

# Windows Operating System Artifacts

*Security is a people problem...*



# Outline

- Dates and Times
- Recycle Bin
- Link Files
- Windows 2000, XP, and Vista Folders
- Recent Folder
- Desktop Folder
- My Documents/Documents
- Temp Folder
- Favorites Folder
- Windows Vista Low Folders
- Cookies Folder
- History Folder
- Temporary Internet Files
- Swap/Hibernation File
- Print Spooling
- Legacy Operating System Artifacts
- Windows Vista Volume Shadow Copy
- Windows Event Logs



# Windows Operating System Artifacts

## Operating System Artifacts

- 윈도우 운영체제는 친숙한 인터페이스를 가짐
- 겉으로는 단순한 작업이지만 시스템 내부적으로는 눈에 보이지 않는 많은 변화가 발생
- 결과적으로 사용자의 행위에 따라 운영체제에 데이터가 변경
- Artifacts는 이러한 변화되는 운영체제 내부의 데이터들을 지칭
- 로그, 파일, 비밀번호, 캐쉬, 히스토리, 최근 사용 문서 등



# Windows Operating System Artifacts

## Date and Times

- 윈도우 운영체제 버전 별로 시간을 저장하는 포맷이 다름
- 보통 로컬 시간과 그리니치 평균시(Greenwich mean time;GMT)를 이용하여 시간 표현
- 윈도우는 파일시스템의 파일 속성으로 시간정보를 기록
- 파일시스템에서 사용되는 시간은 로컬 시간 또는 그리니치 평균시를 사용



# Windows Operating System Artifacts

## Date and Times – Time Zone

- 각 국가별로 GMT를 기준으로 한 Time Zone을 가짐
- 시스템의 Time Zone은 간단한 설정으로 손쉽게 변경 가능



# Windows Operating System Artifacts

## Date and Times – Time Zone

- FAT 파일시스템
  - 디렉터리 엔트리의 32 비트 로컬 시간만 저장
- NTFS
  - 파일 속성에 GMT를 기준으로 한 64-bit Windows Time Stamp 로 저장
  - GMT를 기준으로 한 값이므로 운영체제의 Time Zone 변경 시, 자동으로 값 재설정
- Time Zone에 따라 파일시스템 파일의 시간 정보가 변하므로 수사 시 BIOS 시간과 Time Zone을 우선적으로 파악
- EnCase 4.0 이상부터는 증거 파일에 대한 Time Zone 설정 가능



# Windows Operating System Artifacts

## Date and Times – Unix Time Stamp

- Unix라고 명칭되어 있지만 유닉스 이외의 시스템에서도 공통으로 사용(윈도우 로컬 시간)
- 32 비트 정수형 값을 사용하여 초 단위로 표현
- 기준시 : 1970년 1월 1일, 00:00:00 GMT
- $2^{32}$  : 4,294,967,296
- 2030년 12월 2일 월요일, 19:42:58 GMT를 기준으로 만료
- 새로운 시간 표현 방식이 필요



# Windows Operating System Artifacts

## Date and Times – Windows 64-Bit Time Stamp

- 64 비트 정수형 값을 사용하여 100 나노초 단위의 시간정보 표현
- 기준시 : 1601년 1월 1일, 00:00:00 GMT
- $2^{64}$  : 18,446,744,073,709,500,000
- 대략, 58,000년 이상의 시간정보 표현 가능

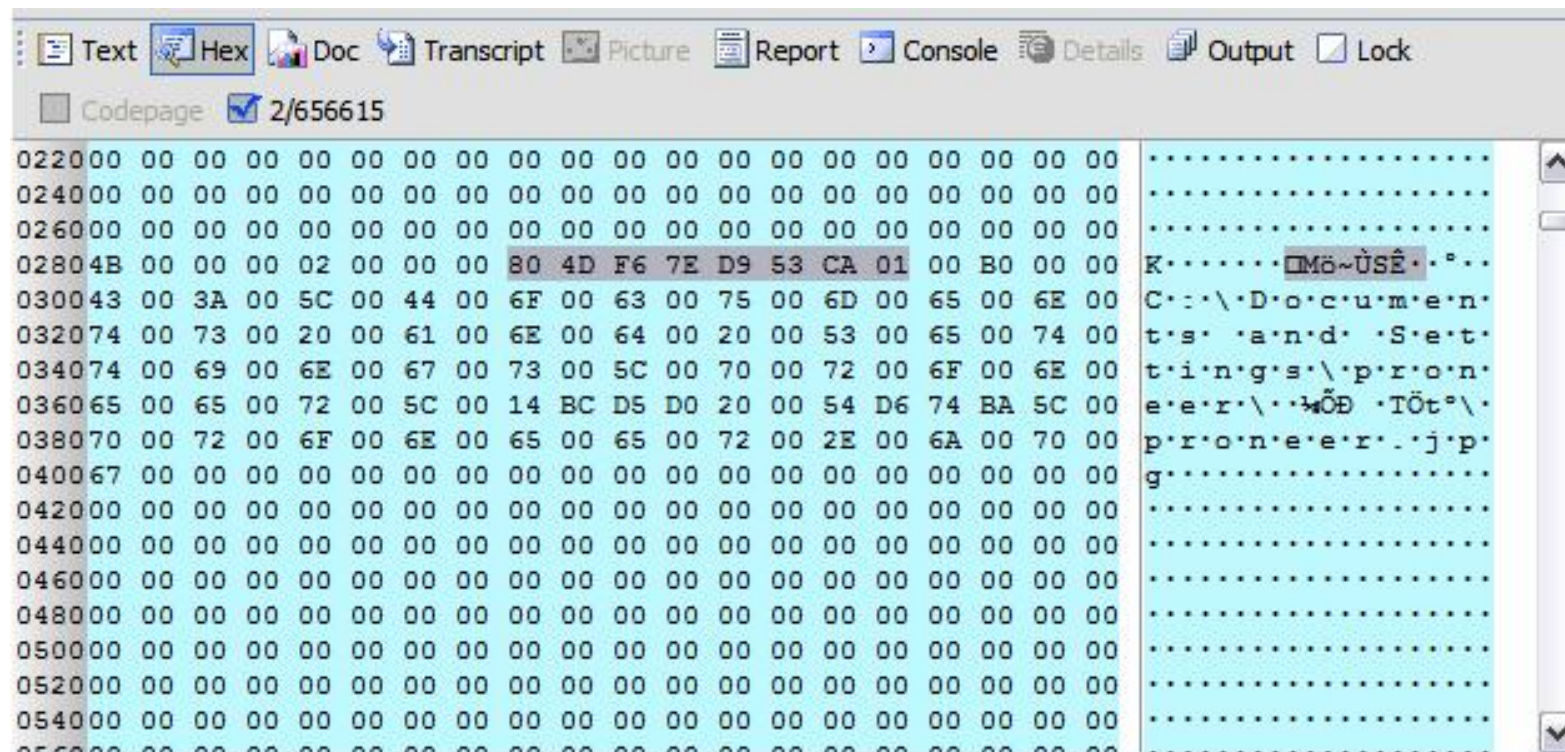




# Windows Operating System Artifacts

## Date and Times – Windows 64-Bit Time Stamp

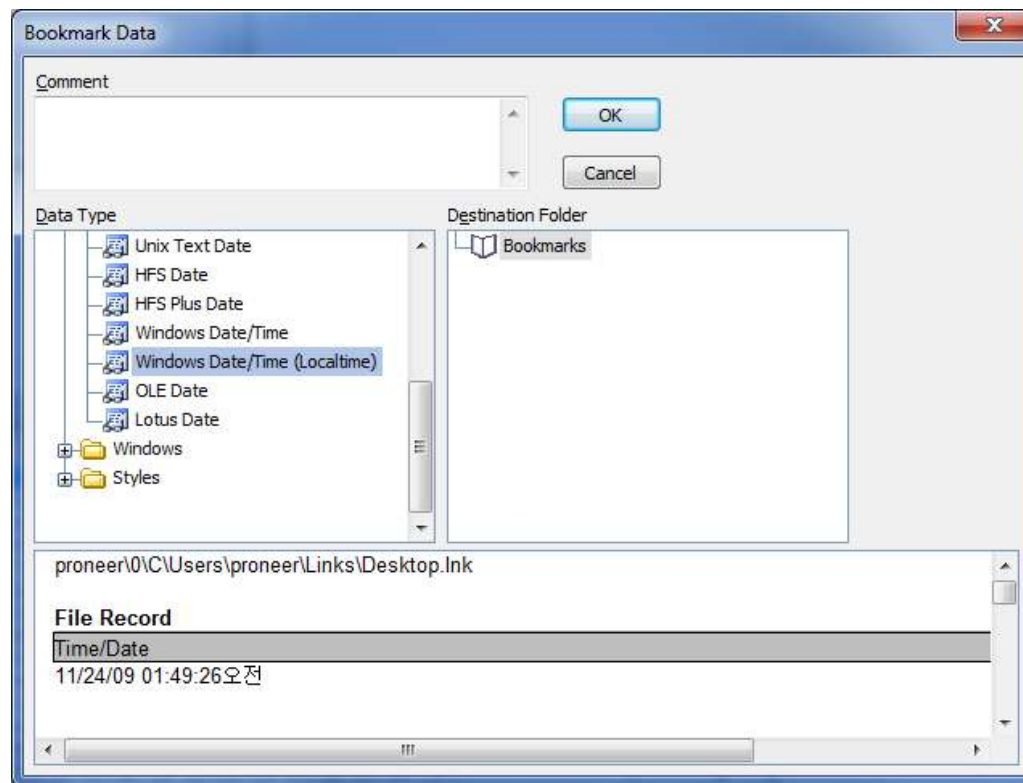
- 64 비트의 값으로 최상위 값은 항상 01h



# Windows Operating System Artifacts

## Date and Times – Windows 64-Bit Time Stamp

- 북마크 데이터에 2개의 시간 정보
- Windows Date/Time(GMT 기준) vs Windows Date/Time (Localtime)



# Windows Operating System Artifacts

## Date and Times – Adjusting for Time Zone Offsets

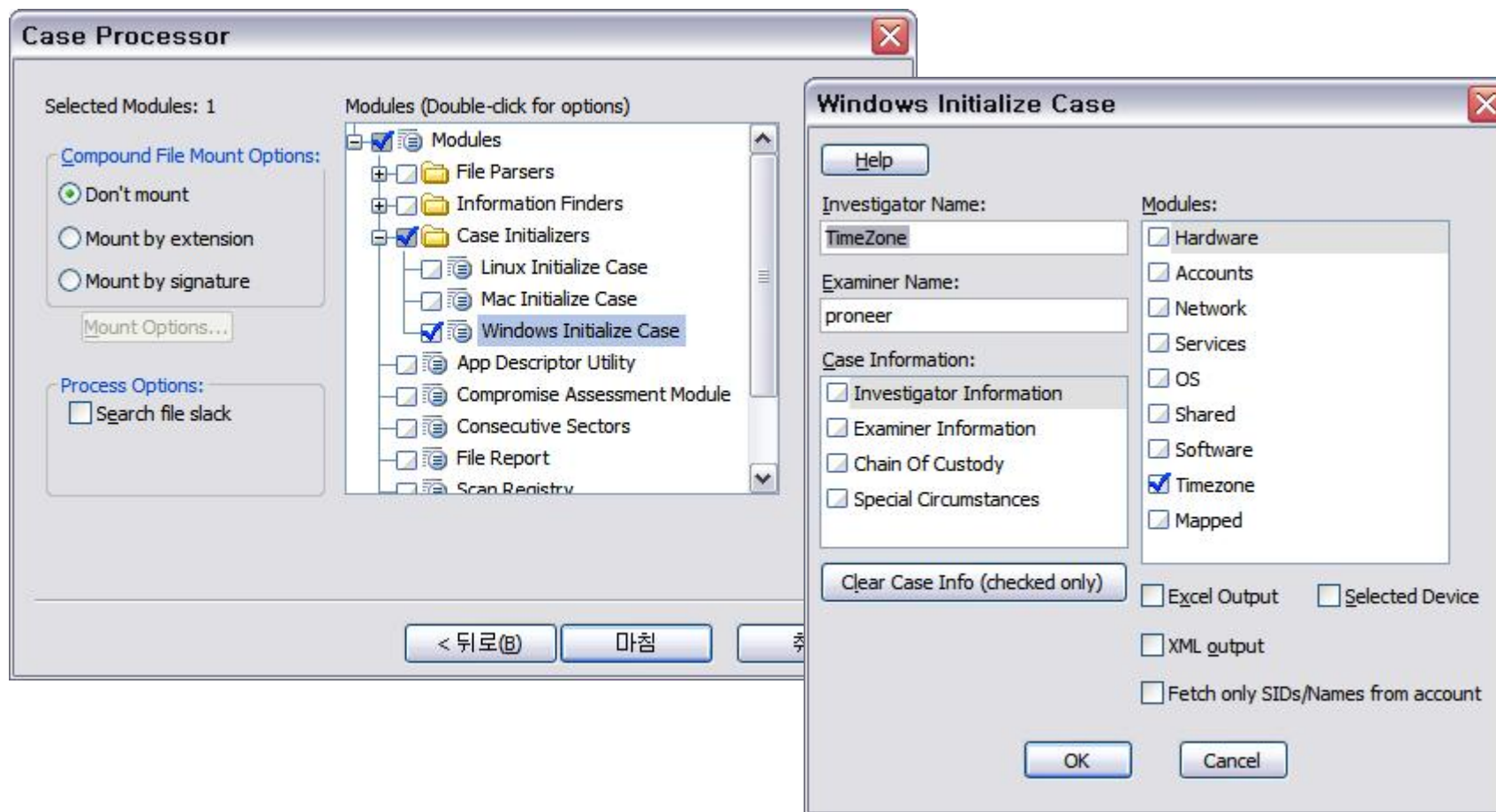
- Time Zone offset은 레지스트리에 저장됨
- *System\NTRegistry\ControlSet00n\Control\TimeZoneInformation*

| Table Report Gallery Timeline Disk Code |                |              |               |                      |              |            |
|---|----------------|--------------|---------------|----------------------|--------------|------------|
|   | Name           | Logical Size | Physical Size | Starting Extent      | File Extents | References |
| <input type="checkbox"/> 1              | StandardStart  | 16           | 16            | 0NTRegistry-B451260  | 1            | 0          |
| <input type="checkbox"/> 2              | StandardName   | 18           | 18            | 0NTRegistry-B451196  | 1            | 0          |
| <input type="checkbox"/> 3              | StandardBias   | 4            | 4             | 0NTRegistry-B451228  | 1            | 0          |
| <input type="checkbox"/> 4              | DaylightStart  | 16           | 16            | 0NTRegistry-B451716  | 1            | 0          |
| <input type="checkbox"/> 5              | DaylightName   | 18           | 18            | 0NTRegistry-B6330692 | 1            | 0          |
| <input type="checkbox"/> 6              | DaylightBias   | 4            | 4             | 0NTRegistry-B451812  | 1            | 0          |
| <input type="checkbox"/> 7              | Bias           | 4            | 4             | 0NTRegistry-B451132  | 1            | 0          |
| <input type="checkbox"/> 8              | ActiveTimeBias | 4            | 4             | 0NTRegistry-B451924  | 1            | 0          |

# Windows Operating System Artifacts

## Date and Times – Adjusting for Time Zone Offsets

- Case Processor를 이용하여 Time Zone 정보 획득

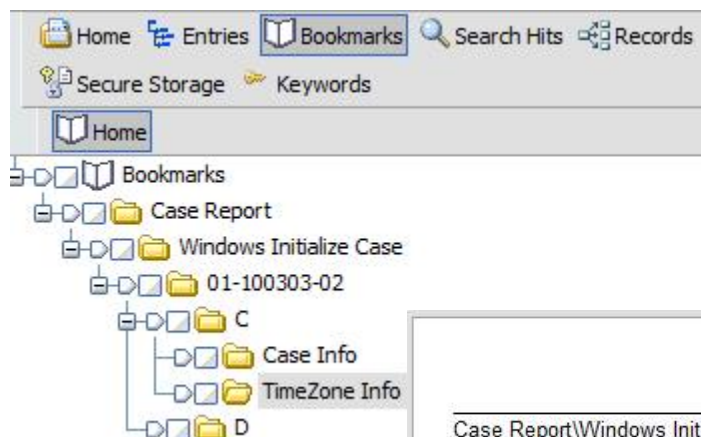




# Windows Operating System Artifacts

## Date and Times – Adjusting for Time Zone Offsets

- Case Processor를 이용하여 획득한 정보 북마크 탭을 통해 확인



### TimeZone Info

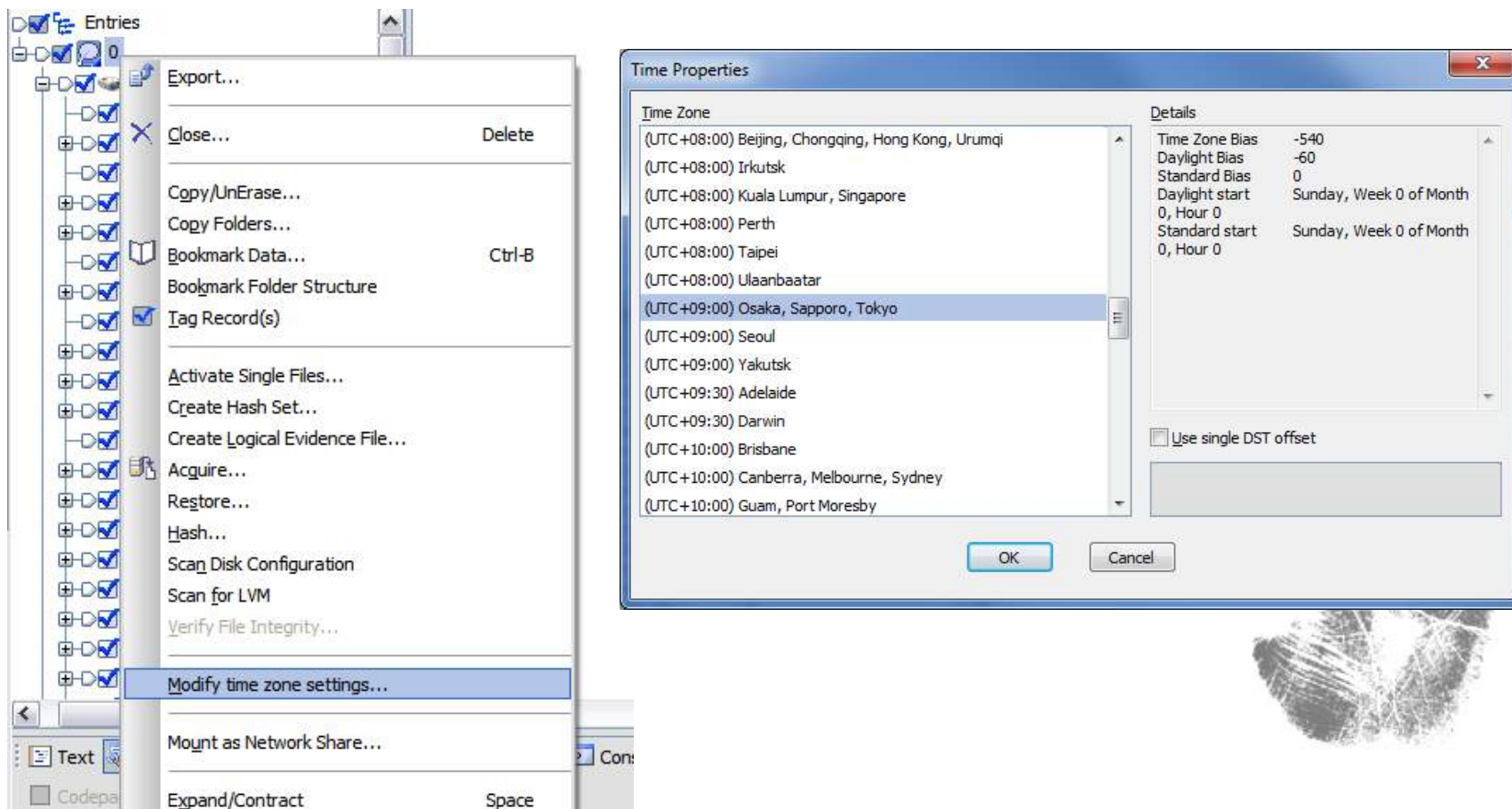
Case Report\Windows Initialize Case\01-100303-02\C\TimeZone Info Page 1

```
Current control set is 001
Default control set is 001
Failed control set is 000
LastKnownGood control set is 002
Standard time bias is 09:00 hours offset from GMT.
StandardName: 대한민국 표준시
Standard time is set to change the Standard bias by 0 minutes.
Standard time is set to change on Sunday of the 0th week of Unknown, at 00:00 hours.
DaylightName: 대한민국 표준시
Daylight savings is set to change the Standard bias by 0 minutes.
Daylight savings time is set to change on Sunday of the 0th week of Unknown, at 00:00 hours.
Active time bias is 09:00 hours offset from GMT.
The current time setting is 9:00 hours offset from GMT.
The offset must be either added or subtracted from GMT depending on the time zone location
```

# Windows Operating System Artifacts

## Date and Times – Adjusting for Time Zone Offsets

- 획득 또는 확인한 Time Zone 정보를 기반으로 Time Zone 설정



# Windows Operating System Artifacts

## Recycle Bin













- 윈도우 상에서 기본적인 파일 삭제 시 휴지통으로 이동
- SHIFT 키를 조합하거나 휴지통 설정을 통해 휴지통 저장을 우회하여 바로 삭제 가능
- 파일 삭제 후 휴지통으로 이동할 시 변화
  - 기존 파일의 디렉터리 엔트리, MFT 엔트리가 삭제됨
  - 휴지통에 위치하는 새로운 디렉터리 엔트리, MFT 엔트리가 생성



# Windows Operating System Artifacts

## Recycle Bin – deleted file

- 삭제된 파일의 경우 다음과 같은 아이콘으로 표현

|                                | Name  | Is Deleted | Last Accessed       | File Created        | Last Written        |
|--------------------------------|---|------------|---------------------|---------------------|---------------------|
| <input type="checkbox"/> 27136 |  ico_bullet[1].gif         | •          | 03/02/10 11:03:47오후 | 03/02/10 11:03:47오후 | 03/02/10 11:03:47오후 |
| <input type="checkbox"/> 27137 |  ico_bar02[1].gif          | •          | 03/02/10 10:56:30오후 | 03/02/10 10:56:30오후 | 03/02/10 10:56:30오후 |
| <input type="checkbox"/> 27138 |  ico_bar01[1].gif          | •          | 03/02/10 11:03:47오후 | 03/02/10 11:03:47오후 | 03/02/10 11:03:47오후 |
| <input type="checkbox"/> 27139 |  ico_arrow[2].gif          | •          | 03/02/10 10:57:23오후 | 03/02/10 10:57:23오후 | 03/02/10 10:57:23오후 |
| <input type="checkbox"/> 27140 |  ico_arrow-orange02[1].gif | •          | 03/02/10 10:56:31오후 | 03/02/10 10:56:31오후 | 03/02/10 10:56:31오후 |
| <input type="checkbox"/> 27141 |  def_pic_f[1].jpg          | •          | 03/02/10 10:57:15오후 | 03/02/10 10:57:15오후 | 03/02/10 10:57:15오후 |
| <input type="checkbox"/> 27142 |  hair_f_2952_3[1].gif      | •          | 03/02/10 10:56:43오후 | 03/02/10 10:56:43오후 | 03/02/10 10:56:43오후 |
| <input type="checkbox"/> 27143 |  hair_f_2861_3[1].gif      | •          | 03/02/10 10:56:43오후 | 03/02/10 10:56:43오후 | 03/02/10 10:56:43오후 |
| <input type="checkbox"/> 27144 |  hair_f_2456_3[1].gif      | •          | 03/02/10 10:56:43오후 | 03/02/10 10:56:43오후 | 03/02/10 10:56:43오후 |
| <input type="checkbox"/> 27145 |  hair_f_2076_3[1].gif      | •          | 03/02/10 10:56:43오후 | 03/02/10 10:56:43오후 | 03/02/10 10:56:43오후 |
| <input type="checkbox"/> 27146 |  default_keyword[1].htm   | •          | 03/02/10 11:03:43오후 | 03/02/10 11:03:43오후 | 03/02/10 11:03:43오후 |
| <input type="checkbox"/> 27147 |  folder_managerok[1].htm | •          | 03/02/10 11:03:23오후 | 03/02/10 11:03:23오후 | 03/02/10 11:03:23오후 |


















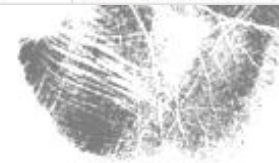


# Windows Operating System Artifacts

## Recycle Bin – overwritten file

- 덮어쓰진 파일의 경우 다음과 같은 아이콘으로 표현

|                                | Name  | Is Deleted ▲ | Is Overwritten ▲ | Last Accessed       | File Created        | Last Written        |
|--------------------------------|---|--------------|------------------|---------------------|---------------------|---------------------|
| <input type="checkbox"/> 27233 |  imgbrd_folder_new[1].htm        | •            | •                | 03/02/10 11:03:27오후 | 03/02/10 11:03:26오후 | 03/02/10 11:03:27오후 |
| <input type="checkbox"/> 27234 |  imgbrd_list[1].htm              | •            | •                | 03/02/10 10:59:41오후 | 03/02/10 10:59:40오후 | 03/02/10 10:59:41오후 |
| <input type="checkbox"/> 27235 |  imgbrd_list[2].htm              | •            | •                | 03/02/10 11:03:29오후 | 03/02/10 11:03:28오후 | 03/02/10 11:03:29오후 |
| <input type="checkbox"/> 27236 |  imgbrd_list[3].htm              | •            | •                | 03/02/10 11:02:23오후 | 03/02/10 11:02:22오후 | 03/02/10 11:02:23오후 |
| <input type="checkbox"/> 27237 |  indexview[1].js                 | •            | •                | 03/02/10 10:57:17오후 | 03/02/10 10:56:34오후 | 03/02/10 10:56:34오후 |
| <input type="checkbox"/> 27238 |  ioh0423_mh[1].htm               | •            | •                | 03/02/10 10:57:16오후 | 03/02/10 10:56:29오후 | 03/02/10 10:56:30오후 |
| <input type="checkbox"/> 27239 |  jquery.event.drag-1.5.min[1].js | •            | •                | 03/02/10 10:57:16오후 | 03/02/10 10:56:34오후 | 03/02/10 10:56:34오후 |
| <input type="checkbox"/> 27240 |  jquery.flash[1].js              | •            | •                | 03/02/10 10:57:16오후 | 03/02/10 10:56:33오후 | 03/02/10 10:56:33오후 |
| <input type="checkbox"/> 27241 |  K-6[1].jpg                      | •            | •                | 03/02/10 11:03:29오후 | 03/02/10 11:03:29오후 | 03/02/10 11:03:29오후 |
| <input type="checkbox"/> 27242 |  link[2].htm                     | •            | •                | 03/02/10 11:03:41오후 | 03/02/10 11:03:41오후 | 03/02/10 11:03:41오후 |
| <input type="checkbox"/> 27243 |  loading[1].gif                 | •            | •                | 03/02/10 10:56:33오후 | 03/02/10 10:56:33오후 | 03/02/10 10:56:33오후 |
| <input type="checkbox"/> 27244 |  main_inside[1].htm            | •            | •                | 03/02/10 10:56:39오후 | 03/02/10 10:56:37오후 | 03/02/10 10:56:39오후 |
| <input type="checkbox"/> 27245 |  main_inside[2].htm            | •            | •                | 03/02/10 10:57:26오후 | 03/02/10 10:57:26오후 | 03/02/10 10:57:26오후 |
| <input type="checkbox"/> 27246 |  main_inside[3].htm            | •            | •                | 03/02/10 11:03:46오후 | 03/02/10 11:03:45오후 | 03/02/10 11:03:46오후 |
| <input type="checkbox"/> 27247 |  btn_reno2-set01[1].gif        | •            | •                | 03/02/10 10:57:26오후 | 03/02/10 10:57:26오후 | 03/02/10 10:57:26오후 |



# Windows Operating System Artifacts

## Recycle Bin

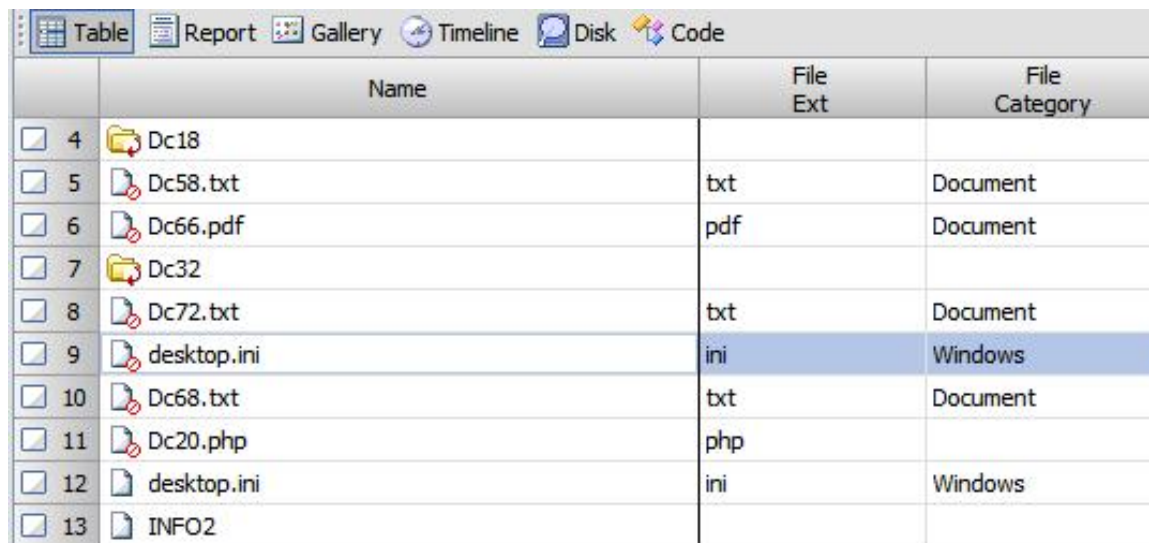
- 휴지통에 생성되는 파일 이름은 별도의 규칙을 가지고 만들어짐
- 휴지통 파일 이름 생성 규칙 :
  - *D [original drive letter of file] [index number] . [original file extension]*
- 예를 들어, C:\My Files\letter.doc 파일이 삭제되어 휴지통으로 이동될 경우
- 휴지통에 생성되는 파일 이름은 DC1.doc (기존에 휴지통으로 이동한 파일이 없을 경우)
- [index number]는 XP 이전의 경우 0부터 시작, XP 이후부터는 1부터 시작



