THUMBS DB FILES FORENSIC ISSUES

Dustin Hurlbut

Thumbs.db – Definition

A thumbnail view is commonly known to be a miniature picture that represents a larger graphic. Thumbnails are used in FTK and FTK Imager to present large numbers of graphics to the user in a small amount of space. The investigator can review the images to locate files of interest.

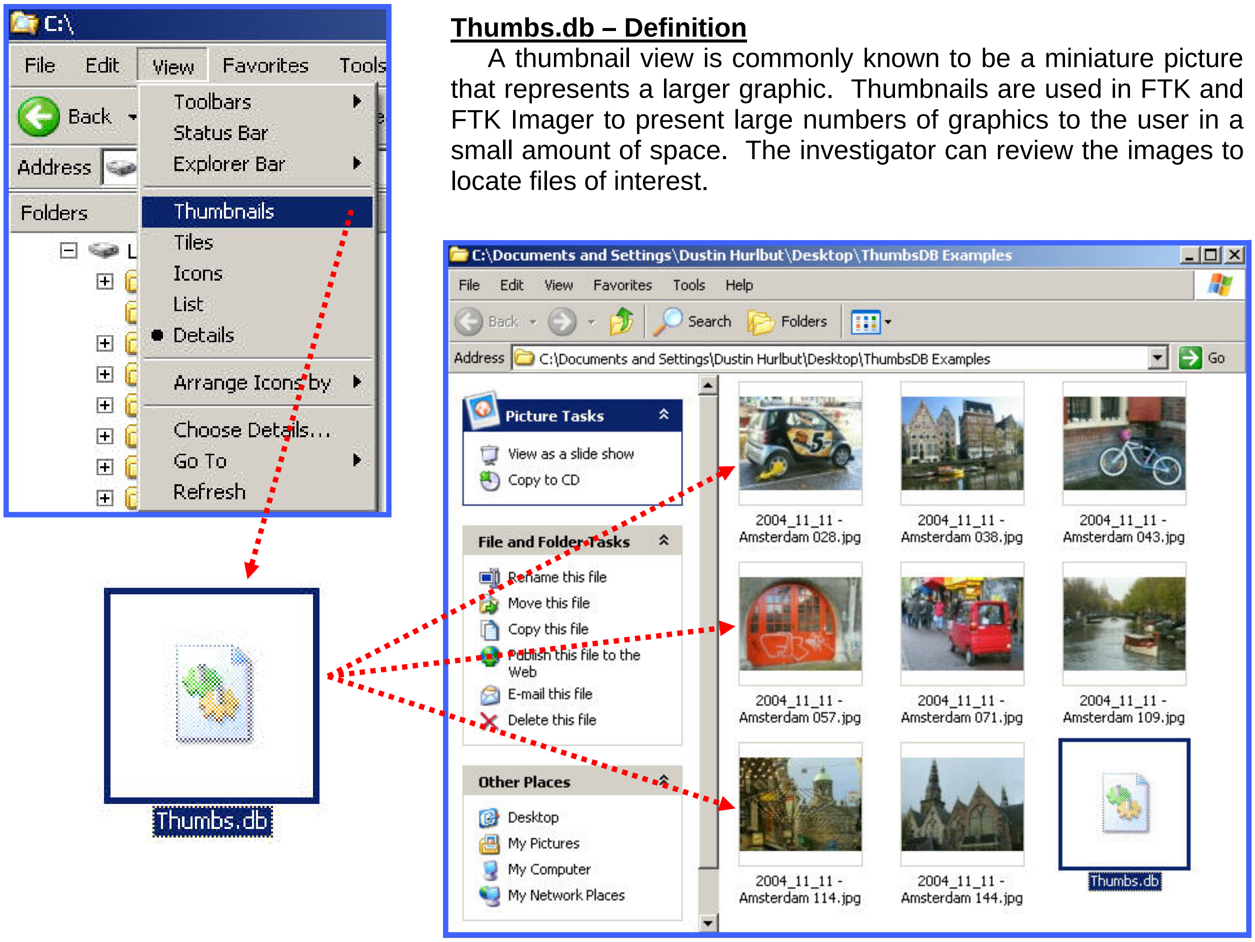


Figure 1 - Thumbs.db and Thumbnail Views in Windows Explorer

The Microsoft Windows operating system also has the ability to generate thumbnail views of files and display them to the user. Starting with Windows ME, the user can select View > Thumbnails from the Windows Explorer drop down menu. This will display the graphics in that particular folder as thumbnails instead of the details or icon views normally selected (see Figure 1).

The thumbnail viewer is particularly handy for users with large amounts of graphics. Thumbnails make it is easier to sort through large numbers of files by viewing small depictions of the photos instead of the standard arcane names often used, especially in the realm of digital cameras.

Thumbnails also speed up the processing of graphics hence the reason they were created in the Microsoft operating systems. Aside from these advantages, the downside of thumbnails is that when accessed, a hidden system file is created in the folder the files are stored in. These system files aren't visible to the common user and as such can take up successively more drive space. This may be bad for the user, but good for the forensic investigator. This system file is called a thumbs.db and is actually a database of the miniature images that exist in the folder from which they were initiated.

Operating System Issues

Windows stores the following formats as thumbnails: JPEG, BMP, GIF, and HTM. Each thumbnail created in a folder is represented in this database as a small JPEG file, regardless of the file's original format. Each folder with initiated thumbnail views will have thumbs.db file.

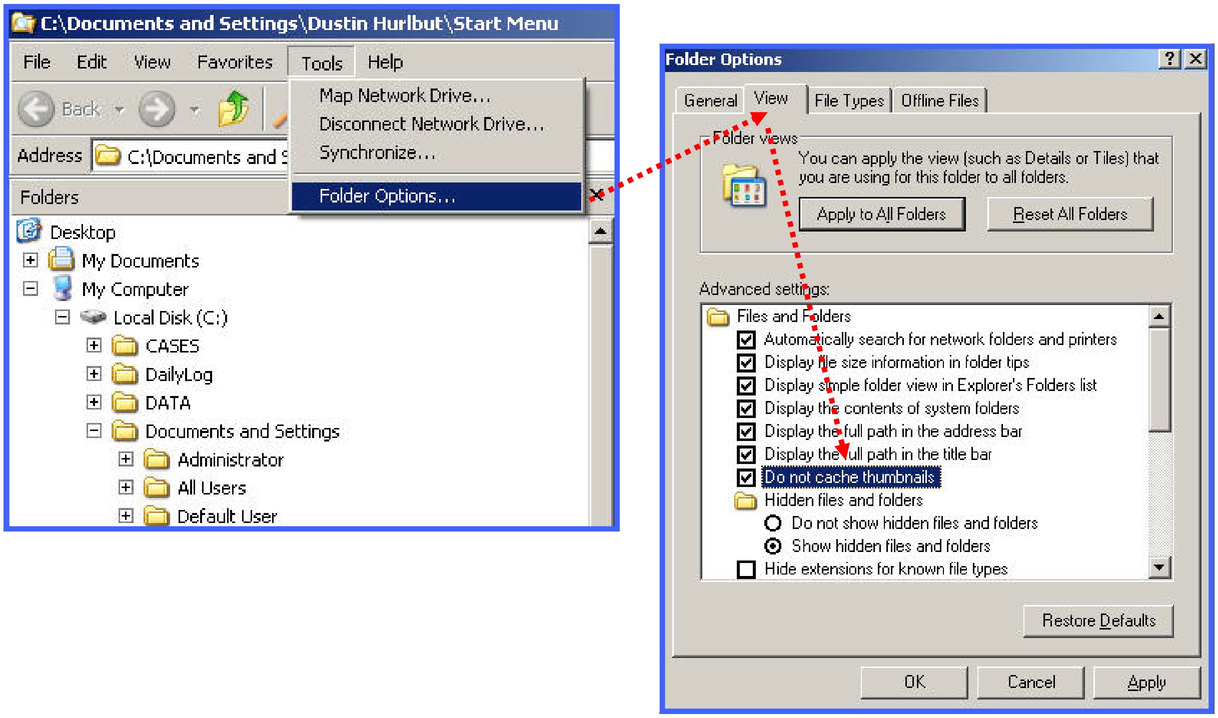
System	Windows ME	Windows 2000	Windows XP	Windows 2003
Drive	Yes	Yes	No	No
Filename	Yes	Yes	Yes	Yes
Path	Yes	Yes	No	No

Figure 2 - Thumbs.db Variations

The early versions of thumbs.db files as they appeared in Windows ME and Windows 2000 contained not only the thumbnail image of the parent file, but also the filename, drive letter, and path to that image. Later versions, Windows XP and Windows 2003, store the image and its filename but not the path. See Figure 2 for variations in these operating systems.

