

FTK 1.81.6: Deleted Files: Windows 7

June 17, 2011

Richard Crocker

Reviewer:

Dr. Philip Craiger
Kevin Kulbacki

Description:

This test is designed to test Forensic Toolkit 1.81.6 capabilities on the discovery, analysis, and recovery of deleted files and folders from a Windows 7 Evidence Drive. On a separate workstation we created a selection of files and subsequently deleted the files using several different deletion methods including: sending to the Recycle Bin and not emptying, sending to the Recycle Bin and subsequently emptying, Shift-Deletion method. We shut the workstation down and created a forensic duplicate of the evidentiary drive and calculated a hash for the drive. We then imported the image to Forensic Toolkit 1.81.6 and then attempted to locate each file using Forensic Toolkit 1.81.6.

Test Result:

Forensic Toolkit 1.81.6 was able to discover and match (with verified hash values) six of the ten test files. Forensic Toolkit was able to discover all four files that were part of the group of files sent the Recycle Bin but not emptied. It is noteworthy that one file (Wireshark 1.2.8 Intel.dmg) was not represented in the FTK "From Recycle Bin" container; it had to be located via search. Forensic Toolkit was able to recover two of the three files that were members of the group of files that were sent to the Recycle Bin and then emptied. Forensic Toolkit was unable to locate or carve any of the three files from the group that was Shift-deleted.

It is unclear at this point what differentiated the files that were located and those that were not. It is not within the scope of this test to do a bit-level master file table analysis of the test files.

File Name	Located/Hash Match	Found Name	Deleted Process
10.1.1.17.946.pdf	N		Shift-Delete
290719612_5a27cbaf61.jpg	N		Shift-Delete
Photo 18.jpg	Y/Y	\$RJ4MMO3.jpg	Recycle Bin, Emptied
Wireshark 1.2.8 Intel.dmg	Y/Y	\$RPJ39H4.dmg_1	Recycle Bin, Not Emptied
putty.exe	Y/Y	\$R6V9VBY.exe	Recycle Bin, Not Emptied
16036.pdf	N		Shift-Delete
CET4523-Syllabus2.doc	N		Recycle Bin, Emptied
VB6_Graduated_Title_Bar_Sample.zip	Y/Y	\$RWWQ4ZE.zip	Recycle Bin, Not Emptied
drop.avi	Y/Y	\$RTVFDJD.avi	Recycle Bin, Emptied
sample-graphic.gif	Y/Y	\$RI2LH0Z.gif	Recycle Bin, Not Emptied

Configuration of Test Platform:

Workstation 7

Model: Optiplex 620
Dell Service Tag: CQWVJ91
OS Installed: Windows XP-SP3
Date of Install/ dd Imaged: 03/17/2010
md5sum: 1d949e3f9f0808bc337e1b32f571adf5

Win Update Status:
 All Critical Updates
 NO Optional
 All Hardware
Date: 03/16/2010

Drivers Installed: (Brand/Model Version Date)
NIC: Broadcom V8.22.1, A03 06/05
Chipset: Intel 8.0.01009, A18 06/08
Modem: Conexant 1.10, A02 06/05
Video: Intel 945G 6.14.10.4299 06/05

Tool being tested:

Title: FTK
 Manufacturer: AccessData

Version or date: 1.81.6

Notes regarding test data set:

The evidence hard drive attached to the Tableau Write Blocker contains a new copy of Windows 7 with device drivers and Firefox 3.6.3 installed. This hard drive has been populated with evidence data for testing. (*See Evidence Script Document*)

Hard Drive configuration:

Manufacturer: Seagate
Model: Barracuda 7200.10
P/N: 9CY131-313
S/N: 9QZDB9K2
Size: 80 GB

All hash values obtained from Linux distribution Knoppix 5.3.1
(*See Knoppix Script*)

File Detail:

10.1.1.17.946.pdf

Size: 388 KB
Md5 Hash: 6f7cbb66d4971826a07289a7ba8c182c
Deletion Method: Shift - Delete

290719612_5a27cbaf61.jpg

Size: 109 KB
Md5 Hash: 102abdc5268107c7d760c255d92b5937
Deletion Method: Shift - Delete

Photo 18.jpg

Size: 70 KB
Md5 Hash: 27734a42c061f0bc6e44db24a221a462
Deletion Method: Sent to Recycle Bin; Bin emptied

Wireshark 1.2.8 Intel.dmg

Size: 41,488 KB
Md5 Hash: 4e8f07b8527883c4047d416a9264d67f
Deletion Method: Sent to Recycle Bin, not emptied

putty.exe

Size: 444 KB
Md5 Hash: 9bb6826905965c13be1c84cc0ff83f42
Deletion Method: Sent to Recycle Bin, not emptied

16036.pdf

Size: 635 KB
Md5 Hash: 94b83b3b1553af6e0a0879d5d6f3ec30
Deletion Method: Shift - Delete

CET4523-Syllabus2.doc

Size: 27 KB

Md5 Hash: 21098346ed84fc7f4053b0090181c8fd

Deletion Method: Sent to Recycle Bin; Bin emptied

VB6_Graduated Title Bar Sample.zip

Size: 39 KB

Md5 Hash: 0a94f3508b87a22958c1f6fee16cf9a8

Deletion Method: Sent to Recycle Bin, not emptied

drop.avi

Size: 660 KB

Md5 Hash: fa60ba1b78299bfae5ac619e34012052

Deletion Method: Sent to Recycle Bin; Bin emptied

sample-graphic.gif

Size: 4 KB

Md5 Hash: 6df90889977c579779821785a86b4672

Deletion Method: Sent to Recycle Bin, not emptied

Test Notes:

Forensic Toolkit manual version 1.80 page 36 states that the “Deleted Files” tab in the overview window refers to “*Complete files or folders recovered from slack or free space.*”

Page 51 the manual states that the designation of “*del*” in the File List Column refers to a deleted and recovered file.

Page 79 of the manual states that the contents of a file are always added in logical form; that is, they do not include file slack or deleted files. For this test we acquired the entire physical drive in order to avoid this limitation.

Page 121 of the manual states that in the File Source Info window of a particular file includes a marker called “*Deleted*” Forensic Toolkit will indicate a ‘Yes’ or ‘No’ to indicated if a file had been deleted or not.

Page 182 of the manual lists the file types that Forensic Toolkit is capable of carving from slack or free space (i.e. deleted files). Those file types are: AOL/AIM Buddy Lists, BMP, EMF, GIF, HTML, JPEG, OLE and PDF.

Page 306 summarizes how Forensic Toolkit locates and handles deleted files on a NTFS file system (the file system used here):

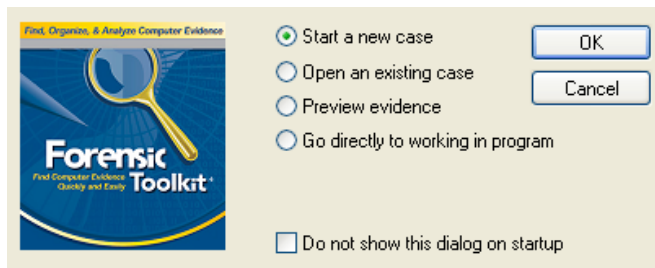
FTK examines the Master File Table (MFT) to find files that are marked deleted because the allocation byte in a record header indicates a deleted file or folder. FTK then recovers the file’s data

using the MFT record's data attribute extent list if the data is non-resident.

