The Forensic Analysis of the Microsoft Windows Vista Recycle Bin

By Mitchell Machor
MMachor@gmail.com

1/22/2008

- 1 - Introduction

Contrary to due belief, when a file is deleted on a Microsoft operating system, it still exists on the computer. It is hidden away in a location commonly known as the Recycle Bin. The file is retained within the confines of the Recycle Bin until either the user chooses to empty the Recycle Bin. The user may bypass sending a file to the Recycle Bin by holding down the shift key while deleting the file. In the case that it is placed into the Recycle Bin the file is moved to a hidden, system folder where it is renamed and stored until further instructions are given as to what is to happen to the file. The file can still be restored at this point or the user may choose to more permanently rid them self of the file. In order to achieve this, there needs to be information stored pertaining to the file in its original state.

This file is being created as in the past Windows utilized a different means of managing the Windows Recycle bin. The past Recycle Bins had a master database that held all of the information named INFO2. Vista has decided to forgo the INFO2 file and create a separate record file for each file deleted. This will explain the location and structure of the files that may need to be analyzed in a forensic investigation.

- 2 - Background

To understand how the information files are structured and how they naming convention works, there must first be an understanding of how the Recycle Bin works. When a user "deletes" a file in Windows, the file itself is not actually deleted. The file is at this point copied into the Recycle Bins system folder where it is held until the user gives further instructions on what to do with the file. This location varies dependent on the versioin of Windows the user is running. The table below shows locations from both past versions of Windows as well as Windows Vista.

Operating System	Common File System Structure	Location of Deleted Files
Windows 95/98/ME	FAT32	C:\Recycled\INFO2
Windows NT/2K/XP	NTFS	C:\Recycler\<USER SID>\INFO2
Windows Vista	NTFS	C:\$Recycle.Bin\<USER SID>\

Table 1 – File Locations

When a file is "deleted" and Windows moves it to the Recycle Bin is automatically renamed. In the past the renaming of the files was quite simply DC#.xxx. The DC is standard and the # are integer numbers assigned in the order that the files are received by the Recycle Bin. The xxx is where the Recycle Bin holds on to the original extension of the file. In Vista, however, the renaming of files consists of $R and a set of random letters and numbers still holding onto the files original extension. At this time a second file is also created being named $I and a set of random letters and numbers matching the ones given to the $R name. This file also keeps the original files extension. The file names will be identical with the exception of the $I versus the $R. When the Recycle Bin is emptied, both files in the pair are deleted.

