Welcome to EnCase Seminar !!

Security is a people problem…

forensic-proof.com

20 October 2009

Outline

Toward Understanding EnCase

- Week 1 : Hardware and File System Analysis (Chapter 1, 2)
- Week 2 : Acquiring Digital Evidence (Chapter 4)
- Week 3 : EnCase Concepts and Environment (Chapter 5, 6)
- Week 4 : Understanding , Searching For, and Bookmarking Data (Chapter 7)
- Week 5 : File Signature Analysis and Hash Analysis (Chapter 8)
- Week 6 : Windows Operating System Artifacts – Part I (Chapter 9)
- Week 7 : Windows Operating System Artifacts – Part II (Chapter 9)
- Week 8 : Advanced EnCase (Chapter 10)

Outline

Toward Understanding EnCase

- ~~Week 1 : Hardware and File System Analysis (Chapter 1, 2)~~
- ~~Week 2 : Acquiring Digital Evidence (Chapter 4)~~
- ~~Week 3 : EnCase Concepts and Environment (Chapter 5, 6)~~
- ~~Week 4 : Understanding , Searching For, and Bookmarking Data (Chapter 7)~~
- ~~Week 5 : File Signature Analysis and Hash Analysis (Chapter 8)~~
- ~~Week 6 : Windows Operating System Artifacts – Part I (Chapter 9)~~
- Week 7 : Windows Operating System Artifacts – Part II (Chapter 9)
- Week 8 : Advanced EnCase (Chapter 10)

Windows Operating System Artifacts

Last week

- Windows dates and times
- Adjusting for time zone offsets
- Recycle Bin and INFO records
- Windows Vista Recycle Bin
- Link files
- Windows 2000, XP, and Vista folders
- Recent folder

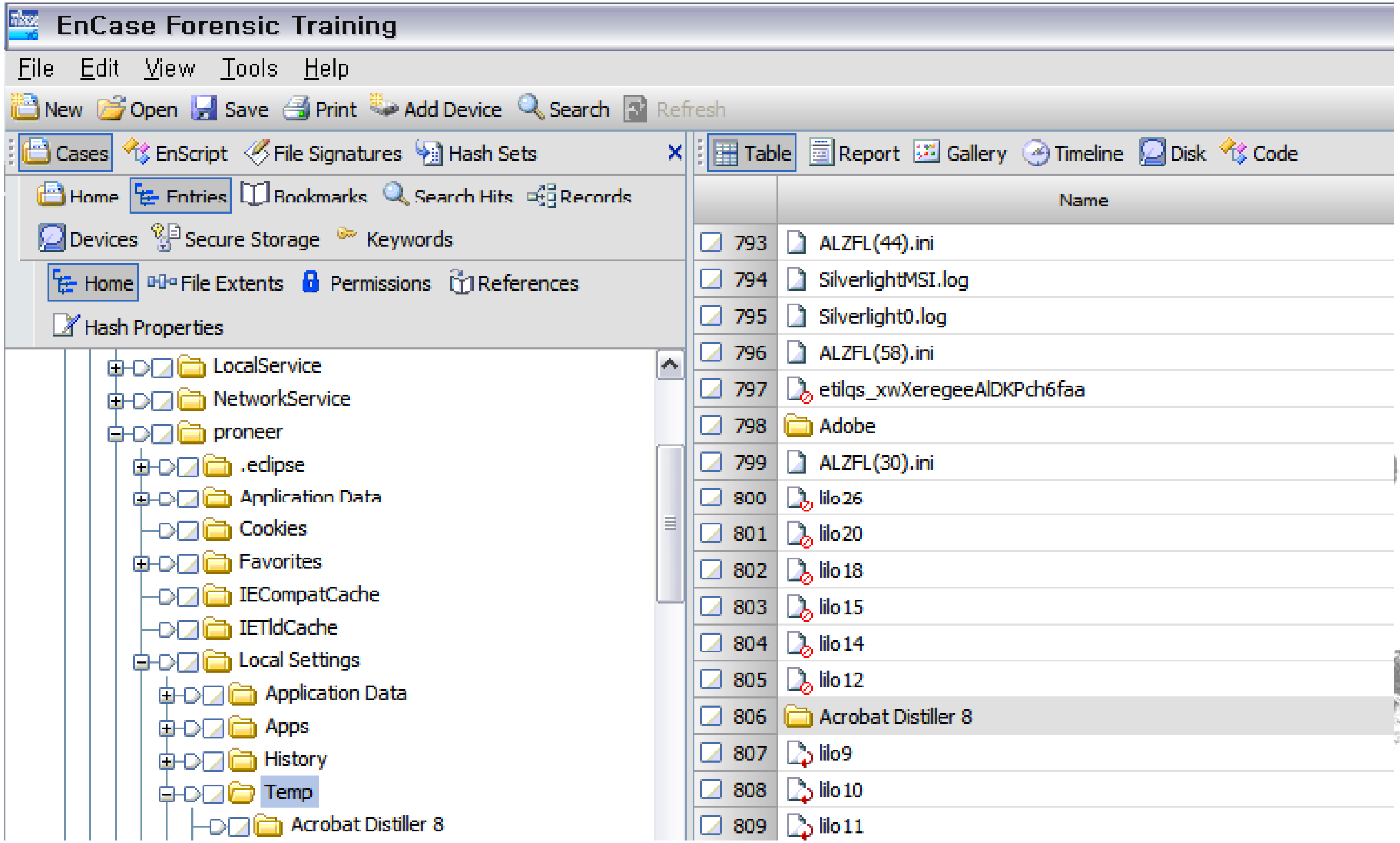
Temp Folder (1)

- **MS-DOS** and **Microsoft Windows**, set by the *environment variable 'TEMP'*
  - *C:\Temp*
  - *%WINDIR%Temp*

- **XP** : C:\Documents and Settings*\% UserName %\Local Settings\Temp*
- **Vista** : C:\Users*\%UserName%\AppData\Local\Temp*

- it's still user relocatable…

Temp Folder (2)


EnCase Forensic Training
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases EnScript File Signatures Hash Sets
Home Entries Bookmarks Search Hits Records
Devices Secure Storage Keywords
Home File Extents Permissions References
Hash Properties
LocalService
NetworkService
proneer
.eclipse
Application Data
Cookies
Favorites
IECompatCache
IETldCache
Local Settings
Application Data
Apps
History
Temp
Acrobat Distiller 8
Table Report Gallery Timeline Disk Code

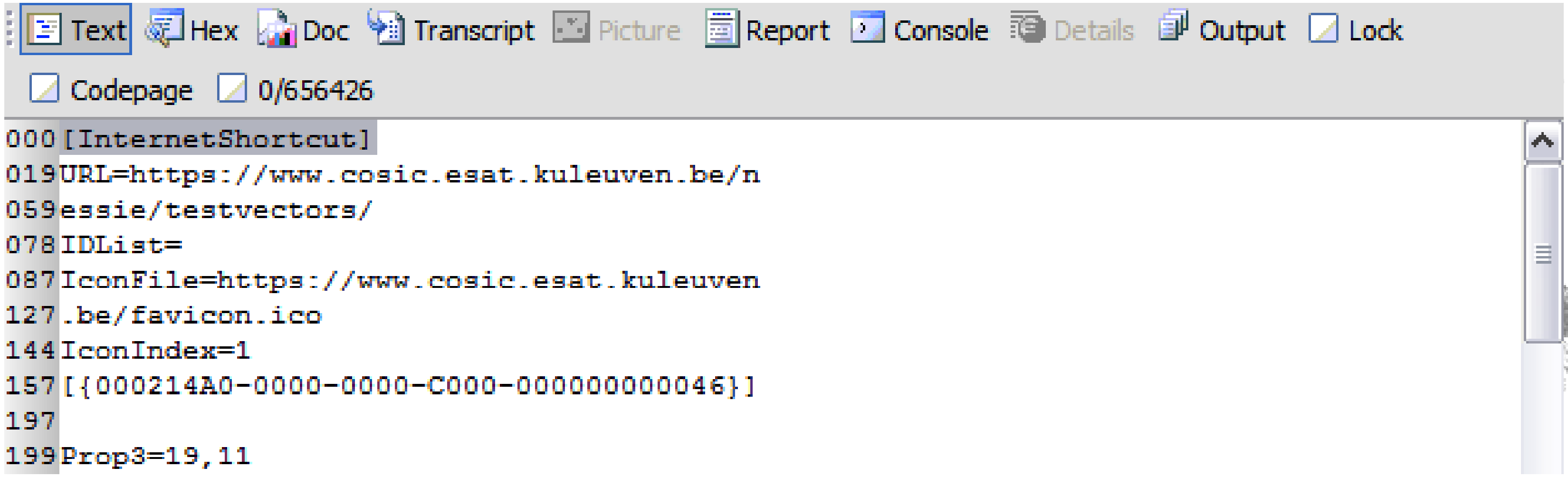
	Name
793	ALZFL(44).ini
794	SilverlightMSI.log
795	Silverlight0.log
796	ALZFL(58).ini
797	etilqs_xwXeregeeAlDKPch6faa
798	Adobe
799	ALZFL(30).ini
800	lilo26
801	lilo20
802	lilo18
803	lilo15
804	lilo14
805	lilo12
806	Acrobat Distiller 8
807	lilo9
808	lilo10
809	lilo11