# Windows Operating System Artifacts

## Recycle Bin – The INFO2 File

- 삭제된 파일은 파일 이름을 통해서 더 이상 원본 파일 이름, 위치를 알 수 없음
- 간단한 데이터베이스인 INFO2 파일을 통해 원본 파일과 위치를 표현
- INFO2 파일에 저장되는 정보
  - 파일의 원본 이름 및 경로 (ASCII, Unicode 모두 저장)
  - 삭제된 날짜 및 시간
  - 인덱스 번호



|    | 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           |

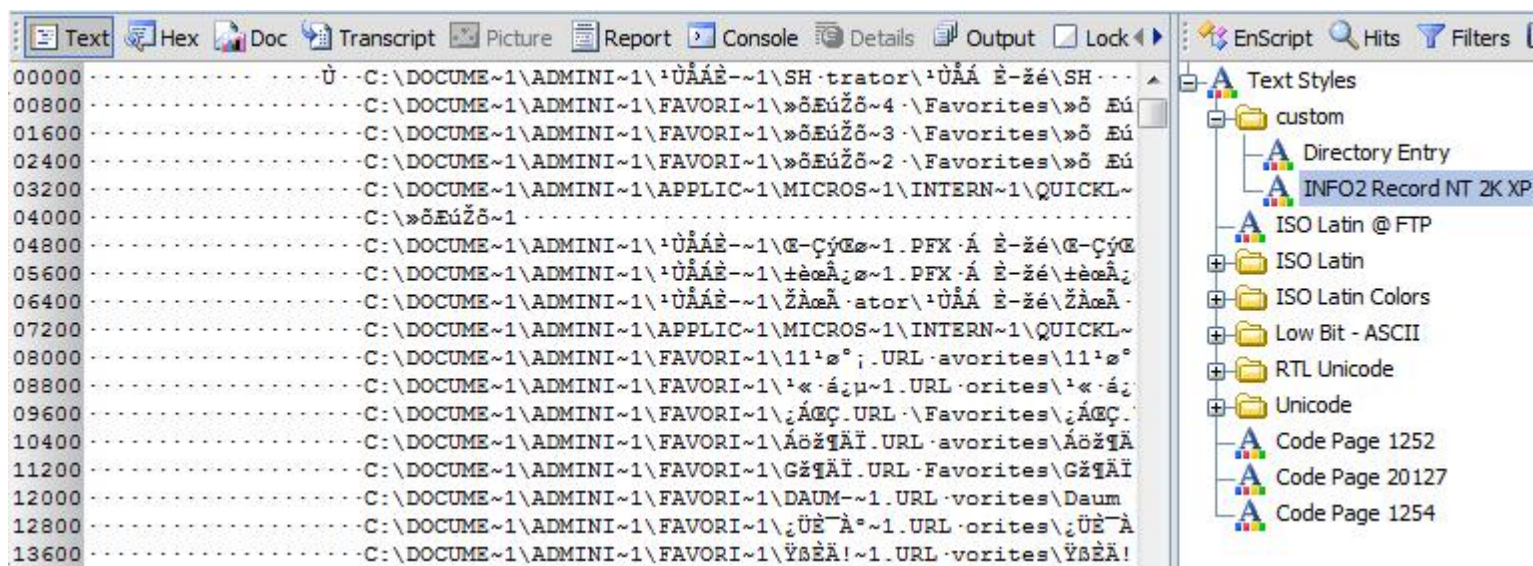
- 윈도우 버전에 따라 INFO2 레코드의 길이가 차이가 있음
- 각 레코드는 삭제된 하나의 파일에 대한 정보를 저장



# Windows Operating System Artifacts

## Recycle Bin – The INFO2 File

- 윈도우 XP 에서 INFO2 파일 레코드는 800 바이트이므로 Text Styles을 편집하여 레코드를 정렬

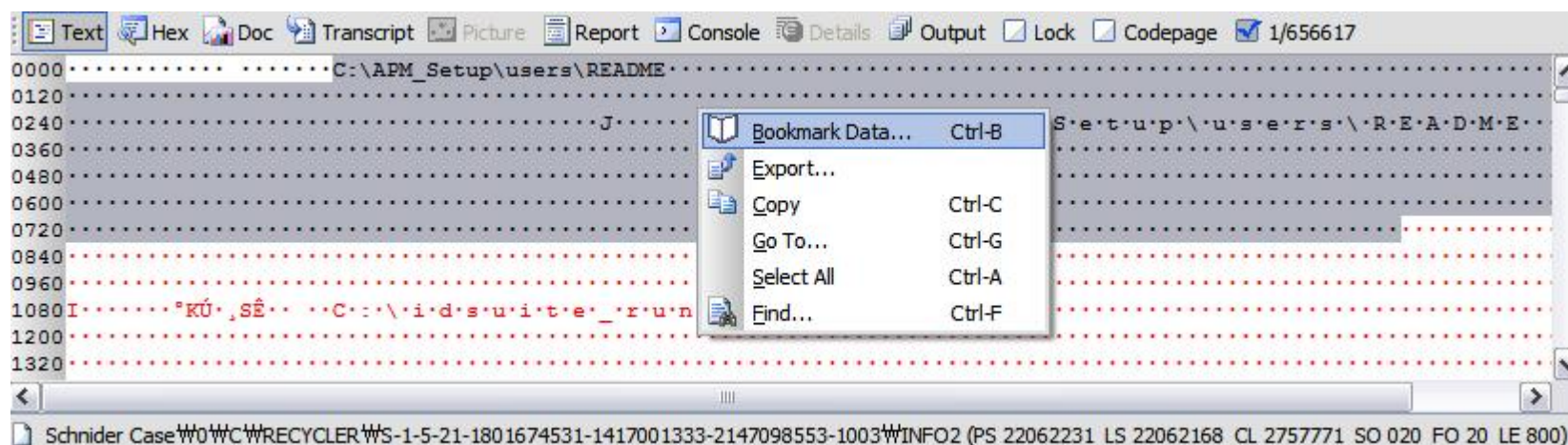




# Windows Operating System Artifacts

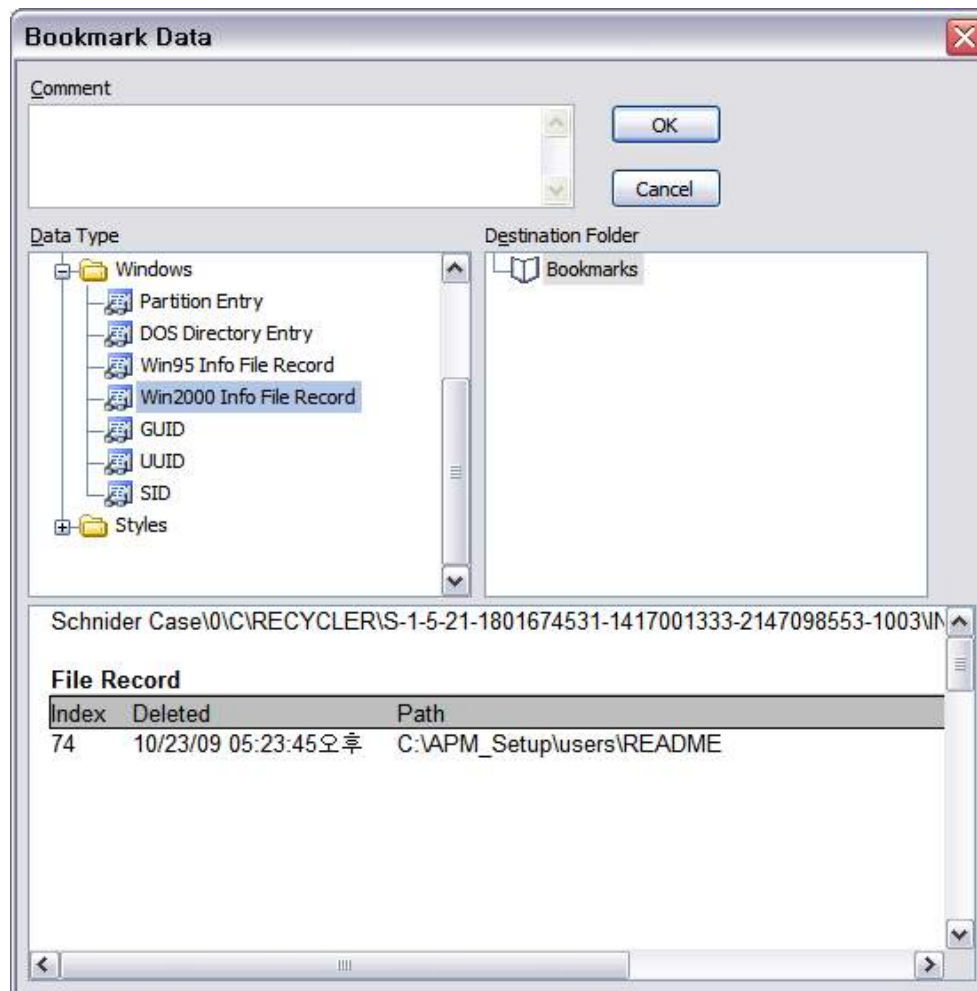
## Recycle Bin – The INFO2 File

- 북마크 데이터를 이용해 INFO2 레코드 해석 가능



# Windows Operating System Artifacts

## Recycle Bin – The INFO2 File



# Windows Operating System Artifacts

## Recycle Bin – Determining the Owner of Files

- 윈도우 NT/2K/XP/2003에서 파일 삭제시 휴지통에 각 사용자의 폴더가 생성
- 사용자 폴더명은 시스템에서 할당 받은 사용자의 SID(Security ID)가 사용됨
- 사용자의 SID는 시스템에서 GUID(Globally Unique Identification Number) 역할
- SID에 대한 사용자 정보는 SAM 레지스트리에 저장
- 증거 파일 로드 시 자동적으로 SAM 레지스트리를 파싱한 후 SID와 관련 정보를 저장
- Details 탭을 통해 SID에 해당하는 사용자 정보를 손쉽게 확인 가능

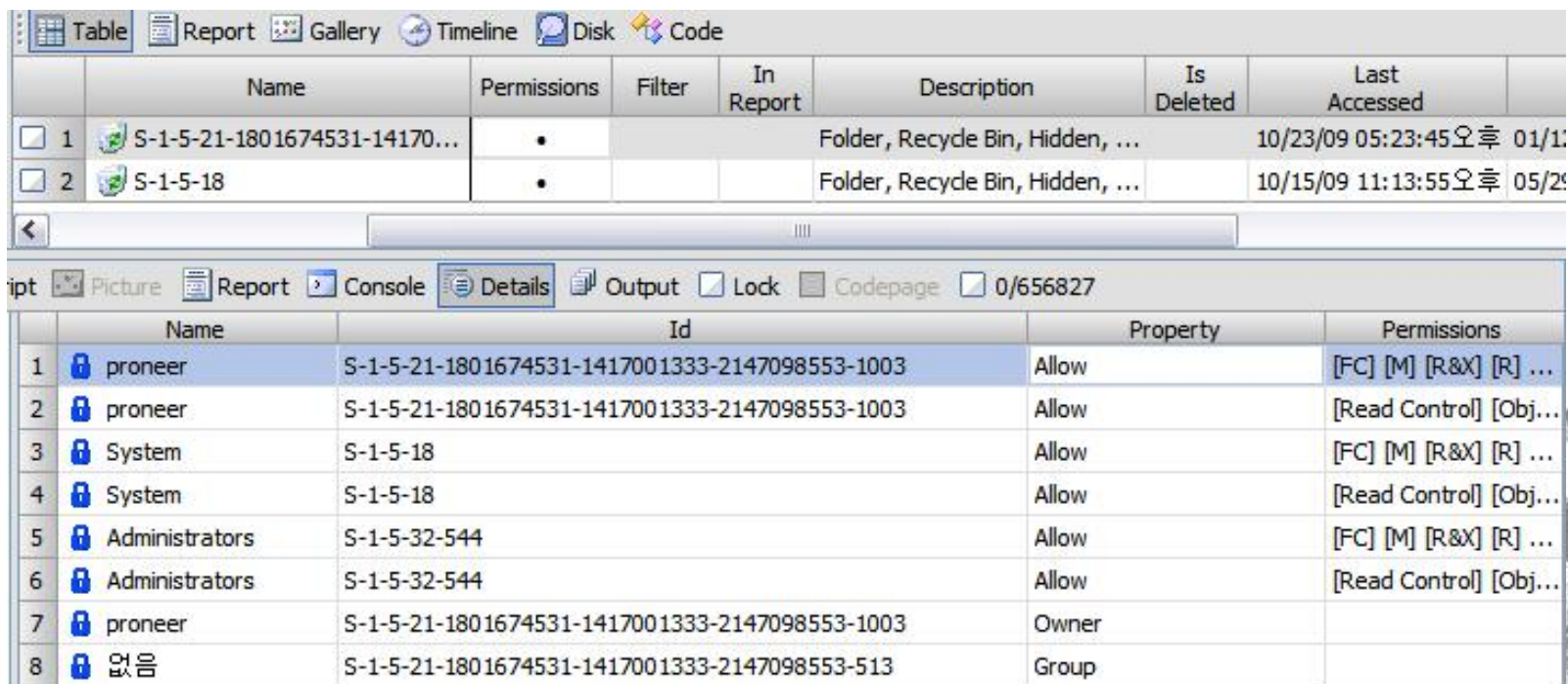




# Windows Operating System Artifacts

## Recycle Bin – Determining the Owner of Files

- 휴지통 폴더의 SID와 SAM 레지스트리 정보를 기반으로 삭제된 파일의 소유자 확인 가능
- EnCase는 Details 탭을 통해 손쉽게 해당 정보 확인 가능



The screenshot displays the EnCase software interface. The top section shows a list of folders in the Recycle Bin. The bottom section shows the 'Details' tab for a selected folder, displaying a list of permissions.

|                            | Name                         | Permissions | Filter | In Report | Description                      | Is Deleted | Last Accessed              |
|----------------------------|------------------------------|-------------|--------|-----------|----------------------------------|------------|----------------------------|
| <input type="checkbox"/> 1 | S-1-5-21-1801674531-14170... | •           |        |           | Folder, Recycle Bin, Hidden, ... |            | 10/23/09 05:23:45 오후 01/11 |
| <input type="checkbox"/> 2 | S-1-5-18                     | •           |        |           | Folder, Recycle Bin, Hidden, ... |            | 10/15/09 11:13:55 오후 05/29 |

|   | 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    |                        |

# Windows Operating System Artifacts

## Recycle Bin – Determining the Owner of Files

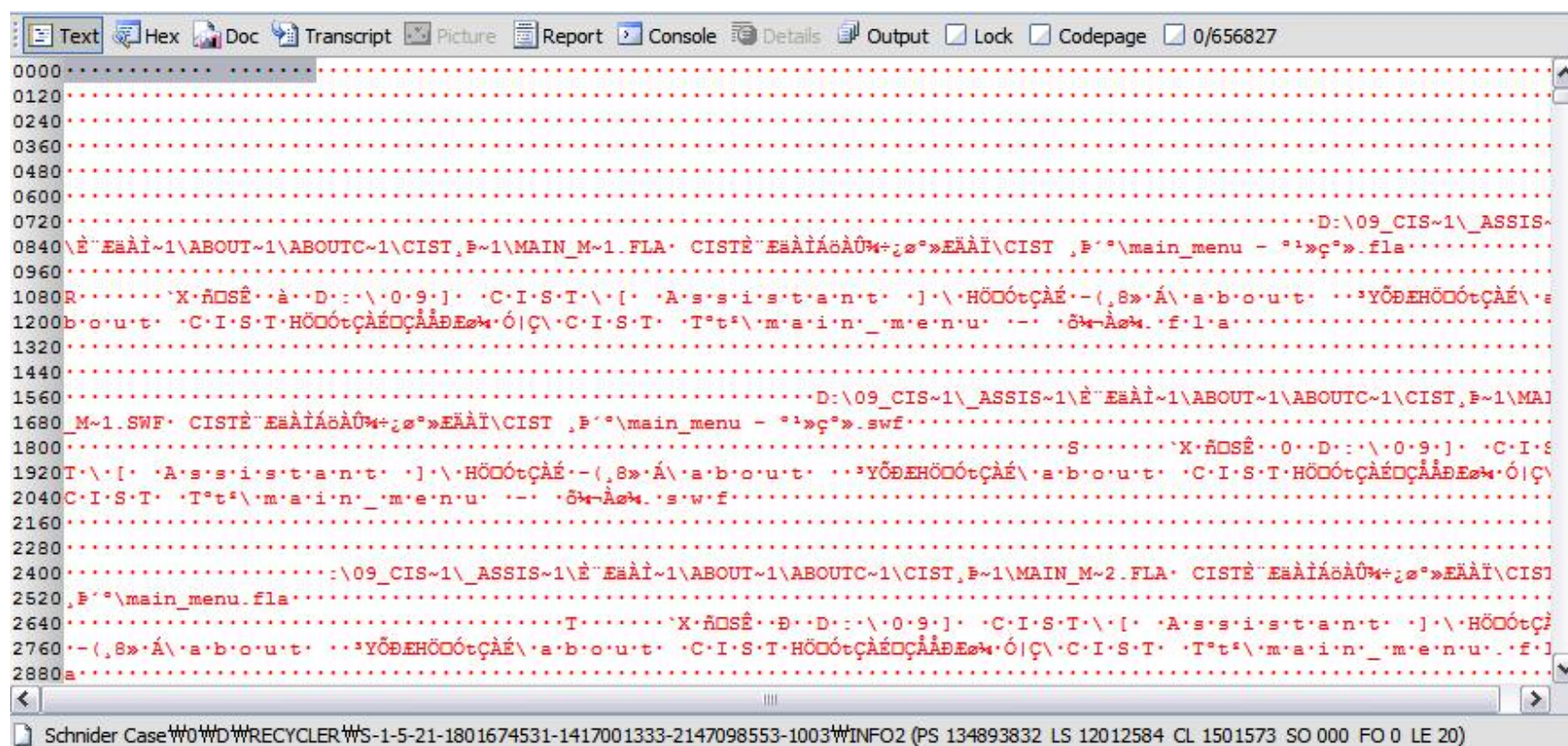
- 사용자가 휴지통을 비울 경우,  
휴지통에 존재하는 모든 파일의 디렉터리 엔트리 및 MFT 엔트리는 삭제된 것으로 표시
- INFO2 파일은 크기가 20 바이트로 줄어들면서 20바이트를 초기화
- 20 바이트 이후의 파일 슬랙을 이용해 휴지통을 비우기 전의 파일 정보 획득 가능
- 단, INFO2 파일이 연속적이지 않을 경우 조각난 클러스터의 정보는 획득하기 어려움
- 이 경우 Case Processor의 Recycle Info Record Finder를 이용하여 조각난 INFO2 파일을 검색



## Windows Operating System Artifacts

## Recycle Bin – Determining the Owner of Files

- 휴지통을 비운 후 초기화된 20바이트 이후의 슬랙 영역에 INFO2 Record가 존재하는 것을 확인



# Windows Operating System Artifacts

## Recycle Bin – Files Restored or Deleted from the Recycle Bin

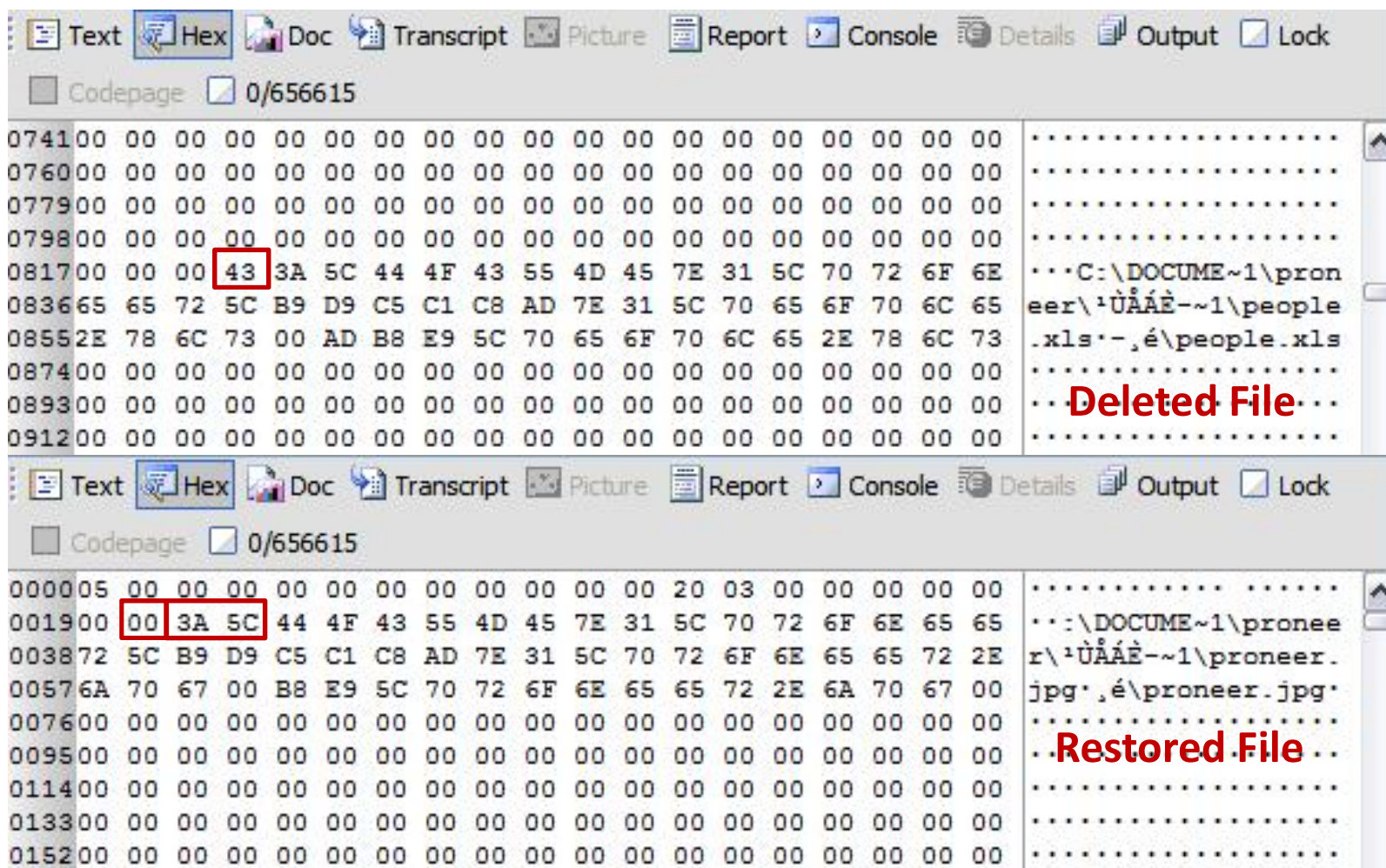
- 휴지통으로 이동된 파일에 대한 삭제와 복구에는 미묘한 차이가 존재
- 파일을 복구할 경우, 파일의 본래 위치에 디렉터리 및 MFT 엔트리를 새롭게 생성하여 복구
- 휴지통에 존재했던 삭제된 파일의 디렉터리 및 MFT 엔트리는 삭제된 것으로 표시
- 복구 시 INFO2 파일에서 복구된 파일을 표시하기 위해 원본 경로의 첫 바이트를 0x00으로 초기화
- FAT 파일시스템에서 파일 삭제 시 디렉터리 엔트리 첫 바이트를 0xE5로 변경하면 디렉터리 엔트리 검색 시 삭제된 것으로 인식
- FAT 파일시스템의 0xE5와 같은 효과로 첫 바이트를 0x00으로 변경





# Windows Operating System Artifacts

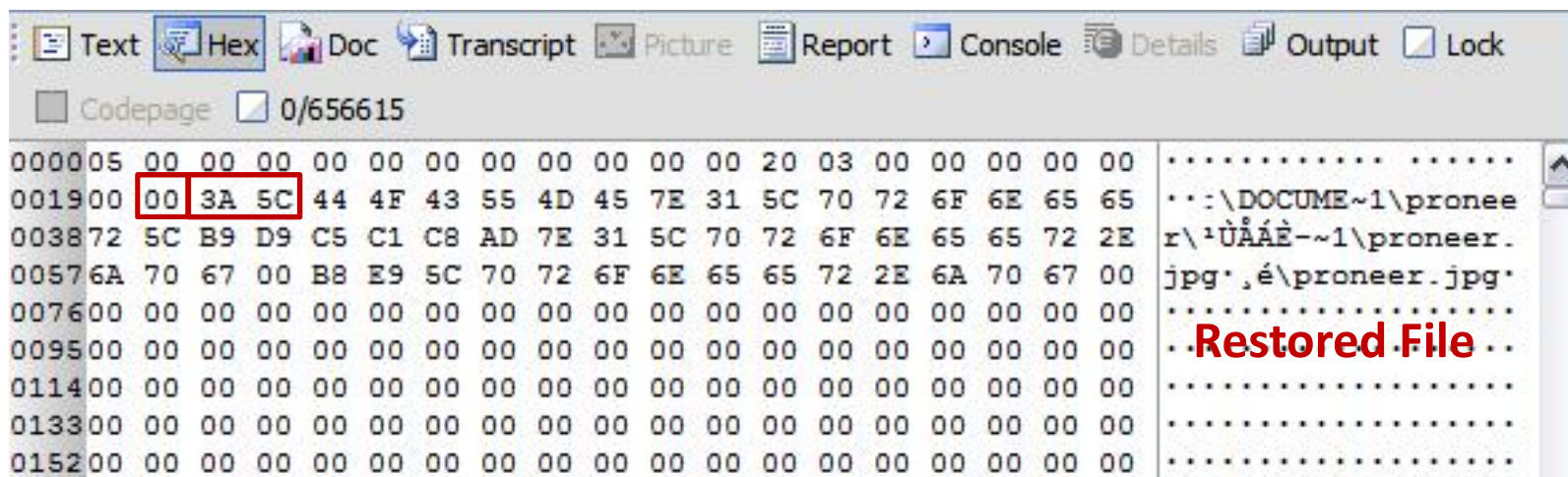
## Recycle Bin – Files Restored or Deleted from the Recycle Bin



# Windows Operating System Artifacts

## Recycle Bin – Files Restored or Deleted from the Recycle Bin

- 복구된 파일은 첫 바이트가 0x00으로 바뀌었기 때문에 이후의 “:₩”(0x3A5C)가 항상 존재
- 따라서, INFO2 파일의 레코드를 검색하면 복구된 파일을 쉽게 파악 가능



# Windows Operating System Artifacts

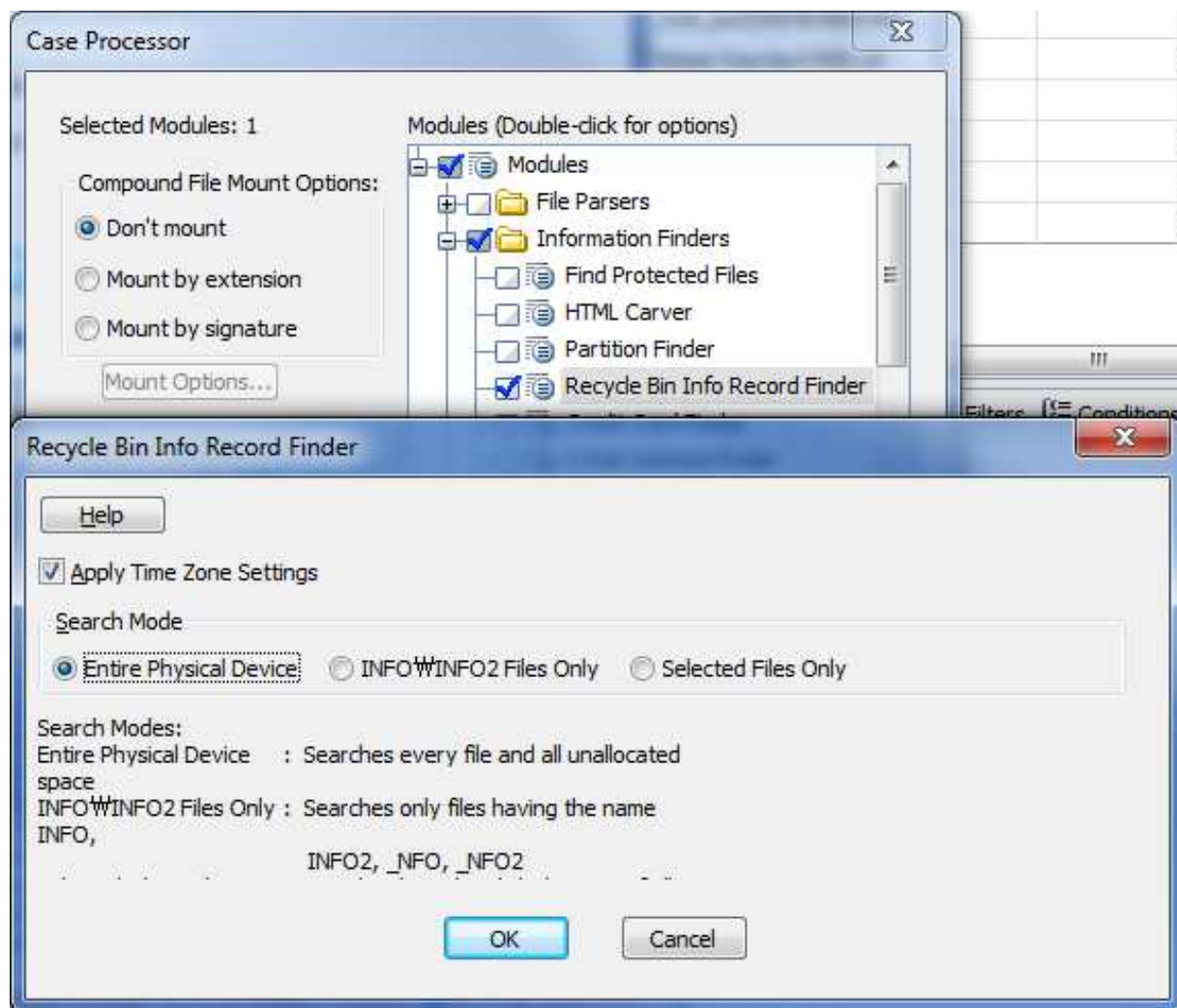
## Recycle Bin – Using an EnScript to Determine the Status of Recycle Bin Files

