

Forensic Analysis of Microsoft Windows Recycle Bin Records

by Keith J. Jones
keith.jones@foundstone.com

4/1/03
(revised 5/6/03)

Table of Contents

<i>1. Introduction.....</i>	<i>2</i>
<i>2. Background.....</i>	<i>2</i>
<i>3. The INFO2 File Data Structures.....</i>	<i>4</i>
<i>4. Rifiuti – The Open Source INFO2 File Parser.....</i>	<i>10</i>

Listing of Tables

Table 1 - Location of the INFO2 Files.....	2
Table 2 - The Structures within the INFO2 File.....	9

Listing of Figures

Figure 1 - The Recycle Bin.....	3
Figure 2 - The Recycle Record Length.....	5
Figure 3 - The Recycled File Name.....	6
Figure 4 - The Recycle Record Index Number.....	7
Figure 5 - The Drive Number.....	7
Figure 6 - The Deleted Time Stamp.....	8
Figure 7 - The Recycled File Size.....	9
Figure 8 - Rifiuti in Action.....	10
Figure 9 - Rifiuti's Output.....	11

1. Introduction

Contrary to popular belief, when a file is deleted from a computer it is not really deleted. This is especially true for Microsoft Windows Operating Systems. Windows utilizes a repository for deleted files called the *Recycle Bin*. The existence of the Recycle Bin allows a user to retrieve a document he accidentally deleted. In order for Windows to undelete a file in this manner, certain information must be stored in records so that the original information about the file may be restored, such as the file name. The file containing this information is named `INFO2` and resides in the Recycle bin directory. This paper will discuss the internal data structures of the `INFO2` file useful when conducting forensic analysis of a suspect's computer systems.

This research was conducted because the data proprietary Microsoft Windows files lack proper documentation needed by forensic analysts. Furthermore, there is a lack of publicly available open source tools that will reconstruct the `INFO2` file. This research attempts to solve both of these problems.

2. Background

It is necessary to examine how the Recycle Bin facility operates before we discuss the structures within the `INFO2` file. When a user “deletes” a file through Windows Explorer, a copy of the file is moved to the Recycle Bin directory on the hard drive. The location of this directory is dependant on the version of Windows running on the computer. Table 1 lists the locations of the `INFO2` file within the Recycle Bin directory on different versions of Microsoft Windows.

Table 1 - Location of the `INFO2` Files

<i>Operating System</i>	<i>Common File System Type</i>	<i>Location of the Recycle Bin Directory</i>
Windows 95/98/ME	FAT32	C:\Recycled\INFO2
Windows NT/2k/XP	NTFS	C:\Recycler\ <i><USER SID></i> \INFO2

When a file is moved to the Recycle Bin, it is typically renamed to `DC#.EXT`, where “#” is an integer and “EXT” is the original file's extension (see Figure 1). For example, if `JONES.TXT` was moved to the Recycle Bin, it may become a file such as `DC1.TXT`. The number (#) is important in this new filename because it is unique. As more files are moved to the Recycle Bin, this integer increases by one. This integer, as we will see later, is an index (or reference) into the `INFO2` file.

```
C:\WINDOWS\System32\cmd.exe
C:\RECYCLER\S-1-5-21-1482476501-1532298954-1801674531-1005>dir /a
Volume in drive C has no label.
Volume Serial Number is 3452-DE76

Directory of C:\RECYCLER\S-1-5-21-1482476501-1532298954-1801674531-1005

04/11/2003  11:35 AM  <DIR>          .
04/11/2003  11:35 AM  <DIR>          ..
04/08/2003  06:39 PM           1,926 Dc1.lnk
04/08/2003  06:39 PM           1,952 Dc2.lnk
04/08/2003  05:13 PM             779 Dc3.lnk
04/11/2003  11:17 AM       1,897,672 Dc4.exe
04/11/2003  11:32 AM     125,173,760 Dc5
04/11/2003  11:07 AM  <DIR>          Dc6
04/11/2003  11:33 AM     600,000,000 Dc7.aa
04/08/2003  06:40 PM             65 desktop.ini
04/11/2003  11:35 AM             5,620 INFO2
           8 File(s)       727,081,774 bytes
           3 Dir(s)    11,881,926,656 bytes free

C:\RECYCLER\S-1-5-21-1482476501-1532298954-1801674531-1005>_
```

Figure 1 - The Recycle Bin

When at least one file has been moved to the Recycle Bin, the INFO2 file will exist. When the Recycle Bin is emptied, the INFO2 file is cleansed and the previously recycled file information will not exist there anymore. Additionally, the unique index is reset to one. In other words, the previous INFO2 record is deleted and an empty new INFO2 file is created.