Temp Folder (3)

- Temporarily store files
- Often programs create working copies of open documents (changing extension)
    - *good place to look after running a file signature analysis*
- Some programs deleted them when done, leave *behind their garbage*
- *hidden or backup copies* of files
- Programs often write their temporary *install files and folders*

Favorites Folder (1)

- C:\Documents and Settings\%UserName%\Favorites
- *Internet shortcut files* for Microsoft Internet Explorer
- Have an extension of *.url (Uniform Resource Locator)*
- A URL file has a unique header “[InternetShortcut]”



```
000[InternetShortcut]
019URL=https://www.cosic.esat.kuleuven.be/n
059essie/testvectors/
078IDList=
087IconFile=https://www.cosic.esat.kuleuven
127.be/favicon.ico
144IconIndex=1
157[{000214A0-0000-0000-C000-000000000046}]
197
199Prop3=19,11
```

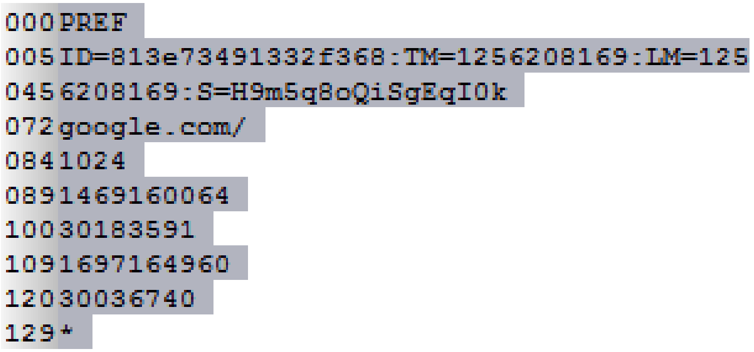
Favorites Folder (2)

- Default favorites can *depending on the Windows version and Service Pack*
- Some users may *add user-defined sites*
- Some *programs may add a URL to their company site*
- Soma *malicious code may add* without the user’s knowledge

Cookies Folder

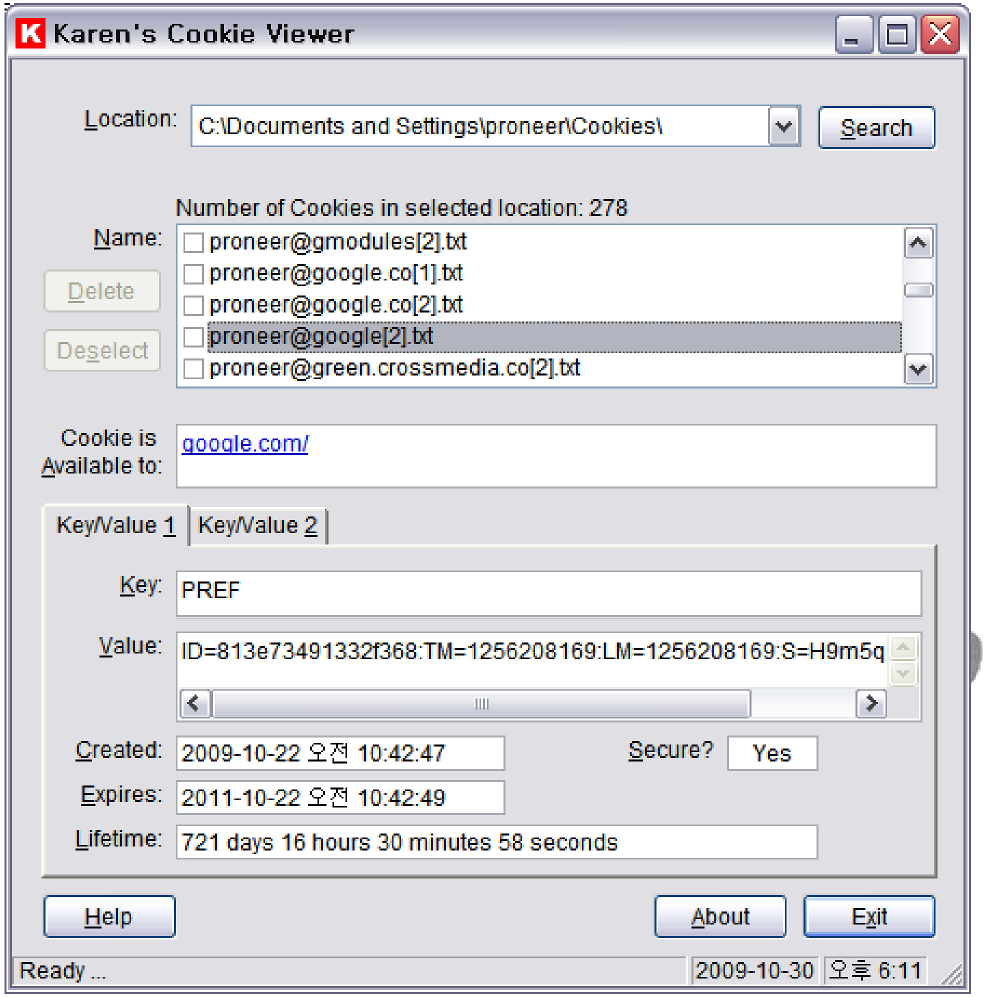
- **XP** : C:\Documents and Settings*\%UserName%\Cookies*
- **Vista** : C:\Users*\%UserName%\AppData\Roaming\Microsoft\Windows\Cookies*
- Created by websites and placed on the user's local computer
- Name form : *user name@domain name.txt*
- The total cookie files is *under the management of an index.dat file*

Cookies Folder



```
000 PREF
005 ID=813e73491332f368:TM=1256208169:LM=125
045 6208169:S=H9m5q8oQiSgEqI0k
072 google.com/
084 1024
089 1469160064
100 30183591
109 1697164960
120 30036740
129 *
```

Cookie name
Cookie value
Host/path for the web server
Expiration time (low)
Expiration time (high)
Creation time (low)
Creation time (high)
Record delimiter (*)



Location: C:\Documents and Settings\proneer\Cookies\

Number of Cookies in selected location: 278

Name:
□ proneer@gmodules[2].txt
□ proneer@google.co[1].txt
□ proneer@google.co[2].txt
□ proneer@google[2].txt
□ proneer@green.crossmedia.co[2].txt