- 앞서 살펴본 바와 같이 INFO2 연속적이지 않은 상태에서 휴지통이 비워지거나 복구된 경우
- 휴지통을 계속 사용함으로써 지워진 INFO2 레코드가 디스크에 조각나 분포하게 됨
- EnCase에서는 이러한 INFO2 레코드를 찾기 위한 EnScript를 지원



# Windows Operating System Artifacts

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





# Windows Operating System Artifacts

## Recycle Bin – Recycle Bin Bypass

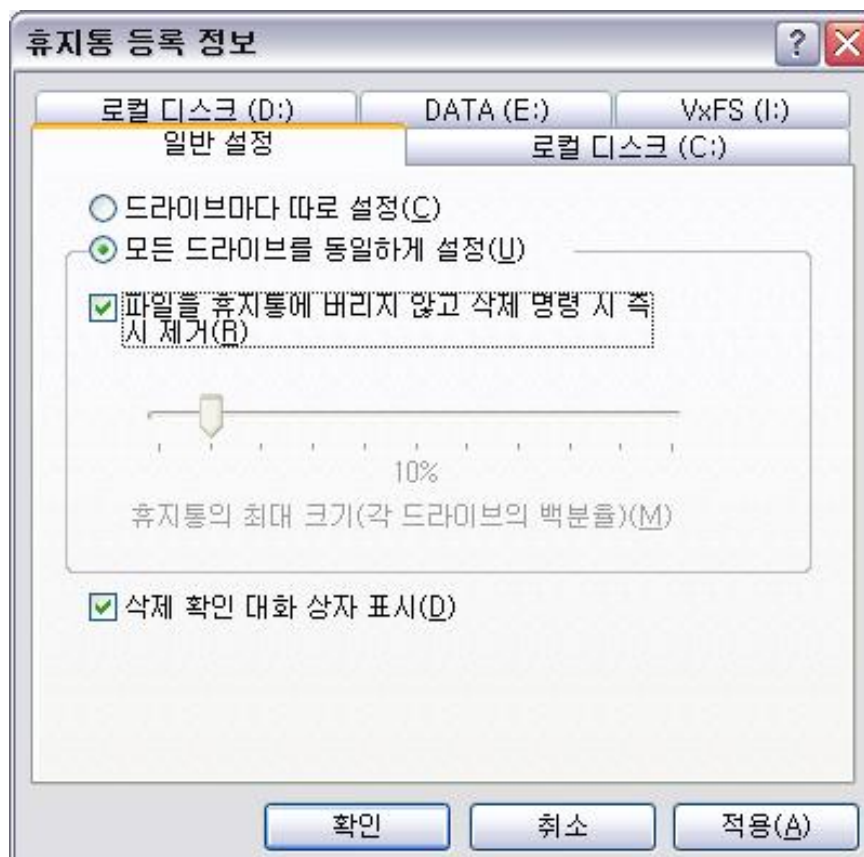
- 파일 삭제 시 삭제된 파일이 휴지통을 거치지 않고 바로 삭제되게 하는 방법
  - SHIFT KEY + DELETE KEY
  - 휴지통 속성 설정
  - 레지스트리 변경



# Windows Operating System Artifacts

## Recycle Bin – Recycle Bin Bypass

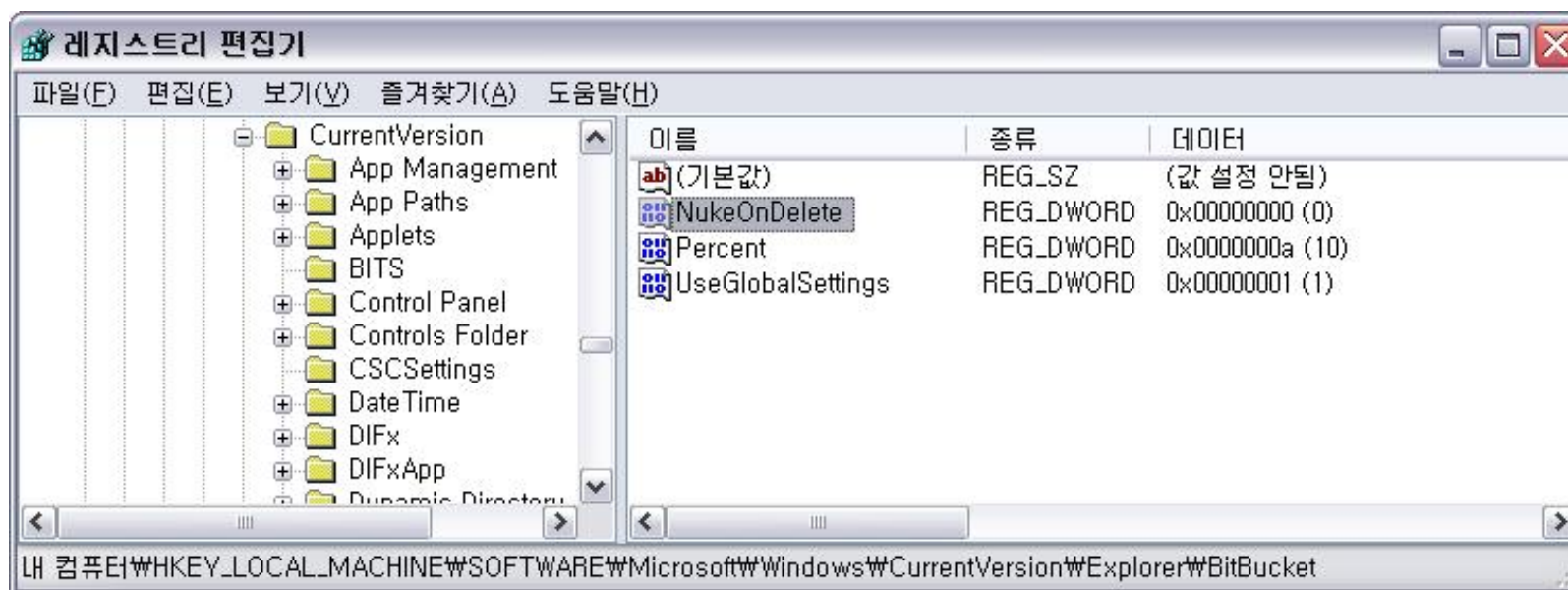
- 휴지통 속성 변경을 이용한 Bypass



# Windows Operating System Artifacts

## Recycle Bin – Recycle Bin Bypass

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket



- Bypass 설정 : 0x01
- Bypass 해제 : 0x00

# Windows Operating System Artifacts

## Recycle Bin – Windows Vista/7 Recycle Bin















- 윈도우 Vista/7으로 넘어오면서 휴지통 파일이 "\$Recycle.Bin"으로 변경
- INFO2 데이터베이스 파일은 새로운 이름으로 변경
- 기존에 INFO2 파일은 하나의 데이터베이스 파일에 모든 삭제된 파일 정보 표현
- Vista/7에서는 삭제된 각 파일마다 "\$I"로 시작하는 각각의 인덱스 파일이 생성됨
- Vista/7 에서는 삭제된 파일을 "\$R"로 시작하는 이름으로 변경
- Vista/7 모두 삭제된 파일의 확장자는 원본과 동일하게 유지



# Windows Operating System Artifacts

## Recycle Bin – Windows Vista/7 Recycle Bin

- 윈도우 Vista/7에서 삭제된 파일의 인덱스 파일과 내용
- 인덱스 파일에는 삭제되기 이전의 위치를 저장

|                             | Name  | In Report | File Ext |
|-----------------------------|---|-----------|----------|
| <input type="checkbox"/> 1  |  \$I00R4U.jpg    |           | jpg      |
| <input type="checkbox"/> 2  |  \$I001KPY.jpg   |           | jpg      |
| <input type="checkbox"/> 3  |  \$I002BM1.jpg   |           | jpg      |
| <input type="checkbox"/> 4  |  \$I003JCG.jpg   |           | jpg      |
| <input type="checkbox"/> 5  |  \$I005TZW.jpg   |           | jpg      |
| <input type="checkbox"/> 6  |  \$I008HH0.jpg   |           | jpg      |
| <input type="checkbox"/> 7  |  \$I00BDAQ.jpg   |           | jpg      |
| <input type="checkbox"/> 8  |  \$I00CA94.jpg   |           | jpg      |
| <input type="checkbox"/> 9  |  \$I00KCZJ.jpg   |           | jpg      |
| <input type="checkbox"/> 10 |  \$I01AAAK.jpg |           | jpg      |
| <input type="checkbox"/> 11 |  \$I01AMHP.jpg |           | jpg      |
| <input type="checkbox"/> 12 |  \$I01BI58.jpg |           | jpg      |
| <input type="checkbox"/> 13 |  \$I01BVU4.jpg |           | jpg      |
| <input type="checkbox"/> 14 |  \$I01JAR3.jpg |           | jpg      |










|     |   |                            |
|-----|---|----------------------------|
| 000 | 01 00 00 00 00 00 00 00 84 80 00 00 00 00 00 00 B0 00 14 B6 D6 FA CA 01 | ..... .....*--ŲŲŲŲ         |
| 024 | 45 00 3A 00 5C 00 44 00 45 00 46 00 43 00 4F 00 4E 00 5C 00 44 00 44 00 | E-:-\ -D-E-F-C-O-N-\ -D-D- |
| 048 | 44 00 5C 00 30 00 30 00 35 00 34 00 32 00 2E 00 6A 00 70 00 67 00 00 00 | D-\ -0-0-5-4-2-.-j-p-g---  |
| 072 | 00       | .....                      |
| 096 | 00       | .....                      |

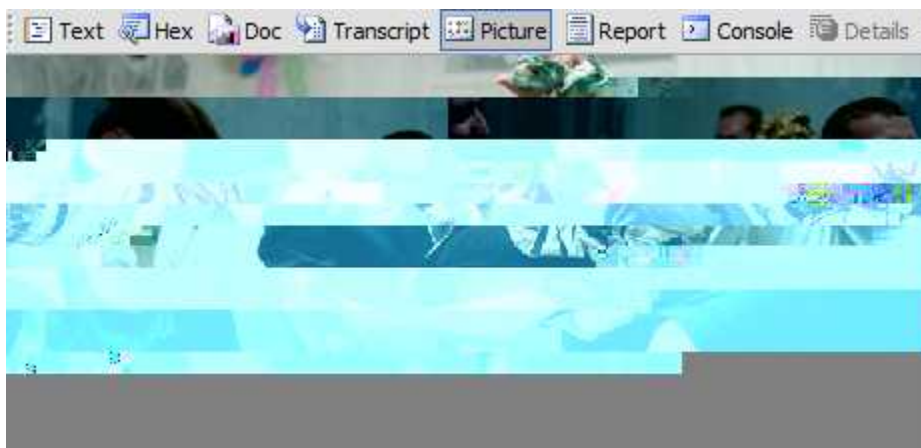


# Windows Operating System Artifacts

## Recycle Bin – Windows Vista/7 Recycle Bin

- EnCase 6.3 버전 이후부터 삭제된 파일인 "\$R"로 시작하는 파일은 원래 이름 그대로 보여줌

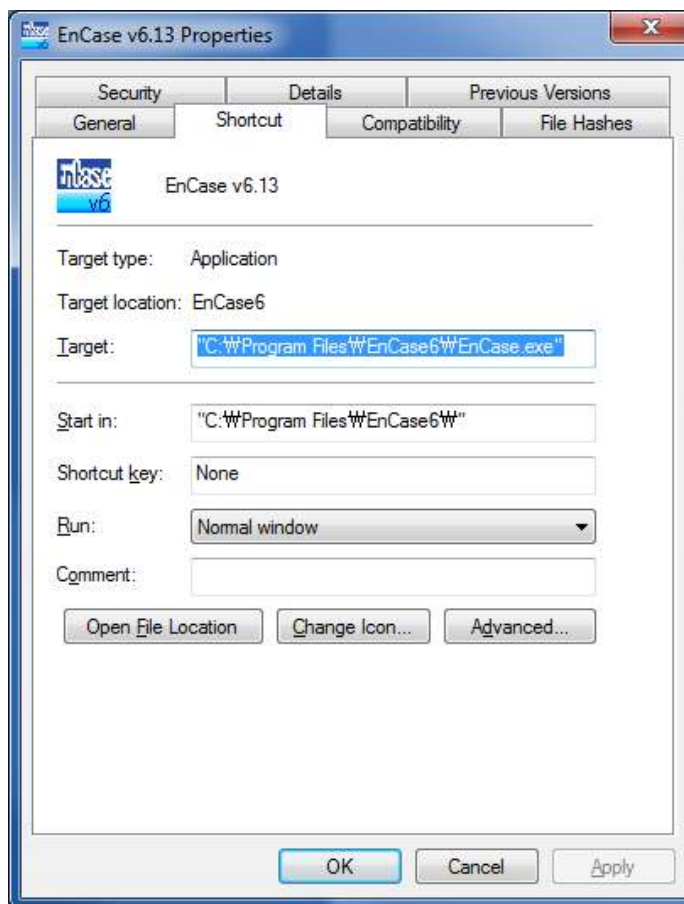
|                               | Name  | In Report | File Ext |
|-------------------------------|---|-----------|----------|
| <input type="checkbox"/> 8741 |  00540.jpg |           | jpg      |
| <input type="checkbox"/> 8742 |  00541.jpg |           | jpg      |
| <input type="checkbox"/> 8743 |  00541.jpg |           | jpg      |
| <input type="checkbox"/> 8744 |  00542.jpg |           | jpg      |
| <input type="checkbox"/> 8745 |  00542.jpg |           | jpg      |
| <input type="checkbox"/> 8746 |  00543.jpg |           | jpg      |
| <input type="checkbox"/> 8747 |  00543.jpg |           | jpg      |
| <input type="checkbox"/> 8748 |  00544.jpg |           | jpg      |
| <input type="checkbox"/> 8749 |  00544.jpg |           | jpg      |



# Windows Operating System Artifacts

## Link Files

- Link Files : shortcut(.lnk) file
- Recent, Start, Desktop, Send To folder 등에 존재





# Windows Operating System Artifacts

## Link Files – Forensic Importance

- 링크 파일은 윈도우 운영체제의 다양한 곳에 존재
- 사용자가 직접 생성하지 않아도 자동적으로 생성되어 사용자의 활동을 파악할 수 있음
- 일반적으로, 프로그램 설치 시 “Program Files” 폴더에 관련 파일이 생성되고, 시작메뉴에 등록됨
- 일부 옵션을 통해 바탕화면, 빠른 실행에도 링크 파일 생성을 지원
- 가장 중요한 점은 사용자의 인지 없이 생성된다는 점
- 사용자가 특정 문서를 실행한 경우 최근 문서 목록에 링크 파일이 생성
- 위와 같은 흔적으로 인해 특정 프로그램의 설치 여부, 특정 데이터 사용 여부를 판별
- 이외에도 시간 정보, 볼륨 시리얼 번호를 이용하여 다양한 분석 가능





# Windows Operating System Artifacts

## Link Files – Forensic Importance

- 링크 파일에 포함되는 정보
  - 타겟 파일이나 폴더가 존재하는 볼륨의 시리얼 번호
  - 타겟 파일 크기
  - 타겟 파일의 MAC 시간 정보



## Windows Operating System Artifacts

## Link Files – Forensic Importance

- 링크 파일에 포함되는 정보
  - 타겟 파일이나 폴더가 존재하는 볼륨의 시리얼 번호

|                             | Name   | In Report | File Ext |
|-----------------------------|--|-----------|----------|
| <input type="checkbox"/> 11 | 01416.rar.lnk                                      |           | lnk      |
| <input type="checkbox"/> 12 | 01417.rar.lnk                                      |           | lnk      |
| <input type="checkbox"/> 13 | 05] PICTURES.lnk                                   |           | lnk      |
| <input type="checkbox"/> 14 | 100APPLE.lnk                                       |           | lnk      |
| <input type="checkbox"/> 15 | 7f811b0f9c4f4d16(theHoff).rar.lnk                  |           | lnk      |
| <input type="checkbox"/> 16 | [ ENCASE ].lnk                                     |           | lnk      |
| <input type="checkbox"/> 17 | [ SHARED DATA ].lnk                                |           | lnk      |
| <input type="checkbox"/> 18 | [20091024] EnCase #6 Windows Operating System A... |           | lnk      |
| <input type="checkbox"/> 19 | [20091031] EnCase #7 Windows Operating System A... |           | lnk      |

Output

Lock

Codepage

0/983483

00 20 00

21 B8 22

L.....À.....F|..

...0|o"0<é·|!,"éüê·|!,"

éüê·

...|...PàOè è:i·c0·+0

0|../E:\

...d·1·...°<t|...\_SHARE~

1·L·...i·a9Öu°<t|\*·...

.....[·

·S·H·A·R·E·D· ·D·A·T·A·

·J·...E·...1C 00 00

·1·...D·...|Ö·

·...DATA·E:\[ SHARED DA

TA ]··(·...·...1SPSâ|

XF\*L8C»ü·|&|mÎ·

...X·...prioneer-pc

...·Öü|'8·!D«á'Îü|·(è·

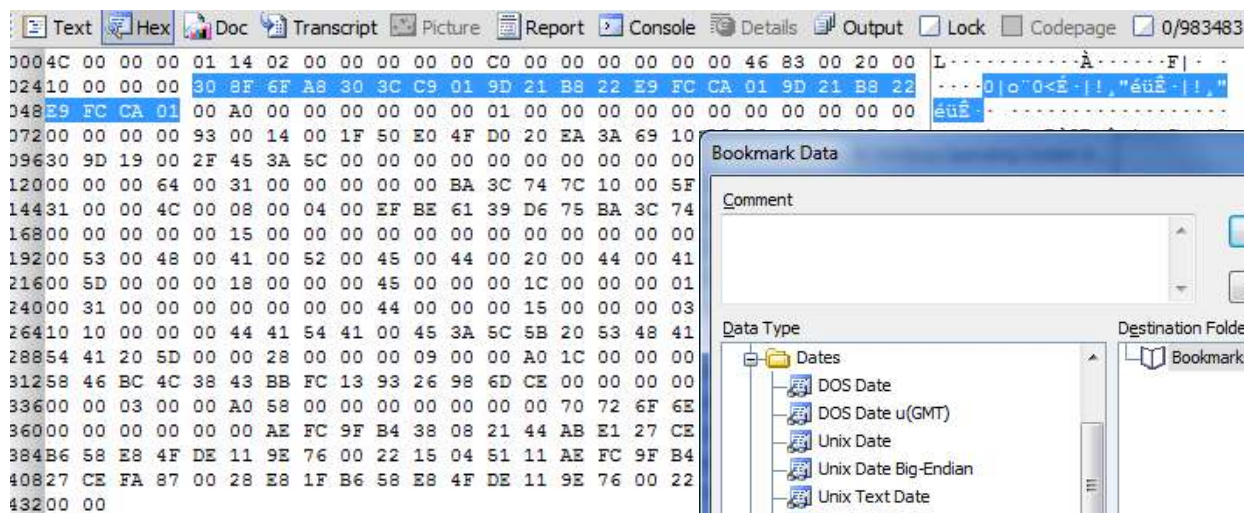
TXèOè·|v·"·Q·Öü|'8·!D«á

'Îü|·(è·TXèOè·|v·"·Q·...

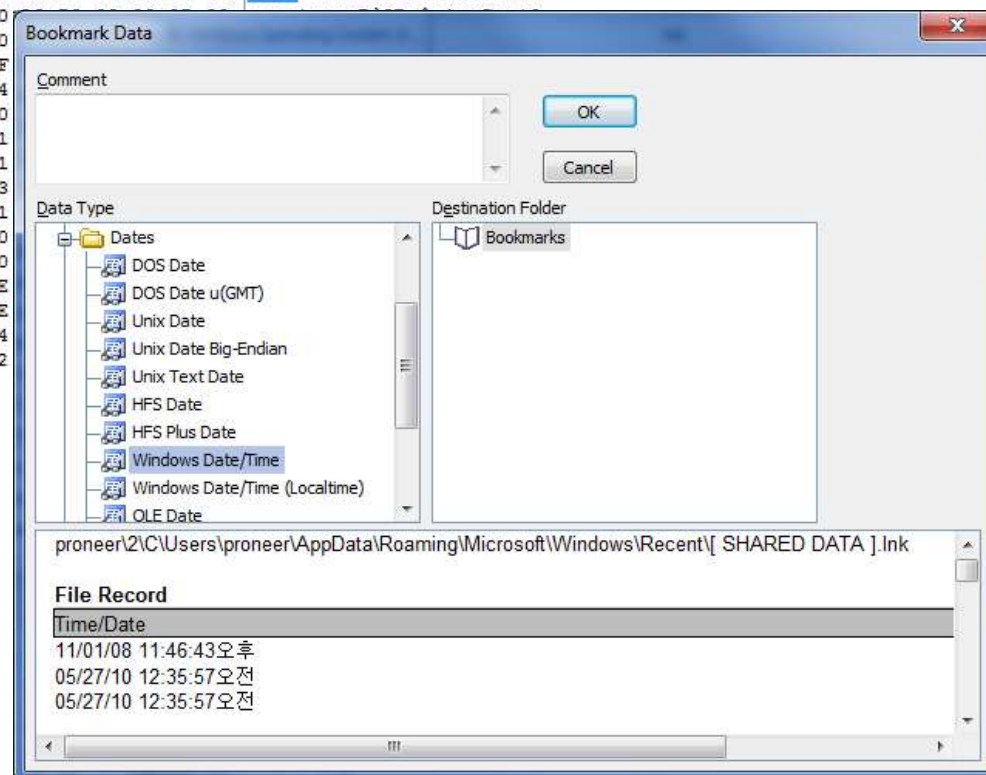
# Windows Operating System Artifacts

## Link Files – Forensic Importance

- 링크 파일에 포함되는 정보
  - 타겟 파일의 MAC 시간 정보



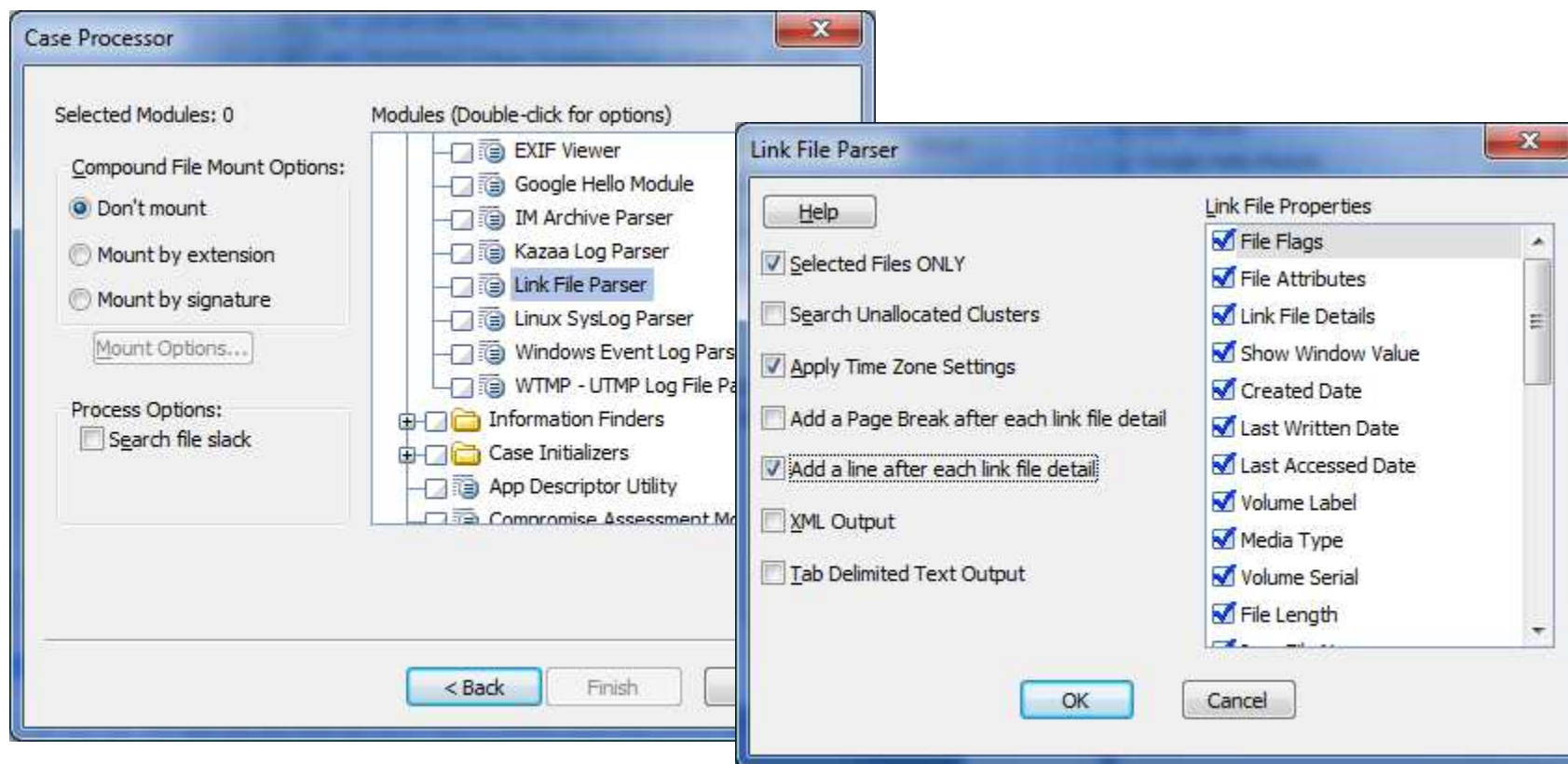
000 4C 00 00 00 01 14 02 00 00 00 00 C0 00 00 00 00 00 46 83 00 20 00 L .....À.....F| ..  
024 10 00 00 00 30 8F 6F A8 30 3C C9 01 9D 21 B8 22 E9 FC CA 01 9D 21 B8 22 .....0|o"O<È·|!,"éüÈ·|!,"  
048 E9 FC CA 01 00 A0 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 éüÈ·  
072 00 00 00 00 93 00 14 00 1F 50 E0 4F D0 20 EA 3A 69 10 .....  
096 30 9D 19 00 2F 45 3A 5C 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
120 00 00 00 64 00 31 00 00 00 00 00 BA 3C 74 7C 10 00 5F .....  
144 31 00 00 4C 00 08 00 04 00 EF BE 61 39 D6 75 BA 3C 74 .....  
168 00 00 00 00 15 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
192 00 53 00 48 00 41 00 52 00 45 00 44 00 20 00 44 00 41 .....  
216 00 5D 00 00 00 18 00 00 00 45 00 00 00 1C 00 00 00 01 .....  
240 00 31 00 00 00 00 00 00 00 44 00 00 00 15 00 00 00 03 .....  
264 10 10 00 00 00 44 41 54 41 00 45 3A 5C 5B 20 53 48 41 .....  
288 54 41 20 5D 00 00 28 00 00 00 09 00 00 A0 1C 00 00 00 .....  
312 58 46 BC 4C 38 43 BB FC 13 93 26 98 6D CE 00 00 00 00 .....  
336 00 00 03 00 00 A0 58 00 00 00 00 00 00 00 70 72 6F 6E .....  
360 00 00 00 00 00 AE FC 9F B4 38 08 21 44 AB E1 27 CE .....  
384 B6 58 E8 4F DE 11 9E 76 00 22 15 04 51 11 AE FC 9F B4 .....  
408 27 CE FA 87 00 28 E8 1F B6 58 E8 4F DE 11 9E 76 00 22 .....  
432 00 00



# Windows Operating System Artifacts

## Link Files – Using the Link File Parser EnScript

- 링크파일은 복잡한 구조를 가짐
  - <http://www.stdlib.com/art6-Shortcut-File-Format-lnk.html>
- EnCase 에는 링크 파일을 자동으로 파싱해 주는 EnScript가 기본적으로 지원