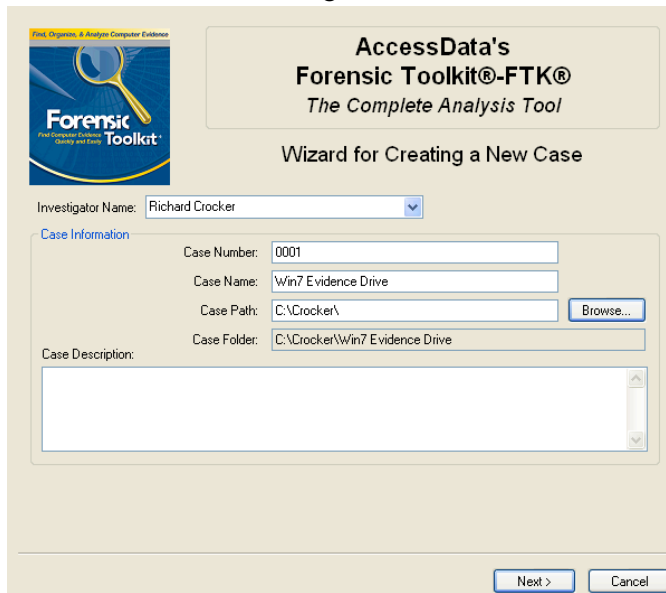
If the deleted file's parent directory exists, the recovered file is shown in the directory where it originally existed. Deleted files whose parent directories were deleted are shown in their proper place as long as their parent directory's MFT entry has not been recycled.

Procedures:

1. Connect FTK dongle to Workstation 7.
2. Connect Windows 7 Evidence drive to Workstation 7 via Tableau Write Blocker.
3. Open FTK.
4. Start new case.



5. Create case number & designate file location



6. Click next

Forensic Examiner Information

The following information will appear on the Case Information page of the report:

Agency/Company:

Examiner's Name:

Address:

Phone: Fax:

E-Mail:

Comments:

< Back Next > Cancel

7. Default logging options, click next

Case Log Options

The case log is a text file named FTK.log in the case folder. It gets created automatically by FTK and contains a record of events that occur during the course of the case. You can choose which type of events you would like to be logged.

You can also add your own comments to the log file at any time by selecting "Add Case Log Entry..." under the "Tools" menu item, and you can view the log file by selecting "View Case Log" under the "Tools" menu item.

Events to go in the Case Log

<input checked="" type="checkbox"/> Case and evidence events	Events related to the addition and processing of file items when evidence is added or when using Analysis Tools later in the case.
<input checked="" type="checkbox"/> Error messages	Events related to any error conditions encountered during the case.
<input checked="" type="checkbox"/> Bookmarking events	Events related to the addition and modification of bookmarks.
<input checked="" type="checkbox"/> Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
<input checked="" type="checkbox"/> Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
<input checked="" type="checkbox"/> Other events	Other events not related to the above, such as copying, viewing, and ignoring files.

< Back Next > Cancel

8. Select Data Carve as an option (Data Carve options default – all selected), click next

Processes to Perform

Evidence is added to a case in several steps. Some of the processes are always performed, while others are optional, depending on your needs and time/resource constraints.

<input checked="" type="checkbox"/> MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to uniquely identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD5 hashes are used by the KFF to identify known files.	
<input checked="" type="checkbox"/> SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.	
<input checked="" type="checkbox"/> KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.	
<input checked="" type="checkbox"/> Entropy Test	For unknown file types, an entropy test is used to determine whether the file's data is compressed or encrypted. Such files contain no plain text and will not be indexed. Unnecessary indexing of such files can waste large amounts of time and resources.	
<input checked="" type="checkbox"/> Full Text Index	The Forensic Toolkit includes a very powerful search engine, dtSearch, which enables the investigator to do instantaneous searching of textual data. In order to take advantage of this search feature, the data must first be indexed.	
<input checked="" type="checkbox"/> Store Thumbnails	Create and store thumbnails for all graphics in the case. This option speeds up browsing through the Graphics view at the expense of consuming more space in the case folder.	
<input checked="" type="checkbox"/> Decrypt EFS Files	Automatically locate and attempt to decrypt EFS encrypted files found on NTFS partitions within the case. (Requires AccessData Password Recovery Toolkit 5.20 or newer)	
<input checked="" type="checkbox"/> File Listing Database	Create a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Preprocessing File Listing Database Column Setting. This database can be recreated with custom column settings in Copy Special.	DB Options
<input type="checkbox"/> HTML File Listing	Create an HTML version of the File Listing.	
<input checked="" type="checkbox"/> Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.	Carving Options
<input type="checkbox"/> Registry Reports	Generate common registry reports during preprocessing.	

[< Back](#)
[Next >](#)
[Cancel](#)

9. Refine Case options left default. Click next.

Refine Case - Default

In order to save time and resources, and/or to eliminate irrelevant data, you may choose to exclude certain kinds of data from the case. Here, you can choose default inclusion/exclusion settings that will apply to each evidence item that gets added to the case. To exclude data, make any changes to the settings below. Note: any items that get excluded will not appear anywhere in the case, and will be inaccessible.

[Include All Items](#)
[Optimal Settings](#)
[Email Emphasis](#)
[Text Emphasis](#)
[Graphics Emphasis](#)

Unconditionally Add

☒ File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)

☒ Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)

☒ KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

☐ Extract files from KFF ignorable containers

Conditionally Add

Add other items to the case only if they satisfy BOTH the file status and the file type criteria

File Status Criteria			File Type Criteria	
Deletion Status:	Encryption Status:	Email Status:	<input checked="" type="checkbox"/> Documents	<input checked="" type="checkbox"/> Executables
<input type="radio"/> Deleted	<input type="radio"/> Encrypted	<input type="radio"/> From email	<input checked="" type="checkbox"/> Spreadsheets	<input checked="" type="checkbox"/> Archives
<input type="radio"/> Not deleted	<input type="radio"/> Not encrypted	<input type="radio"/> Not from email	<input checked="" type="checkbox"/> Databases	<input checked="" type="checkbox"/> Folders
<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="checkbox"/> Graphics	<input checked="" type="checkbox"/> Other Known
<input checked="" type="checkbox"/> Include Duplicate Files	<input checked="" type="checkbox"/> OLE Streams		<input checked="" type="checkbox"/> Multimedia	<input checked="" type="checkbox"/> Unknown
			<input checked="" type="checkbox"/> Email msgs	

[< Back](#)
[Next >](#)
[Cancel](#)

10. Refine Index options left default, click next

Add Evidence

Any number of evidence items can be added to the case. There are several types of evidence items:

- Acquired image of drive: Several formats supported; can be an image of a logical or physical drive
- Local drive: Can be a logical or physical drive
- Folder: Adds all files in the specified folder, including contents of subfolders
- Individual File: Adds a single file. NOTE: Disk image files should be added as acquired images.

The default refinement options, set previously, can be overridden independently for each evidence item, and additional types of refinements can also be made. These refinements can include the exclusion of date/size ranges, as well as specific folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced...

Add Evidence...
Edit Evidence...
Remove Evidence
Refine Evidence - Advanced...

Display Name	Source	Name/N...	Type	Refined	Time Zone	Comment
Win7 Evidence Drive\Part...	Disk1		NTFS	N	N/A	
Win7 Evidence Drive\Part...	Disk1		NTFS	N	N/A	
Win7 Evidence Drive\Unp...	Disk1		Unpartition...	N	N/A	

< Back
Next >
Cancel

13. Click Finish.

New Case Setup is Now Complete

Case Settings

Case directory where the file database, index, and other case-specific files will be stored:

C:\Crocker\Win7 Evidence Drive

Number of Evidence Items: 3

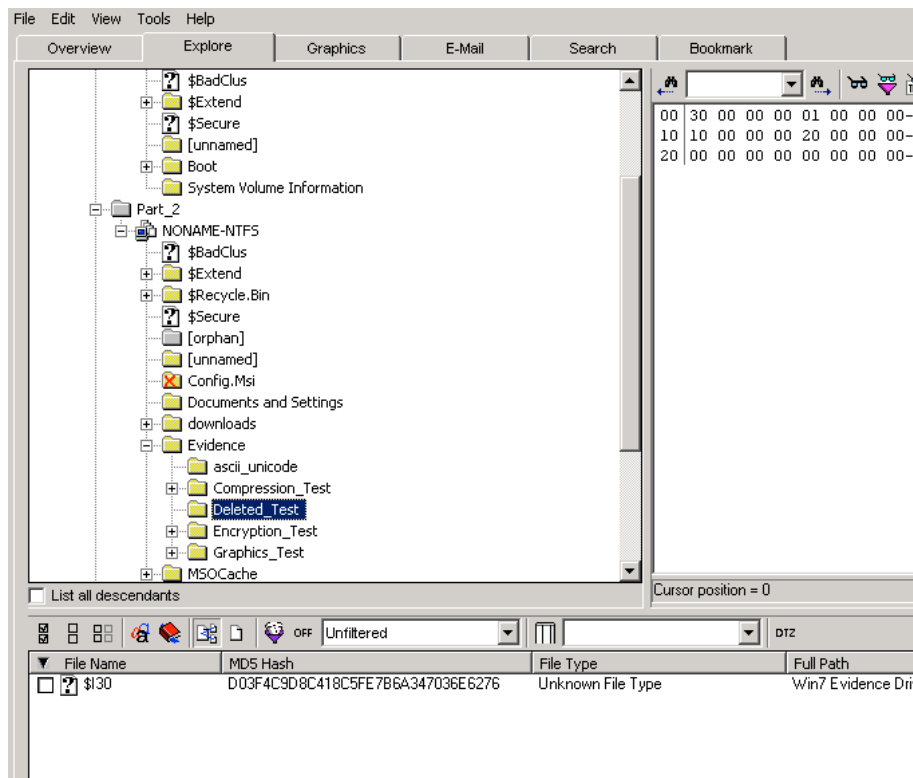
Processes to be Performed:

File Extraction:	Yes	Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.
File Identification:	Yes	
MD5 Hash:	Yes	
SHA1 Hash:	Yes	
KFF Lookup:	Yes	
Entropy Test:	Yes	Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.
Full Text Index:	Yes	
Store Thumbnails:	Yes	
Decrypt EFS Files:	Yes	
File Listing Database:	Yes	
File Listing HTML:	No	
Data Carving:	No	
Registry Reports:	No	

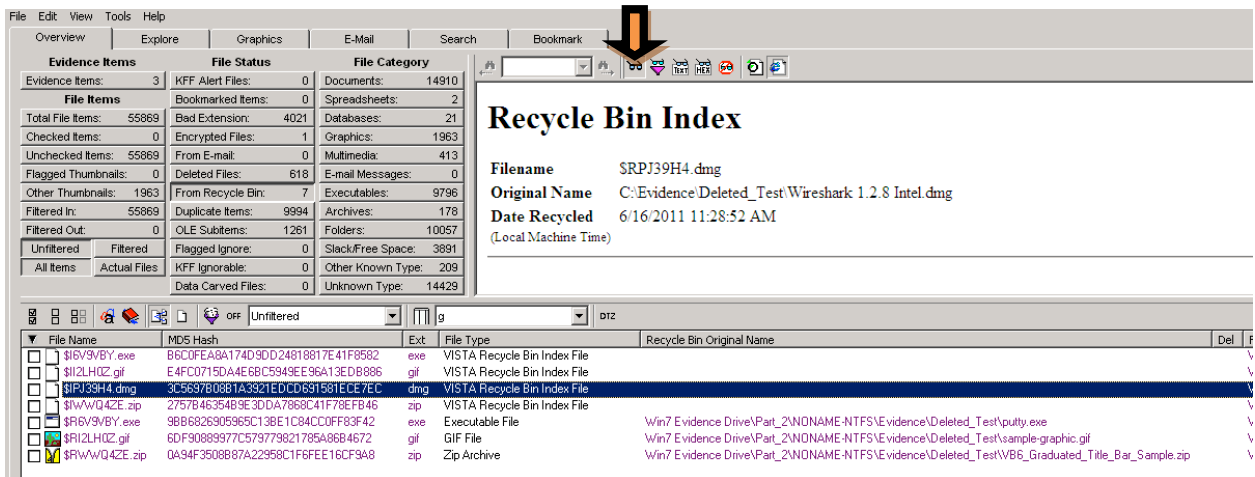
Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence

< Back
Finish
Cancel

14. Navigate to the Forensic Toolkit Explore tab, expand the Evidence\Deleted_Test folder.
Note: None of our test files are located in this folder.



15. Navigate to the Forensic Toolkit Overview Tab and select “From Recycle Bin”.



Listed below is the Index listing of each file found in the From Recycle Bin tab in Forensic Toolkit.

16. The file **\$IPJ39H4.dmg** identifies itself as an index or pointer file to the original file **Wireshark 1.2.8 Intel.dmg**, that has now been renamed **\$RPJ39H4.dmg**. The hash of this particular file **3C5697B08B1A3921EDCD691581ECE7EC** does not match the original known hash of **4e8f07b8527883c4047d416a9264d67f**.

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	3	KFF Alert Files:	0	Documents:	14910
File Items		Bookmarked Items:	0	Spreadsheets:	2
Total File Items:	55869	Bad Extension:	4021	Databases:	21
Checked Items:	0	Encrypted Files:	1	Graphics:	1963
Unchecked Items:	55869	From E-mail:	0	Multimedia:	413
Flagged Thumbnails:	0	Deleted Files:	618	E-mail Messages:	0
Other Thumbnails:	1963	From Recycle Bin:	7	Executables:	9796
Filtered In:	55869	Duplicate Items:	9994	Archives:	178
Filtered Out:	0	OLE Subitems:	1261	Folders:	10057
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	3891
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	209
		Data Carved Files:	0	Unknown Type:	14429

Recycle Bin Index

Filename: \$RPJ39H4.dmg
 Original Name: C:\Evidence\Deleted_Test\Wireshark 1.2.8 Intel.dmg
 Date Recycled: 6/16/2011 11:28:52 AM
 (Local Machine Time)

File Name	MD5 Hash	Ext	File Type	Recycle Bin Original Name	Del
\$I6V9VBVY.exe	B6C0FEA8A174D9DD24818817E41F8582	exe	VISTA Recycle Bin Index File		
\$I12LH0Z.gif	E4FC0715DA4E6BC5949EE96A13EDB886	gif	VISTA Recycle Bin Index File		
\$RPJ39H4.dmg	3C5697808B1A3921EDCD691581ECE7EC	dmg	VISTA Recycle Bin Index File		
\$IvVQ4ZE.zip	2757B4635489E3DDA7868C41F78EFB45	zip	VISTA Recycle Bin Index File		
\$I6V9VBVY.exe	9BB6826905965C13BE1C84C0FF83F42	exe	Executable File	Win7 Evidence Drive\Part_2\NNAME-NTFS\Evidence\Deleted_Test\putty.exe	
\$I12LH0Z.gif	6DF90889977C579779821795A8684672	gif	GIF File	Win7 Evidence Drive\Part_2\NNAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif	
\$IvVQ4ZE.zip	0A34F350887A22959C1F6FEE16CF3A8	zip	Zip Archive	Win7 Evidence Drive\Part_2\NNAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip	

The new target file **\$RPJ39H4.dmg** does not exist in this window. If you will select Forensic Toolkit's Search tab, add the search term "**\$RPJ39H4.dmg**", select Add, then View Cumulative Results. You will notice that Forensic Toolkit locates a file with the name **\$RPJ39H4.dmg_1** this file has a hash value of **4E8F07B8527883C4047D416A9264D67F** that matches the original files (**Wireshark 1.2.8 Intel.dmg**) known hash value exactly.