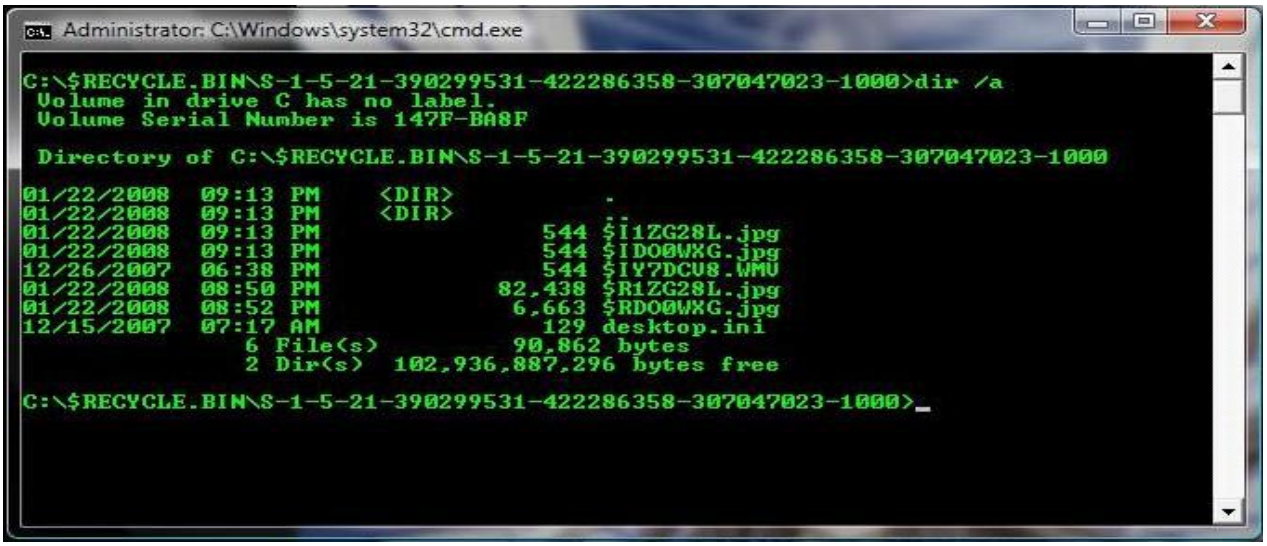


Image 1 – Recycle Bin Directory In Windows Vista

- 3 - The Comparison of the $I Files to INFO2

At this point we have come to the conclusion that the files with the $I have to hold the information necessary to undelete the file if the user chooses to do so. The INFO2 file