# Windows Operating System Artifacts

## Link Files – Using the Link File Parser EnScript

2

---

Case Report\Link File Parser\2Page 1

---

1) proneer\2\C\Users\proneer\AppData\Roaming\Microsoft\Windows\Recent\{300\_46646289fff26adc0}.ppt.lnk

Link File: {300\_46646289fff26adc0}.ppt.lnk

Full Path: proneer\2\C\Users\proneer\AppData\Roaming\Microsoft\Windows\Recent\{300\_46646289fff26adc0}.ppt.lnk

Ink

Offset: 0

Size: 594

File Flags: HASITEMID | ISFILEORFOLDER | HASRELATIVEPATH | HASWORKINGDIRECTORY

File Attributes: ARCHIVE

Show Window Value: SW\_NORMAL\_WT

Created Date: 05/26/10 03:14:57 오후

Last Written Date: 05/22/10 04:47:19 오후

Last Accessed Date: 05/26/10 03:14:57 오후

Volume Label: C

Media Type: Fixed

Volume Serial: 04 4A D8 3B

File Length: 3207680

Icon File Name:

Command Line:

Base Path: C:\Users\proneer\Desktop\{300\_46646289fff26adc0}.ppt

Application Path:

Working Directory: C:\Users\proneer\Desktop

Share Name:

Mapped Drive Letter:

Description:

NetBIOS: åŠXF¼L8C»ü "&~mİ

MAC Address: eb 5b e1 66 df 11

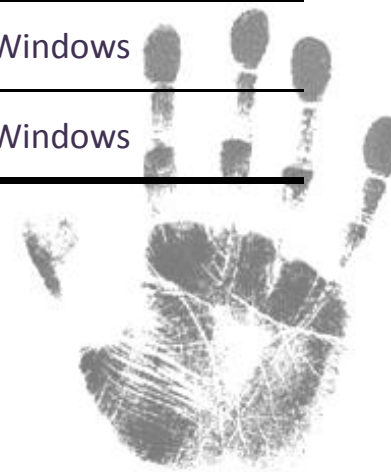


# Windows Operating System Artifacts

## Windows 2000, XP, and Vista Folders

- 윈도우 각 버전 별로 고유한 디렉터리 구조를 가짐

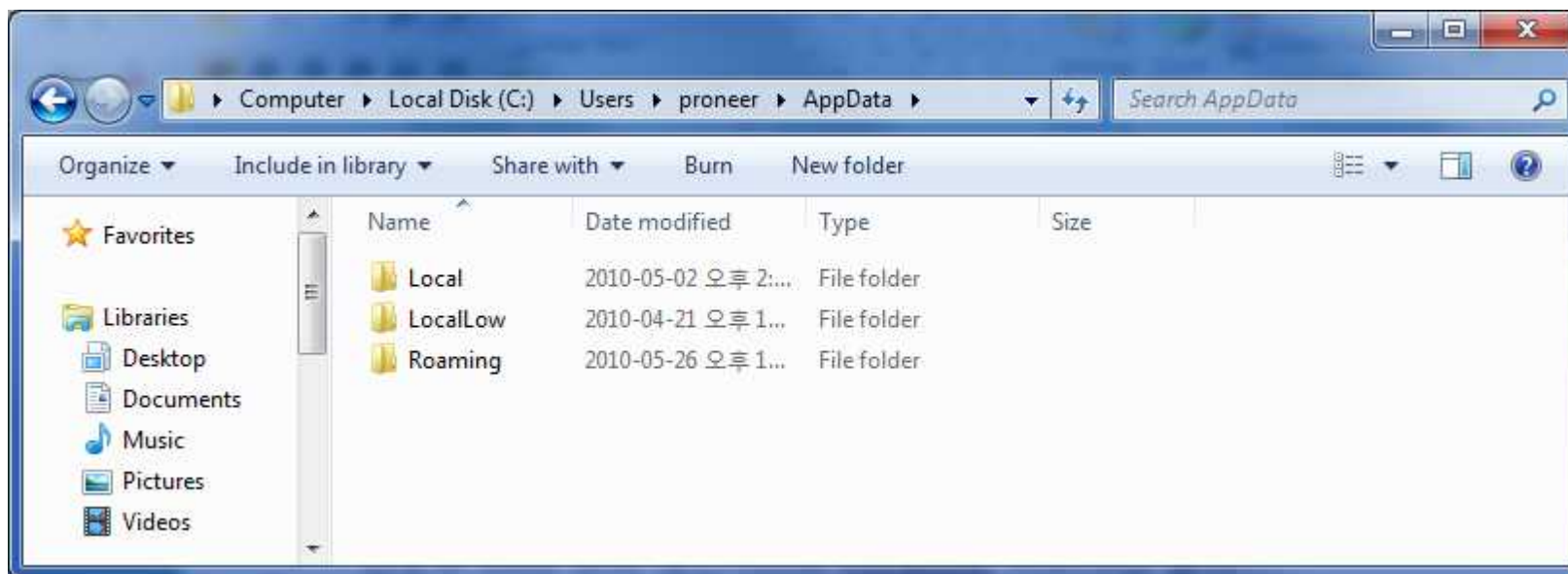
| Operating System | User Profile Folders                                  | Default System Folder |
|------------------|---|-----------------------|
| Windows 9x/ME    | No Documents and Settings Folder                      | C:\Windows            |
| Windows NT       | No Documents and Settings Folder<br>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 Operating System Artifacts

## Windows 2000, XP, and Vista Folders

- 윈도우 Vista 부터 생긴 Local, LocalLow, Roaming 폴더
- C:\Users\[user name]\AppData\



# Windows Operating System Artifacts

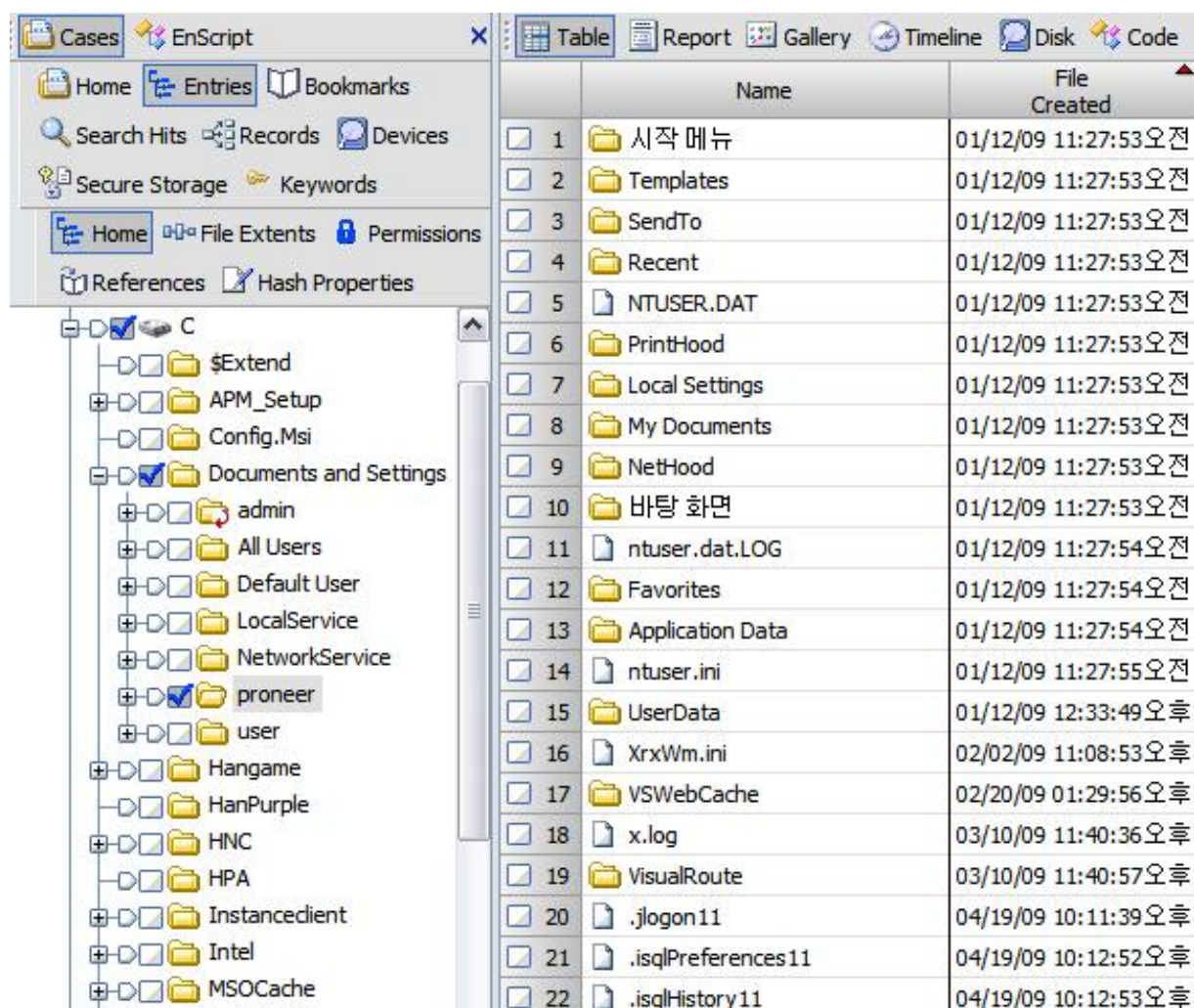
## Windows 2000, XP, and Vista Folders

- “Local, LocalLow”
  - [XP] : Documents and Settings\user name\Local Settings\Application Data\
  - 사용자와 함께 로밍하지 않는 응용프로그램 데이터
  - 데이터의 크기가 비교적 큼
  - LocalLow는 Local 보다 상대적으로 중요한(위험도가 높음) 데이터
- “Roaming”
  - [XP] : Documents and Settings\user name\Application Data\
  - 이전 윈도우 버전은 사용자 프로필 정보가 각 컴퓨터 로컬에 저장(다중 사용자 시스템의 경우)
  - 사용자 관련 데이터 분리
  - 사용자가 다른 컴퓨터에서 로그인 할 때마다 로드할 수 있도록 지원
  - 시스템과 독립적으로 항상 자신의 프로필과 로밍 데이터를 사용하여 로그인 가능



# Windows Operating System Artifacts

## 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

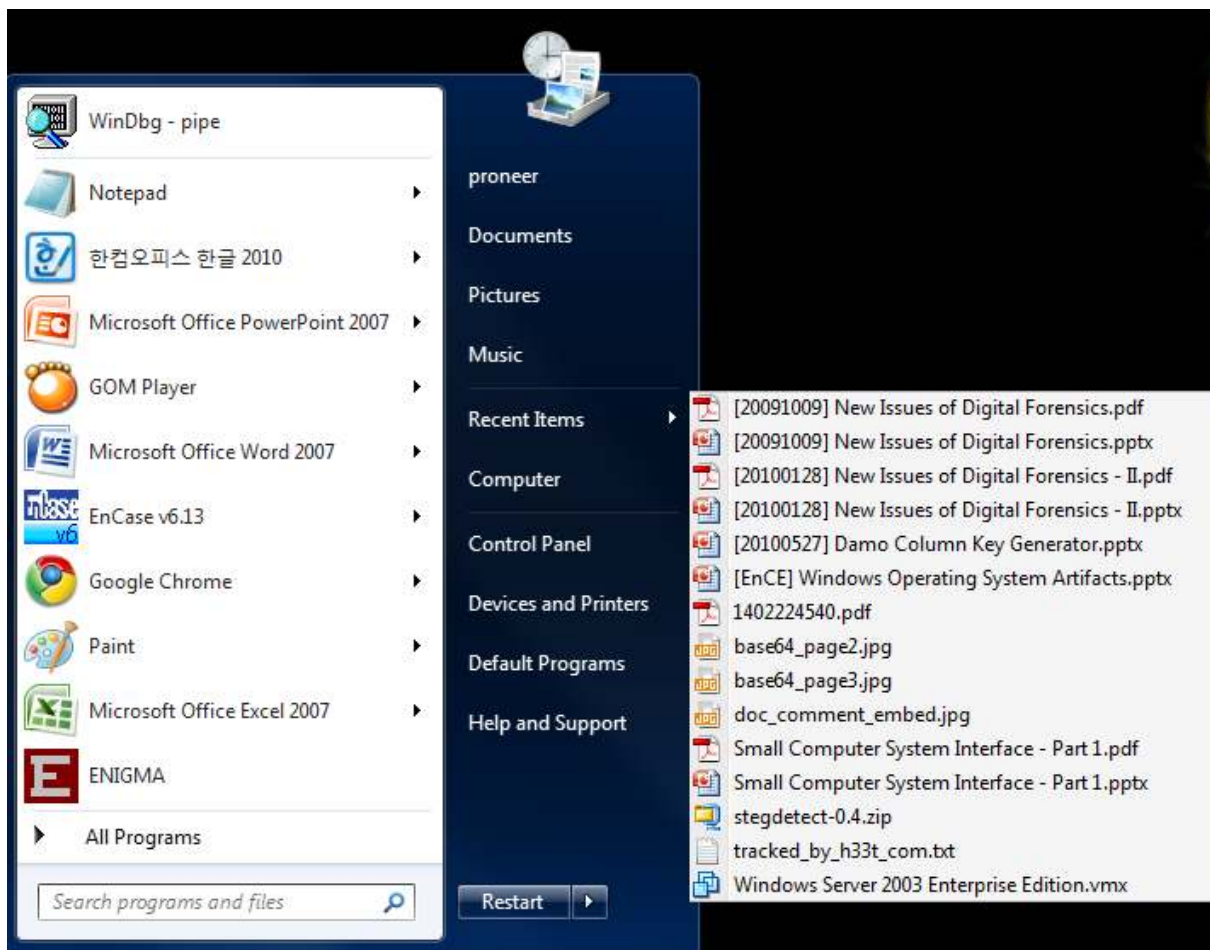
- [XP] : Documents and Settings\W[user name]\Recent\W
- [Vista/7] : Users\W[user name]\AppData\Roaming\Microsoft\Windows\Recent\W
- Recent 폴더는 사용자가 최근에 생성하거나 수정한 파일에 대한 링크 파일 저장
- 특정 프로그램을 실행하거나 디렉터리 탐색을 위해 링크 파일을 주고 사용
- 따라서, 링크 파일은 RAM에 로드될 가능성이 매우 큼
- Swap out 되어 pagefile.sys에 저장될 가능성도 큼
- 파일의 크기가 보통 2KB 미만이기 때문에 파일이 조각날 가능성이 거의 없음
- Link File Parser EnScript를 통해 비활당영역, pagefile.sys로부터 링크 파일 복구 가능
- 링크 파일 내에 존재하는 다양한 정보를 기반으로 의미 있는 해석이 가능



# Windows Operating System Artifacts

## Recent Folder

- [Vista/7] : 시작 메뉴 -> 최근 아이템 확인 (기본적으로 15개의 목록을 보여줌)

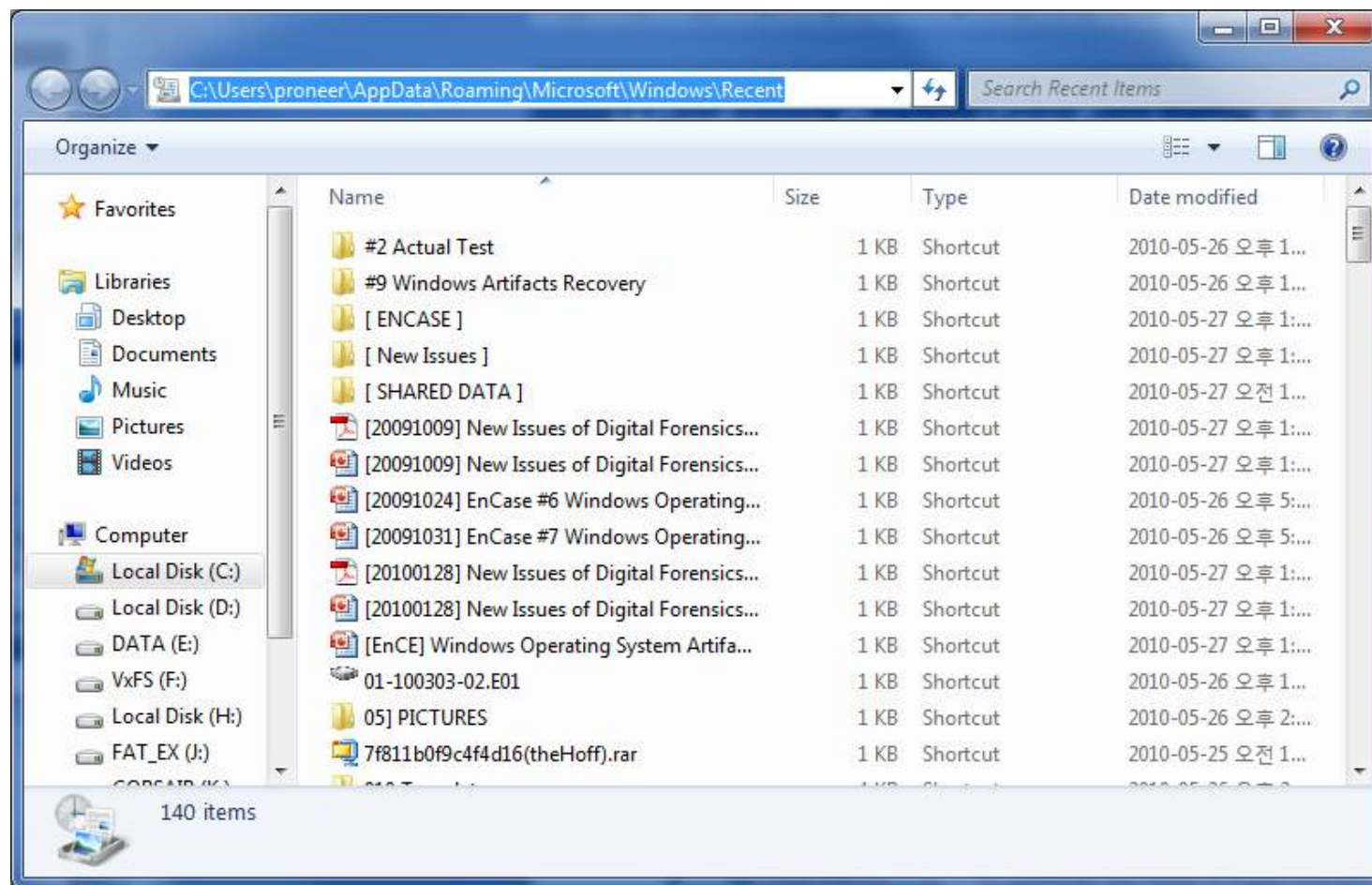




# Windows Operating System Artifacts

## Recent Folder

- 실제 최근 문서 폴더에는 15개보다 더 많은 최근 접근 및 수정 파일에 대한 링크 파일이 존재



# Windows Operating System Artifacts

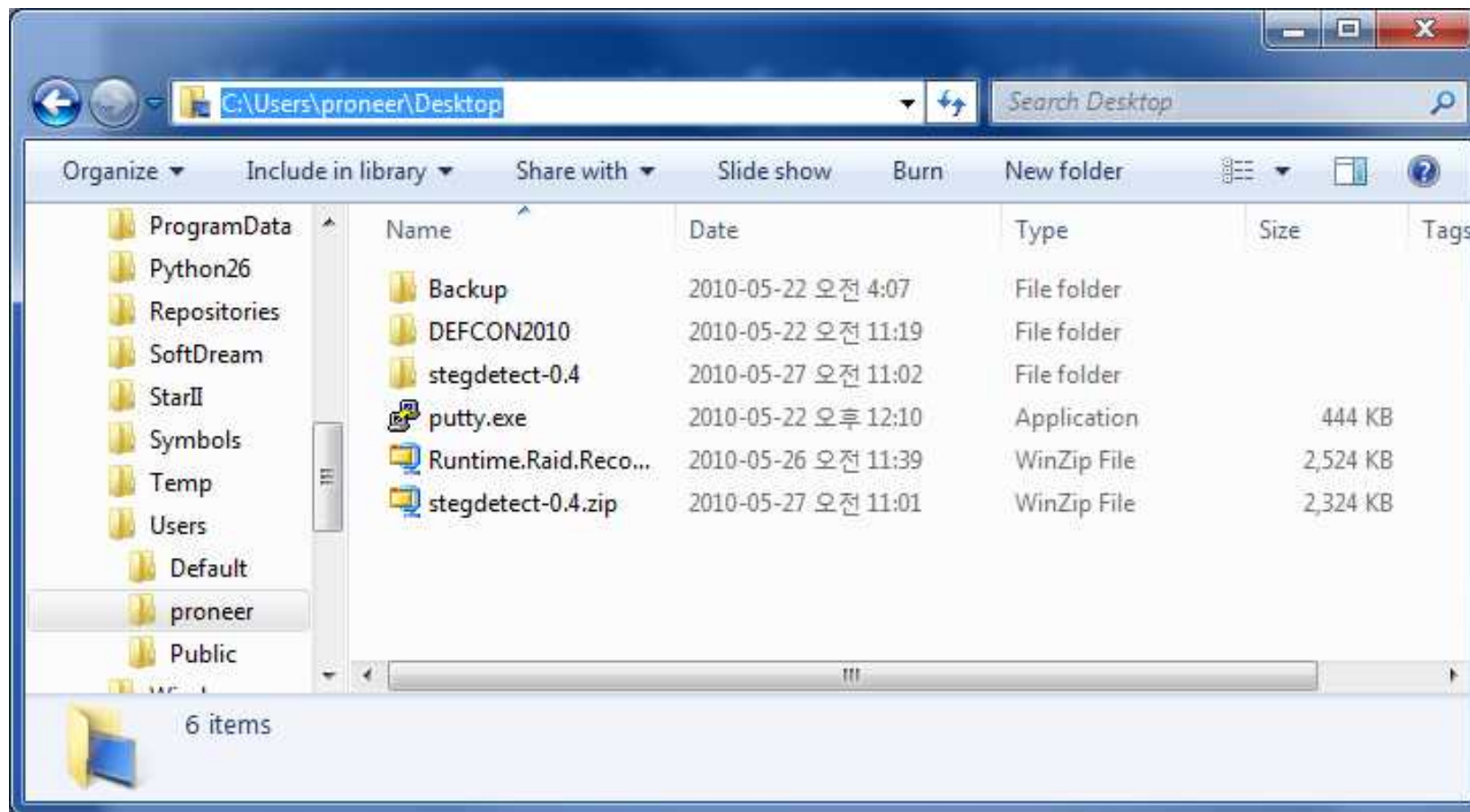
## Desktop Folder

- 윈도우 운영체제의 바탕화면의 내용을 저장하는 폴더
- 윈도우 2000/XP/Vista/7 : 총 3가지의 정보를 사용하여 바탕화면 구성
  - 레지스트리
  - All Users/Desktop(2000/XP) 또는 Public/Desktop(Vista/7) 폴더
  - 사용자 Desktop 폴더
- 위 정보를 바탕으로 사용자마다 독립적인 바탕화면을 구성



# Windows Operating System Artifacts

## Desktop Folder



# Windows Operating System Artifacts

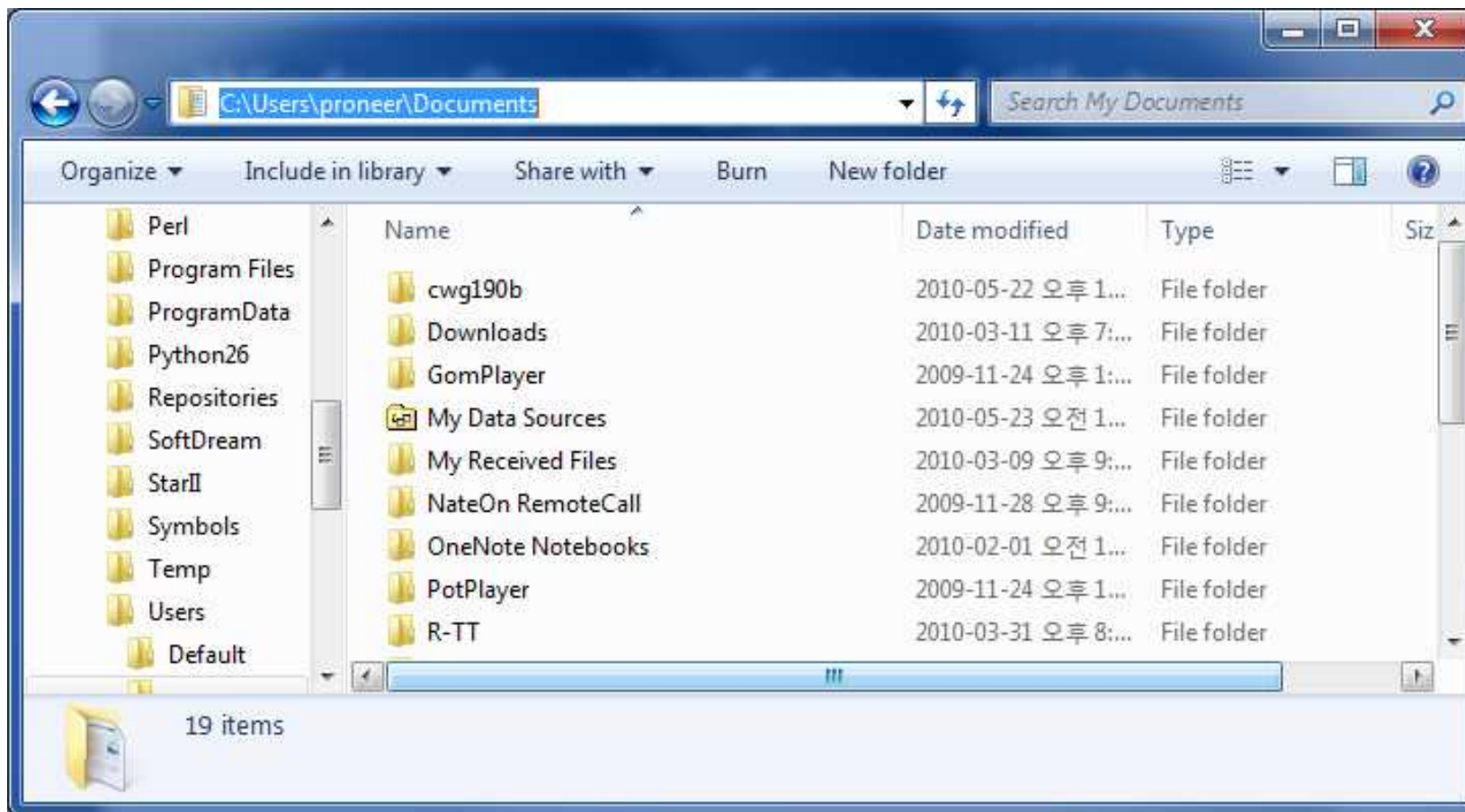
## My Documents/Documents Folder

- [2000/XP] : Documents and Settings\user name\My Documents\
- [Vista/7] : Users\user name\Documents
- [2000/XP] : 기본적인 하위 폴더로 My Pictures, My Music, My Video 존재
- [Vista/7] : 기본적인 하위 폴더로 Pictures, Music, Video 존재
- 대부분의 프로그램에서 기본 저장 폴더로 사용자 폴더 하위의 Documents 폴더를 사용
- 결국, My Documents/Documents는 사용자의 시스템 사용 행위를 판단하는데 중요한 요소



# Windows Operating System Artifacts

## My Documents/Documents Folder



# Windows Operating System Artifacts

## Send To Folder

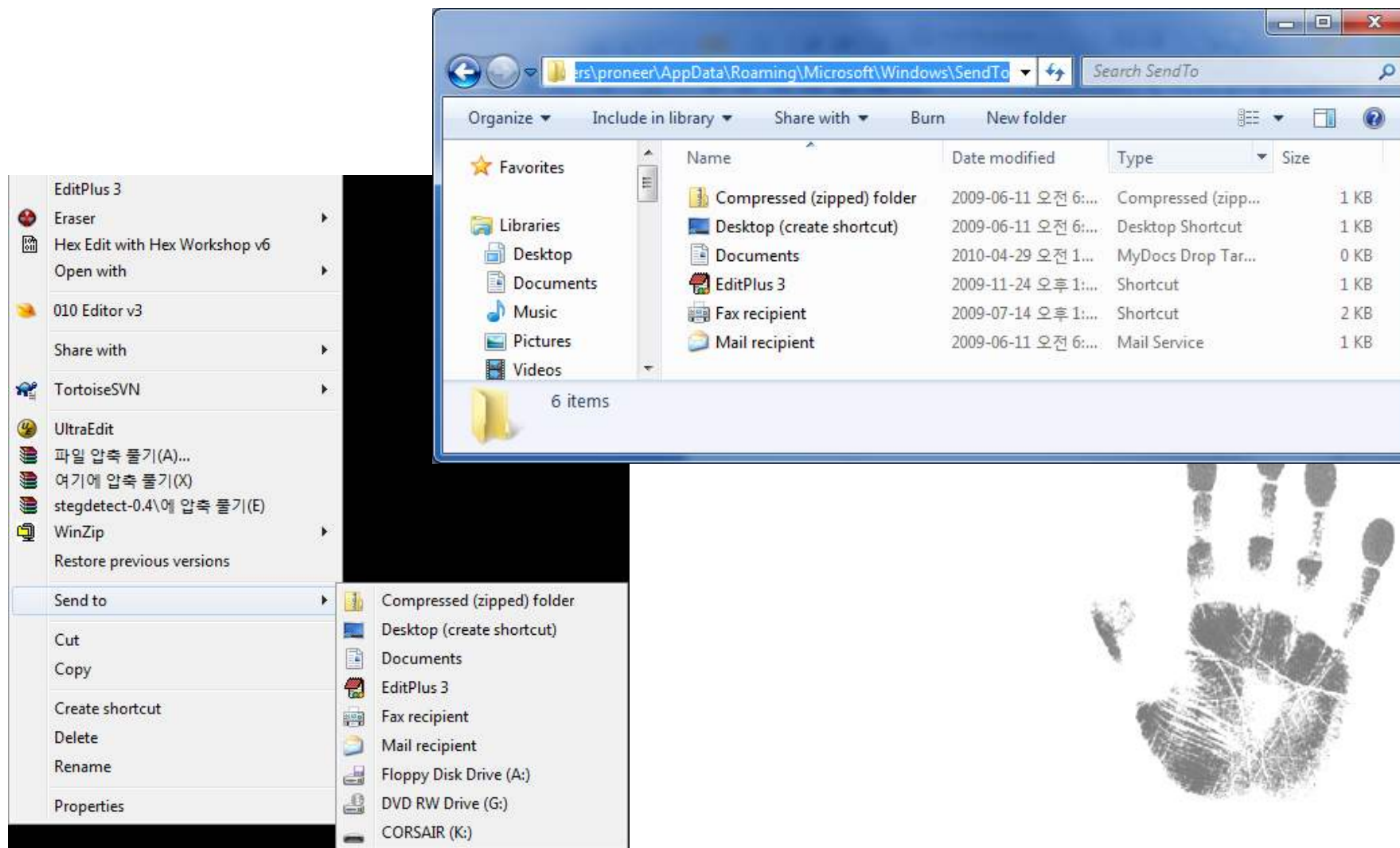
- [2000/XP] : Documents and Settings\user name\SendTo\
- [Vista/7] : Users\user name\AppData\Roaming\Microsoft\Windows\SendTo\
- Explorer 탐색 시 기본적으로 보여줌
- 특정 소프트웨어 설치 시 Send To 폴더에 링크 파일 생성
- 결국, 특정 소프트웨어의 설치 여부 확인 가능





