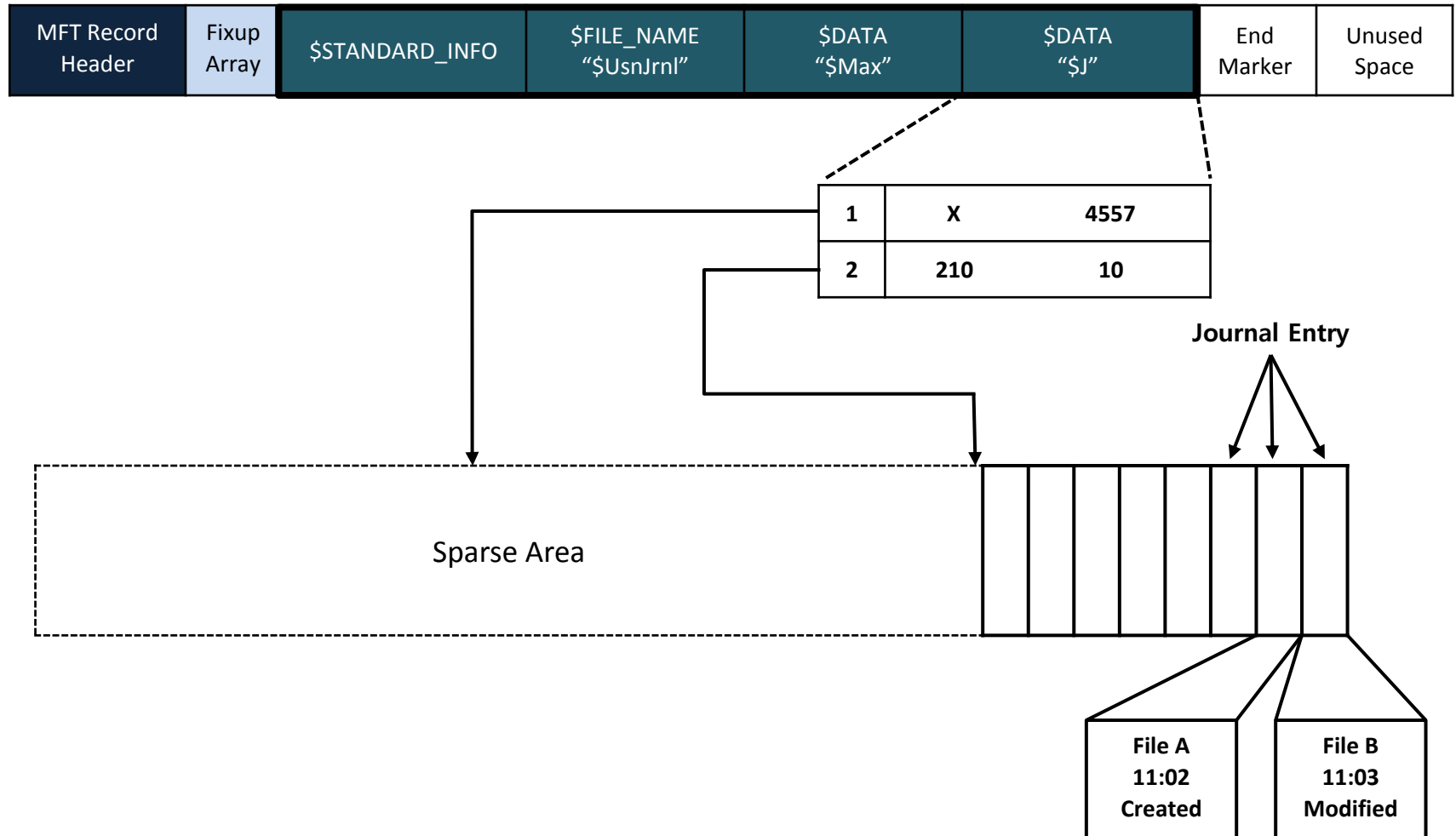
- ✓ 크기 설정

```
$> fsutil usn createjournal m=<MaxSize> a=<AllocationDelta> < VolumePath >
```

- \$UsnJrnl ADS

- ✓ \$Max – 변경 로그에 대한 메타데이터
- ✓ \$J – 실제 변경 레코드

## NTFS \$UsnJrnl (Change Log)



# 파일시스템 로그

## ■ NTFS \$UsnJrnl (Change Log)

- 대부분의 악성코드는 파일시스템 입/출력 사용
- 로그 파일의 수명을 고려하여 용량을 늘리거나 신속한 대응 절차 마련

1	date	time	MFT entry	seq num	parent	filename	type change
144105	12/14/2012	15:38:23.364	0x00000000a472	0x0007	0x000000000b17	TMP000000082CD5F3CA1158680B	file_added; file_created
144106	12/14/2012	15:38:24.425	0x00000000a472	0x0007	0x000000000b17	TMP000000082CD5F3CA1158680B	file_added; file_created; file_deleted; file_closed
144107	12/14/2012	15:38:24.440	0x00000000a472	0x0008	0x000000000165	Detections.log	file_created
144108	12/14/2012	15:38:24.440	0x00000000a472	0x0008	0x000000000165	Detections.log	file_added; file_created
144109	12/14/2012	15:38:26.250	0x00000000a238	0x0001	0x000000000b0d	Microsoft-Windows-Windows Defender%4Operational.evtx	data_overwritten
144110	12/14/2012	15:38:30.259	0x00000000a477	0x0002	0x000000002a16	\$5da39e9580074308c6cfbce61795d0d	file_created
144111	12/14/2012	15:38:30.275	0x00000000a478	0x0002	0x00000000a477	L	file_created
144112	12/14/2012	15:38:30.275	0x00000000a478	0x0002	0x00000000a477	L	file_created; file_closed
144113	12/14/2012	15:38:30.275	0x00000000a479	0x0002	0x00000000a477	U	file_created; attrib_changed
144114	12/14/2012	15:38:30.275	0x00000000a479	0x0002	0x00000000a477	U	file_created; attrib_changed; file_closed
144115	12/14/2012	15:38:30.290	0x00000000a47a	0x0002	0x00000000a477	@	file_created
144116	12/14/2012	15:38:30.290	0x00000000a47a	0x0002	0x00000000a477	@	file_added; file_created
144117	12/14/2012	15:38:30.290	0x00000000a47a	0x0002	0x00000000a477	@	file_added; file_created; file_closed
144118	12/14/2012	15:38:30.290	0x00000000a47b	0x0002	0x00000000a477	n	file_created
144119	12/14/2012	15:38:30.290	0x00000000a47b	0x0002	0x00000000a477	n	file_added; file_created
144120	12/14/2012	15:38:30.290	0x00000000a47b	0x0002	0x00000000a477	n	file_added; file_created; file_closed
144121	12/14/2012	15:38:30.290	0x00000000a477	0x0002	0x000000002a16	\$5da39e9580074308c6cfbce61795d0d	file_created; file_closed
144122	12/14/2012	15:38:32.599	0x00000000a47c	0x0002	0x00000000c461	C	file_created
144123	12/14/2012	15:38:32.630	0x00000000a47c	0x0002	0x00000000c461	C	file_created; file_closed

<http://journeyintoir.blogspot.kr/2013/01/re-introducing-usnjrnl.html>

- NTFS 로그 분석 도구

- **NTFS Log Tracker** – blueangel

- ✓ <https://sites.google.com/site/forensicnote/ntfs-log-tracker>

- **NTFS TriForce** – David Cowen

- ✓ <https://docs.google.com/forms/d/1GzOMe-QHtB12ZnI4ZTjLA06DJP6ZScXngO42ZDGIpR0/viewform>

## ➔ 실습

- 라이브 시스템의 파일시스템 로그 분석하기!!
  - ✓ \$MFT, \$LogFile, \$UsnJrnl:\$J 추출 후 분석

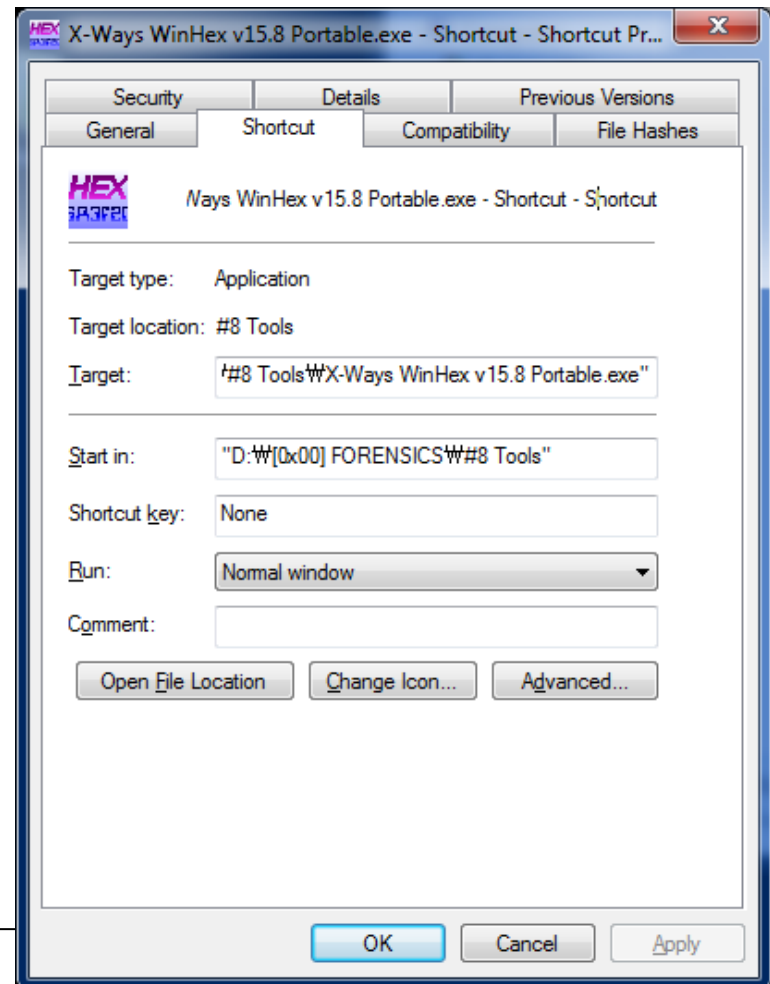
# 바로가기



# 바로가기

## ■ 바로가기 파일이란?

- 링크 파일(LNK)이라고도 불리며 영문 명칭은 "Windows Shortcut", "Shell Link"
- 윈도우에만 존재하는 기능으로 파일, 디렉터리 등 객체를 참조하는 파일
- 커맨드라인이 아닌 GUI에서만 동작
- .lnk 확장자를 가짐



# 바로가기

- 바로가기 파일 저장 위치 (1/2)

- 시작 메뉴

- ✓ %UserProfile%\AppData\Roaming\Microsoft\Windows\Start Menu

- 바탕화면

- ✓ %UserProfile%\Desktop

- 사용자의 내 음악(My Music), 내 그림(My Pictures), 내 비디오(My Videos) 폴더

- ✓ %UserProfile% → "%SystemDrive%\Users\Public" 하위 폴더 링크

- Send To 폴더

- ✓ %UserProfile%\AppData\Roaming\Microsoft\Windows\SendTo

- 빠른 실행 (Quick Launch) 폴더

- ✓ %UserProfile%\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch

- 바로가기 파일 저장 위치 (2/2)

- 최근 문서 (Recent)

- ✓ %UserProfile%\AppData\Roaming\Microsoft\Windows\Recent

- 응용프로그램 최근 문서 (순서는 레지스트리 MRU에 저장)

- ✓ **MS Office:** %UserProfile%\AppData\Roaming\Microsoft\Office\Recent

- ✓ **Hangul:** %UserProfile%\AppData\Roaming\HNC\Office\Recent

- ✓ ... ..

- 사용자 직접 생성

# 바로가기

## ■ 바로가기 파일 구조

- MS 포맷 문서 – [http://msdn.microsoft.com/en-us/library/dd871305\(v=prot.13\).aspx](http://msdn.microsoft.com/en-us/library/dd871305(v=prot.13).aspx)
- 바로가기 기본 구조

구조 이름	설명
<b>SHELL_LINK_HEADER</b> (default)	식별 정보, 타임스탬프, 선택적인 구조의 존재 유무 플래그
<b>LINKTARGET_IDLIST</b> (optional)	ShellLinkHeader의 HasLinkTargetIDList 플래그가 설정되어 있을때만 존재하는 구조로, 링크 대상의 다양한 정보를 리스트 형태로 구성해놓은 구조
<b>LINKINFO</b> (optional)	ShellLinkHeader의 HasLinkInfo 플래그가 설정되어 있을때만 존재하는 구조로 링크 대상을 참조하기 위한 정보를 가진 구조
<b>STRING_DATA</b> (optional)	링크 대상의 문자열 정보(이름, 상대경로, 작업디렉터리 등)를 저장하는 구조로 ShellLinkHeader에 관련된 플래그가 설정되어 있을 때만 존재
<b>EXTRA_DATA</b> (optional)	링크 대상의 화면 표시 정보, 문자열 코드페이지, 환경 변수와 같은 추가적인 정보 저장을 위한 구조

## ■ 바로가기 파일 구조

### • SHELL\_LINK\_HEADER

범위	크기	이름	설명
0 – 3	4 bytes	HeaderSize	헤더의 크기로 항상 0x0000004C(76) 값
4 – 19	16 bytes	LinkCLSID	클래스 식별자로 항상 00021401-0000-0000-C000-000000000046 값 (고정값)
20 – 23	4 bytes	LinkFlags	링크 대상의 다양한 정보에 대한 플래그
24 – 27	4 bytes	FileAttributes	링크 대상의 파일 속성 정보
28 – 35	8 bytes	CreationTime	링크 대상의 생성 시간
36 – 43	8 bytes	AccessTime	링크 대상의 접근 시간
44 – 51	8 bytes	WriteTime	링크 대상의 쓰기 시간
52 – 55	4 bytes	FileSize	링크 대상의 크기
56 – 59	4 bytes	IconIndex	아이콘 인덱스
60 – 63	4 bytes	ShowCommand	링크가 실행될 때 응용프로그램 동작 모드
64 – 65	2 bytes	HotKey	응용프로그램을 바로 실행하기 위한 키보드 조합(핫키 정보)
66 – 75	10 bytes	Reserved	예약된 영역 (항상 0)

# 바로가기

## ▪ 바로가기 파일 구조

### • LINKTARGET\_IDLIST

✓ 링크 대상의 정보를 리스트 형태로 구성해 놓은 구조

### • IDList

✓ ItemIDSize

✓ Data

struct LinkTargetIDList sLinkTargetIDList	
WORD IDListSize	387
struct IDList sIDList[0]	CLSID_MyComputer
WORD ItemIDSize	20
BYTE Type	31
BYTE Unknown	80 'P'
▷ BYTE GUID[16]	àOÐ éi+çØ
struct IDList sIDList[1]	
WORD ItemIDSize	25
▷ BYTE Data[23]	/C:\
▷ struct IDList sIDList[2]	
▷ struct IDList sIDList[3]	
▷ struct IDList sIDList[4]	
WORD TerminalID	0

## ▪ 바로가기 파일 구조

### • LINKINFO

범위	크기	이름	설명
0 – 3	4 bytes	LinkInfoSize	LinkInfo 구조체 크기
4 – 7	4 bytes	LinkInfoHeaderSize	LinkInfo Header section 크기, 보통 0x0000001C (28)
8 – 11	4 bytes	LinkInfoFlags	LinkInfo 플래그, 좌측 2비트만 사용
12 – 15	4 bytes	VolumeIDOffset	VolumeID 위치
16 – 19	4 bytes	LocalBasePathOffset	LocalBasePath 위치 (링크 대상 경로)
20 – 23	4 bytes	CommonNetworkRelativeLinkOffset	Network volume info 위치
24 - 27	4 bytes	CommonPathSuffixOffset	CommonPathSuffix 위치
...	...	...	...

# 바로가기

## ▪ 바로가기 파일 구조

### • LINKINFO → Volume ID

범위	크기	이름	설명
0 – 3	4 bytes	VolumeIDSize	VolumeID 크기
4 – 7	4 bytes	DriveType	드라이브 형식 (이동형, 고정형, 네트워크 드라이브, CD-ROM, RAM Disk)
8 – 11	4 bytes	DriveSerialNumber	드라이브 시리얼 번호
12 – 15	4 bytes	VolumeLabelOffset	볼륨 레이블 위치
16 – 19	4 bytes	VolumeLabelOffsetUnicode	볼륨 레이블 위치 (유니코드)
20 -	가변	VolumeLabel	볼륨 레이블



- 바로가기 파일 구조

- **STRING\_DATA**

- ✓ 바로가기 설명, 링크 대상까지의 상대 경로, 바로가기 활성화 시 작업 디렉터리 위치 저장

- **EXTRA\_DATA**

- ✓ 콘솔에서 실행될 경우 디스플레이 설정 값
- ✓ 코드 페이지 정보
- ✓ 환경 변수 정보
- ✓ 아이콘 위치 주소
- ✓ NetBIOS 이름
- ✓ MAC 주소
- ✓ ...

# 바로가기

- 바로가기 파일 포렌식적 의미

- **SHELL\_LINK\_HEADER**

- ✓ 링크 대상 파일의 속성 (읽기 전용, 숨긴 파일, 시스템, 볼륨 레이블, 암호화, 압축 등)
- ✓ 링크 대상 파일의 생성, 수정, 접근 시간, 크기

- **LINKINFO**

- ✓ 링크 대상 파일의 크기
- ✓ 링크 대상 파일이 위치한 드라이브 형식
- ✓ 링크 대상 파일이 위치한 드라이브 시리얼 번호
- ✓ 링크 대상 파일의 경로 ➔ 외장저장장치 흔적

- **EXTRA\_DATA**

- ✓ NetBIOS 이름
- ✓ MAC 주소

## ▪ 바로가기 파일 활용

- 자동 생성된 바로가기 파일을 이용해 **폴더나 파일의 실행 흔적 분석**
- 링크 대상의 위치를 이용해 외장저장장치를 이용한 **데이터 이동 흔적 분석**
- 애플리케이션 취약점을 악용하는 악성코드일 경우, **실행 흔적 분석**
- 바로가기 파일 자체로 침해를 확인하기는 어렵기 때문에 **타임라인 분석과 연계 분석**

- 바로가기 파일 분석 도구

- **UFTLnkParser** – Ultimate Forensic Tool

- ✓ <http://forensic-proof.com/resources>

- **Windows LNK Parsing Utility (lp)** – TZWorks

- ✓ [https://www.tzworks.net/prototype\\_page.php?proto\\_id=11](https://www.tzworks.net/prototype_page.php?proto_id=11)

- **Lnkanalyser** – Mark Woan

- ✓ <http://www.woanware.co.uk/forensics/lnkanalyser.html>

## ➔ 실습

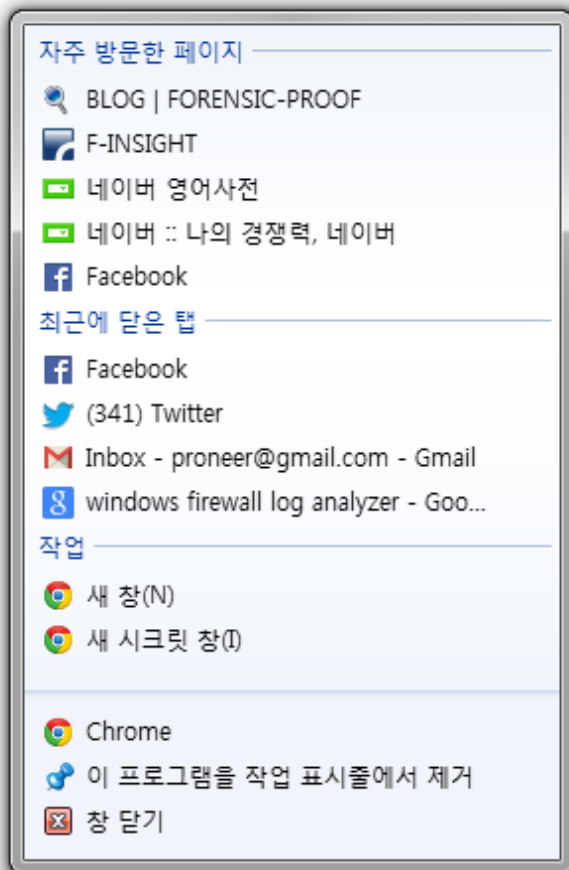
- 010Editor를 이용해 바로가기 파일 포맷 분석하기!!
- 라이브 볼륨에서 바로가기 파일 분석 하기!!
  - ✓ 정상 바로가기 파일 추출
  - ✓ 삭제된 바로가기 파일 복구

