

휴지통 포렌식



JK Kim

@pr0neer

forensic-proof.com

proneer@gmail.com

1. 휴지통
2. 휴지통 파일 구조
3. 휴지통 파일 카빙
4. 휴지통 파일 분석

휴지통

Security is a people problem...

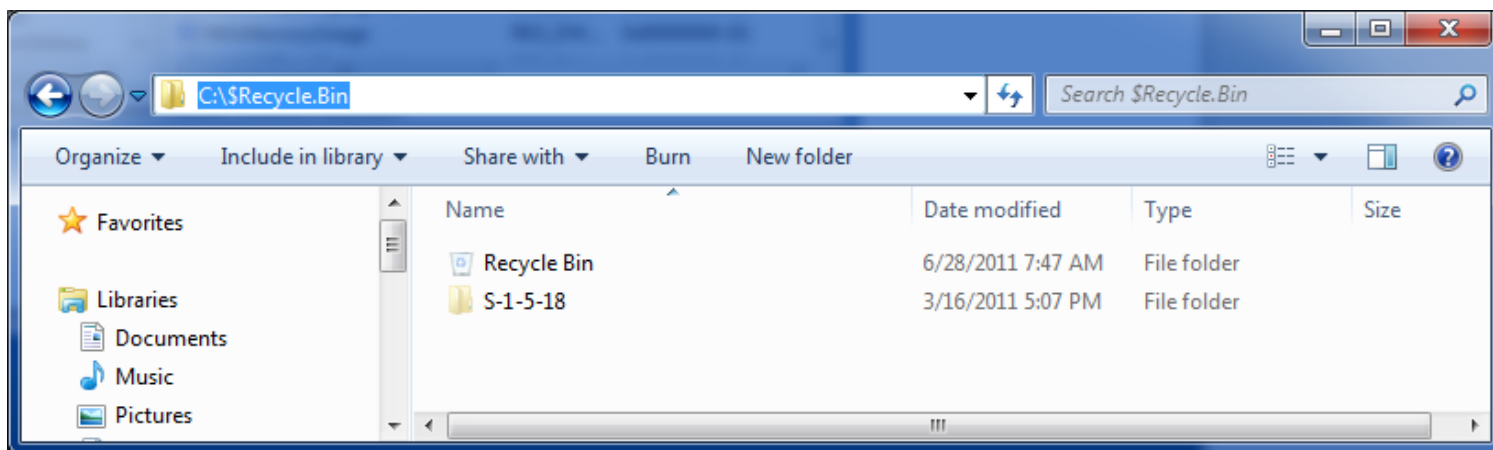
휴지통이란?

- 휴지통 소개

- 윈도우에서 파일을 삭제할 경우, 기본적으로 삭제된 파일은 휴지통(Recycle Bin) 영역으로 이동
- 휴지통 우회 방법
 - SHIFT 조합
 - 레지스트리 설정 → NukeOnDelete

2000/XP – HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket

Vista/7 – HKU\{USER}\Software\Microsoft\Windows\CurrentVersion\Explorer\Bitbucket\Volume\{GUID}



휴지통 폴더

- 운영체제 버전별 기본 폴더

운영체제	기본 파일 시스템	휴지통 폴더
윈도우 9x/ME	FAT32	<volume>\Recycled\
윈도우 NT/2K/XP	NTFS	<volume>\Recycler\<USER SID>\
윈도우 Vista/7	NTFS	<volume>\\$Recycle.Bin\<USER SID>\

