**TP-07-F.03.01**

# 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 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/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):

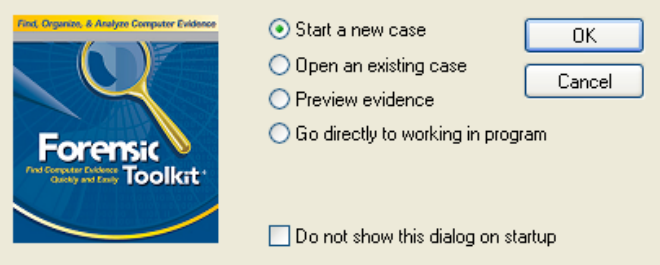
> *FTK examines the Master File Table (MFT) to find files that are marked deleted because the allocation byte in a record header indicates a deleted file or folder. FTK then recovers the file's data*

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

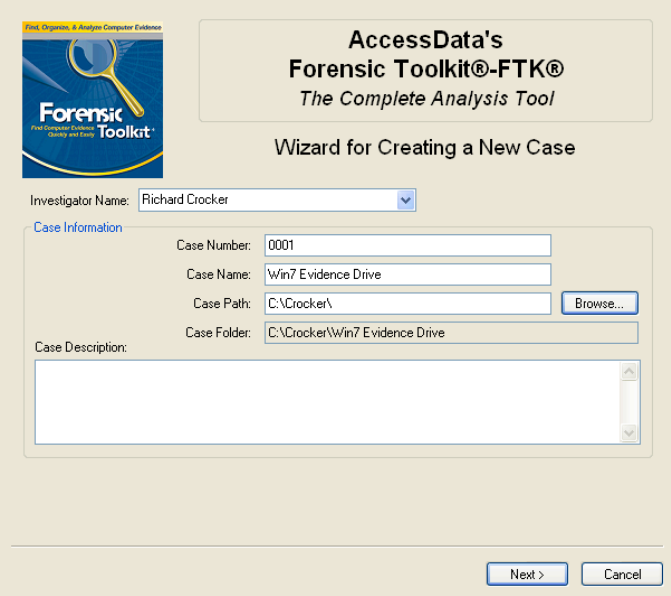
*If the deleted file's parent directory exists, the recovered file is shown in the directory where it originally existed. Deleted files whose parent directories were deleted are shown in their proper place as long as their parent directory's MFT entry has not been recycled.*

**Procedures:**

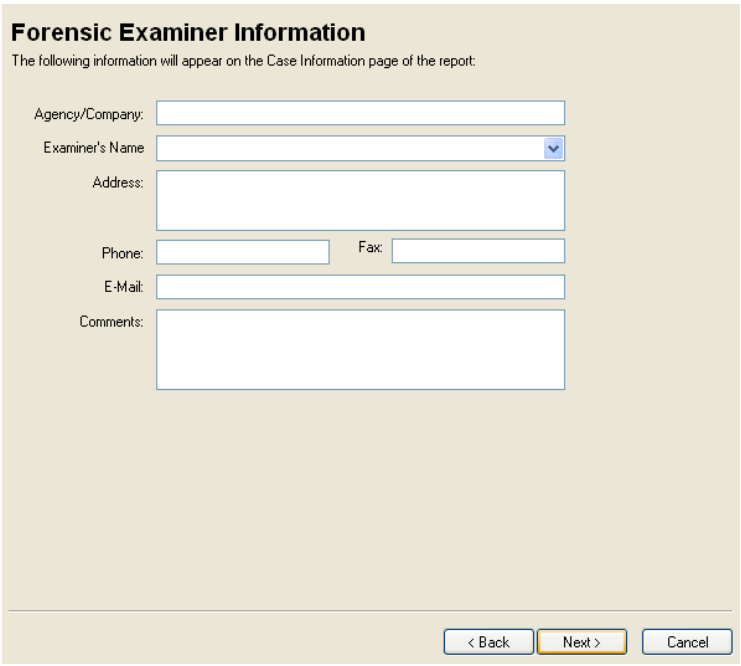
1. Connect FTK dongle to Workstation 7.
2. Connect Windows 7 Evidence drive to Workstation 7 via Tableau Write Blocker.
3. Open FTK.
4. Start new case.