# 점프 목록

# 점프 목록

## ■ 점프 목록이란?

- 윈도우 7부터 새롭게 추가된 응용프로그램 사용 로그로 기본 활성화
- 모든 응용프로그램에 대한 접근 이력 보관



# 점프 목록

## ■ 점프 목록 설정

### • [제어판] → [작업표시줄 및 시작메뉴]

### • 첫 번째 체크박스

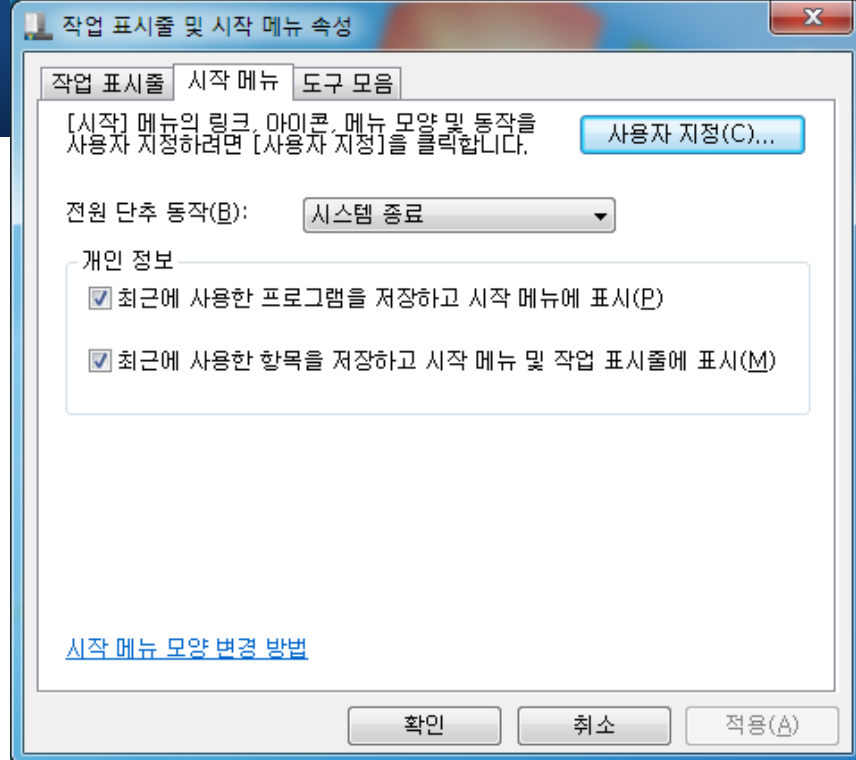
- ✓ 최근 사용한 프로그램 시작 메뉴에 표시 여부
- ✓ 체크 해제한 후 적용 → 시작 메뉴 항목 제거

### • 두 번째 체크박스

- ✓ 점프 목록에 관한 설정
- ✓ 체크 해제한 후 적용을 누르면 이전에 기록된 모든 점프 목록 삭제
- ✓ 고정된(pinned) 점프 목록은 삭제되지 않음

### • 사용자 지정 버튼

- ✓ 시작 메뉴와 점프 목록에 지정할 프로그램 지정이나 목록 수 설정








## ■ 점프 목록 경로

- %UserProfile%\AppData\Roaming\Microsoft\Windows\Recent\

Users\pr0neer\AppData\Roaming\Microsoft\Windows\Recent								5 hours
Filename ^	Ext.	Size	Created	Modified	Accessed	Attr.	ID	
..								
AutomaticDestinations		8.2 KB	12/09/2...	06/20/2...	06/20/20...		16404	
CustomDestinations		8.2 KB	12/09/2...	06/28/2...	06/28/20...		16350	
#1.Ink	Ink	474 bytes	06/20/2...	06/20/2...	06/20/20...	A	214865	
#7 Resume.Ink	Ink	0.5 KB	06/20/2...	06/24/2...	06/24/20...	A	226305	
[#1] 1일차 (레지스트리, 파일 시스템, 파일 복구).Ink	Ink	0.8 KB	06/20/2...	06/20/2...	06/20/20...	A	227446	
[#1] 1일차.Ink	Ink	0.7 KB	06/20/2...	06/27/2...	06/27/20...	A	41141	
[#10-1] OS Artifacts - Event Logs.pptx.Ink	Ink	1.1 KB	06/27/2...	06/27/2...	06/27/20...	A	213929	
[#2-6] File System Forensic Analysis.pdf.Ink	Ink	0.9 KB	06/21/2...	06/21/2...	06/21/20...	A	214837	
[#2-7] Data Recovery Techniques.pdf.Ink	Ink	0.9 KB	06/21/2...	06/21/2...	06/21/20...	A	219680	
[#2] 2일차.Ink	Ink	0.7 KB	06/20/2...	06/28/2...	06/28/20...	A	57701	
[#3-1] File System Forensic Analysis.pdf.Ink	Ink	0.9 KB	06/22/2...	06/22/2...	06/22/20...	A	239334	
[#3-2] Data Recovery Techniques.pdf.Ink	Ink	0.9 KB	06/22/2...	06/22/2...	06/22/20...	A	243716	
[#3-3] Windows 7 File System.pdf.Ink	Ink	0.9 KB	06/22/2...	06/22/2...	06/22/20...	A	215444	
[#3-4] Windows 7 Folder Structure.pdf.Ink	Ink	0.9 KB	06/22/2...	06/22/2...	06/22/20...	A	241208	
[#3-5] OS Artifacts - Prefetch & Superfetch.pptx.Ink	Ink	1.0 KB	06/27/2...	06/27/2...	06/27/20...	A	214426	
[#3-5] OS Artifacts - Prefetch, Superfetch, ReadyBoost.pptx.Ink	Ink	1.0 KB	06/27/2...	06/27/2...	06/27/20...	A	216571	
[#3-5] Windows 7 Artifacts.pptx.Ink	Ink	0.9 KB	06/27/2...	06/27/2...	06/27/20...	A	214003	
[#3] 3일차.Ink	Ink	0.7 KB	06/21/2...	06/27/2...	06/27/20...	A	58175	
[#9-2] OS Artifacts - Shortcut(LNK).pptx.Ink	Ink	1.1 KB	06/27/2...	06/27/2...	06/27/20...	A	89764	
[#FP] Data Recovery Techniques.pdf.Ink	Ink	1.8 KB	06/27/2...	06/27/2...	06/27/20...	A	243912	

# 점프 목록

## ■ 점프 목록 경로

\Users\pr0neer\AppData\Roaming\Microsoft\Windows\Recent							5 hours
Filename ^-^	Ext.	Size	Created	Modified	Accessed	Attr.	ID
 ..							
<input type="checkbox"/>  AutomaticDestinations		8.2 KB	12/09/2...	06/20/2...	06/20/20...		16404
<input type="checkbox"/>  CustomDestinations		8.2 KB	12/09/2	06/28/2	06/28/20		16350

### • AutomaticDestinations

- ✓ 운영체제가 자동으로 남기는 항목
- ✓ 최근 사용한 목록(Recent)이나 자주 사용되는 목록(Frequent)


### • CustomDestinations


- ✓ 응용프로그램이 자체적으로 관리하는 항목
- ✓ 작업(Task) 목록

# 점프 목록

## ■ 점프 목록 파일명

- 각 응용프로그램 별로 고유한 16자리 사용
  - ✓ [http://www.forensicswiki.org/wiki/List\\_of\\_Jump\\_List\\_IDs](http://www.forensicswiki.org/wiki/List_of_Jump_List_IDs)
  - ✓ <http://forensicartifacts.com/tag/jump-lists/>

\\Users\\pr0neer\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\AutomaticDestinations								
Filename ^ -	Ext	Size	Created	Modified	Accessed	Attr.	ID	
								
<input type="checkbox"/> 12dc1ea8e34b5a6.automaticDestinations-ms	autom	53.0 KB	06/15/2...	06/22/2...	06/15/20...	A	61095	
<input type="checkbox"/> 1b4dd67f29cb1962.automaticDestinations-ms	autom	83.1 KB	06/15/2...	06/28/2...	06/15/20...	A	58662	
<input type="checkbox"/> 20f18d57e149e379.automaticDestinations-ms	autom	8.0 KB	06/15/2...	06/25/2...	06/15/20...	A	59221	
<input type="checkbox"/> 2d61cccb4338dfc8.automaticDestinations-ms	autom	17.0 KB	06/18/2...	06/26/2...	06/18/20...	A	210248	
<input type="checkbox"/> 44a3621b32122d64.automaticDestinations-ms	autom	4.0 KB	06/15/2...	06/19/2...	06/15/20...	A	58696	
<input type="checkbox"/> 458f7bc92ebd65ec.automaticDestinations-ms	autom	4.5 KB	06/15/2...	06/27/2...	06/15/20...	A	62186	
<input type="checkbox"/> 4d8bdacf5265a04f.automaticDestinations-ms	autom	31.0 KB	06/15/2...	06/27/2...	06/15/20...	A	92035	

\\Users\\pr0neer\\AppData\\Roaming\\Microsoft\\Windows\\Recent\\CustomDestinations								
Filename ^ -	Ext	Size	Created	Modified	Accessed	Attr.	ID	
								
<input type="checkbox"/> 28c8b86deab549a1.customDestinations-ms	custon	6.3 KB	12/09/2...	06/27/2...	06/27/20...	A	218887	
<input type="checkbox"/> 29db278f507c92bb.customDestinations-ms	custon	3.7 KB	02/07/2...	06/15/2...	06/15/20...	A	16196	
<input type="checkbox"/> 337ed59af273c758.customDestinations-ms	custon	1.6 KB	06/20/2...	06/20/2...	06/20/20...	A	89006	
<input type="checkbox"/> 5afe4de1b92fc382.customDestinations-ms	custon	18.3 KB	12/09/2...	06/15/2...	06/15/20...	A	16353	
<input type="checkbox"/> 5d696d521de238c3.customDestinations-ms	custon	23.3 KB	12/09/2...	06/28/2...	06/28/20...	A	190438	
<input type="checkbox"/> 5d6f13ed567aa2da.customDestinations-ms	custon	8.8 KB	12/10/2...	06/15/2...	06/15/20...	A	16531	
<input type="checkbox"/> 5df4765359170e26.customDestinations-ms	custon	5.6 KB	05/19/2...	06/15/2...	06/15/20...	A	16533	

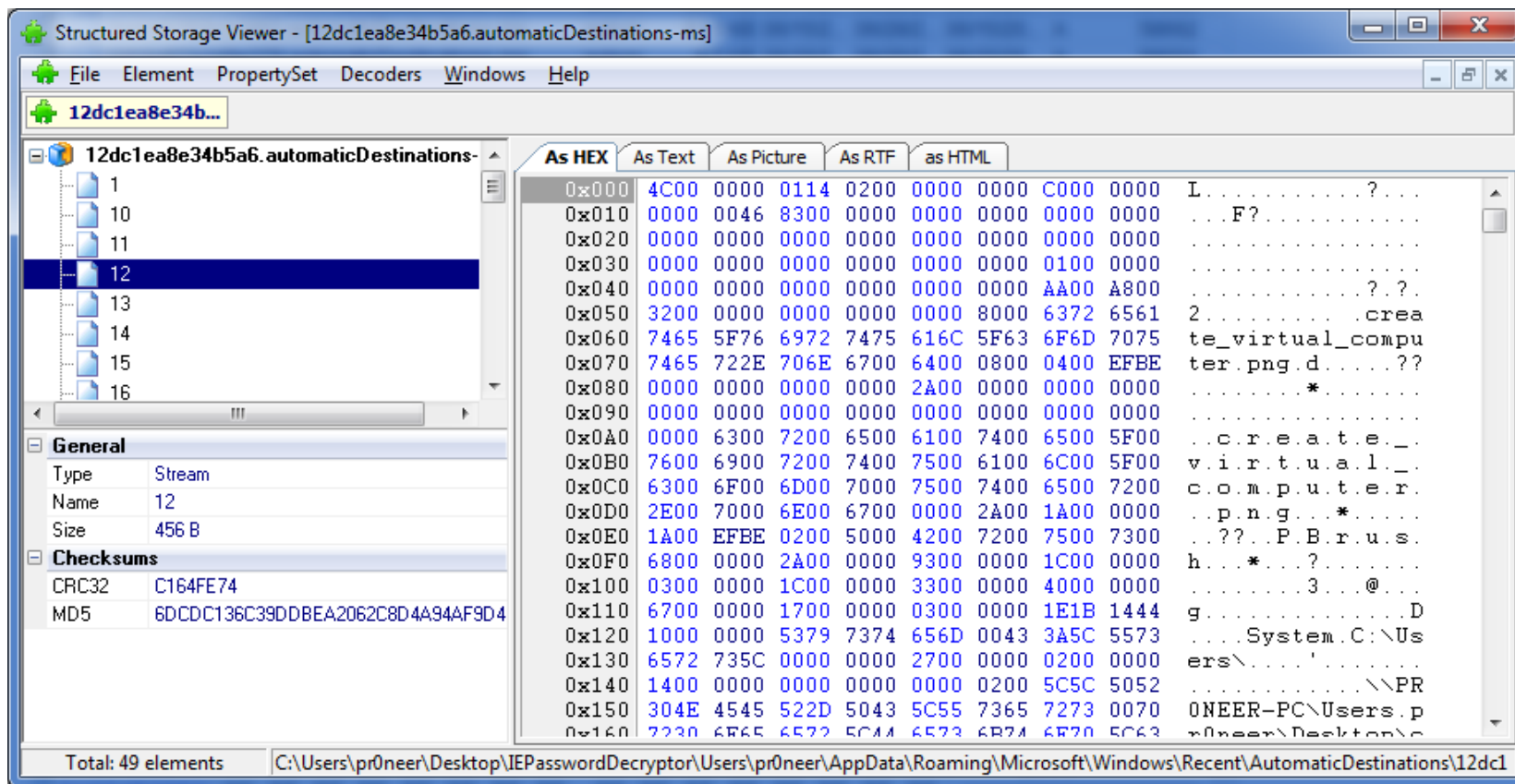
## ■ 점프 목록 파일명

응용프로그램	App ID
Windows Explorer	1b4dd67f29cb1962
Microsoft Word 2003	a8c43ef36da523b1
Microsoft Word 2007	adecfb853d77462a
Microsoft Word 2010	44a3621b32122d64
Internet Explorer 8	28c8b86deab549a1
Notepad	918e0ecb43d17e23
Microsoft Powerpoint 2007	f5ac5390b9115fdb
Adobe Reader 8, 9	23646679aaccfae0
Adobe Acrobat 8 Professional	6807f6e0bc8d4ca7
Paint 6.1	12dc1ea8e34b5a6
Firefox	5c450709f7ae4396
Media Center	b91050d8b077a4e8
Windows Live Mail	d7528034b5bd6f28
Hanword (HWP) 2010	20f18d57e149e379
Gom Audio	458f7bc92ebd65ec
KMPlayer	4d8bdacf5265a04f

# 점프 목록

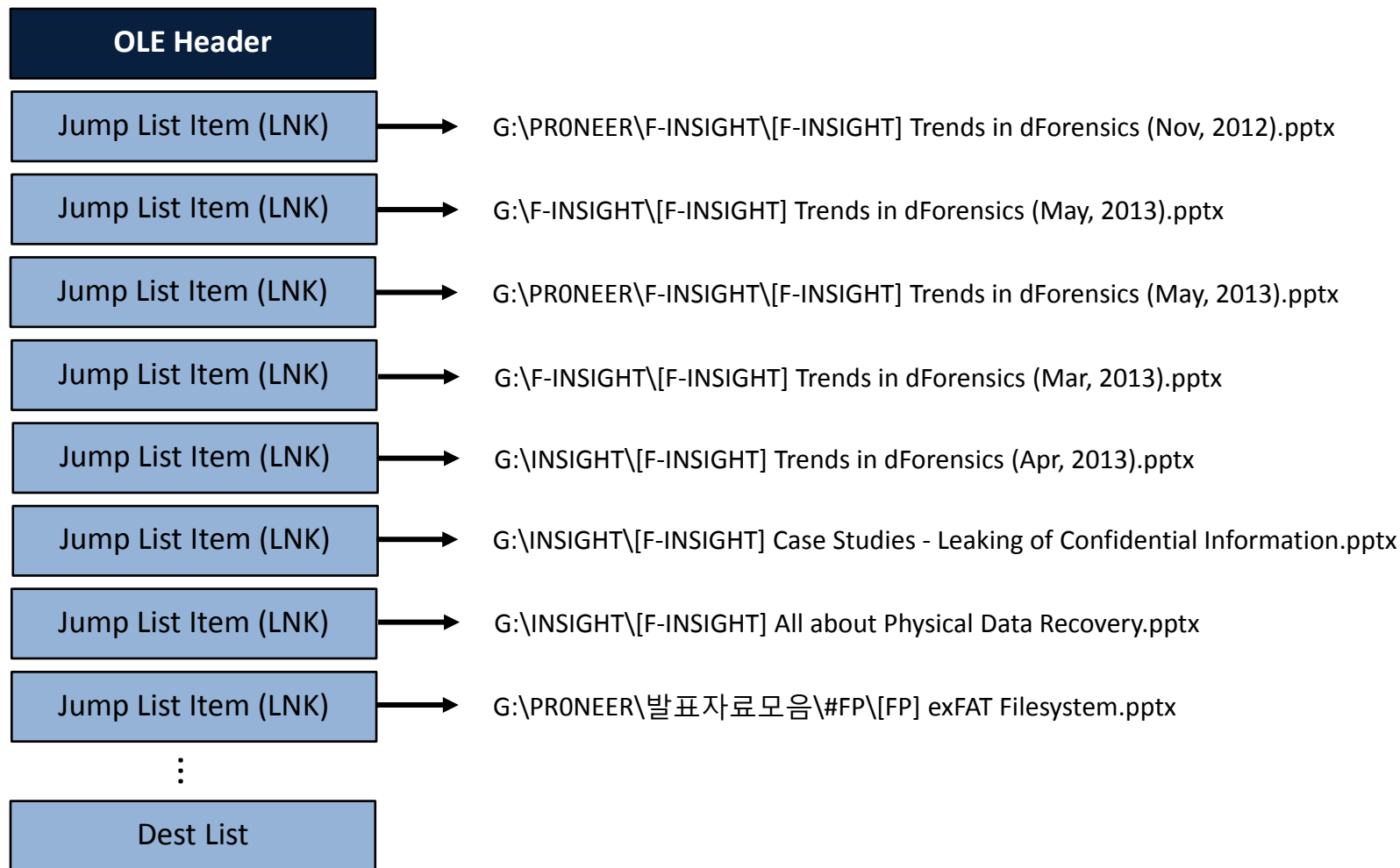
## ■ 점프 목록 파일 구조

- OLE 복합문서(Compound) 파일 구조를 사용
- 점프 목록 각 아이템을 OLE 스트림(바로가기 파일)으로 저장



# 점프 목록

## ■ 점프 목록 파일 구조



# 점프 목록

## ■ 점프 목록 획득 가능한 정보

- 복합문서 구조의 스트림에 바로가기 파일 형식으로 점프목록 저장
- 바로가기 파일에서 획득 가능한 모든 정보
  - ✓ 링크 대상의 속성, 크기, 경로, (생성, 수정, 접근) 시간
  - ✓ 링크 대상이 위치한 곳의 드라이브의 형식, 시리얼 번호, NetBIOS 이름, MAC 주소

DestList Date/Time	DestList Data	Created Timestamp	Drive Type	Serial No.
2012-08-02 오전 8:13:15	C:\Users\기본\Desktop\해버리기부본서\기본서\기본서\기본서\기본서\기본서	2012년 3월 19일 월요일 오전 4:40:10	DRIVE_FIXED	462D6E3A
2012-08-02 오전 8:13:38	검색 결과&보증	0001년 1월 1일 월요일 오전 12:00:00		
2012-08-06 오전 6:00:31	검색 결과&특허	0001년 1월 1일 월요일 오전 12:00:00		
2012-08-06 오전 6:05:10	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:59:50	DRIVE_FIXED	462D6E3A
2012-08-07 오전 12:51:28	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 7월 26일 목요일 오전 5:18:34	DRIVE_FIXED	462D6E3A
2012-08-07 오전 4:16:09	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 6월 7일 목요일 오전 12:56:55	DRIVE_FIXED	462D6E3A
2012-08-07 오전 7:36:14	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:58:19	DRIVE_FIXED	462D6E3A
2012-08-07 오전 7:50:44	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:58:06	DRIVE_FIXED	462D6E3A
2012-08-07 오전 8:02:05	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:59:46	DRIVE_FIXED	462D6E3A
2012-08-08 오전 5:28:32	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:30:18	DRIVE_FIXED	462D6E3A
2012-08-08 오전 5:31:04	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:30:10	DRIVE_FIXED	462D6E3A
2012-08-08 오전 5:32:02	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:30:07	DRIVE_FIXED	462D6E3A
2012-08-08 오전 5:32:32	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:30:08	DRIVE_FIXED	462D6E3A
2012-08-08 오전 5:32:52	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:30:17	DRIVE_FIXED	462D6E3A
2012-08-08 오전 5:33:11	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:30:11	DRIVE_FIXED	462D6E3A
2012-08-08 오전 5:33:31	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:30:06	DRIVE_FIXED	462D6E3A
2012-08-08 오전 6:14:40	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 1:10:43	DRIVE_FIXED	462D6E3A
2012-08-09 오전 2:40:34	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:54:15	DRIVE_FIXED	462D6E3A
2012-08-09 오전 2:51:08	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:59:50	DRIVE_FIXED	462D6E3A
2012-08-09 오전 4:43:44	C:\Users\기본\Desktop\유제비리기부본서\기본서\기본서\기본서\기본서	2012년 3월 2일 금요일 오전 12:57:52	DRIVE_FIXED	462D6E3A

## ■ 점프 목록 활용

- 윈도우 7 기본 활성화
- 최근 접근 문서(Recent)나 UserAssist 키보다 더 많은 정보 포함
- 사용자가 직접 삭제하지 않는 이상 운영체제 설치 시부터 지속적으로 로그 저장
- 악성 파일 실행 흔적
- 외장저장장치 파일 열람 흔적
- 웹 사이트 접속 이력



- 점프 목록 분석 도구

- **Jumplist Parser (jp)** – Plainbit

- **JumpLister** – Mark Woan

- ✓ <http://www.woanware.co.uk/forensics/jumplister.html>

- **JumpListsView** – NirSoft

- ✓ [http://nirsoft.net/utils/jump\\_lists\\_view.html](http://nirsoft.net/utils/jump_lists_view.html)

- **Windows Jump List Parser (jmp)** – TZWorks

- ✓ [https://tzworks.net/prototype\\_page.php?proto\\_id=20](https://tzworks.net/prototype_page.php?proto_id=20)

## ➔ 실습

- 라이브 환경에서 점프 목록 분석하기!!