- 볼륨마다 휴지통 폴더 존재

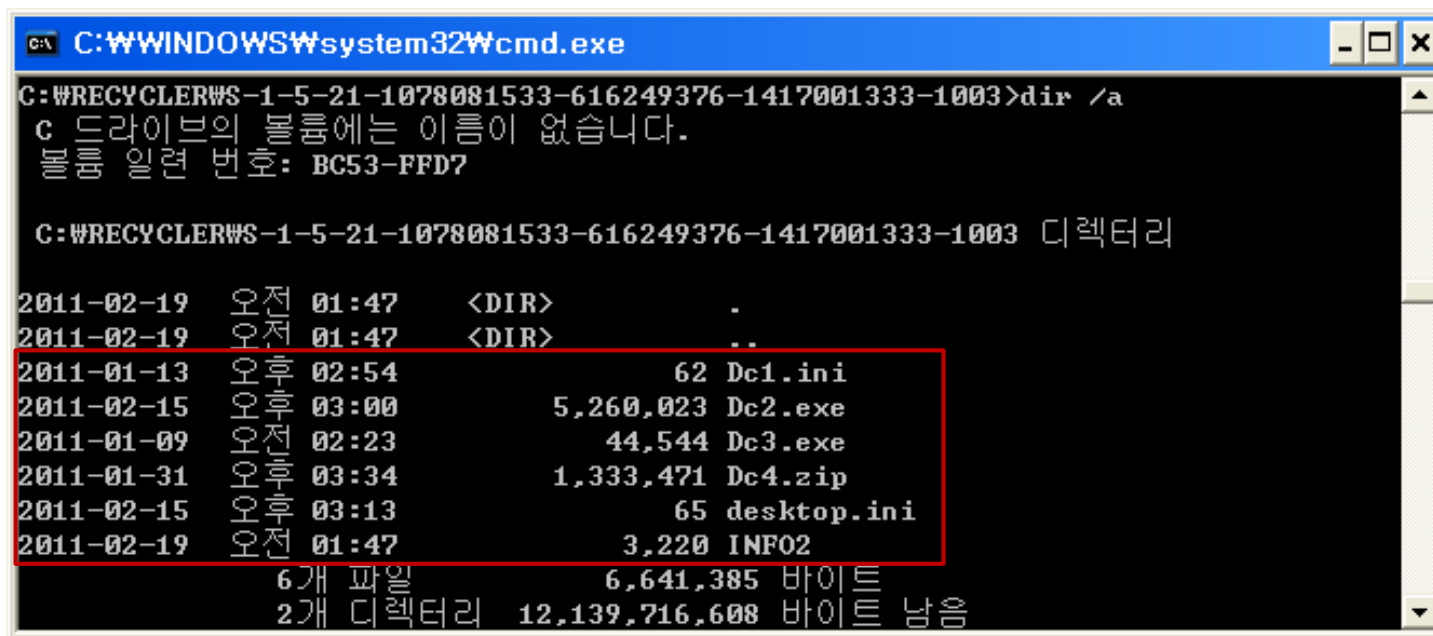
- 각 볼륨마다 독립된 휴지통 공간
- 특정 볼륨에서 지운 파일은 해당 볼륨의 휴지통으로 이동

- 사용자 SID(Security ID) 별로 폴더 존재

- 각 사용자마다 독립된 휴지통 공간
- 특정 사용자가 지운 파일은 해당 사용자 SID 휴지통 폴더로 이동

삭제된 파일

- NT/2K/XP에서 삭제된 파일 목록



```
C:\WINDOWS\system32\cmd.exe
C:\#RECYCLERWS-1-5-21-1078081533-616249376-1417001333-1003>dir /a
C 드라이브의 볼륨에는 이름이 없습니다.
볼륨 일련 번호: BC53-FFD7

C:\#RECYCLERWS-1-5-21-1078081533-616249376-1417001333-1003 디렉터리

2011-02-19 오전 01:47 <DIR> .
2011-02-19 오전 01:47 <DIR> ..
2011-01-13 오후 02:54          62 Dc1.ini
2011-02-15 오후 03:00     5,260,023 Dc2.exe
2011-01-09 오전 02:23     44,544 Dc3.exe
2011-01-31 오후 03:34    1,333,471 Dc4.zip
2011-02-15 오후 03:13         65 desktop.ini
2011-02-19 오전 01:47       3,220 INFO2

        6개 파일             6,641,385 바이트
        2개 디렉터리    12,139,716,608 바이트 남음
```