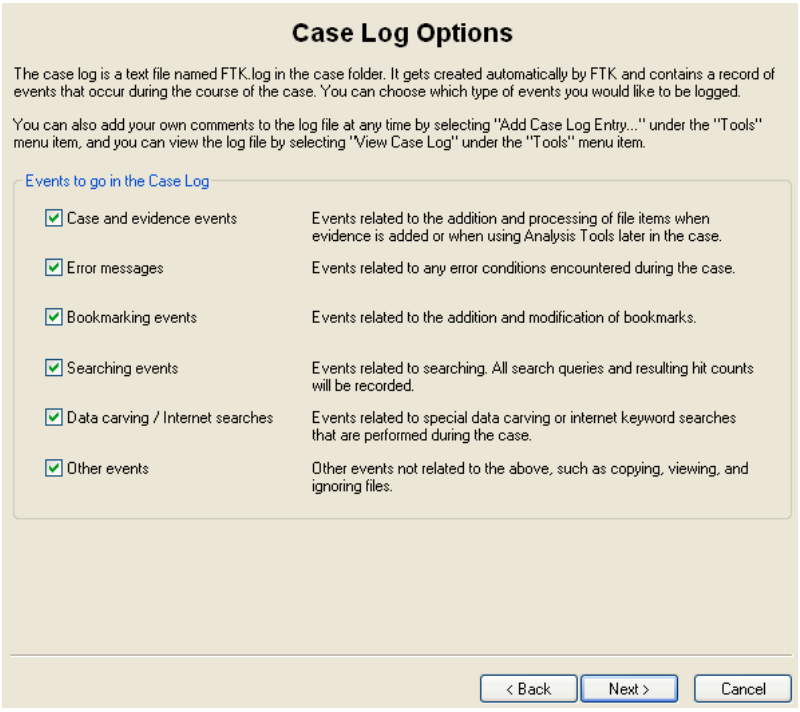

5. Create case number & designate file location



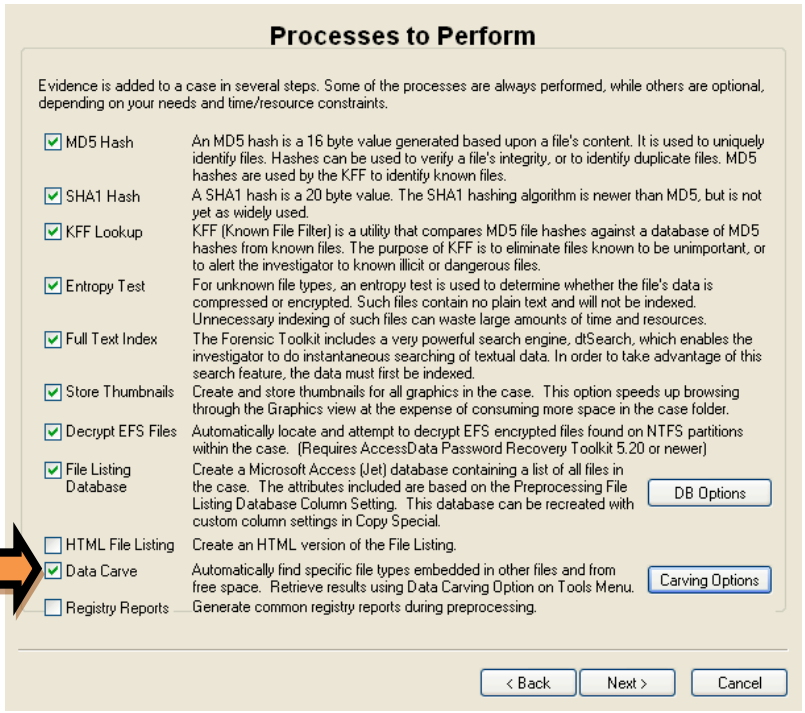

6. Click next



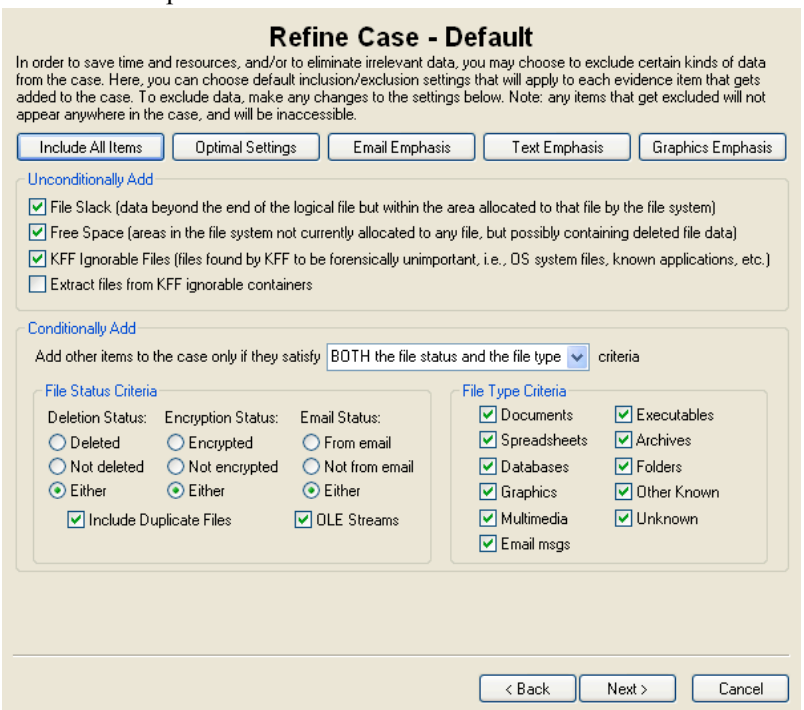

7. Default logging options, click next



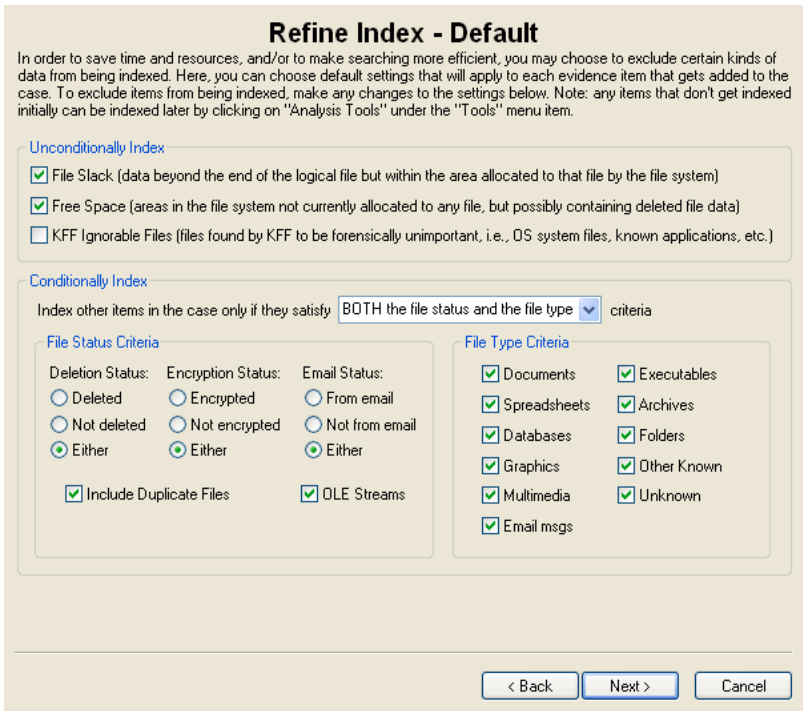

8. Select Data Carve as an option (Data Carve options default – all selected), click next



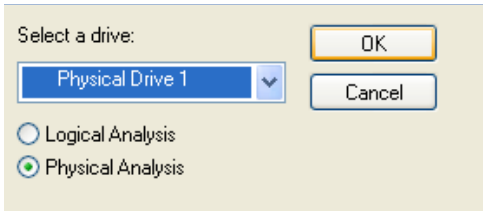

9. Refine Case options left default. Click next.

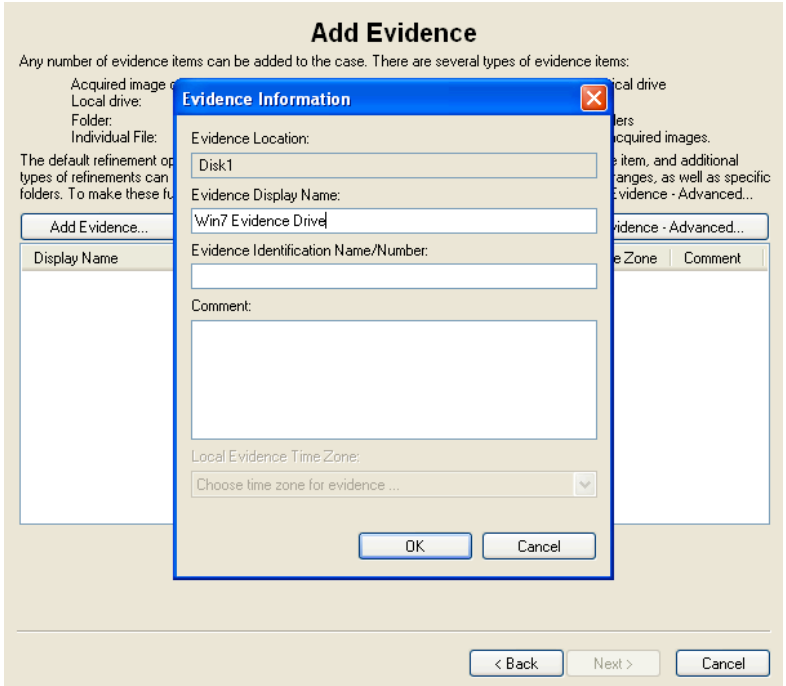