It is important to note that in Windows 2000 when it is located in an NTFS formatted drive, will create the thumbnails as an Alternate Data Stream (ADS) rather then create a separate thumbs.db file. This ADS information is actually part of the original graphic file so no alternative thumbs.db file is necessary and will not appear in the folder. The thumbs.db file in Windows 2000 will only appear when the folder is in a FAT formatted environment. Alternate Data Streams cannot exist in a FAT system.

An interesting aspect of thumbs.db files is that when a graphic is viewed and an entry made for it in the database, it is maintained indefinitely by the operating system. If the file is deleted, the image will remain unless the thumbs.db file or the entire folder are deleted.


C:\Documents and Settings\Dustin Hurlbut\Start Menu

Folder Options

You can apply the view (such as Details or Tiles) that you are using for this folder to all folders.

Advanced settings:

Files and Folders
- ☑ Automatically search for network folders and printers
- ☑ Display file size information in folder tips
- ☑ Display simple folder view in Explorer's Folders list
- ☑ Display the contents of system folders
- ☑ Display the full path in the address bar
- ☑ Display the full path in the title bar
- ☑ Do not cache thumbnails

Hidden files and folders
- ○ Do not show hidden files and folders
- ● Show hidden files and folders
- □ Hide extensions for known file types

Figure 3 - Turning Off Thumbnails

Thumbnails are turned on by default so the thumbs.db file will be created anytime the user chooses to view them. The user can turn this feature off in XP (see Figure 3) by selecting Tools > Folder Options, select the View Tab and then check the "Do not cache thumbnails" box. This will turn off the creation of thumbs.db files. With this feature disabled, thumbnails will still be visible if selected, but they will not be saved in a thumbs.db file. They will be kept in memory until the system is turned off. They can also be turned off using the Registry in Windows XP by selecting a value of 1 in the following key: **HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\DisableThumbnailCache**. In 2000, the following key enables them individually by file type: **HKEY_CLASSES_ROOT\<FileType>\ShellEx\**, followed by the default setting of: **7376D660-C583-11D0-A3A5-00C04FD706EC** where <filetype> is the particular file extension.

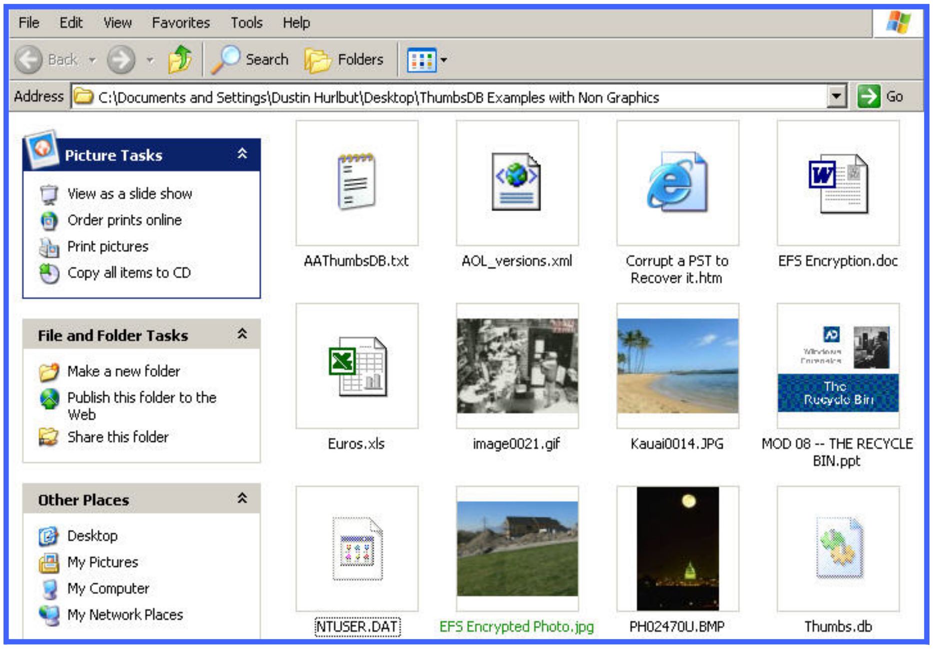
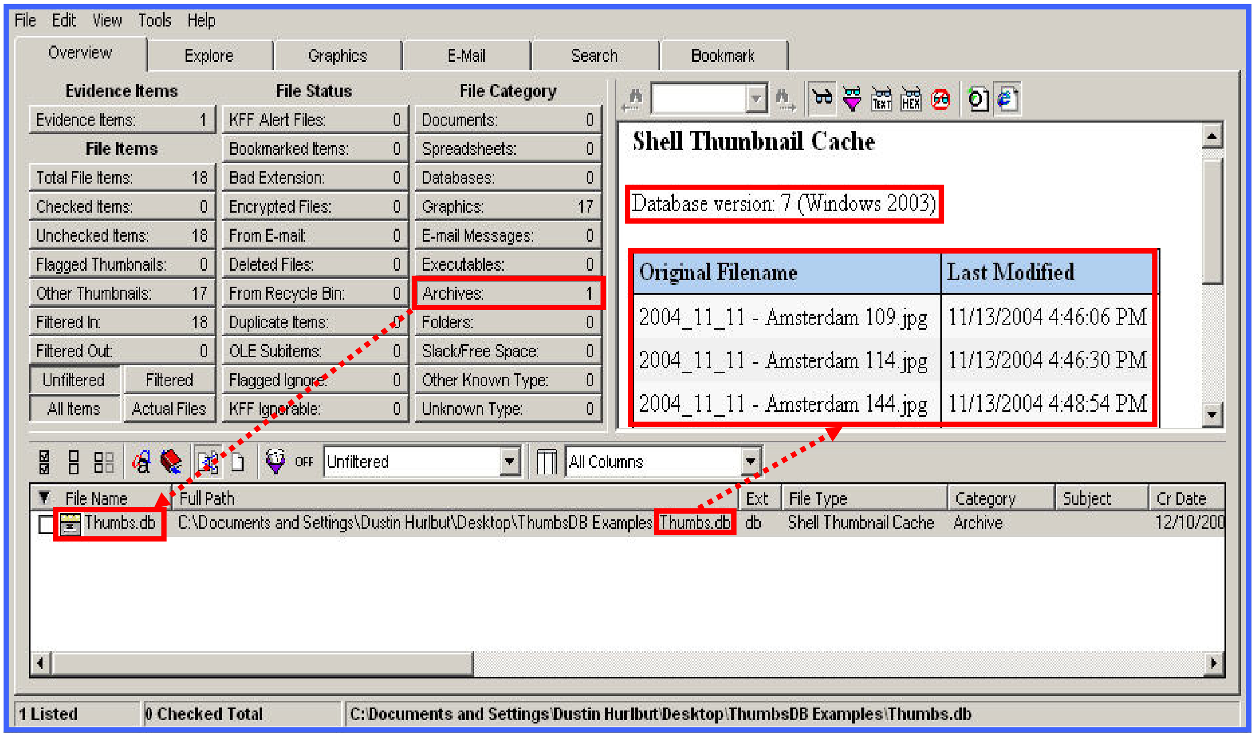


Figure 4 - Thumbs DB Icon Views

If a file does not fit the type of graphic Windows will display as a thumbnail, it will display an appropriate icon instead. For example, in Figure 4, you will see a text document icon for a text file, Word icon for a Word document, or an Excel icon for a spreadsheet. Windows will also display the first slide of a PowerPoint thumbnail in place of an icon and other application icons in many cases. There are programs out there that can display other types of graphic thumbnails in the Windows environment.

Viewing Thumbs.db Files in FTK

FTK will display thumbs.db database records as well as the miniature graphics generated in each. If you click on the thumbs.db file (see Figure 5), you will see an HTML representation of the record information such as filename and modified time (and path information if created in Windows ME or 2000). Often, this can lead the investigator to look for supporting information such as removable media, .LNK files, or other artifacts that may support the existence of suspect evidence.



Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	18	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	17
Unchecked Items:	18	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	0	Executables:	0
Other Thumbnails:	17	From Recycle Bin:	0	Archives:	1
Filtered In:	18	Duplicate Items:	0	Folders:	0
Filtered Out:	0	OLE Subitems:	0	Slack/Free Space:	0
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	0
All Items	Actual Files	KFF Ignorable:	0	Unknown Type:	0

Shell Thumbnail Cache

Database version: 7 (Windows 2003)

Original Filename	Last Modified
2004_11_11 - Amsterdam 109.jpg	11/13/2004 4:46:06 PM
2004_11_11 - Amsterdam 114.jpg	11/13/2004 4:46:30 PM
2004_11_11 - Amsterdam 144.jpg	11/13/2004 4:48:54 PM

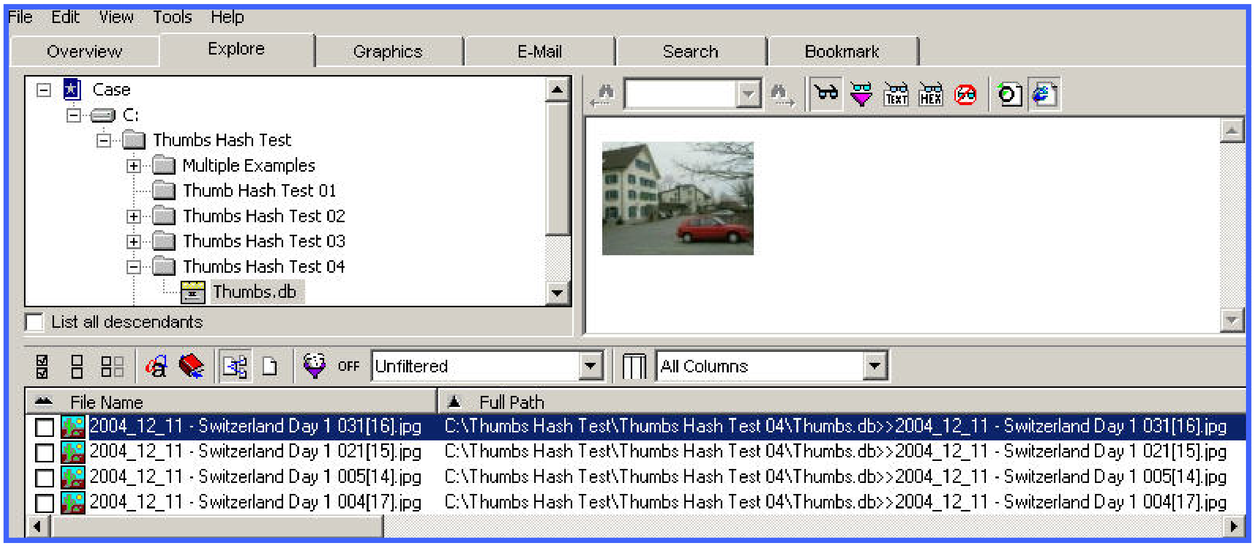
OFF Unfiltered · All Columns

File Name	Full Path	Ext	File Type	Category	Subject	Cr Date
Thumbs.db	C:\Documents and Settings\Dustin Hurlbut\Desktop\ThumbsDB Examples\Thumbs.db	db	Shell Thumbnail Cache	Archive		12/10/200

1 Listed · 0 Checked Total · C:\Documents and Settings\Dustin Hurlbut\Desktop\ThumbsDB Examples\Thumbs.db

Figure 5 - Viewing Thumbs.db Files in FTK

FTK stores thumbs.db files in the Archive container. Since each thumbs.db file in every folder bears the same name, it is helpful to create a custom column setting for viewing the thumbs.db's that has the path setting visible. This allows you to sort quickly through different files and their respective locations.



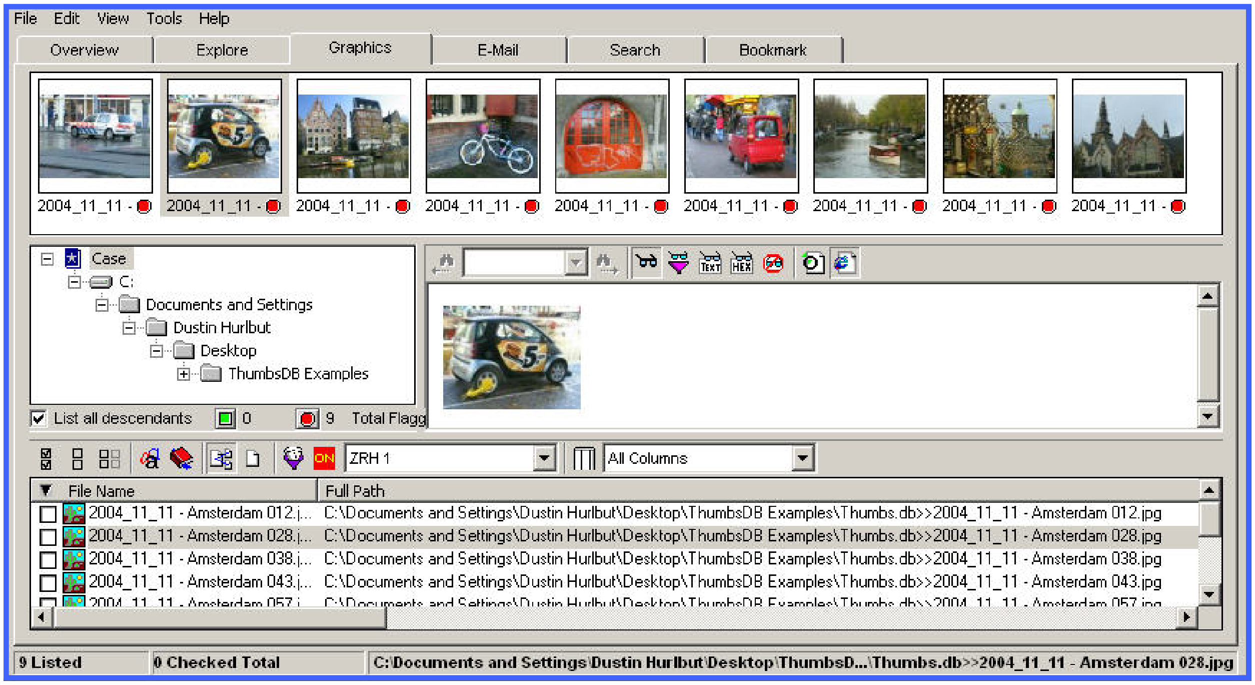
☐ List all descendants

Unfiltered | All Columns

File Name	Full Path
☐ 2004_12_11 - Switzerland Day 1 031[16].jpg	C:\Thumbs Hash Test\Thumbs Hash Test 04\Thumbs.db>>2004_12_11 - Switzerland Day 1 031[16].jpg
☐ 2004_12_11 - Switzerland Day 1 021[15].jpg	C:\Thumbs Hash Test\Thumbs Hash Test 04\Thumbs.db>>2004_12_11 - Switzerland Day 1 021[15].jpg
☐ 2004_12_11 - Switzerland Day 1 005[14].jpg	C:\Thumbs Hash Test\Thumbs Hash Test 04\Thumbs.db>>2004_12_11 - Switzerland Day 1 005[14].jpg
☐ 2004_12_11 - Switzerland Day 1 004[17].jpg	C:\Thumbs Hash Test\Thumbs Hash Test 04\Thumbs.db>>2004_12_11 - Switzerland Day 1 004[17].jpg

Figure 6 - Viewing Thumbnails in FTK's Explore Tab

To view the actual thumbnail graphic in FTK, select the thumbs.db file of interest in the Explore tab and then select the desired graphic below in the File List pane (See Figure 6). All graphic thumbnails are stored in the Graphics tab as seen in Figure 7. From here, you can view all the miniatures stored in a specific thumbs.db file or you can view all the graphics in the case.



☑ List all descendants 🟩 0 ● 9 Total Flagg

ZRH 1 | All Columns

File Name	Full Path
☐ 2004_11_11 - Amsterdam 012.j...	C:\Documents and Settings\Dustin Hurlbut\Desktop\ThumbsDB Examples\Thumbs.db>>2004_11_11 - Amsterdam 012.jpg
☐ 2004_11_11 - Amsterdam 028.j...	C:\Documents and Settings\Dustin Hurlbut\Desktop\ThumbsDB Examples\Thumbs.db>>2004_11_11 - Amsterdam 028.jpg
☐ 2004_11_11 - Amsterdam 038.j...	C:\Documents and Settings\Dustin Hurlbut\Desktop\ThumbsDB Examples\Thumbs.db>>2004_11_11 - Amsterdam 038.jpg
☐ 2004_11_11 - Amsterdam 043.j...	C:\Documents and Settings\Dustin Hurlbut\Desktop\ThumbsDB Examples\Thumbs.db>>2004_11_11 - Amsterdam 043.jpg
☐ 2004_11_11 - Amsterdam 057.j...	C:\Documents and Settings\Dustin Hurlbut\Desktop\ThumbsDB Examples\Thumbs.db>>2004_11_11 - Amsterdam 057.jpg

9 Listed | **0 Checked Total** | **C:\Documents and Settings\Dustin Hurlbut\Desktop\ThumbsD...\Thumbs.db>>2004_11_11 - Amsterdam 028.jpg**