3. The INFO2 File Data Structures

So far, we know that the `INFO2` file has to record the following sets of information for each file moved to the Recycle Bin in order to undelete a needed document:

- The file's original full path name
- The file's size
- The date and time the file was moved to the Recycle Bin
- The file's unique ID number within the Recycle Bin

Upon opening the `INFO2` file in a hex editor, we will locate these structures. When viewing the `INFO2` file in a hex editor, it is easy to see¹ that each recycle record is 0x320 bytes long (see Figure 2). If we examine the `INFO2` file header, we see that “20 03 00 00”, which translates to 0x320, is found at byte offset 0xC. The first valid recycle record is located immediately after the recycle record size information.

¹ Notice that this hex editor writes the starting byte, the ending byte, and the length of the selected text in the upper right hand corner.

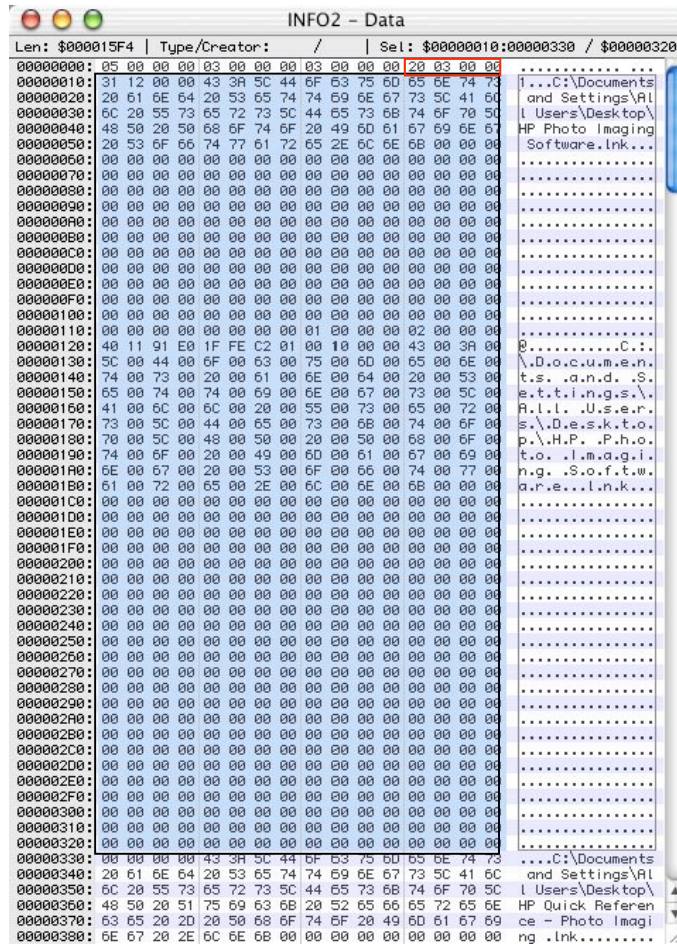


Figure 2 - The Recycle Record Length

As you can see, the file name is located twice in the recycle record. There is an ASCII version near the beginning of the record and a UNICODE version near the end. It will be easier to output the ASCII version, located at 0x04 bytes after the beginning of the recycle record. In this example, the file we are examining is called "C:\Documents and Settings\All Users\Desktop\HP Quick Reference - Photo Imaging .lnk".

