FTK 1.81.6: Deleted Files: Windows 7

June 17, 2011

<u>Richard Crocker</u>

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 empting, sending to the Recycle Bin and subsequently empting, 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/Has h 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.zi p	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 5a27cba	f61.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	l.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	
10000.041	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_Tit	le_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):

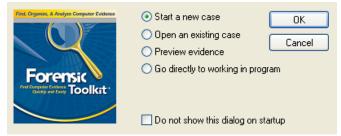
FTK examines the Master File Table (MFT) to find files that are marked deleted because the allocation byte in a record header indicates a deleted file or folder. FTK then recovers the file's data

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

Forensic Tool		AccessData's Forensic Toolkit®-FTK The Complete Analysis Tool Wizard for Creating a New Ca	1
Investigator Name:	Richard Crocker	~	
Case Information	Case Number: Case Name: Case Path: Case Folder:	0001 Win7 E vidence Drive C: \Crocker\ C: \Crocker\Win7 E vidence Drive	Browse
		Next>	Cancel

6. Click next

	aminer Information will appear on the Case Information page of the report:
Agency/Company:	
Examiner's Name	
Address:	
Disease	Fax:
Phone:	
E-Mail:	
Comments:	
	<pre></pre>

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	
Events to go in the Case Log	
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.
Error messages	Events related to any error conditions encountered during the case.
Bookmarking events	Events related to the addition and modification of bookmarks.
Searching events	Events related to searching. All search queries and resulting hit counts will be recorded.
Data carving / Internet searches	Events related to special data carving or internet keyword searches that are performed during the case.
✓ Other events	Other events not related to the above, such as copying, viewing, and ignoring files.
	<pre></pre>

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

		case in several steps. Some of the processes are always performed, while others are option ds and time/resource constraints.
	MD5 Hash	An MD5 hash is a 16 byte value generated based upon a file's content. It is used to unique identify files. Hashes can be used to verify a file's integrity, or to identify duplicate files. MD! hashes are used by the KFF to identify known files.
	🗹 SHA1 Hash	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is n vet as widely used.
	KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, to alert the investigator to known fillior or dangerous files.
	🗹 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.
	🔽 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 th search feature, the data must first be indexed.
	V 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.
	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)
	✔ 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.
	HTML File Listing	Create an HTML version of the File Listing.
	🗹 Data Carve	Automatically find specific file types embedded in other files and from free space. Retrieve results using Data Carving Option on Tools Menu.
1	Registry Reports	Generate common registry reports during preprocessing.

9. Refine Case options left default. Click next.

Refine Case - In order to save time and resources, and/or to eliminate irrelevant dal from the case. Here, you can choose default inclusion/exclusion sett added to the case. To exclude data, make any changes to the settin appear anywhere in the case, and will be inaccessible.	a, you may choose to exclude certain kinds of data ings that will apply to each evidence item that gets				
Include All Items Optimal Settings Email Emphasi	s Text Emphasis Graphics Emphasis				
Unconditionally Add Unconditionally Add File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system) Firee 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 statu File Status Criteria	us and the file type 🖌 criteria				
Deletion Status: Encryption Status: Email Status:	Documents Executables				
O Deleted O Encrypted O From email	Spreadsheets Archives				
Not deleted O Not encrypted O Not from email	✓ Databases ✓ Folders				
 Either Either Either 	Graphics Other Known				
✓ Include Duplicate Files ✓ OLE Streams	 ✓ Multimedia ✓ Unknown ✓ Email msgs 				
	< Back Next > Cancel				

10. Refine Index options left default, click next

In order to save time and resources, and/or to m data from being indexed. Here, you can choose case. To exclude items from being indexed, mak initially can be indexed later by clicking on "Anal	default settings that v e any changes to the	efficient, you may choose will apply to each evidence settings below. Note: ar	ce item that gets added to the			
Unconditionally Index ✓ File Slack (data beyond the end of the logi ✓ Free Space (areas in the file system not cu _ KFF Ignorable Files (files found by KFF to b	rrently allocated to ar	ny file, but possibly contai	ning deleted file data)			
KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., DS system files, known applications, etc.) Conditionally Index Index other items in the case only if they satisfy BOTH the file status and the file type ♥ criteria File Status Criteria Index other items in the case only if they satisfy Deletion Status: Encryption Status: Deleted Encrypted Not deleted Not encrypted Not deleted Not encrypted Either Either Include Duplicate Files OLE Streams						
		< Back	Next > Cancel			

11. Press add Evidence button, add local write-blocked evidence drive (E:), check physical analysis. Click OK. Name Drive Win7 Evidence Drive *logically*. Press Ok.