Figure 7 - Viewing Thumbnails in FTK's Graphics Tab

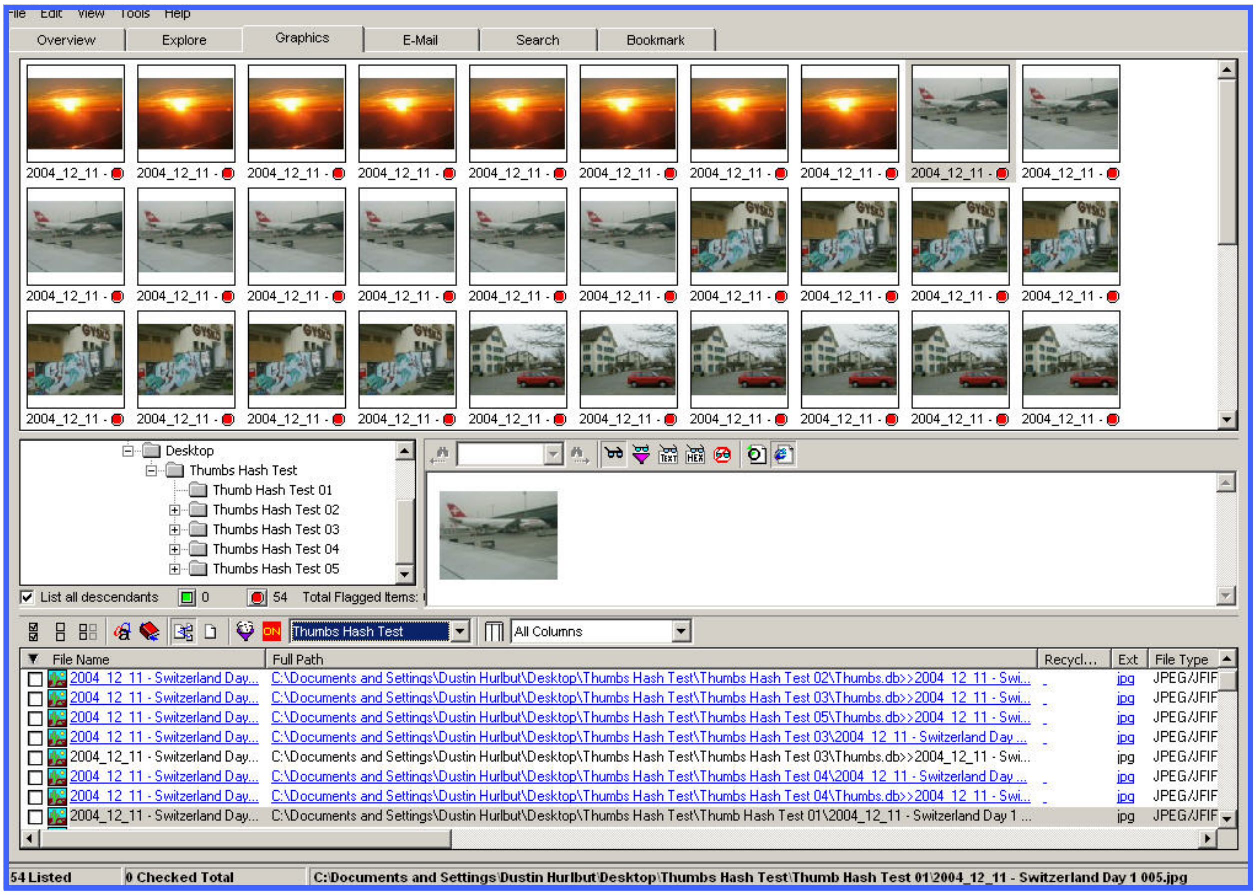
Forensic Issues - Thumbs.db Files

There are a number of forensic issues associated with Thumbs.db files. Most importantly, thumbs.db files will contain an image of every graphic in the folder if the user viewed them as thumbnails. This may be unknown to the user as they are hidden system files. Each time files are added to the folder, new records and miniature graphics will be created in the thumbs.db.

As an example, a suspect in a child pornography case could easily have hundreds of graphics stored in their system in thumbs.db files. Once created, they maintain information on each of the individual files. If graphics files are deleted from the folder, the thumbs.db file will retain them. So, a suspect who has deleted evidence of photos prior to seizure of the computer, may still have thumbnail images of the graphics stored in the thumbs.db files. These graphics will remain, even if the folder is renamed or they may be located in unallocated space as deleted files. This can be potentially important evidence, especially in light of a suspect who denies those types of files were on their system.

A real world example of the forensic utility of thumbs.db files in this instance is demonstrated by a recent case examination by Forensic Examiner Tanja Giacovelli of Alste Technologies in Germany. She was investigating an allegation of child pornography on a suspect's computer. The suspect denied having child porn on his system and indeed, there were no full size images on the fixed media. However, there were thumbs.db files left on the computer that contained apparent suspect material.

The suspect also had several CDs which did contain child pornography. Inadvertently, he had copied existing thumbs.db files over to CD from his folders along with the actual graphics. Using FTK, FTK Imager, and the Known File Filter, Tanja compared hashes of the thumbnails in the thumbs.db archives from the main computer with the thumbnails found in the thumbs.db files on the CDs and discovered exact matches. Thus she was able to show the thumbs.db files located on the suspect's system were the same as those on the CDs allowing her to deduce that the full sized graphics on the CDs were indeed on the suspect's computer at one time.



	File Name	Full Path	Recycl...	Ext	File Type
□	2004_12_11 - Switzerland Day...	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumbs Hash Test 02\Thumbs.db>>2004_12_11 - Swi...		jpg	JPEG/JFIF
□	2004_12_11 - Switzerland Day...	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumbs Hash Test 03\Thumbs.db>>2004_12_11 - Swi...		jpg	JPEG/JFIF
□	2004_12_11 - Switzerland Day...	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumbs Hash Test 05\Thumbs.db>>2004_12_11 - Swi...		jpg	JPEG/JFIF
□	2004_12_11 - Switzerland Day...	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumbs Hash Test 03\2004_12_11 - Switzerland Day ...		jpg	JPEG/JFIF
□	2004_12_11 - Switzerland Day...	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumbs Hash Test 03\Thumbs.db>>2004_12_11 - Swi...		jpg	JPEG/JFIF
□	2004_12_11 - Switzerland Day...	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumbs Hash Test 04\2004_12_11 - Switzerland Day ...		jpg	JPEG/JFIF
□	2004_12_11 - Switzerland Day...	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumbs Hash Test 04\Thumbs.db>>2004_12_11 - Swi...		jpg	JPEG/JFIF
□	2004_12_11 - Switzerland Day...	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumb Hash Test 01\2004_12_11 - Switzerland Day 1 ...		jpg	JPEG/JFIF

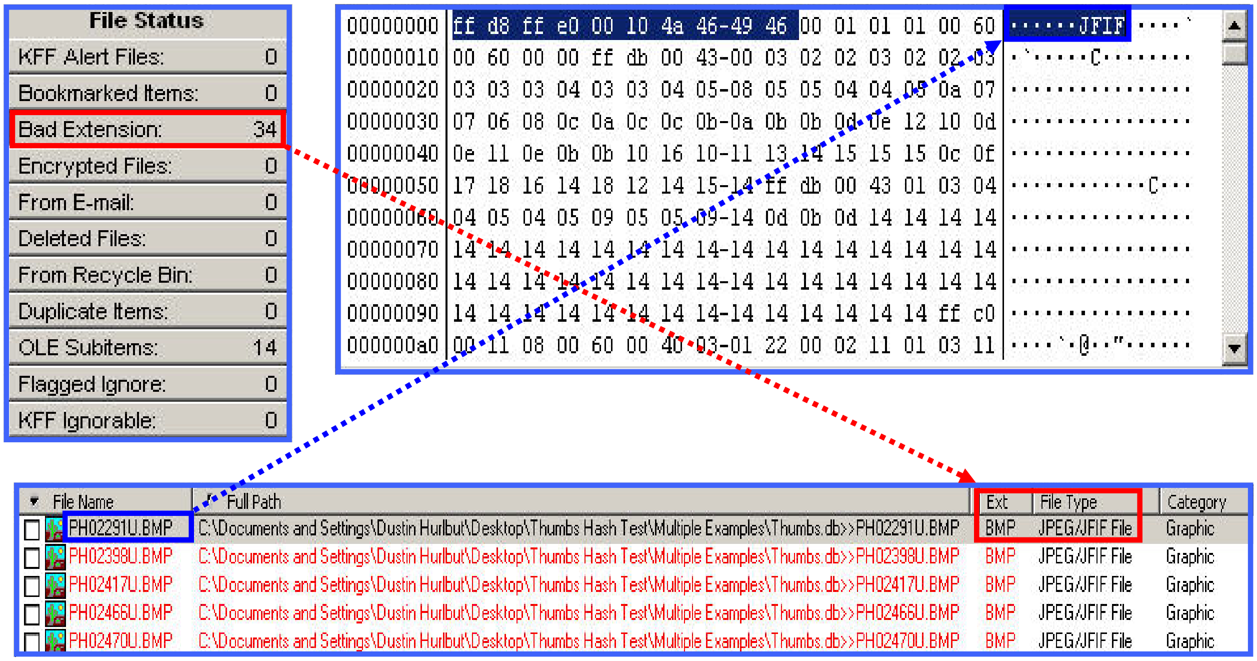
54 Listed | 0 Checked Total | C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Thumb Hash Test 01\2004_12_11 - Switzerland Day 1 005.jpg

Figure 8 - FTK View of Hashed Duplicate Thumbs.db Items

The example in Figure 8 demonstrates comparing hashes of duplicate thumbnails in a case. These thumbnails were created and then hashed by FTK. They were subsequently copied, recreated, and hashed again producing the duplicates. This can be valuable information in a graphics case to show possession or distribution by a suspect. This example simulates locating thumbnail graphics on a system along with duplicates on other media.