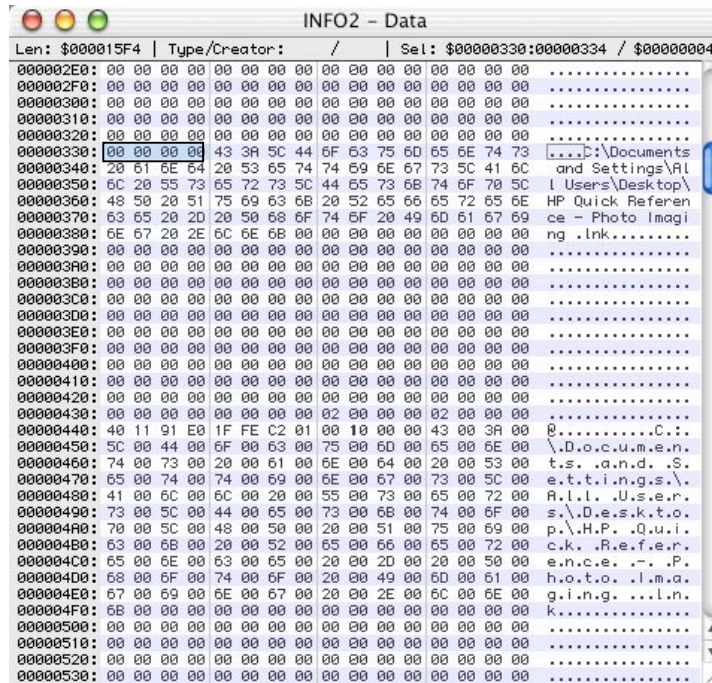


Figure 3 - The Recycled File Name

The next piece of information we will want to identify within a recycle record is the unique index number. When comparing different recycle records within the same INFO2 file, we see the value at offset 0x108 increases by one for each listed file. This particular recycle record in the example is number 02.

INFO2 - Data		
Len: \$000015F4	Type/Creator: /	Sel: \$00000330:00000438 / \$00000108
000002E0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002F0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000300:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000310:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000320:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000330:	00 00 00 00 43 3A 5C 44 6F 63 75 60 65 6E 74 73C:\Documents
00000340:	20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 41 6C	and Settings\Al
00000350:	6C 20 55 73 65 72 73 5C 44 65 73 68 74 6F 70 50	l Users\Desktop\
00000360:	48 50 20 51 75 69 63 68 20 52 65 66 65 72 65 6E	HP Quick Referen
00000370:	63 65 20 2D 20 50 68 6F 74 6F 20 49 60 61 67 69	ce - Photo Imagi
00000380:	6E 67 20 2E 6C 6E 6B 00 00 00 00 00 00 00 00	ng .lnk.....
00000390:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003A0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003B0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003C0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003D0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003E0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003F0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000400:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000410:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000420:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000430:	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00
00000440:	40 11 91 E0 1F FE C2 01 00 10 00 00 43 00 3A 00	0.....C.:.
00000450:	5C 00 44 00 6F 00 63 00 75 00 60 00 65 00 6E 00	\.D.o.c.u.m.e.n.
00000460:	74 00 73 00 20 00 61 00 6E 00 64 00 20 00 53 00	t.s..a.n.d..S.
00000470:	65 00 74 00 74 00 69 00 6E 00 67 00 73 00 5C 00	e.t.t.i.n.g.s.\
00000480:	41 00 6C 00 6C 00 20 00 55 00 73 00 65 00 72 00	R.l.l..U.s.e.r.
00000490:	73 00 5C 00 44 00 65 00 73 00 68 00 74 00 6F 00	s.\D.e.s.k.t.o.
000004A0:	70 00 5C 00 48 00 50 00 20 00 51 00 75 00 69 00	p.\.H.P..Q.u.i.
000004B0:	63 00 6B 00 20 00 52 00 65 00 66 00 65 00 72 00	c.k..R.e.f.e.r.
000004C0:	65 00 6E 00 63 00 65 00 20 00 20 00 20 00 50 00	e.n.c.e.-.P.
000004D0:	68 00 6F 00 74 00 6F 00 20 00 49 00 60 00 61 00	h.o.t.o..l.m.a.
000004E0:	67 00 69 00 6E 00 67 00 20 00 2E 00 6C 00 6E 00	g.i.n.g...l.n.
000004F0:	68 00 00 00 00 00 00 00 00 00 00 00 00 00 00	k.....
00000500:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000510:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000520:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000530:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figure 4 - The Recycle Record Index Number

The next bit of information seems to be the drive number where the file originated before it was moved to the Recycle Bin. The data is encoded using the following scheme: 0x00 is drive "A:", 0x01 is drive "B:", and 0x02 is drive "C:", and so on. This information is located 0x10C bytes from the beginning of the recycle record. The recycled file in this example was originally from drive C:.