Cookie is Available to: google.com/

Key: PREF

Value: ID=813e73491332f368:TM=1256208169:LM=1256208169:S=H9m5q

Created: 2009-10-22 오전 10:42:47

Secure? Yes

Expires: 2011-10-22 오전 10:42:49

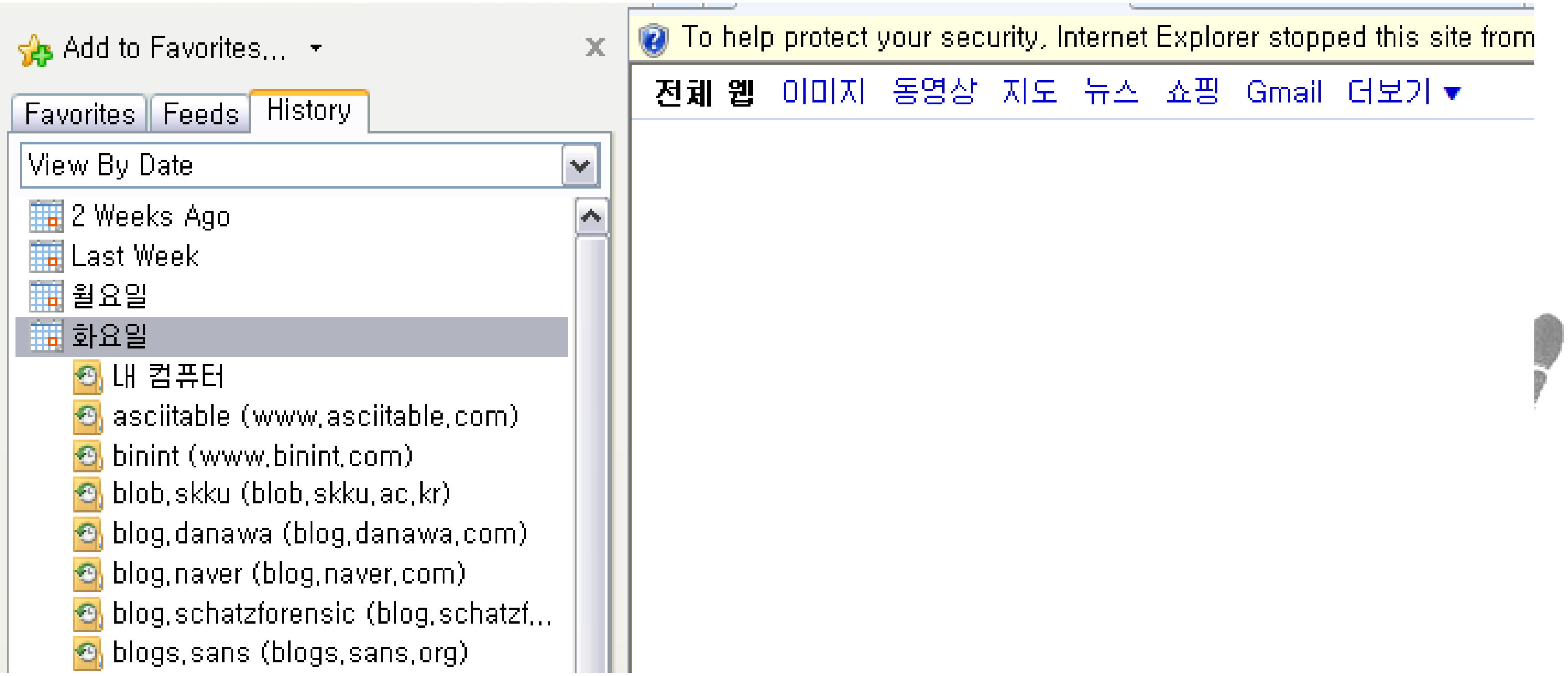
Lifetime: 721 days 16 hours 30 minutes 58 seconds

Ready ... | 2009-10-30 | 오후 6:11

Windows Operating System Artifacts

History Folder

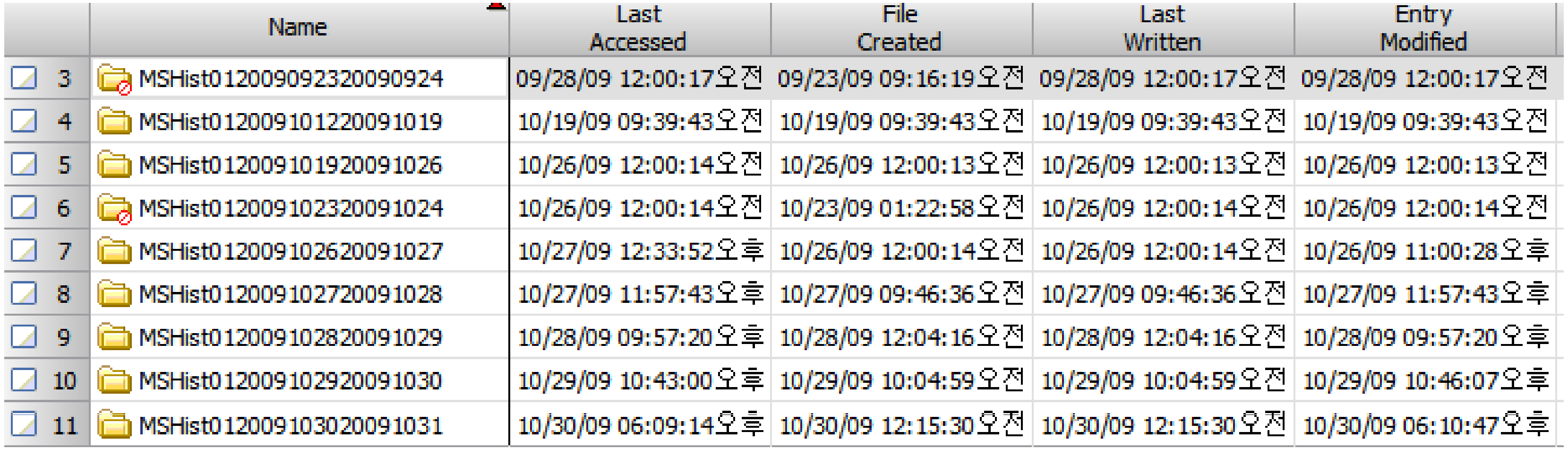
- **XP** : C:\Documents and Settings\*%UserName%\Local Settings\History\History.IE5*
- **Vista** : C:\Users\*%UserName%\AppData\Local\Microsoft\Windows\History\History.IE5*



Add to Favorites...
Favorites
Feeds
History
View By Date
2 Weeks Ago
Last Week
월요일
화요일
내 컴퓨터
asciitable (www.asciitable.com)
binint (www.binint.com)
blob.skku (blob.skku.ac.kr)
blog.danawa (blog.danawa.com)
blog.naver (blog.naver.com)
blog.schatzforensic (blog.schatzf...
blogs.sans (blogs.sans.org)
To help protect your security, Internet Explorer stopped this site from
전체 웹
이미지
동영상
지도
뉴스
쇼핑
Gmail
더보기 ▾