Select a drive: Physical Drive C Logical Analysis Physical Analysi		
Acquired image o Local drive:	Add Evidence rems can be added to the case. There are several types of evidence i Evidence Information	ical drive
Folder: Individual File: The default refinement op types of refinements can folders. To make these fu	Evidence Location: Disk1 Evidence Display Name:	ers icquired images. attem, and additional anges, as well as specific vidence - Advanced
Add Evidence	Win7 Evidence Drive	vidence - Advanced
Display Name	Evidence Identification Name/Number:	e Zone Comment
	Comment: Local Evidence Time Zone: Choose time zone for evidence	
	OK Cancel	
	< Back	lext > Cancel

12. Click next.

		_			
Ad	2	E 1/		on	C D
nu	u	L V	IU		60

	A	aa	EVIC	lence				
Any number of evidence items	can be added to the	e case	. There a	are several type	s of	eviden	ce items:	
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 all files in the specified folder, including contents of subfolders Hodefault 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 specified folders. To make these further refinements, highlight an evidence item in the list and press Refine Evidence - Advanced								
Add Evidence	Edit Evidence		Remo	ove Evidence		Ref	ine Evidence -	Advanced
Display Name	Source	Nam	ne/N	Туре	R	efined	Time Zone	Comment
Win7 Evidence Drive\Part Win7 Evidence Drive\Part Win7 Evidence Drive\Unp	Disk1 Disk1 Disk1			NTFS NTFS Unpartition	N N N		N/A N/A N/A	
				<	Bac		Next >	Cancel

13. Click Finish.

		3				
Processes	to be Performed:					
	File Extraction:	Yes				
1	File Identification:	Yes	Remember that although each of these processes			
1	MD5 Hash:	Yes	adds to the initial processing time, they each play			
	SHA1 Hash:	Yes	an important role in the investigation process.			
1	KFF Lookup:	Yes	Processes that are not performed initially can be			
1	Entropy Test:	Yes	initiated at a later point in the investigation except			
1	Full Text Index:	Yes	the HTML file listing and automated Registry Reports. Additional evidence can also be added			
	Store Thumbnails:	Yes	later.			
1	Decrypt EFS Files:	Yes				
1	File Listing Database:	Yes				
1	File Listing HTML:	No				
I	Data Carving:	No				
1	Registry Reports:	No				

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.

File	Edit	View	Tools	Help					
	Overv	riew		Explore	Graphics	E-Mail	Search	Bookmark	
² \$BadClus ² \$Extend ² \$Secure ¹ [unnamed] ¹ Boot ¹ System Volume Information									
	List a	i II desce	endants	MSOCache				Cursor position = 0)
	v D		<u> </u>		53. orr. Hafiltavad				DTZ
Ē			<i>(</i> a 愌		🖗 off Unfiltered	•		_	
	File	Name \$130		MD5 H	tash 1C9D8C418C5FE78	364347036E6276	File Type Unknown File Ty	IDe	Full Path Win7 Evidence Dri [.]
	_								

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

File Edit View Tools Hel	þ			
Overview Exp	lore Graphics	E-Mail Sea	earch Bookmark	
Evidence Items	File Status	File Category		
Evidence Items: 3	KFF Alert Files: 0	Documents: 14910		_
File Items	Bookmarked Items: 0	Spreadsheets: 2	2	
Total File Items: 55869	Bad Extension: 4021	Databases: 21	Recycle Bin Index	
Checked Items: 0	Encrypted Files: 1	Graphics: 1963	3	
Unchecked Items: 55869	From E-mail: 0	Multimedia: 413		
Flagged Thumbnails: 0	Deleted Files: 618	E-mail Messages: 0	Filename SRPJ39H4.dmg	
Other Thumbnails: 1963	From Recycle Bin: 7	Executables: 9796	6 Original Name C: Evidence Deleted Test Wireshark 1.2.8 Intel.dmg	
Filtered In: 55869	Duplicate Items: 9994	Archives: 178	B Date Recycled 6/16/2011 11:28:52 AM	
Filtered Out: 0	OLE Subitems: 1261	Folders: 10057		
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free Space: 3891	(Local Machine Fine)	
All Items Actual Files	KFF Ignorable: 0	Other Known Type: 209	9	
	Data Carved Files: 0	Unknown Type: 14429	9	
	🖹 🗋 🤤 off Unfiltered	- -		-
📲 🗄 🔠 🍕 🃚 🖻	,	1.000		_
File Name	MD5 Hash		ile Type Recycle Bin Original Name Del	F
\$16V9VBY.exe	B6C0FEA8A174D9DD248188		ISTA Recycle Bin Index File	N
\$112LHOZ.gif	E4FC0715DA4E6BC5949EE9		ISTA Recycle Bin Index File	<u></u>
SIPJ39H4.dmg	3C5697B08B1A3921EDCD69		ISTA Recycle Bin Index File	1
SIWWQ4ZE.zip	2757B46354B9E3DDA7868C		ISTA Recycle Bin Index File	N
R6V9VBY.exe	9BB6826905965C13BE1C840		xecutable File Win7 Evidence Drive\Part_2\N0NAME-NTFS\Evidence\Deleted_Test\putty.exe	V
🗖 🌇 \$R12LH0Z.gif	6DF90889977C57977982178		IF File Win7 Evidence Drive\Part_2\N0NAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif	N
🗖 M \$RWWQ4ZE.zip	0A94F3508B87A22958C1F6F	EE16CF9A8 zip Zip	ip Archive Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\\V86_Graduated_Title_Bar_Sample.zip	Ň