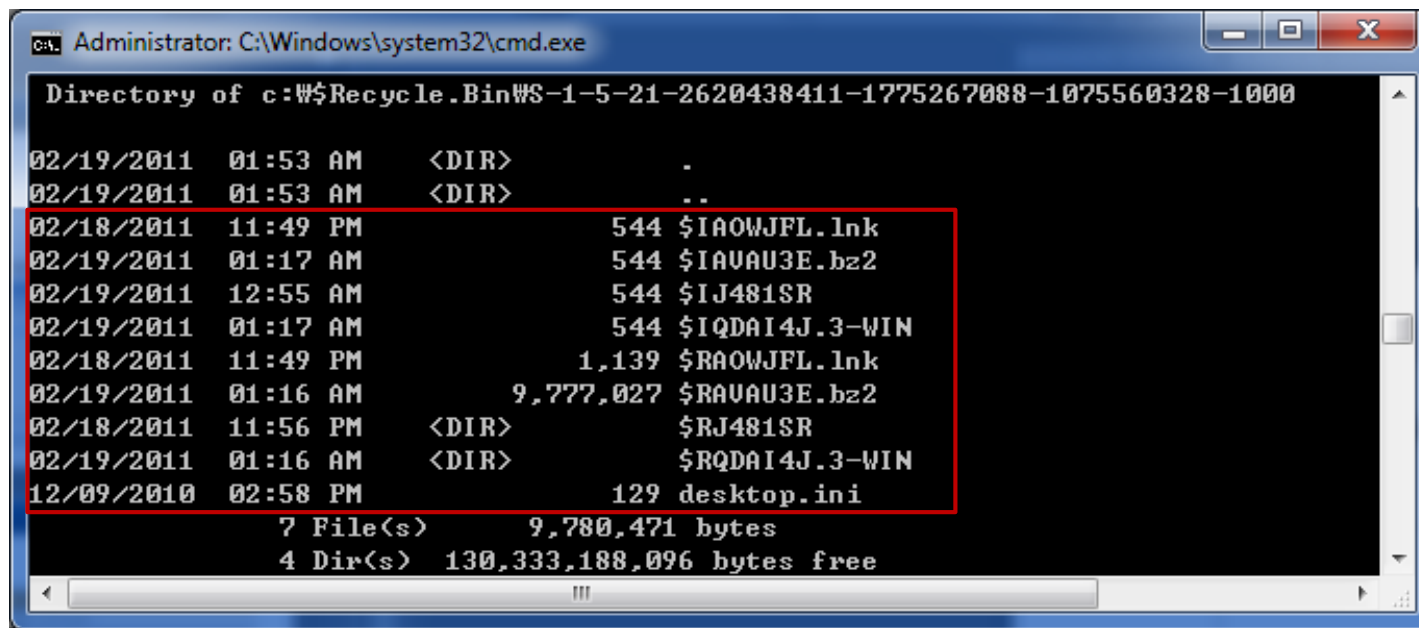
- 삭제된 파일 형식

- D [원본 파일이 위치한 볼륨명] [인덱스 번호] . [원본 파일 확장자]

- 원본 파일 경로, 삭제된 시간 등의 정보는 **INFO2** 파일로 관리

삭제된 파일

- Vista/7에서 삭제된 파일 목록



```
Administrator: C:\Windows\system32\cmd.exe

Directory of c:\Windows\Recycle.Bin\5-21-2620438411-1775267088-1075560328-1000

02/19/2011  01:53 AM    <DIR>          .
02/19/2011  01:53 AM    <DIR>          ..
02/18/2011  11:49 PM                544 $IAOWJFL.lnk
02/19/2011  01:17 AM                544 $IAU3E.bz2
02/19/2011  12:55 AM                544 $IJ481SR
02/19/2011  01:17 AM                544 $IQDAI4J.3-WIN
02/18/2011  11:49 PM            1,139 $RAOWJFL.lnk
02/19/2011  01:16 AM      9,777,027 $RAU3E.bz2
02/18/2011  11:56 PM    <DIR>          $RJ481SR
02/19/2011  01:16 AM    <DIR>          $RQDAI4J.3-WIN
12/09/2010  02:58 PM            129 desktop.ini

              7 File(s)          9,780,471 bytes
              4 Dir(s) 130,333,188,096 bytes free
```

