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)

Date and Times

- Dates and times are ubiquitous on any modern operating system
- Their uses are countless, and their storage formats vary
- *local time* vs. *Greenwich mean time(GMT)*

Date and Times - Time Zone

- The world is divided into *time zones* and computers must keep track of time relative to those time zones
- The various OS must implement *methods differences*
- In order that accurately interpret date and time stamps

  ➔ understanding OS and EnCase resolve these differences
- For Windows, file attributes *dates and times (MAC)*
- The File system in use determines whether the date and time is stored in *local time or in GMT*

Windows Operating System Artifacts

Date and Times - Time Zone

- FAT file system are stored in the *32-byte DOS directory entry in local time*
- This time zone for which computer configured

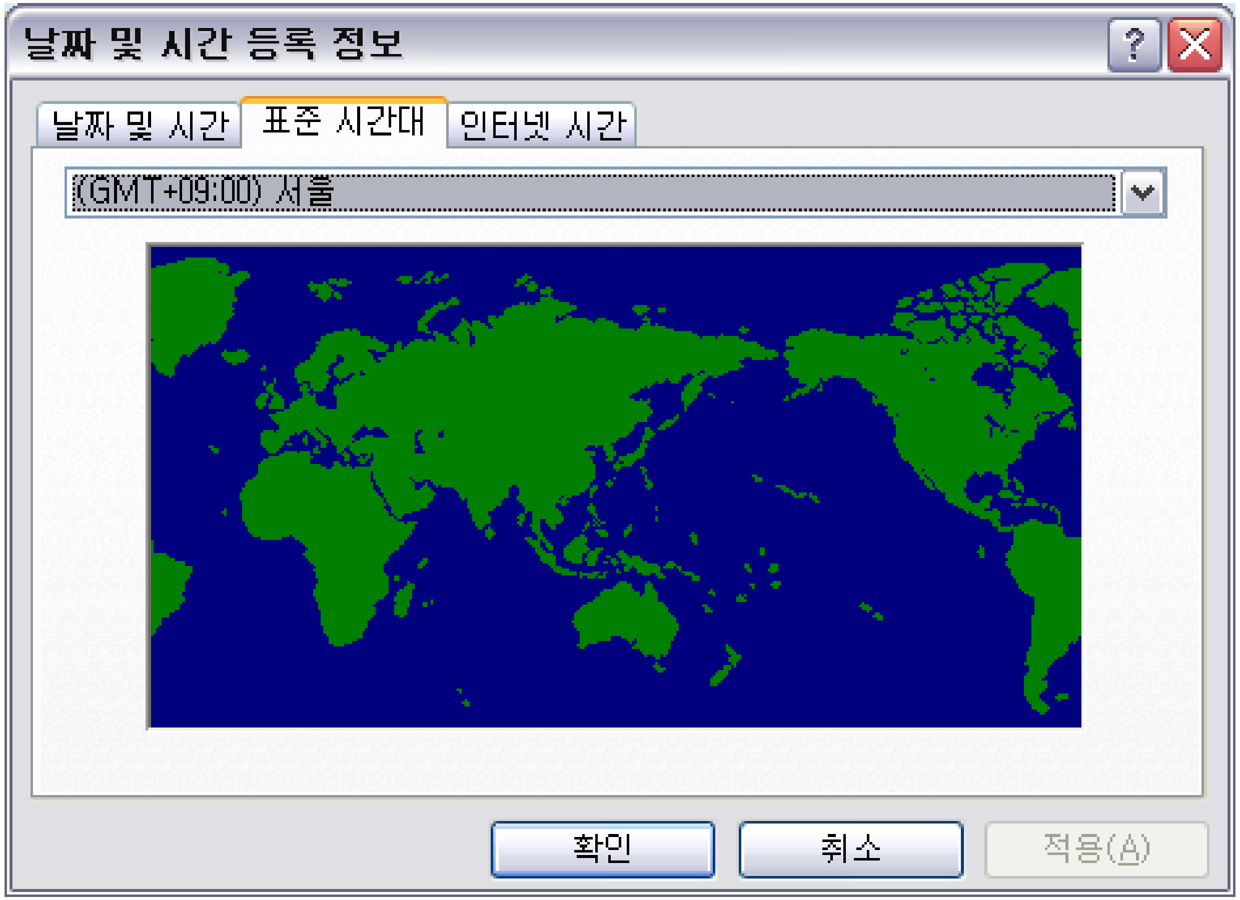
- NTFS, stored for file creation, last written, last accessed, and last entry modified are stored *in GMT using a 64-bit Windows date and time stamp*
- *The OS displays the user based on the local time zone offset*

Date and Times - Time Zone

- Computers can be moved from one zone to another, *incorrectly configure..*
- The time and time zone offset may not be accurate
- *To resolve these issues, need to know the machine's BIOS time*

➔ apply the correct time zone offset

Date and Times - Time Zone



(GMT+09:00) 서울

Date and Times – Unix Time Stamp

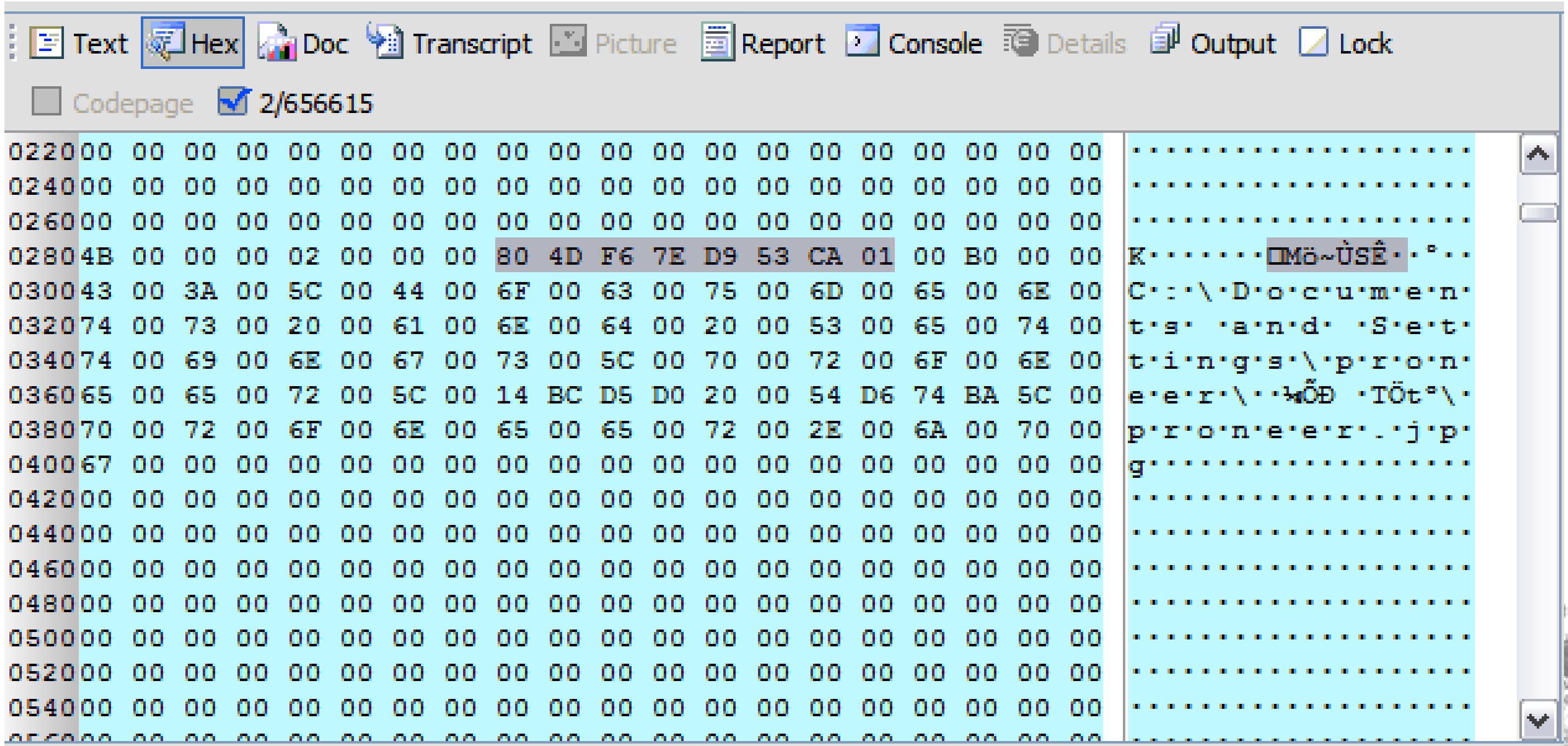
- uses a label Unix, do not think this date format is *limited to Unix machines*
- 32-bit integer value that represents the number of seconds
- Starting on January 1, 1970, 00:00:00 GMT ~
- 2^{32} : 4,294,967,296
- *Monday, December, 2, 2030, at 19:42:58 GMT seconds will have lapsed*

Date and Times – Windows 64-Bit Time Stamp

- 64-bit integer
- Windows tracks the number of 100-nanosecond intervals
- Starting on January 1, 1601, at 00:00:00 GMT
- 2^{64} : 18,446,744,073,709,500,000
- This time stamp can address a date range of 58,000 plus years

Date and Times – Windows 64-Bit Time Stamp

- 8 byte string (64 bits), *most significant value is 01h*

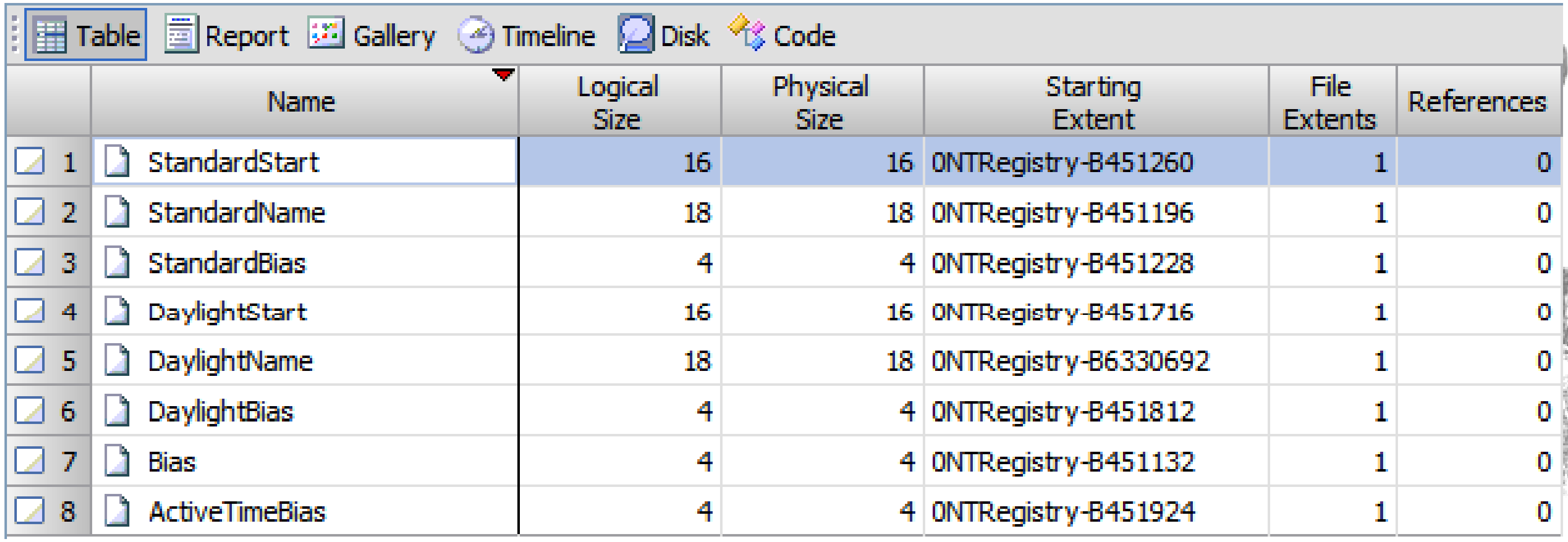


```
0220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0240 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0260 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0280 4B 00 00 00 02 00 00 00 80 4D F6 7E D9 53 CA 01 00 B0 00 00  K·······□Mö~ÙSÊ··°··
0300 43 00 3A 00 5C 00 44 00 6F 00 63 00 75 00 6D 00 65 00 6E 00  C·:·\·D·o·c·u·m·e·n·
0320 74 00 73 00 20 00 61 00 6E 00 64 00 20 00 53 00 65 00 74 00  t·s· ·a·n·d· ·S·e·t·
0340 74 00 69 00 6E 00 67 00 73 00 5C 00 70 00 72 00 6F 00 6E 00  t·i·n·g·s·\·p·r·o·n·
0360 65 00 65 00 72 00 5C 00 14 BC D5 D0 20 00 54 D6 74 BA 5C 00  e·e·r·\··¼ÕÐ ·TÖtº\·
0380 70 00 72 00 6F 00 6E 00 65 00 65 00 72 00 2E 00 6A 00 70 00  p·r·o·n·e·e·r·.·j·p·
0400 67 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  g···················
0420 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0440 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0460 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0480 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0520 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
0540 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ····················
```