# 레지스트리

## ■ 레지스트리란?

### • 윈도우 레지스트리 (Windows Registry)

- ✓ 윈도우 운영체제에서 운영체제와 응용프로그램 운영에 필요한 정보를 저장하기 위해 고안한 계층형 데이터베이스 (<http://support.microsoft.com/kb/256986>)
- ✓ 부팅 과정부터 로그인, 서비스 실행, 응용프로그램 실행, 사용자 행위 등 모든 활동에 관여함
- ✓ 윈도우 3.11, 9x, Me, NT, 2000, XP, 2003, Vista, 2008, 7, 2012, 8 에서 사용

### • 포렌식 분석의 필요성

- ✓ 윈도우 시스템 분석의 필수 요소
  - 운영체제 정보, 사용자 계정 정보, 시스템 정보, 응용프로그램 실행 흔적, 최근 접근 문서 등
  - 자동 실행 항목(Autoruns), 악성코드 탐지, 저장장치 연결 흔적 등
- ✓ 사용자/시스템/저장매체 사용 흔적 분석 ➔ 추가적인 포렌식 분석 대상 선별

# 레지스트리

- 하이브(Hive)

- 하이브 파일

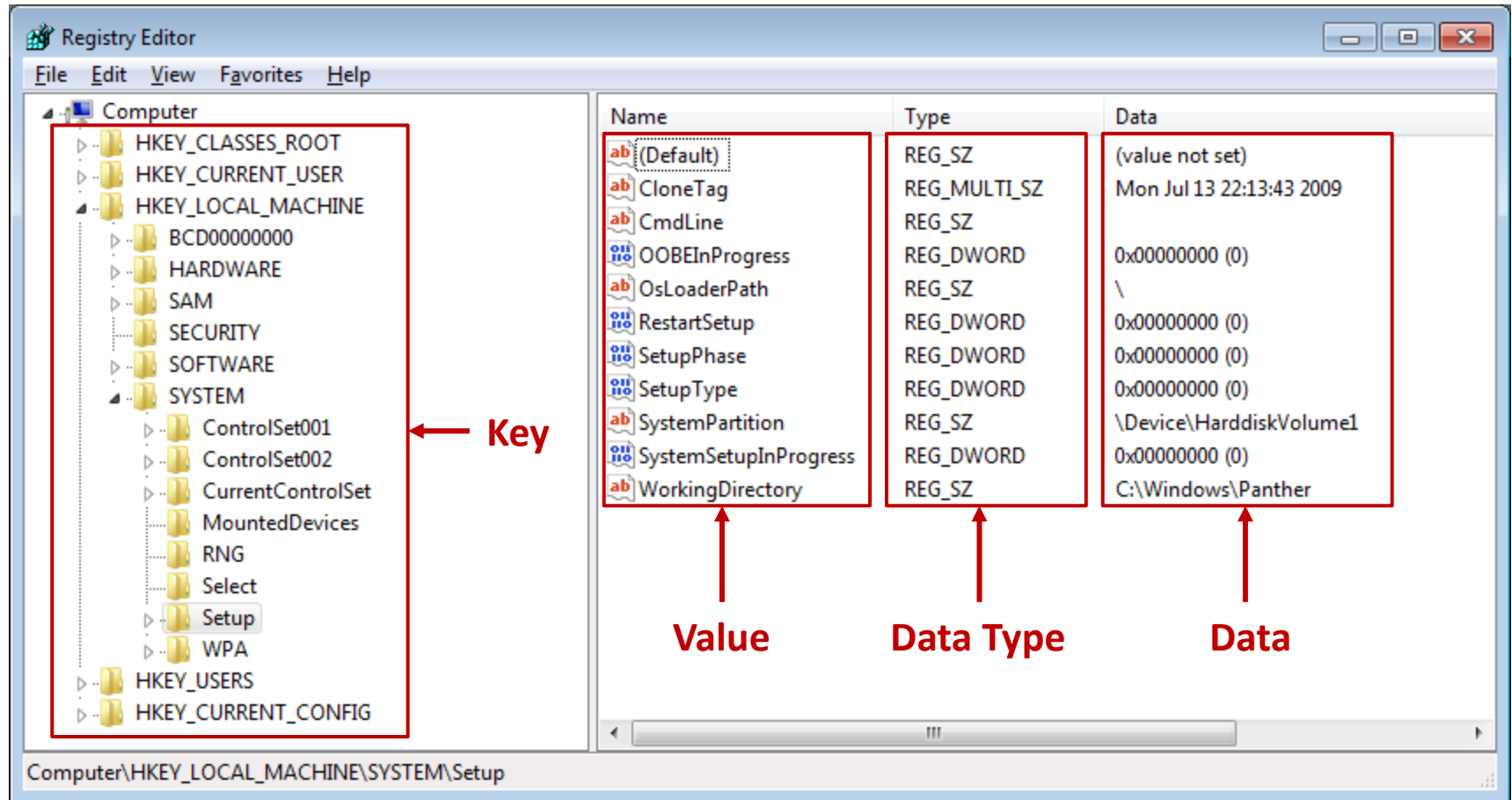
- ✓ 레지스트리 정보를 저장하고 있는 물리적인 파일
    - ✓ 키(Key) 값들이 논리적인 구조로 저장
    - ✓ 부팅 과정부터 커널에 의해 하이브 파일이 관리됨
      - 핸들이 열려있어 라이브 상태에서 수집하려면 별도의 도구 필요

- 하이브 셋

- ✓ 레지스트리 전체를 구성하는 하이브 파일 목록
    - ✓ SAM, SECURITY, SYSTEM, SOFTWARE, Default, NTUSER.DAT, UsrClass.dat, COMPONENTS 등

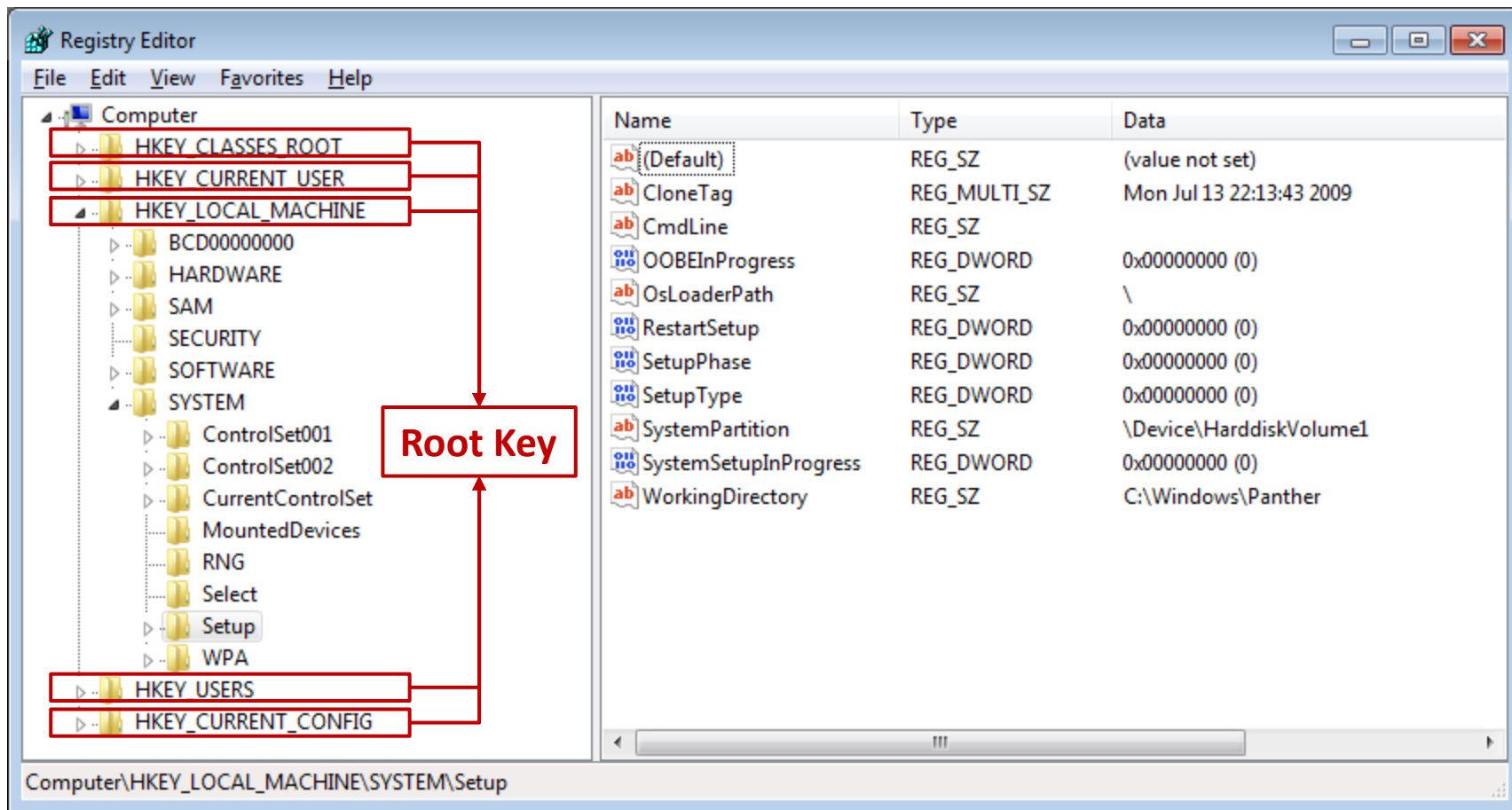
# 레지스트리

## ■ 데이터 구조



# 레지스트리

## 루트키



## 루트키 구성 정보

루트키	약어	설명
HKEY_CLASSES_ROOT	HKCR	HKLM\SOFTWARE\Classes와 HKU\<SID>\Classes 모음
HKEY_CURRENT_USER	HKCU	HKU 아래 사용자 프로파일 중 현재 로그인한 사용자의 하위키
HKEY_LOCAL_MACHINE	HKLM	시스템에 존재하는 하이브 파일과 메모리 하이브 모음
HKEY_USERS	HKU	사용자 루트 폴더에 존재하는 NTUSER.DAT 파일의 내용
HKEY_CURRENT_CONFIG	HKCC	HKLM\SYSTEM\CurrentControlSet\Hardware Profiles\Current의 내용
HKEY_PERFORMANCE_DATA	HKPD	성능 카운트(레지스트리 편집기를 통해 접근 불가, 레지스트리 함수로만 접근)

- "CURRENT"가 들어가는 루트키는 메모리에서만 유지
- "CLASSES\_ROOT"도 타 루트키가 링크된 가상 공간
- **실제 하이브 파일로 존재하는 루트키**
  - ✓ HKEY\_USERS → Default, NTUSER.DAT
  - ✓ HKEY\_LOCAL\_MACHINE → SAM, SECURITY, SYSTEM, SOFTWARE



# 레지스트리

## ■ 하이브 파일 경로

레지스트리 경로	하이브 파일 경로
HKEY_LOCAL_MACHINE\BCD00000000	{Boot Partition}\Boot\BCD
HEKY_LOCAL_MACHINE\COMPONENTS	%SystemRoot%\System32\Config\COMPONENTS
HEKY_LOCAL_MACHINE\SYSTEM	%SystemRoot%\System32\Config\SYSTEM
HEKY_LOCAL_MACHINE\SAM	%SystemRoot%\System32\Config\SAM
HEKY_LOCAL_MACHINE\SECURITY	%SystemRoot%\System32\Config\SECURITY
HEKY_LOCAL_MACHINE\SOFTWARE	%SystemRoot%\System32\Config\SOFTWARE
HEKY_LOCAL_MACHINE\HARDWARE	Volatile
HKEY_USERS\<SID of local service account>	%SystemRoot%\ServiceProfiles\LocalService\NTUSER.DAT
HKEY_USERS\<SID of network service account>	%SystemRoot%\ServiceProfiles\NetworkService\NTUSER.DAT
HKEY_USERS\<SID of username>	%UserProfile%\NTUSER.DAT
HKEY_USERS\<SID of username>_Classes	%UserProfile%\AppData\Local\Microsoft\Windows\Usrclass.dat
HKEY_USERS\.DEFAULT	%SystemRoot%\System32\Config\DEFAULT
HKEY_USERS\systemprofile	%SystemRoot%\System32\Config\systemprofile\NUSER.DAT

# 레지스트리

- 백업과 로그

- 레지스트리 파일 백업

- ✓ %SystemRoot%\System32\config\RegBack\

- 레지스트리 로그

- ✓ %SystemRoot%\System32\config\[hive name].LOG

- ✓ %SystemRoot%\System32\config\[hive name].LOG1

- ✓ %SystemRoot%\System32\config\[hive name].LOG2

- 백업이나 로그도 동일한 하이브 구조를 가짐

# 레지스트리

## ■ 볼륨 새도 복사본

### • VSS (Volume Shadow Copy)의 레지스트리 스냅샷

- ✓ 비스타 이후부터는 시스템 복원 지점을 위해 VSS 사용
- ✓ 특정 시점에 파일, 폴더에 대한 스냅샷 저장
- ✓ \System Volume Information\

\System Volume Information			
Name	Ext.	Size	Created
..			
SPP		4.1 KB	12/09/2010 15:0...
Windows Backup		152 B	12/20/2010 14:5...
{3808876b-c176-4e48-b7ae-04046e6cc752}		64.0 KB	12/09/2010 15:0...
{3904f4ac-2567-11e0-bad1-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		337 MB	01/22/2011 01:2...
{3904f503-2567-11e0-bad1-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.4 GB	01/22/2011 03:3...
{39ff4f77-29c5-11e0-8489-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.7 GB	01/28/2011 03:0...
{6b2bdddf-2931-11e0-9b4e-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		221 MB	01/26/2011 18:5...
{6b2bddfb-2931-11e0-9b4e-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.1 GB	01/26/2011 19:2...
{6ec7ed76-2221-11e0-90cd-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		260 MB	01/18/2011 01:5...
{7d153fec-22aa-11e0-ab33-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		436 MB	01/18/2011 12:5...
{93503091-1f74-11e0-9f30-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		217 MB	01/15/2011 03:4...
{93503095-1f74-11e0-9f30-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.3 GB	01/15/2011 03:5...
{9b592008-22f5-11e0-a0c9-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		305 MB	01/18/2011 20:3...
{9b5920a0-22f5-11e0-a0c9-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		1.4 GB	01/19/2011 03:0...
{e2b5df93-1f1f-11e0-981b-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		304 MB	01/14/2011 00:4...
{e2b5dfc2-1f1f-11e0-981b-005056c00008}{3808876b-c176-4e48-b7ae-04046e6cc752}		440 MB	01/14/2011 02:0...
LightningSand.CFD	CFD	29.4 KB	12/17/2010 13:1...
MountPointManagerRemoteDatabase		0 B	12/10/2010 07:5...
Syscache.hve	hve	8.8 MB	12/10/2010 07:5...
Syscache.hve.LOG1	LO...	256 KB	12/10/2010 07:5...
Syscache.hve.LOG2	LO...	0 B	12/10/2010 07:5...
tracking.log	log	20.0 KB	12/10/2010 07:5...

# 레지스트리

## ■ 침해 아티팩트

### • UserAssist

- ✓ NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\
- ✓ 응용프로그램 사용 로그 - 응용프로그램 종류, 최종 실행 시각, 실행 횟수 등 확인 가능
- ✓ <http://www.symantec.com/connect/forums/system-tool-malware-or-spyware>

User Account	Name	Type ▲	Last Execution Time (UTC+09:00)	Execution...	Session ID
forensic32	Microsoft.Windows.ControlPanel	CTLSESSION	none	0	0
forensic32	{F38BF404-1D43-42F2-9305-67DE0B28FC23}\explorer.exe	CTLSESSION	2013-07-25 14:39:25 Thu	3	0
forensic32	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\wmstsc.exe	CTLSESSION	2013-07-30 09:53:23 Tue	9	0
forensic32	\\Users\\forensic32\\Desktop\\xw_forensics16.7\\setup.exe	CTLSESSION	2013-01-11 15:09:02 Fri	0	0
forensic32	\\cft12\\CFT.exe	CTLSESSION	2013-01-11 18:06:17 Fri	0	0
forensic32	\\CFTLab\\CFTLab.exe	CTLSESSION	2013-01-29 18:03:06 Tue	0	0
forensic32	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\\cmd.exe	CTLSESSION	2013-08-01 00:11:56 Thu	28	0
forensic32	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\\taskmgr.exe	CTLSESSION	none	0	0
forensic32	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\\rundll32.exe	CTLSESSION	2013-07-31 15:10:05 Wed	2	0
forensic32	Microsoft.Windows.PhotoViewer	CTLSESSION	none	0	0
forensic32	{D65231B0-B2F1-4857-A4CE-A8E7C6EA7D27}\\NOTEPAD.EXE	CTLSESSION	2013-07-31 21:29:19 Wed	28	0
forensic32	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Internet Explorer\\explore.exe	CTLSESSION	2013-06-21 16:23:00 Fri	0	0
forensic32	Microsoft.InternetExplorer.Default	CTLSESSION	2013-07-27 17:28:04 Sat	2	0
forensic32	\\CFTLab\\CFTDiag.exe	CTLSESSION	2013-01-15 21:04:26 Tue	0	0
forensic32	\\Users\\forensic32\\Desktop\\리소스 측정 프로그램\\ToolMonitor.exe	CTLSESSION	2013-07-15 09:54:14 Mon	0	0
forensic32	Microsoft.Windows.Shell.RunDialog	CTLSESSION	none	0	0
forensic32	\\Users\\forensic32\\Desktop\\xw_forensics16.7\\xwforensics.exe	CTLSESSION	2013-02-13 17:36:18 Wed	0	0
forensic32	\\GetData.Mount.Image.Pro.v3.2.6\\GetData.Mount.Image.Pro.v3.2.6\\crack\\MIPGUI.exe	CTLSESSION	2013-01-23 10:25:23 Wed	0	0
forensic32	\\GetData.Mount.Image.Pro.v3.2.6\\GetData.Mount.Image.Pro.v3.2.6\\MIP-Setup.exe	CTLSESSION	2013-01-23 10:25:05 Wed	0	0
forensic32	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\GetData\\Mount Image Pro v3\\MIPGUI.exe	CTLSESSION	2013-03-26 16:06:31 Tue	0	0
forensic32	\\Users\\forensic32\\Desktop\\(1224)DATAForensics.exe	CTLSESSION	2013-06-21 16:27:18 Fri	0	0
forensic32	\\Users\\forensic32\\Desktop\\CFTLab\\CFTLab.exe	CTLSESSION	2013-01-23 10:35:53 Wed	0	0
forensic32	{7C5A40EF-A0FB-4BFC-874A-C0F2E0B9FA8E}\\Windows NT\\Accessories\\WORDPAD.EXE	CTLSESSION	2013-01-24 11:01:01 Thu	0	0
forensic32	\\run.exe	CTLSESSION	2013-01-29 19:05:59 Tue	0	0