INFO2 - Data		
Len: \$000015F4	Type/Creator: /	Sel: \$00000330:0000043C / \$0000010C
000002E0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000002F0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000300:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000310:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000320:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000330:	00 00 00 00 43 3A 5C 44 6F 63 75 60 65 6E 74 73C:\Documents
00000340:	20 61 6E 64 20 53 65 74 74 69 6E 67 73 5C 41 6C	and Settings\Al
00000350:	6C 20 55 73 65 72 73 5C 44 65 73 68 74 6F 70 50	l Users\Desktop\
00000360:	48 50 20 51 75 69 63 68 20 52 65 66 65 72 65 6E	HP Quick Referen
00000370:	63 65 20 2D 20 50 68 6F 74 6F 20 49 60 61 67 69	ce - Photo Imagi
00000380:	6E 67 20 2E 6C 6E 6B 00 00 00 00 00 00 00 00	ng .lnk.....
00000390:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003A0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003B0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003C0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003D0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003E0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
000003F0:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000400:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000410:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000420:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000430:	00 00 00 00 00 00 00 00 02 00 00 00 02 00 00
00000440:	40 11 91 E0 1F FE C2 01 00 10 00 00 43 00 3A 00	0.....C.:.
00000450:	5C 00 44 00 6F 00 63 00 75 00 60 00 65 00 6E 00	\.D.o.c.u.m.e.n.
00000460:	74 00 73 00 20 00 61 00 6E 00 64 00 20 00 53 00	t.s..a.n.d..S.
00000470:	65 00 74 00 74 00 69 00 6E 00 67 00 73 00 5C 00	e.t.t.i.n.g.s.\
00000480:	41 00 6C 00 6C 00 20 00 55 00 73 00 65 00 72 00	R.l.l..U.s.e.r.
00000490:	73 00 5C 00 44 00 65 00 73 00 68 00 74 00 6F 00	s.\D.e.s.k.t.o.
000004A0:	70 00 5C 00 48 00 50 00 20 00 51 00 75 00 69 00	p.\.H.P..Q.u.i.
000004B0:	63 00 6B 00 20 00 52 00 65 00 66 00 65 00 72 00	c.k..R.e.f.e.r.
000004C0:	65 00 6E 00 63 00 65 00 20 00 20 00 20 00 50 00	e.n.c.e.-.P.
000004D0:	68 00 6F 00 74 00 6F 00 20 00 49 00 60 00 61 00	h.o.t.o..l.m.a.
000004E0:	67 00 69 00 6E 00 67 00 20 00 2E 00 6C 00 6E 00	g.i.n.g...l.n.
000004F0:	68 00 00 00 00 00 00 00 00 00 00 00 00 00 00	k.....
00000500:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000510:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000520:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00000530:	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Figure 5 - The Drive Number

It is very useful for the investigator to know *when* a file was moved to the recycle bin. For an example, imagine a suspect moving subject matter to the recycle bin after a temporary restraining order was executed. Knowing when the file was “deleted” may prove the suspect ignored the restraining order. The field that contains this time stamp is 0x110 bytes from the beginning of the recycle record and is 8 bytes in length.