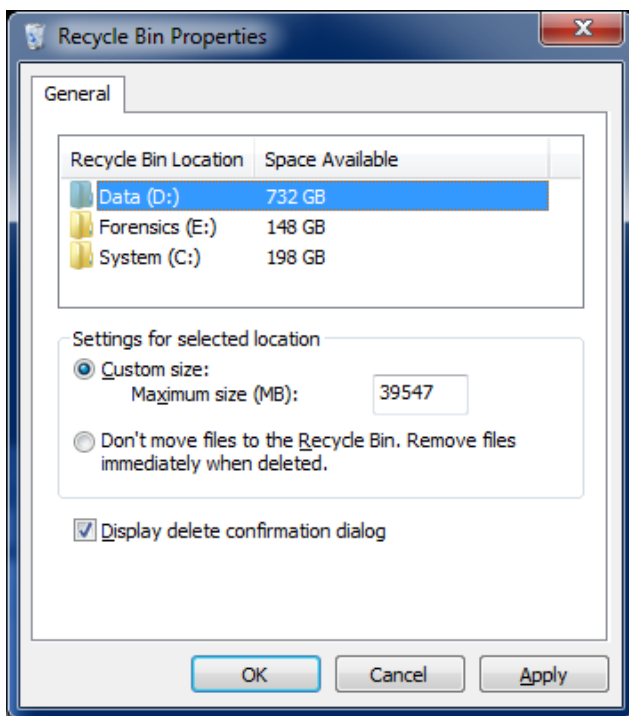
- 삭제된 파일 형식
 - \$R [임의 문자열] . [원본 파일 확장자]
- 원본 파일 경로, 삭제된 시간 등의 정보는 \$I [임의 문자열] . [원본 파일 확장자] 파일로 관리

파일의 삭제와 복원

- **휴지통 이용 파일 삭제 시 변화**
 - 파일을 삭제할 경우 해당 파일의 MFT 엔트리(NTFS 경우) 삭제
 - 휴지통 폴더의 새로운 파일 이름으로 MFT 엔트리 생성
 - 결과적으로, 파일 삭제 시 파일 메타 정보의 변경만 일어나고 파일 내용(데이터 영역)은 변화 없음
- **휴지통 이용 파일 복원 시 변화**
 - 파일을 복원할 경우 휴지통 MFT 엔트리 삭제 후, 원본 파일 경로에 새로운 MFT 엔트리 생성
 - 원본 파일 경로를 저장하는 파일
 - **NT/2K/XP** : INFO2
 - **Vista/7** : \$I #####
 - 파일의 시간 정보는 삭제와 복원시 그대로 유지

파일의 삭제와 복원

- 휴지통 최대 크기에 따른 삭제와 복원
 - 휴지통은 설정한 최대 크기를 넘지 않을 경우, 삭제한 파일 모두 복구 가능
 - 최대 크기를 넘길 경우 오래된 파일부터 차례로 삭제
 - 휴지통 크기 설정 : 휴지통 → 등록정보



휴지통 파일 구조

Security is a people problem...

NT/2K/XP – INFO2

- INFO2 파일 구조
 - 파일 헤더
 - 파일 레코드 (반복)

운영체제	휴지통 폴더 이름	INFO2 레코드 길이
윈도우 9X/Me	Recycled	280 bytes
윈도우 NT/2K	Recycler	800 bytes
윈도우 XP/2003	Recycler	800 bytes

NT/2K/XP – INFO2

- INFO2 파일 구조

범위	크기	설명
0 – 11	12 bytes	알 수 없는 영역
12 – 15	4 bytes	파일 레코드 크기, 항상 0x00000320 (800)
~		
0 – 263	264 bytes	원본 파일 경로 (ASCII)
264 – 267	4 bytes	레코드 번호
268 – 271	4 bytes	볼륨 번호 (C = 02, D = 03, E = 04, ...)
272 – 279	8 bytes	삭제된 시간/날짜 (Windows 64-bit Timestamp, FILETIME)
280 – 283	4 bytes	원본 파일 크기
284 – 799	516 bytes	원본 파일 경로 (UNICODE)

휴지통 파일 구조

NT/2K/XP – INFO2

- INFO2 파일 구조

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0A5463000	05	00	00	00	00	00	00	00	00	00	00	00	20	03	00	00	
0A5463010	00	00	00	00	43	3A	5C	54	6F	6F	6C	73	5C	58	2D	57	C:\Tools\X-W
0A5463020	61	79	73	20	57	69	6E	48	65	78	20	76	31	35	2E	38	ays WinHex v15.8
0A5463030	20	50	6F	72	74	61	62	6C	65	2E	65	78	65	00	00	00	Portable.exe
0A5463040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463110	00	00	00	00	00	00	00	00	01	00	00	00	02	00	00	00	
0A5463120	20	B7	1E	3B	7B	35	CC	01	00	30	17	00	43	00	3A	00	. ;{5t 0 C :
0A5463130	5C	00	54	00	6F	00	6F	00	6C	00	73	00	5C	00	58	00	\ Tools\X
0A5463140	2D	00	57	00	61	00	79	00	73	00	20	00	57	00	69	00	- Ways Wi
0A5463150	6E	00	48	00	65	00	78	00	20	00	76	00	31	00	35	00	n Hex v15
0A5463160	2E	00	38	00	20	00	50	00	6F	00	72	00	74	00	61	00	.8 Porta
0A5463170	62	00	6C	00	65	00	2E	00	65	00	78	00	65	00	00	00	ble.exe