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 He	lp			
Overview Exp	olore Graphics	E-Mail	Search Bookmark	
Evidence Items	File Status	File Category	· · · · · · · · · · · · · · · · · · ·	
Evidence Items: 3	KFF Alert Files: 0	Documents: 14		
File Items	Bookmarked Items: 0	Spreadsheets:	2	
Total File Items: 55869	Bad Extension: 4021	Databases:	Recycle Bin Index	
Checked Items: 0	Encrypted Files: 1	Graphics: 1		
Unchecked Items: 55869	From E-mail: 0	Multimedia:	113	
Flagged Thumbnails: C	Deleted Files: 618	E-mail Messages:	Filename \$RPJ39H4.dmg	
Other Thumbnails: 1963	From Recycle Bin: 7	Executables: 9	96 Original Name C:\Evidence\Deleted Test\Wireshark 1.2.8 Intel.dmg	
Filtered In: 55869	Duplicate Items: 9994	Archives:	78 Date Recycled 6/16/2011 11:28:52 AM	
Filtered Out: 0	OLE Subitems: 1261	Folders: 10	67	
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free Space: 3	(Local Machine Time) 191	
All Items Actual Files	KFF Ignorable: 0	Other Known Type:	909	
	Data Carved Files: 0	Unknown Type: 14	29	
📓 🗄 🔠 🧟 🃚 🛙	😫 🗋 🐳 off Unfiltered	•		
▼ File Name	MD5 Hash	Ext	File Type Recycle Bin Original Name D	Del F
\$16V9VBY.exe	B6C0FEA8A174D9DD24818		VISTA Recycle Bin Index File	W
🔲 🗖 🚺 \$112LHCZ.gif	E4FC0715DA4E6BC5949EE9		VISTA Recycle Bin Index File	W
SIPJ39H4.dmg	3C5697B08B1A3921EDCD69		VISTA Recycle Bin Index File	W
\$IWWQ4ZE.zip	2757B46354B9E3DDA7868C		VISTA Recycle Bin Index File	.₩
SR6V9VBY.exe	9BB6826905965C13BE1C84		Executable File Win7 Evidence Drive/Part_2VNDNAME-NTFS/Evidence/Deleted_Test/putty.exe	W
🗖 🌇 \$R12LH0Z.gif	6DF90889977C57977982178		GIF File Win7 Evidence Drive\Part_2\NDNAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif	W
🗖 M \$RWWQ4ZE.zip	0A94F3508B87A22958C1F6F	EE16CF9A8 zip	Zip Archive Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip	W

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								
Search Term: Add import Options 6 10 Indexed Words Co Search Items Hits Files 6 2 B 2 B 2 B 2 B 2	Indexed Search Live Search Search Term Add Import Indexed Words Co Search Terms Add Indexed Words Co Search Terms Add Indexed Words Co Search Terms Hits Indexed Words Co Search Terms Add Indexed Words Co Search Terms Hits Indexed Words Co Search Terms Hits							
📲 🗄 🧐 🌪 😫 🗅 💗 orf Unfiltered 💌 🥅 standard 💌	DI2							
▼ File Name MD5 Hash Full Path	Recycle Bi Ext							
Comparison of the second	2NDNAME-NTFS\\$Recycle.Bin\\$-1-5-21-233280506-6686850667-2065063272-1000\\$I30 2NNDNAME-NTFS\\$Recycle.Bin\\$-1-5-21-233280506-686850667-2065063272-1000\\$IPJ39H4.dmg dmg 2 2NNDNAME-NTFS\\$Recycle.Bin\\$-1-5-21-233280506-686850667-2065063272-1000\\$IPJ39H4.dmg dmg 2 2NNDNAME-NTFS\\$Recycle.Bin\\$-1-5-21-233280506-686850667-2065063272-1000\\$IPJ39H4.dmg dmg 2 2NNDNAME-NTFS\\$Recycle.Bin\\$-1-5-21-233280506-686850667-2065063272-1000\\$IPJ39H4.dmg dmg 2 2NNDNAME-NTFS\\$Recycle.Bin\\$-1-5-21-233280506-686850667-2065063272-1000\\$IPJ39H4.dmg dmg 2							
	2\NONAME-NTFS\\$Recycle.Bin\S-1-5-21-293280506-686850667-2065063272-1000\\$RPJ39H4.dmg_1 dmg							
	2\NDNAME-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 \$I6V9VBY.exe identifies itself as an index or pointer file to the original file putty.exe, that has now been renamed \$R6V9VBY.exe. The hash of <u>this</u> particular file B6C0FEA8A174D9DD24818817E41F8582 does not match the original known hash of file putty.exe (9bb6826905965c13be1c84cc0ff83f42).

