

SEARCH



2012 San Diego International Conference on Child and Family Maltreatment

FTK Demo



FTK Demo

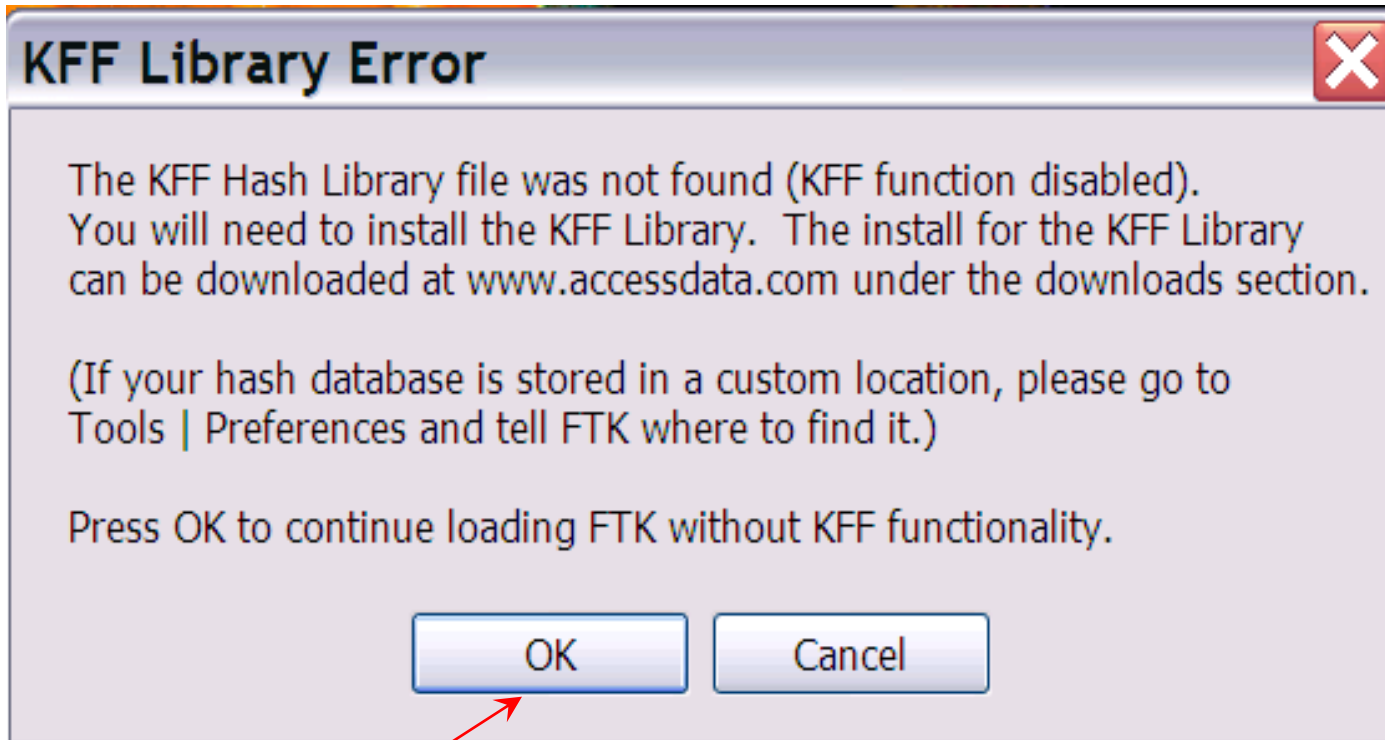
- The Demo version of FTK, `ftk-forensic_toolkit-1.71.exe` is a free demonstration tool from Access Data can be used to demonstrate the usefulness of the FTK software
- SEARCH uses this software to import a RAM dump for demonstration purposes only
- This Demo version of FTK is limited to 5000 file items and can not be used in court

Double Click on the `ftk-forensic_toolkit-1.71.exe` file to start the Demo version of FTK.