휴지통 파일 구조

NT/2K/XP – INFO2

- INFO2 파일 구조 – 복원 후

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0A5463000	05	00	00	00	00	00	00	00	01	00	00	00	20	03	00	00	
0A5463010	00	00	00	00	00	3A	5C	54	6F	6F	6C	73	5C	58	2D	57	: \Tools\X-W
0A5463020	61	79	73	20	57	69	6E	48	65	78	20	76	31	35	2E	38	ays WinHex v15.8
0A5463030	20	50	6F	72	74	61	62	6C	65	2E	65	78	65	00	00	00	Portable.exe
0A5463040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463080	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463090	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630B0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A54630F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
0A5463110	00	00	00	00	00	00	00	00	01	00	00	00	02	00	00	00	
0A5463120	20	B7	1E	3B	7B	35	CC	01	00	30	17	00	43	00	3A	00	. ;{5i 0 C :
0A5463130	5C	00	54	00	6F	00	6F	00	6C	00	73	00	5C	00	58	00	\Tools\X
0A5463140	2D	00	57	00	61	00	79	00	73	00	20	00	57	00	69	00	- Ways Wi
0A5463150	6E	00	48	00	65	00	78	00	20	00	76	00	31	00	35	00	nHex v15
0A5463160	2E	00	38	00	20	00	50	00	6F	00	72	00	74	00	61	00	. 8 Porta
0A5463170	62	00	6C	00	65	00	2E	00	65	00	78	00	65	00	00	00	ble.exe

휴지통 파일 구조

NT/2K/XP – INFO2

- INFO2 파일 구조 – 휴지통 비우기 후

```
0000 .....
0120 .....
0240 .....
0360 .....
0480 .....
0600 .....
0720 .....
0840 \E~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.FLA CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.SWF
0960 .....
1080 R.....X~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.FLA CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.SWF
1200 b~1\MAIN_M~1.SWF CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.FLA CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.SWF
1320 .....
1440 .....
1560 .....
1680 M~1.SWF CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.FLA CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.SWF
1800 .....
1920 T~1\MAIN_M~1.SWF CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.FLA CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.SWF
2040 C~1\MAIN_M~1.SWF CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.FLA CISTE~1\ABOUT~1\ABOUTC~1\CIST,~1\MAIN_M~1.SWF
2160 .....
2280 .....
2400 .....
2520 .....
2640 .....
2760 .....
2880 a.....
```

- 휴지통을 비울 경우 INFO2 파일은 20바이트의 헤더만 유지
- 파일 슬랙을 이용하여 삭제된 파일 정보 확인 → INFO2 파일이 연속이었다면 클러스터 이상의 정보 확인 가능

Vista/7 – \$I 파일

- \$I 파일 구조
 - 고정된 544 바이트 크기로 삭제된 파일마다 하나씩 생성

범위	크기	설명
0 – 7	8 bytes	파일 헤더
8 – 15	8 bytes	원본 파일 크기
16 – 23	8 bytes	삭제된 파일 시간 정보 (Windows 64-bit Timestamp, FILETIME)
24 – 543	520 bytes	원본 파일 경로 (UNICODE)