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Indexed Search | Live Search

Search Term: Add Import Options

Indexed Words | Co... | Search Items | Hits | Files

Edit Item Remove Item Remove All View Item Results >

Cumulative operator: AND OR View Cumulative Results >

26 Hits in 6 Files - QUERY: (\$RPJ39H4.dmg)

- 10 Hits - [\$LogFile_1] Win7 Evidence Drive\Part_2\NNAME-NTFS\LogFile_1
- 8 Hits - [\$1] Win7 Evidence Drive\Part_2\NNAME-NTFS\Extend\UsnJrnl\1
- 2 Hits - [\$130] Win7 Evidence Drive\Part_2\NNAME-NTFS\Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000\130
- 2 Hits - [\$RPJ39H4.dmg_2] Win7 Evidence Drive\Part_2\NNAME-NTFS\Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000
- 2 Hits - [\$RPJ39H4.dmg_1] Win7 Evidence Drive\Part_2\NNAME-NTFS\Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000
- 2 Hits - [\$IP39H4.dmg] Win7 Evidence Drive\Part_2\NNAME-NTFS\Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000

pDDEDDDD
FUUV
odkX
yAih
VUC

File Name	MD5 Hash	Full Path	Recycle Bin...	Ext
\$130	AD2E0EAD689F68D374EFC20E9A0314C9	Win7 Evidence Drive\Part_2\NNAME-NTFS\Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000\130		
\$RPJ39H4.dmg	3C5697808B1A3921EDCD691581ECE7EC	Win7 Evidence Drive\Part_2\NNAME-NTFS\Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000\RPJ39H4.dmg		dmg
\$J	B98ED9245F4AB84932A06C5E70A9873	Win7 Evidence Drive\Part_2\NNAME-NTFS\Extend\UsnJrnl\1		
\$LogFile_1	6549186DB880BE533186232A683311C1	Win7 Evidence Drive\Part_2\NNAME-NTFS\LogFile_1		
\$RPJ39H4.dmg_1	4E8F07B8527883C4047D416A9264D67F	Win7 Evidence Drive\Part_2\NNAME-NTFS\Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000\RPJ39H4.dmg_1		dmg
\$RPJ39H4.dmg_2	00000000000000000000000000000000	Win7 Evidence Drive\Part_2\NNAME-NTFS\Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000\RPJ39H4.dmg_2		dmg

Hence, even though **Wireshark 1.2.8 Intel.dmg** was not represented in the "From Recycle Bin" section of Forensic Toolkit the file was easily located using the Index files.

This file is a member of the file group that was added to the Recycle Bin but was not emptied.

- The file **\$I6V9VBVY.exe** identifies itself as an index or pointer file to the original file **putty.exe**, that has now been renamed **\$R6V9VBVY.exe**. The hash of this particular file **B6C0FEA8A174D9DD24818817E41F8582** does not match the original known hash of file **putty.exe** (9bb6826905965c13be1c84cc0ff83f42).

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items 3 KFF Alert Files: 0 Documents: 14910

File Items

Total File Items: 55869 Bookmarked Items: 0 Spreadsheets: 2

Checked Items: 0 Encrypted Files: 1 Graphics: 1963

Unchecked Items: 55869 From E-mail: 0 Multimedia: 413

Flagged Thumbnails: 0 Deleted Files: 618 E-mail Messages: 0

Other Thumbnails: 1963 From Recycle Bin: 7 Executables: 9796

Filtered In: 55869 Duplicate Items: 9994 Archives: 178

Filtered Out: 0 OLE Subitems: 1261 Folders: 10057

Unfiltered Filtered Flagged Ignore: 0 Slack/Free Space: 3891

All Items Actual Files KFF Ignorable: 0 Other Known Type: 209

Data Carved Files: 0 Unknown Type: 14429

Recycle Bin Index

Filename: **\$R6V9VBY.exe**

Original Name: C:\Evidence Deleted_Test\putty.exe

Date Recycled: 6/16/2011 11:28:52 AM
(Local Machine Time)

File Name	MD5 Hash	Ext	File Type	Recycle Bin Original Name	Del	F
\$I6V9VBY.exe	B6C0FEA8A174D9DD24818817E41F8582	exe	VISTA Recycle Bin Index File			
\$I12LH0Z.gif	E4FC0715DA4E6BC5949EE96A13EDB886	gif	VISTA Recycle Bin Index File			
\$IPJ39H4.dmg	3C5637B08B1A3921EDCD691581CE7EC	dmg	VISTA Recycle Bin Index File			
\$IwWQ4ZE.zip	2757B4635489E30DA7868C41F78FB46	zip	VISTA Recycle Bin Index File			
\$R6V9VBY.exe	9BB6826905965C13BE1C84CC0FF83F42	exe	Executable File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\putty.exe		
\$RI2LH0Z.gif	6DF90889977C579779821785A86B4672	gif	GIF File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif		
\$RWwQ4ZE.zip	0A34F3508B87A22958C1F6FEE16CF9A8	zip	Zip Archive	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip		

The new target file **\$R6V9VBY.exe** is found in this From Recycle Bin view. The hash value of file **\$R6V9VBY.exe** is **9BB6826905965C13BE1C84CC0FF83F42**. This hash value matches exactly the known hash value of file **putty.exe** (9bb6826905965c13be1c84cc0ff83f42).

This file is a member of the file group that was added to the Recycle Bin but was not emptied.

File Edit View Tools Help

Overview Explore Graphics E-Mail Search Bookmark

Evidence Items 3 KFF Alert Files: 0 Documents: 14910

File Items

Total File Items: 55869 Bookmarked Items: 0 Spreadsheets: 2

Checked Items: 0 Encrypted Files: 1 Graphics: 1963

Unchecked Items: 55869 From E-mail: 0 Multimedia: 413

Flagged Thumbnails: 0 Deleted Files: 618 E-mail Messages: 0

Other Thumbnails: 1963 From Recycle Bin: 7 Executables: 9796

Filtered In: 55869 Duplicate Items: 9994 Archives: 178

Filtered Out: 0 OLE Subitems: 1261 Folders: 10057

Unfiltered Filtered Flagged Ignore: 0 Slack/Free Space: 3891

All Items Actual Files KFF Ignorable: 0 Other Known Type: 209

Data Carved Files: 0 Unknown Type: 14429

Error
A viewer for this format is not currently available.

File Name	MD5 Hash	Ext	File Type	Recycle Bin Original Name	Del	Fu
\$I6V9VBY.exe	B6C0FEA8A174D9DD24818817E41F8582	exe	VISTA Recycle Bin Index File			
\$I12LH0Z.gif	E4FC0715DA4E6BC5949EE96A13EDB886	gif	VISTA Recycle Bin Index File			
\$IPJ39H4.dmg	3C5637B08B1A3921EDCD691581CE7EC	dmg	VISTA Recycle Bin Index File			
\$IwWQ4ZE.zip	2757B4635489E30DA7868C41F78FB46	zip	VISTA Recycle Bin Index File			
\$R6V9VBY.exe	9BB6826905965C13BE1C84CC0FF83F42	exe	Executable File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\putty.exe		
\$RI2LH0Z.gif	6DF90889977C579779821785A86B4672	gif	GIF File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif		
\$RWwQ4ZE.zip	0A34F3508B87A22958C1F6FEE16CF9A8	zip	Zip Archive	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip		

18. The file **\$I12LH0Z.gif** identifies itself as an index or pointer file to the original file **sample-graphic.gif**, that has now been renamed **\$RI2LH0Z.gif**. The hash of this particular file **E4FC0715DA4E6BC5949EE96A13EDB886** does not match the original known hash of file **sample-graphic.gif** (6df90889977c579779821785a86b4672).