FTK Demo

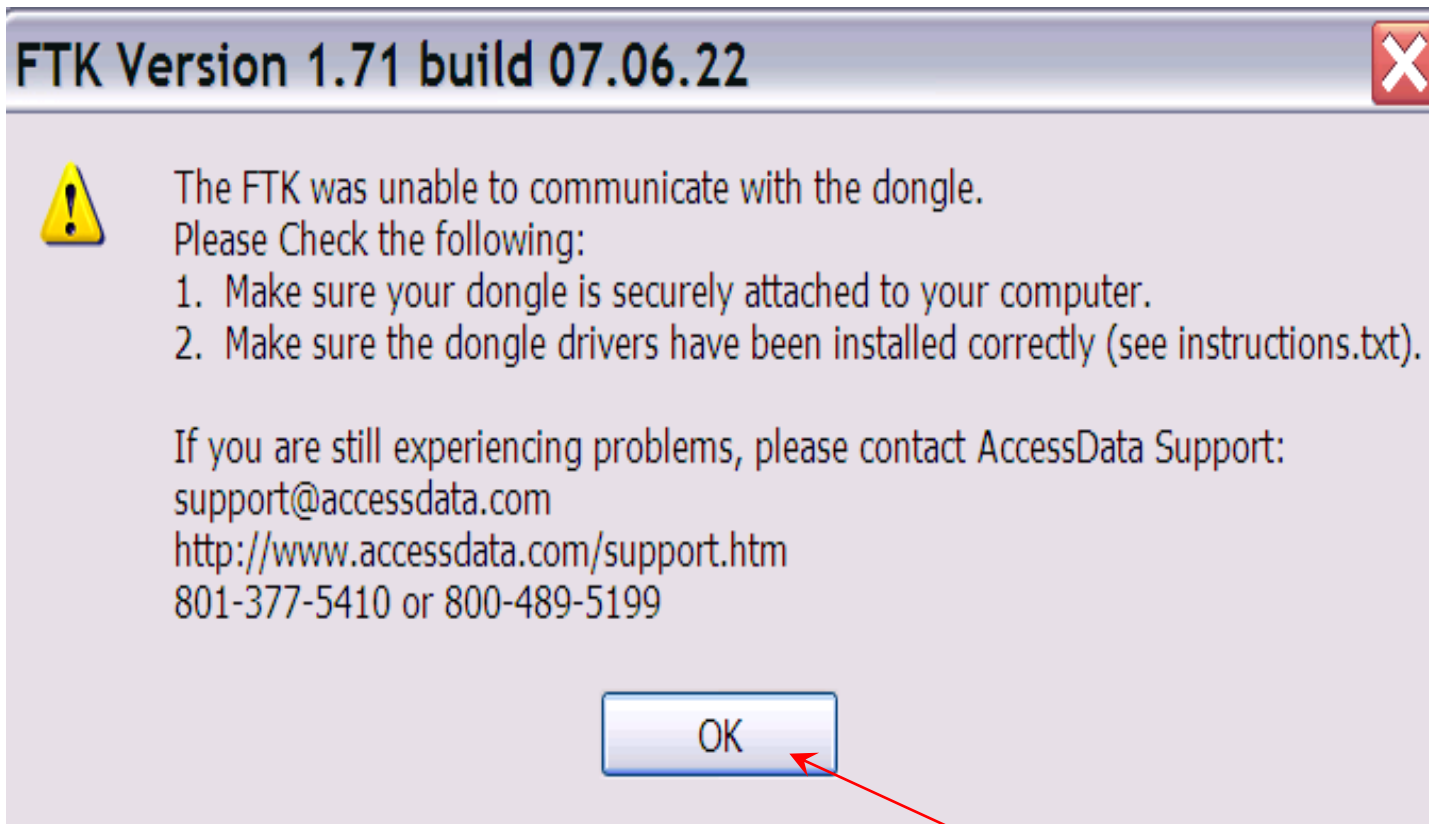
We have no KFF Hash Library so select the "OK" option