10. Refine Index options left default, click next

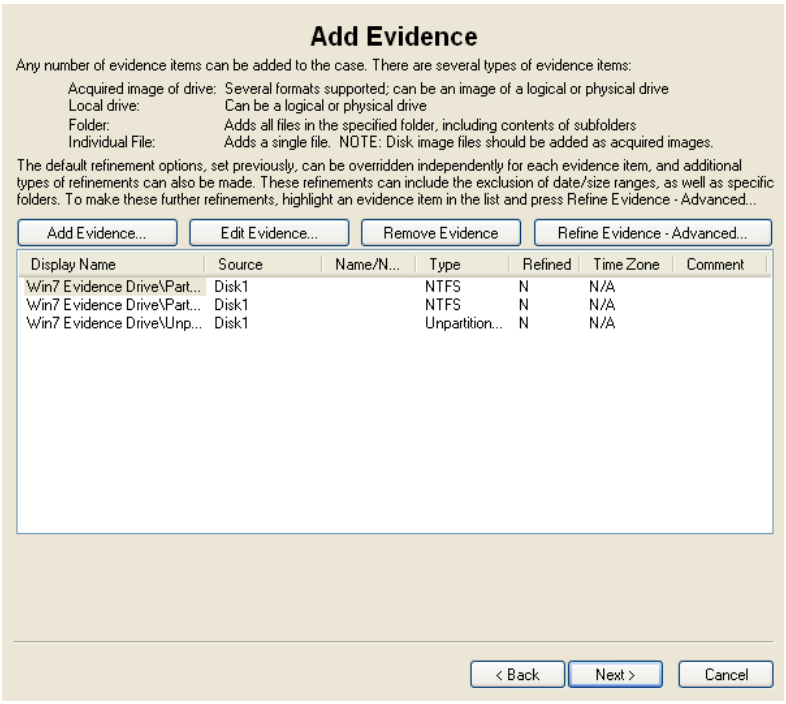



11. Press add Evidence button, add local write-blocked evidence drive (E:), check physical analysis. Click OK. Name Drive Win7 Evidence Drive *logically*. Press Ok.

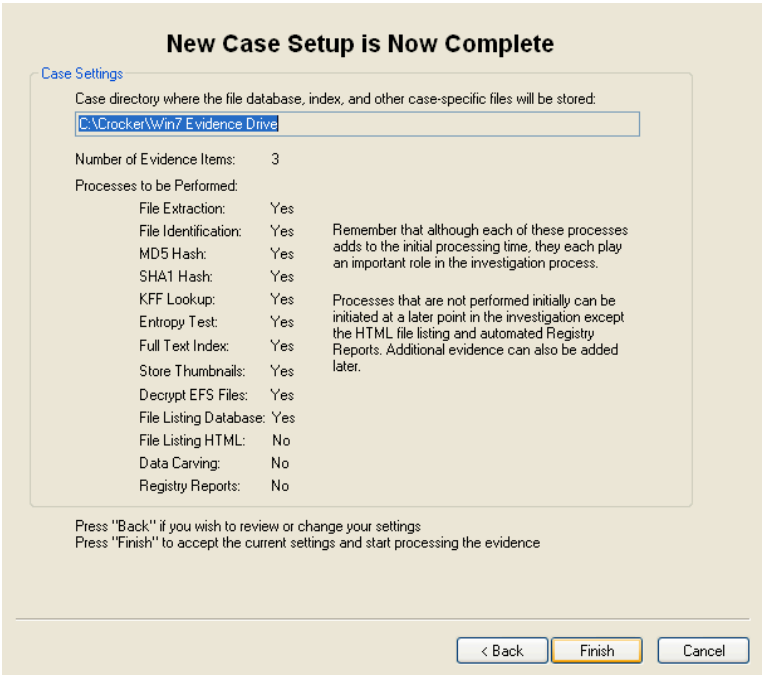


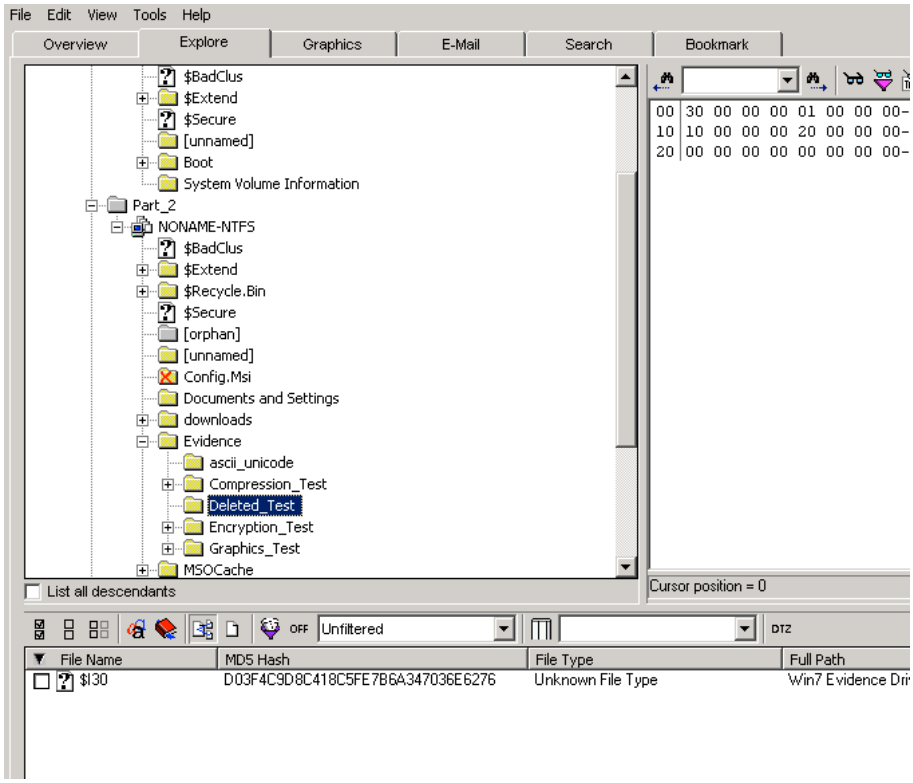

12. Click next.



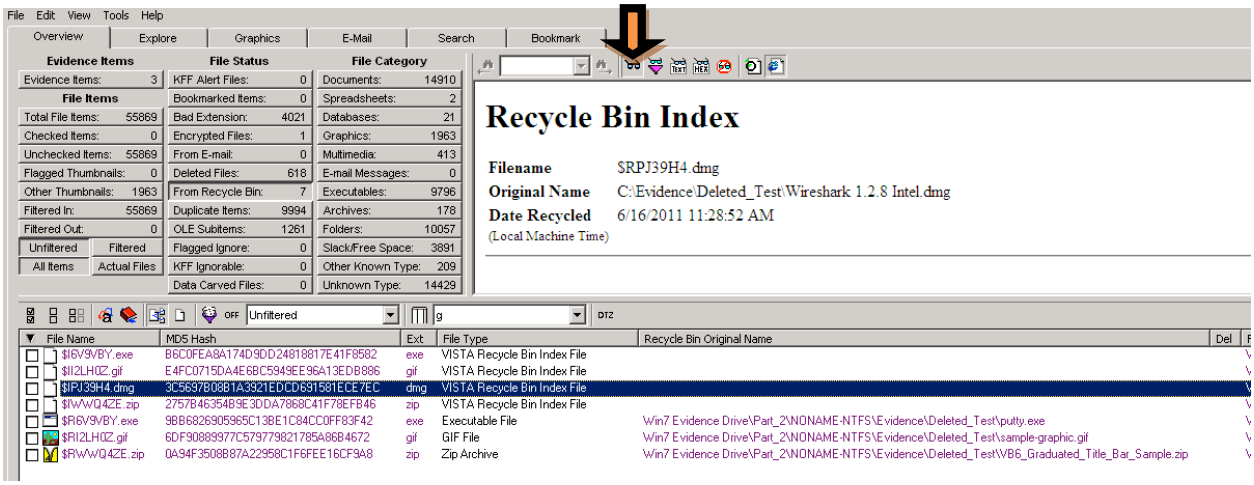

13. Click Finish.




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.