휴지통 파일 구조

Vista/7 – \$I 파일

- \$I 파일 구조

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
00000000	01	00	00	00	00	00	00	00	73	04	00	00	00	00	00	00s.....
00000010	F0	E8	8D	03	7B	CF	CB	01	43	00	3A	00	5C	00	55	00{...C...\U.
00000020	73	00	65	00	72	00	73	00	5C	00	70	00	72	00	30	00	s.e.r.s.\.p.r.O.
00000030	6E	00	65	00	65	00	72	00	5C	00	41	00	70	00	70	00	n.e.e.r.\.A.p.p.
00000040	44	00	61	00	74	00	61	00	5C	00	52	00	6F	00	61	00	D.a.t.a.\.R.o.a.
00000050	6D	00	69	00	6E	00	67	00	5C	00	4D	00	69	00	63	00	m.i.n.g.\.M.i.c.
00000060	72	00	6F	00	73	00	6F	00	66	00	74	00	5C	00	57	00	r.o.s.o.f.t.\.W.
00000070	69	00	6E	00	64	00	6F	00	77	00	73	00	5C	00	50	00	i.n.d.o.w.s.\.P.
00000080	72	00	69	00	6E	00	74	00	65	00	72	00	20	00	53	00	r.i.n.t.e.r. .S.
00000090	68	00	6F	00	72	00	74	00	63	00	75	00	74	00	73	00	h.o.r.t.c.u.t.s.
000000A0	5C	00	70	00	72	00	30	00	6E	00	65	00	65	00	72	00	\.p.r.O.n.e.e.r.
000000B0	20	00	2D	00	20	00	53	00	68	00	6F	00	72	00	74	00	.-. .S.h.o.r.t.
000000C0	63	00	75	00	74	00	2E	00	6C	00	6E	00	6B	00	00	00	c.u.t...l.n.k...
000000D0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000E0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000000F0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000100	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000120	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000150	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000160	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000170	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000180	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000190	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
000001A0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

File Deleted Data/Time

File Header

Original File Size

Original File Path

Vista/7 – \$I 파일

- **\$I 파일의 복원과 휴지통 비우기**
 - 윈도우 Vista/7은 삭제된 파일마다 \$I 파일이 존재하며, 원본 경로와 삭제된 시간 등의 정보 저장
 - 파일의 복원이나 휴지통 비우기 시 \$I 파일은 삭제됨
 - 파일 복구 성능에 따라 복원 및 휴지통 비우기 이전 흔적 분석 가능

휴지통 파일 카빙

Security is a people problem...

시그니처 카빙

- 카빙의 필요성
 - 휴지통 파일(INFO2, \$I)은 휴지통을 사용하는 윈도우 환경에서 필수적인 카빙 대상
 - 파일 삭제 및 휴지통 비우기는 비교적 빈번하게 이루어짐 ➔ 휴지통 파일이 삭제됨
 - 카빙을 통해 삭제된 파일의 흔적 파악

시그니처 카빙

- **INFO2 파일 카빙**

- 파일 헤더의 파일 레코드 크기는 항상 고정이므로 해당 값을 통해 카빙
- **INFO2 File Offset 0C** : 0x000000320 (800)