If encryption is an issue with a case, a JPEG, GIF, BMP or PowerPoint file that is encrypted with the Microsoft Encrypting File System (EFS) can be visible if it is saved in a thumbs.db file. The actual file will continue to be encrypted but the miniature will not. In the case of a PowerPoint file, the first slide of the series will be displayed in an unencrypted form. This security flaw was recognized by Microsoft and fixed in subsequent releases.

Another interesting aspect of the thumbs.db miniatures is that each of the created thumbnails will bear a JFIF (JPEG) header regardless of the original file's extension. This will result in FTK finding bad extensions for each of the thumbs that is not a JPEG file. In Figure 9, any .bmp files that are stored as thumbnails will have JFIF headers and will be classified in the FTK Bad Extension's container.



File Status	
KFF Alert Files:	0
Bookmarked Items:	0
Bad Extension:	34
Encrypted Files:	0
From E-mail:	0
Deleted Files:	0
From Recycle Bin:	0
Duplicate Items:	0
OLE Subitems:	14
Flagged Ignore:	0
KFF Ignorable:	0

```
00000000 ff d8 ff e0 00 10 4a 46-49 46 00 01 01 01 00 60 ······JFIF····`
00000010 00 60 00 00 ff db 00 43-00 03 02 02 03 02 02 03 ·`·····C········
00000020 03 03 03 04 03 03 04 05-08 05 05 04 04 05 0a 07 ················
00000030 07 06 08 0c 0a 0c 0c 0b-0a 0b 0b 0d 0e 12 10 0d ················
00000040 0e 11 0e 0b 0b 10 16 10-11 13 14 15 15 15 0c 0f ················
00000050 17 18 16 14 18 12 14 15-14 ff db 00 43 01 03 04 ·············C···
00000060 04 05 04 05 09 05 05 09-14 0d 0b 0d 14 14 14 14 ················
00000070 14 14 14 14 14 14 14 14-14 14 14 14 14 14 14 14 ················
00000080 14 14 14 14 14 14 14 14-14 14 14 14 14 14 14 14 ················
00000090 14 14 14 14 14 14 14 14-14 14 14 14 14 14 ff c0 ················
000000a0 00 11 08 00 60 00 40 03-01 22 00 02 11 01 03 11 ····`·@··"······
```

File Name	Full Path	Ext	File Type	Category
□ PH02291U.BMP	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Multiple Examples\Thumbs.db>>PH02291U.BMP	BMP	JPEG/JFIF File	Graphic
□ PH02398U.BMP	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Multiple Examples\Thumbs.db>>PH02398U.BMP	BMP	JPEG/JFIF File	Graphic
□ PH02417U.BMP	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Multiple Examples\Thumbs.db>>PH02417U.BMP	BMP	JPEG/JFIF File	Graphic
□ PH02466U.BMP	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Multiple Examples\Thumbs.db>>PH02466U.BMP	BMP	JPEG/JFIF File	Graphic
□ PH02470U.BMP	C:\Documents and Settings\Dustin Hurlbut\Desktop\Thumbs Hash Test\Multiple Examples\Thumbs.db>>PH02470U.BMP	BMP	JPEG/JFIF File	Graphic

Figure 9 - Thumbs.db Bad Extensions in FTK

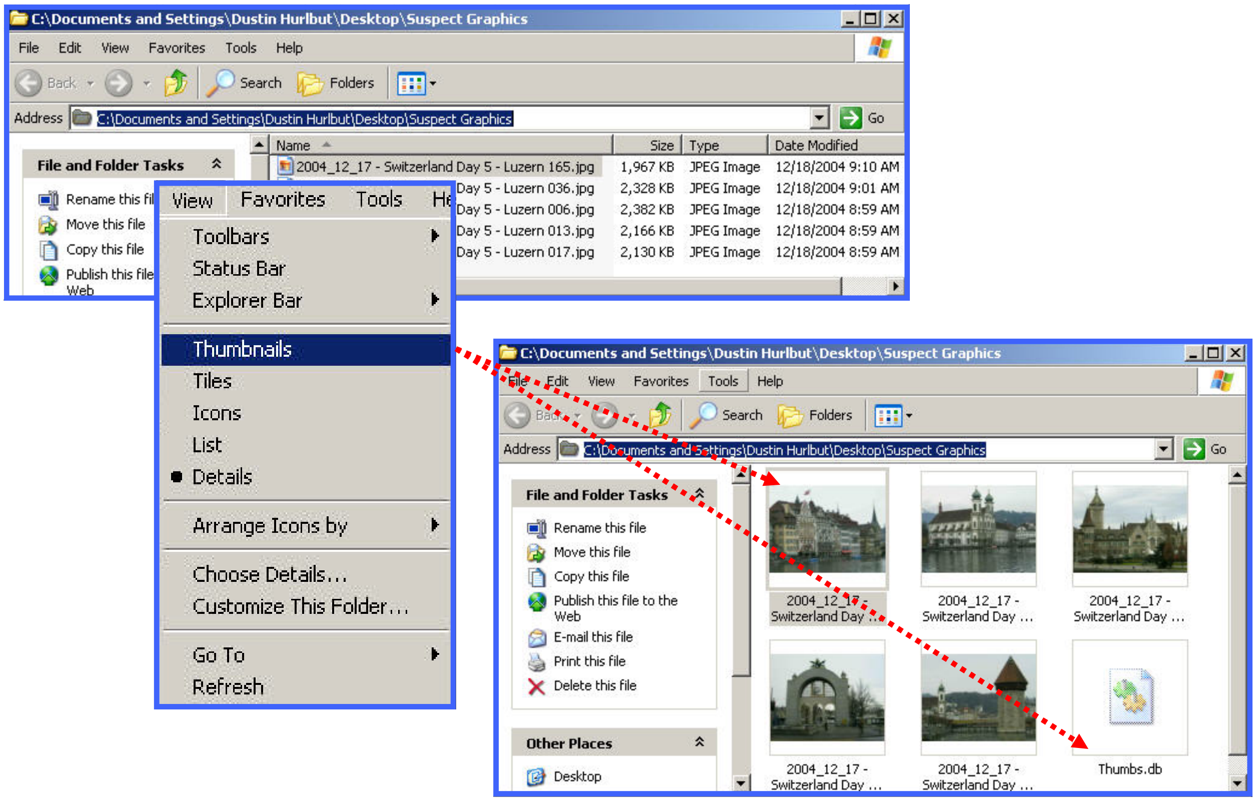
It isn't uncommon to find hundreds of files in the Bad Extension container. While this used to be a low tech method of hiding graphics from older style viewers that read files by extension rather then header, It isn't commonly used anymore. Seeing the bad extensions can lead to questions about why someone would change a .JPG to a .BMP until realizing they are from the thumbnail viewer in Windows.

An Exercise in Hashing Thumbnails

This exercise will duplicate the circumstance cited early of the investigation by Tanja Giacovelli. We'll presuppose we have a suspect who claims to have no child pornography on his system but does have thumbs.db files that appear to have incriminating graphics in them. This exercise will give you experience in creating and viewing thumbs.db files as well as creating a hash set for comparative purposes. This exercise will only work in Windows XP (and on Windows 2000 if the media is formatted in FAT).

Creating the Files - Create a folder on your desktop called "Suspect Graphics". Place four or five graphics in this folder. You can use photos, internet graphics, or sample graphics found in My Documents > My Pictures if you have them.