Date and Times – Adjusting for Time Zone Offsets

- The time zone offset is stored in the registry
- System registry file as you would View File Structure
- Navigate to

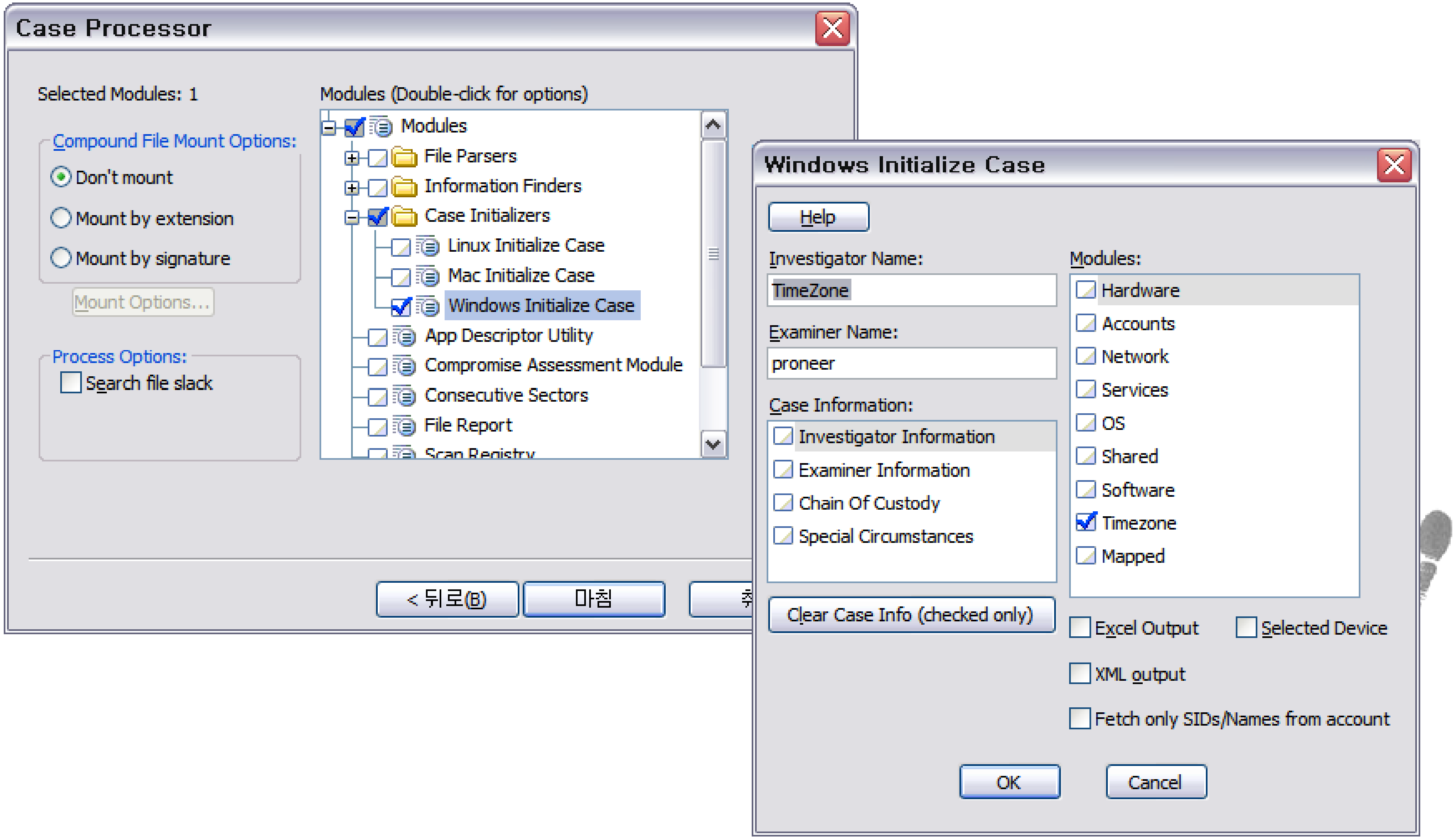
  System\NTRegistry\ControlSet00n\Control\TimeZoneInformation



	Name	Logical Size	Physical Size	Starting Extent	File Extents	References
1	StandardStart	16	16	0NTRegistry-B451260	1	0
2	StandardName	18	18	0NTRegistry-B451196	1	0
3	StandardBias	4	4	0NTRegistry-B451228	1	0
4	DaylightStart	16	16	0NTRegistry-B451716	1	0
5	DaylightName	18	18	0NTRegistry-B6330692	1	0
6	DaylightBias	4	4	0NTRegistry-B451812	1	0
7	Bias	4	4	0NTRegistry-B451132	1	0
8	ActiveTimeBias	4	4	0NTRegistry-B451924	1	0

Windows Operating System Artifacts

Date and Times – Adjusting for Time Zone Offsets



Case Processor

Selected Modules: 1

Compound File Mount Options:
- ● Don't mount
- ○ Mount by extension
- ○ Mount by signature

Process Options:
- □ Search file slack

Modules (Double-click for options)
- ☑ Modules
  - □ File Parsers
  - □ Information Finders
  - ☑ Case Initializers
    - □ Linux Initialize Case
    - □ Mac Initialize Case
    - ☑ Windows Initialize Case
  - □ App Descriptor Utility
  - □ Compromise Assessment Module
  - □ Consecutive Sectors
  - □ File Report
  - □ Scan Registry

Windows Initialize Case

Investigator Name: TimeZone

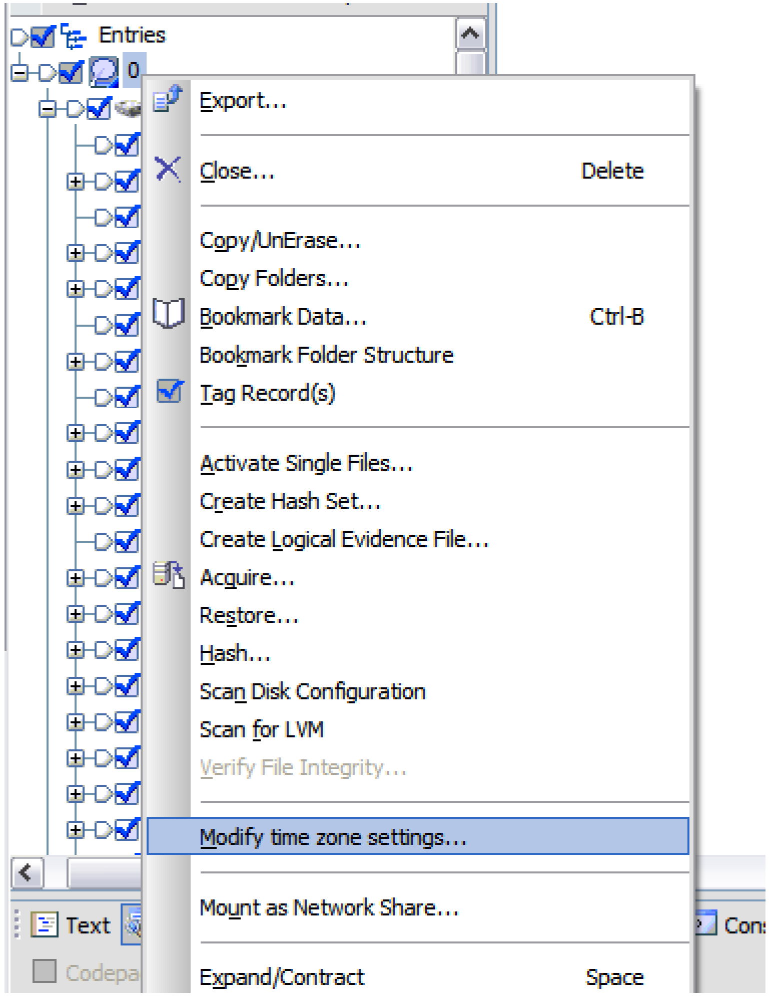
Examiner Name: proneer

Case Information:
- □ Investigator Information
- □ Examiner Information
- □ Chain Of Custody
- □ Special Circumstances

Modules:
- □ Hardware
- □ Accounts
- □ Network
- □ Services
- □ OS
- □ Shared
- □ Software
- ☑ Timezone
- □ Mapped

- □ Excel Output
- □ Selected Device
- □ XML output
- □ Fetch only SIDs/Names from account

Date and Times – Adjusting for Time Zone Offsets



Recycle Bin

- By default when a user deletes a file in Windows ➔ Recycle Bin
- When a file is deleted…
  - a directory entry or MFT entry is deleted.
  - a directory entry or MFT entry is made for the file in the Recycle Bin.
- The new file name bears no resemblance to the original file name.

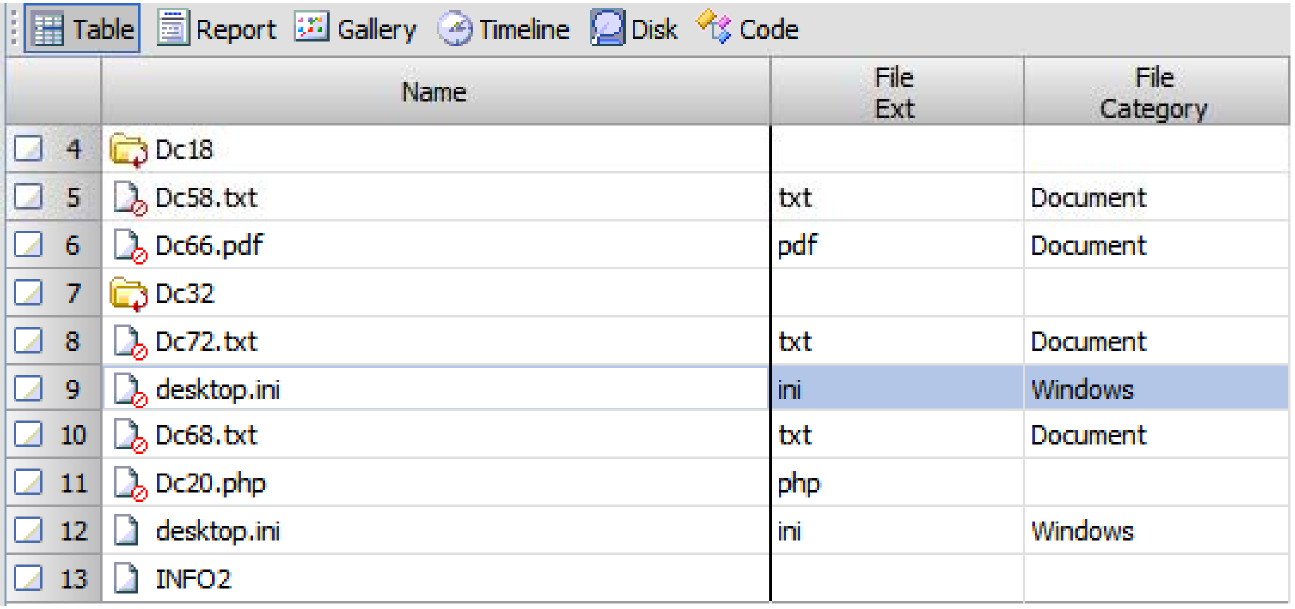
Recycle Bin

- The new file naming rule :
  - D [*original drive letter of file*] [*index number*] . [*original file extension*]
  - For example,
    - C:\My Files\letter.doc were deleted and sent to the Recycle Bin.
    - its new file name in the Recycle Bin would be **DC1.doc** (if first file sent)

Windows Operating System Artifacts

Recycle Bin – The INFO2 File

- The deleted file no longer bears its original file name, location, and so on..
- The **INFO2** file is a database containing information about the files in the Recycle Bin.