FTK Demo

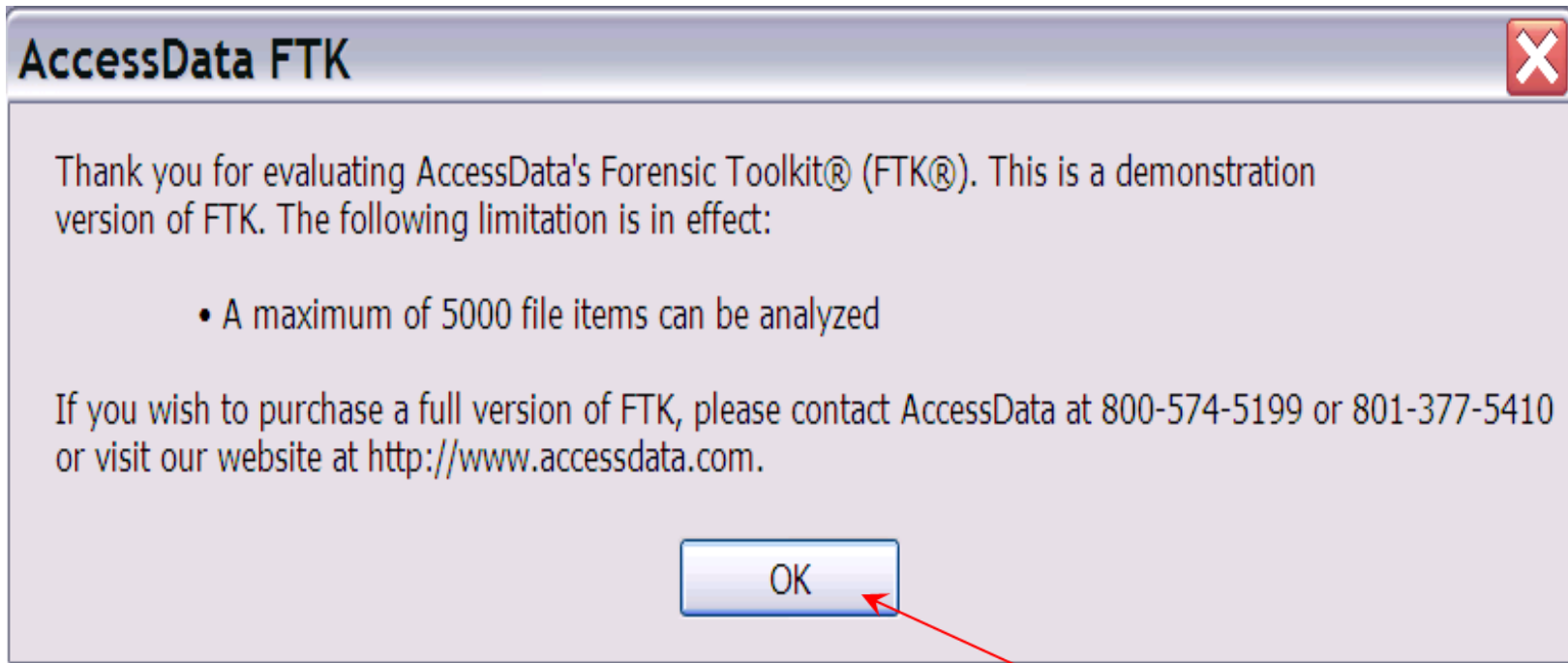
We have no FTK dongle, select "OK"





FTK Demo

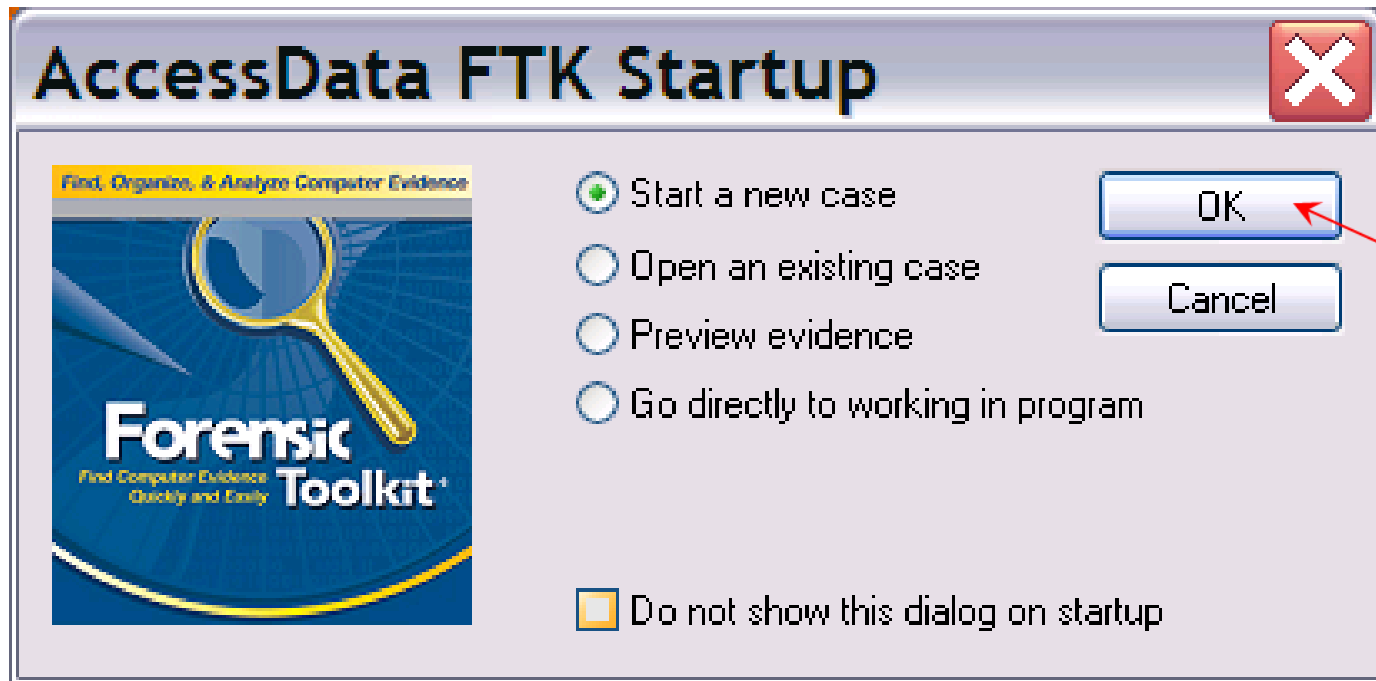
The Demo version can only handle 5000 file items at a time, select "OK"