Creating the Thumbnails - Navigate to this folder in Windows Explorer and Select View > Thumbnails. This will create the thumbs.db file and display the graphics as thumbnails. See Figure 10 for these preliminary steps.



C:\Documents and Settings\Dustin Hurlbut\Desktop\Suspect Graphics

Address C:\Documents and Settings\Dustin Hurlbut\Desktop\Suspect Graphics

Name	Size	Type	Date Modified
2004_12_17 - Switzerland Day 5 - Luzern 165.jpg	1,967 KB	JPEG Image	12/18/2004 9:10 AM
Day 5 - Luzern 036.jpg	2,328 KB	JPEG Image	12/18/2004 9:01 AM
Day 5 - Luzern 006.jpg	2,382 KB	JPEG Image	12/18/2004 8:59 AM
Day 5 - Luzern 013.jpg	2,166 KB	JPEG Image	12/18/2004 8:59 AM
Day 5 - Luzern 017.jpg	2,130 KB	JPEG Image	12/18/2004 8:59 AM

Figure 10 - Creating Sample Thumbnails and a Thumbs.db

If you don't see the thumbs.db file on your system, first make sure you have show hidden files and folders selected in your Windows Explorer Options Tab. Go to Windows Explorer, select Tools > Folder Options, select the View tab and check the "Show hidden files and folders" option as well as unselecting "Hide extensions for known file types" and unselecting "Hide protected operating system files". If you still don't see it, you may have a Windows 2000 operating system working on an NTFS drive in which case you will not have a thumbs.db but rather Alternate Data Streams handling the thumbnails.

Simulating the Suspect Moving the Graphics - Now we will simulate the suspect moving the graphics to removable media off the computer system. As in Tanja's example, the suspect inadvertently moved the thumbs.db files as well as the actual graphics to a CD. Start by creating a second folder on the Desktop named "Moved Suspect Graphics". Then copy the graphics and the existing thumbs.db file to this new folder.

Suspect Graphics
Copying Graphics Files and the Thumbs.db
Moved Suspect Graphics

Figure 11 - Copying the Files from the Suspect System to a Simulated Removable Media

Next, delete the files from the Suspect Graphics folder taking care not to delete the thumbs.db file. We have now duplicated what the suspect did. He copied the files to CD along with the thumbs.db and then deleted the graphics files from the original location leaving the thumbs.db file behind. Remember, the thumbs.db file is a protected system hidden file. If the suspect didn't have his Explorer set to view such files he would not see it to delete it.

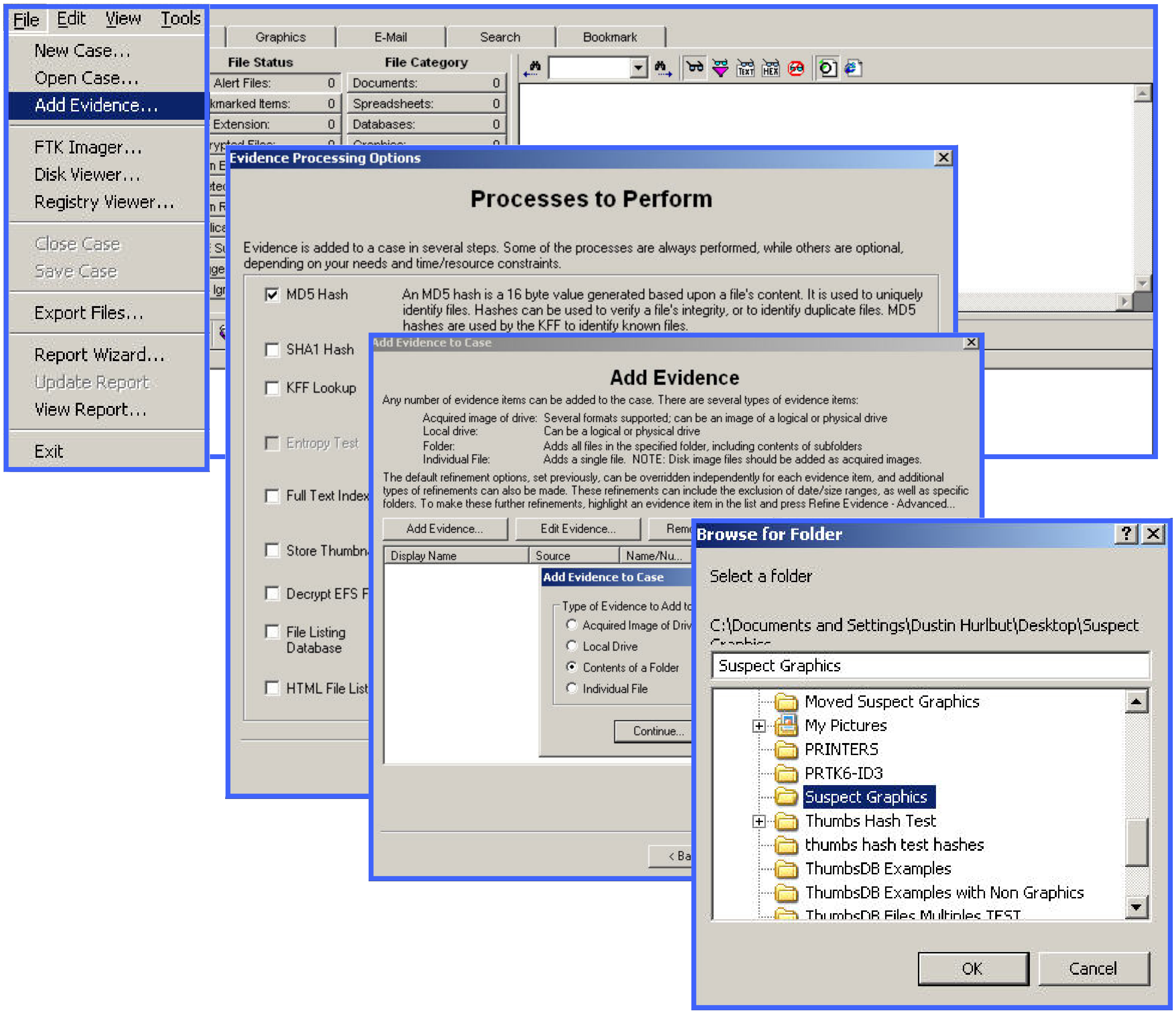
Hashing the Thumbnails - Now we have the Suspect Graphics folder containing only a thumbs.db file. This thumbs.db file will contain miniature images of the original graphics we deleted. We will hash these items and add them to the hash library to compare to the copied thumbnails in the Moved Suspect Graphics folder.

Step 1 - Open FTK and select "Go directly to working in program".

Step 2 - Select File > Add Evidence, select Next, and deselect all processes to perform except MD5 Hash finishing with Next.

Step 3 - Select Add Evidence, Contents of a Folder and continue.

Step 4 - Navigate to the Suspect Graphics folder on the Desktop, select OK, and Next, and Next again to bring in the folder to FTK.



Alert Files: 0
kmarked Items: 0
Extension: 0
Documents: 0
Spreadsheets: 0
Databases: 0

Evidence Processing Options

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.

☑ 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.

☐ SHA1 Hash

☐ KFF Lookup

☐ Entropy Test

☐ Full Text Index

☐ Store Thumbn

☐ Decrypt EFS F

☐ File Listing Database

☐ HTML File List

Add Evidence to Case

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 to Case

Type of Evidence to Add to

○ Acquired Image of Driv
○ Local Drive
● Contents of a Folder
○ Individual File

Browse for Folder

Select a folder

C:\Documents and Settings\Dustin Hurlbut\Desktop\Suspect Graphics

Suspect Graphics

Moved Suspect Graphics
My Pictures
PRINTERS
PRTK6-ID3
Suspect Graphics
Thumbs Hash Test
thumbs hash test hashes
ThumbsDB Examples
ThumbsDB Examples with Non Graphics
ThumbsDB Files Multiples TEST

Figure 12 - Adding Suspect Graphics Folder to FTK

Next, we'll create the hash set of the original thumbs.db by using the FTK command of Copy Special. This will create the hash set we need to export to our custom hash database.

Step 1 - Select the Overview tab and then select the Total File Items container button.