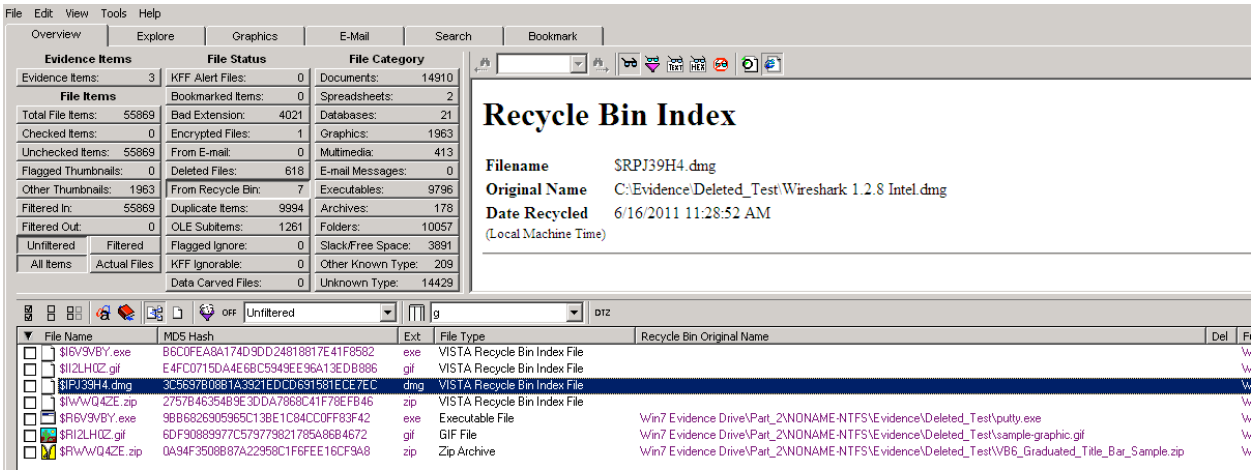



15. Navigate to the Forensic Toolkit Overview Tab and select “From Recycle Bin”.

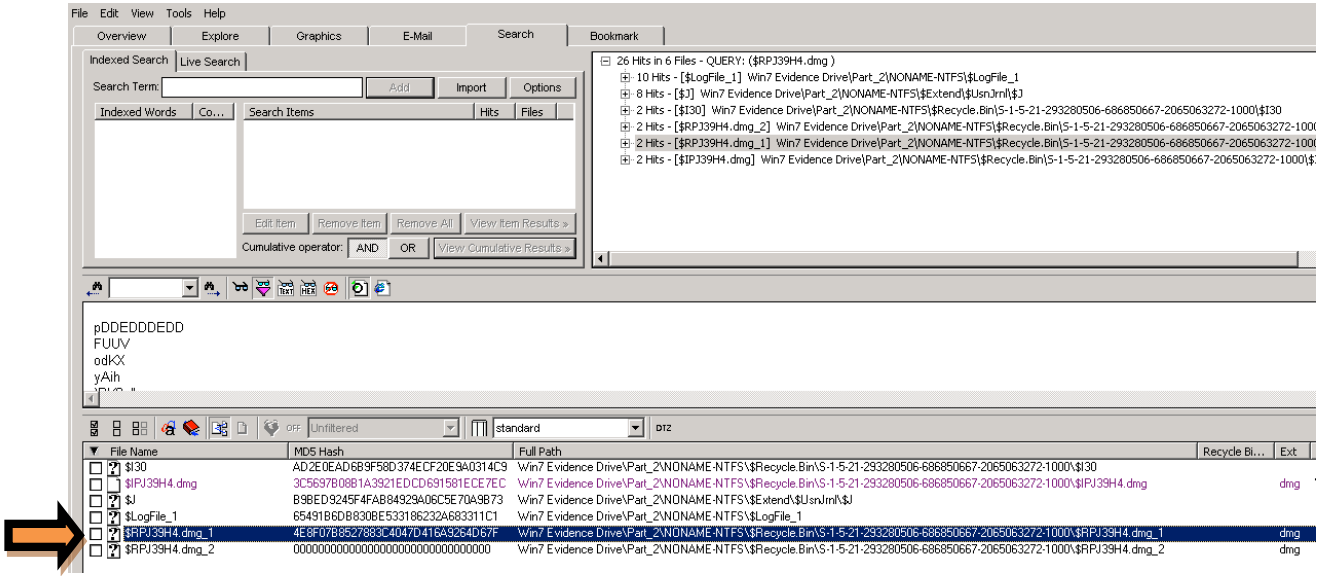



Listed below is the Index listing of each file found in the From Recycle Bin tab in Forensic Toolkit.

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**.



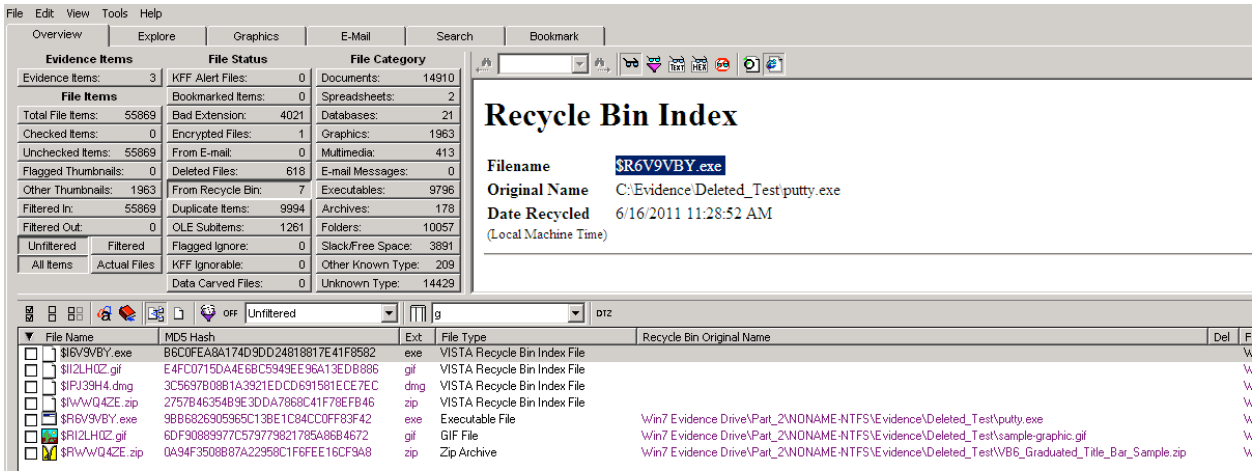

The new target file **$RPJ39H4.dmg** does not exist in this window. If you will select Forensic Toolkit's Search tab, add the search term "$RPJ39H4.dmg", select Add, then View Cumulative Results. You will notice that Forensic Toolkit locates a file with the name **$RPJ39H4.dmg_1** this file has a hash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




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.