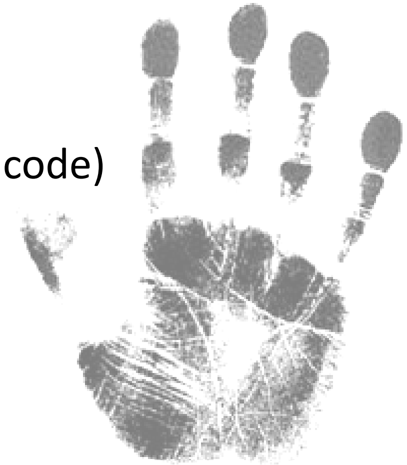
	Name	File Ext	File Category
□ 4	Dc18		
□ 5	Dc58.txt	txt	Document
□ 6	Dc66.pdf	pdf	Document
□ 7	Dc32		
□ 8	Dc72.txt	txt	Document
□ 9	desktop.ini	ini	Windows
□ 10	Dc68.txt	txt	Document
□ 11	Dc20.php	php	
□ 12	desktop.ini	ini	Windows
□ 13	INFO2		

Windows Operating System Artifacts

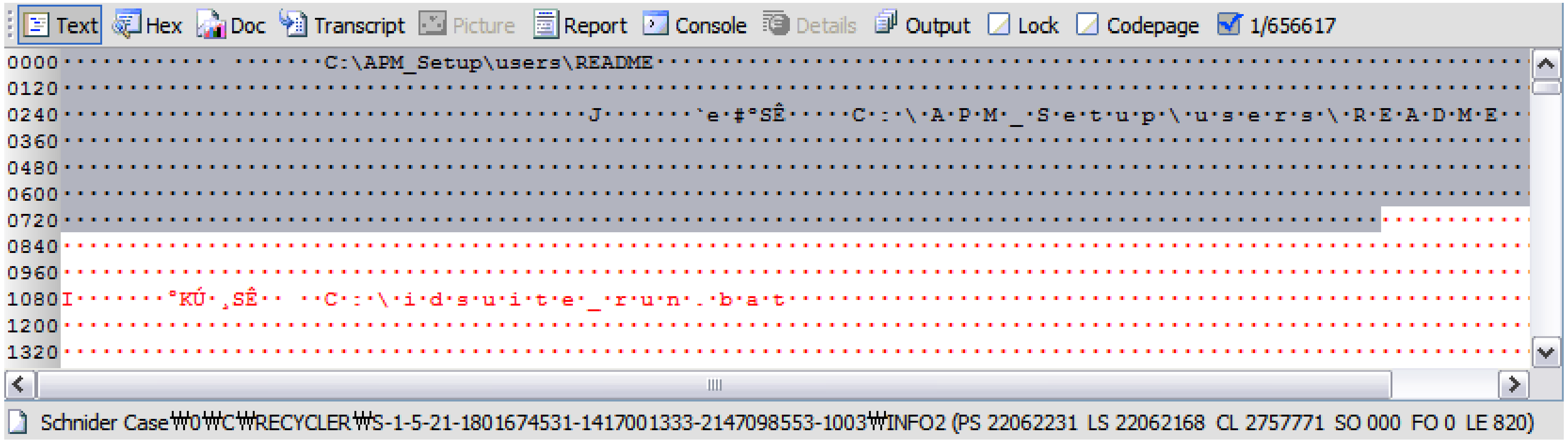
Recycle Bin – The INFO2 File

Operating System	Recycle Bin Folder Name	INFO2 Record Length
Windows 9x/ME	Recycled	280 Bytes
Windows NT	Recycler	800 Bytes
Windows 2000	Recycler	800 Bytes
Windows XP/2003	Recycler	800 Bytes

- the contents of the INFO2 file :
  - The file’s original file name and path (entered twice, ASCII and Unicode)
  - The date and time of deletion
  - The index number
- Additional information visit : http://forensic-proof.com/

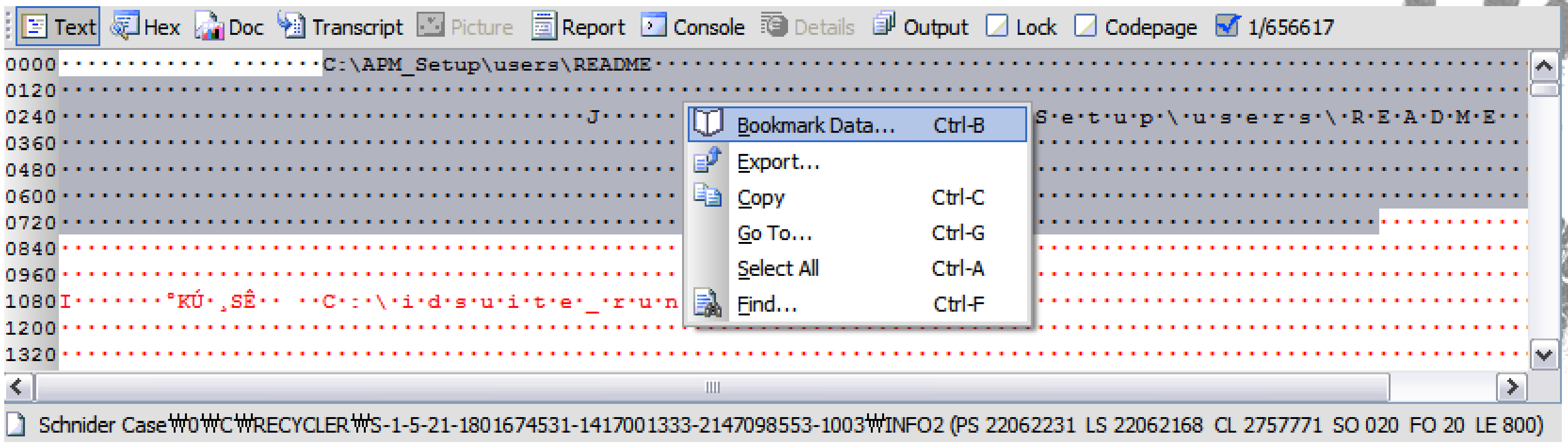


Recycle Bin – The INFO2 File



```
0000·············  ·······C:\APM_Setup\users\README·················································
0120··········································································································
0240········································J·······`e·#°SÊ····C·:·\·A·P·M·_·S·e·t·u·p·\·u·s·e·r·s·\·R·E·A·D·M·E··
0360··········································································································
0480··········································································································
0600··········································································································
0720··········································································································
0840··········································································································
0960··········································································································
1080I·······°KÚ·¸SÊ··  ··C·:·\·i·d·s·u·i·t·e·_·r·u·n·.·b·a·t··························································
1200··········································································································
1320··········································································································
```

Schnider Case₩0₩C₩RECYCLER₩S-1-5-21-1801674531-1417001333-2147098553-1003₩INFO2 (PS 22062231 LS 22062168 CL 2757771 SO 000 FO 0 LE 820)

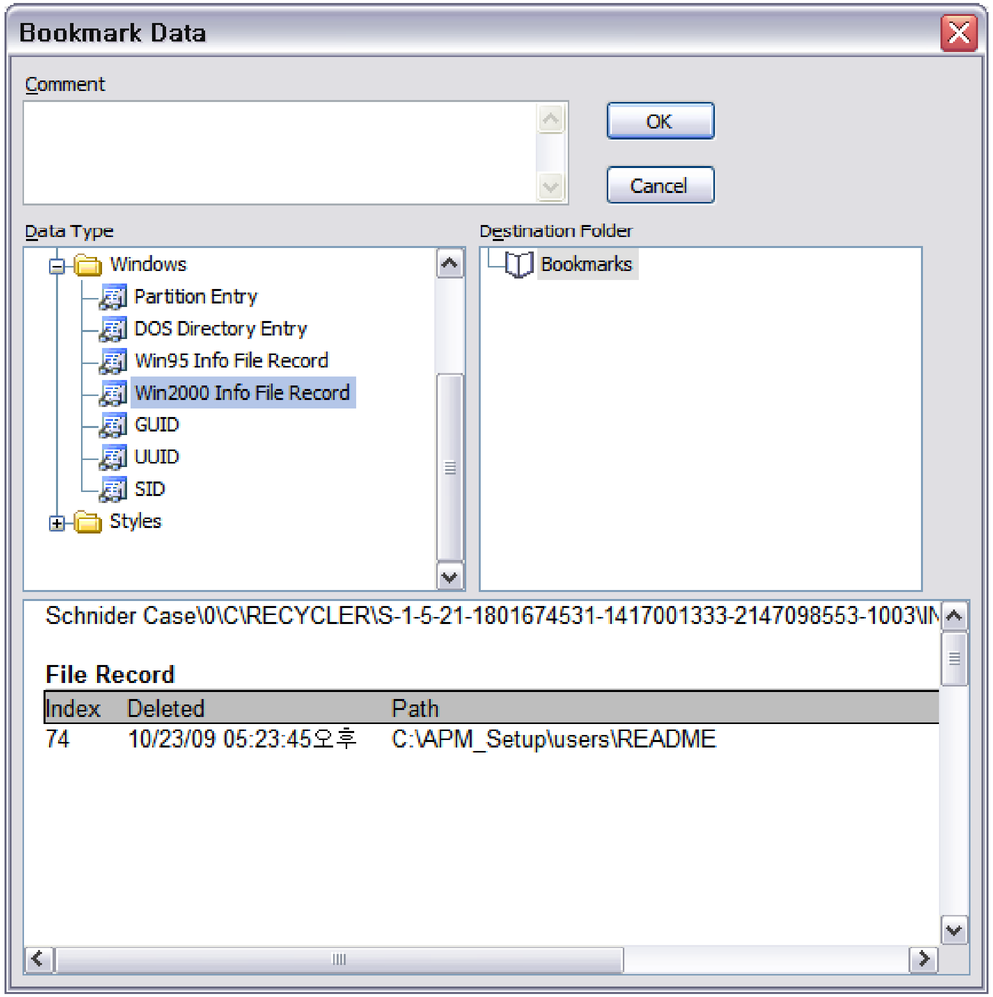


```
0000·············  ·······C:\APM_Setup\users\README·················································
0120··········································································································
0240········································J·····                    S·e·t·u·p·\·u·s·e·r·s·\·R·E·A·D·M·E··
0360·····················································                    ·······························
0480·····················································                    ·······························
0600·····················································                    ·······························
0720·····················································                    ·······························
0840·····················································                    ·······························
0960·····················································                    ·······························
1080I·······°KÚ·¸SÊ··  ··C·:·\·i·d·s·u·i·t·e·_·r·u·n                    ·······························
1200·····················································                    ·······························
1320··········································································································
```

Schnider Case₩0₩C₩RECYCLER₩S-1-5-21-1801674531-1417001333-2147098553-1003₩INFO2 (PS 22062231 LS 22062168 CL 2757771 SO 020 FO 20 LE 800)