# Windows Operating System Artifacts

## Send To Folder



# Windows Operating System Artifacts

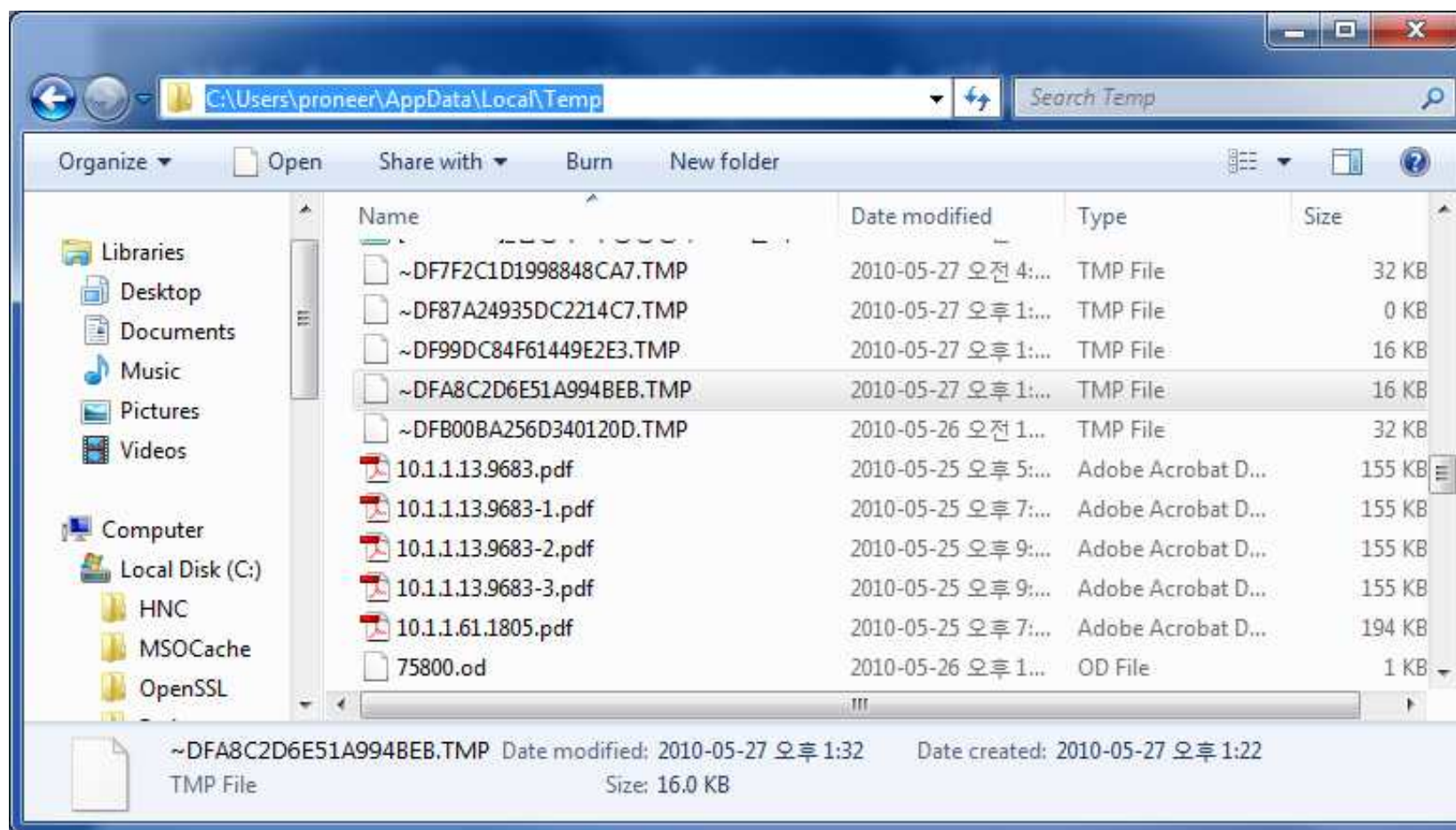
## Temp Folder

- [2000/XP] : Documents and Settings\W[user name]\WLocal Settings\WTemp\W
- [Vista/7] : Users\W[user name]\WAppData\WLocal\WTemp\W
- 프로그램 설치 및 실행 시 설치데이터의 임시 사용 공간
- Internet Explorer를 통해 파일 다운로드 시 임시적인 저장 공간
- 프로그램 종료 및 삭제 이후에도 해당 폴더의 내용이 삭제되지 않는 경우가 종종 있음
- 프로그램의 설치 및 사용 여부 확인 가능
- 다운로드 받은 파일 흔적 확인



# Windows Operating System Artifacts

## Temp Folder



# Windows Operating System Artifacts

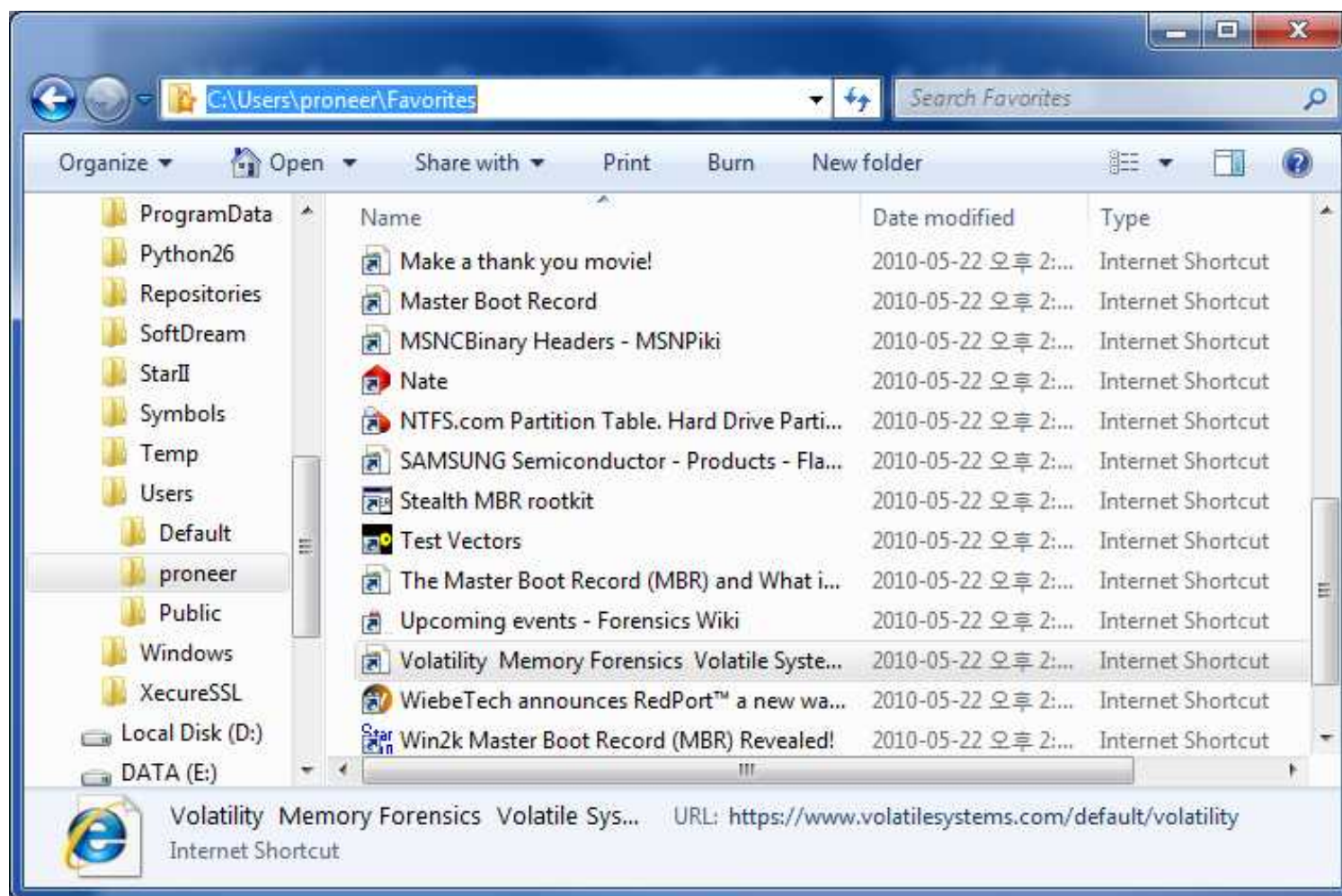
## Favorite Folder

- [2000/XP] : Documents and Settings\W[user name]\Favorites\
- [Vista/7] : :\Users\W[user name]\Favorites
- Internet Explorer에 대한 인터넷 즐겨찾기
- URL(Uniform Resource Locator) 파일 형식으로 저장
- 윈도우 설치 시 기본적인 즐겨 찾기가 생성
- 이후 사용자가 직접적으로 변경하거나 추가
- 사용자의 인터넷 방문 형태 확인 가능 (자주 방문하는 페이지 등)



# Windows Operating System Artifacts

## Favorite Folder

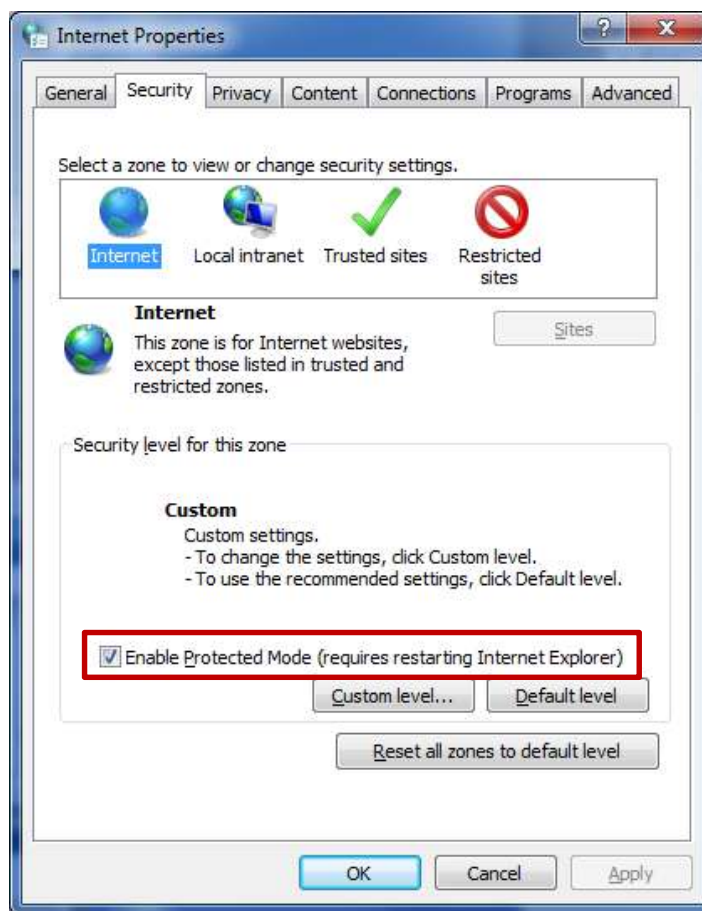




# Windows Operating System Artifacts

## Windows Vista/7 Low Folders

- Vista/7 에서 Internet Explorer은 기본적으로 보호 모드(protected mode)로 실행
- 보호 모드는 악의적인 공격으로부터 보호를 위해 Internet Explorer 프로세스를 매우 제한적인 권한으로 실행





# Windows Operating System Artifacts

## Windows Vista/7 Low Folders

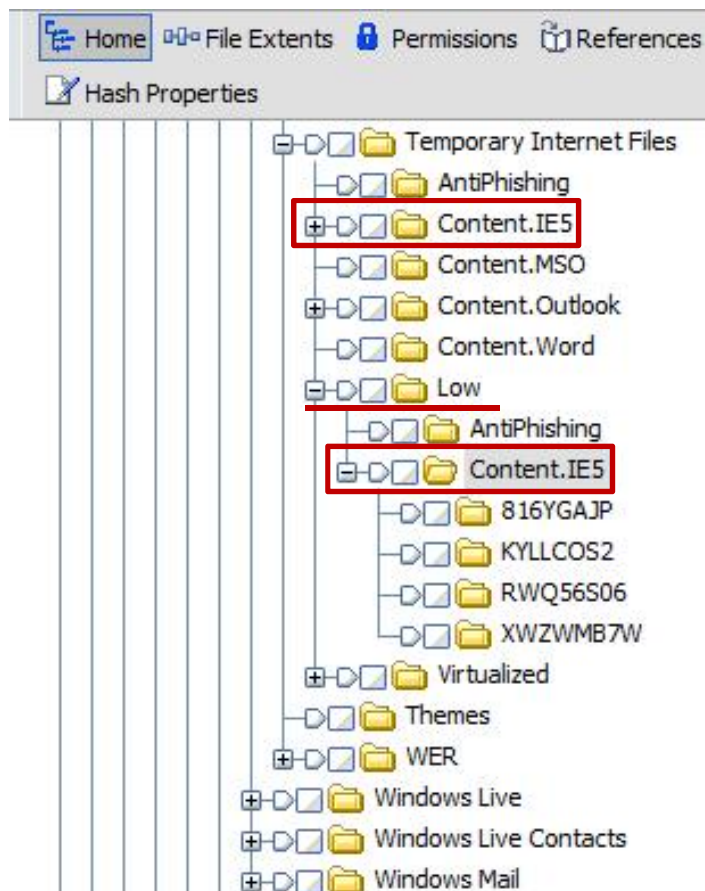
- 보호 모드에서 동작하는 Internet Explorer → Low Integrity Process
- Low Integrity Process는 사용자 프로필, 시스템 파일, 레지스트리에 쓰기 권한이 제한
- 단, Low Integrity Mandatory Label로 정해진 폴더, 파일, 레지스트리 키에만 쓰기 가능
- 결국, 보호 모드에서 동작하는 Internet Explorer 프로세스가 쓰기 위한 별도의 공간을 할당  
→ Low 폴더
- Low 폴더는 쿠키, 히스토리, 임시인터넷 파일 폴더의 하위 폴더로 존재



# Windows Operating System Artifacts

## Windows Vista/7 Low Folders

- 임시 인터넷 파일 폴더의 Low 폴더 → 두 개의 임시 인터넷 파일 경로가 존재



# Windows Operating System Artifacts

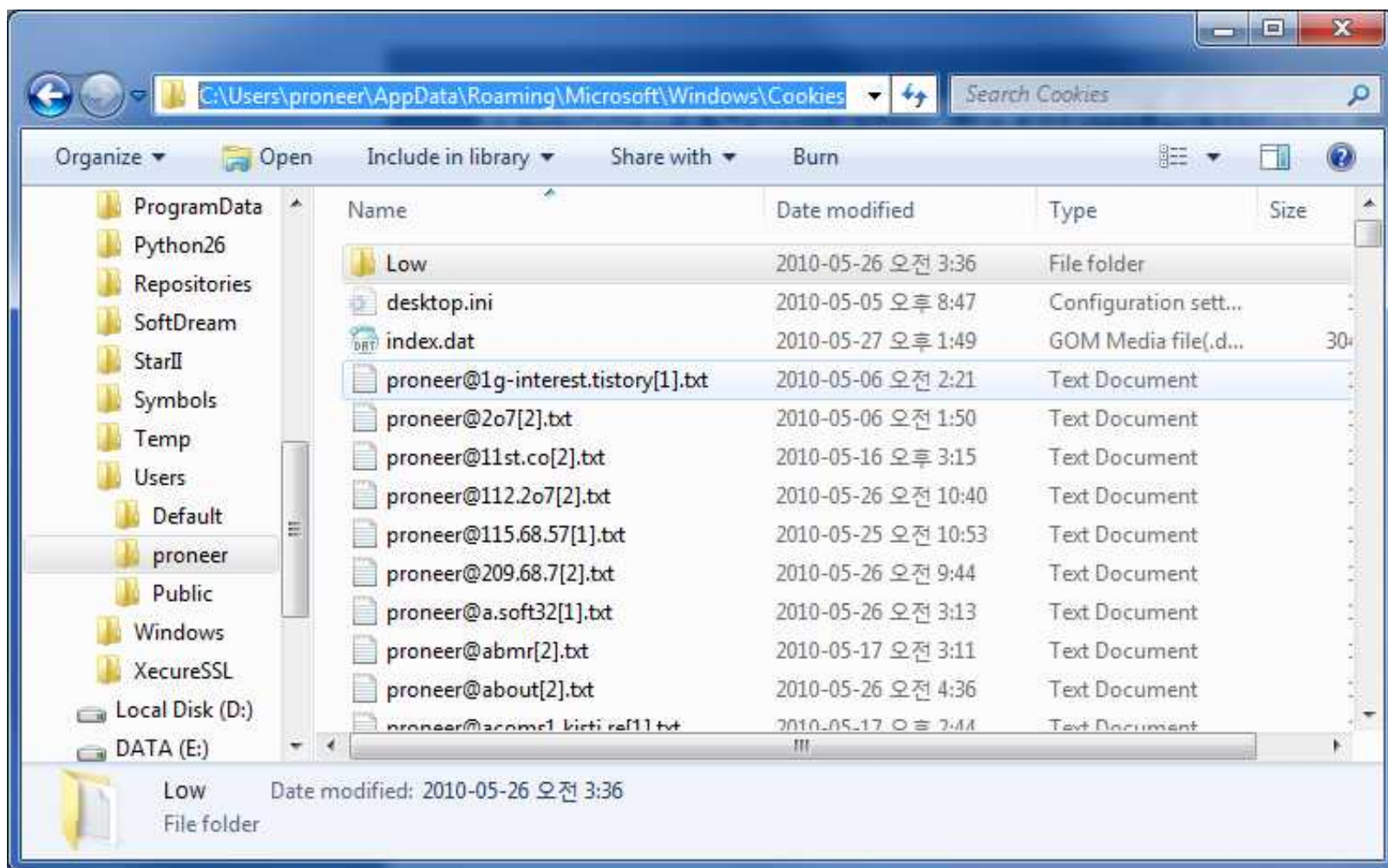
## Cookies Folder

- [2000/XP] : Documents and Settings\user name\Cookies\
- [Vista/7] : \Users\user name\AppData\Roaming\Microsoft\Windows\Cookies\
- 웹 사이트 방문 시 로컬 컴퓨터에 생성되는 정보
- 쿠키 이름 : *user\_name@domain\_name.txt*
- 폴더의 쿠키 파일에 대한 인덱스 정보를 저장하는 index.dat 존재
- index.dat 파일에는 쿠키 파일의 마지막 수정 시간과 만료 시간 저장



# Windows Operating System Artifacts

## Cookies Folder



# Windows Operating System Artifacts

## Cookies Folder

```
000PREF
005ID=813e73491332f368:TM=1256208169:LM=125
0456208169:S=H9m5q8oQiSgEqI0k
072google.com/
0841024
0891469160064
10030183591
1091697164960
12030036740
129*
```

Cookie name

Cookie value

Host/path for the web server

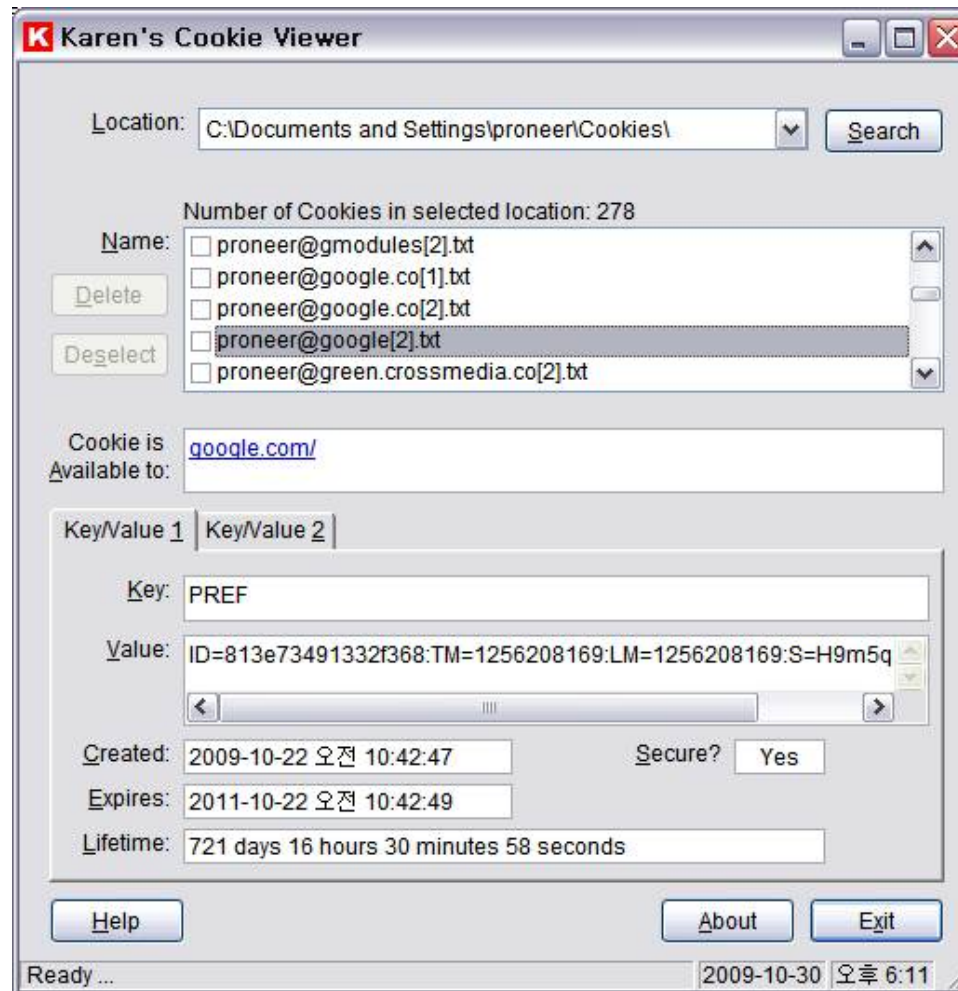
Expiration time (low)

Expiration time (high)

Creation time (low)

Creation time (high)

Record delimiter (\*)

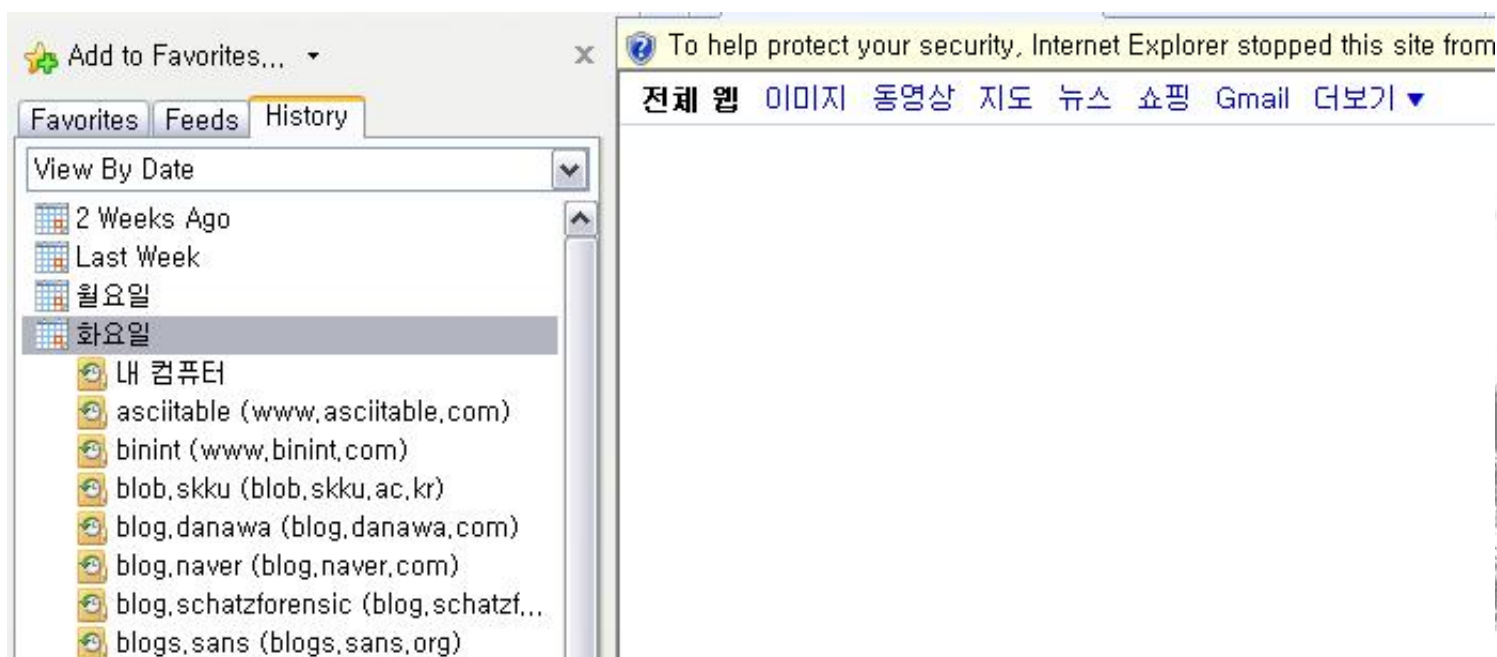




# Windows Operating System Artifacts

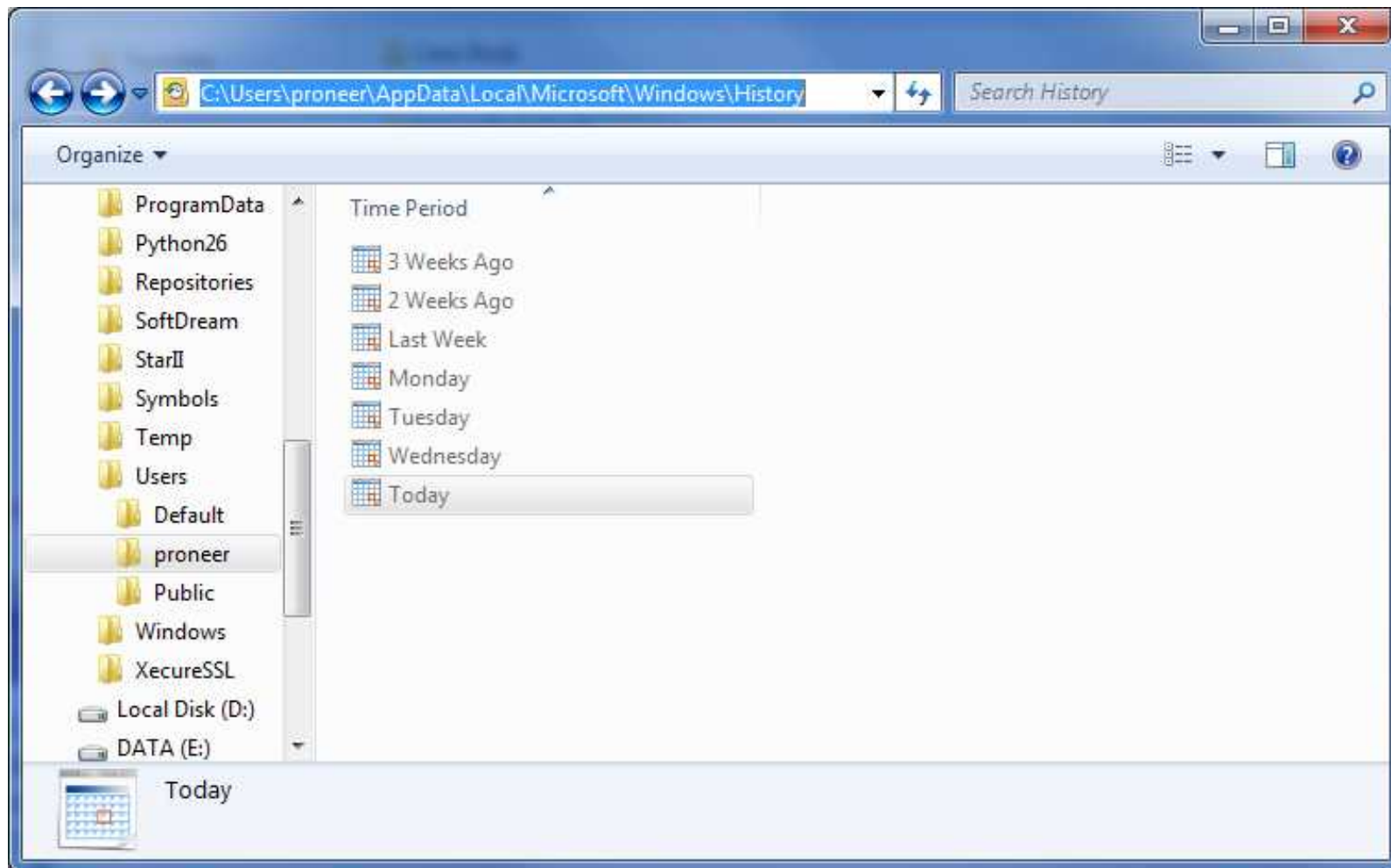
## History Folder

- [2000/XP] : Documents and Settings\W[user name]\W Local Settings\History\W
- [Vista/7] : :\WUsers\W[user name]\WAppData\Local\WMicrosoft\Windows\History\W
- Internet Explorer를 통한 웹 사이트 방문에 대한 기록