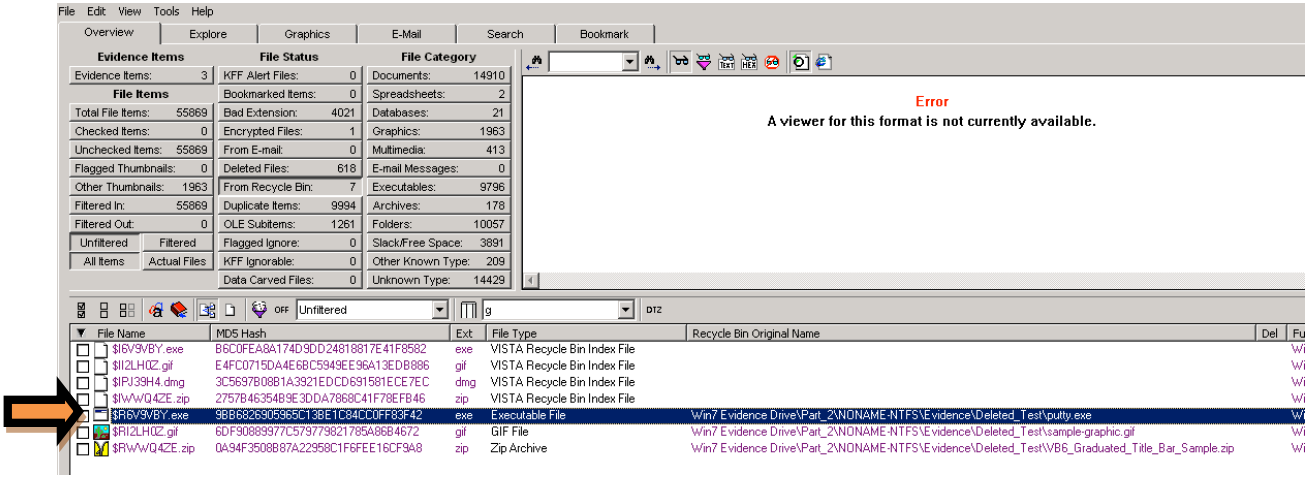
This file is a member of the file group that was added to the Recycle Bin but was not emptied.

17. 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 this particular file **B6C0FEA8A174D9DD24818817E41F8582** does not match the original known hash of file **putty.exe (**9bb6826905965c13be1c84cc0ff83f42**)**.

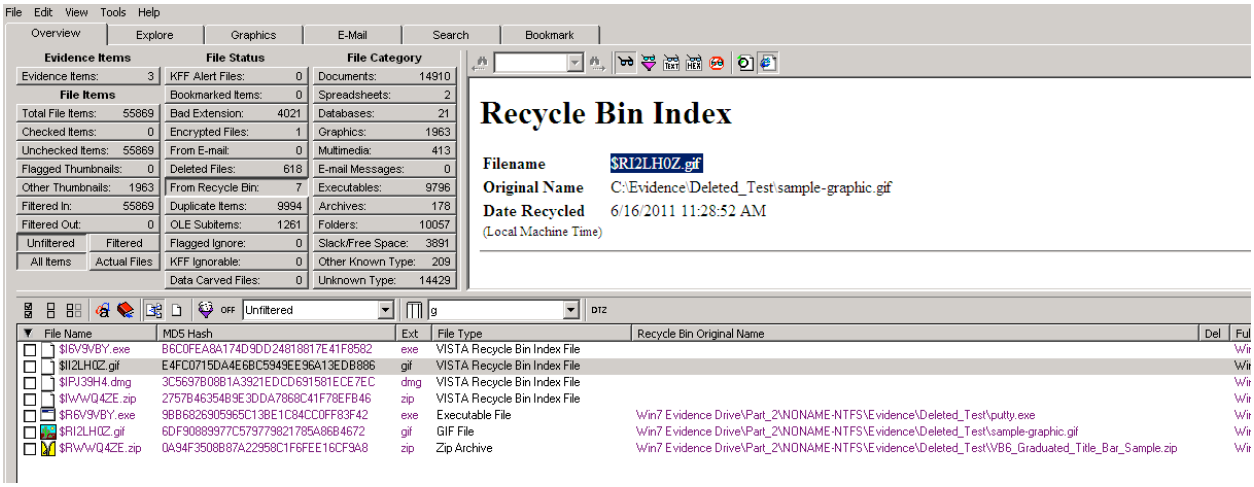



The new target file **$R6V9VBY.exe** is found in this From Recycle Bin view. The hash value of file **$R6V9VBY.exe** is **9BB6826905965C13BE1C84CC0FF83F42**. This hash value matches exactly the known hash value of file **putty.exe (**9bb6826905965c13be1c84cc0ff83f42**)**.

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

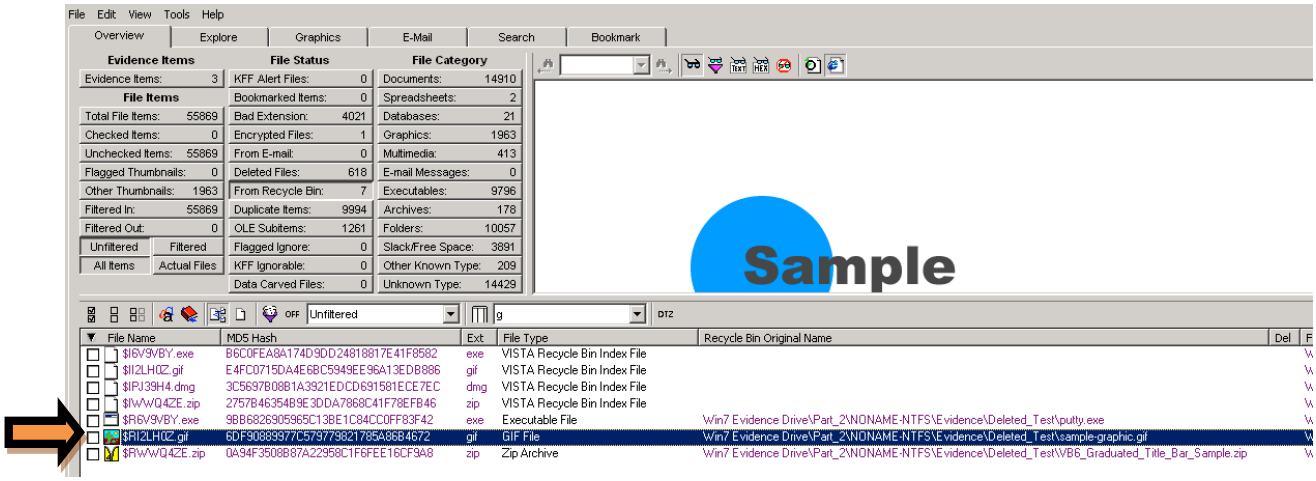



18. The file **$II2LH0Z.gif** identifies itself as an index or pointer file to the original file **sample-graphic.gif**, that has now been renamed **$RI2LH0Z.gif**. The hash of this particular file **E4FC0715DA4E6BC5949EE96A13EDB886** does not match the original known hash of file **sample-graphic.gif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