- 침해 아티팩트

- MUICache

- ✓ UsrClass.dat\Software\Classes\LocalSettings\MuiCache\
- ✓ MUI (Multilingual User Interface) 다중 언어 지원을 위해 프로그램 이름 캐시
- ✓ 새로운 프로그램 실행 시, 자동으로 리소스 영역에서 프로그램 이름을 추출하여 저장
- ✓ [http://www.symantec.com/security\\_response/writeup.jsp?docid=2005-062609-2020-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2005-062609-2020-99&tabid=2)
- ✓ [http://www.symantec.com/security\\_response/writeup.jsp?docid=2012-032105-4929-99&tabid=2](http://www.symantec.com/security_response/writeup.jsp?docid=2012-032105-4929-99&tabid=2)
- ✓ <http://securityrepublic.blogspot.kr/2009/10/zbot.html>

# 레지스트리

- 침해 아티팩트

- LEGACY\_\*

- ✓ HKLM\System\ControlSet00#\Enum\Root\
- ✓ 악성코드가 직접 생성하기 보다는 실행 시 운영체제에 의해 생성되는 키
- ✓ 윈도우 서비스로 동작하는 악성코드 정보
- ✓ 레지스트리 키 마지막 수정 시간은 악성 서비스의 처음 실행 시간
- ✓ <http://www.threatexpert.com/report.aspx?md5=88dbcc682635b4013bcba5ad28bb976b>
- ✓ <http://www.threatexpert.com/report.aspx?md5=639e367974dea212fc97f06c2c7ea84d>

- 침해 아티팩트

- Tracing

- ✓ HKLM\SOFTWARE\Microsoft\Tracing
- ✓ 라우팅 및 원격 액세스(Routing and Remote Access) 서비스가 기록하는 추적정보
- ✓ 복잡한 네트워크 장애를 해결할 목적으로 저장
- ✓ [http://www.f-secure.com/v-descs/packed\\_w32\\_tibs\\_gu.shtml](http://www.f-secure.com/v-descs/packed_w32_tibs_gu.shtml)
- ✓ <http://forum.avast.com/index.php?topic=139648.10;wap2>
- ✓ [http://about-threats.trendmicro.com/malware.aspx?language=au&name=TROJ\\_ANOMALY.AU](http://about-threats.trendmicro.com/malware.aspx?language=au&name=TROJ_ANOMALY.AU)

- 침해 아티팩트

- 다양한 레지스트리 키, 값

- ✓ 악성코드 실행에 따라 다양한 레지스트리 값 생성
    - ✓ 동적 분석을 통해 발견한 레지스트리 지표를 이용해 악성코드 감염 식별
    - ✓ 타임라인 분석을 통해 악성코드 실행과 레지스트리 값 간의 관계 파악
    - ✓ [FP] 레지스트리 포렌식과 보안 – <http://forensic-proof.com/slides>



# 레지스트리

- 레지스트리 분석 도구

- **REGA** – DFRC

- ✓ <http://forensic.korea.ac.kr/tools/rega.html>

- **RegRipper** – Harlan Carvey

- ✓ <https://code.google.com/p/regripper/>

- **MUICacheView** – NirSoft

- ✓ [http://www.nirsoft.net/utils/muicache\\_view.html](http://www.nirsoft.net/utils/muicache_view.html)

- **UserAssistView** – NirSoft

- ✓ [http://www.nirsoft.net/utils/userassist\\_view.html](http://www.nirsoft.net/utils/userassist_view.html)

## ➔ 실습

- 라이브 시스템의 레지스트리 파일 분석하기!!
  - ✓ %SystemRoot%\System32\Config\DEFAULT
  - ✓ %SystemRoot%\System32\Config\SAM
  - ✓ %SystemRoot%\System32\Config\SECURITY
  - ✓ %SystemRoot%\System32\Config\SOFTWARE
  - ✓ %SystemRoot%\System32\Config\SYSTEM
  - ✓ %SystemRoot%\ServiceProfiles\LocalService\NTUSER.DAT
  - ✓ %SystemRoot%\ServiceProfiles\NetworkService\NTUSER.DAT
  - ✓ %SystemRoot%\System32\Config\systemprofile\NTUSER.DAT
  - ✓ %UserProfile%\NTUSER.DAT
  - ✓ %UserProfile%\AppData\Local\Microsoft\Windows\UsrClass.dat

# AV 로그

## ▪ AV 탐지 유형

- AV에서 탐지될 경우, 악성코드 유형에 따라 정밀 분석 필요
  - ✓ 바이러스 (Virus)
  - ✓ 웜 (Worm)
  - ✓ 트로이목마 (Trojan)
  - ✓ 백도어 (Backdoor)
  - ✓ 루트킷 (Rootkit)
  - ✓ 봇 (Bot)
  - ✓ 스파이웨어 (Spyware)
  - ✓ 애드웨어 (Adware)

## ■ AV 탐지 유형

- 탐지 로그 이외에 동작과 관련한 다양한 로그 포함

AhnLab V3 Lite

정밀 검사 PC 최적화 PC 관리 도구

이벤트 로그 **진단 로그** 검색소

모두 보기 2013-07-01 2013-07-31 전체: 23

날짜	진단명	대상	상태	검사 방법
2013-07-31 13:01:46	Win-Trojan/Siggen, 3276...	K:\xp-tdungan-c-drive.E01_NO...	치료 불가(치료 대상...	PC 실시간 검사
2013-07-31 13:01:45	Win-Trojan/Siggen, 3276...	K:\xp-tdungan-c-drive.E01_NO...	치료 가능(코드: 900)	PC 실시간 검사
2013-07-31 13:01:43	Win-Trojan/Siggen, 3276...	K:\xp-tdungan-c-drive.E01_NO...	치료 불가(치료 대상...	PC 실시간 검사
2013-07-31 13:01:43	Win-Trojan/Siggen, 3276...	K:\xp-tdungan-c-drive.E01_NO...	치료 가능(코드: 900)	PC 실시간 검사
2013-07-31 13:01:23	Win-Trojan/Siggen, 3276...	K:\xp-tdungan-c-drive.E01_NO...	치료 불가(치료 대상...	PC 실시간 검사
2013-07-31 13:01:23	Win-Trojan/Siggen, 3276...	K:\xp-tdungan-c-drive.E01_NO...	치료 가능(코드: 900)	PC 실시간 검사
2013-07-30 18:07:12	유해 사이트 접근 차단	blog.unmaskparasites.com/favi...	연결 차단(유해 사이...	웹 보안
2013-07-25 12:38:45	의심 파일 실행	j:\PROJECTS\forecopy\forec...	탐지	클라우드 평판...
2013-07-25 10:57:40	의심 파일 실행	j:\PROJECTS\forecopy\forec...	탐지	클라우드 평판...
2013-07-25 10:53:45	의심 파일 실행	j:\PROJECTS\forecopy\forec...	탐지	클라우드 평판...
2013-07-19 17:53:50	의심 파일 실행	c:\Users\FORENS~1\AppData...	탐지	클라우드 평판...
2013-07-16 21:21:29	의심 파일 실행	f:\DATA\Doctor\Smart Nebula.e...	탐지	클라우드 평판...
2013-07-16 19:11:52	유해 사이트 접근 차단	blog.unmaskparasites.com/favi...	연결 차단(유해 사이...	웹 보안
2013-07-16 19:11:06	유해 사이트 접근 차단	blog.unmaskparasites.com/favi...	연결 차단(유해 사이...	웹 보안
2013-07-16 13:50:39	의심 파일 실행	f:\DATA\Doctor\Smart Nebula.e...	탐지	클라우드 평판...
2013-07-09 18:32:05	유해 사이트 접근 차단	blog.unmaskparasites.com/favi...	연결 차단(유해 사이...	웹 보안

파일로 저장

## ▪ AV 별 로그 형식

### • 안랩 V3

✓ 로그 → (텍스트 인코딩 | 바이너리)

- %SystemDrive%\Program Files\AhnLab\[%ProductName%\log

✓ 검역소 → 바이너리

- %SystemDrive%\Program Files\AhnLab\[%ProductName%\Quarantine

### • 이스트소프트 알약 (AlYac)

✓ 로그 → 바이너리

- %SystemDrive%\ProgramData\ESTSoft\AlYac\log

✓ 검역소 → 바이너리

- %SystemDrive%\ProgramData\ESTSoft\AlYac\quarantine

## ■ AV 별 로그 형식

### • 윈도우 디펜더 (Windows Defender)

✓ 로그 → 이벤트 로그와 통합

✓ 검역소 → 바이너리

- %SystemDrive%\ProgramData\Microsoft\Windows Defender\Quarantine

### • 시만텍 엔드포인트 프로텍션 (SEP)

✓ 로그 → 텍스트 형식

- %SystemDrive%\Program Files\Symantec\Symantec Endpoint Protection\...

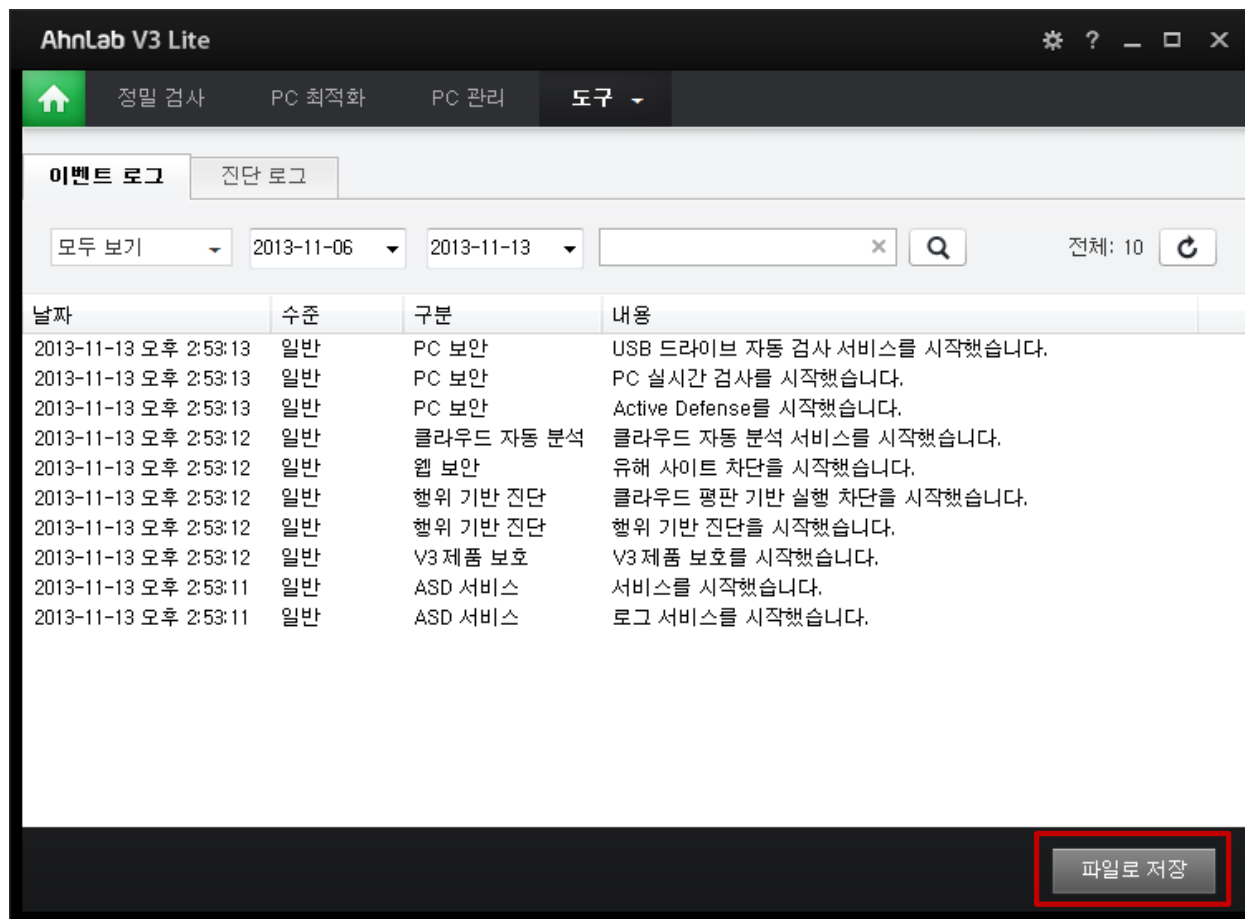
✓ 검역소 → 바이너리

- %SystemDrive%\Program Files\Symantec\Symantec Endpoint Protection\Quarantine

## ■ AV 로그 분석 방법

### • 라이브 수집 시

✓ AV에서 지원하는 “내보내기” 기능을 이용하여 텍스트로 로그 저장





## ▪ AV 로그 분석 방법

### • 오프라인 분석 시

#### ✓ 텍스트 로그 형식 (정형화)

- 텍스트 편집기나 별도의 스크립트를 이용해 분석

#### ✓ 텍스트 인코딩 형식

- 동일한 버전 설치 후 로그를 인젝션하여 분석

#### ✓ 바이너리 형식

- 동일한 버전 설치 후 바이너리 파일을 인젝션하여 분석

# 볼륨 새도 복사본

## ■ 볼륨 스냅샷 서비스

### • VSS (Volume Snapshot Service)

- ✓ 윈도우의 시스템 복원 기능으로 XP의 "시스템 복원 지점"이 Vista 이후 변화됨
- ✓ 특정 시각의 파일, 폴더 등을 수동 또는 자동으로 복사본(스냅샷)을 생성하는 서비스
- ✓ 윈도우 포렌식 분석의 필수 데이터!!!

### • VSS 목적

- ✓ 볼륨 백업본을 통해 시스템 복원 기능 제공 (이전 버전, 삭제된 파일 복구 등)
- ✓ 파일 잠금 문제 회피
  - 읽기 전용인 볼륨 새도 복사본으로 다른 파일의 쓰기 간섭을 회피

### • 볼륨 스냅샷 서비스 지원

- ✓ 윈도우 Server 2003/2008/2012
- ✓ 윈도우 Vista, 7, 8

# 볼륨 새도 복사본

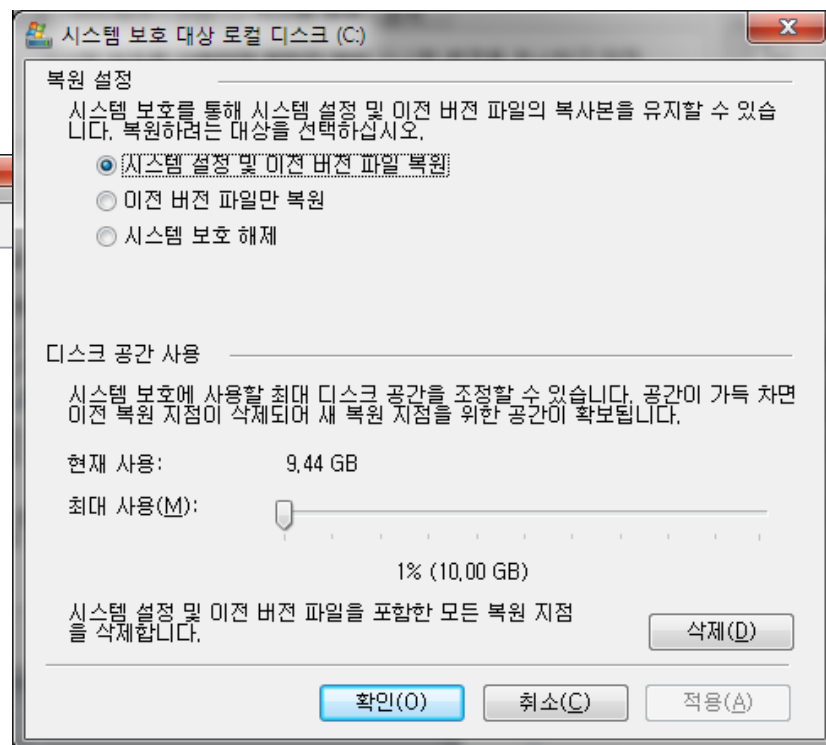
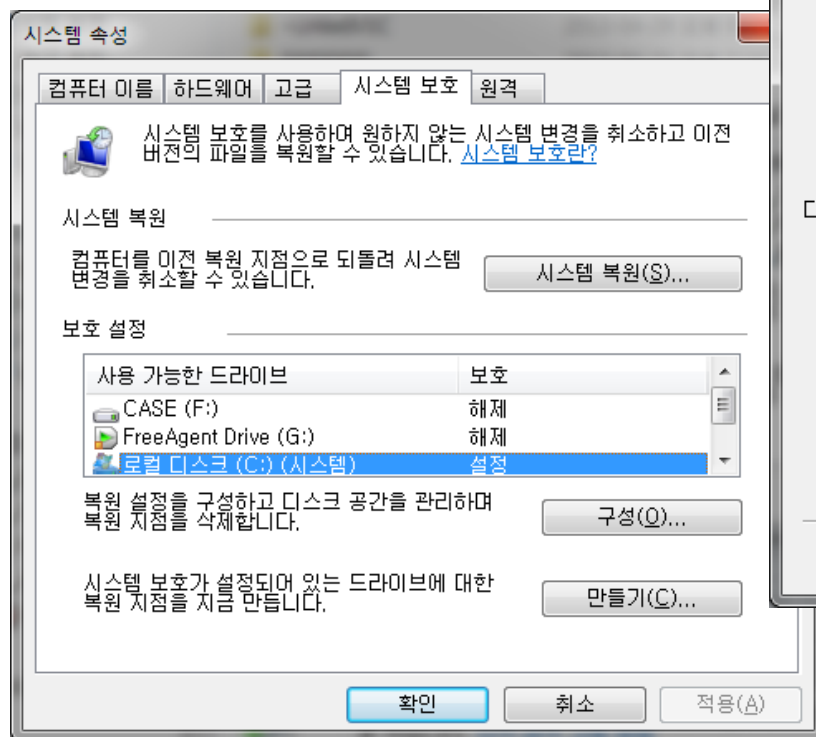
## ■ 볼륨 스냅샷 서비스 설정

### • 시스템 복원 설정

✓ [시스템 등록 정보] → [고급 시스템 설정] → [시스템 보호 탭]

✓ 시스템 볼륨은 기본 설정

✓ 나머지 볼륨은 사용자 정의

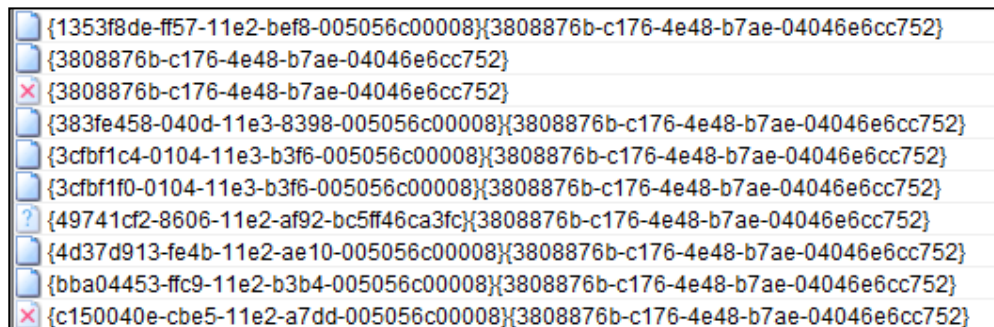


# 볼륨 새도 복사본

## ■ 볼륨 새도 복사본 관리

### • 볼륨 새도 복사본 저장 경로

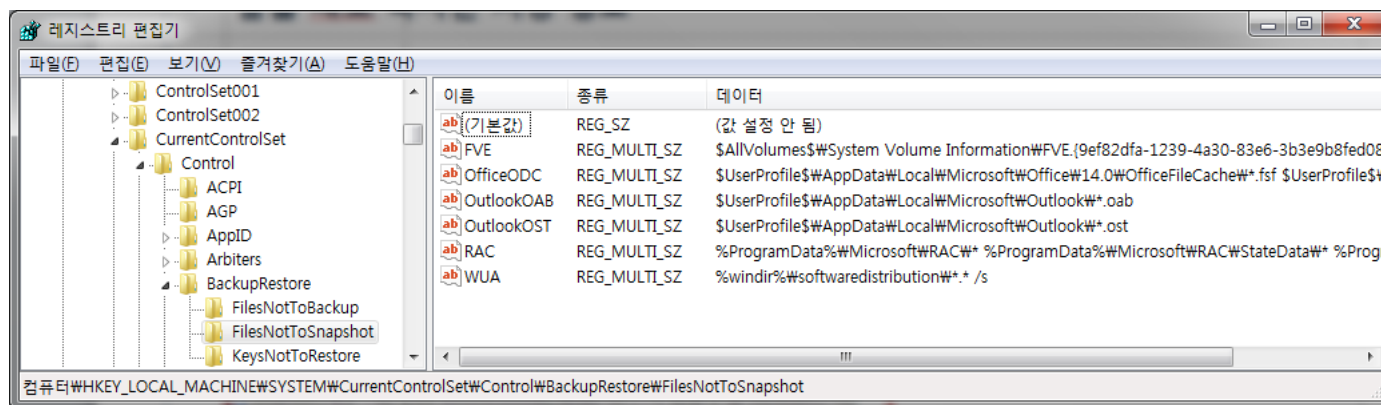
✓ %SystemDrive%\System Volume Information