Windows Operating System Artifacts

Recycle Bin – The INFO2 File



Schnider Case\0\C\RECYCLER\S-1-5-21-1801674531-1417001333-2147098553-1003\IN

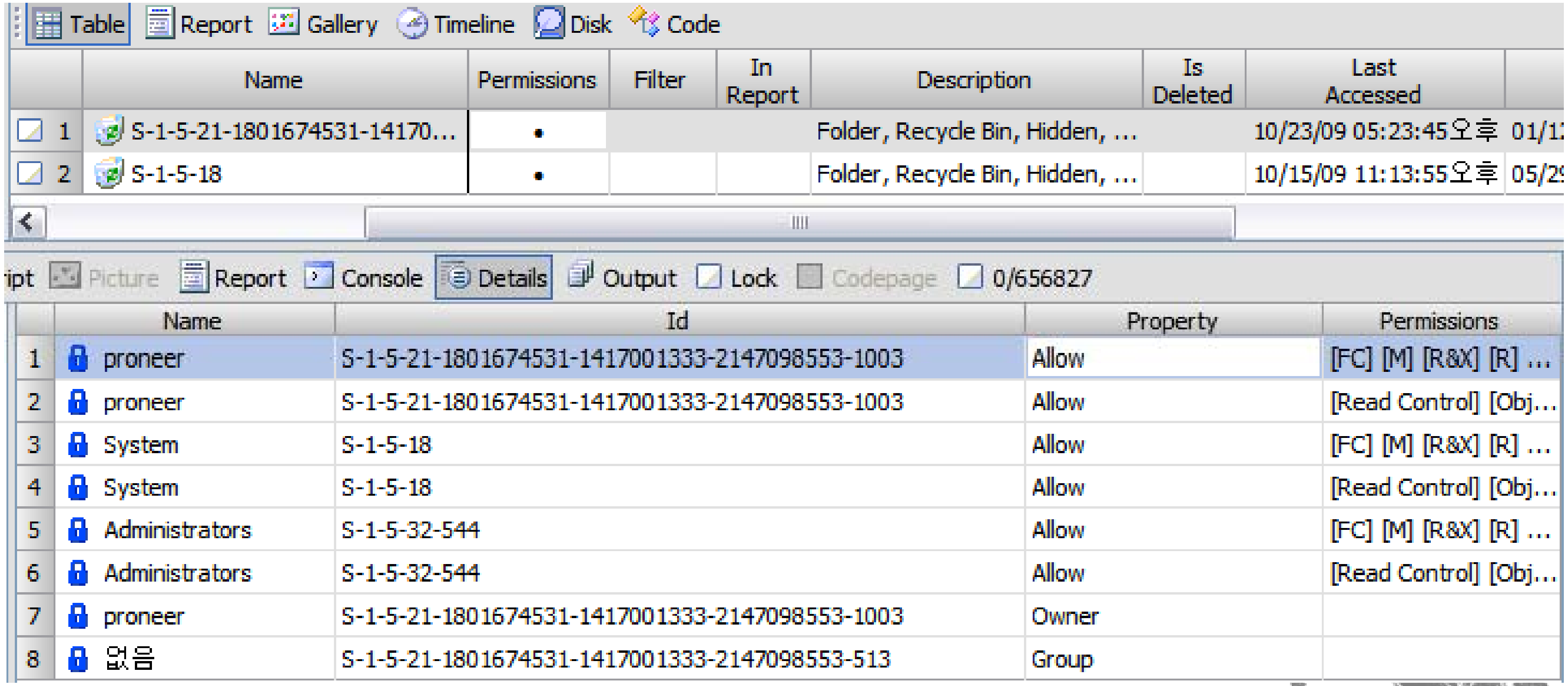
File Record

Index	Deleted	Path
74	10/23/09 05:23:45오후	C:\APM_Setup\users\README

Recycle Bin – Determining the Owner of Files

- Windows NT/2K/XP/2003,
  - a Recycle Bin folder bearing the user's security ID (SID) ➔ uniquely name folder
- Deleted files can be traced back to their owner through the SID
- SID involves mounting the Security Account Manager (SAM) registry file

Recycle Bin – Determining the Owner of Files



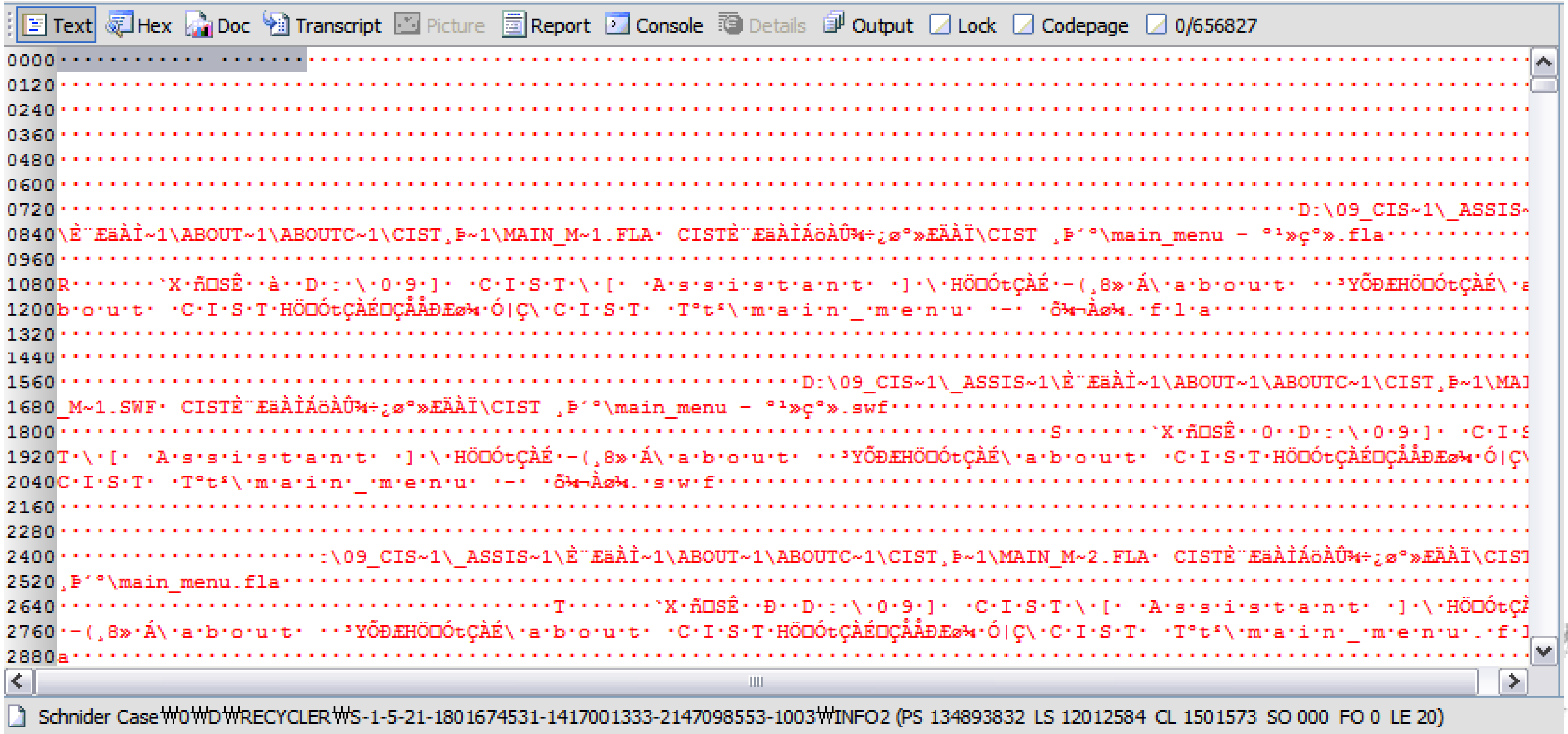
	Name	Permissions	Filter	In Report	Description	Is Deleted	Last Accessed	
□ 1	S-1-5-21-1801674531-14170…	•			Folder, Recycle Bin, Hidden, …		10/23/09 05:23:45오후	01/1
□ 2	S-1-5-18	•			Folder, Recycle Bin, Hidden, …		10/15/09 11:13:55오후	05/2

	Name	Id	Property	Permissions
1	proneer	S-1-5-21-1801674531-1417001333-2147098553-1003	Allow	[FC] [M] [R&X] [R] …
2	proneer	S-1-5-21-1801674531-1417001333-2147098553-1003	Allow	[Read Control] [Obj…
3	System	S-1-5-18	Allow	[FC] [M] [R&X] [R] …
4	System	S-1-5-18	Allow	[Read Control] [Obj…
5	Administrators	S-1-5-32-544	Allow	[FC] [M] [R&X] [R] …
6	Administrators	S-1-5-32-544	Allow	[Read Control] [Obj…
7	proneer	S-1-5-21-1801674531-1417001333-2147098553-1003	Owner	
8	없음	S-1-5-21-1801674531-1417001333-2147098553-513	Group	

Recycle Bin – Determining the Owner of Files

- When the user empties the entire Recycle Bin,
  - directory or MFT entries for all files are marked as deleted
- The INFO2 database is adjusted to its default or empty size of 20 bytes (Windows XP/2003)
- So, you examine the file slack that immediately follows the 20-bytes header

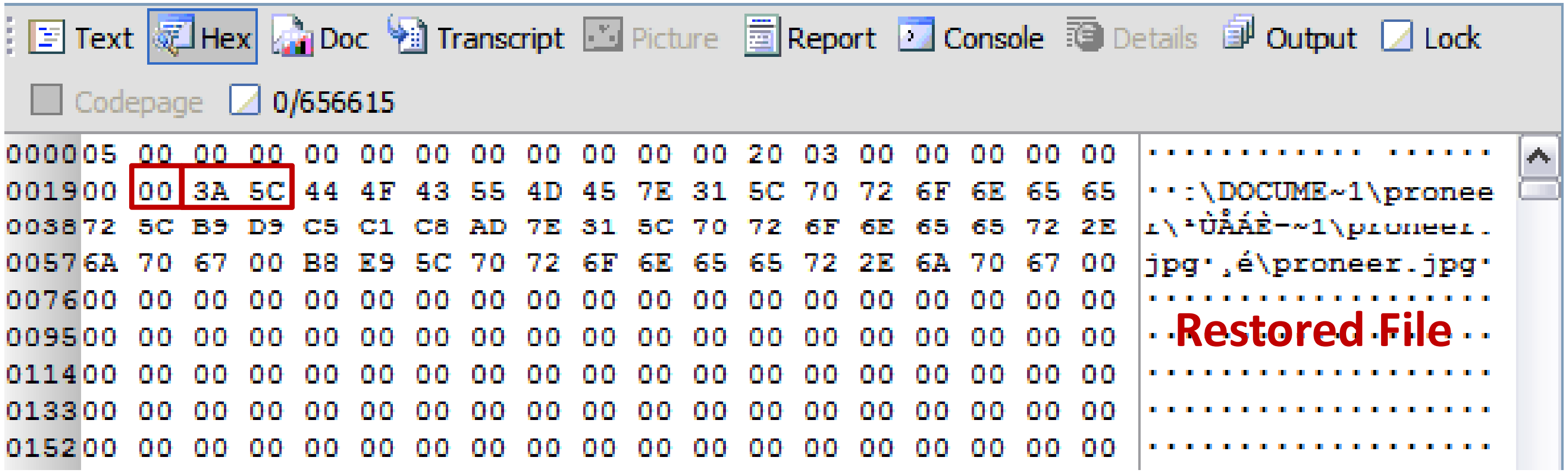
Recycle Bin – Determining the Owner of Files



```
0000············· ·······································································································
0120························································································································
0240························································································································
0360························································································································
0480························································································································
0600························································································································
0720·····································································································D:\09_CIS~1\_ASSIS~
0840\È¨ÆäÀÌ~1\ABOUT~1\ABOUTC~1\CIST¸Þ~1\MAIN_M~1.FLA· CISTÈ¨ÆäÀÌÁöÀÛ¾÷¿ø°»ÆÄÀÏ\CIST ¸Þ´º\main_menu - º¹»ç°».fla··········
0960························································································································
1080R·······`X·ñ□SÊ··à··D·:·\·0·9·]· ·C·I·S·T·\·[· ·A·s·s·i·s·t·a·n·t· ·]·\·HÖ□ÓtÇÀÉ·–(¸8»·Á\·a·b·o·u·t· ··³YÕÐÆHÖ□ÓtÇÀÉ\·a
1200b·o·u·t· ·C·I·S·T·HÖ□ÓtÇÀÉ□ÇÅÅÐÆø¾·Ó|Ç\·C·I·S·T· ·Tºt²\·m·a·i·n·_·m·e·n·u· ·–· ·õ¾¬Åø¾.·f·l·a························
1320························································································································
1440························································································································
1560·························································D:\09_CIS~1\_ASSIS~1\È¨ÆäÀÌ~1\ABOUT~1\ABOUTC~1\CIST¸Þ~1\MAI
1680_M~1.SWF· CISTÈ¨ÆäÀÌÁöÀÛ¾÷¿ø°»ÆÄÀÏ\CIST ¸Þ´º\main_menu - º¹»ç°».swf··················································
1800·································································S·······`X·ñ□SÊ··0··D·:·\·0·9·]· ·C·I·S
1920T·\·[· ·A·s·s·i·s·t·a·n·t· ·]·\·HÖ□ÓtÇÀÉ·–(¸8»·Á\·a·b·o·u·t· ··³YÕÐÆHÖ□ÓtÇÀÉ\·a·b·o·u·t· ·C·I·S·T·HÖ□ÓtÇÀÉ□ÇÅÅÐÆø¾·Ó|Ç\
2040C·I·S·T· ·Tºt²\·m·a·i·n·_·m·e·n·u· ·–· ·õ¾¬Åø¾.·s·w·f·························································
2160························································································································
2280························································································································
2400·····················:\09_CIS~1\_ASSIS~1\È¨ÆäÀÌ~1\ABOUT~1\ABOUTC~1\CIST¸Þ~1\MAIN_M~2.FLA· CISTÈ¨ÆäÀÌÁöÀÛ¾÷¿ø°»ÆÄÀÏ\CIST
2520¸Þ´º\main_menu.fla·····································································································
2640········································T·······`X·ñ□SÊ··Ð··D·:·\·0·9·]· ·C·I·S·T·\·[· ·A·s·s·i·s·t·a·n·t· ·]·\·HÖ□ÓtÇÀ
2760·–(¸8»·Á\·a·b·o·u·t· ··³YÕÐÆHÖ□ÓtÇÀÉ\·a·b·o·u·t· ·C·I·S·T·HÖ□ÓtÇÀÉ□ÇÅÅÐÆø¾·Ó|Ç\·C·I·S·T· ·Tºt²\·m·a·i·n·_·m·e·n·u·.·f·l
2880a·······················································································································
```