File Edit View Tools Help			
Overview Explo	re Graphics	E-Mail Se	arch Bookmark
Evidence Items	File Status	File Category	
Evidence Items: 3	KFF Alert Files: 0	Documents: 1491	
File Items	Bookmarked Items: 0		2
Total File Items: 55869	Bad Extension: 4021	Databases: 2'	Recycle Bin Index
Checked Items: 0	Encrypted Files: 1	Graphics: 196	3
Unchecked Items: 55869	From E-mail: 0	Multimedia: 41:	3
Flagged Thumbnails: 0	Deleted Files: 618	E-mail Messages: I	Filename \$R6V9VBY.exe
Other Thumbnails: 1963	From Recycle Bin: 7	Executables: 979	6 Original Name C:\Evidence\Deleted Test\putty.exe
Filtered In: 55869	Duplicate Items: 9994	Archives: 17	B Date Recycled 6/16/2011 11:28:52 AM
Filtered Out: 0	OLE Subitems: 1261	Folders: 1005	
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free Space: 389	
All Items Actual Files	KFF Ignorable: 0	Other Known Type: 20	9
	Data Carved Files: 0	Unknown Type: 1442	a
🛛	🗋 🏺 OFF Unfiltered	• • •	DIZ
🔻 File Name	MD5 Hash	Ext Fi	ile Type Recycle Bin Original Name Del
	B6C0FEA8A174D9DD248188	317E41F8582 exe VI	ISTA Recycle Bin Index File
	E4FC0715DA4E6BC5949EE9		ISTA Recycle Bin Index File
	3C5697B08B1A3921EDCD69		ISTA Recycle Bin Index File
	2757B46354B9E3DDA7868C		ISTA Recycle Bin Index File
	9BB6826905965C13BE1C840		xecutable File Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\putty.exe
	6DF90889977C57977982178		IF File Win7 E vidence Drive/Part_2/NONAME-NTFS/E vidence/Deleted_Test/sample-graphic.gif
🗖 M \$RWWQ4ZE.zip	0A94F3508B87A22958C1F6F	EE16CF9A8 zip Zi	ip Archive Win7 Evidence Drive\Part_2\NDNAME-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.

Overview Exp	ore Graphics	E-Mail Searc	h Bookmark	
Evidence Items	File Status	File Category	M 1	→
Evidence Items: 3	KFF Alert Files: 0	Documents: 14910		
File Items	Bookmarked Items: 0) Spreadsheets: 2		Error
Total File Items: 55869	Bad Extension: 4021	Databases: 21		
Checked Items: 0	Encrypted Files: 1	Graphics: 1963		A viewer for this format is not currently available.
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	1	
🖁 🗄 🔡 🔏 🃚 🖪	🗈 🗳 🖙 Unfiltered	_ [] g	▼ DT2	
Tile Name	MD5 Hash	Ext File	Туре	Recycle Bin Original Name
\$16V9VBY.exe	B6C0FEA8A174D9DD24818		A Recycle Bin Index File	
1 1 \$10A BAD L'EXE	E 45007455 A 45000504055	96A13EDB886 aif VIST	A Recycle Bin Index File	
🔲 🗋 \$112LH0Z.gif	E4FC0715DA4E6BC5949EE	an iner		
\$112LH0Z.gif	3C5697B08B1A3921EDCD6	91581ECE7EC dmg VIST	A Recycle Bin Index File	
\$II2LH0Z.gif \$IPJ39H4.dmg \$IWWQ4ZE.zip	3C5697B08B1A3921EDCD6 2757B46354B9E3DDA7868	91581ECE7EC dmg VIST C41F78EFB46 zip VIST	A Recycle Bin Index File	
\$112LH0Z.gif	3C5697B08B1A3921EDCD6	91581ECE7EC dmg VIST C41F78EFB46 zip VIST 4CCOFF83F42 exe Exec	A Recycle Bin Index File utable File	Win7 E vidence Drive\Part_2NDNAME.NTFS\Evidence\Deleted_Test\putty.exe Win7 E vidence Drive\Part_2NDNAME.NTFS\Evidence\Deleted_Test\sample-graphic.git

 The file \$II2LH0Z.gif identifies itself as an index or pointer file to the original file samplegraphic.gif, that has now been renamed \$RI2LH0Z.gif. The hash of <u>this</u> particular file E4FC0715DA4E6BC5949EE96A13EDB886 does not match the original known hash of file sample-graphic.gif (6df90889977c579779821785a86b4672).