{1353f8de-ff57-11e2-bef8-005056c00008}	{3808876b-c176-4e48-b7ae-04046e6cc752}
{3808876b-c176-4e48-b7ae-04046e6cc752}	{3808876b-c176-4e48-b7ae-04046e6cc752}
{383fe458-040d-11e3-8398-005056c00008}	{3808876b-c176-4e48-b7ae-04046e6cc752}
{3c8bf1c4-0104-11e3-b3f6-005056c00008}	{3808876b-c176-4e48-b7ae-04046e6cc752}
{3c8bf1f0-0104-11e3-b3f6-005056c00008}	{3808876b-c176-4e48-b7ae-04046e6cc752}
{49741cf2-8606-11e2-af92-bc5ff46ca3fc}	{3808876b-c176-4e48-b7ae-04046e6cc752}
{4d37d913-fe4b-11e2-ae10-005056c00008}	{3808876b-c176-4e48-b7ae-04046e6cc752}
{bba04453-ffc9-11e2-b3b4-005056c00008}	{3808876b-c176-4e48-b7ae-04046e6cc752}
{c150040e-cbe5-11e2-a7dd-005056c00008}	{3808876b-c176-4e48-b7ae-04046e6cc752}

### • 복사본 제외 파일 목록

✓ HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot

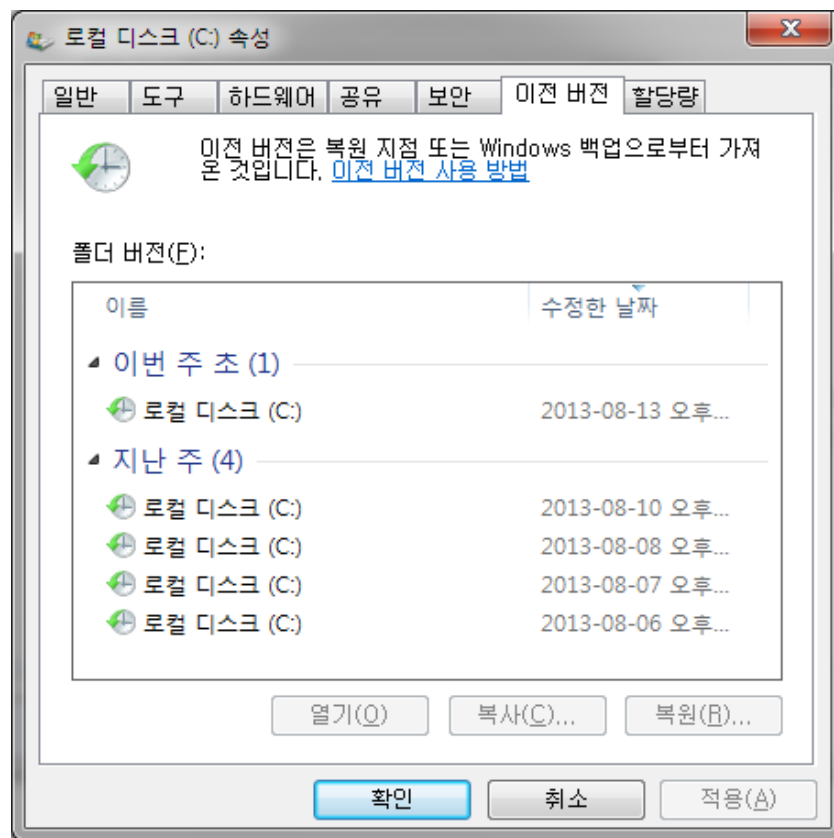


# 볼륨 새도 복사본

## ■ 볼륨 새도 복사본 생성

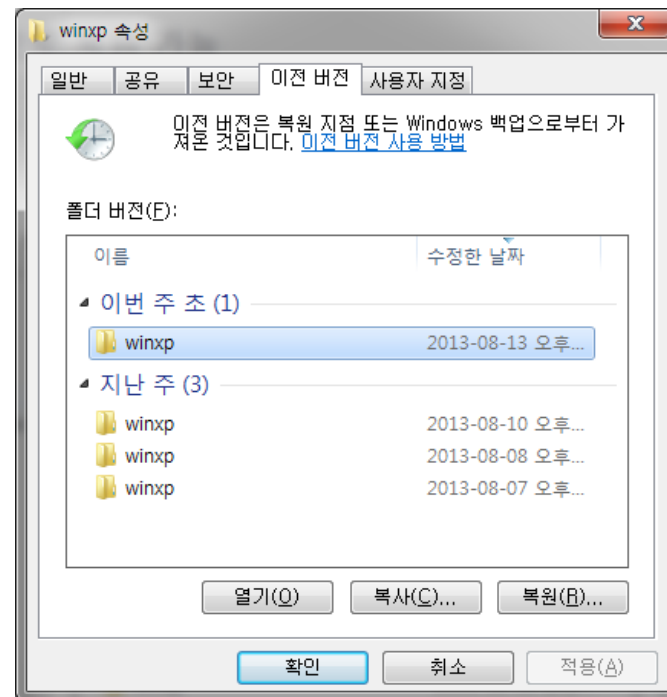
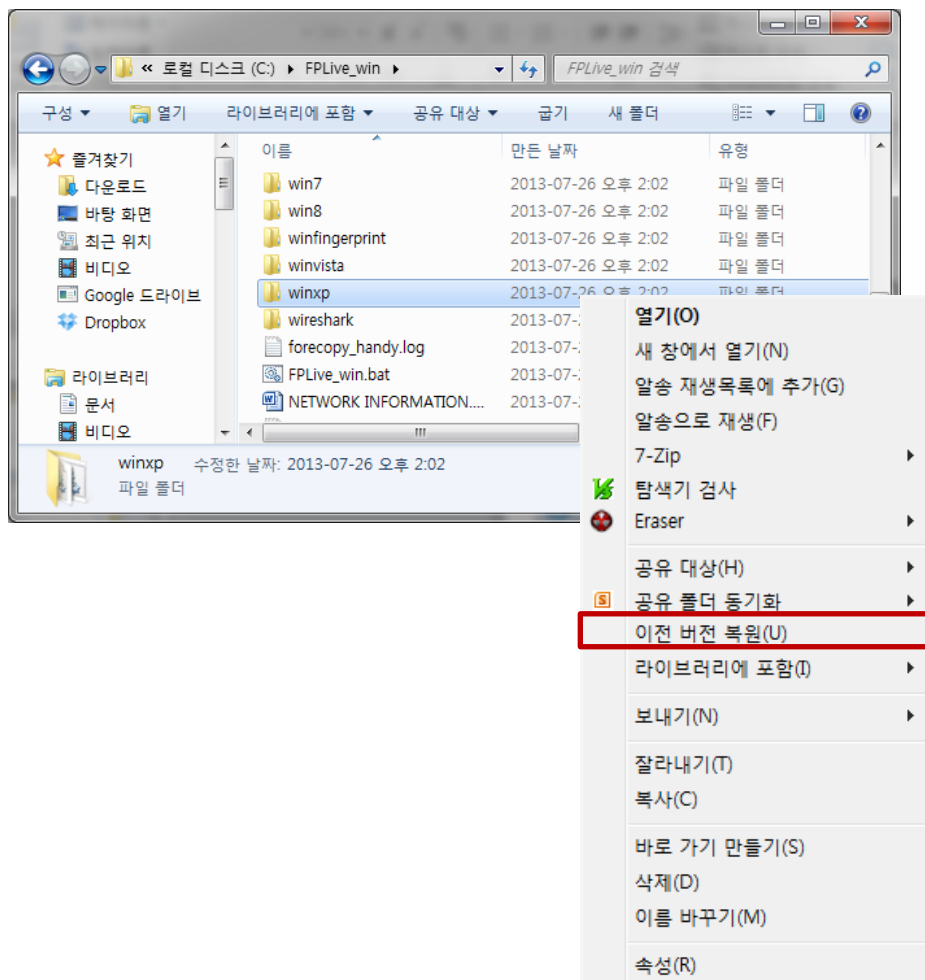
### • 볼륨 새도 복사본 생성 시점

- ✓ 수동 (Vista/7)
- ✓ 매 24시간 마다 (Vista)
- ✓ 매 7일 마다 (7)
- ✓ 윈도우 업데이트 전 (Vista/7)
- ✓ 서명되지 않은 드라이버 설치 시 (Vista/7)
- ✓ 프로그램에서 스냅샷 API 호출 시 (Vista/7)



# 볼륨 새도 복사본

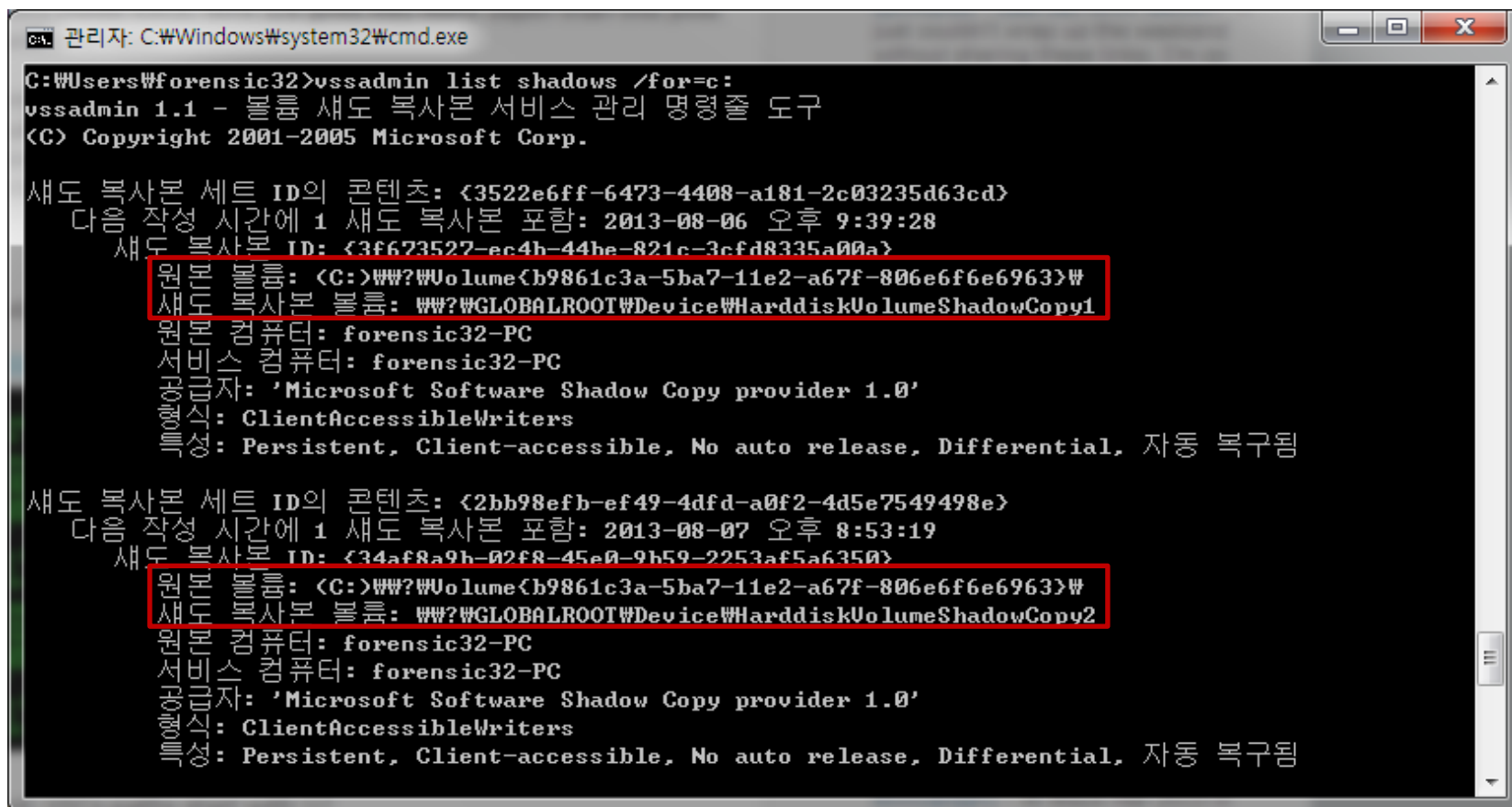
- 볼륨 새도 복사본 복원
  - 파일/폴더 단위의 백업 및 복원 기능



# 볼륨 새도 복사본

- 볼륨 새도 복사본 수집
  - 볼륨 새도 복사본 확인

```
C:\> vssadmin list shadows /for=c:
```



```
관리자: C:\Windows\system32\cmd.exe
C:\Users\forensic32>vssadmin list shadows /for=c:
vssadmin 1.1 - 볼륨 새도 복사본 서비스 관리 명령줄 도구
(C) Copyright 2001-2005 Microsoft Corp.

새도 복사본 세트 ID의 콘텐츠: {3522e6ff-6473-4408-a181-2c03235d63cd}
다음 작성 시간에 1 새도 복사본 포함: 2013-08-06 오후 9:39:28
새도 복사본 ID: {3f673527-ec4b-44be-821c-3cfd8335a00a}
원본 볼륨: (C:)\\?\\Volume{b9861c3a-5ba7-11e2-a67f-806e6f6e6963}\\
새도 복사본 볼륨: \\?\\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy1
원본 컴퓨터: forensic32-PC
서비스 컴퓨터: forensic32-PC
공급자: 'Microsoft Software Shadow Copy provider 1.0'
형식: ClientAccessibleWriters
특성: Persistent, Client-accessible, No auto release, Differential, 자동 복구됨

새도 복사본 세트 ID의 콘텐츠: {2bb98efb-ef49-4dfd-a0f2-4d5e7549498e}
다음 작성 시간에 1 새도 복사본 포함: 2013-08-07 오후 8:53:19
새도 복사본 ID: {34af8a9b-02f8-45e0-9b59-2253af5a6350}
원본 볼륨: (C:)\\?\\Volume{b9861c3a-5ba7-11e2-a67f-806e6f6e6963}\\
새도 복사본 볼륨: \\?\\GLOBALROOT\\Device\\HarddiskVolumeShadowCopy2
원본 컴퓨터: forensic32-PC
서비스 컴퓨터: forensic32-PC
공급자: 'Microsoft Software Shadow Copy provider 1.0'
형식: ClientAccessibleWriters
특성: Persistent, Client-accessible, No auto release, Differential, 자동 복구됨
```



# 볼륨 새도 복사본

- 볼륨 새도 복사본 수집
  - 볼륨 새도 복사본 링크 생성

```
C:\> mklink /d [Target Link Path] [Shadow Copy]
```

관리자: C:\Windows\system32\cmd.exe

```
C:\>mklink /d c:\vsc1 \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\
c:\vsc1 <====> \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\에 대한 기호화된 링크를 만들었습니다.

C:\>dir c:\vsc1
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: C0C2-911A

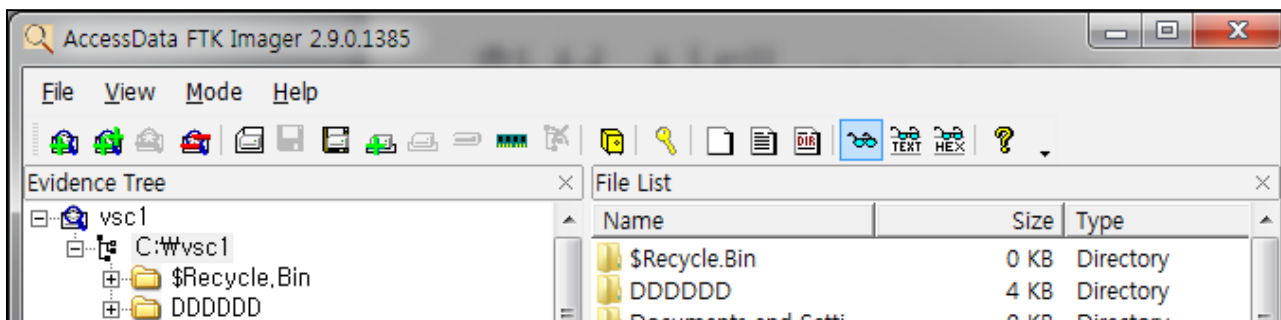
c:\vsc1 디렉터리

2013-03-11 오후 01:13          1,024 .rnd
2009-06-11 오전 06:42             24 autoexec.bat
2013-07-04 오후 03:39           908 CKINFO.TXT
2009-06-11 오전 06:42             10 config.sys
2013-03-25 오전 09:54          <DIR>          DDDDDD
2013-04-30 오전 11:32          <DIR>          ers
2013-07-26 오후 04:03          <DIR>          FPLive_win
2013-07-22 오후 01:19          <DIR>          H.I.T
2013-02-01 오후 05:16          <DIR>          Intel
2013-02-01 오후 02:31          <DIR>          Office
2013-06-26 오후 08:08          <DIR>          OpenSSL-Win32
2013-06-29 오후 07:02          <DIR>          PDFStreamDumper
2009-07-14 오전 11:37          <DIR>          PerfLogs
2013-04-30 오전 11:34          <DIR>          pki_nts
2013-07-19 오후 03:49          <DIR>          PRONEER
2013-08-06 오전 11:46          <DIR>          Program Files
2013-02-15 오전 11:04          <DIR>          Python27
2013-07-04 오후 10:31          <DIR>          SystemUtils
2013-07-30 오후 10:06          <DIR>          Temp
2013-08-01 오전 10:29             0 temp_hts.tmp
```

# 볼륨 새도 복사본

- 볼륨 새도 복사본 수집
  - 볼륨 새도 복사본 이미징
    - ✓ FTK Imager

- [File] → [Add Evidence Item] → [Contents of a Folder]



- ✓ FAU DD - <http://gmgsystemsinc.com/fau/>

```
C:\> dd if=\\.\HarddiskVolumeShadowCopy# of=[output file] --localwrt
```

```
D:\Util\04.Disk\fa-1.3.0.2390a<dd>\fa\FAU.x86>dd if=\\.\HarddiskVolumeShadowCopy3 of=d:\wshadow.dd --localwrt
Copying \\.\HarddiskVolumeShadowCopy3 to d:\wshadow.dd
Output: d:\wshadow.dd
69466062848 bytes
66248+0 records in
66248+0 records out
69466062848 bytes written
```

# 볼륨 새도 복사본

## ■ 볼륨 새도 복사본 수집

### • 볼륨 새도 복사본 전체 복사

```
C:\> robocopy C:\VSC1\Users\proneer F:\VSC1 /S /XJ /COPY:DAT /NFL /NDL /w:0 /r:0
```

- ✓ **/S** : 빈 디렉터리는 제외하고 하위 디렉터리 복사
- ✓ **/XJ** : 교차점은 복사 제외
- ✓ **/COPY:DAT** : 데이터, 속성, 시간 정보도 복사 (D=Data, A=Attributes, T=Timestamps)
- ✓ **/NFL** : 파일 목록을 로깅하지 않음
- ✓ **/NLI** : 디렉터리 목록을 로깅하지 않음
- ✓ **/w:0** : 다시 시도하는 동안 대기 시간
- ✓ **/r:0** : 실패한 복사본에 대한 다시 시도 횟수

### • 특정 파일 형식만 복사

```
C:\> robocopy C:\VSC1\Users F:\VSC1 *.jpg *.bmp *.png /S /XJ /COPY:DAT /NFL /NDL /w:0 /r:0
```

## ▪ 볼륨 새도 복사본 분석

### • 라이브 분석

- ✓ vssadmin + mslink + robocopy
- ✓ FTK Imager, EnCase
- ✓ ShadowExplorer, VSCToolset, ShadowKit

### • 오프라인 분석

- ✓ Reconnoitre – Commercial
- ✓ libvshadow
  - DD 스타일의 RAW 이미지 입력, 리눅스/맥에서 사용

## ■ 볼륨 새도 복사본 분석

### • 분석 가능한 형태로 변환

- ✓ EnCase PDE(Physical Disk Emulator), Arsenal Image Mounter를 이용해 물리 가상 마운트
- ✓ DD/RAW → VMDK 파일로 변환 후 VMWare로 구동 후 분석
  - LiveView
  - ProDiscover
- ✓ DD/RAW → VHD 파일로 변환 후 [컴퓨터 관리] → [VHD 연결]
  - VHDFree