originally held the following information used to “undelete” files found in the Recycle Bin:

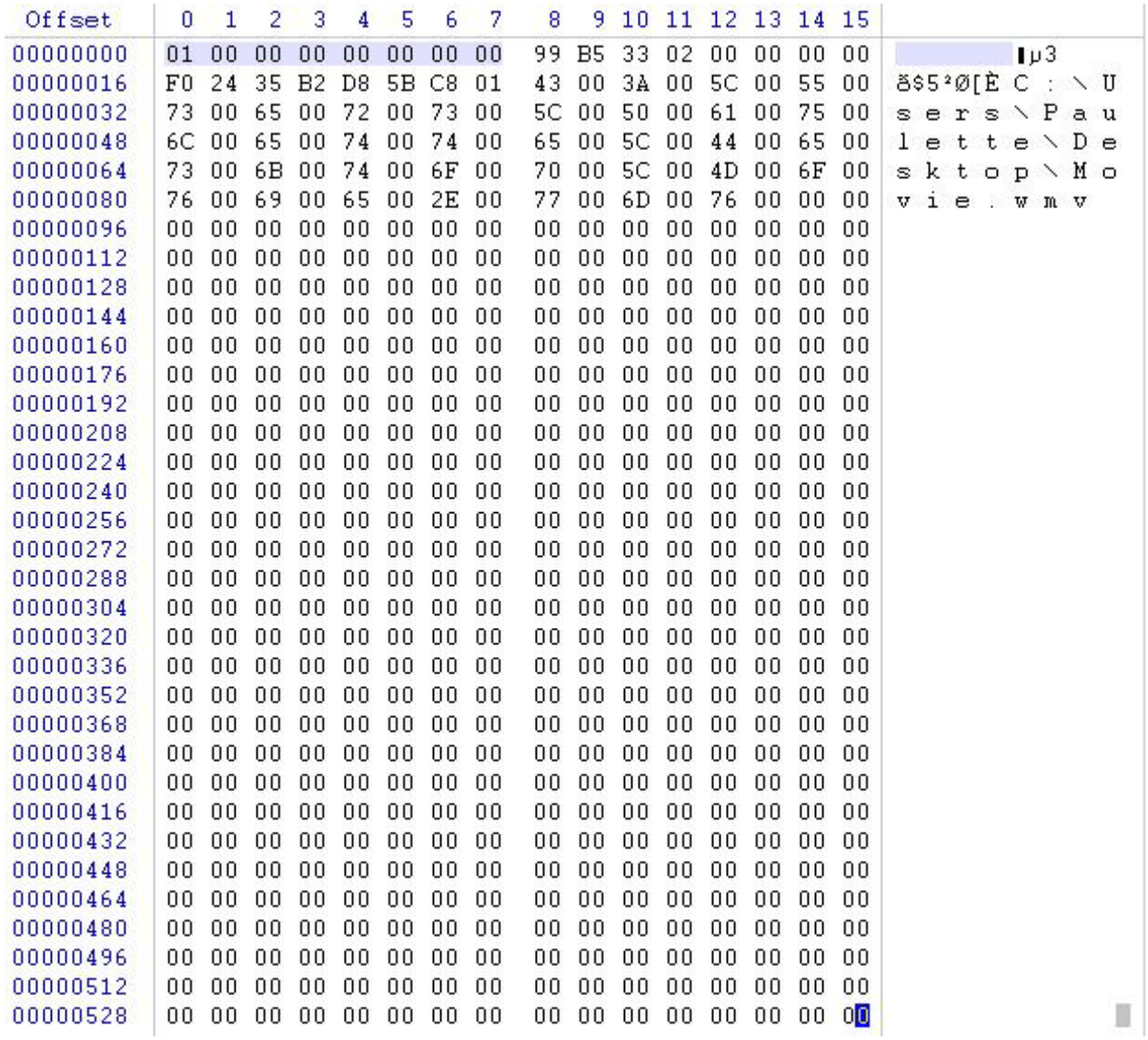
- Original File Name
- Original File Size
- The Date And Time The File Was Deleted
- The Files Unique Identifying Number In The Recycle Bin
- The Drive Number That The File Came From