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	3	KFF Alert Files:	0	Documents:	14910
File Items		Bookmarked Items:	0	Spreadsheets:	2
Total File Items:	55869	Bad Extension:	4021	Databases:	21
Checked Items:	0	Encrypted Files:	1	Graphics:	1963
Unchecked Items:	55869	From E-mail:	0	Multimedia:	413
Flagged Thumbnails:	0	Deleted Files:	618	E-mail Messages:	0
Other Thumbnails:	1963	From Recycle Bin:	7	Executables:	9796
Filtered In:	55869	Duplicate Items:	9994	Archives:	178
Filtered Out:	0	OLE Subitems:	1261	Folders:	10057
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	3891
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	209
		Data Carved Files:	0	Unknown Type:	14429

Recycle Bin Index

Filename: **\$RI2LH0Z.gif**
 Original Name: C:\Evidence\Deleted_Test\sample-graphic.gif
 Date Recycled: 6/16/2011 11:28:52 AM
 (Local Machine Time)

File Name	MDS Hash	Ext	File Type	Recycle Bin Original Name	Del	Full
\$I6V9VB.Y.exe	B6C0FEA8A174D9DD24818817E41F8582	exe	VISTA Recycle Bin Index File			Win7 Evidence Drive\Part_2\NODNAME-NTFS\Evidence\Deleted_Test\putty.exe
\$I12LH0Z.gif	E4FC0715DA4E68C5949EE96A13EDB886	gif	VISTA Recycle Bin Index File			Win7 Evidence Drive\Part_2\NODNAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif
\$IPJ39H4.dmg	3C5697B0881A3921EDCD691581ECE7EC	dmg	VISTA Recycle Bin Index File			Win7 Evidence Drive\Part_2\NODNAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip
\$IWVWQ4ZE.zip	2757B46354B9E3DDA7868C41F78EFB46	zip	VISTA Recycle Bin Index File			
\$R6V9VB.Y.exe	98B6826905965C138E1C84C0FF83F42	exe	Executable File			
\$RI2LH0Z.gif	6DF90889977C579779821785A86B4672	gif	GIF File			
\$RWVWQ4ZE.zip	0A94F3508B87A22958C1F6FEE16CF9A8	zip	Zip Archive			

The new target file **\$RI2LH0Z.gif** is found in this From Recycle Bin view. The hash value of file **\$RI2LH0Z.gif** is **6DF90889977C579779821785A86B4672**. This hash value matches exactly the known hash value of file **sample-graphic.gif** (6df90889977c579779821785a86b4672).

This file is a member of the file group that was added to the Recycle Bin but was not emptied.

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Evidence Items		File Status		File Category	
Evidence Items:	3	KFF Alert Files:	0	Documents:	14910
File Items		Bookmarked Items:	0	Spreadsheets:	2
Total File Items:	55869	Bad Extension:	4021	Databases:	21
Checked Items:	0	Encrypted Files:	1	Graphics:	1963
Unchecked Items:	55869	From E-mail:	0	Multimedia:	413
Flagged Thumbnails:	0	Deleted Files:	618	E-mail Messages:	0
Other Thumbnails:	1963	From Recycle Bin:	7	Executables:	9796
Filtered In:	55869	Duplicate Items:	9994	Archives:	178
Filtered Out:	0	OLE Subitems:	1261	Folders:	10057
Unfiltered	Filtered	Flagged Ignore:	0	Slack/Free Space:	3891
All Items	Actual Files	KFF Ignorable:	0	Other Known Type:	209
		Data Carved Files:	0	Unknown Type:	14429

Sample

File Name	MDS Hash	Ext	File Type	Recycle Bin Original Name	Del	Full
\$I6V9VB.Y.exe	B6C0FEA8A174D9DD24818817E41F8582	exe	VISTA Recycle Bin Index File			Win7 Evidence Drive\Part_2\NODNAME-NTFS\Evidence\Deleted_Test\putty.exe
\$I12LH0Z.gif	E4FC0715DA4E68C5949EE96A13EDB886	gif	VISTA Recycle Bin Index File			Win7 Evidence Drive\Part_2\NODNAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif
\$IPJ39H4.dmg	3C5697B0881A3921EDCD691581ECE7EC	dmg	VISTA Recycle Bin Index File			Win7 Evidence Drive\Part_2\NODNAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip
\$IWVWQ4ZE.zip	2757B46354B9E3DDA7868C41F78EFB46	zip	VISTA Recycle Bin Index File			
\$R6V9VB.Y.exe	98B6826905965C138E1C84C0FF83F42	exe	Executable File			
\$RI2LH0Z.gif	6DF90889977C579779821785A86B4672	gif	GIF File			
\$RWVWQ4ZE.zip	0A94F3508B87A22958C1F6FEE16CF9A8	zip	Zip Archive			

- The file **\$IWVWQ4ZE.zip** identifies itself as an index or pointer file to the original file **VB6_Graduated_Title_Bar_Sample.zip**, that has now been renamed **\$RWVWQ4ZE.zip**. The hash of this particular file **2757B46354B9E3DDA7868C41F78EFB46** does not match the original known hash of file **VB6_Graduated_Title_Bar_Sample.zip** (0a94f3508b87a22958c1f6fee16cf9a8).

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Evidence Items	File Status	File Category
Evidence Items: 3	KFF Alert Files: 0	Documents: 14910
File Items	Bookmarked Items: 0	Spreadsheets: 2
Total File Items: 55869	Bad Extension: 4021	Databases: 21
Checked Items: 0	Encrypted Files: 1	Graphics: 1963
Unchecked Items: 55869	From E-mail: 0	Multimedia: 413
Flagged Thumbnails: 0	Deleted Files: 618	E-mail Messages: 0
Other Thumbnails: 1963	From Recycle Bin: 7	Executables: 9796
Filtered In: 55869	Duplicate Items: 9994	Archives: 178
Filtered Out: 0	OLE Subitems: 1261	Folders: 10057
Unfiltered	Flagged Ignore: 0	Slack/Free Space: 3891
All Items	KFF Ignorable: 0	Other Known Type: 209
	Data Carved Files: 0	Unknown Type: 14429

Recycle Bin Index

Filename **\$RWWQ4ZE.zip**

Original Name C:\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip

Date Recycled 6/16/2011 11:28:52 AM
(Local Machine Time)

File Name	MDS Hash	Ext	File Type	Recycle Bin Original Name	Del	Fu
\$I6V9VB.Y.exe	B6C0FEA8A174D9DD24818817E41F8582	exe	VISTA Recycle Bin Index File			
\$I12LH0Z.gif	E4FC0715DA4E68C5949EE96A13EDB886	gif	VISTA Recycle Bin Index File			
\$I1J39H4.dmg	3C5697B08B1A3921EDCD691581ECE7EC	dmg	VISTA Recycle Bin Index File			
\$RWWQ4ZE.zip	2757B4635489E3DDA7868C41F78EFB46	zip	VISTA Recycle Bin Index File			
\$R6V9VB.Y.exe	9BB6826905965C138E1C84CC0FF83F42	exe	Executable File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\putty.exe		
\$R12LH0Z.gif	6DF90889977C579779821785A86B4672	gif	GIF File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif		
\$RWWQ4ZE.zip	0A94F3508B87A22958C1F6FEE16CF9A8	zip	Zip Archive	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip		

The new target file **\$RWWQ4ZE.zip** is found in this From Recycle Bin view. The hash value of file **\$RWWQ4ZE.zip** is **0A94F3508B87A22958C1F6FEE16CF9A8**. This hash value matches exactly the known hash value of file **VB6_Graduated_Title_Bar_Sample.zip** (0a94f3508b87a22958c1f6fee16cf9a8).

This file is a member of the file group that was added to the Recycle Bin but was not emptied.