File Edit View Tools	s Help								
Overview	Explore	Graphic	s I	E-Mail	1	Search	Bookmark		
Evidence Item		File Status	~ 1	File Cate					
		FF Alert Files:			~ ~	910	<u>.n 🔽 n</u>	, 💌 🛱 📾 🔞 🔕 🚳	
Evidence Items:			0	Documents:		_			
File Items		ookmarked Items:	0	Spreadsheets:		2	D 1		
Total File Items:	55869 Ba	ad Extension:	4021	Databases:		21	Kecvcle	Bin Index	
Checked Items:	0 Er	ncrypted Files:	1	Graphics:	1	963	•		
Unchecked Items:	55869 Fr	rom E-mail:	0	Multimedia:		413			
Flagged Thumbnails:	0 De	eleted Files:	618	E-mail Message	es:	0	Filename	\$RI2LH0Z.gif	
Other Thumbnails:	1963 Fr	rom Recycle Bin:	7	Executables:	9	796	Original Name	C:\Evidence\Deleted Test\sample-graphic.gif	
Filtered In:	55869 Du	uplicate Items:	9994	Archives:		178	Date Recycled	6/16/2011 11:28:52 AM	
Filtered Out:	0 0	LE Subiterns:	1261	Folders:	10	057	•		
Unfiltered Filte		lagged Ignore:	0	Slack/Free Spa		891	(Local Machine Time		
All Items Actua		FF lanorable:	0	Other Known 1		209			
		ata Carved Files:	0	Unknown Type		429			
		ata carveu nies.	0	Orikitowiti type	i. 14	423			
📓 🗄 🔠 🍕 🄇	📚 📴 C) 🐳 off Unfit	ered	•		g	▼ D	12	
▼ File Name	MD	5 Hash			Ext	File Typ	De	Recycle Bin Original Name D	Del Fu
\$16V9VBY.ex	ke B60	COFEA8A174D9DD	248188	17E41F8582	exe	VISTA	Recycle Bin Index File		Wi
\$II2LH0Z.gif		CO715DA4E6BC5	949EE9	6A13EDB886	gif	VISTA	Recycle Bin Index File		Wi
🛛 🗖 🕻 \$IPJ39H4.dm		5697B08B1A3921E			dmg		Recycle Bin Index File		Wi
🗌 🗖 🚺 \$1WWQ4ZE.;	zip 275	57B46354B9E3DD/			zip		Recycle Bin Index File		Wi
🛛 🗖 \$R6V9VBY.e		86826905965C13B			exe	Executa		Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\putty.exe	Wi
🔲 🗖 🎇 \$RI2LH0Z.gif		F90889977C57977			gif	GIF File		Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\sample-graphic.glf	Wi
🛛 🗖 🎽 \$RWWQ4ZE	Elzip III 049	94F3508B87A2295	8C1F6F	EE16CF9A8	zip	Zip Arc	hive	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip	Wi

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.

Overview Expl	lore Graphics	E-Mail S	earch Bookmark	
Evidence Items	File Status	File Category	0 0	w ₩ ₩ 89 0 📳
Evidence Items: 3	KFF Alert Files: 0	Documents: 1491		
File Items	Bookmarked Items: 0	Spreadsheets:	2	
Total File Items: 55869	Bad Extension: 4021	Databases: 2	1	
Checked Items: 0	Encrypted Files: 1	Graphics: 196	3	
Unchecked Items: 55869	From E-mail: 0	Multimedia: 41	3	
Flagged Thumbnails: 0	Deleted Files: 618	E-mail Messages:	0	
Other Thumbnails: 1963	From Recycle Bin: 7	Executables: 979	16	
Filtered In: 55869	Duplicate Items: 9994	Archives: 17	8	
Filtered Out: 0	OLE Subiterns: 1261	Folders: 1005	7	
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free Space: 389	н	
All Items Actual Files	KFF Ignorable: 0	Other Known Type: 20	19	Sample
	Data Carved Files: 0	Unknown Type: 1442	9	
🖁 🗄 🔠 🍕 🃚 📑	🗄 🗋 💱 off Unfiltered	▼ ∏ 9	▼ DT2	
▼ File Name	MD5 Hash	Ext F	ile Type	Recycle Bin Original Name
\$16V9VBY.exe	B6C0FEA8A174D9DD24818		1STA Recycle Bin Index File	
🔲 🗋 \$112LHOZ.gif	E4FC0715DA4E6BC5949EE		1STA Recycle Bin Index File	
SIPJ39H4.dmg	30569780881A3921EDCD6		1STA Recycle Bin Index File	
\$IWWQ4ZE.zip	2757B46354B9E3DDA78680		1STA Recycle Bin Index File	
	9BB6826905965C13BE1C84		xecutable File IF File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\putty.exe Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif
SR6V9VBY.exe	6DF90889977C57977982178	85A86B4672 aif 0		

19. The file \$IWWQ4ZE.zip identifies itself as an index or pointer file to the original file VB6_Graduated_Title_Bar_Sample.zip, that has now been renamed \$RWWQ4ZE.zip. The hash of <u>this</u> particular file 2757B46354B9E3DDA7868C41F78EFB46 does not match the original known hash of file VB6_Graduated_Title_Bar_Sample.zip (0a94f3508b87a22958c1f6fee16cf9a8).