Windows Operating System Artifacts

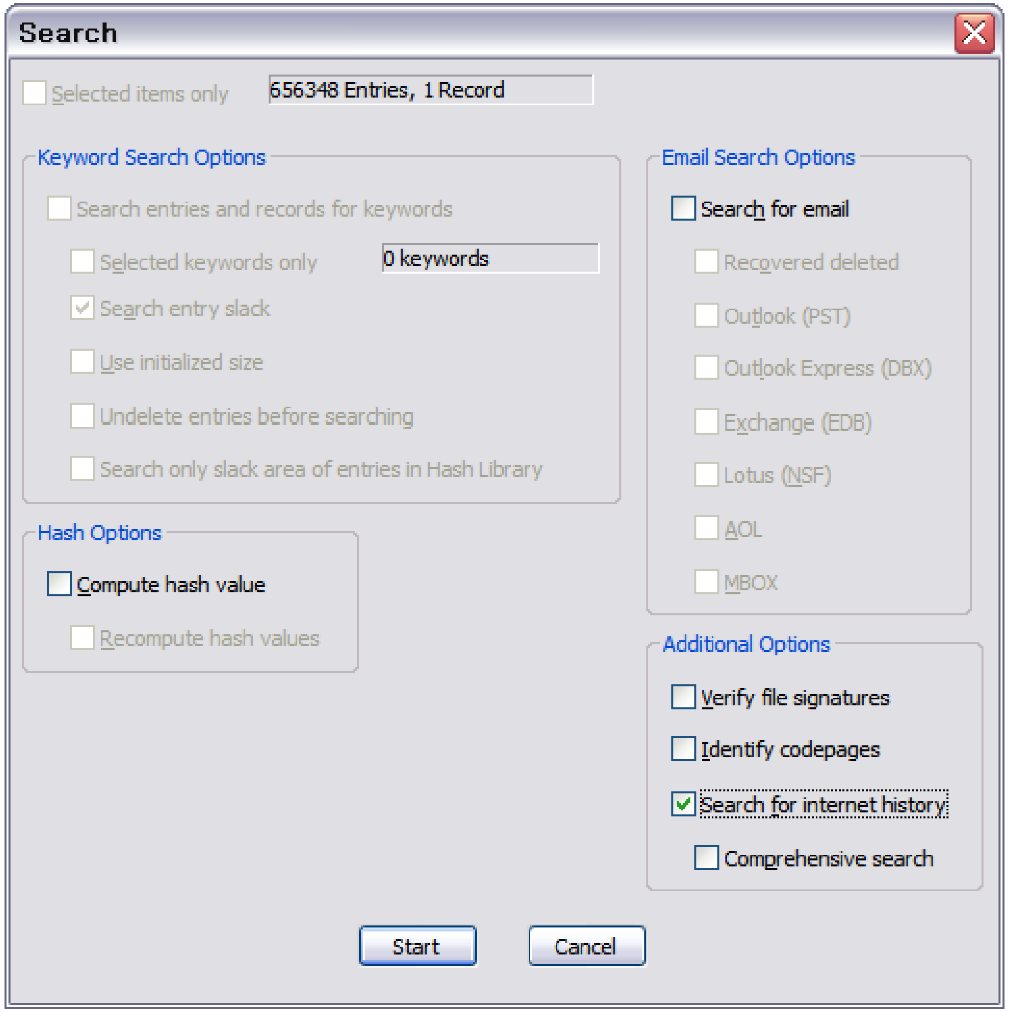
History Folder



	Name	Last Accessed	File Created	Last Written	Entry Modified
3	MSHist012009092320090924	09/28/09 12:00:17오전	09/23/09 09:16:19오전	09/28/09 12:00:17오전	09/28/09 12:00:17오전
4	MSHist012009101220091019	10/19/09 09:39:43오전	10/19/09 09:39:43오전	10/19/09 09:39:43오전	10/19/09 09:39:43오전
5	MSHist012009101920091026	10/26/09 12:00:14오전	10/26/09 12:00:13오전	10/26/09 12:00:13오전	10/26/09 12:00:13오전
6	MSHist012009102320091024	10/26/09 12:00:14오전	10/23/09 01:22:58오전	10/26/09 12:00:14오전	10/26/09 12:00:14오전
7	MSHist012009102620091027	10/27/09 12:33:52오후	10/26/09 12:00:14오전	10/26/09 12:00:14오전	10/26/09 11:00:28오후
8	MSHist012009102720091028	10/27/09 11:57:43오후	10/27/09 09:46:36오전	10/27/09 09:46:36오전	10/27/09 11:57:43오후
9	MSHist012009102820091029	10/28/09 09:57:20오후	10/28/09 12:04:16오전	10/28/09 12:04:16오전	10/28/09 09:57:20오후
10	MSHist012009102920091030	10/29/09 10:43:00오후	10/29/09 10:04:59오전	10/29/09 10:04:59오전	10/29/09 10:46:07오후
11	MSHist012009103020091031	10/30/09 06:09:14오후	10/30/09 12:15:30오전	10/30/09 12:15:30오전	10/30/09 06:10:47오후

History Folder Name	Data Range	Browser History Folder
MSHist012009103020091031	2009.10.31 – 2009.10.31	Today
MSHist012009102920091030	2009.10.29 – 2009.10.30	Thursday
MSHist012009102820091029	2009.10.28 – 2009.10.29	Wednesday
MSHist012009102720091028	2009.10.27 – 2009.10.28	Tuesday
MSHist012009102620091027	2009.10.26 – 2009.10.27	Monday
MSHist012009101920091026	2009.10.19 – 2009.10.26	Last week
MSHist012009101020091019	2009.10.10 – 2009.10.19	2 weeks ago

History Folder



Search

□ Selected items only 656348 Entries, 1 Record

Keyword Search Options

- □ Search entries and records for keywords
- □ Selected keywords only 0 keywords
- ☑ Search entry slack
- □ Use initialized size
- □ Undelete entries before searching
- □ Search only slack area of entries in Hash Library

Hash Options

- □ Compute hash value
- □ Recompute hash values

Email Search Options

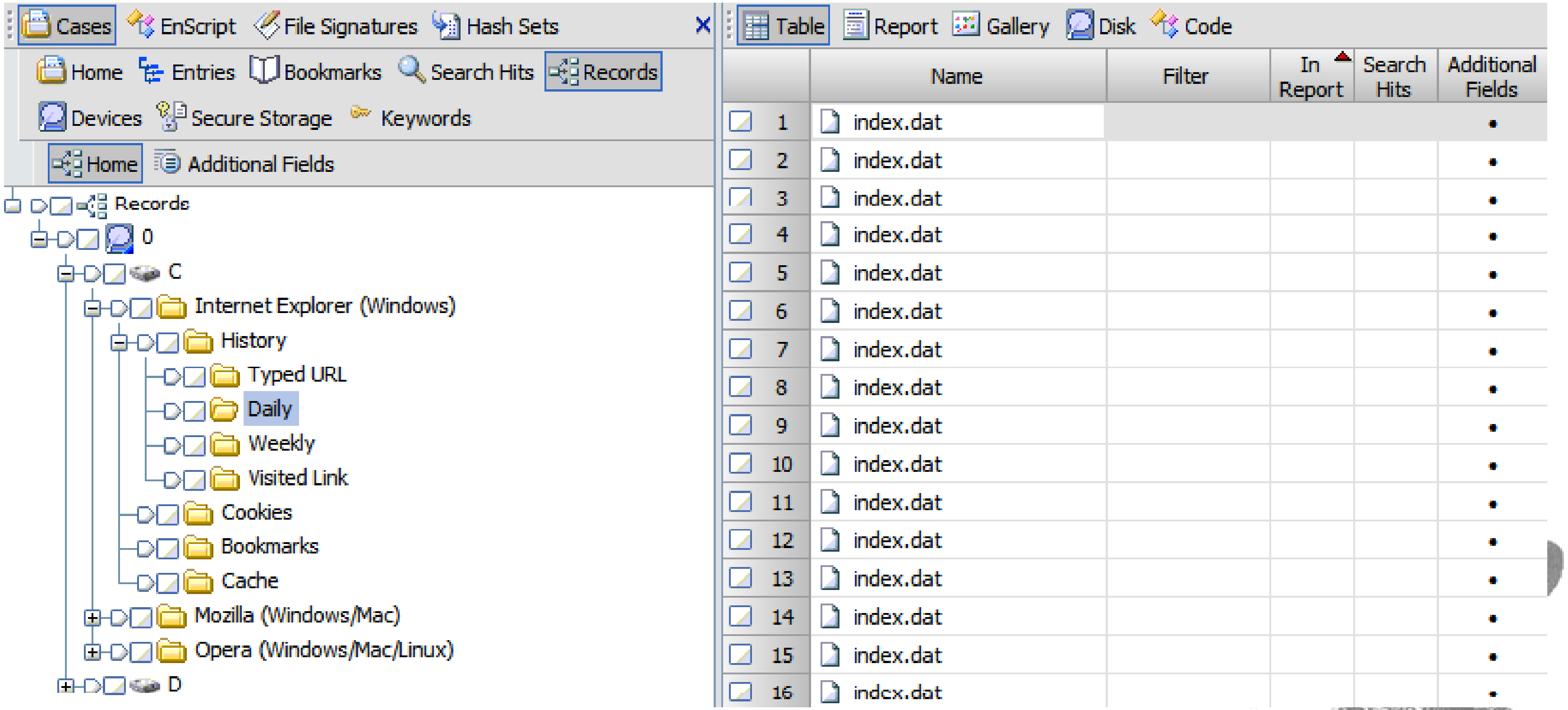
- □ Search for email
- □ Recovered deleted
- □ Outlook (PST)
- □ Outlook Express (DBX)
- □ Exchange (EDB)
- □ Lotus (NSF)
- □ AOL
- □ MBOX

Additional Options

- □ Verify file signatures
- □ Identify codepages
- ☑ Search for internet history
- □ Comprehensive search