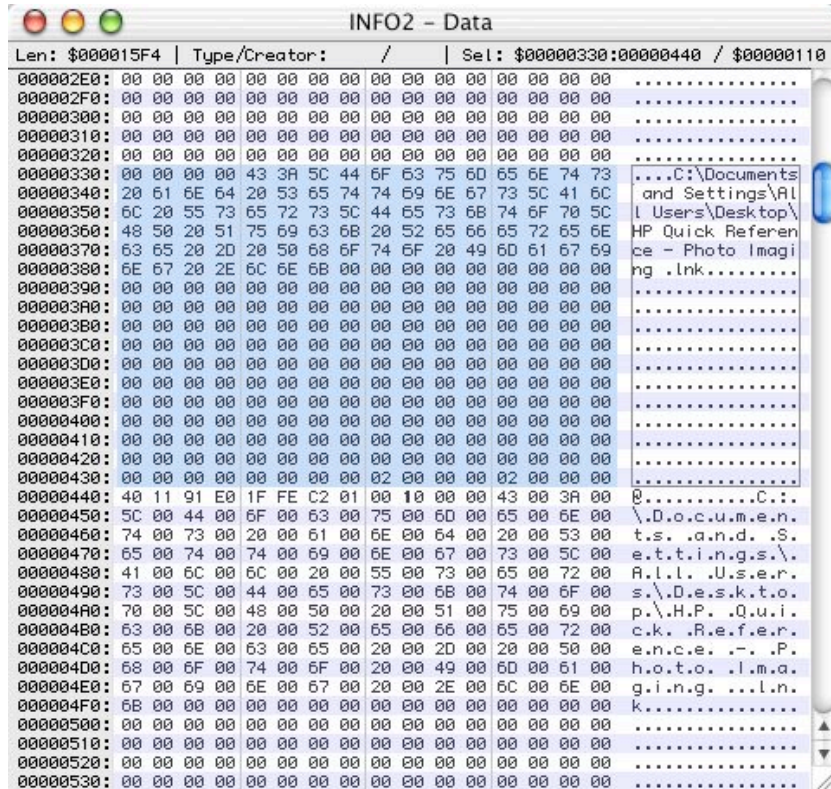


Figure 6 - The Deleted Time Stamp

Now that we know where the deleted time stamp exists, we must translate it to something a human can understand. Windows saves time stamps in “FILETIME” format. FILETIME format is the number of ticks, in 100ns increments, since 00:00 1 Jan, 1601 (UTC). Since the rest of the world uses the Unix definition of time, which is the number of seconds since 00:00 1 Jan 1970, we must be able to translate the FILETIME format to the Unix time format. This is done with the following simple equation:

$$(Unix\ Time) = A * (NT\ Time) + B$$

Since the ticks in FILETIME are at 100ns intervals, we know that “A” is 10⁻⁷. The trick is finding “B”. “B” is the number of seconds between 1 Jan 1601 and 1 Jan 1970. We do not have to painstakingly calculate that value because it is well documented with MSDN and open source initiatives that “B” is 11644473600.

This example has a deletion time of “01 C2 FE 1F E0 91 11 40”, which translates to April 8, 2003 at 22:40:38.

The last field contains the file size. This field is 0x118 bytes from the beginning of the recycle record. The file size reported in the recycle record is not exactly the same as the file size reported from the dir command. The INFO2 file records physical file sizes while the dir command reports logical file sizes. Therefore, the sizes in the INFO2 file should be a multiple of the hard disk’s cluster size. In the example, the cluster size is 4096 bytes.