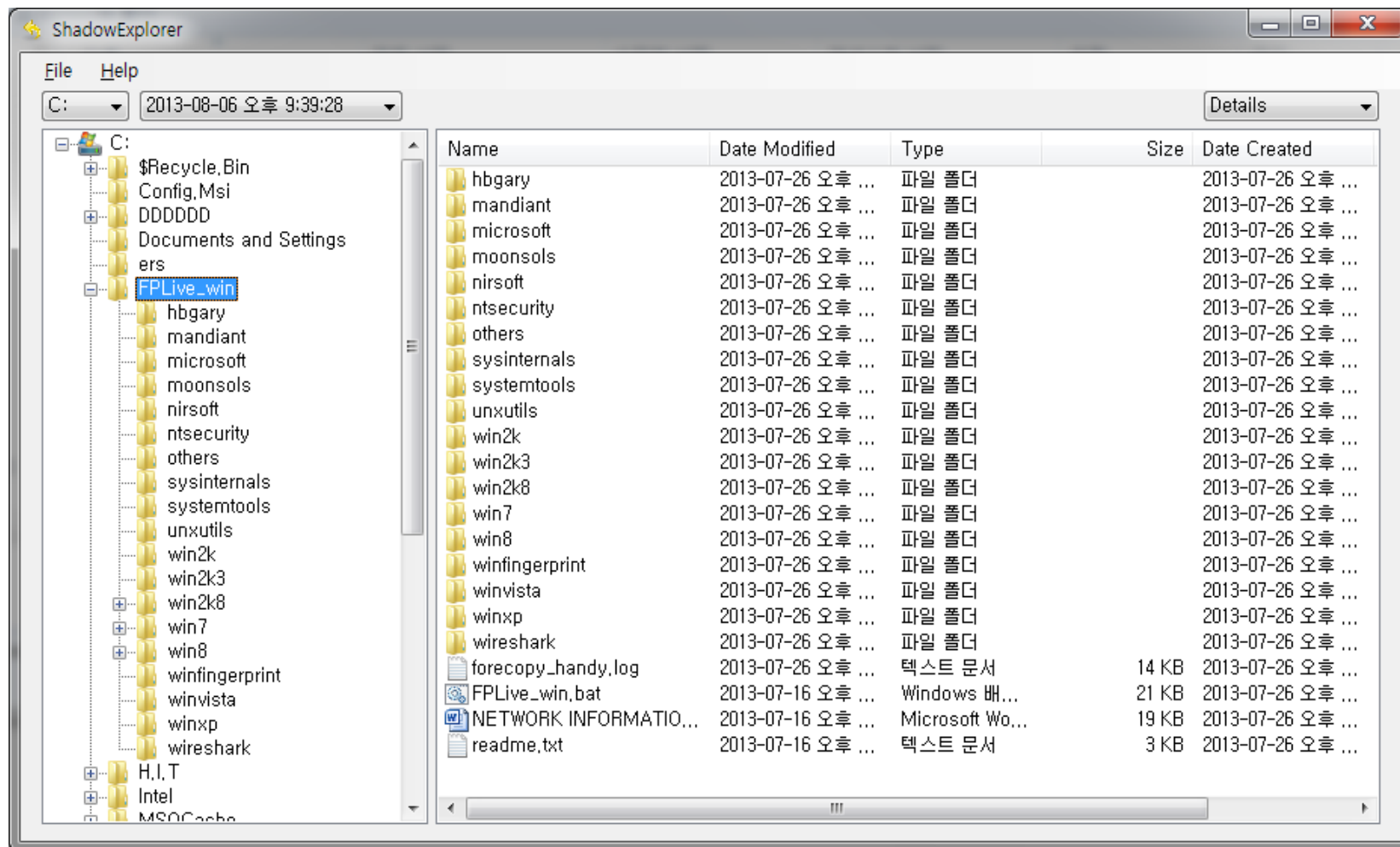
### • 분석의 효율성

- ✓ 오프라인 분석 << 라이브 분석
- ✓ VMDK << VHD << PDE
- ✓ 이미징 << 파일 선별 수집

# 볼륨 새도 복사본

## ■ 볼륨 새도 복사본 분석

- ShadowExplorer – <http://www.shadowexplorer.com/>



## 볼륨 새도 복사본 비교

장치 종류	장치 이름	드라이브명	볼륨 명	시리얼 넘버	ParentIdPrefix	최초연결시각 (SetupAPI L...	부팅이후 연결시각 (UTC+...	Time Source	Key Path of Time Source
USB	USB Root Hub			5&17df1c1b&0	6&b25d31b&0	<b>VSC2</b>			
USB	USB Root Hub			5&2648447&0					
USB	Generic USB Hub (Port_#0002.H...			6&b25d31b&0&2					
USB	USB 입력 장치 (0002.0000.0000....			7&2a63cead&0&...	8&8afd64f&0				
USB	USB 입력 장치 (0002.0000.0000....			7&2a63cead&0&...	8&20a88dda&0				
SCSI	Disk&Ven_Dell&Prod_VIRTUAL_DISK			6&17b13437&0&...			2009-07-14 13:52:51 Tue	[SYSTEM - DISK] ControlSet001 (...	HKEY_LOCAL_MACHINE\WS...
IDE	CdRomHL-DT-ST_DVD-ROM_GDR...			5&28836b88&0&...			2009-07-14 13:52:59 Tue	[SYSTEM - VOLUME] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
IDE	CdRomHL-DT-ST_DVD-ROM_GDR...			5&28836b88&0&...			2009-07-14 13:52:59 Tue	[SYSTEM - CDROM] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
USB	VID_14DD&PID_1005			BAC6F7F7E34A...			2009-07-14 13:53:01 Tue	[SYSTEM - USB] ControlSet001 (C...	HKEY_LOCAL_MACHINE\WS...
IDE	NECVMWare VMware IDE CDR 10 A...	D:		5&290fd3ab&0&...			2013-06-24 14:33:29 Mon	[NTUSER - NTUSER]	HKEY_LOCAL_MACHINE\WS...
SCSI	VMware, VMware Virtual S SCSI D...			5&198200580&0&...			2013-06-24 14:37:06 Mon	[SYSTEM - DISK] ControlSet001 (...	HKEY_LOCAL_MACHINE\WS...
FDC	플로피 디스크 드라이브	A:		6&2bc13940&0&0			2013-06-24 14:37:10 Mon	[SYSTEM - VOLUME] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
IDE	NECVMWare VMware IDE CDR 10 A...	D:		5&290fd3ab&0&...			2013-06-24 14:37:10 Mon	[SYSTEM - VOLUME] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
IDE	NECVMWare VMware IDE CDR 10 A...	D:		5&290fd3ab&0&...			2013-06-24 14:37:10 Mon	[SYSTEM - CDROM] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
USB	USB Composite Device (Port_#00...			6&b25d31b&0&1	7&2a63cead&0		2013-06-24 14:37:11 Mon	[SYSTEM - USB] ControlSet001 (C...	HKEY_LOCAL_MACHINE\WS...
USB	Generic Bluetooth Adapter (Port_...			000650268328	8&20f38eb4&0		2013-06-24 14:37:12 Mon	[SYSTEM - USB] ControlSet001 (C...	HKEY_LOCAL_MACHINE\WS...

장치 종류	장치 이름	드라이브명	볼륨 명	시리얼 넘버	ParentIdPrefix	최초연결시각 (...	부팅이후 연결시각 (UTC+...	Time Source	Key Path of Time Source
USB	USB Root Hub			5&17df1c1b&0	6&b25d31b&0	<b>VSC3</b>			
USB	USB Root Hub			5&2648447&0	6&6ee641b&0				
USB	Generic USB Hub (Port_#0002.H...			6&b25d31b&0&2	7&25aa2865&0				
USB	USB 입력 장치 (0002.0000.0000....			7&2a63cead&0&...	8&8afd64f&0				
USB	USB 입력 장치 (0002.0000.0000....			7&2a63cead&0&...	8&20a88dda&0				
SCSI	Disk&Ven_Dell&Prod_VIRTUAL_DISK			6&17b13437&0&...			2009-07-14 13:52:51 Tue	[SYSTEM - DISK] ControlSet001 (...	HKEY_LOCAL_MACHINE\WS...
IDE	CdRomHL-DT-ST_DVD-ROM_GDR...			5&28836b88&0&...			2009-07-14 13:52:59 Tue	[SYSTEM - VOLUME] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
IDE	CdRomHL-DT-ST_DVD-ROM_GDR...			5&28836b88&0&...			2009-07-14 13:52:59 Tue	[SYSTEM - CDROM] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
USB	VID_14DD&PID_1005			BAC6F7F7E34A...			2009-07-14 13:53:01 Tue	[SYSTEM - USB] ControlSet001 (C...	HKEY_LOCAL_MACHINE\WS...
IDE	NECVMWare VMware IDE CDR 10 A...	D:		5&290fd3ab&0&...			2013-06-24 14:33:29 Mon	[NTUSER - NTUSER]	HKEY_LOCAL_MACHINE\WS...
SCSI	VMware, VMware Virtual S SCSI D...			5&198200580&0&...			2013-06-24 16:08:43 Mon	[SYSTEM - DISK] ControlSet001 (...	HKEY_LOCAL_MACHINE\WS...
IDE	NECVMWare VMware IDE CDR 10 A...	D:		5&290fd3ab&0&...			2013-06-24 16:08:48 Mon	[SYSTEM - VOLUME] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
IDE	NECVMWare VMware IDE CDR 10 A...	D:		5&290fd3ab&0&...			2013-06-24 16:08:48 Mon	[SYSTEM - CDROM] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
FDC	플로피 디스크 드라이브	A:		6&2bc13940&0&0			2013-06-24 16:08:49 Mon	[SYSTEM - VOLUME] ControlSet00...	HKEY_LOCAL_MACHINE\WS...
USB	USB Composite Device (Port_#00...			6&b25d31b&0&1	7&2a63cead&0		2013-06-24 16:08:51 Mon	[SYSTEM - USB] ControlSet001 (C...	HKEY_LOCAL_MACHINE\WS...
USB	Generic Bluetooth Adapter (Port_...			000650268328	8&20f38eb4&0		2013-06-24 16:08:53 Mon	[SYSTEM - USB] ControlSet001 (C...	HKEY_LOCAL_MACHINE\WS...
USB	Unknown Device (Port_#0001.Hu...			6&6ee641b&0&1			2013-06-26 15:09:06 Wed	[SYSTEM - USB] ControlSet001 (C...	HKEY_LOCAL_MACHINE\WS...
USB	USB 입력 장치 (Port_#0002.Hub...			7&25aa2865&0&2	8&390a6c0a&0		2013-06-26 15:09:32 Wed	[SYSTEM - USB] ControlSet001 (C...	HKEY_LOCAL_MACHINE\WS...

## ■ 볼륨 새도 복사본 포렌식

### • 획득 가능한 정보

- ✓ 백업된 시점의 시스템 흔적 (파일시스템, 레지스트리 등)
- ✓ 백업 시점 간에 변화된 시스템 흔적 비교

### • 분석 과정

1. 라이브 분석이 가능하다면 라이브 분석!!!
2. 이미지를 획득한 경우, EnCase PDE나 Arsenal Image Moutner 사용!!
3. 2번이 가능하지 않을 경우, VHD로 변환 후 [VHD 연결]!!!
4. 스냅샷 목록 및 생성 일자 확인!!!
5. 필요한 파일만 선별 수집하여 분석 진행!!!



- 볼륨 새도 복사본 분석 도구

- **Arsenal Image Mounter** – Arsenal Recon

- ✓ <http://arsenalrecon.com/apps/image-mounter/>

- **VSC Toolset** – Jason Hale

- ✓ <http://dfstream.blogspot.kr/p/vsc-toolset.html>

- **ShadowExplorer** – ShadowExplorer

- ✓ <http://www.shadowexplorer.com/downloads.html>

- **Reconnoitre** – Sanderson Forensics

- ✓ <http://sandersonforensics.com/forum/content.php?168-Reconnoitre>

- **Libvshadow** – Joachim Metz

- ✓ <https://code.google.com/p/libvshadow/>

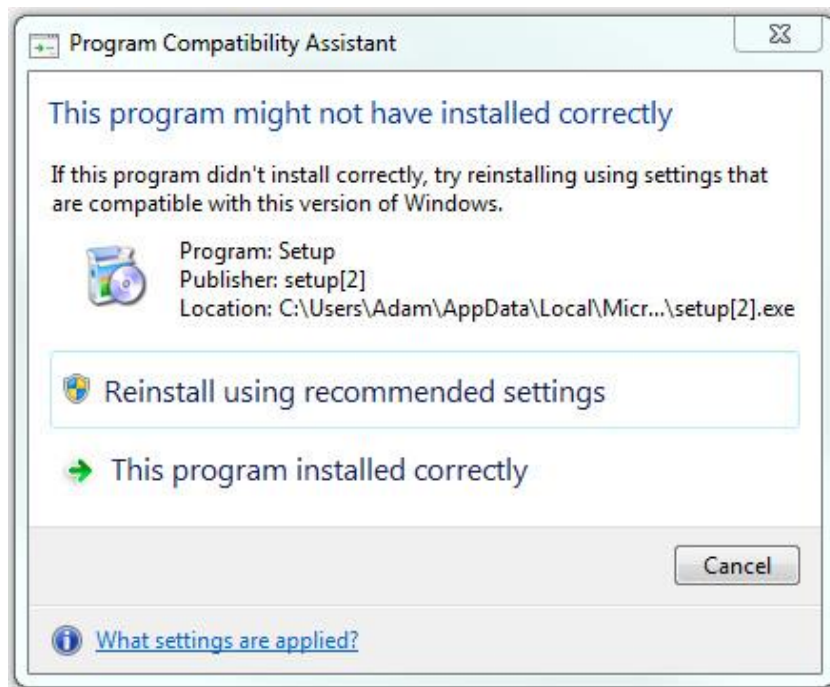
## ➔ 실습

- 라이브 시스템의 블룸 새도 복사본 분석하기!!

# 호환성 아티팩트

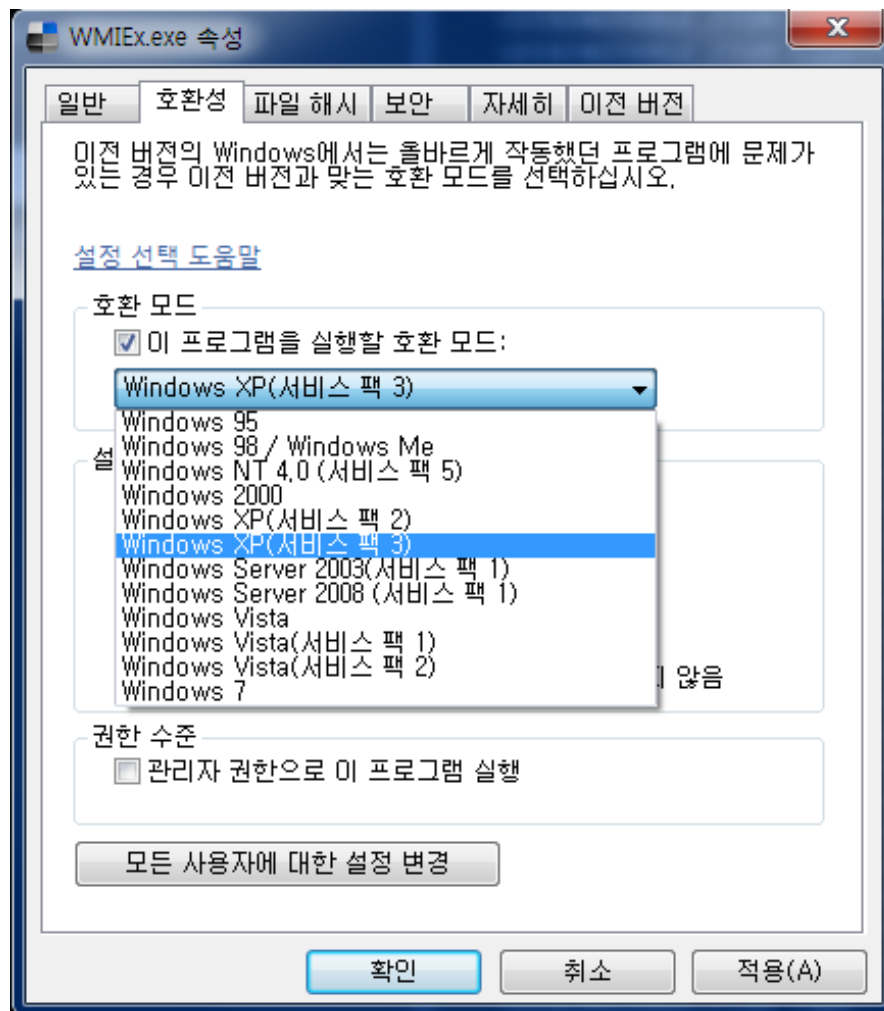
## ■ 응용프로그램 호환성 (Application Compatibility)

- 운영체제의 업데이트에 따라 이전 버전과의 호환성 기능 제공
- 호환성 문제의 대부분은 버전에 따라 달라진 API 문제
- 운영체제는 호환성 문제가 있는 API를 탐지한 후, 대체 API로 연결



## ■ 응용프로그램 호환성 (Application Compatibility)

- 호환 모드를 통해 직접 원하는 환경 상태에서 프로그램 실행 가능



## ■ 응용프로그램 호환성 (Application Compatibility)

### • 응용프로그램 실행

✓ Kernel32.dll → CreateProcessInternalW() → BasepCheckBadApp()

### • 호환성 확인 순서

✓ 응용프로그램 호환성 캐시

✓ 응용프로그램 호환성 데이터베이스

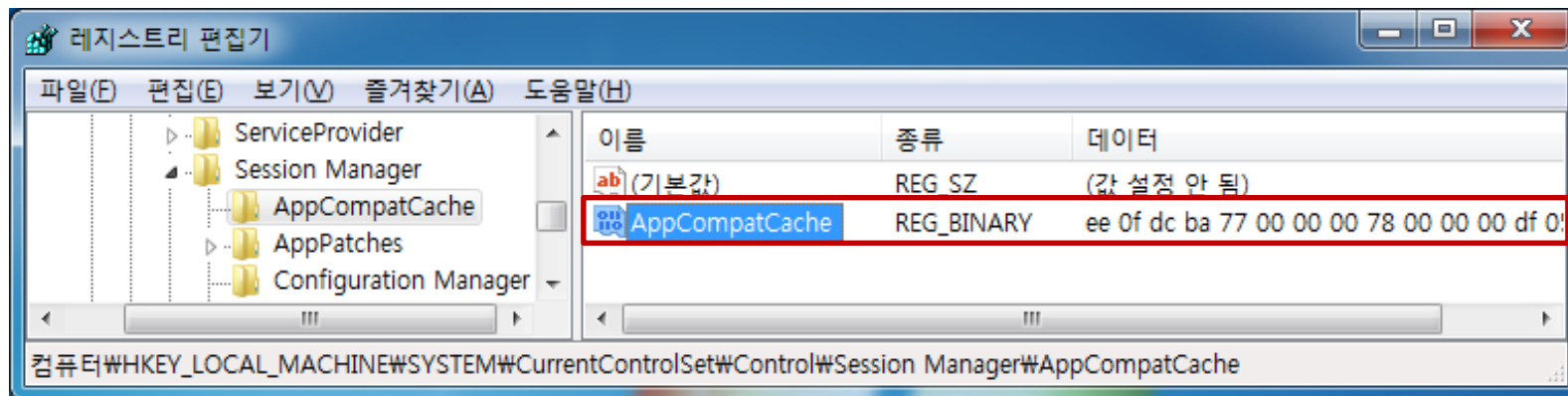
### • 응용프로그램 호환성 플래그

✓ 호환성 문제가 발생한 응용프로그램 정보 이외에 사용자의 호환성 설정 정보 저장

# 응용프로그램 호환성 아티팩트

## ■ 응용프로그램 호환성 캐시

- 호환성 문제가 발생했던 응용프로그램의 정보 저장
- 호환성 캐시 저장 경로 ➔ 레지스트리
  - ✓ 키 : HKLM\SYSTEM\ControlSet00\Control\Session Manager\AppCompatCache
  - ✓ 값 : AppCompatCache