File Edit View Tools Help

Overview | Explore | Graphics | E-Mail | Search | Bookmark

Evidence Items	File Status	File Category
Evidence Items: 3	KFF Alert Files: 0	Documents: 14910
File Items	Bookmarked Items: 0	Spreadsheets: 2
Total File Items: 55869	Bad Extension: 4021	Databases: 21
Checked Items: 0	Encrypted Files: 1	Graphics: 1963
Unchecked Items: 55869	From E-mail: 0	Multimedia: 413
Flagged Thumbnails: 0	Deleted Files: 618	E-mail Messages: 0
Other Thumbnails: 1963	From Recycle Bin: 7	Executables: 9796
Filtered In: 55869	Duplicate Items: 9994	Archives: 178
Filtered Out: 0	OLE Subitems: 1261	Folders: 10057
Unfiltered	Flagged Ignore: 0	Slack/Free Space: 3891
All Items	KFF Ignorable: 0	Other Known Type: 209
	Data Carved Files: 0	Unknown Type: 14429

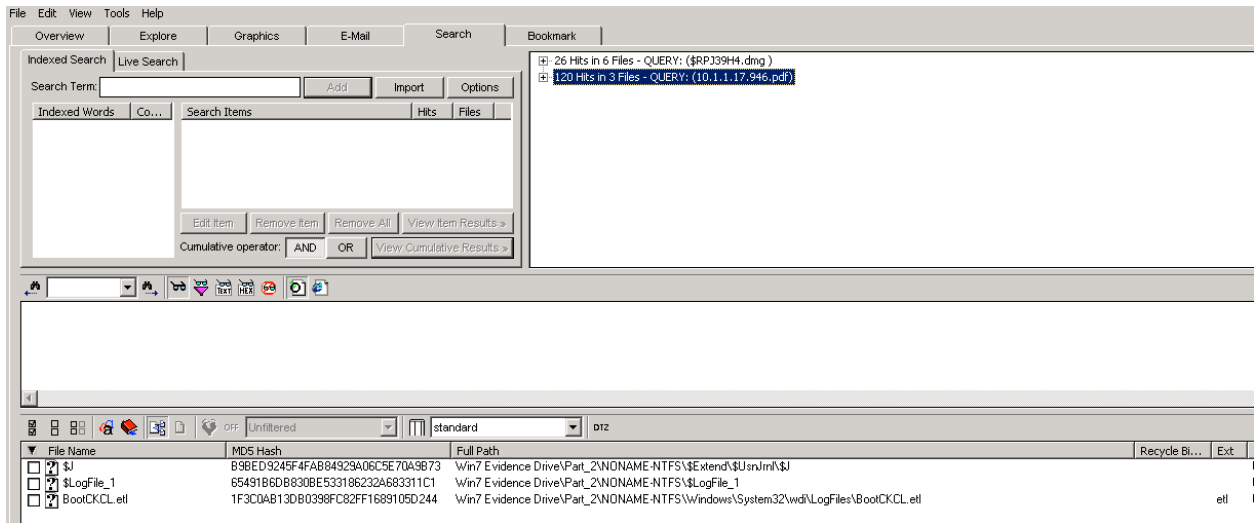
Name	Size	Modified	Comment
\$RWWQ4ZE.zip			
cTitleBar.cls	35,358	11/22/2002 5:34 PM	
fNonMDITest.frm	5,169	6/18/98 11:50 PM	
fNonMDITest.frx	106	6/18/98 11:50 PM	
fTest.frm	1,230	6/18/98 11:29 PM	
fTest.frx	1,273	6/18/98 11:29 PM	
fToolWindow.frm	2,383	5/24/98 6:43 PM	
gTest6.vbg	64	11/22/2002 5:33 PM	
mTest.frm	3,349	11/22/2002 5:16 PM	

File Name	MDS Hash	Ext	File Type	Recycle Bin Original Name	Del	Fu
\$I6V9VB.Y.exe	B6C0FEA8A174D9DD24818817E41F8582	exe	VISTA Recycle Bin Index File			
\$I12LH0Z.gif	E4FC0715DA4E68C5949EE96A13EDB886	gif	VISTA Recycle Bin Index File			
\$I1J39H4.dmg	3C5697B08B1A3921EDCD691581ECE7EC	dmg	VISTA Recycle Bin Index File			
\$RWWQ4ZE.zip	2757B4635489E3DDA7868C41F78EFB46	zip	VISTA Recycle Bin Index File			
\$R6V9VB.Y.exe	9BB6826905965C138E1C84CC0FF83F42	exe	Executable File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\putty.exe		
\$R12LH0Z.gif	6DF90889977C579779821785A86B4672	gif	GIF File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif		
\$RWWQ4ZE.zip	0A94F3508B87A22958C1F6FEE16CF9A8	zip	Zip Archive	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip		

20. Navigate to the Forensic Toolkit Search Tab and enter **10.1.1.17.946.pdf**, select Add then View Cumulative Results. There are four result files, three of which are are pagfile.sys entries.

No file matching the original contents or original hash value were located by Forensic Toolkit 1.81.6.

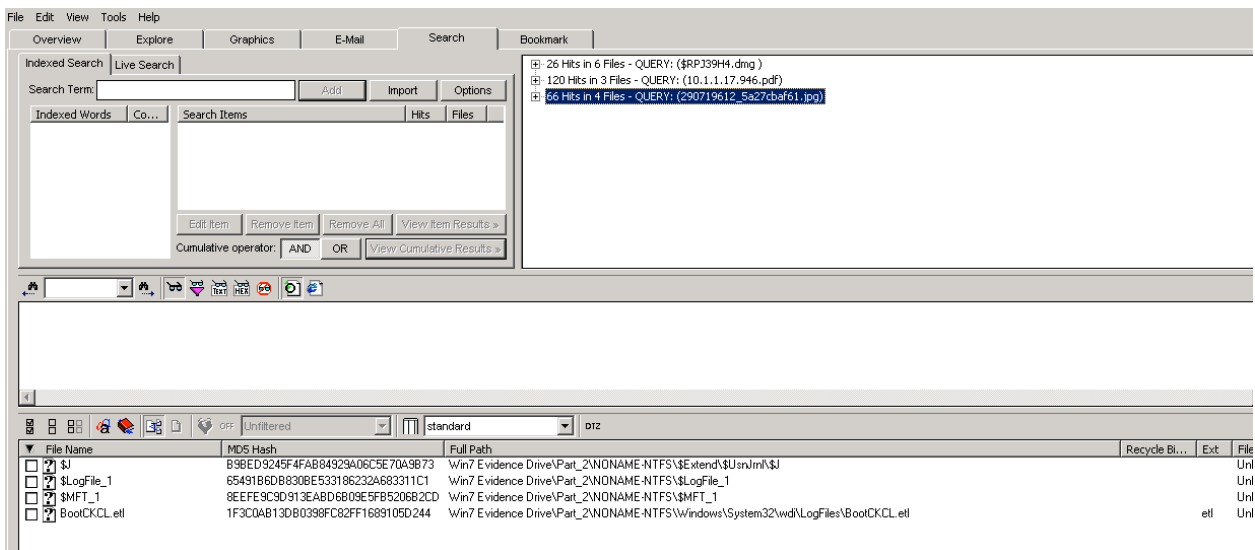
This file is a member of the file group that was Shift-Deleted.



21. Navigate to the Forensic Toolkit Search Tab and enter **290719612_5a27cbaf61.jpg**, select Add then View Cumulative Results. One entry from the Master File Table.

No file matching the original contents or original hash value were located by Forensic Toolkit 1.81.6.

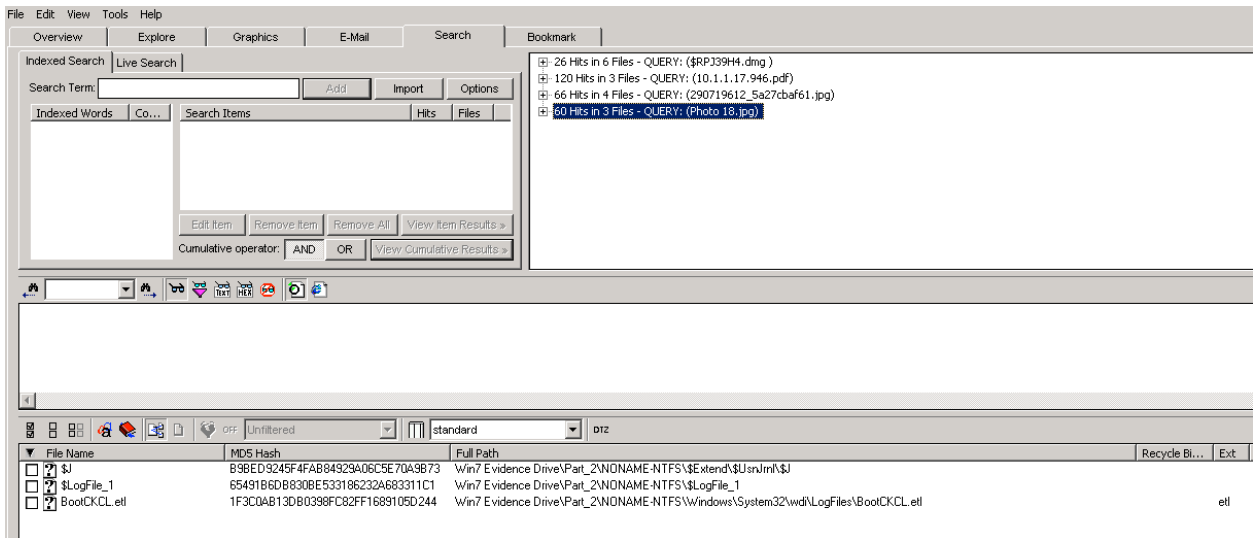
This file is a member of the file group that was Shift-Deleted.