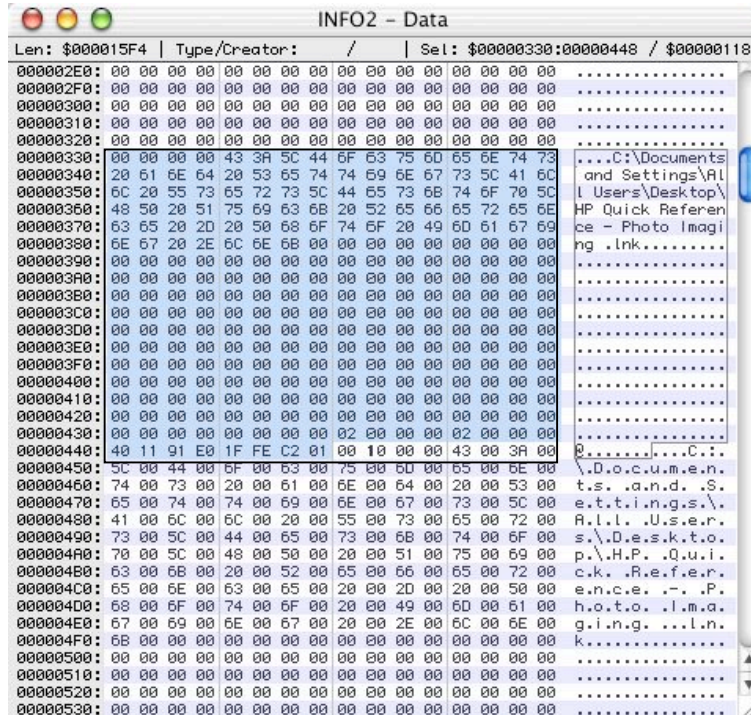


Figure 7 - The Recycled File Size

The following table summarizes the structures discovered in the INFO2 file:

Table 2 - The Structures within the INFO2 File

<i>Data Structure</i>	<i>Length (in bytes)</i>	<i>Byte Offset</i>
Recycle Record Size	4	0xC
Recycled File Name	Variable, NULL terminated	Start of Record+0x04
Recycle Record Unique ID	4	Start of Record+0x108
Drive Number for Recycled File	4	Start of Record+0x10C
Deletion Time	8	Start of Record+0x110
Deleted Physical File Size	4	Start of Record+0x118

4. Rifiuti – The Open Source INFO2 File Parser

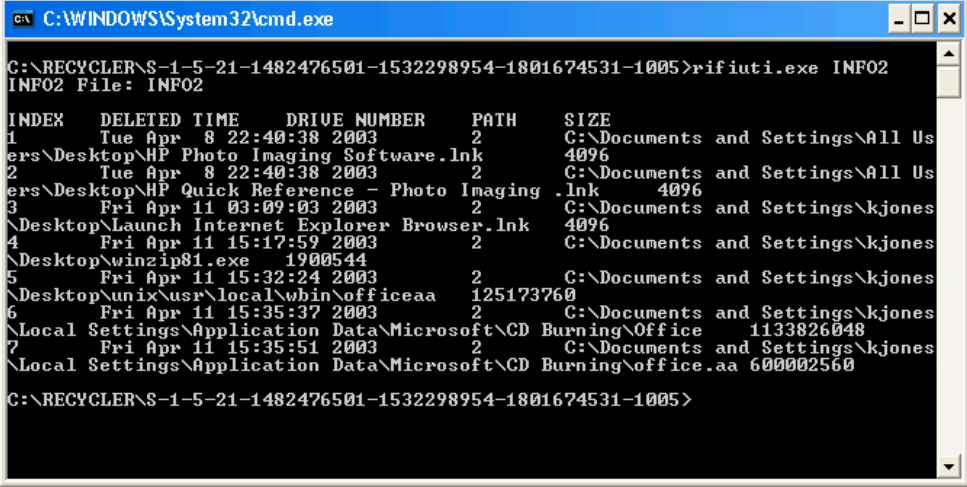
Now that we have an understanding of the internal structures, we can reconstruct an INFO2 file. We can easily develop a tool to automate everything we have done by hand so far. The author developed a tool named Rifiuti, the Italian word for trash, to parse the information in an INFO2 file and return the results in a field delimited format. Rifiuti's command line arguments are as follows:

```
[kjones: rifiuti] kjones% ./rifiuti

Usage: rifiuti [options] <filename>
       -t Field Delimiter (TAB by default)
```