## ■ 응용프로그램 호환성 캐시

### • 호환성 캐시 구조

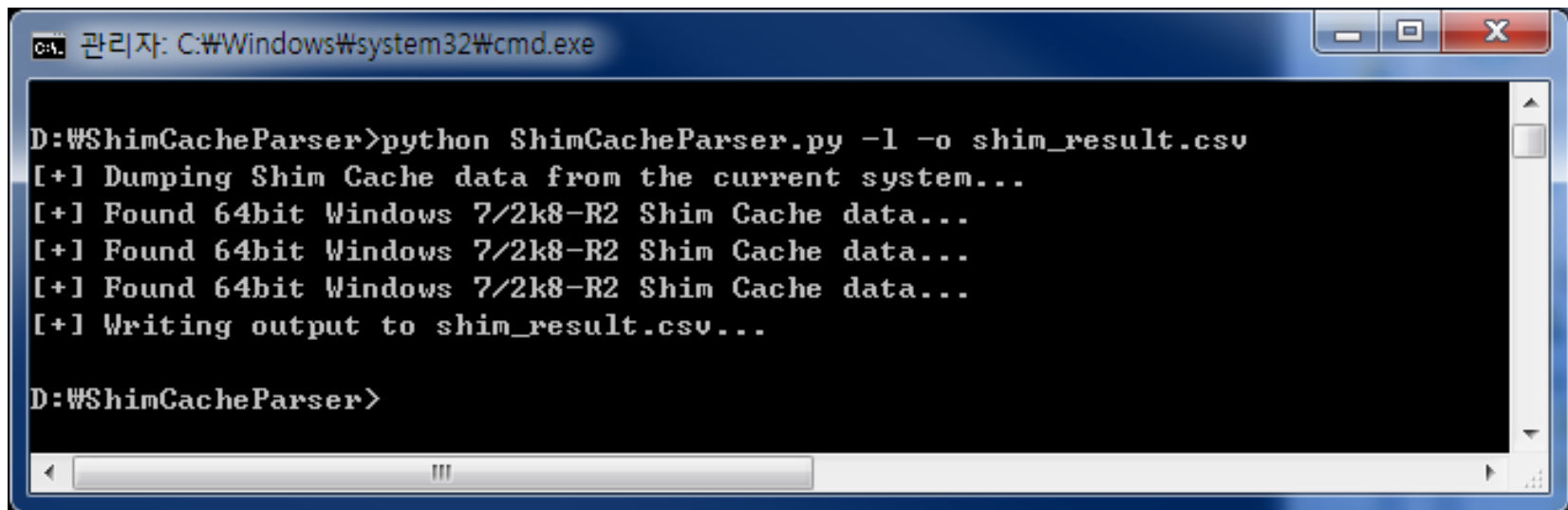
```
//32-bit Win7/2k8R2 AppCompatCache Entry Structure
typedef struct AppCompatCacheEntry32_Win7{
    USHORT wLength;
    USHORT wMaximumLength;
    DWORD dwPathOffset;
    FILETIME ftLastModTime;
    DWORD dwInsertFlags;
    DWORD dwShimFlags;
    DWORD dwBlobSize;
    DWORD dwBlobOffset;
} APPCOMPATCACHE_ENTRY32_WIN7;

//64-bit Win7/2k8R2 AppCompatCache Entry Structure
typedef struct AppCompatCacheEntry64_Win7{
    USHORT wLength;
    USHORT wMaximumLength;
    DWORD dwPadding;
    QWORD dwPathOffset;
    FILETIME ftLastModTime;
    DWORD dwInsertFlags;
    DWORD dwShimFlags;
    QWORD qwBlobSize;
    QWORD qwBlobOffset;
} APPCOMPATCACHE_ENTRY64_WIN7;
```



# 응용프로그램 호환성 아티팩트

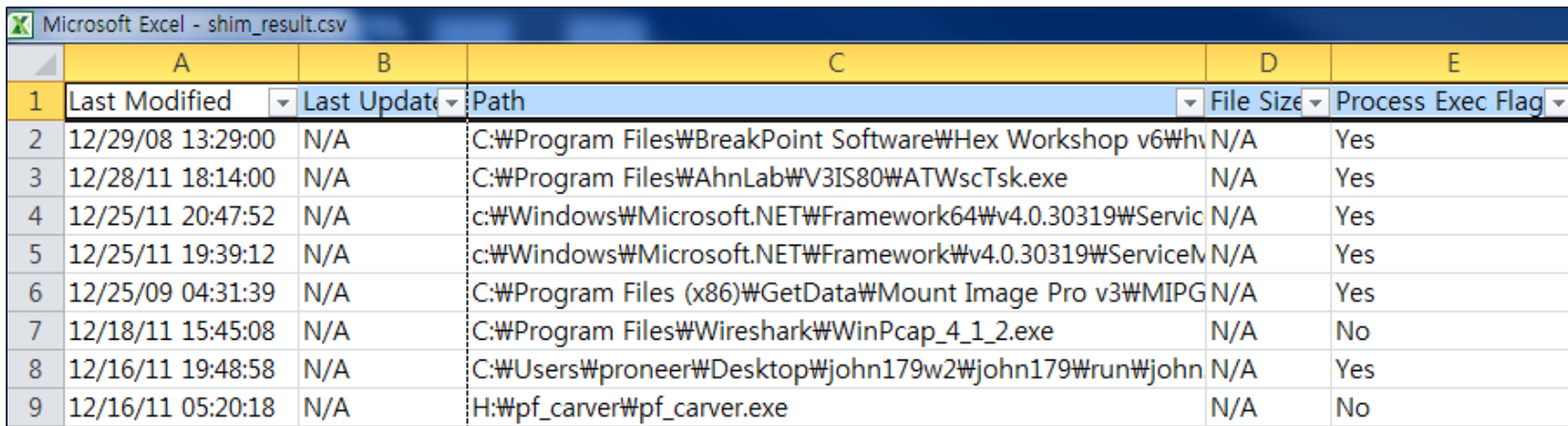
- 응용프로그램 호환성 캐시
  - ShimCacheParser – <https://github.com/mandiant/ShimCacheParser>



```
관리자: C:\Windows\system32\cmd.exe

D:\ShimCacheParser>python ShimCacheParser.py -l -o shim_result.csv
[+] Dumping Shim Cache data from the current system...
[+] Found 64bit Windows 7/2k8-R2 Shim Cache data...
[+] Found 64bit Windows 7/2k8-R2 Shim Cache data...
[+] Found 64bit Windows 7/2k8-R2 Shim Cache data...
[+] Writing output to shim_result.csv...

D:\ShimCacheParser>
```



	A	B	C	D	E
1	Last Modified	Last Update	Path	File Size	Process Exec Flag
2	12/29/08 13:29:00	N/A	C:\Program Files\BreakPoint Software\Hex Workshop v6\h...	N/A	Yes
3	12/28/11 18:14:00	N/A	C:\Program Files\AhnLab\V3IS80\ATWscTsk.exe	N/A	Yes
4	12/25/11 20:47:52	N/A	c:\Windows\Microsoft.NET\Framework64\v4.0.30319\Service...	N/A	Yes
5	12/25/11 19:39:12	N/A	c:\Windows\Microsoft.NET\Framework\v4.0.30319\ServiceM...	N/A	Yes
6	12/25/09 04:31:39	N/A	C:\Program Files (x86)\GetData\Mount Image Pro v3\MIPG...	N/A	Yes
7	12/18/11 15:45:08	N/A	C:\Program Files\Wireshark\WinPcap_4_1_2.exe	N/A	No
8	12/16/11 19:48:58	N/A	C:\Users\proneer\Desktop\john179w2\john179wrun\john...	N/A	Yes
9	12/16/11 05:20:18	N/A	H:\wpf_carver\wpf_carver.exe	N/A	No

## ■ 응용프로그램 호환성 데이터베이스

- 호환성 캐시에서 해결방안을 못 찾았을 경우, 호환성 데이터베이스 활용

- 호환성 데이터베이스 파일 경로

- ✓ %SystemRoot%\AppPatch(64)\

- SDB(Shim Database)

- ✓ 호환성 문제가 있는 프로그램 목록과 해결 방안

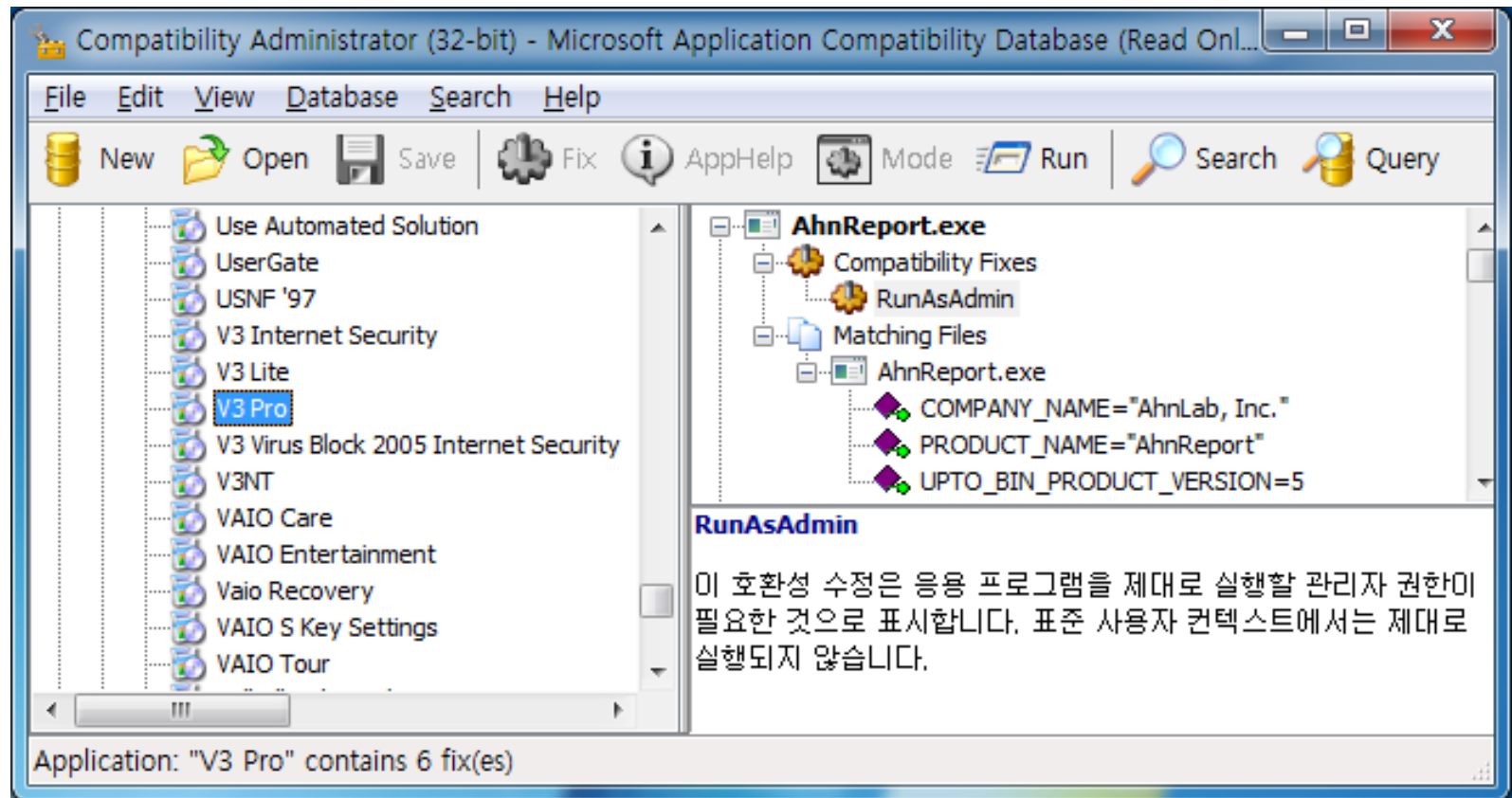
- sysmain.sdb
    - drvmain.sdb
    - msimain.sdb
    - pcamain.sdb

# 응용프로그램 호환성 아티팩트

## ■ 응용프로그램 호환성 데이터베이스

### • Microsoft Application Compatibility Toolkit (ACT)

✓ <http://www.microsoft.com/en-us/download/details.aspx?displaylang=en&id=7352>



## ■ 응용프로그램 호환성 플래그

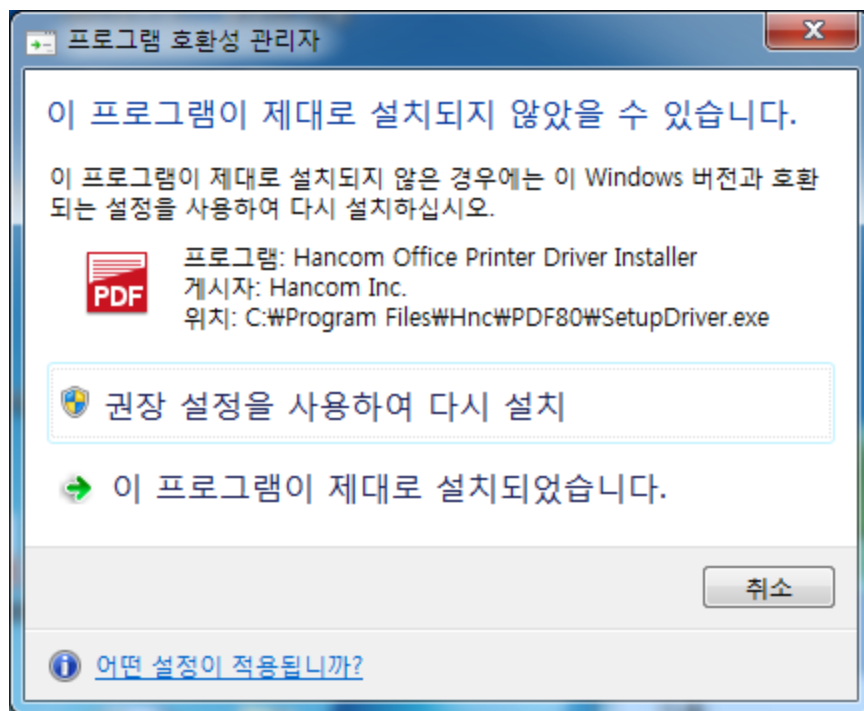
- “이 프로그램이 제대로 설치되었습니다” 선택 시 레지스트리에 정보 저장

- ✓ HKCU\Software\Microsoft\Windows NT\CurrentVersion\

**AppCompatFlags\Compatibility Assistant\Persisted**

- ✓ HKLM\Software\Microsoft\Windows NT\CurrentVersion\

**AppCompatFlags\Compatibility Assistant\Persisted**

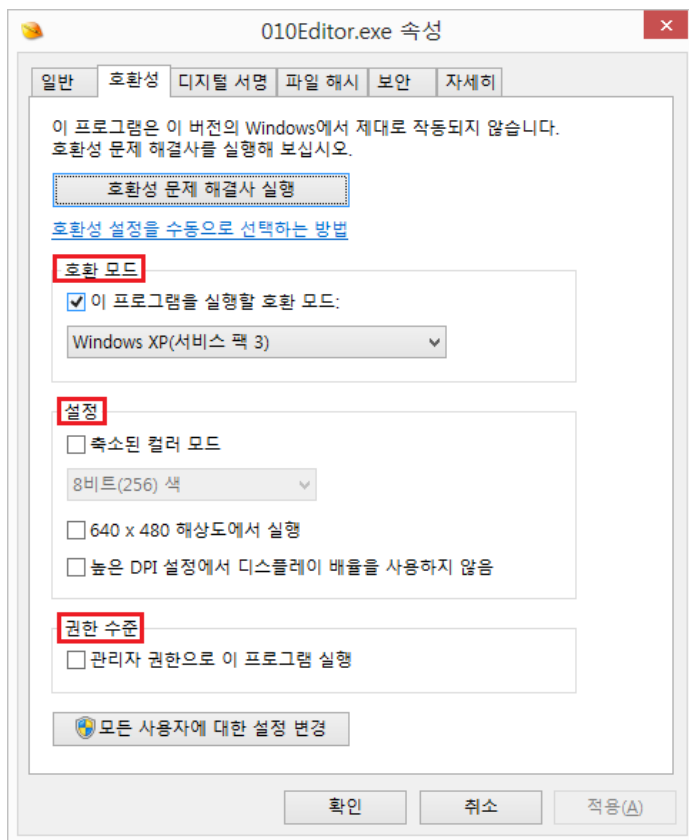


# 응용프로그램 호환성 아티팩트

## ■ 응용프로그램 호환성 플래그

- 프로그램 속성 → 호환성 탭 설정 변경

- ✓ HKCU\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers
- ✓ HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Layers



## ▪ 최근 파일 캐시

- 프로그램 실행 시 경로를 임시 저장하기 위한 공간으로 단순 경로 나열
  - ✓ %SystemRoot%\AppCompat\Programs\RecentFileCache.bcf
- 캐시 되는 경우
  - ✓ 실행 파일 → 실행 파일로 파생된 경우 (드롭퍼)
  - ✓ 다른 볼륨이나 시스템에서 복사(인터넷 다운로드 포함)된 경우

- 응용프로그램 호환성 아티팩트 분석 도구
  - 호환성 아티팩트 분석 도구
    - ✓ **REGA** – DFRC
      - <http://forensic.korea.ac.kr/tools/rega.html>
    - ✓ **ShimCacheParser** – Mandiant
      - <https://github.com/mandiant/ShimCacheParser>

## ➔ 실습

- 라이브 시스템의 응용프로그램 호환성 아티팩트 분석하기!!

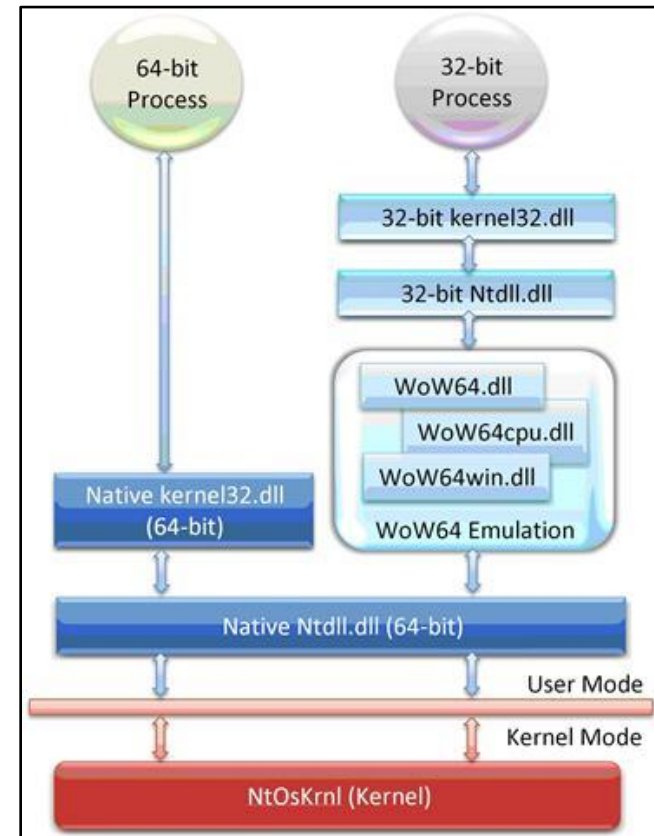
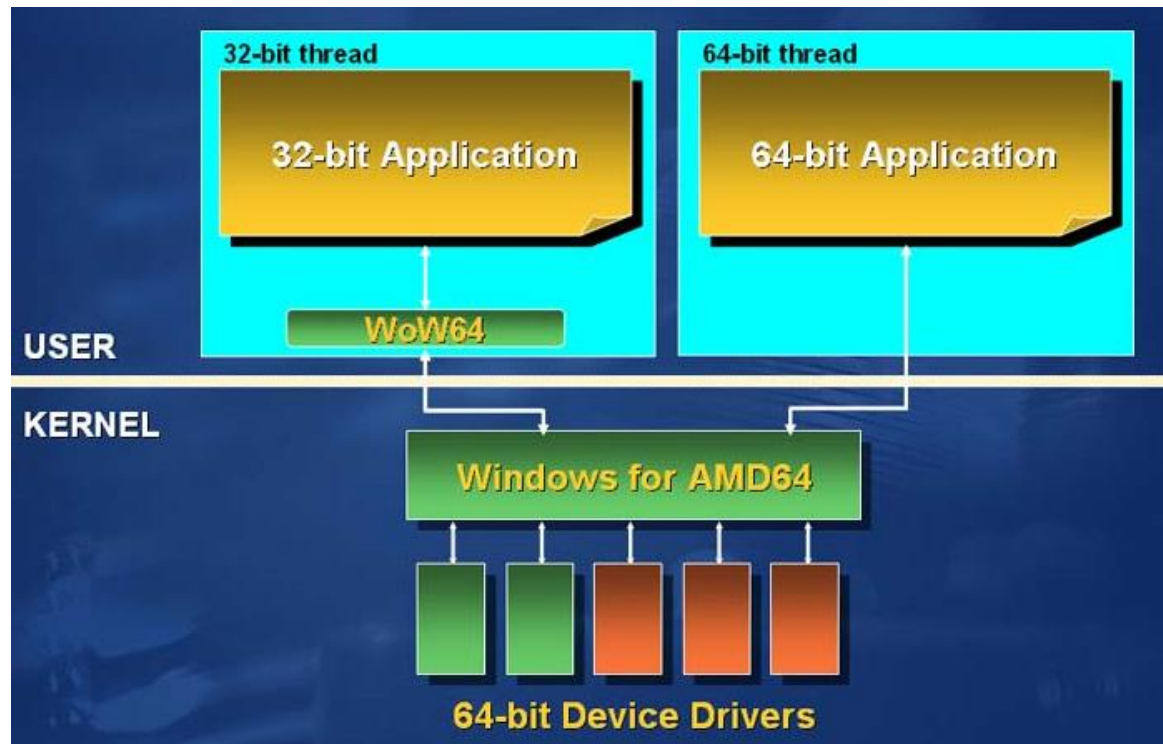