File Edit View Tools Help	0				
Overview Expl	· · · ·	E-Mail	Search Bookmark		
Evidence Items	File Status	File Category		be 🚔 🖼 🗃 🚱 🗿 🚳	
Evidence Items: 3	KFF Alert Files: 0	Documents: 14	1910		
File Items	Bookmarked Items: 0	Spreadsheets:	2		
Total File Items: 55869	Bad Extension: 4021	Databases:	21 Recycle B	in Index	
Checked Items: 0	Encrypted Files: 1	Graphics: 1	963	in much	
Unchecked Items: 55869	From E-mail: 0	Multimedia:	413		
Flagged Thumbnails: 0	Deleted Files: 618	E-mail Messages:	0 Filename	\$RWWQ4ZE.zip	
Other Thumbnails: 1963	From Recycle Bin: 7	Executables: 9	0796 Original Name	C:\Evidence\Deleted Test\VB6 Graduated Title Bar Sample.zip	
Filtered In: 55869	Duplicate Items: 9994	Archives:	178 Date Recycled	6/16/2011 11:28:52 AM	
Filtered Out: 0	OLE Subiterns: 1261		Date Recycleu	0/10/2011 11:28:32 Alvi	
Unfiltered Filtered	Flagged Ignore: 0		(Local Machine Time)		
All Items Actual Files	KFF lanorable: 0		209		
	Data Carved Files: 0		4429		
📓 🗄 🔠 🍕 🃚 📑	🖁 🗋 🐳 off Unfiltered		g 🔽 Dīz		
🝸 File Name	MD5 Hash	Ext	File Type	Recycle Bin Original Name	Del F
\$16V9VBY.exe	B6C0FEA8A174D9DD248188	317E41F8582 exe	VISTA Recycle Bin Index File		W
🔲 🗋 \$112LH0Z.gif	E4FC0715DA4E6BC5949EE9		VISTA Recycle Bin Index File		W
🔲 🗋 \$IPJ39H4.dmg	3C5697B08B1A3921EDCD69	1581ECE7EC dmg	VISTA Recycle Bin Index File		W
\$lwwQ4ZE.zip	2757B46354B9E3DDA7868C		VISTA Recycle Bin Index File		W
SR6V9VBY.exe	9BB6826905965C13BE1C840	CCOFF83F42 exe	Executable File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\putty.exe	W
🗖 🔛 \$RI2LHOZ.gif	6DF90889977C57977982178	5A86B4672 gif	GIF File	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\sample-graphic.gif	W
🗖 🚺 \$RWWQ4ZE.zip	0A94F3508B87A22958C1F6F	EE16CF9A8 zip	Zip Archive	Win7 Evidence Drive\Part_2\NONAME-NTFS\Evidence\Deleted_Test\VB6_Graduated_Title_Bar_Sample.zip	W

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.

Overview Expl	ore Graphics	E-Mail Searc	h Bookmark			
Evidence Items	File Status	File Category	بر آن الا الا الا الا الا الا الا الا الا ال	• 🐳 🗃 🗃 🔁 🚺 🍋		
Evidence Items: 3	KFF Alert Files: 0		Name	Size	Modified	Comment
File Items	Bookmarked Items: 0	Spreadsheets: 2		3126	Wodined	
Total File Items: 55869	Bad Extension: 4021	Databases: 21	🖻 🔄 \$RWWQ4ZE.zip			
Checked Items: 0	Encrypted Files: 1	Graphics: 1963	- 🗋 cTitleBar.cls	,	11/22/2002 5:34 PM	
Unchecked Items: 55869	From E-mail: 0	Multimedia: 413	fNonMDITest.frm	-1	6/18/98 11:50 PM	
Flagged Thumbnails: 0	Deleted Files: 618	E-mail Messages: 0	fNonMDITest.frx	106	6/18/98 11:50 PM	
Other Thumbnails: 1963	From Recycle Bin: 7	Executables: 9796	- 🗋 fTest.frm	1,230	6/18/98 11:29 PM	
Filtered In: 55869	Duplicate Items: 9994	Archives: 178	- 🛅 fTest.frx	1,273	6/18/98 11:29 PM	
Filtered Out: 0	OLE Subiterns: 1261	Folders: 10057	- 🛅 fToolWindow.frm	2,383	5/24/98 6:43 PM	
Unfiltered Filtered	Flagged Ignore: 0	Slack/Free Space: 3891	- 🗋 gTest6.vbg	64	11/22/2002 5:33 PM	
All Items Actual Files	KFF Ignorable: 0	Other Known Type: 209	mfTest.frm	3,349	11/22/2002 5:16 PM	
Metual lies	Data Carved Files: 0	Unknown Type: 14429		4 200		
🖉 🗄 🔠 🍕 🃚 📑	🗋 😜 📭 Unfiltered	_ []] 9	▼ DTZ			
	MD5 Hash	Ext File T		Recycle Bin Original Name		
	B6C0FEA8A174D9DD24818		A Recycle Bin Index File			
	E4FC0715DA4E6BC5949EE9		A Recycle Bin Index File			
	3C5697B08B1A3921EDCD69		A Recycle Bin Index File			
	2757B46354B9E3DDA7868C		A Recycle Bin Index File	NG 75 11 DI 10 100		
	9BB6826905965C13BE1C84		utable File		ONAME-NTFS\Evidence\Deleter ONAME-NTFS\Evidence\Deleter	
	6DF90889977C57977982178	15A86B4672 gif GIFF				