FTK Demo

Click on "Start a New Case, the click on "OK"





FTK Demo

You must fill in

- Investigator's Name,
 - Case Number,
 - Case Name,
- and the
- Path where you wish to save the case.

New Case

Find, Organize, & Analyze Computer Evidence

Forensic Toolkit
Find Computer Evidence Quickly and Easily

**AccessData's
Forensic Toolkit®-FTK®**
The Complete Analysis Tool

Wizard for Creating a New Case

Investigator Name: Test

Case Information

Case Number: 0001

Case Name: Test Case

Case Path: C:\Documents and Settings\CArmstrong\Desktop\ Browse...

Case Folder: C:\Documents and Settings\CArmstrong\Desktop\Test Case

Case Description:

Next > Cancel



FTK Demo

Leave the Case Information window blank, click "Next"

FTK Report Wizard - Case Information ✕

Forensic Examiner Information

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

Agency/Company:

Examiner's Name:

Address:

Phone: Fax:

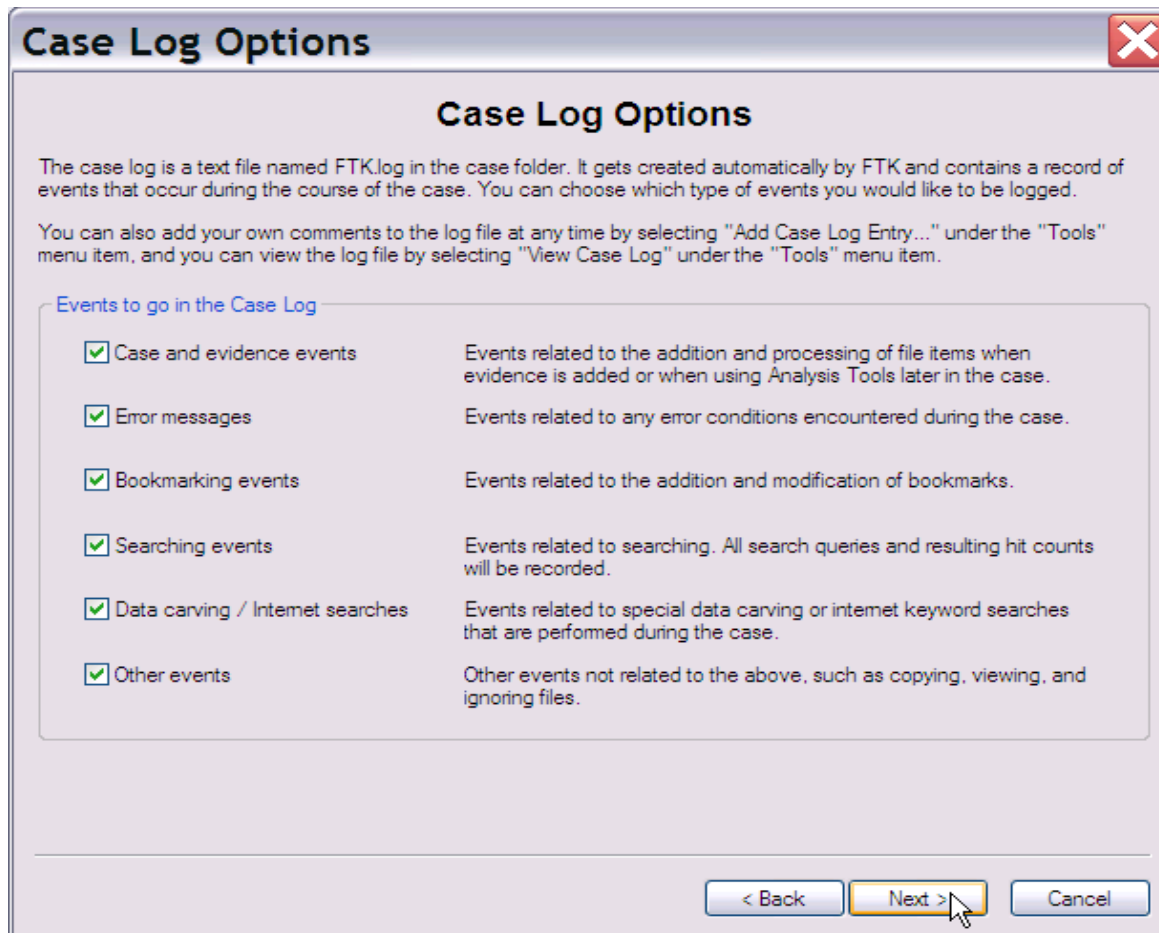
E-Mail:

Comments:

< Back **Next >** Cancel



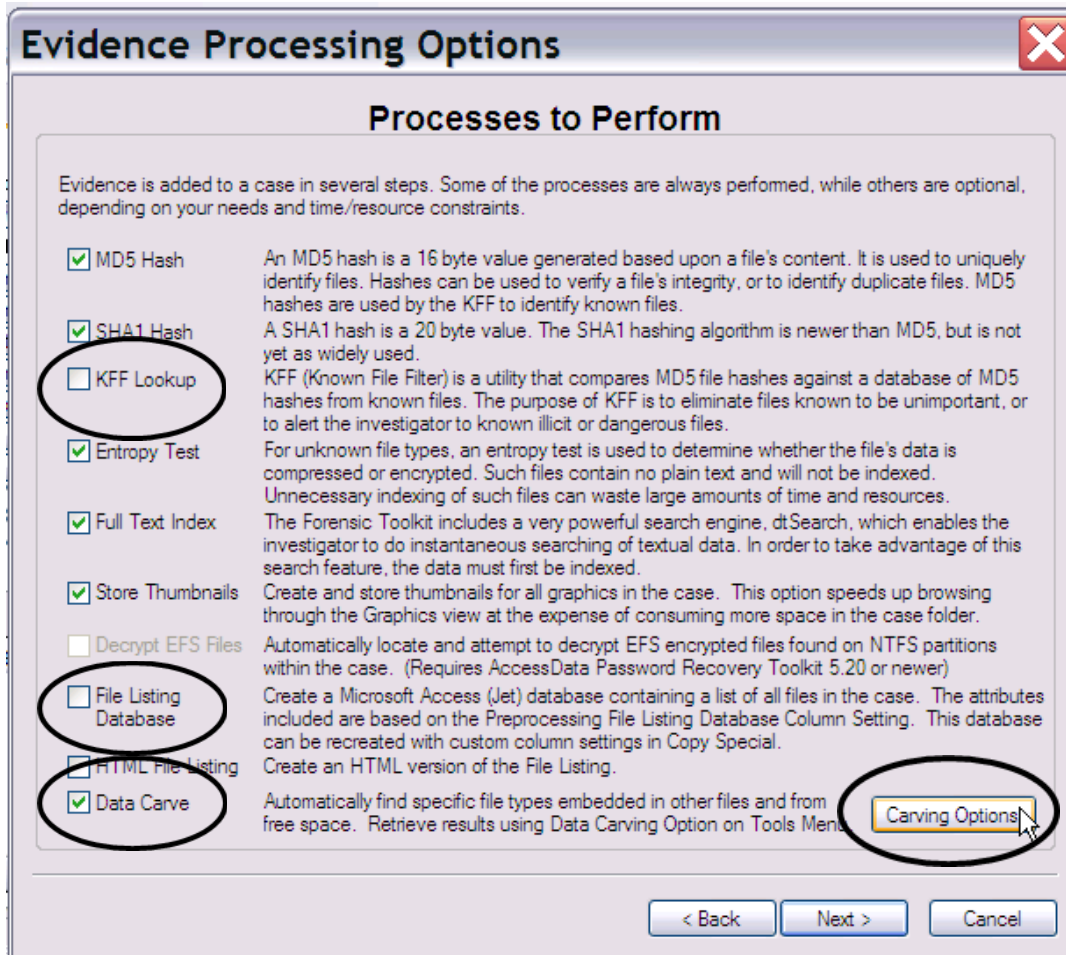
Leave the Case Log Options default, click "Next"