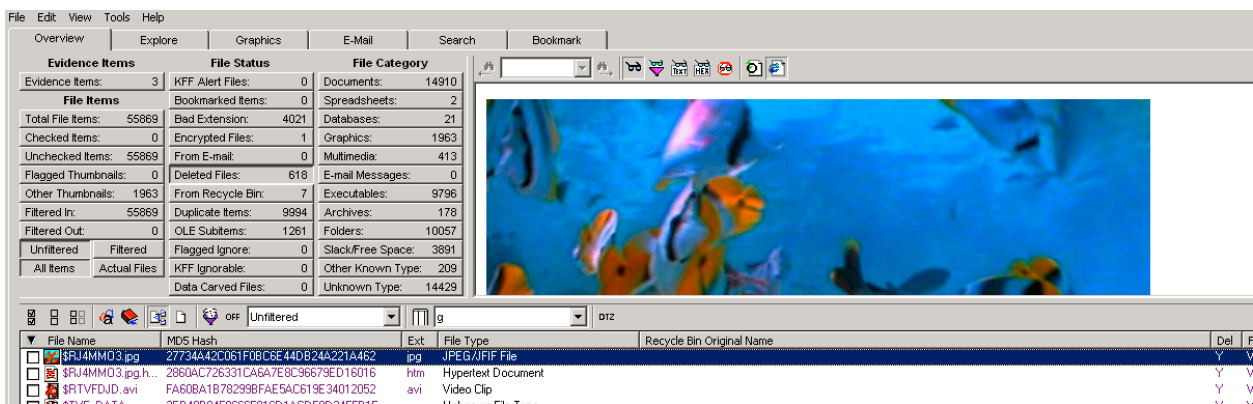
22. Navigate to the Forensic Toolkit Search Tab and enter **Photo 18.jpg**, select Add then View Cumulative Results. All entries are from various log files.

No file matching the original contents or original hash value were located by Forensic Toolkit 1.81.6.

This file is a member of the file group that was sent to the Recycle Bin then Emptied.



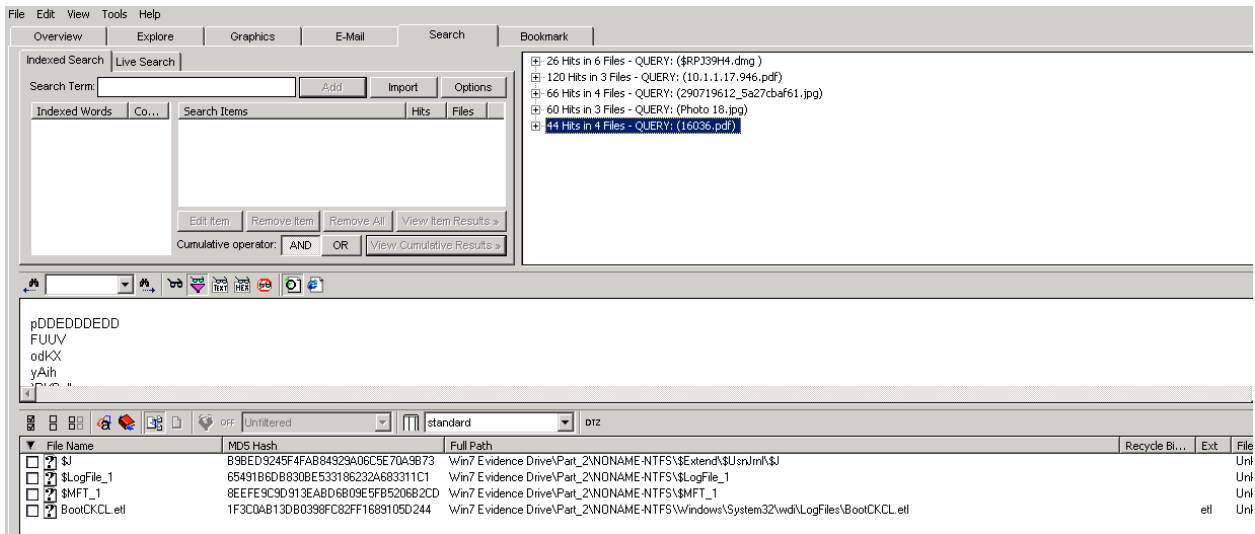
Navigate to the Forensic Toolkit “Overview” tab and select “Deleted Files” you will notice that the file **SRJ4MMO3.jpg** has a hash value of **27734A42C061F0BC6E44DB24A221A462** this matches the known hash value of the target file **Photo 18.jpg** (27734a42c061f0bc6e44db24a221a462). Upon inspection it can be determined that this is indeed our target file.



23. Navigate to the Forensic Toolkit Search Tab and enter **16036.pdf**, select Add then View Cumulative Results. All entries are from various log files.

No file matching the original contents or original hash value were located by Forensic Toolkit 1.81.6.

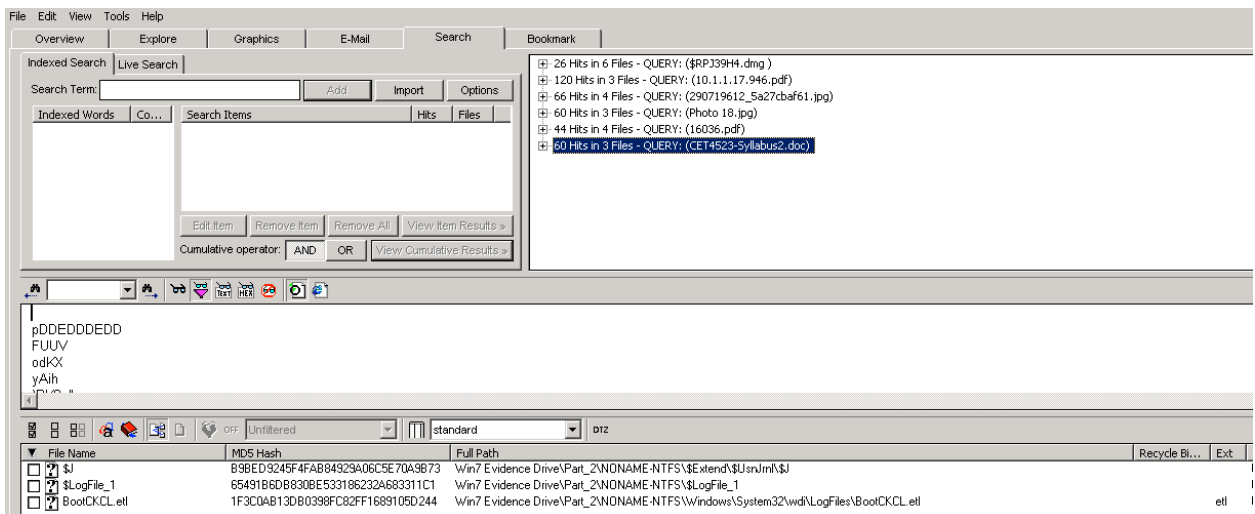
This file is a member of the file group that was Shift-Deleted.