Windows Operating System Artifacts

History Folder



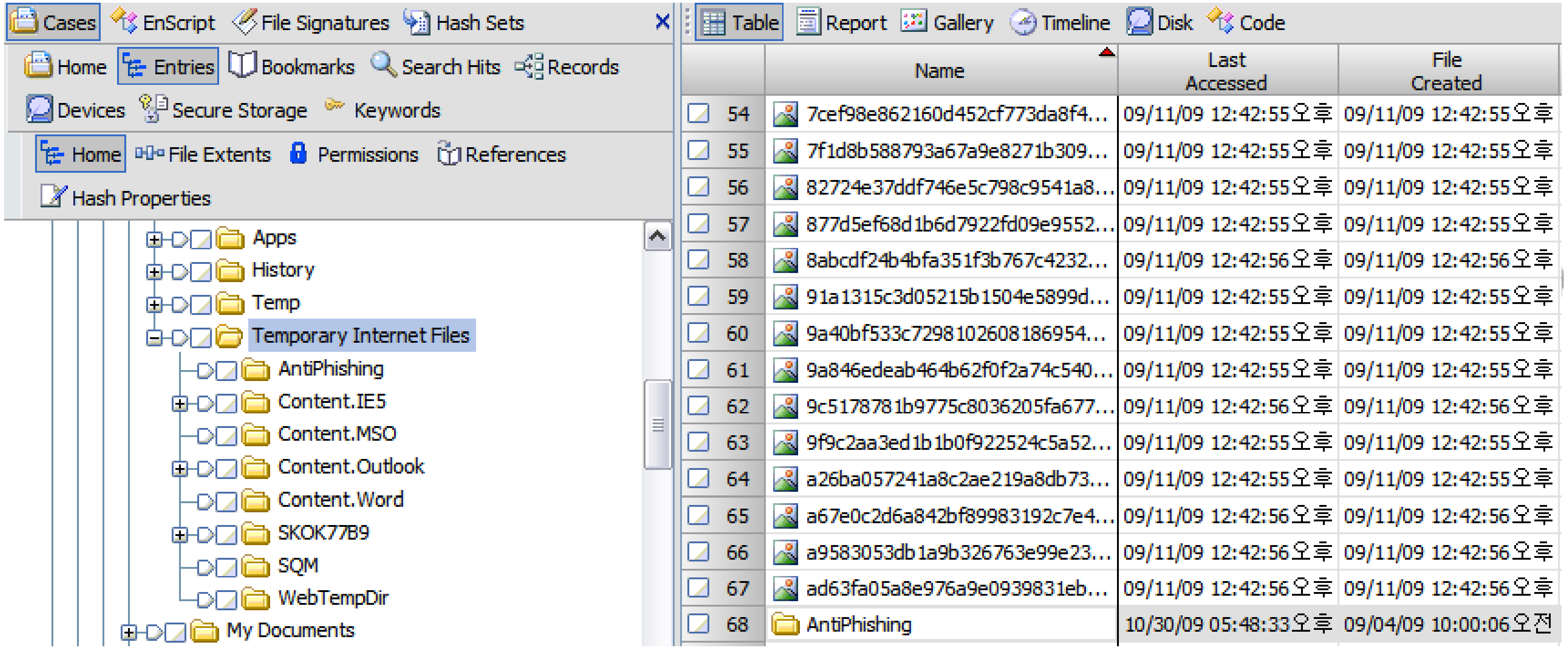
- Records
  - 0
    - C
      - Internet Explorer (Windows)
        - History
          - Typed URL
          - Daily
          - Weekly
          - Visited Link
        - Cookies
        - Bookmarks
        - Cache
      - Mozilla (Windows/Mac)
      - Opera (Windows/Mac/Linux)
    - D

		Name	Filter	In Report	Search Hits	Additional Fields
☐	1	index.dat				•
☐	2	index.dat				•
☐	3	index.dat				•
☐	4	index.dat				•
☐	5	index.dat				•
☐	6	index.dat				•
☐	7	index.dat				•
☐	8	index.dat				•
☐	9	index.dat				•
☐	10	index.dat				•
☐	11	index.dat				•
☐	12	index.dat				•
☐	13	index.dat				•
☐	14	index.dat				•
☐	15	index.dat				•
☐	16	index.dat				•

Windows Operating System Artifacts

Temporary Internet Files

- **XP** : C:\Documents and Settings*\%UserName%\Local Settings\Temporary Internet Files*
- **Vista** : C:\Users*\%UserName%\AppData\Local\Microsoft\Windows\Temporary Internet Files*



	Name	Last Accessed	File Created
54	7cef98e862160d452cf773da8f4...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
55	7f1d8b588793a67a9e8271b309...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
56	82724e37ddf746e5c798c9541a8...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
57	877d5ef68d1b6d7922fd09e9552...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
58	8abcdf24b4bfa351f3b767c4232...	09/11/09 12:42:56오후	09/11/09 12:42:56오후
59	91a1315c3d05215b1504e5899d...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
60	9a40bf533c7298102608186954...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
61	9a846edeab464b62f0f2a74c540...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
62	9c5178781b9775c8036205fa677...	09/11/09 12:42:56오후	09/11/09 12:42:56오후
63	9f9c2aa3ed1b1b0f922524c5a52...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
64	a26ba057241a8c2ae219a8db73...	09/11/09 12:42:55오후	09/11/09 12:42:55오후
65	a67e0c2d6a842bf89983192c7e4...	09/11/09 12:42:56오후	09/11/09 12:42:56오후
66	a9583053db1a9b326763e99e23...	09/11/09 12:42:56오후	09/11/09 12:42:56오후
67	ad63fa05a8e976a9e0939831eb...	09/11/09 12:42:56오후	09/11/09 12:42:56오후
68	AntiPhishing	10/30/09 05:48:33오후	09/04/09 10:00:06오전

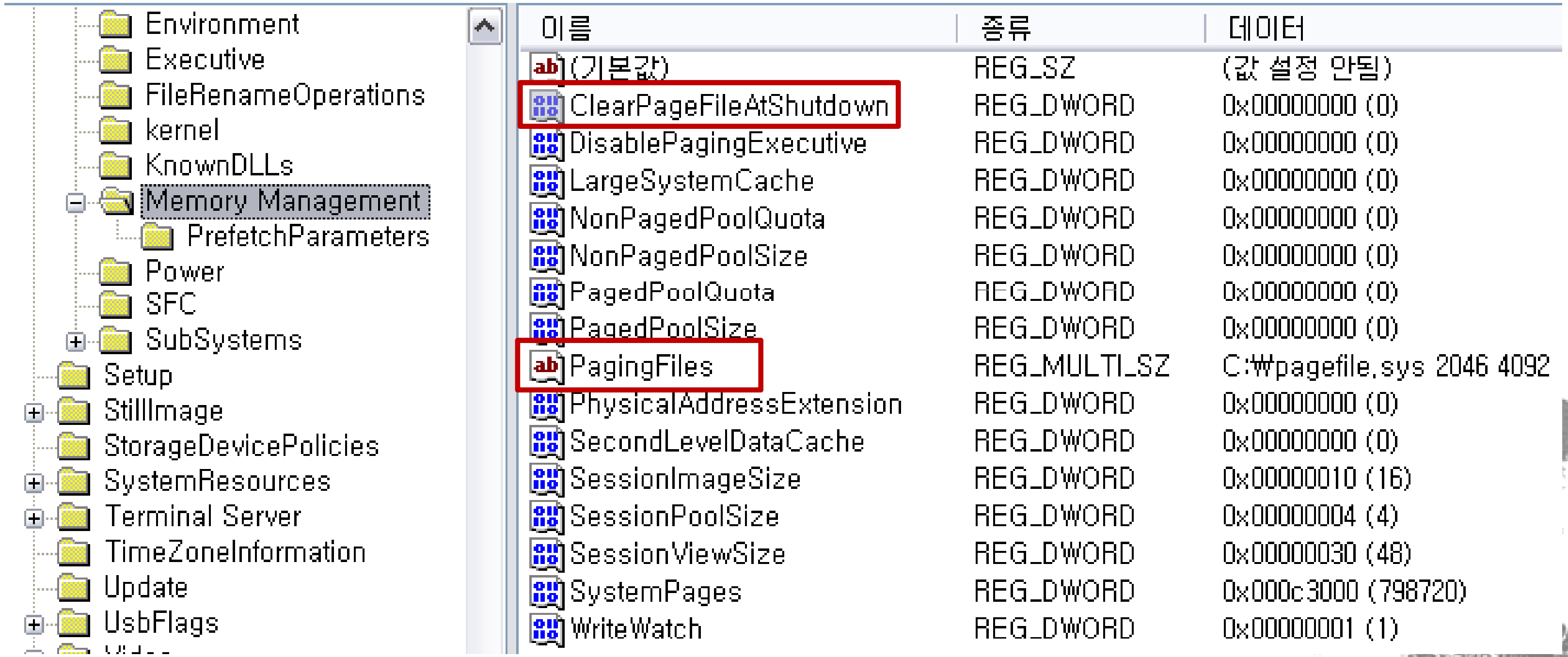
Windows Operating System Artifacts

Swap File

- Windows and other OS have *a limited supply of RAM with which to function*
- When run out of RAM, write some of the data *dedicated purpose is to cache RAM memory ➔ page file*
- Located in the root of the system drive (*pagefile.sys*)