- **\$I 파일 카빙**

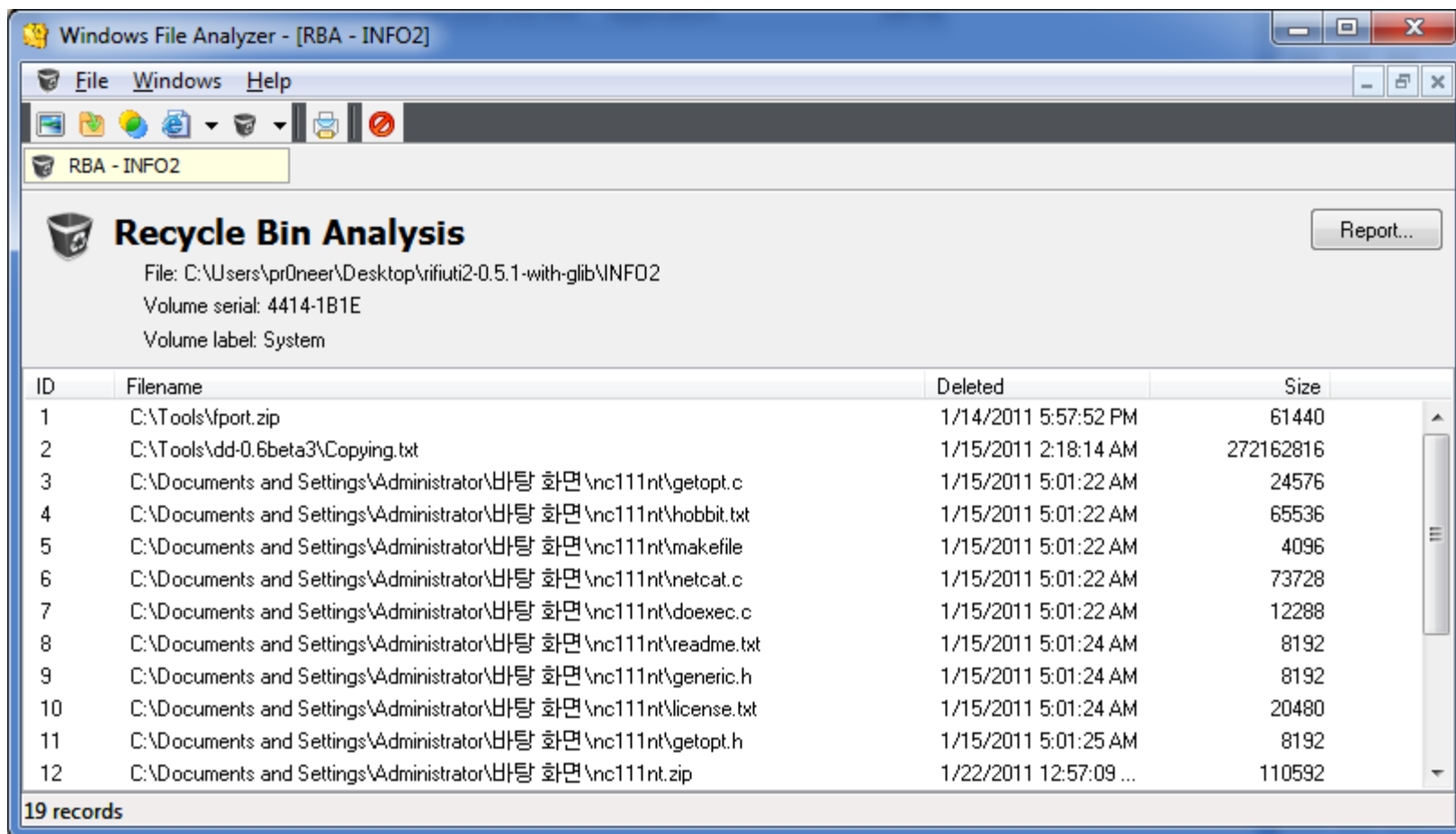
- 파일 헤더의 8바이트 값을 이용해 카빙 ➔ 추가 검증 필요
- **\$I File Offset 00** : 0x00000000 00000001

휴지통 파일 분석

Security is a people problem...

휴지통 분석 도구

- Windows File Analyzer (<http://www.mitec.cz/wfa.html>)



휴지통 분석 도구

- INFO2 파일 분석 도구 – rifiuti2 (<http://code.google.com/p/rifiuti2/>)

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\pr0neer\Desktop\rifiuti2-0.5.1-with-glib>rifiuti.exe INFO2
Recycle bin file: 'INFO2'
Version: 5

Index Deleted Time      Gone? Size  Path
1      2011-01-14 17:57:52 No    61440 C:\Tools\port.zip
2      2011-01-15 02:18:14 No    272162816 C:\Tools\dd-0.6beta3\Copying.txt
3      2011-01-15 05:01:22 No    24576 C:\Documents and Settings\Administrator\Wnc111nt\getopt.c
4      2011-01-15 05:01:22 No    65536 C:\Documents and Settings\Administrator\Wnc111nt\hobbit.txt
5      2011-01-15 05:01:22 No    4096 C:\Documents and Settings\Administrator\Wnc111nt\makefile
6      2011-01-15 05:01:22 No    73728 C:\Documents and Settings\Administrator\Wnc111nt\netcat.c
7      2011-01-15 05:01:22 No    12288 C:\Documents and Settings\Administrator\Wnc111nt\doexec.c
8      2011-01-15 05:01:24 No    8192 C:\Documents and Settings\Administrator\Wnc111nt\readme.txt
9      2011-01-15 05:01:24 No    8192 C:\Documents and Settings\Administrator\Wnc111nt\generic.h
10     2011-01-15 05:01:24 No    20480 C:\Documents and Settings\Administrator\Wnc111nt\license.txt
11     2011-01-15 05:01:25 No    8192 C:\Documents and Settings\Administrator\Wnc111nt\
```