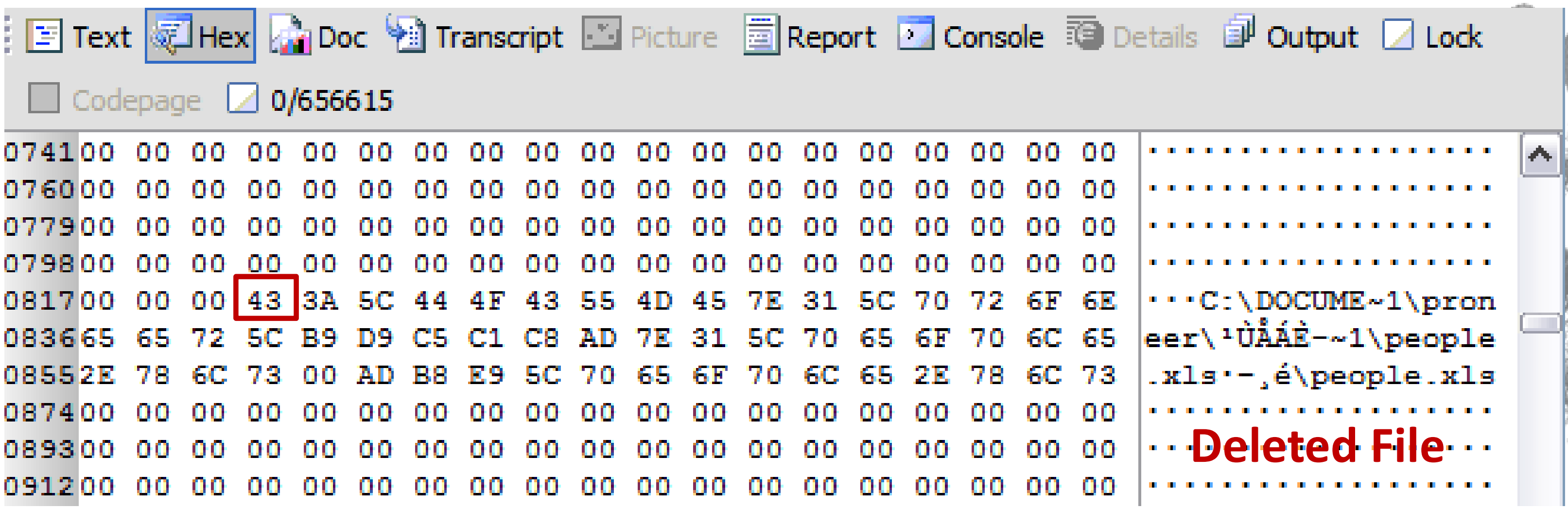
Schnider Case₩0₩D₩RECYCLER₩S-1-5-21-1801674531-1417001333-2147098553-1003₩INFO2 (PS 134893832 LS 12012584 CL 1501573 SO 000 FO 0 LE 20)

Recycle Bin – Files Restored or Deleted from the Recycle Bin



```
000005 00 00 00 00 00 00 00 00 00 00 00 20 03 00 00 00 00 00  ............ ......
001900 00 3A 5C 44 4F 43 55 4D 45 7E 31 5C 70 72 6F 6E 65 65  ..:\DOCUME~1\pronee
003872 5C B9 D9 C5 C1 C8 AD 7E 31 5C 70 72 6F 6E 65 65 72 2E  r\¹ÙÅÁÈ-~1\proneer.
00576A 70 67 00 B8 E9 5C 70 72 6F 6E 65 65 72 2E 6A 70 67 00  jpg.¸é\proneer.jpg.
007600 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
009500 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
011400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
013300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
015200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
```

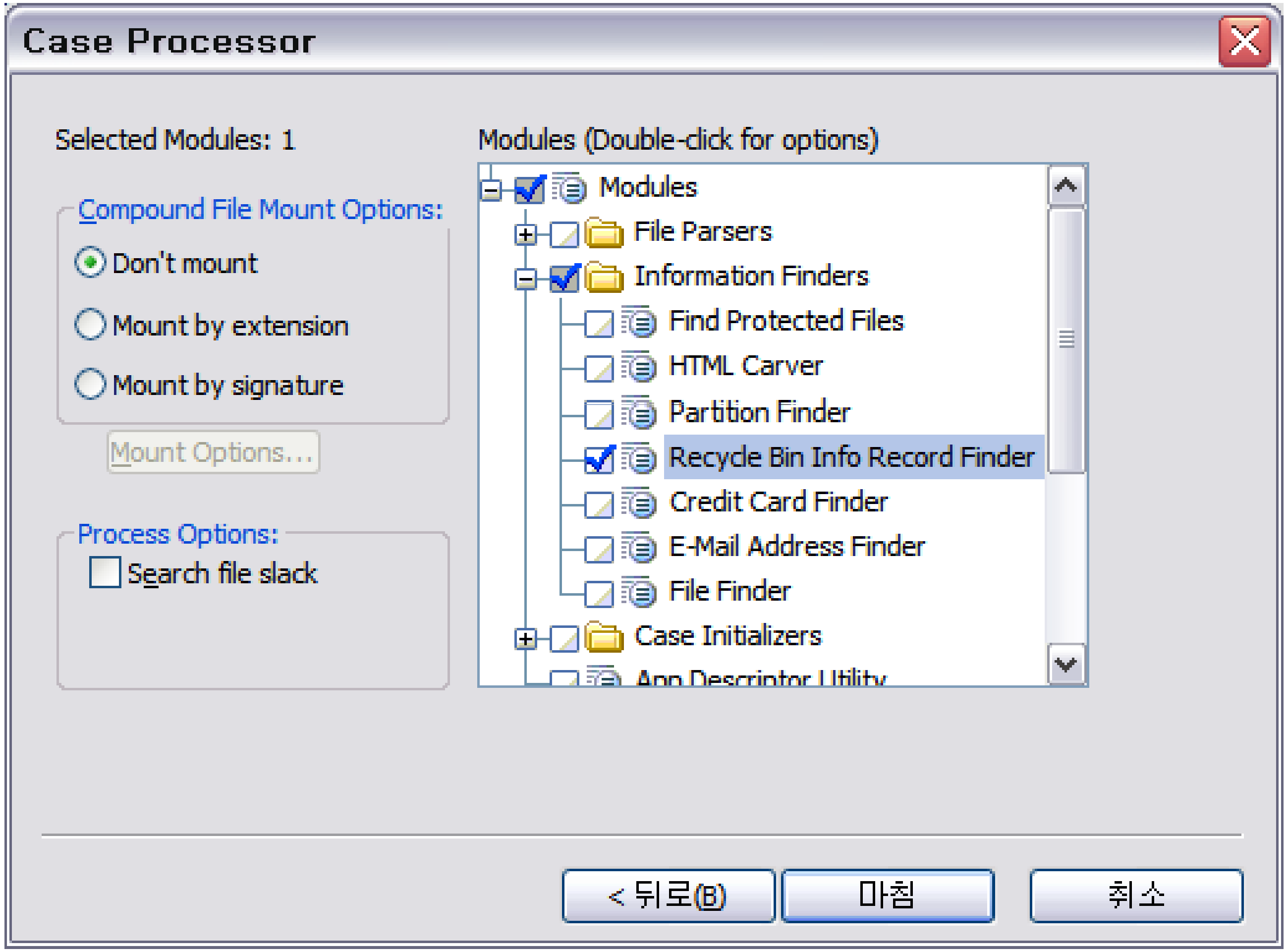
Restored File



```
074100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
076000 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
077900 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
079800 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
081700 00 00 43 3A 5C 44 4F 43 55 4D 45 7E 31 5C 70 72 6F 6E  ...C:\DOCUME~1\pron
083665 65 72 5C B9 D9 C5 C1 C8 AD 7E 31 5C 70 65 6F 70 6C 65  eer\¹ÙÅÁÈ-~1\people
08552E 78 6C 73 00 AD B8 E9 5C 70 65 6F 70 6C 65 2E 78 6C 73  .xls.-¸é\people.xls
087400 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
089300 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
091200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ...................
```

Deleted File

Recycle Bin – Using an EnScript to Determine the Status of Recycle Bin Files



Case Processor

Selected Modules: 1

Compound File Mount Options:

- ● Don't mount
- ○ Mount by extension
- ○ Mount by signature

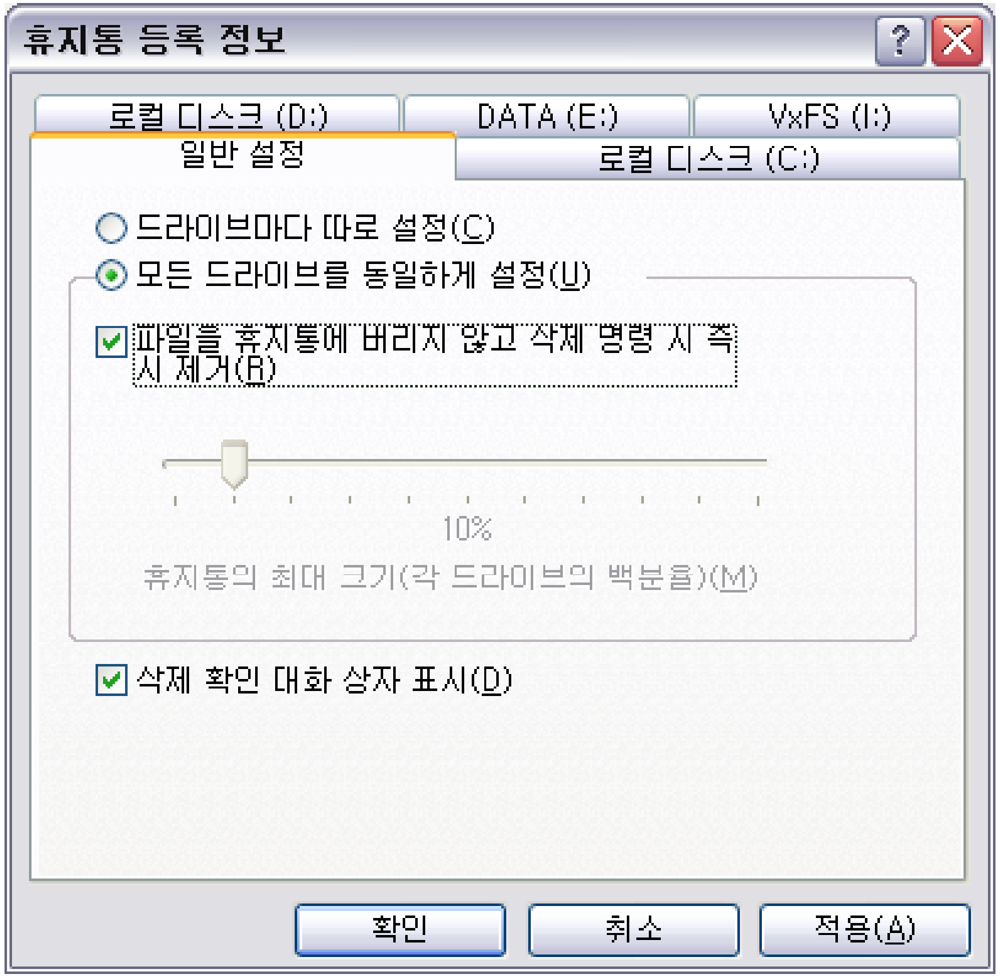
Process Options:

- □ Search file slack

Modules (Double-click for options)

- ☑ Modules
  - □ File Parsers
  - ☑ Information Finders
    - □ Find Protected Files
    - □ HTML Carver
    - □ Partition Finder
    - ☑ Recycle Bin Info Record Finder
    - □ Credit Card Finder
    - □ E-Mail Address Finder
    - □ File Finder
  - □ Case Initializers
  - □ App Descriptor Utility

Recycle Bin – Bypass



휴지통 등록 정보

○ 드라이브마다 따로 설정(C)

● 모든 드라이브를 동일하게 설정(U)

☑ 파일을 휴지통에 버리지 않고 삭제 명령 시 즉시 제거(R)

10%

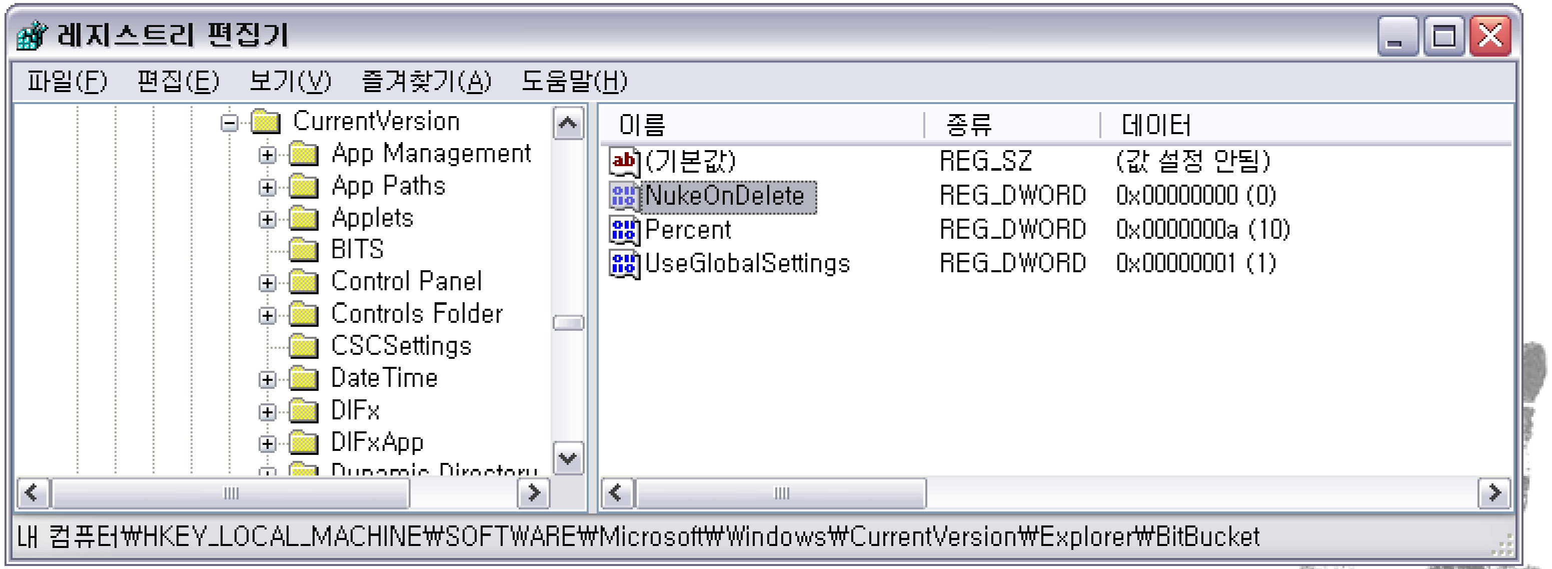
휴지통의 최대 크기(각 드라이브의 백분율)(M)

☑ 삭제 확인 대화 상자 표시(D)

Windows Operating System Artifacts

Recycle Bin – Bypass

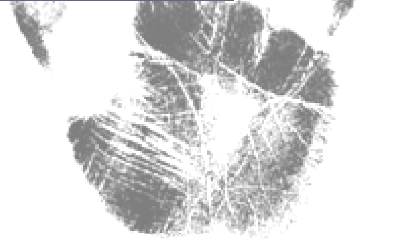
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket



이름	종류	데이터
(기본값)	REG_SZ	(값 설정 안됨)
NukeOnDelete	REG_DWORD	0x00000000 (0)
Percent	REG_DWORD	0x0000000a (10)
UseGlobalSettings	REG_DWORD	0x00000001 (1)

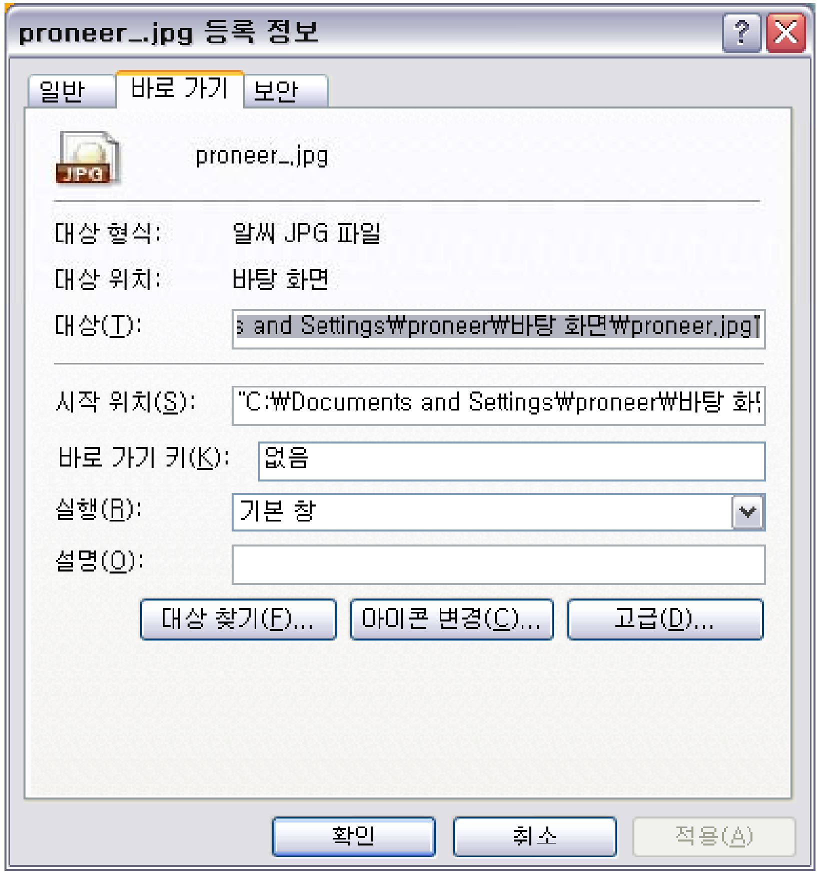
내 컴퓨터₩HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩Windows₩CurrentVersion₩Explorer₩BitBucket

- 0x01h : Set



Link Files

- *Link Files* are also known as shortcuts (.lnk)



proneer_.jpg

대상 형식: 알씨 JPG 파일

대상 위치: 바탕 화면

대상(T): s and Settings₩proneer₩바탕 화면₩proneer.jpg"

시작 위치(S): "C:₩Documents and Settings₩proneer₩바탕 화

바로 가기 키(K): 없음

실행(R): 기본 창

설명(O):

Link Files – Forensic Importance

- *Link files* are ubiquitous
- The operating system creates many *link files* by default
- The Recycle Bin is a typical default desktop *link file*
- when applications are installed, *link files* are placed in various locations
- *Link files* can be created on the desktop or on the Quick Launch taskbar
- Certain actions by the user create *link files* without their knowledge

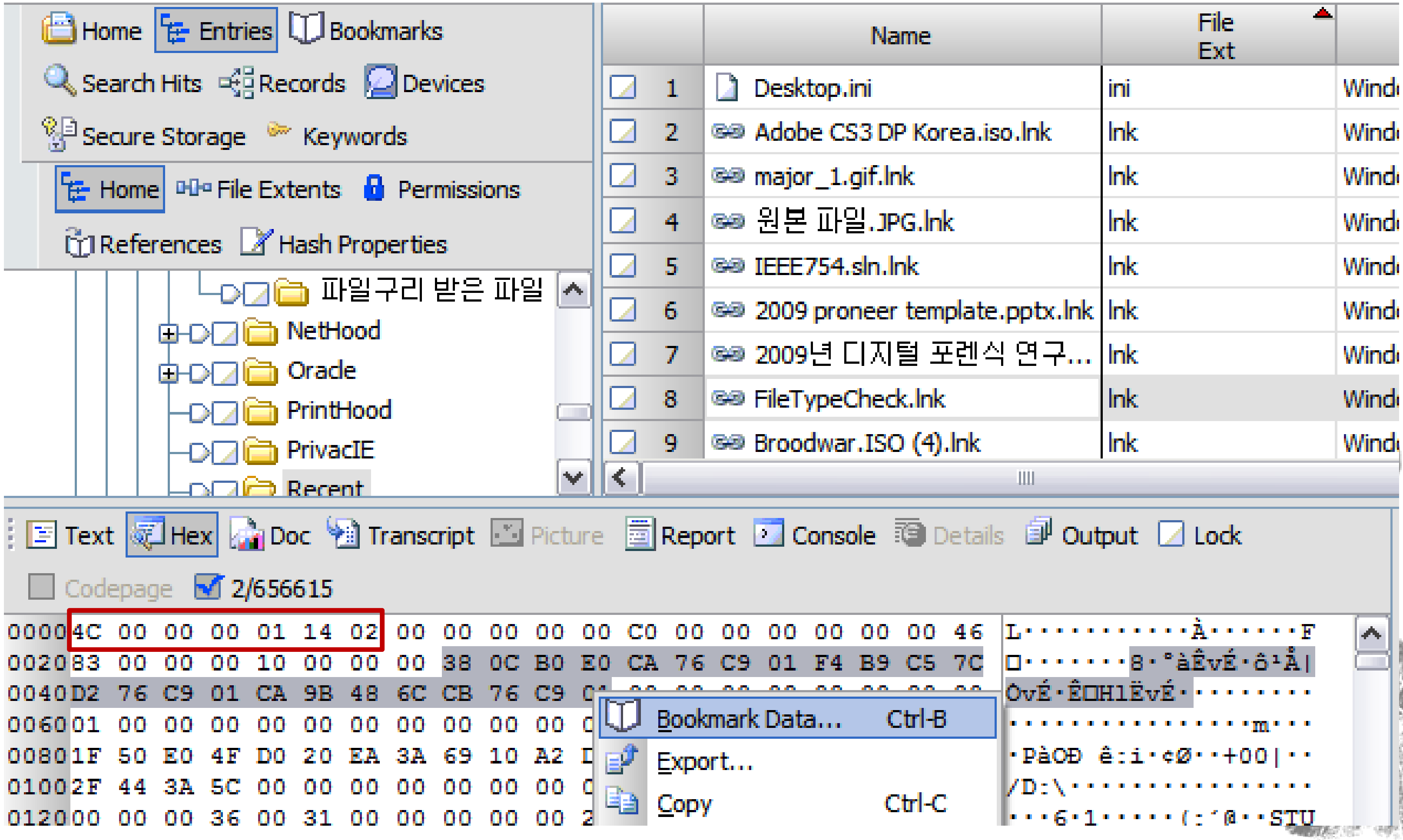
Link Files – Forensic Importance

- When a user open a document, a link file is created in the Recent folder
- Link files, like any other file, have MAC time stamps
- Program was installed on one date and a link file was created later ➔ reveal
- Each time a link file is “used”, knowingly or unknowingly,
- information about the target file is updated ➔ modified each time