Swap File

- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

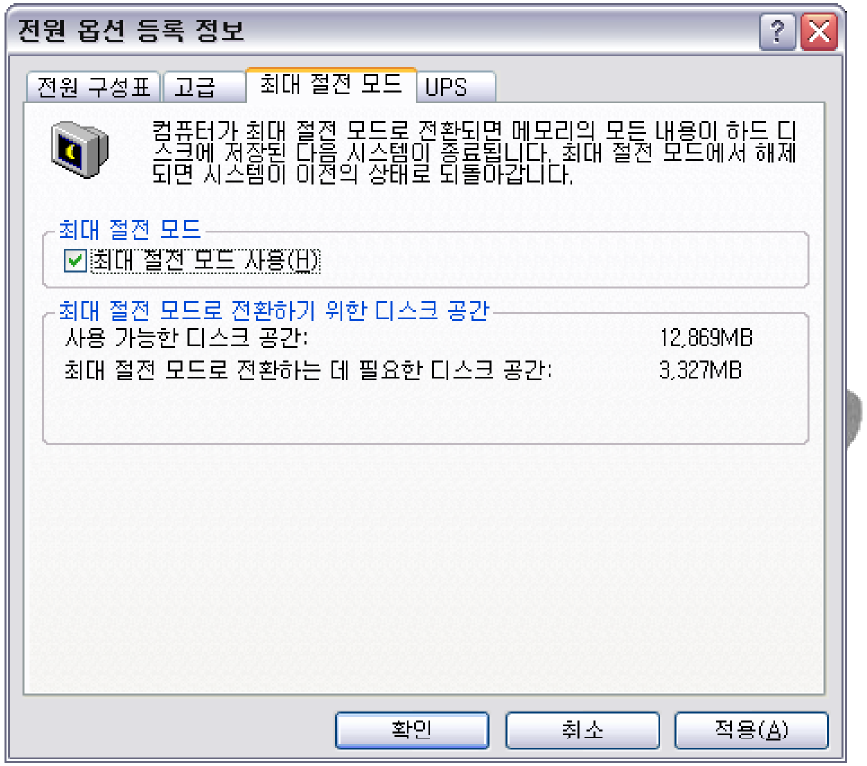


Environment
Executive
FileRenameOperations
kernel
KnownDLLs
Memory Management
PrefetchParameters
Power
SFC
SubSystems
Setup
StillImage
StorageDevicePolicies
SystemResources
Terminal Server
TimeZoneInformation
Update
UsbFlags

이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안됨)
ClearPageFileAtShutdown	REG_DWORD	0x00000000 (0)
DisablePagingExecutive	REG_DWORD	0x00000000 (0)
LargeSystemCache	REG_DWORD	0x00000000 (0)
NonPagedPoolQuota	REG_DWORD	0x00000000 (0)
NonPagedPoolSize	REG_DWORD	0x00000000 (0)
PagedPoolQuota	REG_DWORD	0x00000000 (0)
PagedPoolSize	REG_DWORD	0x00000000 (0)
PagingFiles	REG_MULTI_SZ	C:₩pagefile.sys 2046 4092
PhysicalAddressExtension	REG_DWORD	0x00000000 (0)
SecondLevelDataCache	REG_DWORD	0x00000000 (0)
SessionImageSize	REG_DWORD	0x00000010 (16)
SessionPoolSize	REG_DWORD	0x00000004 (4)
SessionViewSize	REG_DWORD	0x00000030 (48)
SystemPages	REG_DWORD	0x000c3000 (798720)
WriteWatch	REG_DWORD	0x00000001 (1)

Hibernation File

- Windows 2000, XP, and Vista *have a “hibernate” option*
- For a machine to power off, the contents of RAM must be written to a file
  - *hibernation file (hiberfil.sys),*
  - located in the root of the system drive



컴퓨터가 최대 절전 모드로 전환되면 메모리의 모든 내용이 하드 디스크에 저장된 다음 시스템이 종료됩니다. 최대 절전 모드에서 해제되면 시스템이 이전의 상태로 되돌아갑니다.

최대 절전 모드

☑ 최대 절전 모드 사용(H)

최대 절전 모드로 전환하기 위한 디스크 공간

사용 가능한 디스크 공간: 12,869MB

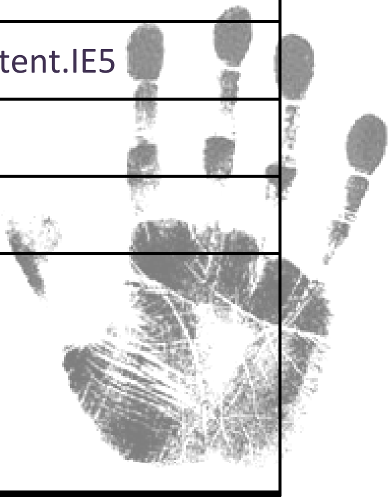
최대 절전 모드로 전환하는 데 필요한 디스크 공간: 3,327MB

Print Spooling

- skip…

Legacy Operating System Artifacts

Description	File Name and Path
Swap file	C:\WIN386.SWP
Recent folder whose contents appear in the Windows 9x Start -> Document menu	C:\Recent
Desktop items	C:\Desktop
My Documents folder	C:\My Documents
Internet cache and index.dat	C:\Windows\Temporary Internet Files\Content.IE5
Cookies files	C:\Windows\Cookies
Internet History files	C:\Windows\History
User profiles (if configured) (Each user will have their own set of the files contained in this directory	C:\Windows\Profiles\<user name>\

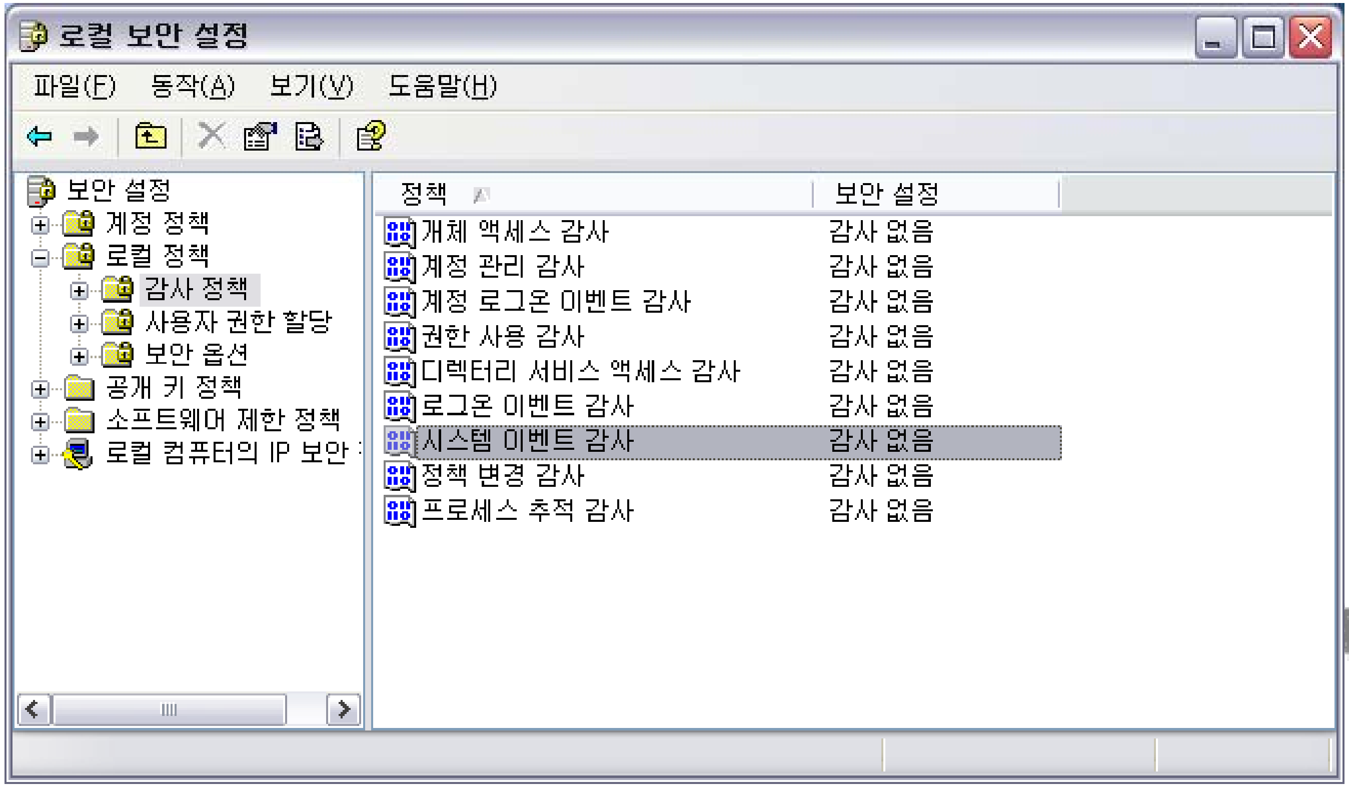


Windows Vista Volume Shadow Copy

- skip…

Windows Event Logs

- Kinds of Information Available in Event Logs
  - Default Setting : *No auditing*