24. Navigate to the Forensic Toolkit Search Tab and enter **CET4523-Syllabus2.doc**, select Add then View Cumulative Results. All entries are from various log files.

No file matching the original contents or original hash value were located by Forensic Toolkit 1.81.6.

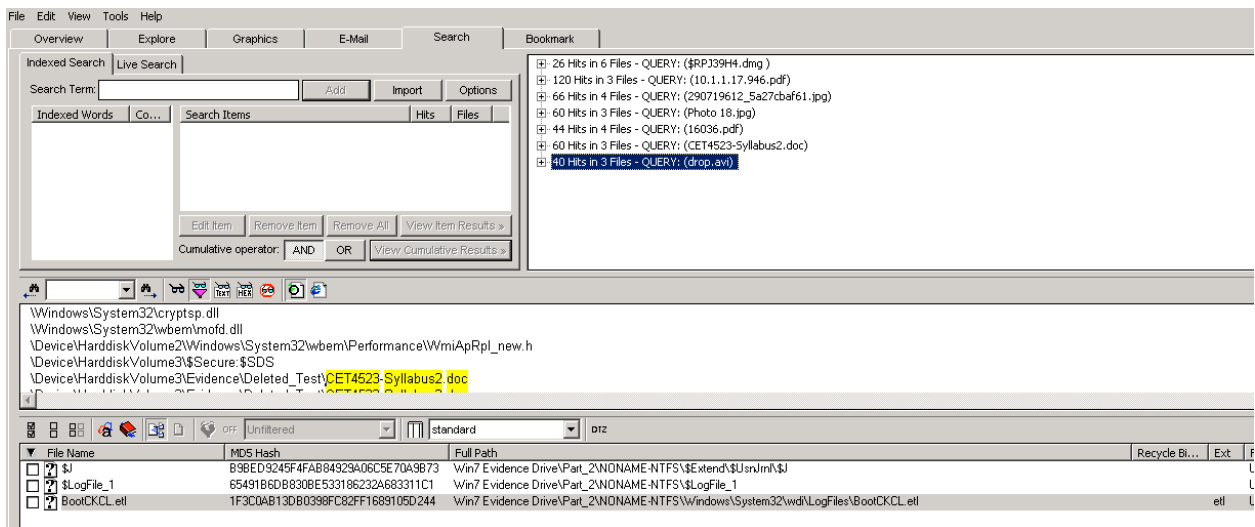
This file is a member of the file group that was sent to the Recycle Bin then Emptied.



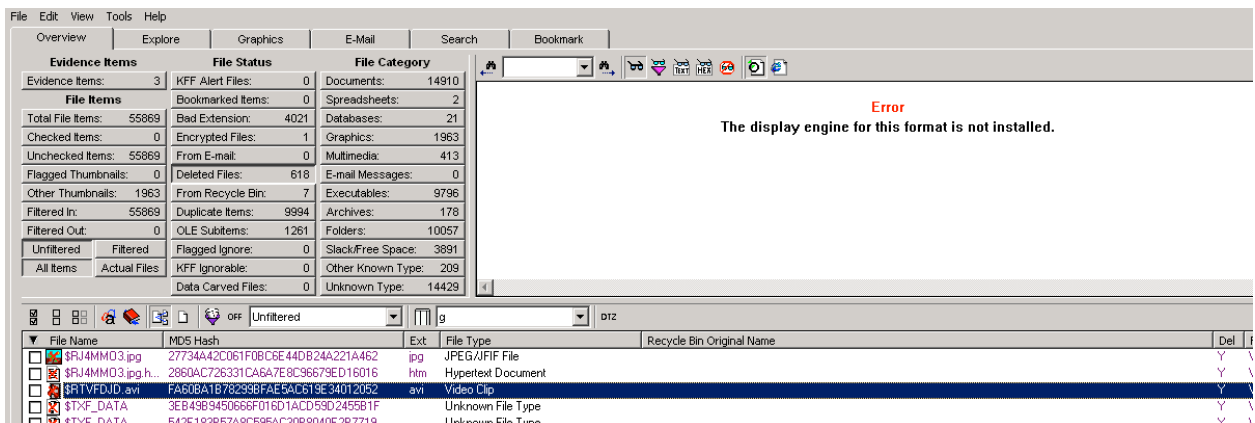
25. Navigate to the Forensic Toolkit Search Tab and enter **drop.avi**, select Add then View Cumulative Results. All entries are from various log files and the Master File Table.

No file matching the original contents or original hash value were located by Forensic Toolkit 1.81.6.

This file is a member of the file group that was sent to the Recycle Bin then Emptied.



Navigate to the Forensic Toolkit “Overview” tab and select “Deleted Files” you will notice that the file **\$RTVFDJD.avi** has a hash value of **FA60BA1B78299BFAE5AC619E34012052** this matches the known hash value of the target file **drop.avi** (fa60ba1b78299bfae5ac619e34012052). Upon inspection it can be determined that this is indeed our target file.



Observations:

The Recycle Bin provides a safety net when deleting files or folders. When you delete any of these items from your hard disk, Windows places it in the Recycle Bin and the Recycle Bin icon changes from empty to full. Items deleted from a floppy disk or a network drive are permanently deleted and are not sent to the Recycle Bin.

Items in the Recycle Bin remain there until you decide to permanently delete them from your computer. These items still take up hard disk space and can be undeleted or restored back to their original location. When it fills up, Windows automatically cleans out enough space in the Recycle Bin to accommodate the most recently deleted files and folders.

Windows allocates one Recycle Bin for each partition or hard disk.

It is possible to remove an item permanently by holding down SHIFT while dragging the item to the Recycle Bin or pressing the SHIFT key and DELETE key simultaneously. Both processes bypass the Recycle Bin.

Results:

Expected Results:

Forensic Toolkit 1.81.6 should be able to discover all deleted files whose master file table entries are still intact and be able to recover all deleted files that have not been overwritten in slack or free space. Forensic Toolkit 1.81.6 should also be able to recover deleted files that have well known signatures (see test notes for a list of file types) as long as they are not fragmented.

Actual Results:

Forensic Toolkit 1.81.6 was able to discover and match (with verified hash values) six of the ten test files. Forensic Toolkit was able to discover all four files that were part of the group of files sent the Recycle Bin but not emptied. It is noteworthy that one file (Wireshark 1.2.8 Intel.dmg) was not represented in the FTK “From Recycle Bin” container; it had to be located via search. Forensic Toolkit was able to recover two of the three files that were members of the group of files that were sent to the Recycle Bin and then emptied. Forensic Toolkit was unable to locate or carve any of the three files from the group that was Shift-deleted.

It is unclear at this point what differentiated the files that were located and those that were not. It is not within the scope of this test to do a bit-level master file table analysis of the test files.

File Name	Located/Hash Match	Found Name	Deleted Process
10.1.1.17.946.pdf	N		Shift-Delete
290719612_5a27cbaf61.jpg	N		Shift-Delete
Photo 18.jpg	Y/Y	\$RJ4MMO3.jpg	Recycle Bin, Emptied
Wireshark 1.2.8 Intel.dmg	Y/Y	\$RPJ39H4.dmg_1	Recycle Bin, Not Emptied
putty.exe	Y/Y	\$R6V9VBY.exe	Recycle Bin, Not Emptied
16036.pdf	N		Shift-Delete

CET4523-Syllabus2.doc	N		Recycle Bin, Emptied
VB6_Graduated_Title_Bar_Sample.zip	Y/Y	\$RWWQ4ZE.zip	Recycle Bin, Not Emptied
drop.avi	Y/Y	\$RTVFDJD.avi	Recycle Bin, Emptied
sample-graphic.gif	Y/Y	\$RI2LH0Z.gif	Recycle Bin, Not Emptied