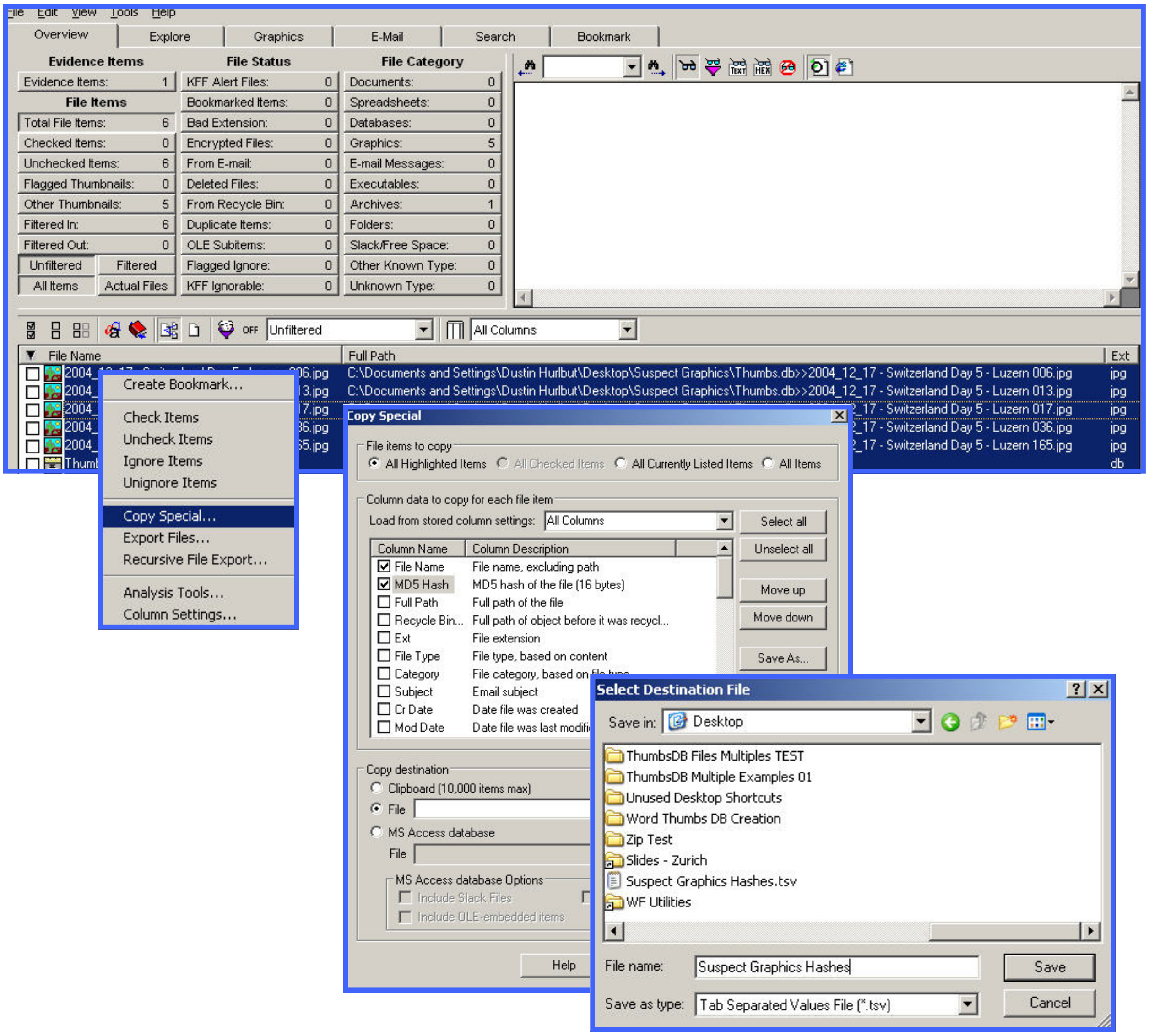
Step 2 - In the File List Pane at the bottom, highlight all the graphics and the thumbs.db file, right click and select Copy Special.

Step 3 - In the Copy Special dialog box, select "Unselect All".

Step 4 - Place a checkmark next to the File Name column and the MD5 Hash column (near the bottom).

Step 5 - Select a copy destination of "File" and browse to the Desktop naming it Suspect Graphics Hashes.

Step 6 - Select the Copy button to send the hash list to the file on the Desktop.



Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	6	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	5
Unchecked Items:	6	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	0	Executables:	0
Other Thumbnails:	5	From Recycle Bin:	0	Archives:	1
Filtered In:	6	Duplicate Items:	0	Folders:	0
Filtered Out:	0	OLE Subitems:	0	Slack/Free Space:	0
Unfiltered / Filtered		Flagged Ignore:	0	Other Known Type:	0
All Items / Actual Files		KFF Ignorable:	0	Unknown Type:	0

File Name	Full Path	Ext
2004_...06.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Suspect Graphics\Thumbs.db>>2004_12_17 - Switzerland Day 5 - Luzern 006.jpg	jpg
2004_...3.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Suspect Graphics\Thumbs.db>>2004_12_17 - Switzerland Day 5 - Luzern 013.jpg	jpg
2004_...7.jpg	..._17 - Switzerland Day 5 - Luzern 017.jpg	jpg
2004_...6.jpg	..._17 - Switzerland Day 5 - Luzern 036.jpg	jpg
2004_...5.jpg	..._17 - Switzerland Day 5 - Luzern 165.jpg	jpg
Thumb...		db

Copy Special

File items to copy: ● All Highlighted Items ○ All Checked Items ○ All Currently Listed Items ○ All Items

Column data to copy for each file item

Load from stored column settings: All Columns

Column Name	Column Description
☑ File Name	File name, excluding path
☑ MD5 Hash	MD5 hash of the file (16 bytes)
□ Full Path	Full path of the file
□ Recycle Bin...	Full path of object before it was recycl...
□ Ext	File extension
□ File Type	File type, based on content
□ Category	File category, based on file type
□ Subject	Email subject
□ Cr Date	Date file was created
□ Mod Date	Date file was last modifi...

Copy destination: ○ Clipboard (10,000 items max) ● File ○ MS Access database

MS Access database Options: □ Include Slack Files □ Include OLE-embedded items

Select Destination File

Save in: Desktop

- ThumbsDB Files Multiples TEST
- ThumbsDB Multiple Examples 01
- Unused Desktop Shortcuts
- Word Thumbs DB Creation
- Zip Test
- Slides - Zurich
- Suspect Graphics Hashes.tsv
- WF Utilities

File name: Suspect Graphics Hashes

Save as type: Tab Separated Values File (*.tsv)

Figure 13 - Creating Hash Sets in FTK with Copy Special

We now have a hash list of the thumbnails that existed in the thumbs.db file as well as of the thumbs.db itself. Now, we want to compare them to what is in the Moved Suspect Graphics folder we created. However, we have another step to take before leaving the current FTK session. We need to place those hashes we want to compare into the hash library.

Step 1 - Go to the Tools menu in FTK and select Import KFF Hashes.

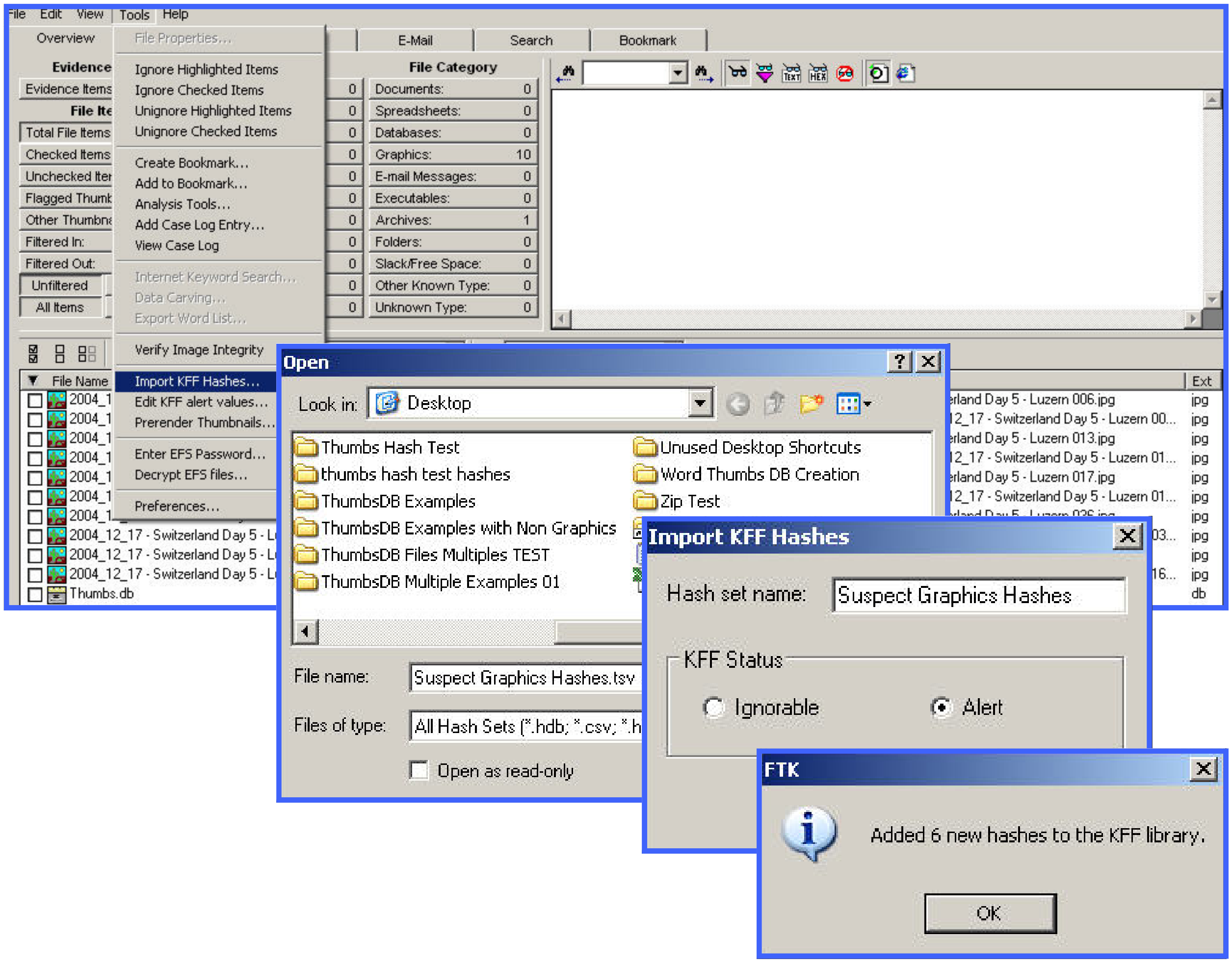
Step 2 - Browse to the file Suspect Graphics Hashes.CSV and select Open.