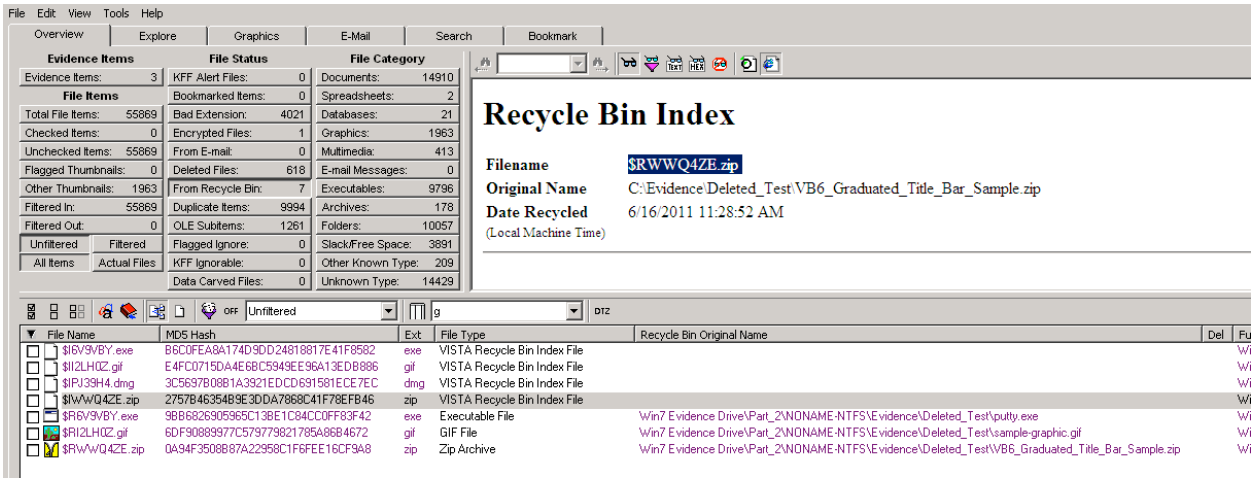



The new target file **$RI2LH0Z.gif** is found in this From Recycle Bin view. The hash value of file **$RI2LH0Z.gif** is **6DF90889977C579779821785A86B4672**. This hash value matches exactly the known hash value of file **sample-graphic.gif (**6df90889977c579779821785a86b4672**)**.

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

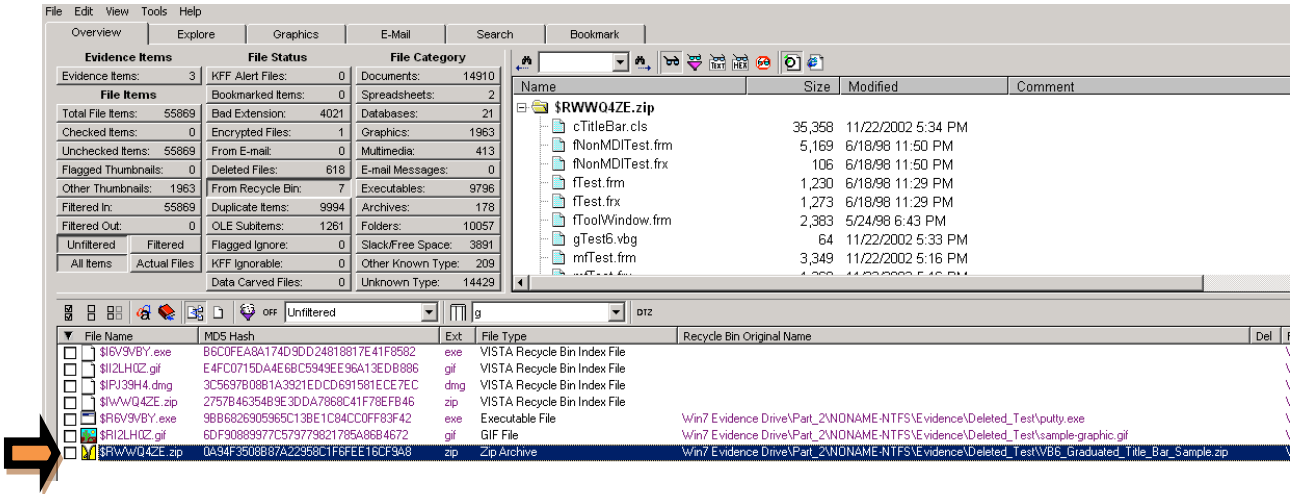



19. The file **$IWWQ4ZE.zip** identifies itself as an index or pointer file to the original file **VB6_Graduated_Title_Bar_Sample.zip**, that has now been renamed **$RWWQ4ZE.zip**. The hash of this particular file **2757B46354B9E3DDA7868C41F78EFB46** does not match the original known hash of file **VB6_Graduated_Title_Bar_Sample.zip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




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**)**.

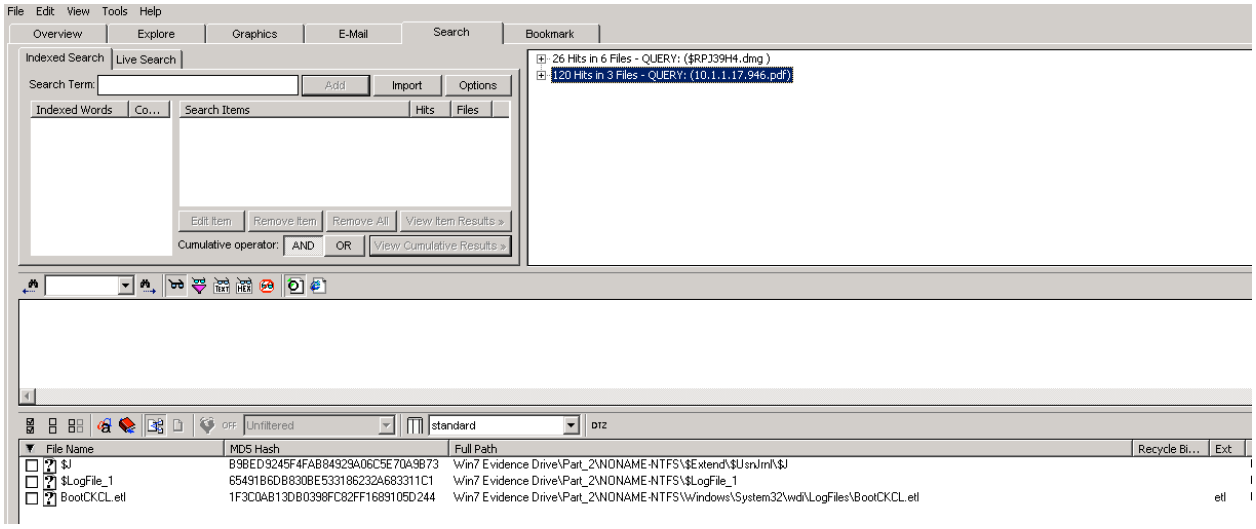
This file is a member of the file group that was added to the Recycle Bin but was not emptied.




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.