# WOW64

# WOW64

## ▪ WOW64 → Windows 32-bit On Windows 64-bit

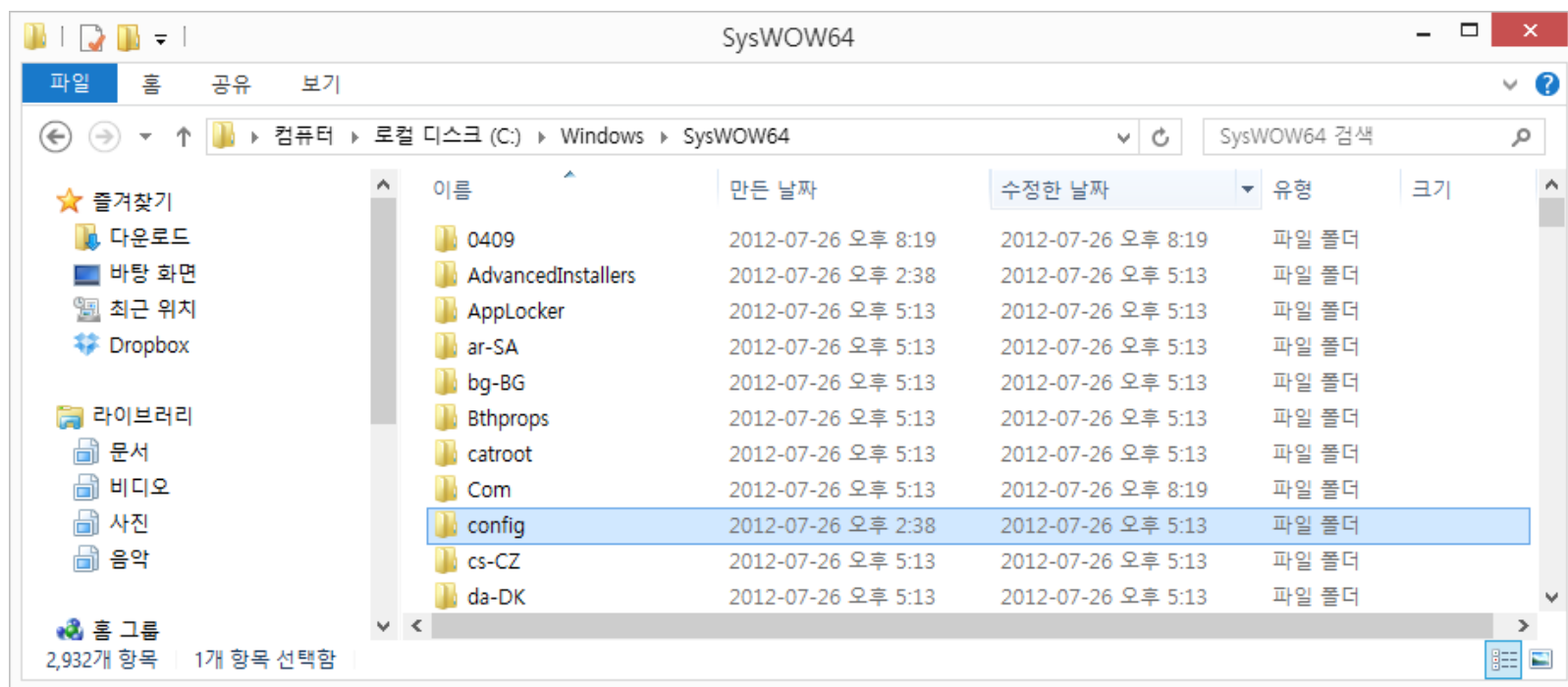
- 64비트 시스템의 32비트 동작 환경을 지원하는 에뮬레이터
- 32비트 관련 데이터는 모두 WoW64 경로로 리다이렉트



## ■ 파일시스템 아티팩트

### • %SystemRoot%\SysWOW64

- ✓ %SystemRoot%\system32 폴더의 리다이렉트 폴더
- ✓ System32 폴더 하위에 접근하는 32비트 프로그램 데이터는 해당 폴더로 리다이렉트
- ✓ %SystemRoot%\SysWOW64\config 폴더 조사



- 레지스트리 아티팩트

- HKLM\SOFTWARE\Wow6432Node

- ✓ 리다이렉트되는 항목 – [http://msdn.microsoft.com/en-us/library/windows/desktop/aa384253\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/windows/desktop/aa384253(v=vs.85).aspx)

- HKLM\SOFTWARE
    - HKLM\SOFTWARE\Classes\CLSID
    - HKLM\SOFTWARE\Classes\DirectShow
    - HKLM\SOFTWARE\Classes\Interface
    - HKLM\SOFTWARE\Classes\Media Type
    - HKLM\SOFTWARE\Classes\MediaFoundation
    - HKU\SOFTWARE\CLSID
    - HKU\SOFTWARE\DirectShow
    - HKU\SOFTWARE\Interface
    - HKU\SOFTWARE\Media Type
    - HKU\SOFTWARE\MediaFoundation

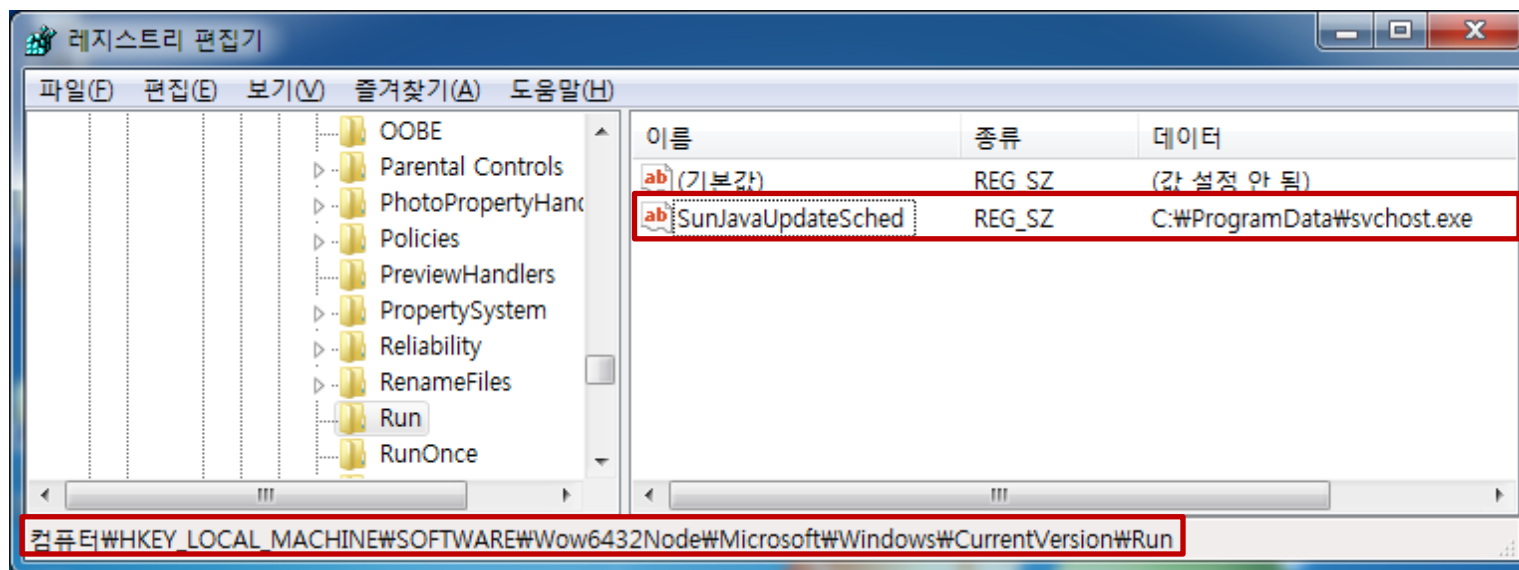
## ■ 레지스트리 아티팩트

### • HKLM\SOFTWARE\Wow6432Node

✓ 64비트 환경에서 동작한 32비트 악성코드의 흔적이 남음

✓ V3 진단명

- Win-Trojan/Jorik.48128.AD (45bc9ad077dec8a5b682f02900f844ae)



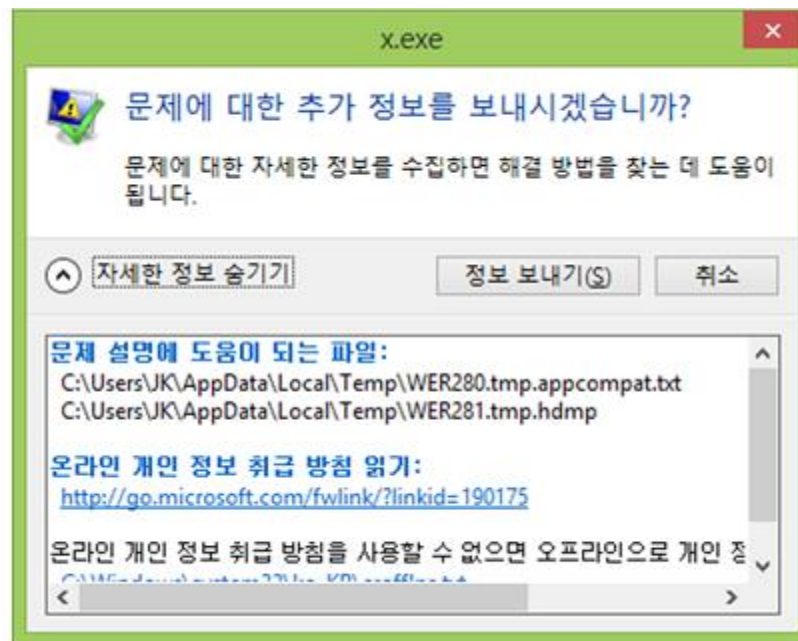
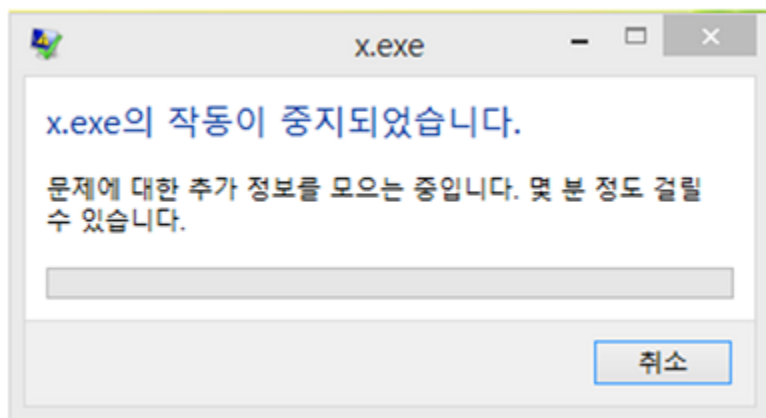
## ➔ 실습

- 라이브 시스템의 WOW64 아티팩트 분석하기!!

# 윈도우 문제 보고

## ■ WER, Windows Error Reporting

- XP부터 추가된 기능으로 오류 발생 시 디버깅 정보를 수집하여 보고하는 기능
- MS 파트너(ISV, IHV, OEM 등)일 경우, 보고된 정보 확인 가능
- 발생 빈도가 높거나 심각한 오류는 핫픽스(Hotfix)를 통해 업데이트

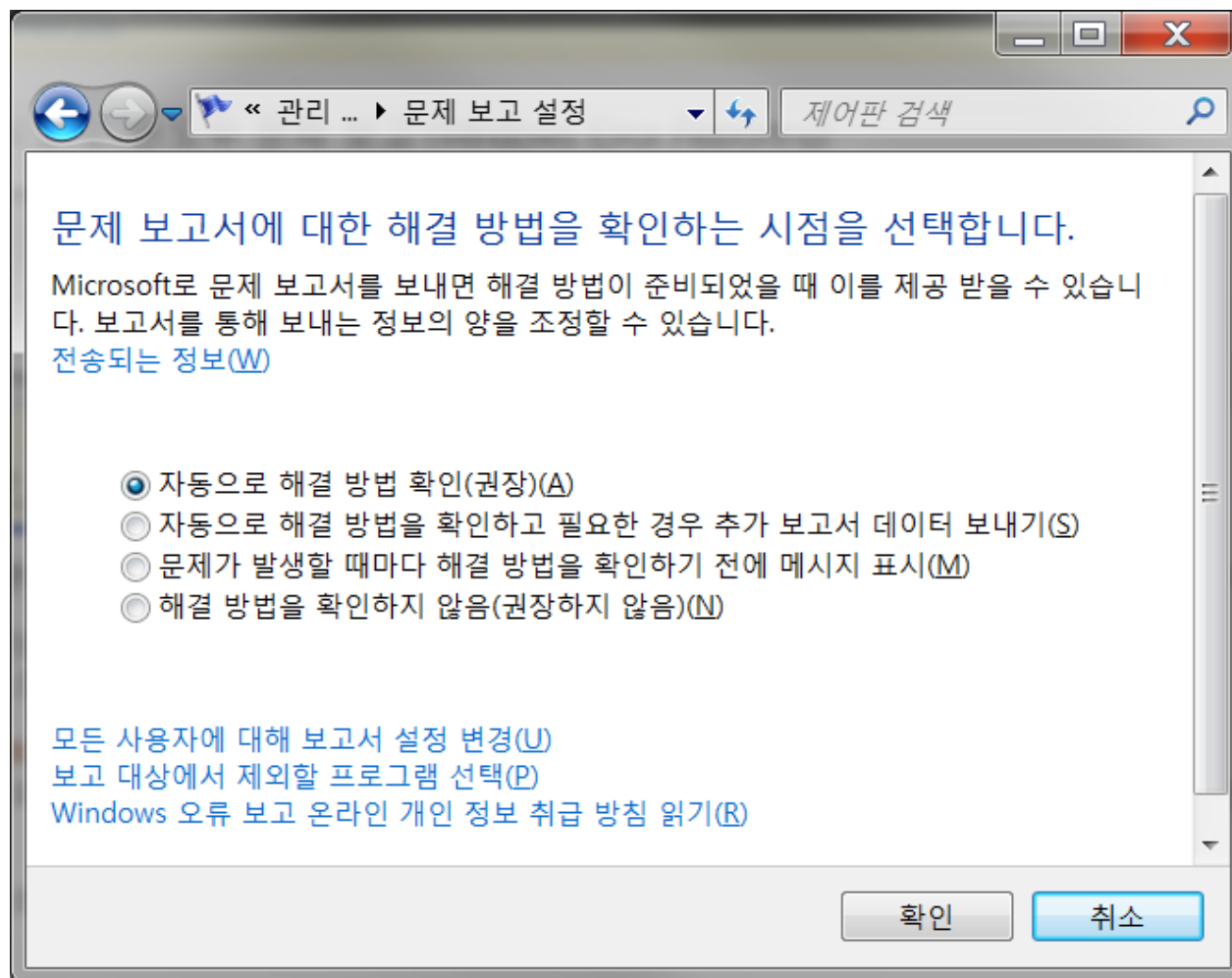




# 윈도우 문제 보고

## ■ 윈도우 문제 보고 설정

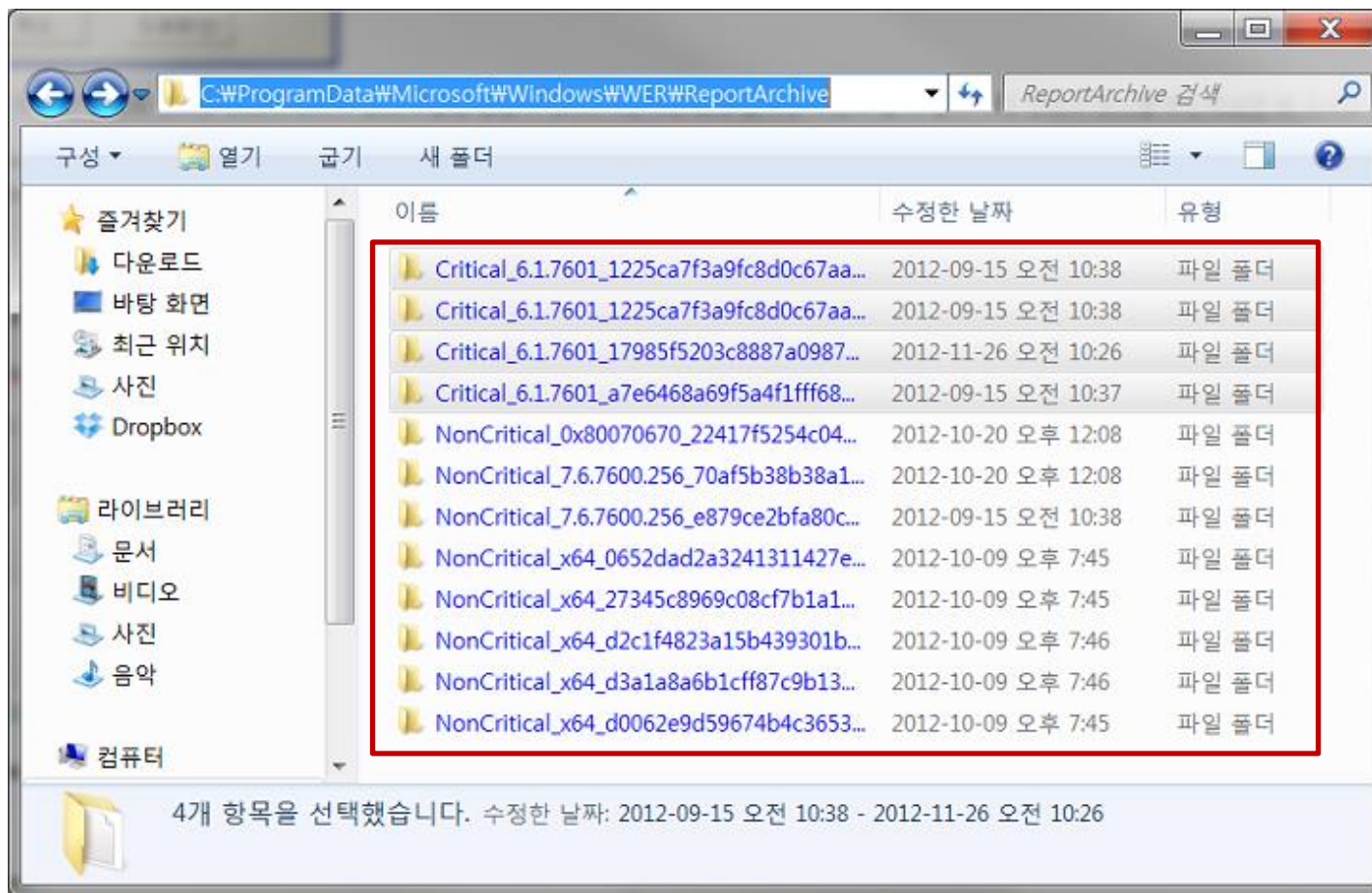
- [제어판] → [관리 센터] → [관리 센터 설정 변경] → [문제 보고 설정]



# 윈도우 문제 보고

## ■ 윈도우 문제 보고 경로

- %SystemDrive%\ProgramData\Microsoft\WER\ReportArchive
- %UserProfile%\AppData\Local\Microsoft\Windows\WER



## ■ 윈도우 문제 보고 샘플

### • Sample.Report.wer

```
Version=1
EventType=APPCRASH
EventTime=129925356137537695
ReportType=2
Consent=1
UploadTime=129925356139257701
... ..

UI[2]=C:\$Recycle.Bin\x.exe
UI[3]=x.exe의 작동이 중지되었습니다.
UI[4]=온라인으로 문제에 대한 해결 방법을 확인할 수 있습니다.
... ..

UI[7]=프로그램 닫기
LoadedModule[0]=C:\$Recycle.Bin\x.exe
LoadedModule[1]=C:\Windows\SYSTEM32\ntdll.dll
LoadedModule[2]=C:\Windows\SYSTEM32\KERNEL32.DLL
... ..

FriendlyEventName=작동이 중지됨
ConsentKey=APPCRASH
AppName=x.exe
AppPath=C:\$Recycle.Bin\x.exe
NsPartner=windows
NsGroup=windows8
```

# 윈도우 문제 보고

## ■ 윈도우 문제 보고 이벤트

### • WER 이벤트 로그

✓ %SystemRoot%\system32\winevt\Logs\Microsoft-Windows-WER-Diag%4Operational.evtx



## ➔ 실습

- 라이브 시스템의 윈도우 문제 보고서 분석하기!!