This is where there is a difference between the INFO2 and Vista. In Windows Vista the $I file contains information only relevant to the file that it is paired up with. The information contained in these files is as follows:

- Original File Name
- Original File Size
- The Date And Time The File Was Deleted

Due to the fact that there is only one record in each of the information files, there is no need for the unique identifier that was present in the INFO2 file. Each of these files is 544 bytes long. We will now take a look at one using a hex editor to layout the file structure.

- 4 - The Header of the $I File



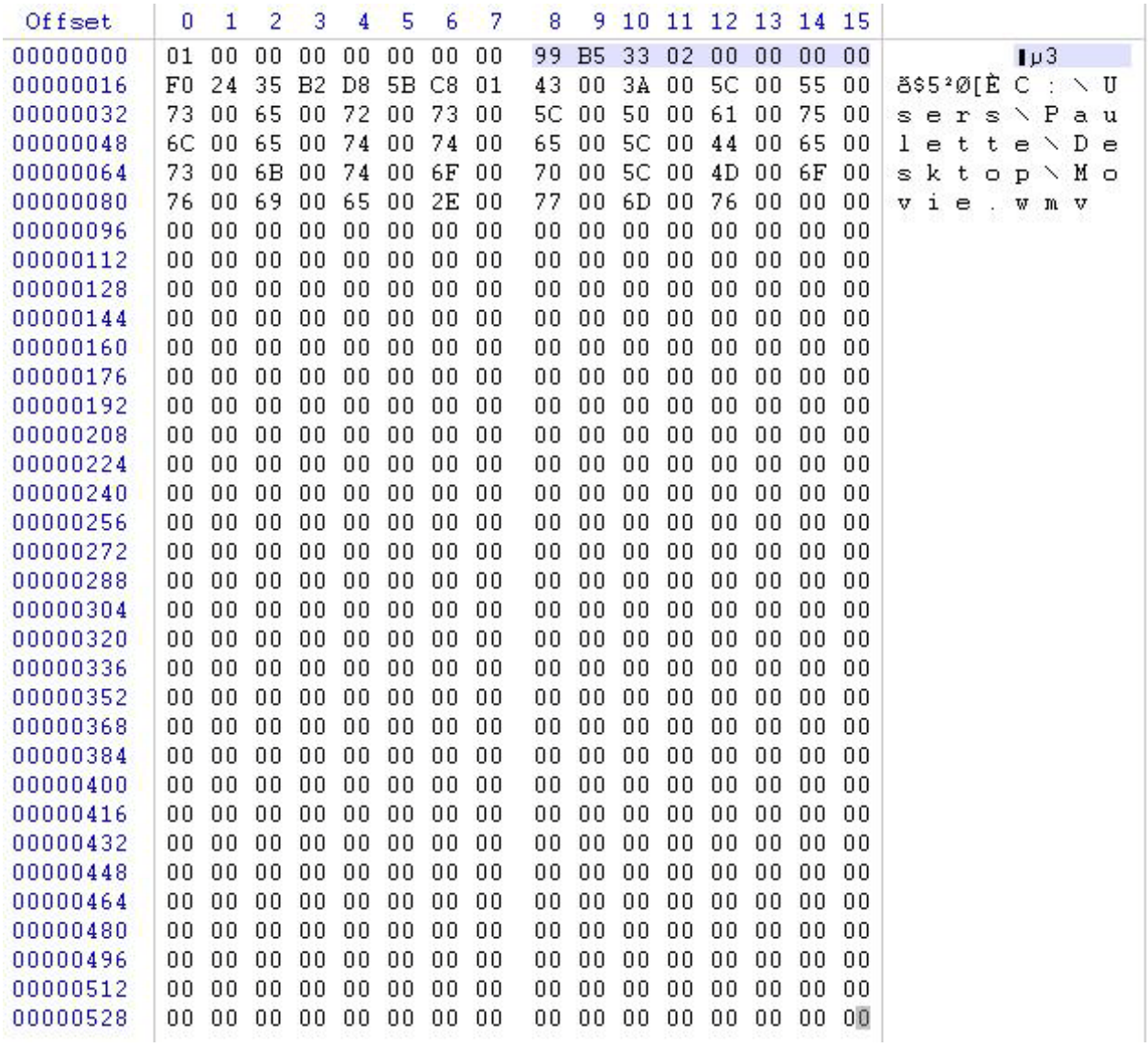
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	01	00	00	00	00	00	00	00	99	B5	33	02	00	00	00	00
00000016	F0	24	35	B2	D8	5B	C8	01	43	00	3A	00	5C	00	55	00
00000032	73	00	65	00	72	00	73	00	5C	00	50	00	61	00	75	00
00000048	6C	00	65	00	74	00	74	00	65	00	5C	00	44	00	65	00
00000064	73	00	6B	00	74	00	6F	00	70	00	5C	00	4D	00	6F	00
00000080	76	00	69	00	65	00	2E	00	77	00	6D	00	76	00	00	00
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000144	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
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000304	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
00000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000384	00	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	00
00000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000528	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

															▮	µ	3	
ð	$	5	²	Ø	[	È	C	:	\	U	s	e	r	s	\	P	a	u
l	e	t	t	e	\	D	e	s	k	t	o	p	\	M	o	v	i	e
.	w	m	v															

Image 2 – The File Header

The first eight bytes found in a $I file will be a 01 followed by seven sets of 00. This does not seem to have much value, however as it is present a mention of it has been made.