# Windows Operating System Artifacts

## History Folder



# Windows Operating System Artifacts

## History Folder

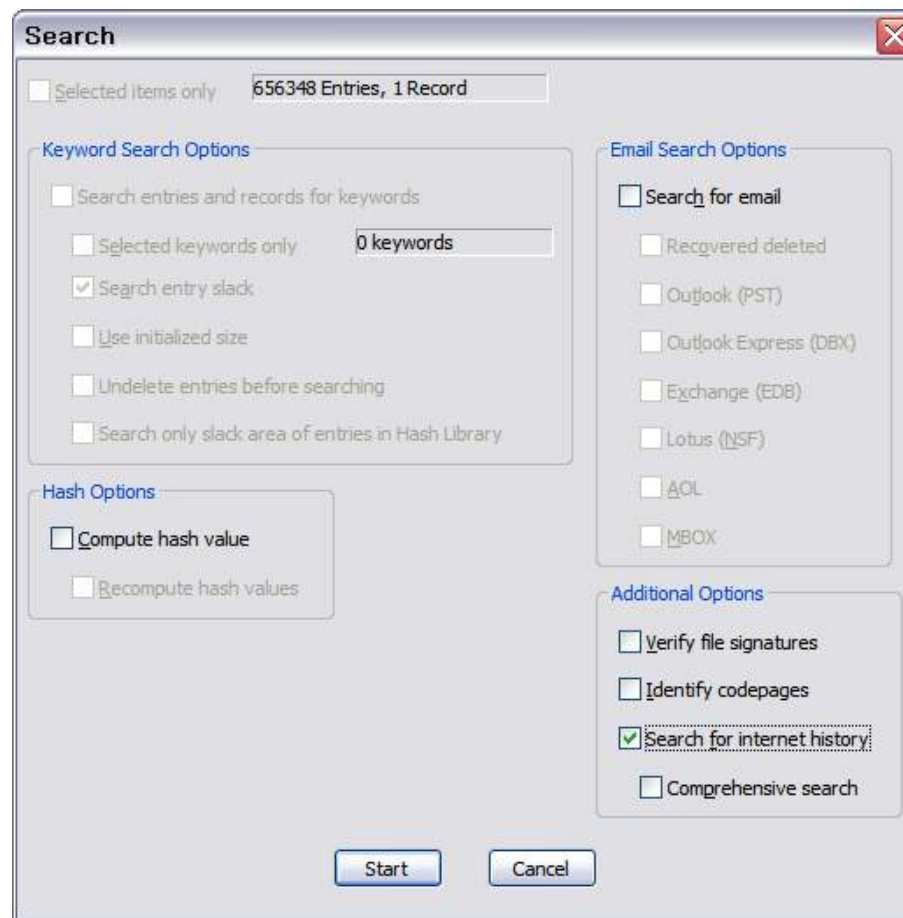
|                             | Name                     | Last Accessed       | File Created        | Last Written        | Entry Modified      |
|-----------------------------|--------------------------|---------------------|---------------------|---------------------|---------------------|
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> 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 |
| <input type="checkbox"/> 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            |

# Windows Operating System Artifacts

## History Folder

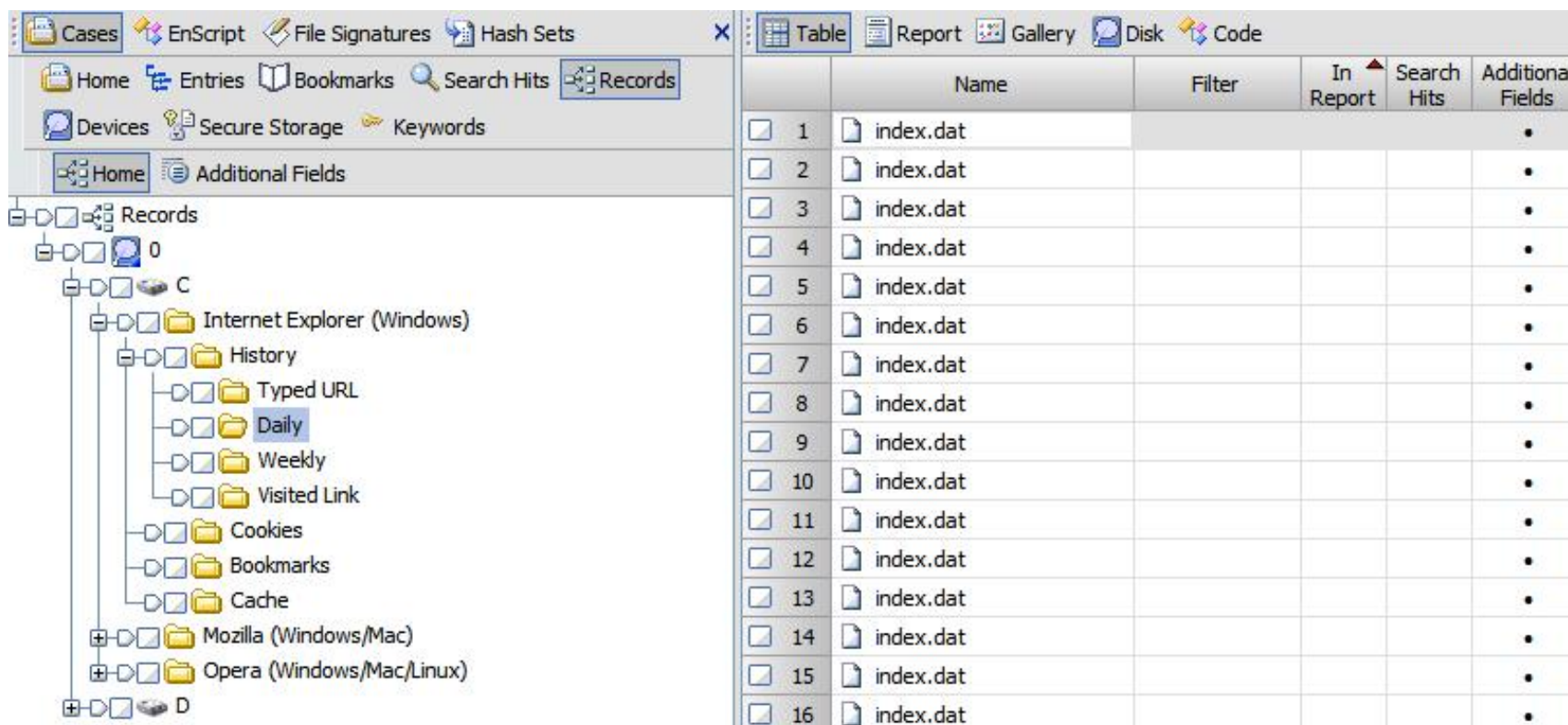
- EnCase에서는 인터넷 히스토리에 대한 자동 검색 기능 존재



# Windows Operating System Artifacts

## History Folder

- 인터넷 히스토리 검색 후 Records 탭에서 검색 결과 확인



The screenshot displays a forensic analysis tool interface. The top menu bar includes 'Cases', 'EnScript', 'File Signatures', 'Hash Sets', 'Table', 'Report', 'Gallery', 'Disk', and 'Code'. Below this, a sub-menu bar shows 'Home', 'Entries', 'Bookmarks', 'Search Hits', and 'Records' (which is selected). Further down, there are icons for 'Devices', 'Secure Storage', and 'Keywords'. The left sidebar shows a tree view of the file system, with 'Records' expanded to show '0' and 'C'. Under 'C', 'Internet Explorer (Windows)' is expanded, showing 'History', 'Typed URL', 'Daily' (selected), 'Weekly', 'Visited Link', 'Cookies', 'Bookmarks', and 'Cache'. Below these are 'Mozilla (Windows/Mac)' and 'Opera (Windows/Mac/Linux)'. The main pane on the right shows a table of search results.

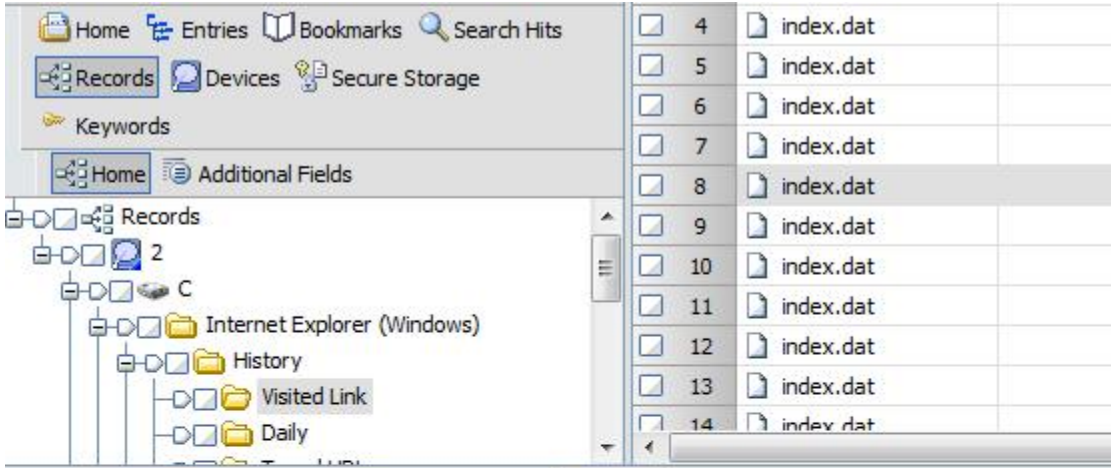
|                             | Name      | Filter | In Report | Search Hits | Additional Fields |
|-----------------------------|-----------|--------|-----------|-------------|-------------------|
| <input type="checkbox"/> 1  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 2  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 3  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 4  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 5  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 6  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 7  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 8  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 9  | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 10 | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 11 | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 12 | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 13 | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 14 | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 15 | index.dat |        |           |             | •                 |
| <input type="checkbox"/> 16 | index.dat |        |           |             | •                 |



# Windows Operating System Artifacts

## History Folder

- Report를 통해 각 index.dat 아이템 확인



The screenshot shows a forensic tool interface. On the left, a file tree is expanded to show the path: Home > Records > 2 > C > Internet Explorer (Windows) > History > Visited Link. On the right, a list of 14 index.dat files is displayed, numbered 4 through 14. The file 'index.dat' at index 8 is highlighted.

| Index | File Name |
|-------|-----------|
| 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 |

At the bottom, the 'Report' tab is active, displaying the following details for the selected index.dat file:

| Field                  | Value                            |
|------------------------|----------------------------------|
| Name                   | index.dat                        |
| Additional Fields      | •                                |
| Message Size           | 256                              |
| Title                  | Kim Jinkook (pr0neer) on Twitter |
| Profile Name           | proneer                          |
| Url Name               | http://twitter.com/pr0neer       |
| Type                   | URL                              |
| Url Host               | twitter.com/                     |
| Expiration             | 03/14/10 02:31:22오후              |
| Visit Count            | 29                               |
| Last Accessed          | 02/16/10 11:38:30오후              |
| Internet Artifact Type | History\Visited Link             |
| Browser Type           | Internet Explorer (Windows)      |





# Windows Operating System Artifacts

## Temporary Internet Files

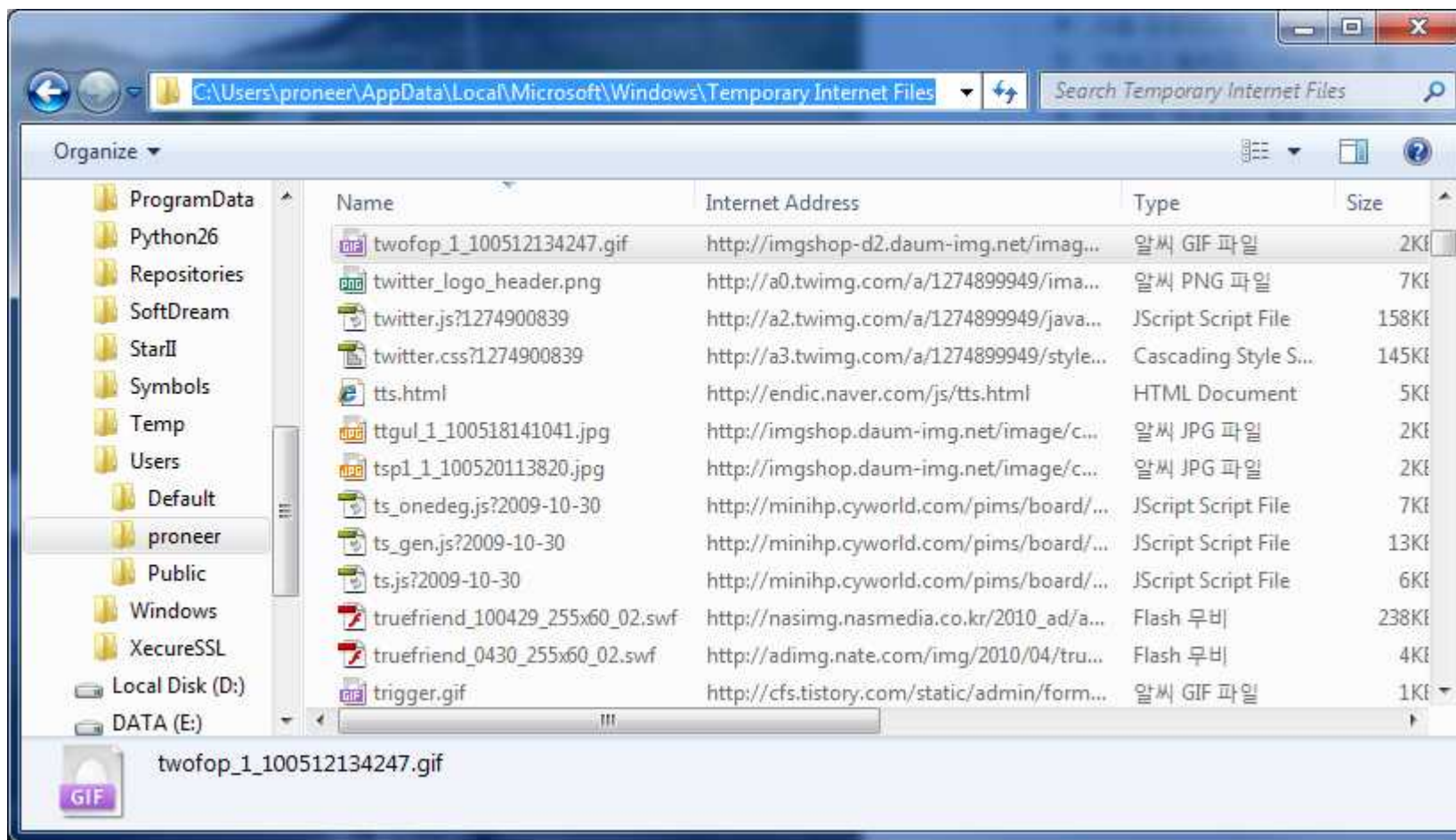
- [2000/XP] : Documents and Settings\user name\Local Settings\Temporary Internet Files\
- [Vista/7] : \Users\user name\AppData\Local\Microsoft\Windows\Temporary Internet Files\
- Temporary Internet Files 폴더에도 파일들에 대한 인덱스 파일 (index.dat) 파일 존재
- Temporary Internet Files 폴더 내용을 통해 방문 한 사이트 및 행위를 판단



# Windows Operating System Artifacts

## Temporary Internet Files

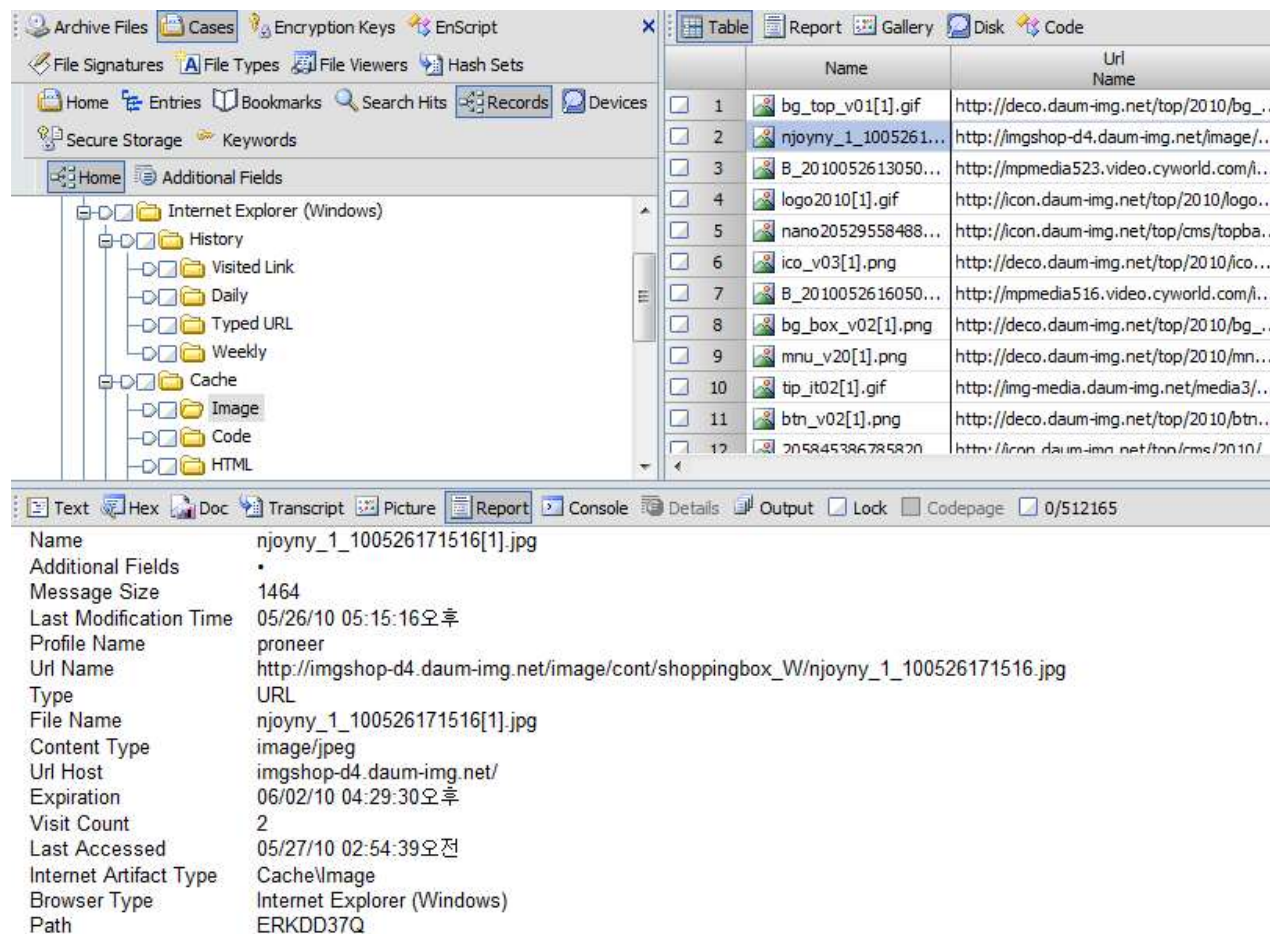
- Temporary Internet Files 폴더 확인



# Windows Operating System Artifacts

## Temporary Internet Files

- 검색된 웹 Cache 정보를 통한 Temporary Internet Files 파일 확인



The screenshot displays a forensic tool interface with a tree view on the left showing the 'Internet Explorer (Windows)' folder expanded to 'Cache'. The main pane shows a table of cache records. Below the table, a detailed view of a selected file is shown.

|    | Name                | Url Name                                  |
|----|---------------------|---|
| 1  | bg_top_v01[1].gif   | http://deco.daum-img.net/top/2010/bg_...  |
| 2  | njoyny_1_1005261... | http://imgshop-d4.daum-img.net/image/...  |
| 3  | B_2010052613050...  | http://mpmedia523.video.cyworld.com/i...  |
| 4  | logo2010[1].gif     | http://icon.daum-img.net/top/2010/logo... |
| 5  | nano20529558488...  | http://icon.daum-img.net/top/cms/topba... |
| 6  | ico_v03[1].png      | http://deco.daum-img.net/top/2010/ico...  |
| 7  | B_2010052616050...  | http://mpmedia516.video.cyworld.com/i...  |
| 8  | bg_box_v02[1].png   | http://deco.daum-img.net/top/2010/bg_...  |
| 9  | mnu_v20[1].png      | http://deco.daum-img.net/top/2010/mn...   |
| 10 | tip_it02[1].gif     | http://img-media.daum-img.net/media3/...  |
| 11 | btn_v02[1].png      | http://deco.daum-img.net/top/2010/btn...  |
| 12 | 205845386785820     | http://icon.daum-img.net/top/cms/2010/... |

|                        |   |
|------------------------|---|
| Name                   | njoyny_1_100526171516[1].jpg  |
| Additional Fields      | *   |
| Message Size           | 1464  |
| Last Modification Time | 05/26/10 05:15:16오후   |
| Profile Name           | proneer   |
| Url Name               | http://imgshop-d4.daum-img.net/image/cont/shoppingbox_W/njoyny_1_100526171516.jpg |
| Type                   | URL   |
| File Name              | njoyny_1_100526171516[1].jpg  |
| Content Type           | image/jpeg  |
| Url Host               | imgshop-d4.daum-img.net/  |
| Expiration             | 06/02/10 04:29:30오후   |
| Visit Count            | 2   |
| Last Accessed          | 05/27/10 02:54:39오전   |
| Internet Artifact Type | Cache\Image   |
| Browser Type           | Internet Explorer (Windows)   |
| Path                   | ERKDD37Q  |



# Windows Operating System Artifacts

## Swap File

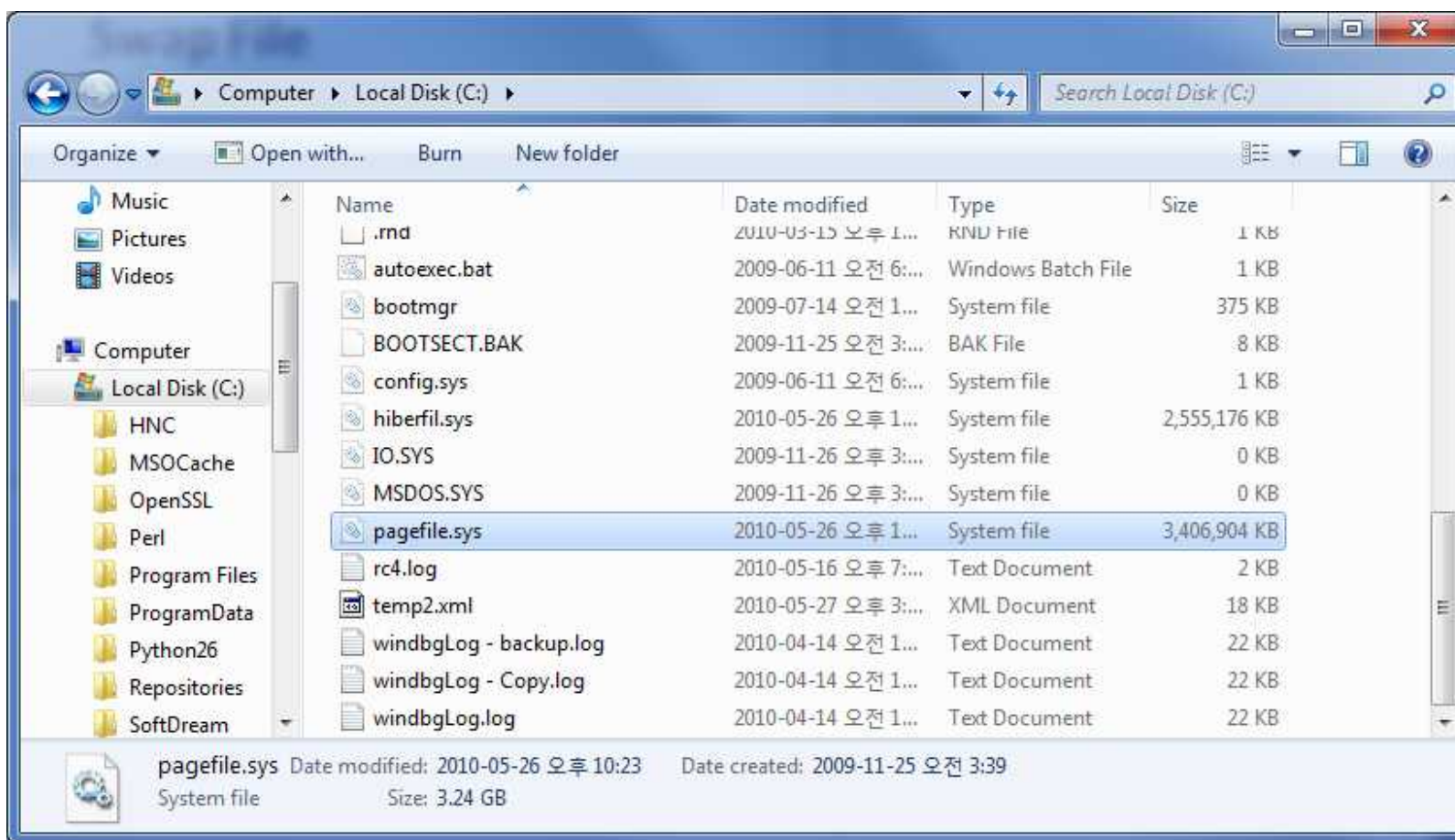
- 제한된 RAM 크기를 보완하기 위해 디스크의 일정 영역을 캐시처럼 사용
- 윈도우 운영체제의 스왑 파일은 "page file"
- 시스템의 운영체제 설치 드라이브 최상위 폴더에 위치
- RAM에서 스왑 아웃(swap out 또는 page out)된 데이터가 저장
- RAM에 쓰여졌던 데이터들이므로 매우 중요한(복호화 된 패스워드 등) 역할