Step 3 - Name the hash set Suspect Graphics Hashes and set them to Alert.

Step 4 - You will receive a dialog box stating the number of new hashes you added to the library.

NOTE: If you wish to create a custom hash library for this exercise instead of using the standard AccessData KFF library, you can download the "empty.hdb" file from the AccessData website and use it instead. Just make sure you change the pointer to that library from the default in the Tools > Options menu in FTK.

empty.hdb is located at the bottom of the downloads web page



Open

Look in: Desktop

File name: Suspect Graphics Hashes.tsv

Files of type: All Hash Sets (*.hdb; *.csv; *.h

□ Open as read-only

Import KFF Hashes

Hash set name: Suspect Graphics Hashes

KFF Status

○ Ignorable ● Alert

FTK

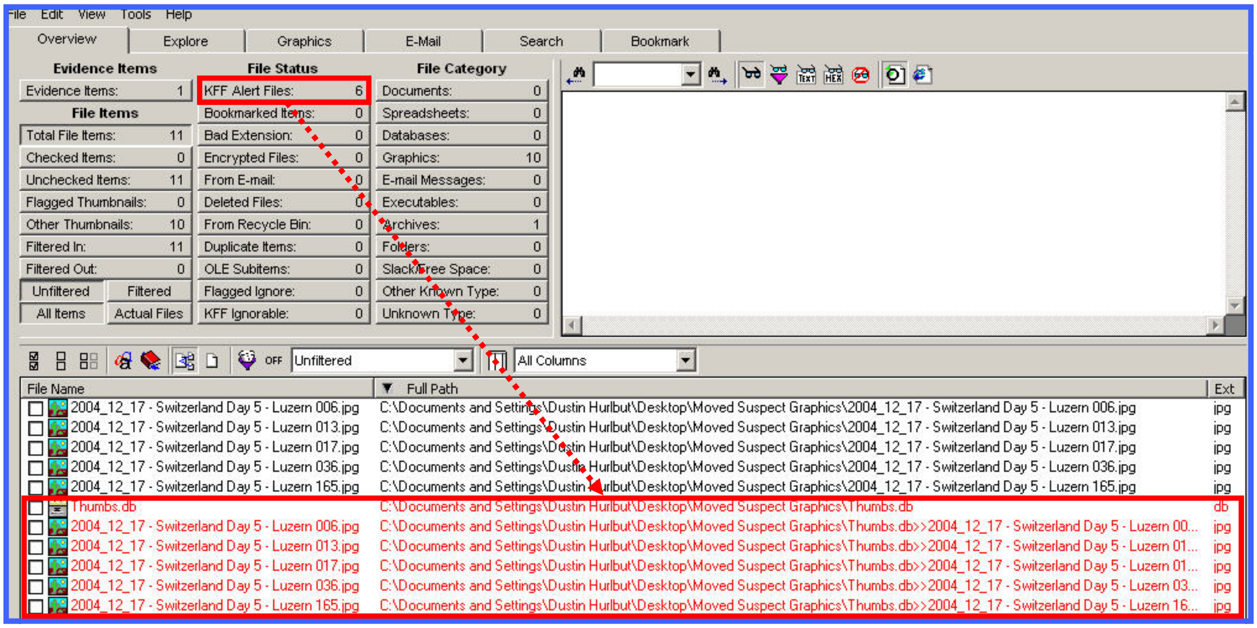
Added 6 new hashes to the KFF library.

OK

Figure 14 - Importing New Hashes into FTK

Now, we're ready to compare the hashes in the thumbnails copied over previously in the Moved Suspect Graphics folder. Close the current case in FTK and start another with File > Add Evidence and add the folder Moved Suspect Graphics. Be sure to select the process of MD5 Hash and KFF Lookup to compare the previous hashes.

When you are done, you should have KFF Alerts showing the graphic thumbnails that compared to the original as well as the original thumbs.db file itself (See Figure 15). This demonstrates that those files are duplicates of the ones found in the Moved Suspect Graphics folder.



Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	6	Documents:	0
File Items		Bookmarked Items:	0	Spreadsheets:	0
Total File Items:	11	Bad Extension:	0	Databases:	0
Checked Items:	0	Encrypted Files:	0	Graphics:	10
Unchecked Items:	11	From E-mail:	0	E-mail Messages:	0
Flagged Thumbnails:	0	Deleted Files:	0	Executables:	0
Other Thumbnails:	10	From Recycle Bin:	0	Archives:	1
Filtered In:	11	Duplicate Items:	0	Folders:	0
Filtered Out:	0	OLE Subitems:	0	Slack/Free Space:	0
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	0
All Items	Actual Files	KFF Ignorable:	0	Unknown Type:	0

File Name	Full Path	Ext
□ 2004_12_17 - Switzerland Day 5 - Luzern 006.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\2004_12_17 - Switzerland Day 5 - Luzern 006.jpg	jpg
□ 2004_12_17 - Switzerland Day 5 - Luzern 013.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\2004_12_17 - Switzerland Day 5 - Luzern 013.jpg	jpg
□ 2004_12_17 - Switzerland Day 5 - Luzern 017.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\2004_12_17 - Switzerland Day 5 - Luzern 017.jpg	jpg
□ 2004_12_17 - Switzerland Day 5 - Luzern 036.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\2004_12_17 - Switzerland Day 5 - Luzern 036.jpg	jpg
□ 2004_12_17 - Switzerland Day 5 - Luzern 165.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\2004_12_17 - Switzerland Day 5 - Luzern 165.jpg	jpg
□ Thumbs.db	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\Thumbs.db	db
□ 2004_12_17 - Switzerland Day 5 - Luzern 006.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\Thumbs.db>>2004_12_17 - Switzerland Day 5 - Luzern 00...	jpg
□ 2004_12_17 - Switzerland Day 5 - Luzern 013.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\Thumbs.db>>2004_12_17 - Switzerland Day 5 - Luzern 01...	jpg
□ 2004_12_17 - Switzerland Day 5 - Luzern 017.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\Thumbs.db>>2004_12_17 - Switzerland Day 5 - Luzern 01...	jpg
□ 2004_12_17 - Switzerland Day 5 - Luzern 036.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\Thumbs.db>>2004_12_17 - Switzerland Day 5 - Luzern 03...	jpg
□ 2004_12_17 - Switzerland Day 5 - Luzern 165.jpg	C:\Documents and Settings\Dustin Hurlbut\Desktop\Moved Suspect Graphics\Thumbs.db>>2004_12_17 - Switzerland Day 5 - Luzern 16...	jpg

Figure 15 - KFF Alert Hits from Moved Suspect Graphics Folder

We have simulated a suspect placing graphics on a USB drive or a CD and inadvertently adding the thumbs.db file. The suspect then deletes the original graphics leaving the thumbs.db behind on their computer. We then compared what is found on the suspect's main system with those files found on the removable media and found exact matches via hashes.

Thumbs.db files can be crucial to a case, especially in circumstances where the suspect does not store the graphics files on their system. Since they are hidden system files, often suspects will not be aware of the presence and you can use them to show constructive possession or even distribution.

AccessData