- 5 - The File Size



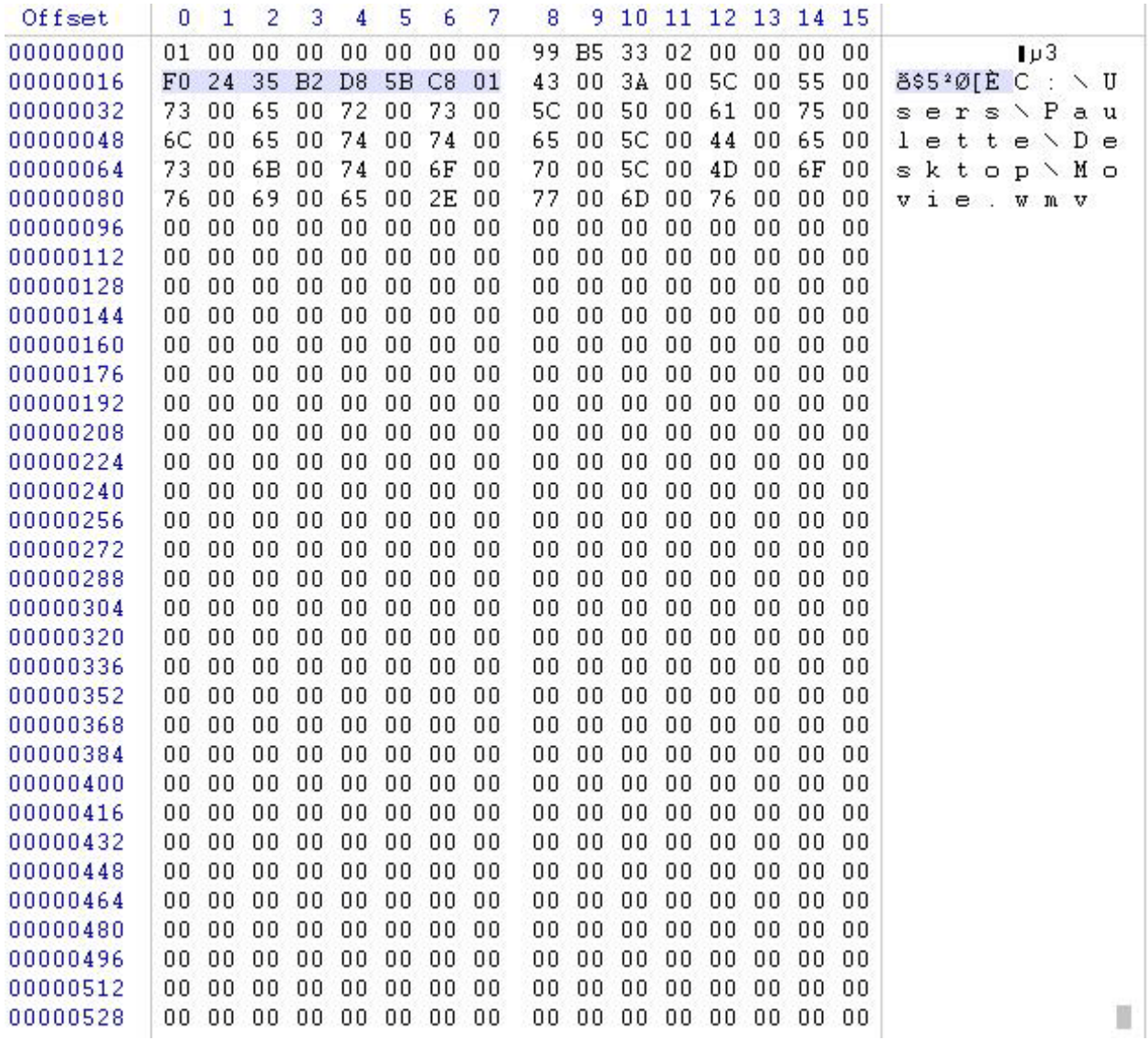
Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
00000000	01	00	00	00	00	00	00	00	99	B5	33	02	00	00	00	00
00000016	F0	24	35	B2	D8	5B	C8	01	43	00	3A	00	5C	00	55	00
00000032	73	00	65	00	72	00	73	00	5C	00	50	00	61	00	75	00
00000048	6C	00	65	00	74	00	74	00	65	00	5C	00	44	00	65	00
00000064	73	00	6B	00	74	00	6F	00	70	00	5C	00	4D	00	6F	00
00000080	76	00	69	00	65	00	2E	00	77	00	6D	00	76	00	00	00
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000144	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
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000304	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
00000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000384	00	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	00
00000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000528	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00

															▮	µ	3	
ð	$	5	²	Ø	[	È	C	:	\	U						
s	e	r	s	\	P	a	u									
l	e	t	t	e	\	D	e									
s	k	t	o	p	\	M	o									
v	i	e	.	w	m	v										

Image 2 – The File Size

The file size is stored in the $I file at offset 0x08 through offset 0x0F. The file size is stored as a hex and needs to be read in reverse if viewing with a hex editor as shown above. The size above is displayed as 99 B5 33 02 00 00 00 00. The proper way to recover the file size out of the file is to reverse the order as to obtain 00 00 00 00 02 33 B5 99. Placing these numbers even into Windows Calculator and converting back to decimal from the hex value gives us 36,943,257 bytes. The information retrieved from the original file matches as 35.2 MB (36,943,257 bytes) was copied from the files properties.