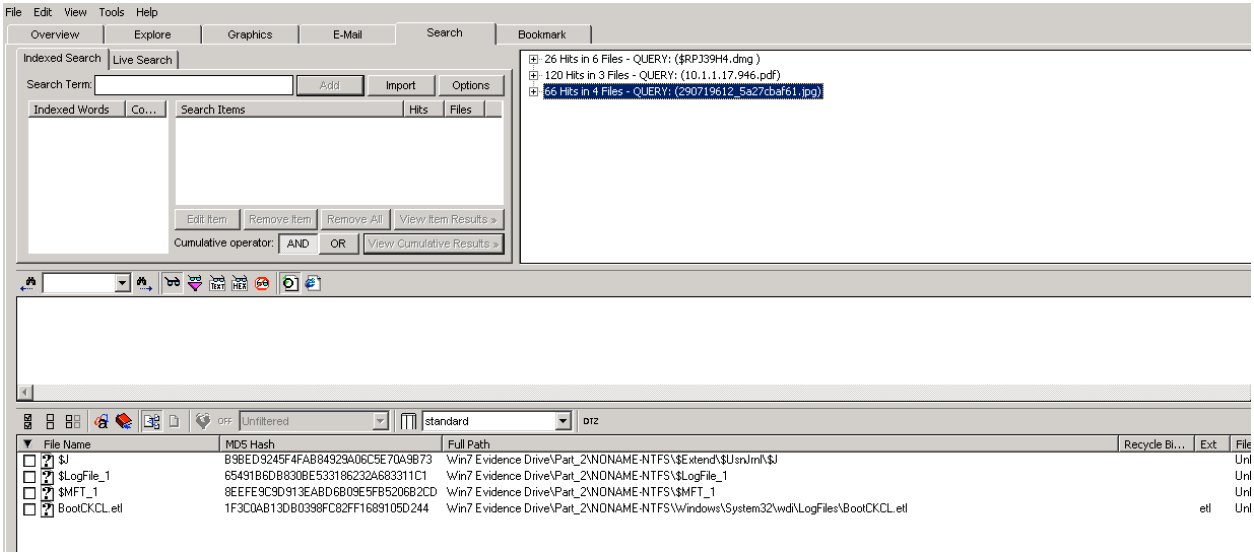
    This file is a member of the file group that was Shift-Deleted.




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.

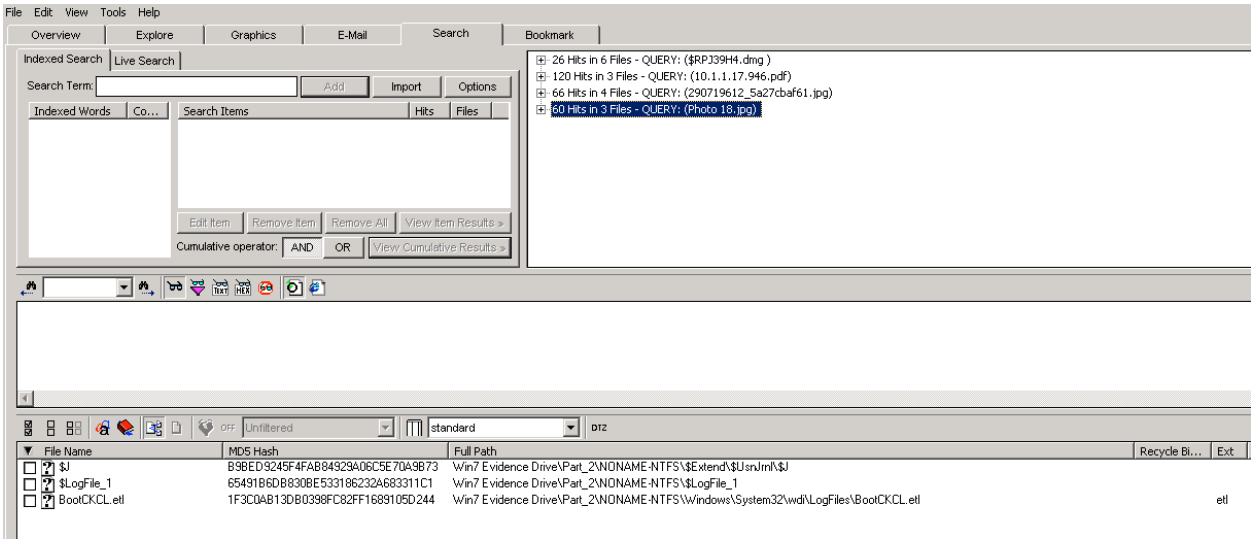
    This file is a member of the file group that was Shift-Deleted.



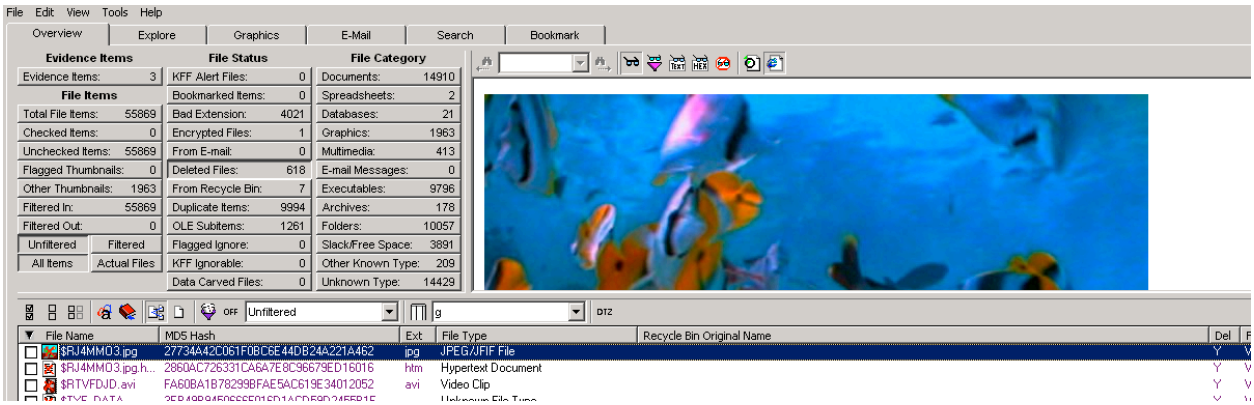

22. Navigate to the Forensic Toolkit Search Tab and enter **Photo 18.jpg**, select Add then View Cumulative Results. All entries are from various log files.

    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.



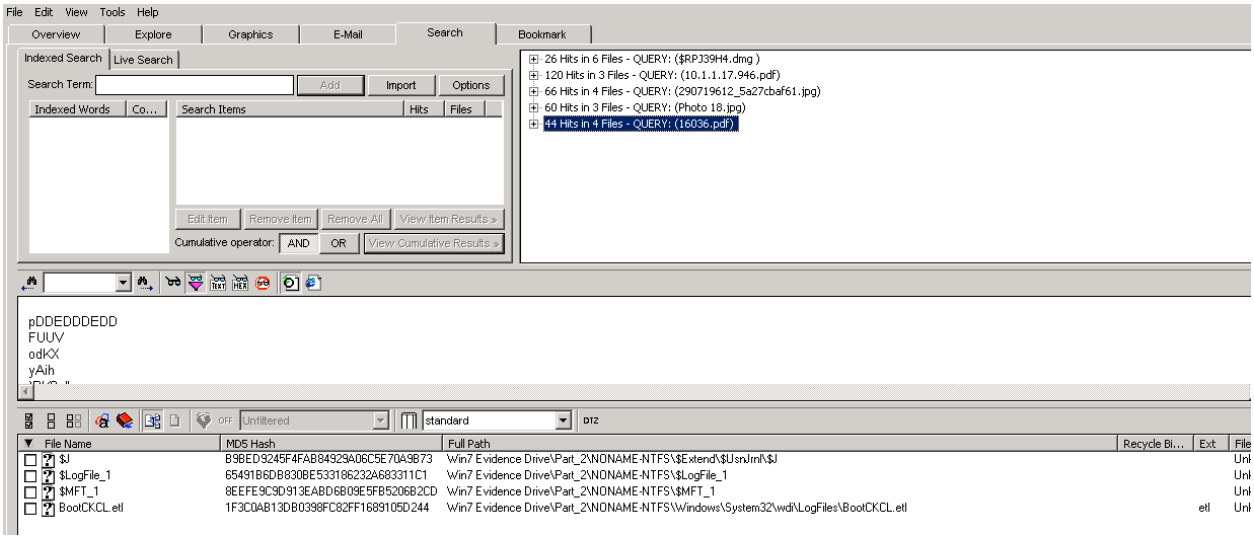

Navigate to the Forensic Toolkit "Overview" tab and select "Deleted Files" you will notice that the file **$RJ4MMO3.jpg** has a hash value of **27734A42C061F0BC6E44DB24A221A462** this matches the known hash value of the target file **Photo 18.jpg** (27734a42c061f0bc6e44db24a221a462). Upon inspection 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.