# Windows Operating System Artifacts

## Swap File

- 시스템 드라이브 최상위에 위치하는 페이지 파일

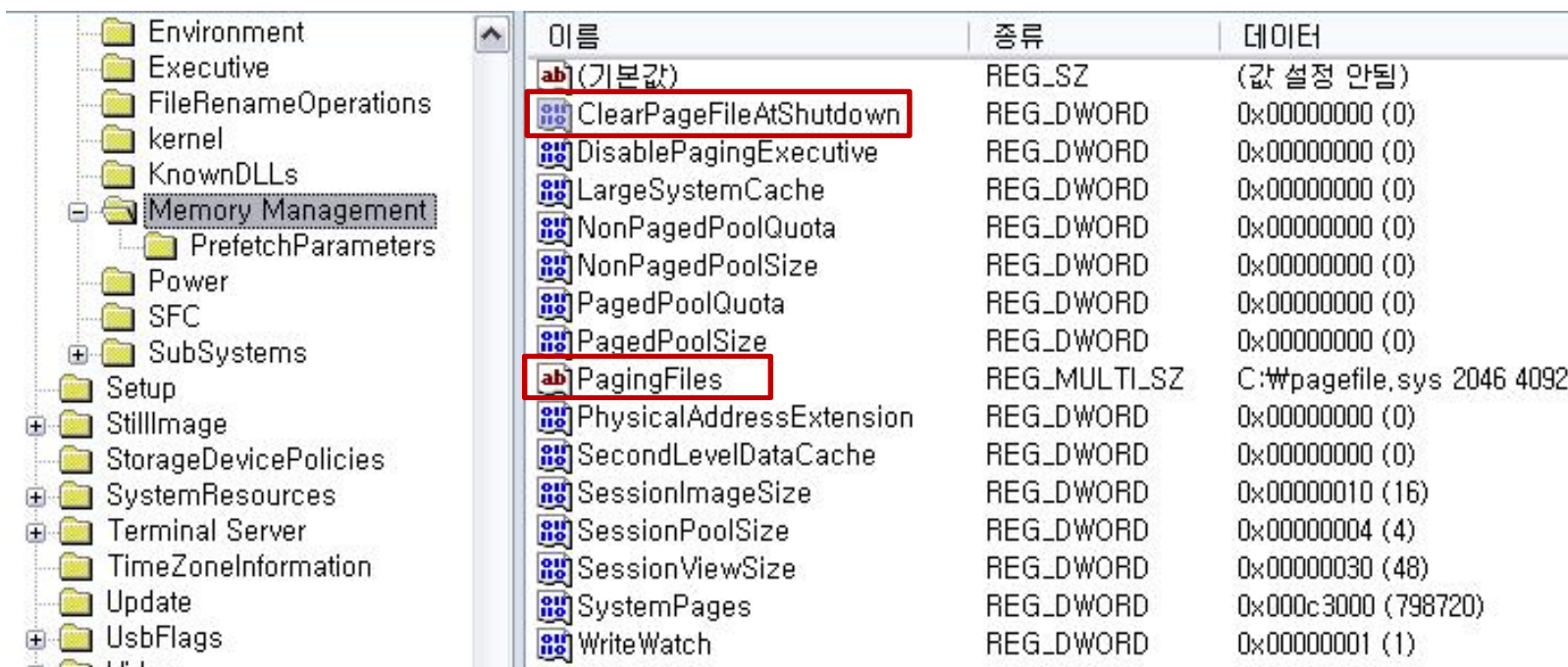




# Windows Operating System Artifacts

## Swap File

- HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
- 레지스트리 값을 통해 페이지파일의 위치를 변경시키거나 위치 확인 가능 (PagingFiles)
- 레지스트리 설정을 통해 시스템 종료 시 페이지파일 삭제 가능 (ClearPageFileAtShutdown)



| 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)            |

# Windows Operating System Artifacts

## Hibernation File

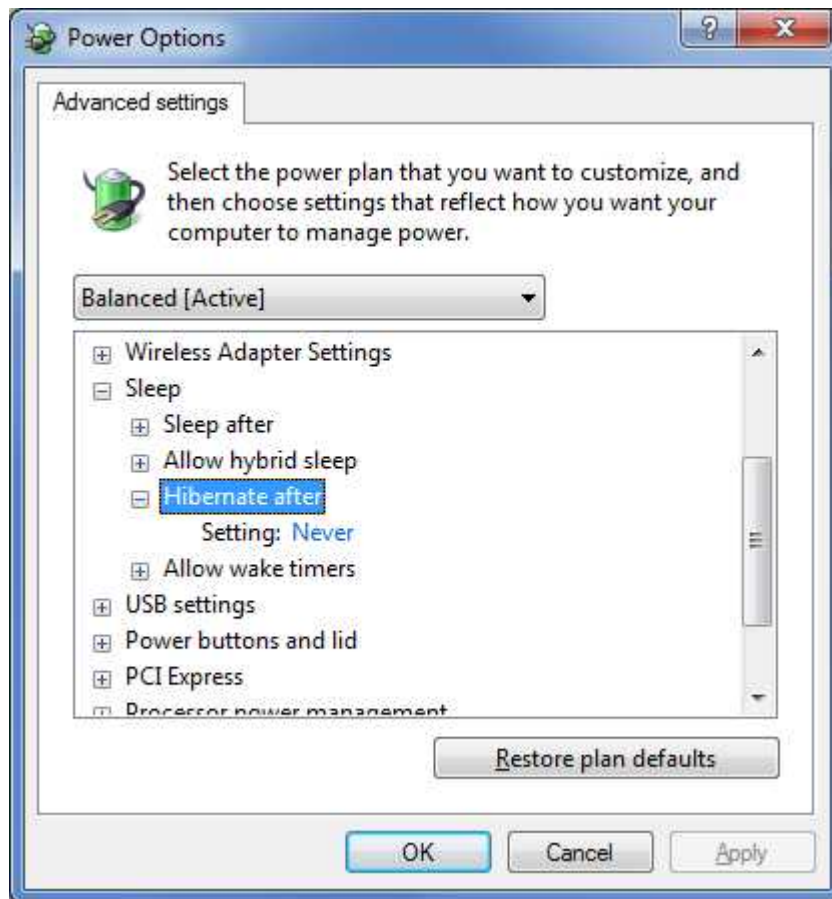
- 윈도우 2000/XP/Vista/7에서는 시스템에 "hibernate" 기능 설정 가능
- 노트북 제품에서는 기본적으로 설정 (절전을 위해)
- "hibernate" 기능 동작 시 시스템의 RAM을 파일로 저장 ➔ 최소한의 전력만 유지
- 기존 상태로 복귀 시 저장된 RAM 파일을 다시 메모리에 로드 ➔ 이전 상태로 변경



# Windows Operating System Artifacts

## Hibernation File

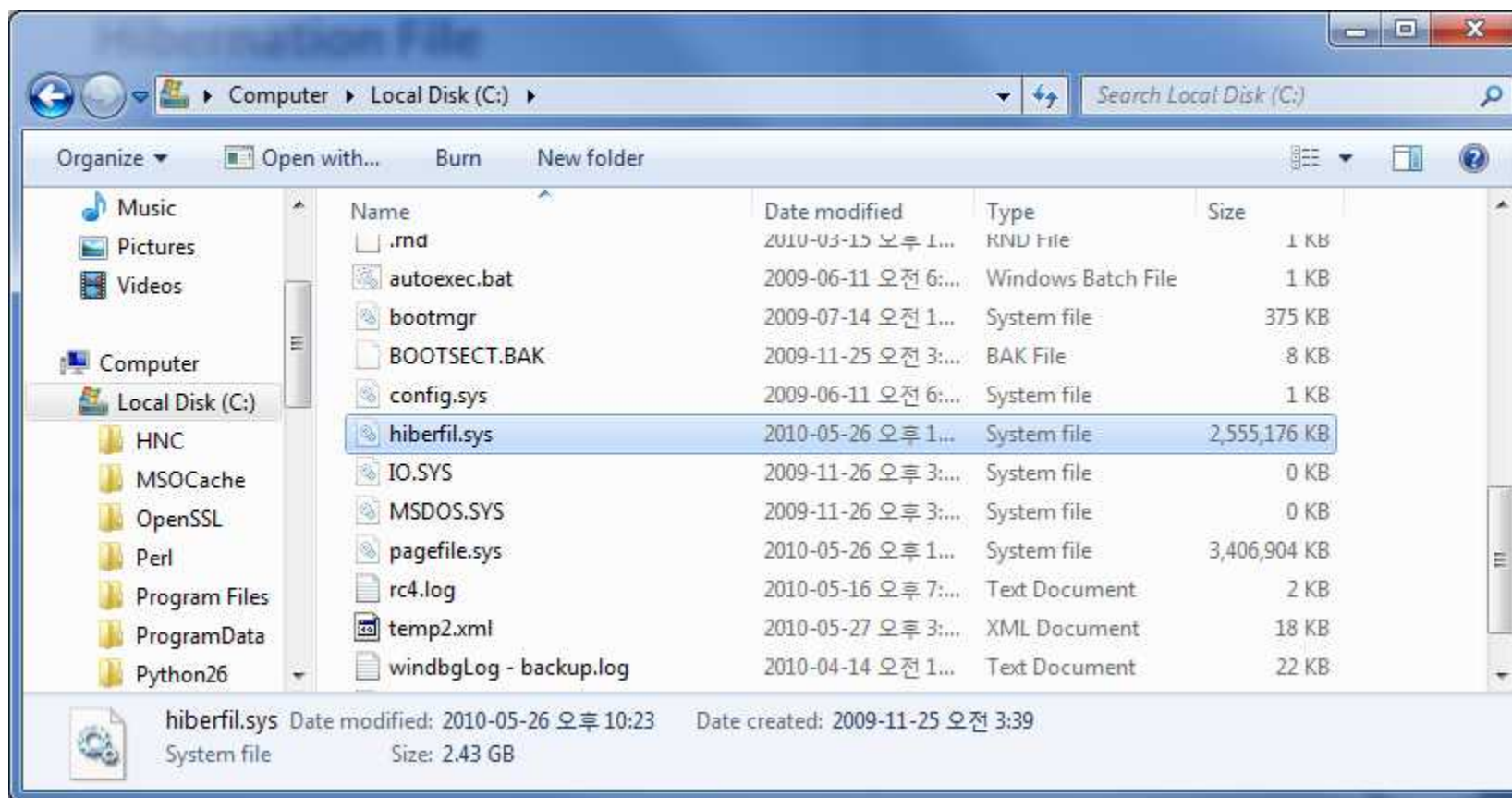
- 전원 옵션에서 "hibernate" 설정 가능



# Windows Operating System Artifacts

## Hibernation File

- 기본적으로 페이지 파일과 함께 시스템 루트 디렉터리에 위치



# Windows Operating System Artifacts

## Print Spooling

- 프린트 스푼링 작업은 프린트 하기 위한 문서의 복사본(스푼링 파일)을 가지고 백그라운드로 실행
- 대용량 파일을 프린트 시 잠시 대기하는 시간은 스푼링 파일을 생성하는 시간
- 작업 풀(Queue) 구조를 이용해 프린트 데이터를 프린터로 전송
- 프린트 작업이 모두 완료되면 스푼링 파일을 삭제
- 기본적으로 RAW, EMF 의 두가지 스푼링 모두가 존재 (대부분 기본적으로 EMF 모드 사용)
- RAW 모드
  - 프린트하고자 하는 데이터의 그래픽 덤프 파일을 스푼
- EMF 모드
  - 프린트하고자 하는 데이터를 EMF 파일로 변환한 후 스푼

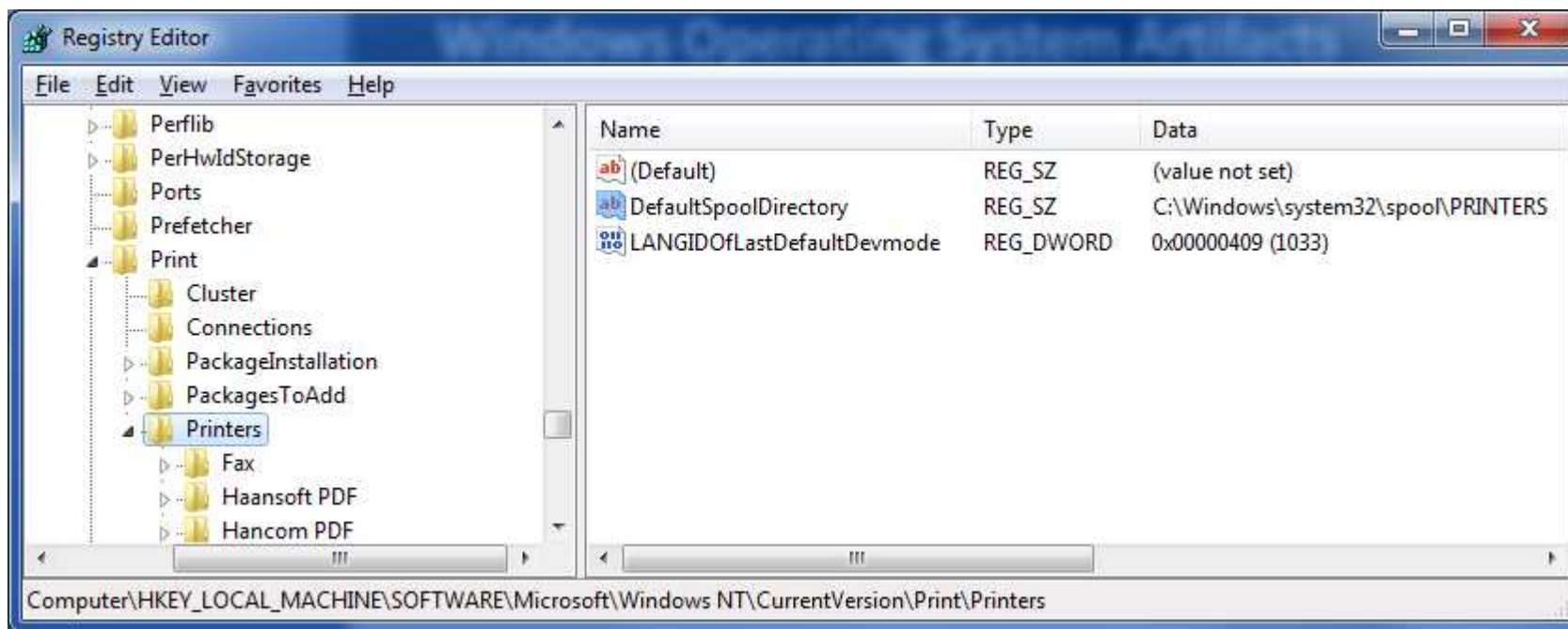




# Windows Operating System Artifacts

## Print Spooling

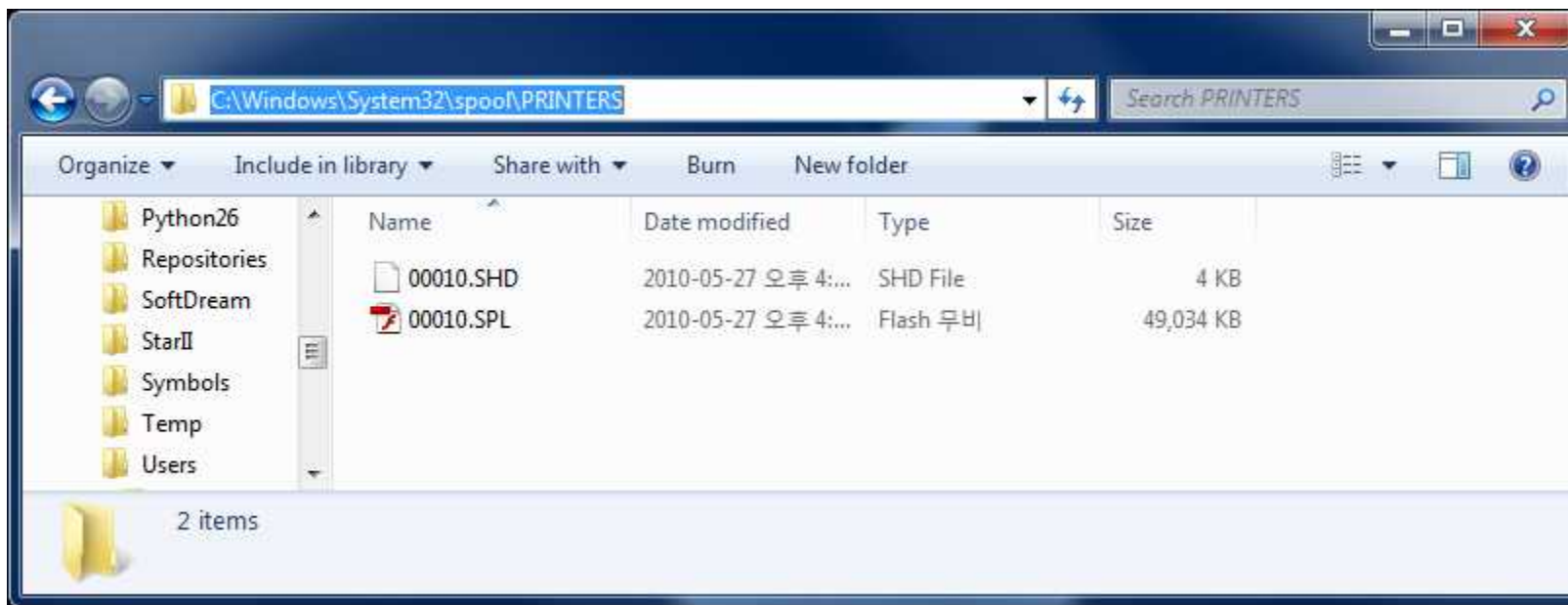
- [NT/2000] : Winnt\system32\spool\printers\
- [XP/2003/Vista/7] : Windows\system32\spool\printers\
- 레지스트리 값을 통해 기본 스푼 디렉터리 확인 가능
- HKLM\Software\Microsoft\Windows NT\CurrentVersion\Print\Printer\DefaultSpoolDirectory



# Windows Operating System Artifacts

## Print Spooling

- 프린트 스푼링 작업 시 기본적으로 두 개의 파일이 생성 (.SHD, .SPL)
- 파일명은 일반적으로 5개의 숫자로 표현



# Windows Operating System Artifacts

## Print Spooling

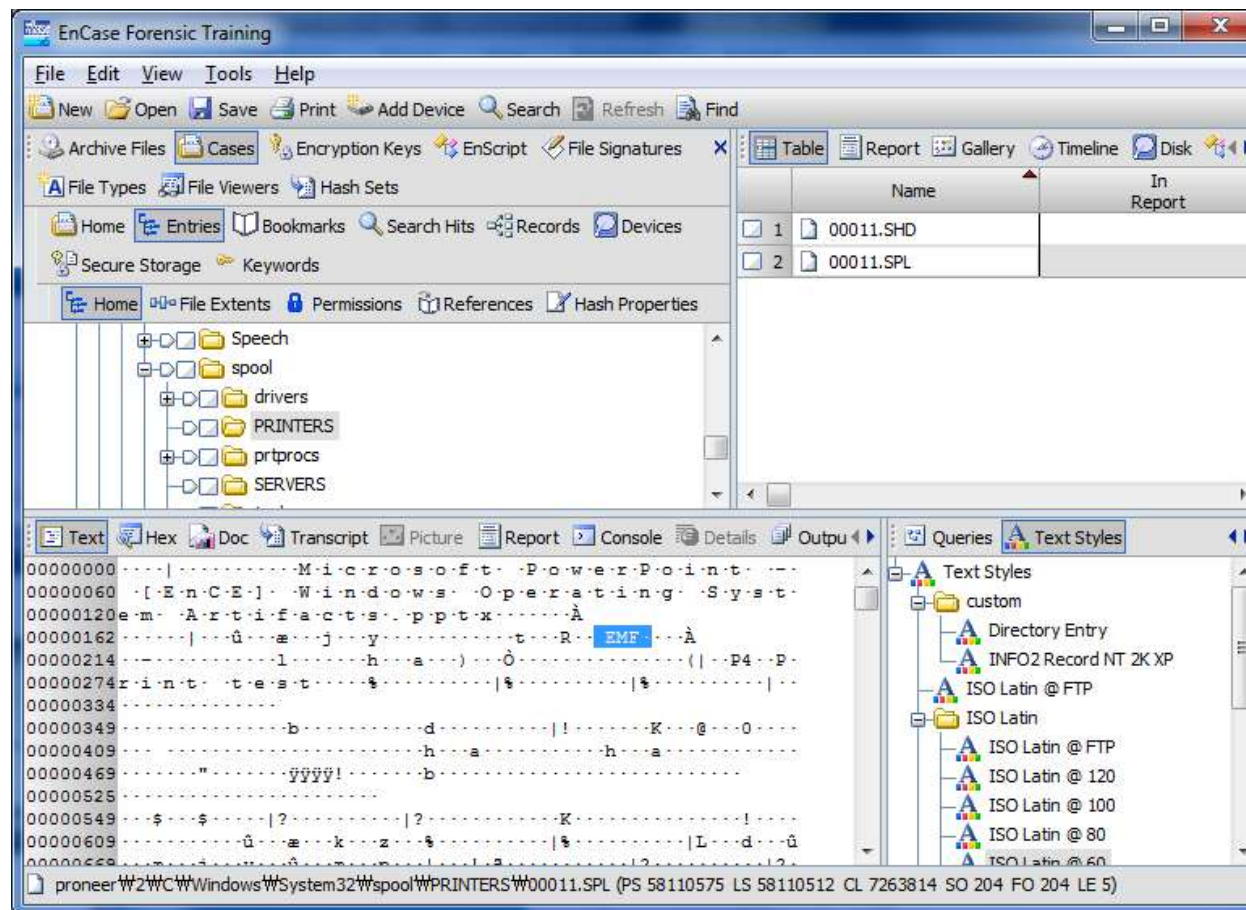
- SHD (Shadow) 파일
  - 프린트, 사용자, 파일, 프린트 모드 등의 기본적인 정보 저장
- SPL (Spool) 파일
  - RAW, EMF 모드에 맞게 프린트 하고자 하는 데이터의 변환된 파일



# Windows Operating System Artifacts

## Print Spooling

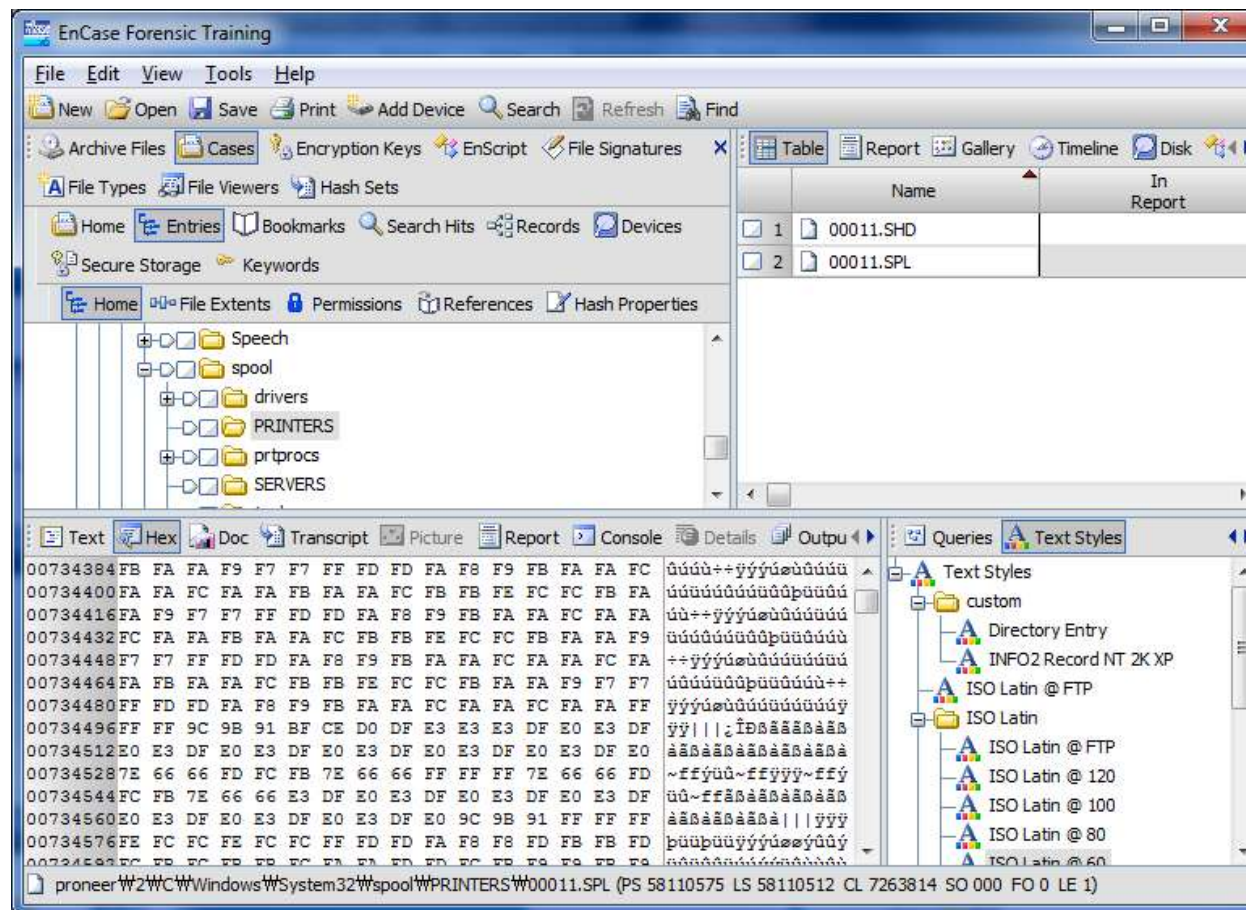
- EnCase를 통해 확인한 스푼 디렉터리와 SHD 파일 데이터



# Windows Operating System Artifacts

## Print Spooling

- EnCase를 통해 확인한 스푼 디렉터리와 SPL 파일 데이터





# Windows Operating System Artifacts

## Print Spooling – EMF Header for Different Versions of Windows

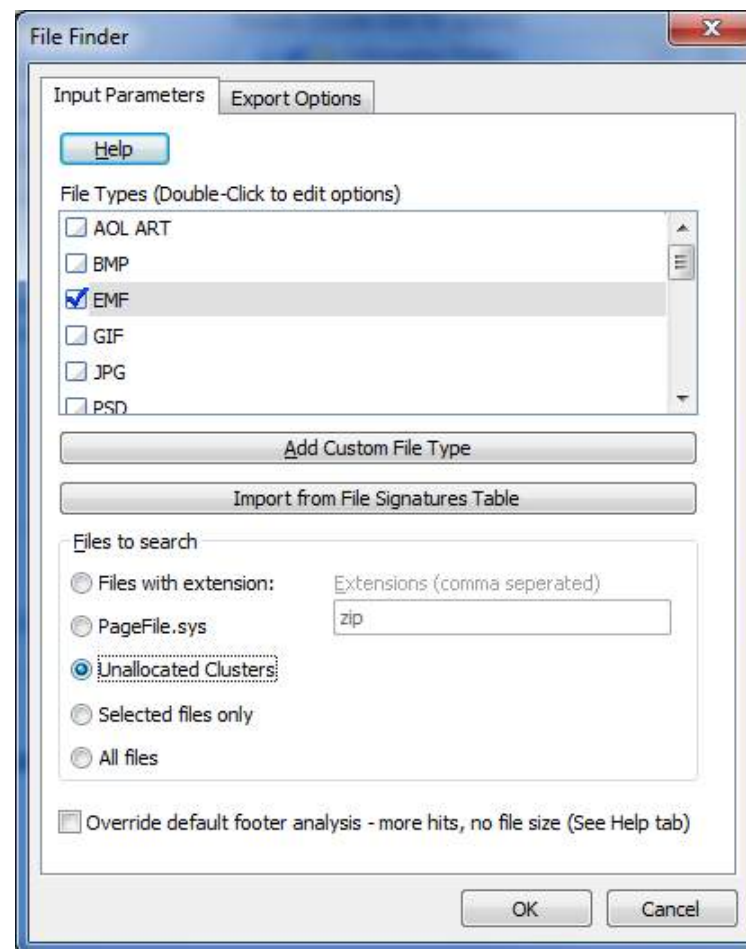
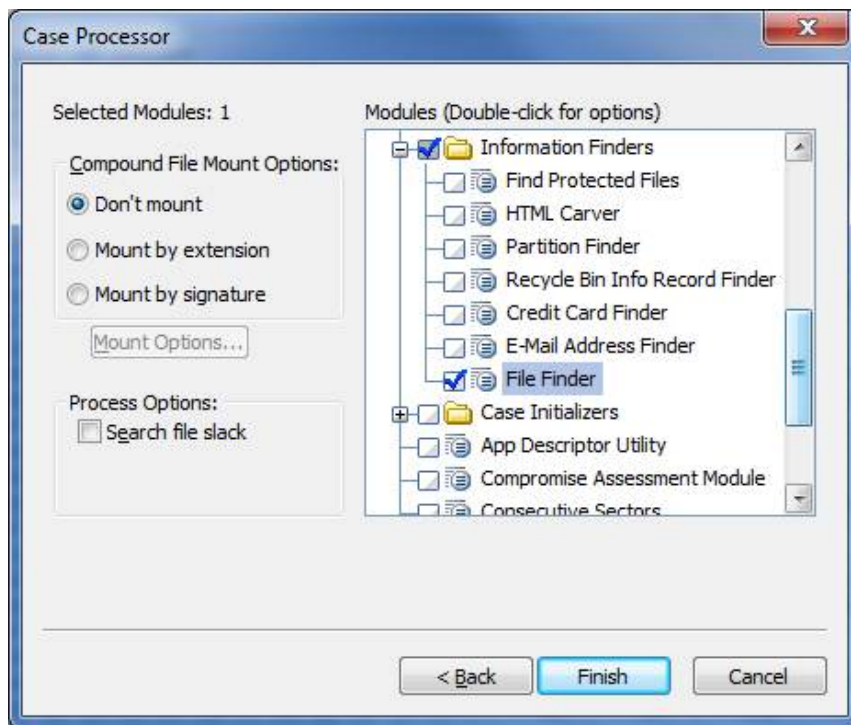
| Operating System                 | EMF Header (EnCase GREP Search Strings)  |
|----------------------------------|--|
| Windows XP                       | \x01\x00\x00\x00\x5C\x01\x01\x00\x00\x00\x84\x00                                     |
| Windows 9x upgraded to XP        | \x01\x00\x00\x00\x5C\x01\x01\x00\x00\x00\x84\x00<br>\x01\x00\x00\x00\x58\x00\x00\x00 |
| Windows 2000                     | \x01\x00\x00\x00\xD8\x17\x01\x00\x00\x00\x58\x6E                                     |
| Windows NT and 2000              | \x01\x00\x00\x00\x18\x17   |
| Windows 9*                       | \x01\x00\x00\x00\x58\x00   |
| Windows 2000, XP, 2003, Vista, 7 | \x01\x00\x00\x00..\ \x00.{34,34}EMF  |
| Universal Search String          | \x01\x00\x00\x00[\x5C\x84\xD8\x58\x18][\x01\x17\x6E\x00]                             |



# Windows Operating System Artifacts

## Print Spooling

- EnCase는 삭제된 EMF 파일을 찾기 위한 EnScript 지원



# Windows Operating System Artifacts

## Legacy Operating System Artifacts

- Windows 9x 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 Operating System Artifacts