- 6 - Deleted Date and Time Stamp



Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	01	00	00	00	00	00	00	00	99	B5	33	02	00	00	00	00	▮µ3
00000016	F0	24	35	B2	D8	5B	C8	01	43	00	3A	00	5C	00	55	00	ð$5²Ø[È C : \ U
00000032	73	00	65	00	72	00	73	00	5C	00	50	00	61	00	75	00	s e r s \ P a u
00000048	6C	00	65	00	74	00	74	00	65	00	5C	00	44	00	65	00	l e t t e \ D e
00000064	73	00	6B	00	74	00	6F	00	70	00	5C	00	4D	00	6F	00	s k t o p \ M o
00000080	76	00	69	00	65	00	2E	00	77	00	6D	00	76	00	00	00	v i e . w m v
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000144	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	
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000304	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	
00000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000384	00	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	00	
00000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000528	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Image 3 – Delete Date and Time Stamp

It can often become vital for an investigator to know when the file was moved to the Recycle Bin. This information can be found beginning at offset 0x10 and spanning 8 bytes. The date and time stamp highlighted above is F0 24 35 B2 D8 5B C8 01. In this form it is not of much use as it is not in a format that can be easily understood. Windows stores its time stamps in the number of seconds that have elapsed since Midnight, January 1, 1601. An easier way to find the time is to perform the following equation on the value:

File Deleted = 10^-7 * Windows Time - 11644473600

This will then translate the decoded Windows time stamp to the standard UNIX timestamp. A program such as Decode can then be used to find the date and time value of the resulting number. The value in this instance is 01 C8 5B D8 B2 35 24 F0. Using the above formula and pluging the resulting number into Decode the delete date and time are: Mon, 21 January 2008 02:52:44 GMT.

The value of 11644473600 is the number of seconds that have passed between the dates of Midnight January 1, 1601 and Midnight, January 1, 1970. This has been documented by Microsoft in the MSDN references as well as many other sources.

- 7 - Original File Name

Offset	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
00000000	01	00	00	00	00	00	00	00	99	B5	33	02	00	00	00	00	▮ ▮µ3
00000016	F0	24	35	B2	D8	5B	C8	01	43	00	3A	00	5C	00	55	00	ð$5²Ø[È C : \ U
00000032	73	00	65	00	72	00	73	00	5C	00	50	00	61	00	75	00	s e r s \ P a u
00000048	6C	00	65	00	74	00	74	00	65	00	5C	00	44	00	65	00	l e t t e \ D e
00000064	73	00	6B	00	74	00	6F	00	70	00	5C	00	4D	00	6F	00	s k t o p \ M o
00000080	76	00	69	00	65	00	2E	00	77	00	6D	00	76	00	00	00	v i e . w m v
00000096	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000112	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000128	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000144	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	
00000176	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000192	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000208	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000224	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000240	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000256	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000272	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000288	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000304	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	
00000336	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000352	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000368	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000384	00	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	00	
00000416	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000432	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000448	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000464	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000480	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000496	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000512	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000528	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

Image 4 – File Name

The filename is located at offset 0x18 and spans the rest of the information found in the file. The ASCII characters are spaced apart with an empty byte between them. Once the end of the filename is reached the rest of the file is padded with empty bytes until it reaches 544 bytes in length.

- 8 - Conclusion

The following table will re-establish the structure of the $I files that accompany the $R deleted files that are found in the newly structured Windows Vista Recycle Bin directory.

Data Structure	Length in Bytes	Offset to Beginning of Structure
File Header	8 Bytes	0x00
File Size	8 Bytes	From Beginning of File 0x08
File Delete Date and Time	8 Bytes	From Beginning of File 0x10
File Name and Path (Before Being Deleted)	Up To 520 Bytes	From Beginning of File 0x18