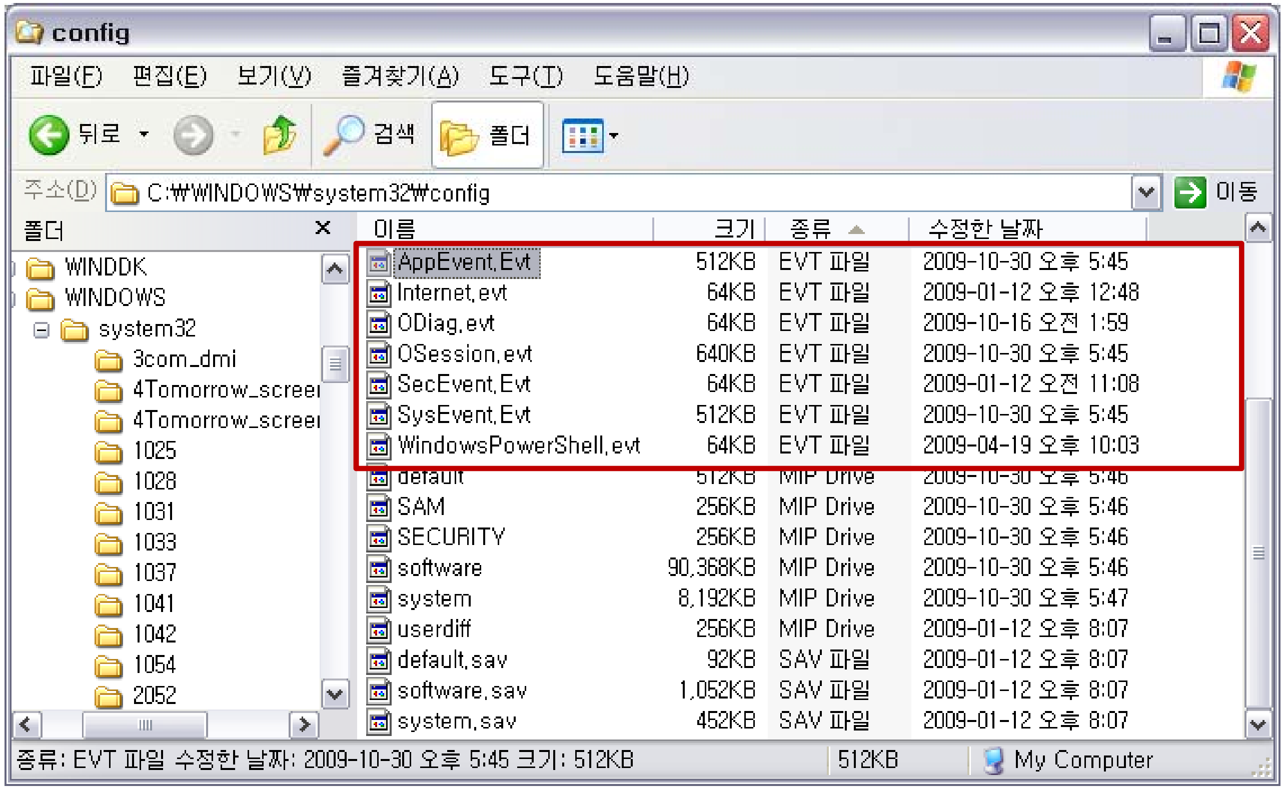
정책	보안 설정
개체 액세스 감사	감사 없음
계정 관리 감사	감사 없음
계정 로그온 이벤트 감사	감사 없음
권한 사용 감사	감사 없음
디렉터리 서비스 액세스 감사	감사 없음
로그온 이벤트 감사	감사 없음
시스템 이벤트 감사	감사 없음
정책 변경 감사	감사 없음
프로세스 추적 감사	감사 없음

Windows Event Logs

- Windows, except for Windows Vista, stores data in three file in the folder C:\Windows\System32\config :
  - *SecEvent.Evt* : The Security event log
  - *SysEvent.Evt* : The System event log
  - *AppEvent.Evt* : The Application log

Windows Event Logs

- Windows, except for Windows Vista, stores data in three file in the folder C:\Windows\System32\config :