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.

File Edit View Tools Help	
Overview Explore Graphics E-Mail Search	Bookmark
Indexed Search Live Search	⊕-26 Hits in 6 Files - QUERY: (\$RPJ39H4.dmg)
Search Term: Add Import Options	Herein 120 Hits in 3 Files - QUERY: (10.1.1.17.946.pdf)
Indexed Words Co Search Items Hits Files	
Edit.item Remove item Remove All View item Results » Cumulative operator: AND OR View Cumulative Results »	
· · · · · · · · · · · · · · · · · · ·	
<u>a</u>	
📓 🗄 🔠 🏀 📴 🗋 🐳 orr Unfiltered 🛛 🔽 🕅 standard	▼ DTZ
▼ File Name MD5 Hash Full Path	Recycle Bi Ext
B9BED9245F4FAB84929A06C5E70A9B73 Win7 Evide	nce Drive\Part_2\NONAME-NTFS\\$Extend\\$UsnJml\\$J
	nce Drive/Part_2NDNAME-NTFS\\$LogFile_1 IIII nce Drive/Part_2NDNAME-NTFS\\Vindows\System32\wdi\LogFiles\BootCKCL.et! et IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII

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.

File Edit View Tool	ls Help						
Overview	Explore	Graphics	E-Mail	Search	Bookmark		
Indexed Search L	ive Search					n 6 Files - QUERY: (\$RPJ39H4.dmg)	
Search Term:		1	Add	mport Options		in 3 Files - QUERY: (10.1.1.17.946.pdf)	
Indexed Words	Co Se	arch Items		Hits Files		n 4 Files - QUERY: (290719612_5a27cbaf61.jpg)	
Indexed words		architems		1105	·		
			1	[
	_	dit item Remove it		View Item Results »	411		
	Cum	ulative operator: Al	ND OR View	v Cumulative Results »	111		
*		🖥 🗟 🙆					
<u>Å</u>		7 TEXT HEX 😕 💟	1 2				
4							
	📚 📑 D 🛛	💜 🕫 Unfiltered	T	standard	•	DTZ	
▼ File Name		MD5 Hash		Full Path		Recycle Bi	Ext Fil
□?! ^{\$}}			FAB84929A06C5E				
\$LogFile_1 \$MFT_1			0BE533186232A68 3EABD6B09E5FB5			2NDNAME-NTFS\\$LogFile_1 2NDNAME-NTFS\\$MFT 1	Ur Ur
BootCKCL.el	tl		0398FC82FF16891			NONAME-NTFS/Windows/System32/wdi/LogFiles/BootCKCL.et/	et Ur

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.

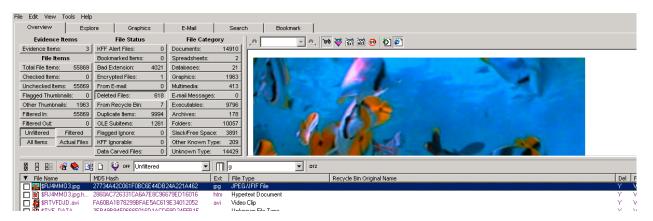
No file matching the original contents or original hash value were located by Forensic Toolkit 1.81.6.

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

Tile Edit View Tools Help	
Overview Explore Graphics E-Mail SearCh Bookmark	
Indexed Search Live Search Search Term Add Indexed Words Co Search Terms Hits Files QUERY: (101.1.1.7.946.pdf) Hits in 3 Files QUERY: (200719612_5a27cba61.pg) Hits in 3 Files QUERY: (Photo 16).pg) Hits in 3 Files QUERY: (Photo 16).pg) Hits in 3 Files QUERY: (Photo 16).pg)	
x	
A Regional Andread A Region of the second A R	
The Name MDS hash Full Path Recycle Bi	Ext
Image: System B9BED9245F4FAB84929A06C5E70A9B73 Win7 Evidence Drive/Part_2/WONAME-NTFS\\$Extendf\$UsrJml\\$J	
	etl

Navigate to the Forensic Toolkit "Overview" tab and select "Deleted Files" you will notice that the file **\$RJ4MMO3.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.