Link Files – Forensic Importance

- Link file various attributes
  - The complete path
  - Volume serial number on which the target file or folder exist
  - File’s size in bytes
  - MAC time stamps of the target file

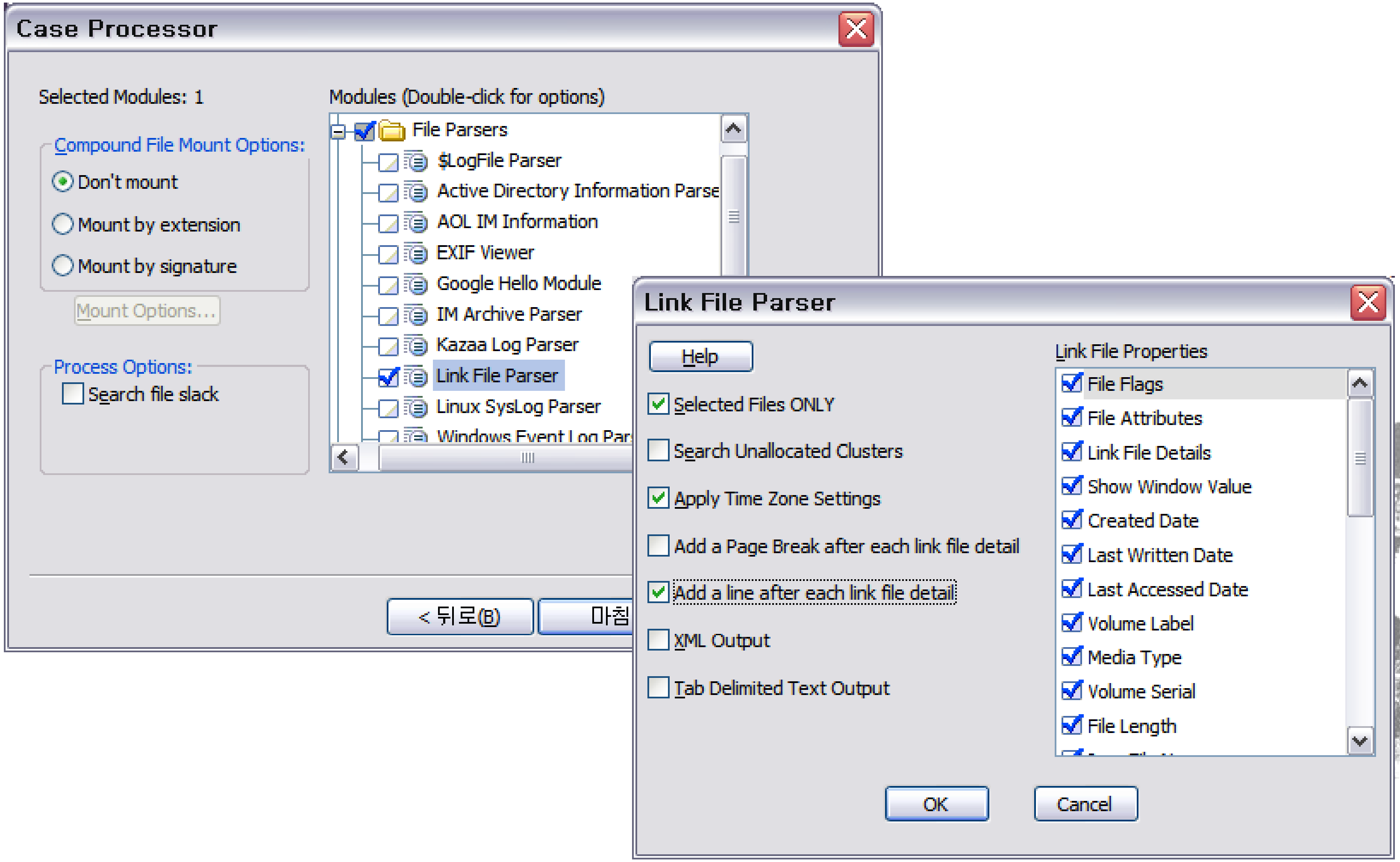
Link Files – Forensic Importance



		Name	File Ext	
□	1	Desktop.ini	ini	Wind
□	2	Adobe CS3 DP Korea.iso.lnk	lnk	Wind
□	3	major_1.gif.lnk	lnk	Wind
□	4	원본 파일.JPG.lnk	lnk	Wind
□	5	IEEE754.sln.lnk	lnk	Wind
□	6	2009 proneer template.pptx.lnk	lnk	Wind
□	7	2009년 디지털 포렌식 연구...	lnk	Wind
□	8	FileTypeCheck.lnk	lnk	Wind
□	9	Broodwar.ISO (4).lnk	lnk	Wind

```
00004C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 00 00 00 46  L···········À······F
002083 00 00 00 10 00 00 00 38 0C B0 E0 CA 76 C9 01 F4 B9 C5 7C  □·······8·°àÊvÉ·ô¹Å|
0040D2 76 C9 01 CA 9B 48 6C CB 76 C9 01                          ÒvÉ·Ê□HlËvÉ·········
006001 00 00 00 00 00 00 00 00 00 00 0                           ··················m···
00801F 50 E0 4F D0 20 EA 3A 69 10 A2 D                           ·PàOÐ ê:i·¢Ø··+00|··
01002F 44 3A 5C 00 00 00 00 00 00 00 0                           /D:\··················
012000 00 00 36 00 31 00 00 00 00 00 2                           ···6·1·····(:´@··STU
```

Link Files – Using the Link File Parser EnScript



Case Processor

Selected Modules: 1

Compound File Mount Options:

- ● Don't mount
- ○ Mount by extension
- ○ Mount by signature

Mount Options...

Process Options:

- □ Search file slack

Modules (Double-click for options)

- ☑ File Parsers
  - □ $LogFile Parser
  - □ Active Directory Information Parse
  - □ AOL IM Information
  - □ EXIF Viewer
  - □ Google Hello Module
  - □ IM Archive Parser
  - □ Kazaa Log Parser
  - ☑ Link File Parser
  - □ Linux SysLog Parser
  - □ Windows Event Log Par

< 뒤로(B) 마침

Link File Parser

Help

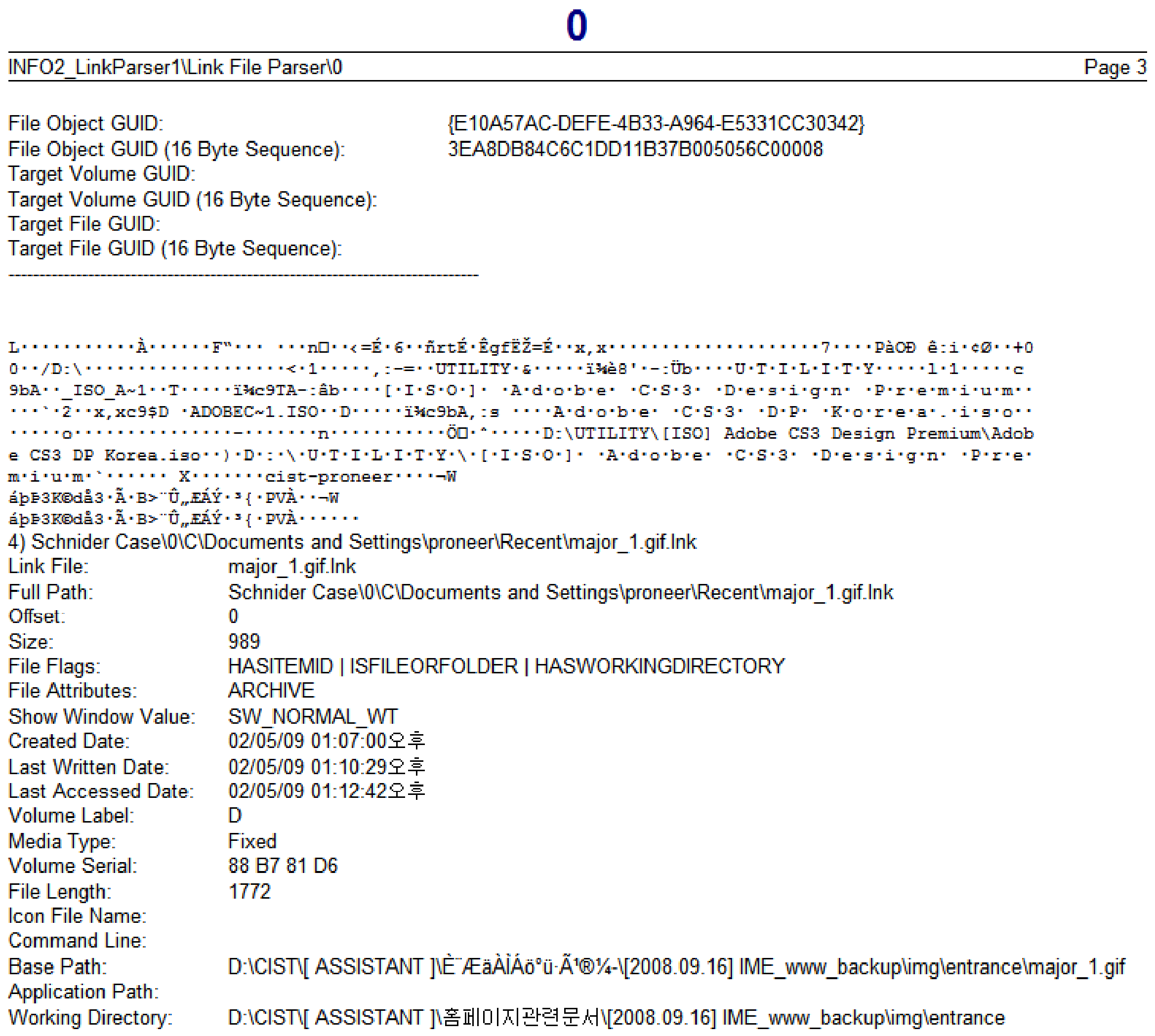
- ☑ Selected Files ONLY
- □ Search Unallocated Clusters
- ☑ Apply Time Zone Settings
- □ Add a Page Break after each link file detail
- ☑ Add a line after each link file detail
- □ XML Output
- □ Tab Delimited Text Output

Link File Properties

- ☑ File Flags
- ☑ File Attributes
- ☑ Link File Details
- ☑ Show Window Value
- ☑ Created Date
- ☑ Last Written Date
- ☑ Last Accessed Date
- ☑ Volume Label
- ☑ Media Type
- ☑ Volume Serial
- ☑ File Length

OK Cancel

Link Files – Using the Link File Parser EnScript



0

INFO2_LinkParser1\Link File Parser\0 Page 3

```
File Object GUID:                              {E10A57AC-DEFE-4B33-A964-E5331CC30342}
File Object GUID (16 Byte Sequence):           3EA8DB84C6C1DD11B37B005056C00008
Target Volume GUID:
Target Volume GUID (16 Byte Sequence):
Target File GUID:
Target File GUID (16 Byte Sequence):
------------------------------------------------------------------------------


L···········À······F"··· ···n□··<=É·6··ñrtÉ·ÊgfËŽ=É··x,x····················7····PàOÐ ê:i·¢Ø··+0
0··/D:\···················<·1·····,:-=··UTILITY·&·····ï¾è8'·-:Üb····U·T·I·L·I·T·Y·····1·1·····c
9bA··_ISO_A~1··T·····ï¾c9TA-:âb····[·I·S·O·]· ·A·d·o·b·e· ·C·S·3· ·D·e·s·i·g·n· ·P·r·e·m·i·u·m··
···`·2··x,xc9$D ·ADOBEC~1.ISO··D·····ï¾c9bA,:s ····A·d·o·b·e· ·C·S·3· ·D·P· ·K·o·r·e·a·.·i·s·o··
·····o················-········n············ÖO□·^·····D:\UTILITY\[ISO] Adobe CS3 Design Premium\Adob
e CS3 DP Korea.iso··)·D·:·\·U·T·I·L·I·T·Y·\·[·I·S·O·]· ·A·d·o·b·e· ·C·S·3· ·D·e·s·i·g·n· ·P·r·e·
m·i·u·m·`······ X·······cist-proneer····¬W
áþÞ3K©då3·Ã·B>¨Û„ÆÁÝ·³{·PVÀ··¬W
áþÞ3K©då3·Ã·B>¨Û„ÆÁÝ·³{·PVÀ······
4) Schnider Case\0\C\Documents and Settings\proneer\Recent\major_1.gif.lnk
Link File:              major_1.gif.lnk
Full Path:              Schnider Case\0\C\Documents and Settings\proneer\Recent\major_1.gif.lnk
Offset:                 0
Size:                   989
File Flags:             HASITEMID | ISFILEORFOLDER | HASWORKINGDIRECTORY
File Attributes:        ARCHIVE
Show Window Value:      SW_NORMAL_WT
Created Date:           02/05/09 01:07:00오후
Last Written Date:      02/05/09 01:10:29오후
Last Accessed Date:     02/05/09 01:12:42오후
Volume Label:           D
Media Type:             Fixed
Volume Serial:          88 B7 81 D6
File Length:            1772
Icon File Name:
Command Line:
Base Path:              D:\CIST\[ ASSISTANT ]\È¨ÆäÀÌÁö°ü·Ã¹®¼-\[2008.09.16] IME_www_backup\img\entrance\major_1.gif
Application Path:
Working Directory:      D:\CIST\[ ASSISTANT ]\홈페이지관련문서\[2008.09.16] IME_www_backup\img\entrance
```