The “-t” option will allow the investigator to change the field delimiter. The output will be sent to standard out (the console) by default. It is suggested that Rifiuti is run in the following manner:

```
./rifiuti INFO2 > INFO2.txt
```



```
C:\WINDOWS\System32\cmd.exe
C:\RECYCLER\S-1-5-21-1482476501-1532298954-1801674531-1005>rifiuti.exe INFO2
INFO2 File: INFO2

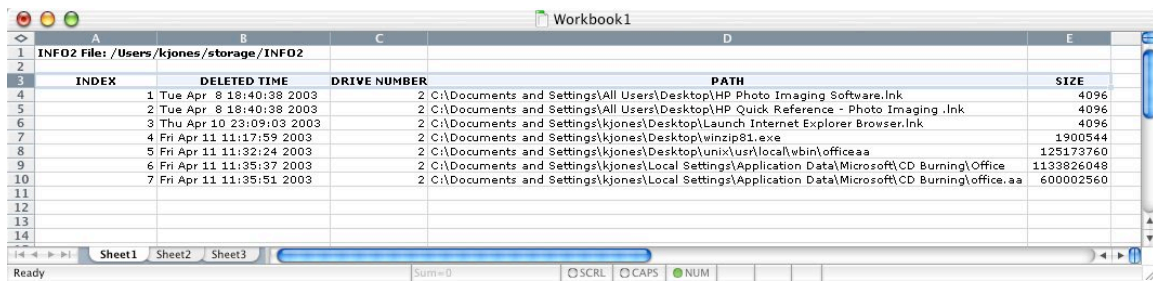
INDEX  DELETED TIME      DRIVE NUMBER  PATH                                     SIZE
1      Tue Apr  8 22:40:38 2003          2      C:\Documents and Settings\All Users\
Desktop\HP Photo Imaging Software.lnk  4096
2      Tue Apr  8 22:40:38 2003          2      C:\Documents and Settings\All Users\
Desktop\HP Quick Reference - Photo Imaging.lnk  4096
3      Fri Apr 11 03:09:03 2003          2      C:\Documents and Settings\kjones\
Desktop\Launch Internet Explorer Browser.lnk  4096
4      Fri Apr 11 15:17:59 2003          2      C:\Documents and Settings\kjones\
Desktop\winzip81.exe 1900544
5      Fri Apr 11 15:32:24 2003          2      C:\Documents and Settings\kjones\
Desktop\unix\usr\local\sbin\officeaa 125173760
6      Fri Apr 11 15:35:37 2003          2      C:\Documents and Settings\kjones\
Local Settings\Application Data\Microsoft\CD Burning\Office 1133826048
7      Fri Apr 11 15:35:51 2003          2      C:\Documents and Settings\kjones\
Local Settings\Application Data\Microsoft\CD Burning\office.aa 600002560

C:\RECYCLER\S-1-5-21-1482476501-1532298954-1801674531-1005>
```

Figure 8 - Rifiuti in Action

Rifiuti shows us that there are some interesting files in this user's recycle bin! Just by examining the file names alone, we see that the suspect is attempting to create a CD with some files named “Office”. Could this be an illegal attempt to distribute Microsoft Office? To find out, we would have to examine the files in the recycle bin directory (see Figure 1) further.

It is important to note that Rifiuti's output can be easily imported into your favorite spreadsheet program so that you may sort, search, and filter the data. Furthermore, a spreadsheet will allow you to format the data so that it is appropriate for a report.



INDEX	DELETED TIME	DRIVE NUMBER	PATH	SIZE
1	Tue Apr 8 18:40:38 2003	2	C:\Documents and Settings\All Users\Desktop\HP Photo Imaging Software.Ink	4096
2	Tue Apr 8 18:40:38 2003	2	C:\Documents and Settings\All Users\Desktop\HP Quick Reference - Photo Imaging .Ink	4096
3	Thu Apr 10 23:09:03 2003	2	C:\Documents and Settings\kjones\Desktop\Launch Internet Explorer Browser.Ink	4096
4	Fri Apr 11 11:17:59 2003	2	C:\Documents and Settings\kjones\Desktop\winzip81.exe	1900544
5	Fri Apr 11 11:32:24 2003	2	C:\Documents and Settings\kjones\Desktop\unix\usr\local\wbin\officeaa	125173760
6	Fri Apr 11 11:35:37 2003	2	C:\Documents and Settings\kjones\Local Settings\Application Data\Microsoft\CD Burning\Office	1133826048
7	Fri Apr 11 11:35:51 2003	2	C:\Documents and Settings\kjones\Local Settings\Application Data\Microsoft\CD Burning\office.aa	600002560

Figure 9 - Rifiuti's Output

Rifiuti is open source and released under the liberal FreeBSD license. Rifiuti can be compiled on Windows (using Cygwin), Mac OS X, Linux, and *BSD.