File Edit View Tools Help	
	Bookmark
Indexed Search Live Search Search Add Import Options	
Indexed Words Co Search Items Hits Files Hits Files	
Cumulative operator: AND OR View Cumulative Results >	
pDEEDDEEDD FUUV odKX yAih	
🖁 🗄 🔠 🙀 🍫 📑 🗅 🗳 077 Unfiltered 🔽 🥅 standard	▼ D12
▼ File Name MD5 Hash Full Path	Recycle Bi Ext File Drive\Part_2\NDNAME-NTFS\\\$Extend\\$UsrJml\\$J Unk
□ 🛐 \$LogFile_1 65491B6DB830BE533186232A683311C1 Win7 Evidence	Drive/Part_2NDINAME.HTFS\\$Extend3\\$UsrJml\\$J Uni Drive/Part_2NUDNAME.HTFS\\$LogFile_1 Uni Drive/Part_2NUDNAME.HTFS\\$LogFile_1 Uni Unive/Part_2NUDNAME.HTFS\\$LogFile_1 Uni
BootCKCL.etl 1F3C0AB13DB0398FC82FF1689105D244 Win7 Evidence	Drive\Part_2\NONAME-NTFS\Windows\System32\wdi\LogFiles\BootCKCL.etl etl Uni

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.

File Edit View T	ools Help						
Overview	Explore	Graphics	E-Mail	Search	Bookmark		
Indexed Search Search Term: Indexed Word	s Co 5e	arch Items dil item Remove ite ulative operator: AN	em Remove All	port Options Hits Files View Item Results > Cumulative Results >		in 6 Files - QUERY: (\$RP339H4.dmg) in 3 Files - QUERY: (10.1.1.17.946.pdf) in 3 Files - QUERY: (2007)3612_627Cbaf61.jpg) in 3 Files - QUERY: (Photo 18.pg) in 3 Files - QUERY: (CloS5.pdf) in 3 Files - QUERY: (CE14523-Syllabus2.doc)	
<u>"</u>	▲ ₩ 🗡 🖌	🖥 🗟 🙆	@]				
pDDEDDDED FUUV odKX yAih	DD						
		🚳 077 Unfiltered	~	standard	-	DIZ	
T File Name		MD5 Hash		Full Path			Recycle Bi Ext
□ <u>?</u> \$J			AB84929A06C5E7			2\NDNAME-NTFS\\$Extend\\$UsnJm\\\$J	
BootCKCI			BE533186232A683 3398FC82FF168910			2\NDNAME-NTFS\\$LogFile_1 2\NDNAME-NTFS\Windows\System32\wdi\LogFiles\BootCKCL.etl	eti

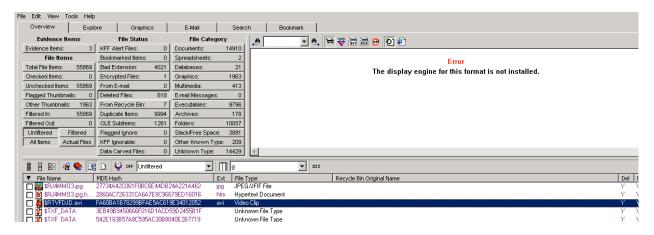
25. Navigate to the Forensic Toolkit Search Tab and enter **drop.avi**, select Add then View Cumulative Results. All entries are from various log files and the Master File Table.

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.

Edit View Tools Help
Overview Explore Graphics E-Mail Search Bookmark
Indexed Search Live Search Search Term: Add Indexed Words Co Search Items Hits Files - CUERY: (\$RP139H4.dmg) Indexed Words Co Search Items Hits Files - CUERY: (UR1.1.17.946.pdf) Indexed Words Co Search Items Hits Edit.item Remove All View item Results > CUERY: (drop.av)
Windows\System32\cryptsp.dll Windows\System32\wbem\mofd.dll
\Device\Harddisk\Volume2\Windows\System32\wber\Performance\WmiApRpl_new.h
Device/Harddisk/Volume3/\$Secure:\$SDS Device/Harddisk/Volume3/Evidence/Deleted_Test/ <mark>CET4523-</mark> Syllabus2_doc
🚦 🗄 😽 🍕 😫 🗈 🔯 077 Unfiltered 🗾 🥅 standard 💽 DTZ
File Name MDS Hash Full Path Recycle Bi Ext F
1 \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$ \$\$

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/Has h 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.zi p	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