Windows Operating System Artifacts

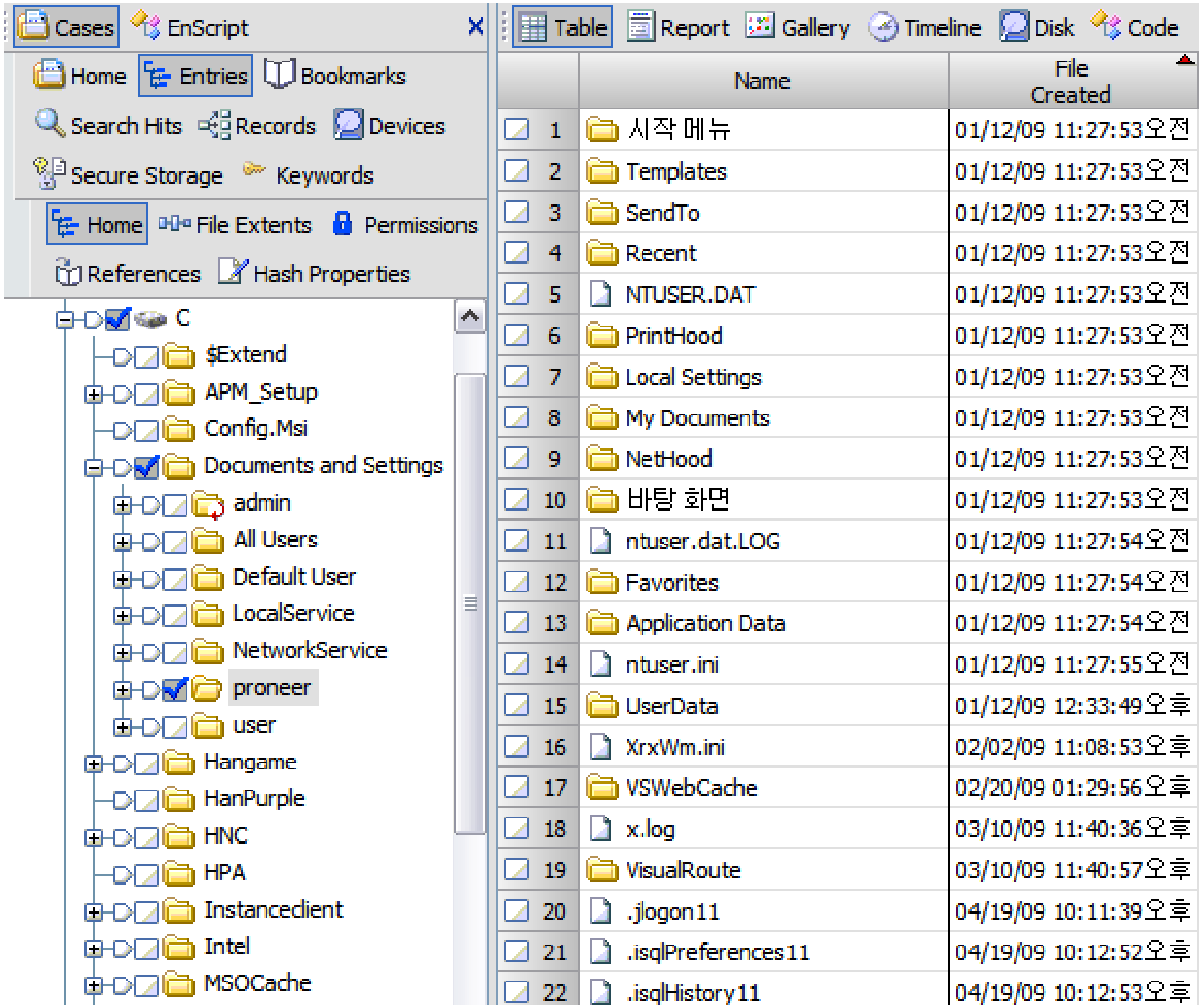
Windows 2000, XP, and Vista Folders

Operating System	User Profile Folders	Default System Folder
Windows 9x/ME	No Documents and Settings Folder	C:\Windows
Windows NT	No Documents and Settings Folder C:\WINNT\Profiles	C:\WINNT
Windows 2000	C:\Documents and Settings	C:\WINNT
Windows XP/2003	C:\Documents and Settings	C:\Windows
Windows Vista	C:\Users	C:\Windows

Windows 2000, XP, and Vista Folders

- All version (NT, 2000, XP, 2003, Vista) create a unique artifact when the user first logs on the system
- Folder is created that bears the name of the logged-on user
- At the same time, subfolders are created at first logon

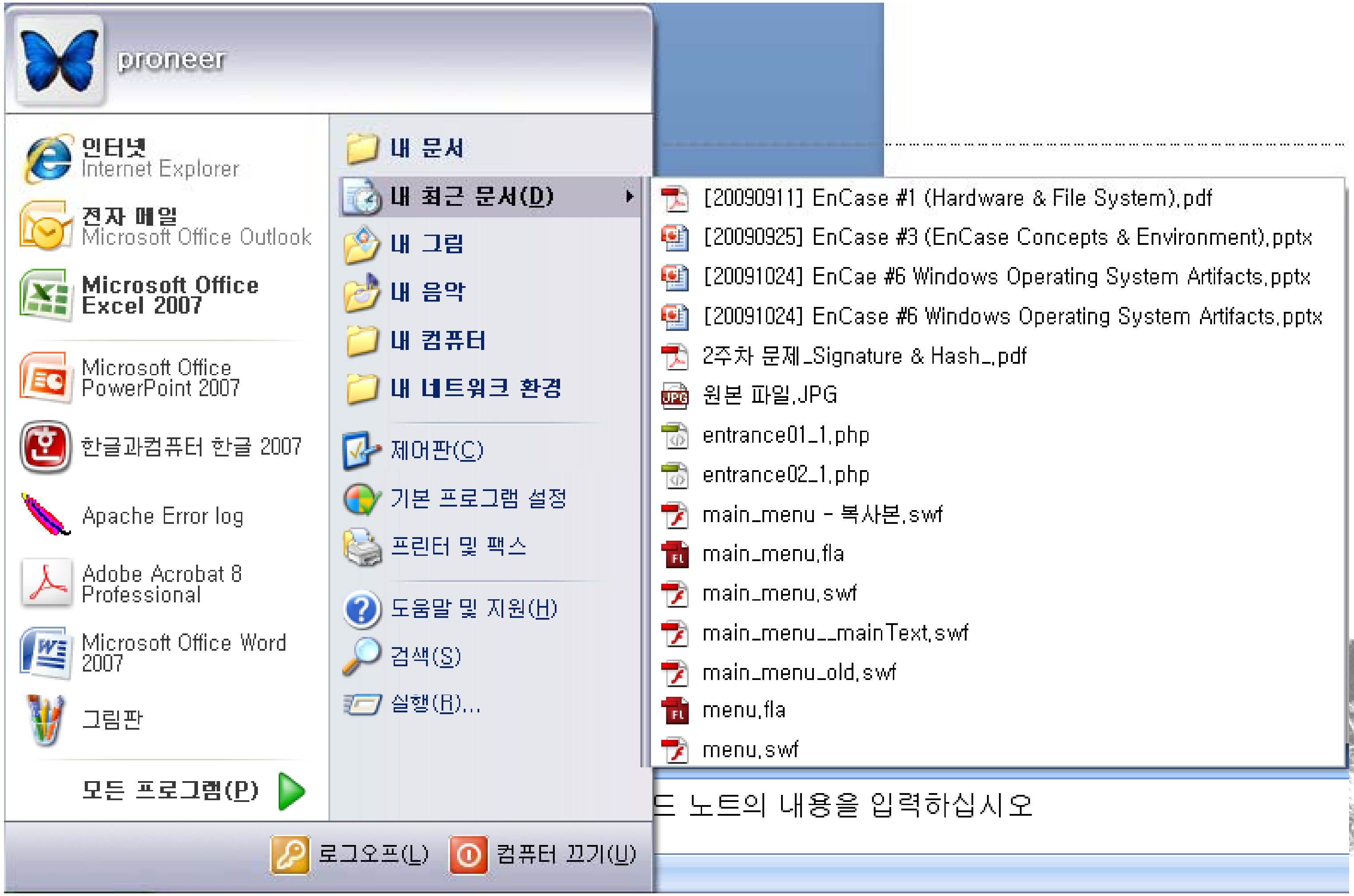
Windows 2000, XP, and Vista Folders



		Name	File Created
☐	1	시작 메뉴	01/12/09 11:27:53오전
☐	2	Templates	01/12/09 11:27:53오전
☐	3	SendTo	01/12/09 11:27:53오전
☐	4	Recent	01/12/09 11:27:53오전
☐	5	NTUSER.DAT	01/12/09 11:27:53오전
☐	6	PrintHood	01/12/09 11:27:53오전
☐	7	Local Settings	01/12/09 11:27:53오전
☐	8	My Documents	01/12/09 11:27:53오전
☐	9	NetHood	01/12/09 11:27:53오전
☐	10	바탕 화면	01/12/09 11:27:53오전
☐	11	ntuser.dat.LOG	01/12/09 11:27:54오전
☐	12	Favorites	01/12/09 11:27:54오전
☐	13	Application Data	01/12/09 11:27:54오전
☐	14	ntuser.ini	01/12/09 11:27:55오전
☐	15	UserData	01/12/09 12:33:49오후
☐	16	XrxWm.ini	02/02/09 11:08:53오후
☐	17	VSWebCache	02/20/09 01:29:56오후
☐	18	x.log	03/10/09 11:40:36오후
☐	19	VisualRoute	03/10/09 11:40:57오후
☐	20	.jlogon11	04/19/09 10:11:39오후
☐	21	.isqlPreferences11	04/19/09 10:12:52오후
☐	22	.isqlHistory11	04/19/09 10:12:53오후

Windows Operating System Artifacts

Recent Folder



[20090911] EnCase #1 (Hardware & File System).pdf
[20090925] EnCase #3 (EnCase Concepts & Environment).pptx
[20091024] EnCae #6 Windows Operating System Artifacts.pptx
[20091024] EnCase #6 Windows Operating System Artifacts.pptx
2주차 문제_Signature & Hash_.pdf
원본 파일.JPG
entrance01_1.php
entrance02_1.php
main_menu - 복사본.swf
main_menu.fla
main_menu.swf
main_menu__mainText.swf
main_menu_old.swf
menu.fla
menu.swf

드 노트의 내용을 입력하십시오

Windows Operating System Artifacts

Recent Folder

- Windows XP : *C:\Documents and Settings\<user name>\Recent*
- Windows Vista : *C:\Users\<user name>\AppData\ Roaming*

  \ Microsoft\ Windows\Recent

- Examine in a case in the Recent Folder :
  - sort the files chronologically by last written time
  - to see what kind of files the user has been accessing
  - quickly point the way to the user’s favored or hidden storage locations
  - saving you lots of time and quickly focusing your resources in the right direction

Question & Answer