## Windows Vista/7 Volume Shadow Copy

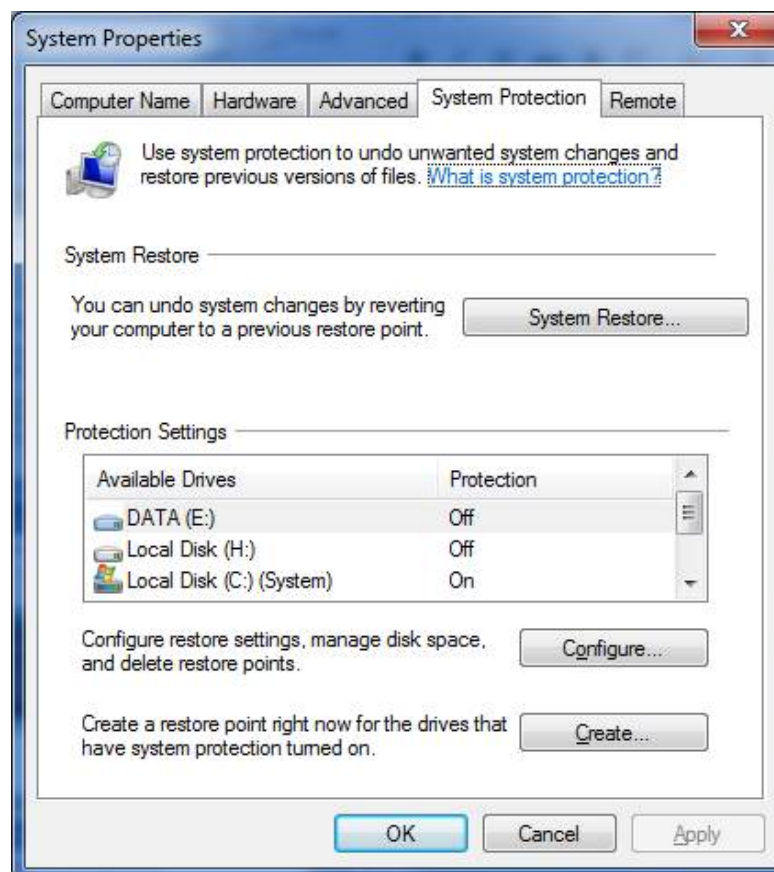
- 윈도우는 복원 지점을 스냅샷 된 시스템 복원
  - 스냅샷 저장 폴더
    - C:\System Volume Information\restore{GUID}\WRP### ( #는 복원지점 순서번호)
- 윈도우 XP, ME 에서는 복원 시점의 레지스트리 하이브, 중요한 파일 변경 사항을 기록 후 복원
- 윈도우 Vista/7 에서는 복원 지점이 Volume Shadow Copy(VSS)를 이용
- 단순한 시스템 변경 사항 기록이 아닌 시스템 백업 기능 추가
- 복원 지점은 복원 시점의 시스템 정보를 저장
- VSS의 경우 파일에 대한 백업 기능도 지원하므로 이전 파일 복구 가능
- 포렌식 조사를 위해서 현재 할당된 파일 정보 외에 복원 지점 정보를 고려해야 함



# Windows Operating System Artifacts

## Windows Vista/7 Volume Shadow Copy

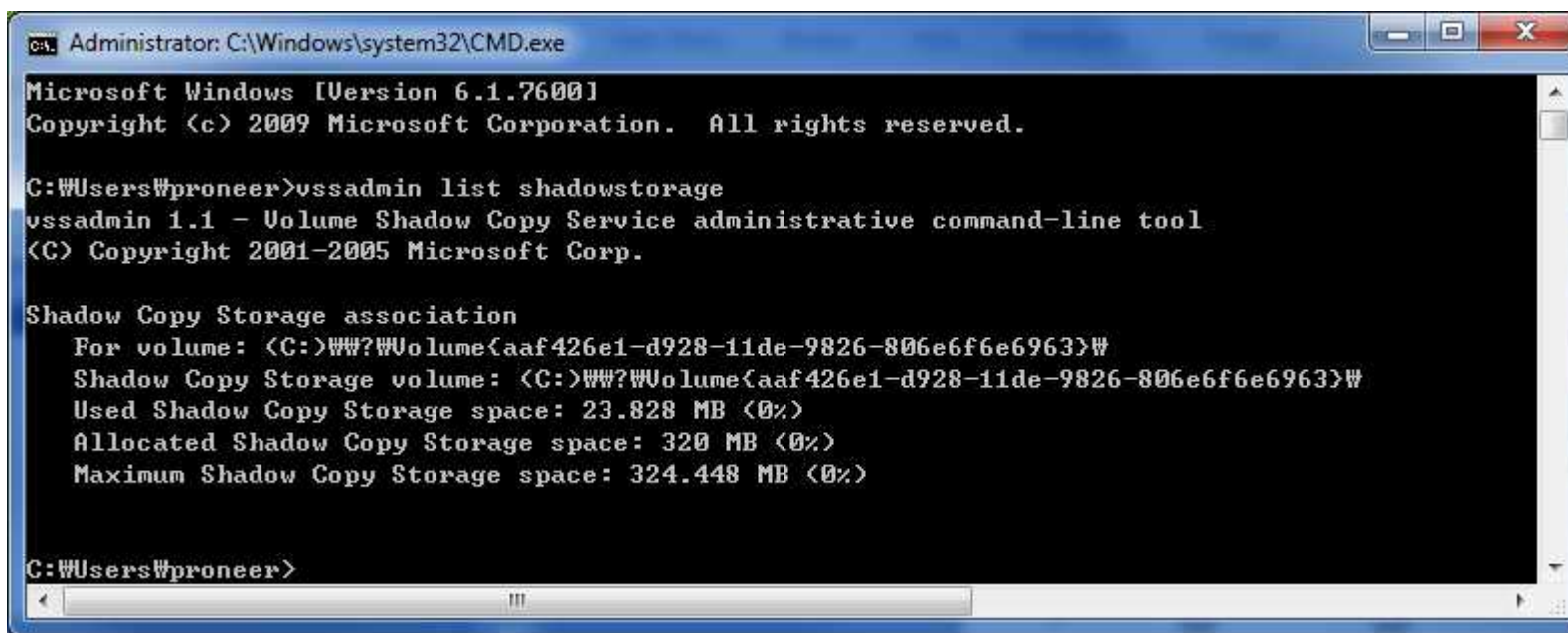
- 시스템 복원 지점 설정
- 내 컴퓨터 → 등록정보 → 시스템보호 탭을 이용해 설정 가능



# Windows Operating System Artifacts

## Windows Vista/7 Volume Shadow Copy

- 현재 시스템에서 사용하고 있는 VSS 정보 확인
- 명령 : vssadmin list shadowstorage



```
Administrator: C:\Windows\system32\CMD.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\proneer>vssadmin list shadowstorage
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line tool
(C) Copyright 2001-2005 Microsoft Corp.

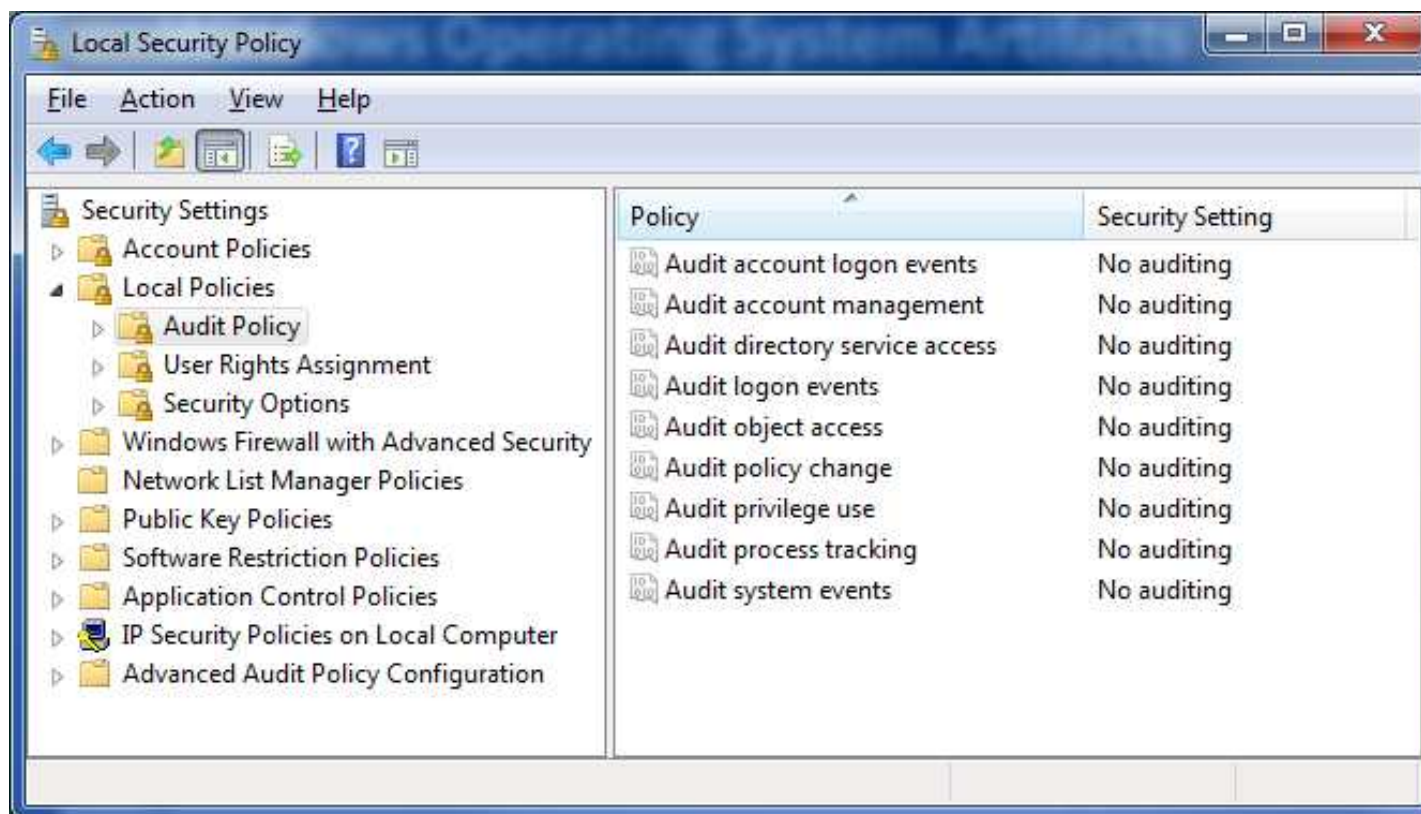
Shadow Copy Storage association
  For volume: (C:)\\?\\Volume{aaf426e1-d928-11de-9826-806e6f6e6963}\\
  Shadow Copy Storage volume: (C:)\\?\\Volume{aaf426e1-d928-11de-9826-806e6f6e6963}\\
  Used Shadow Copy Storage space: 23.828 MB (0%)
  Allocated Shadow Copy Storage space: 320 MB (0%)
  Maximum Shadow Copy Storage space: 324.448 MB (0%)

C:\Users\proneer>
```

# Windows Operating System Artifacts

## Windows Event Logs – Kinds of Information Available in Event Logs

- 윈도우에서 감사에 대한 설정은 기본적으로 "No auditing"
- 로컬 보안 정책에서 감사에 대한 설정을 할 경우 이벤트 로그가 기록됨





# Windows Operating System Artifacts

## Windows Event Logs – Windows 2000/XP Event Logs

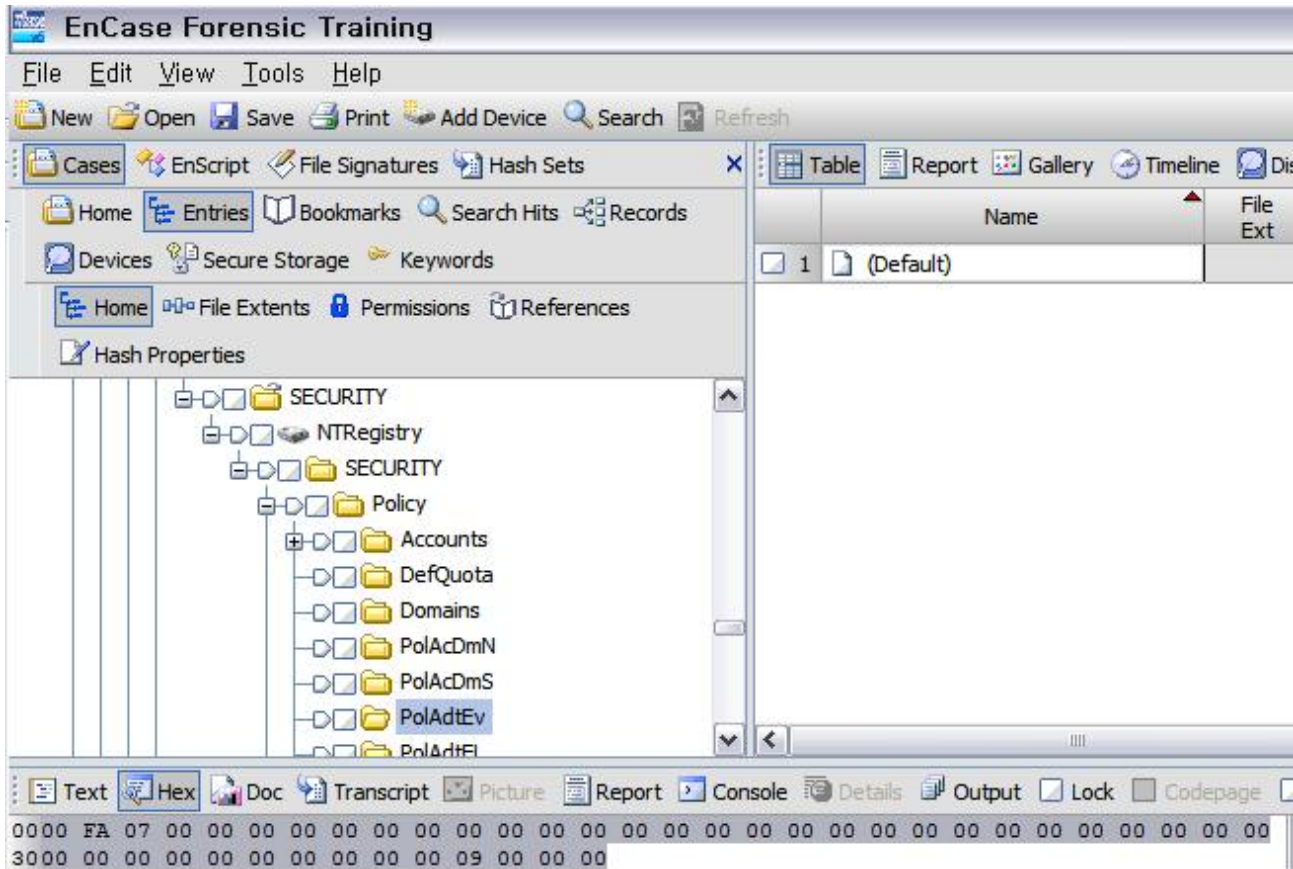
- [2000/XP] : C:\Windows\System32\config :
  - **secevent.evt** : 보안 로그
  - **sysevent.evt** : 시스템 로그
  - **apptevent.evt** : 응용프로그램 로그
- 이벤트 뷰어를 통해 이벤트 로그 확인



## Windows Operating System Artifacts

# Windows Event Logs – Determining Levels of Auditing

- 로컬 보안 정책의 감사에 대한 설정 값은 레지스트리에 저장
- HKEY\_LOCAL\_MACHINE\Security\Policy\PolAdtEv



# Windows Operating System Artifacts

## Windows Event Logs – Determining Levels of Auditing

- HKEY\_LOCAL\_MACHINE\Security\Policy\PolAdtEv 값의 의미

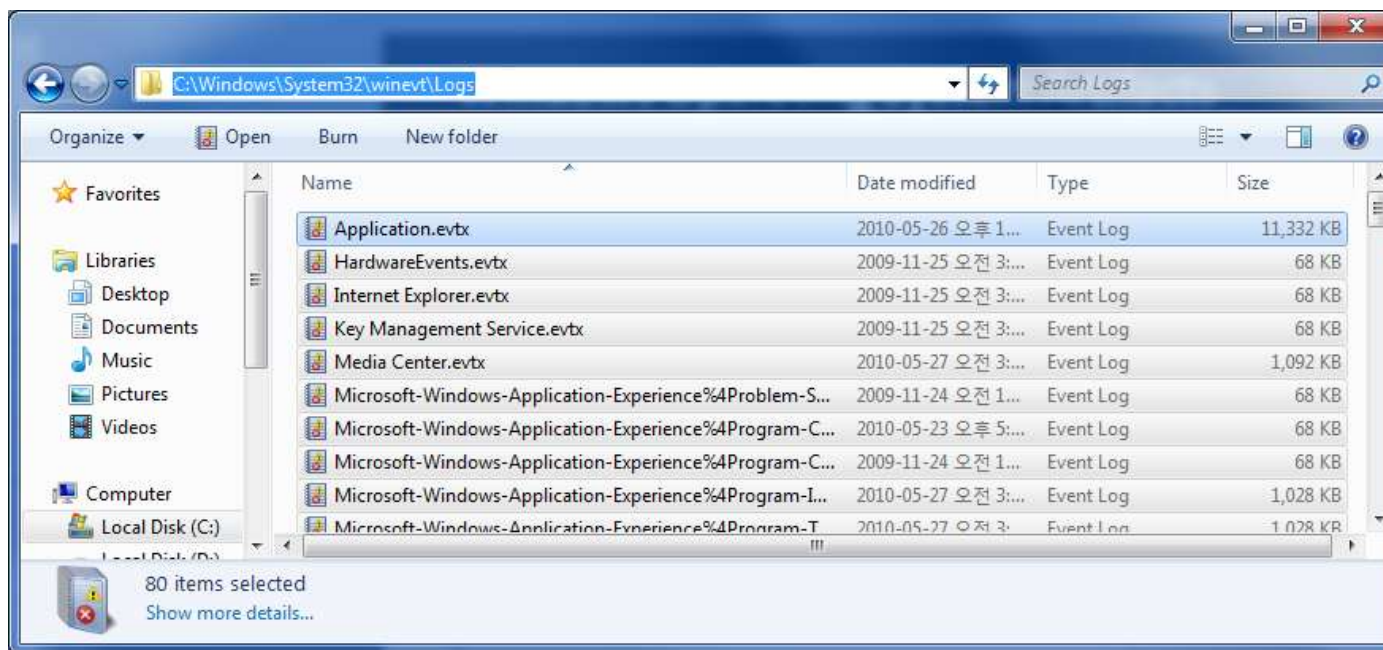
| Byte Offset | Audit Type                             |
|-------------|--|
| 00          | 00 No Auditing / 01 Auditing           |
| 04          | System Events Audit Setting            |
| 08          | Logon Events Audit Setting             |
| 12          | Object Access Audit Setting          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

| Byte Value | Audit Setting              |
|------------|----------------------------|
| 00         | No Auditing                |
| 01         | Audit Successes            |
| 02         | Audit Failures             |
| 03         | Audit Success and Failures |

# Windows Operating System Artifacts

## Windows Event Logs – Windows Vista/7 Event Logs

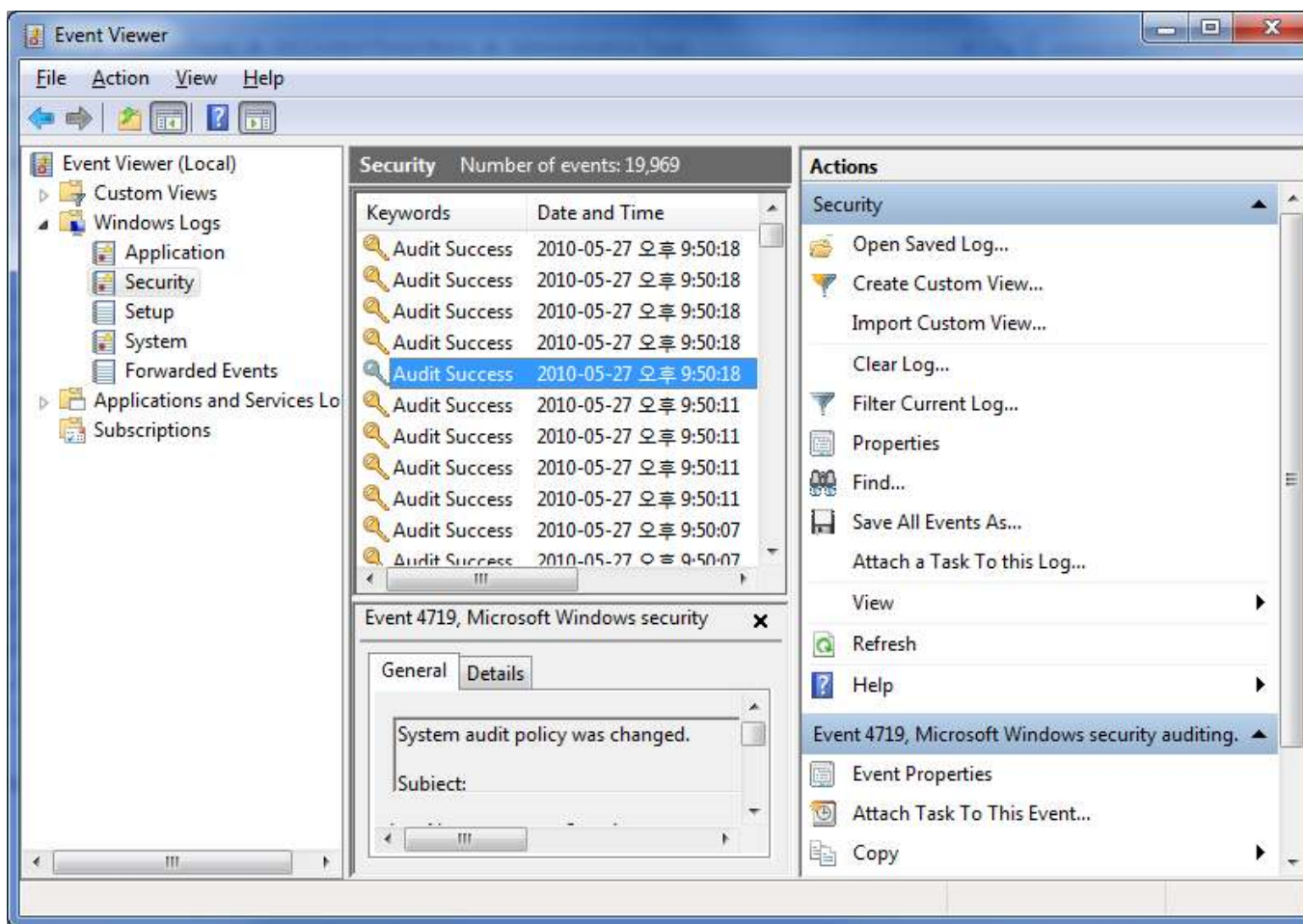
- [Vista/7] : C:\Windows\System32\winevt\Logs
  - **security.evtx** : 보안 로그
  - **system.evtx** : 시스템 로그
  - **application.evtx** : 응용프로그램 로그
- 기본적인 이벤트 로그 외에 확장된 이벤트 로그까지 포함하여 50개 이상의 이벤트 로그 저장



# Windows Operating System Artifacts

## Windows Event Logs – Windows Vista/7 Event Logs

- 윈도우 7 이벤트 뷰어

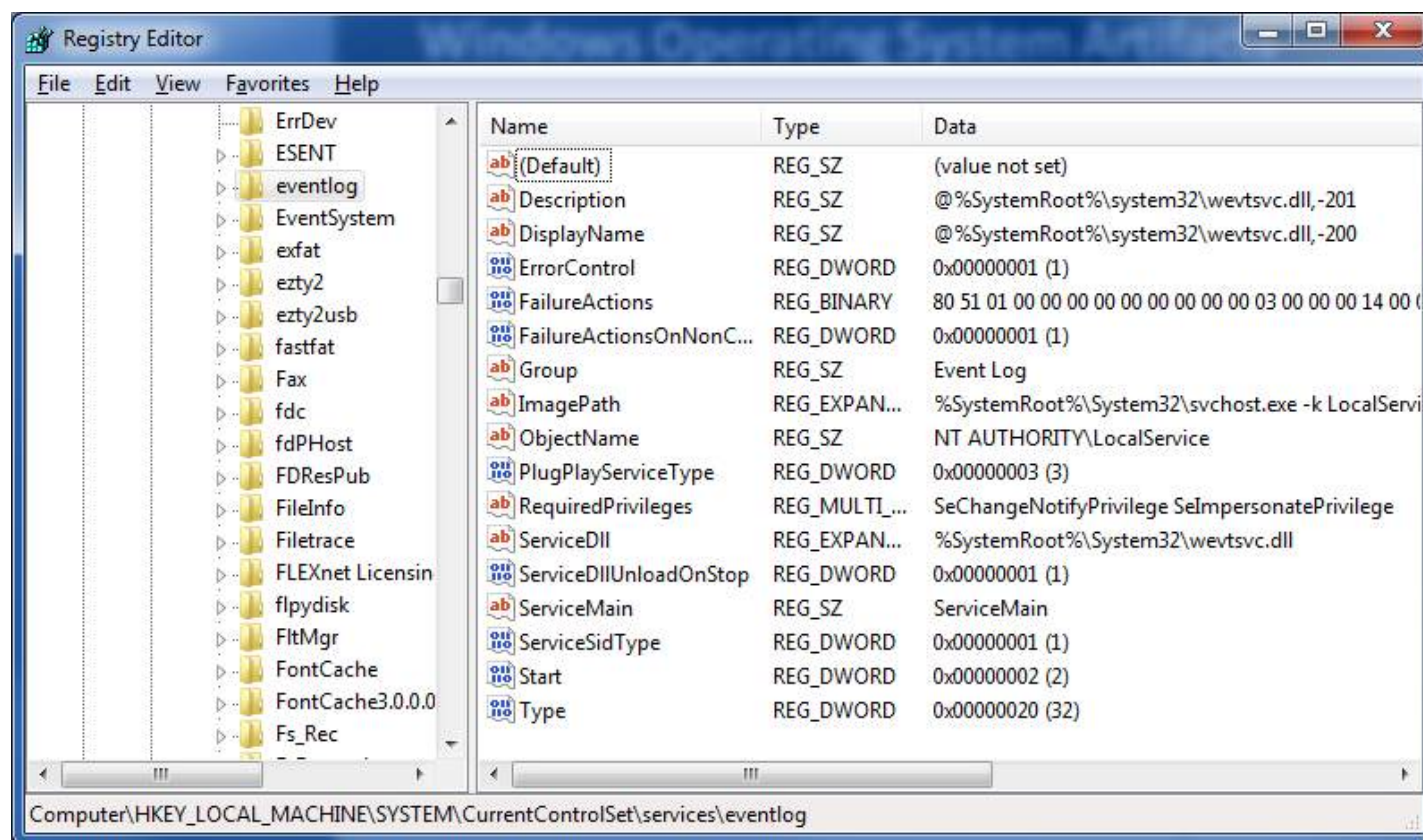




# Windows Operating System Artifacts

## Windows Event Logs – Using the Windows Event Log Parser

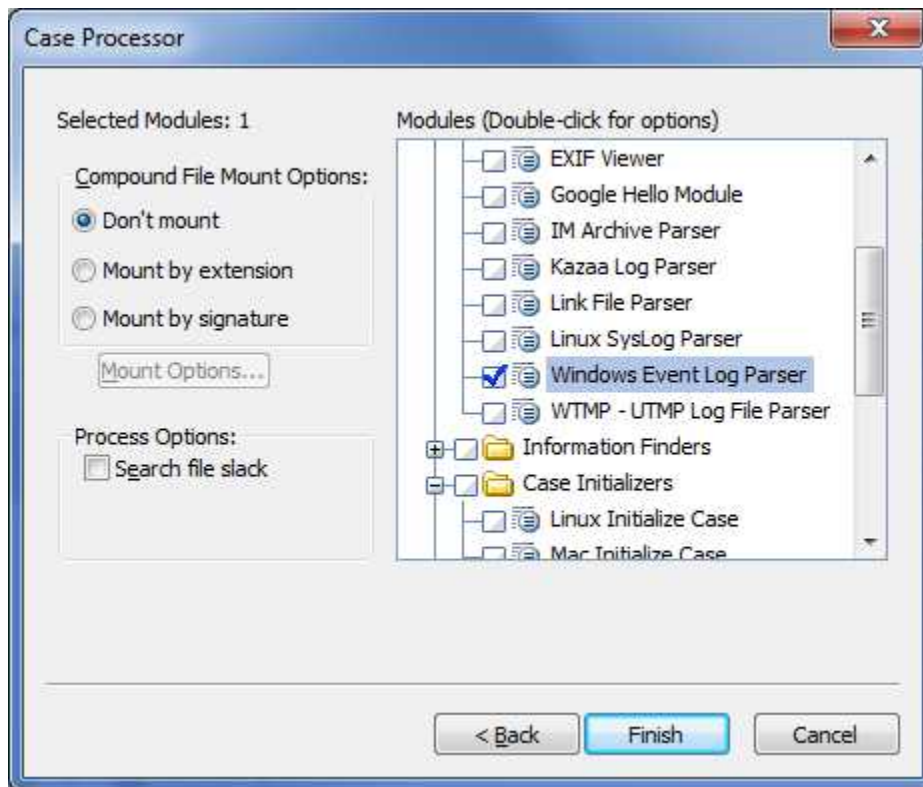
- EnCase 6.6 이후부터 Vista/7 이벤트 로그 파싱 가능
- HKLM\SYSTEM\CurrentControlSet\Services\Eventlog 경로의 DLL을 이용하여 결과 출력



# Windows Operating System Artifacts

## Windows Event Logs – Using the Windows Event Log Parser

- EnCase에서는 이벤트 로그에 대한 EnScript 파서를 제공



# Windows Operating System Artifacts

## Exercise 9.1 – Windows Artifacts Recovery

- ##



# Question & Answer