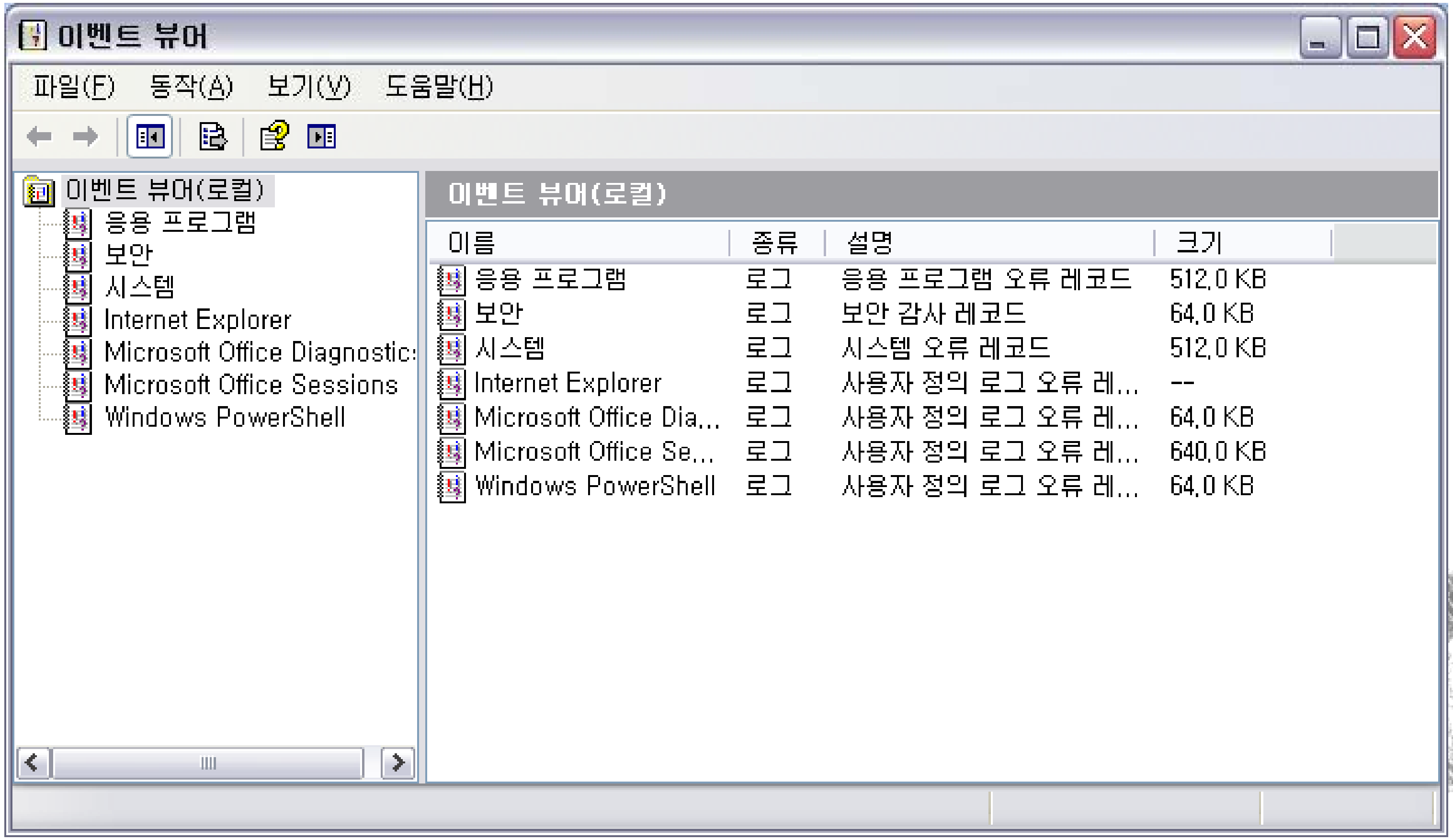
C:₩WINDOWS₩system32₩config

이름	크기	종류	수정한 날짜
AppEvent.Evt	512KB	EVT 파일	2009-10-30 오후 5:45
Internet.evt	64KB	EVT 파일	2009-01-12 오후 12:48
ODiag.evt	64KB	EVT 파일	2009-10-16 오전 1:59
OSession.evt	640KB	EVT 파일	2009-10-30 오후 5:45
SecEvent.Evt	64KB	EVT 파일	2009-01-12 오전 11:08
SysEvent.Evt	512KB	EVT 파일	2009-10-30 오후 5:45
WindowsPowerShell.evt	64KB	EVT 파일	2009-04-19 오후 10:03
default	512KB	MIP Drive	2009-10-30 오후 5:46
SAM	256KB	MIP Drive	2009-10-30 오후 5:46
SECURITY	256KB	MIP Drive	2009-10-30 오후 5:46
software	90,368KB	MIP Drive	2009-10-30 오후 5:46
system	8,192KB	MIP Drive	2009-10-30 오후 5:47
userdiff	256KB	MIP Drive	2009-01-12 오후 8:07
default.sav	92KB	SAV 파일	2009-01-12 오후 8:07
software.sav	1,052KB	SAV 파일	2009-01-12 오후 8:07
system.sav	452KB	SAV 파일	2009-01-12 오후 8:07

종류: EVT 파일 수정한 날짜: 2009-10-30 오후 5:45 크기: 512KB | 512KB | My Computer

Windows Event Logs

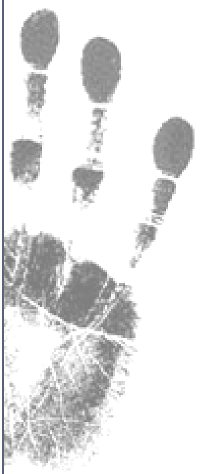
- Natively Event Viewer



이벤트 뷰어(로컬)
- 응용 프로그램
- 보안
- 시스템
- Internet Explorer
- Microsoft Office Diagnostic:
- Microsoft Office Sessions
- Windows PowerShell

이벤트 뷰어(로컬)

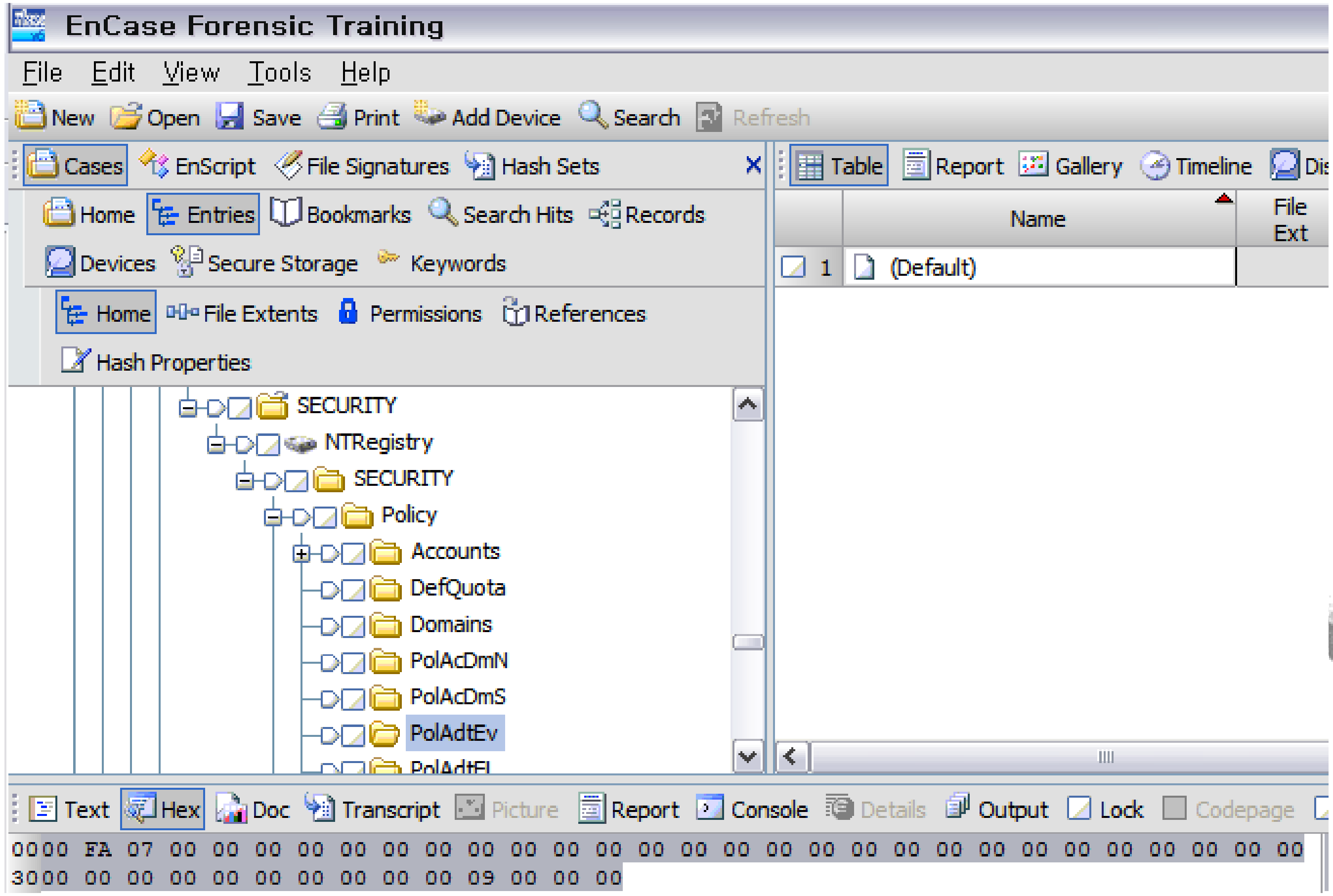
이름	종류	설명	크기
응용 프로그램	로그	응용 프로그램 오류 레코드	512,0 KB
보안	로그	보안 감사 레코드	64,0 KB
시스템	로그	시스템 오류 레코드	512,0 KB
Internet Explorer	로그	사용자 정의 로그 오류 레...	--
Microsoft Office Dia...	로그	사용자 정의 로그 오류 레...	64,0 KB
Microsoft Office Se...	로그	사용자 정의 로그 오류 레...	640,0 KB
Windows PowerShell	로그	사용자 정의 로그 오류 레...	64,0 KB



Windows Operating System Artifacts

Windows Event Logs

- Determining Levels of Auditing


EnCase Forensic Training
File Edit View Tools Help
New Open Save Print Add Device Search Refresh
Cases EnScript File Signatures Hash Sets
Home Entries Bookmarks Search Hits Records
Devices Secure Storage Keywords
Home File Extents Permissions References
Hash Properties
Table Report Gallery Timeline Dis
Name
File Ext
1 (Default)
SECURITY
NTRegistry
SECURITY
Policy
Accounts
DefQuota
Domains
PolAcDmN
PolAcDmS
PolAdtEv
PolAdtEl
Text Hex Doc Transcript Picture Report Console Details Output Lock Codepage

```
0000 FA 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
3000 00 00 00 00 00 00 00 00 00 09 00 00 00
```

forensic-proof.com

20 October 2009

Windows Event Logs

- Determining Levels of Auditing

Byte Offset	Description
00	00 No Auditing / 01 Auditing
04	System Events Audit Setting
08	Logon Events Audit Setting
12	Object Access Audit Setting
16	Privilege Use Audit Setting
20	Process Tracking Audit Setting
24	Policy Chance Audit Setting
28	Account Management Audit Setting
32	Directory Service Access Audit Setting
36	Account Logon Audit Setting

Windows Event Logs

- Windows Vista, C:\Windows\system32\winevt\logs :
  - *Security.Evtx* : The Security event log
  - *System.Evtx* : The System event log
  - *Application.Evtx* : The Application log

Exercise 9.1

- Windows Artifacts Recovery :

Question & Answer