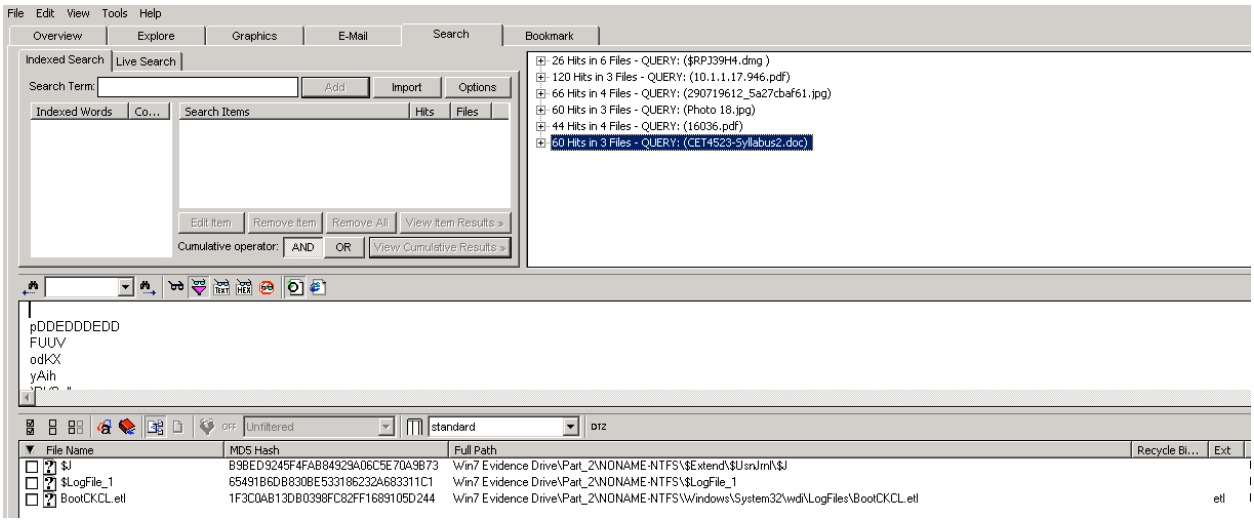
    This file is a member of the file group that was Shift-Deleted.




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.

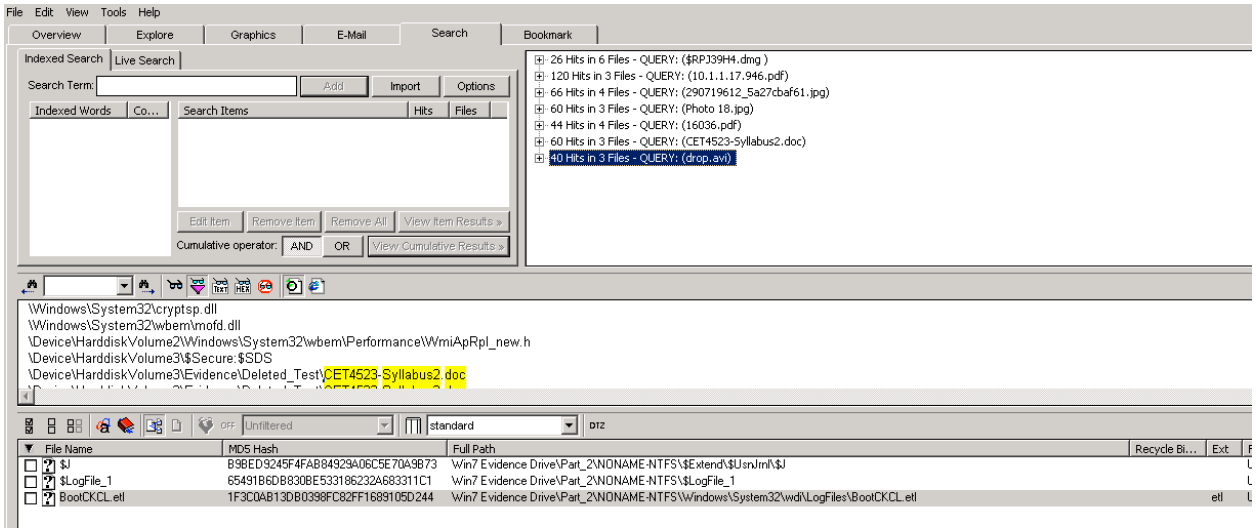
    This file is a member of the file group that was sent to the Recycle Bin then Emptied.



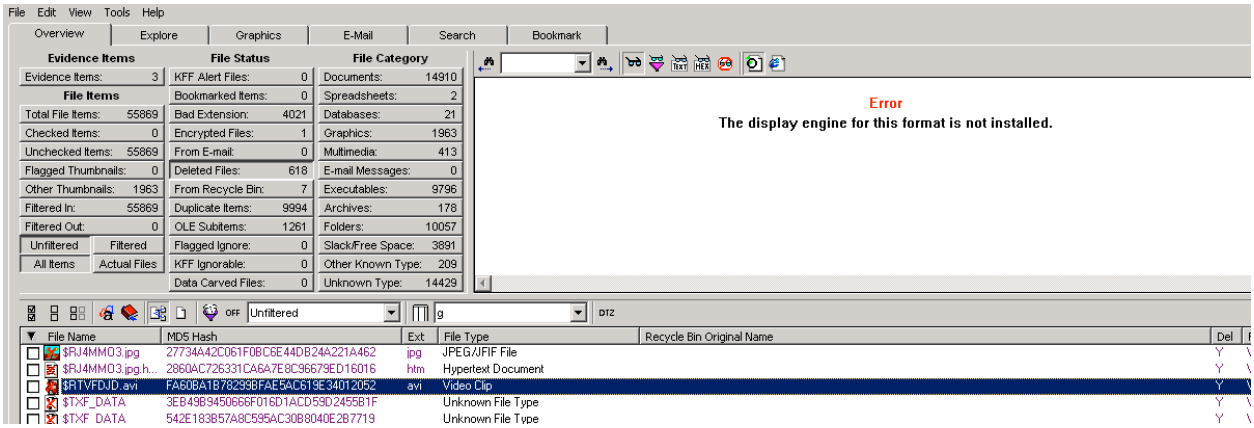

25. Navigate to the Forensic Toolkit Search Tab and enter **drop.avi**, select Add then View Cumulative Results. All entries are from various log files and the Master File Table.

    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 |