FTK Demo

In the Evidence Processing Options window we make changes.



Uncheck "KFF Lookup"

Uncheck "File Listing Database"

Check "Data Carve"

Click "Carving Options"

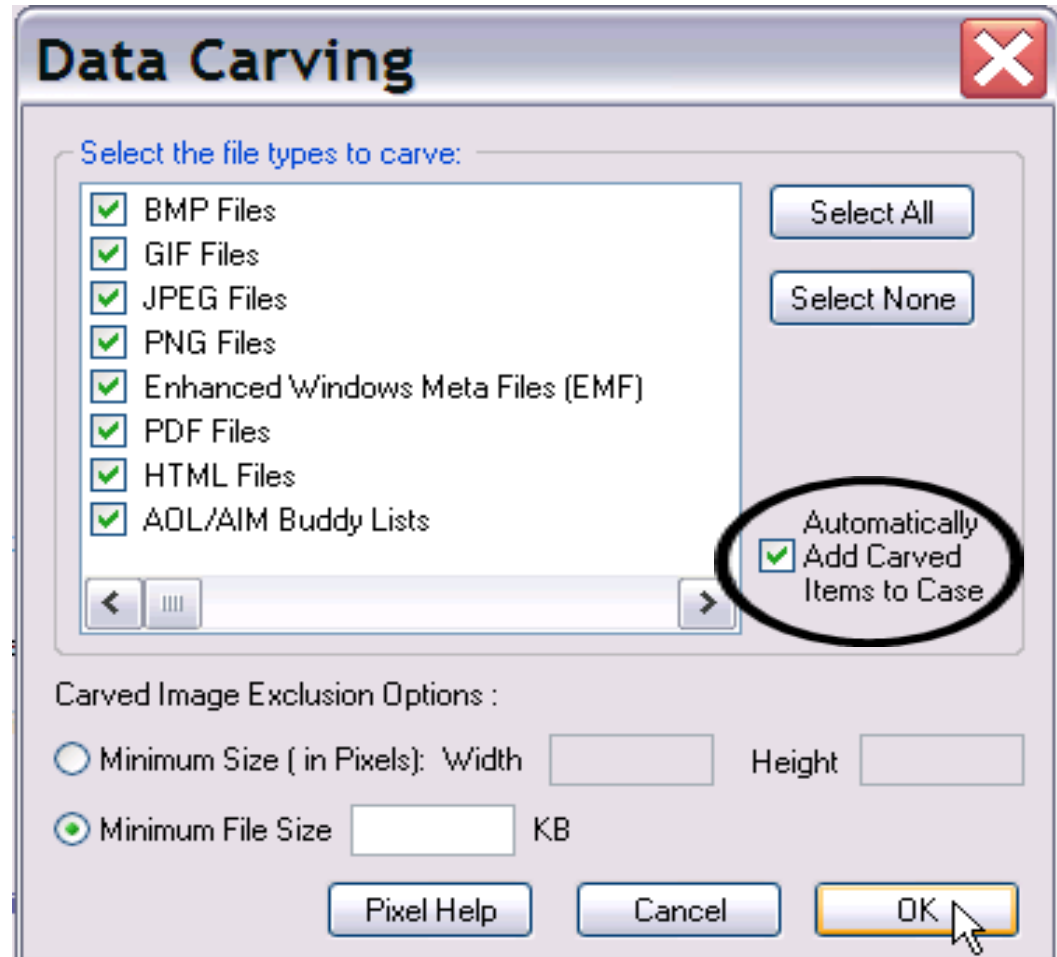


FTK Demo

“Carving Options” will take you to a second window, titled “Data Carving”

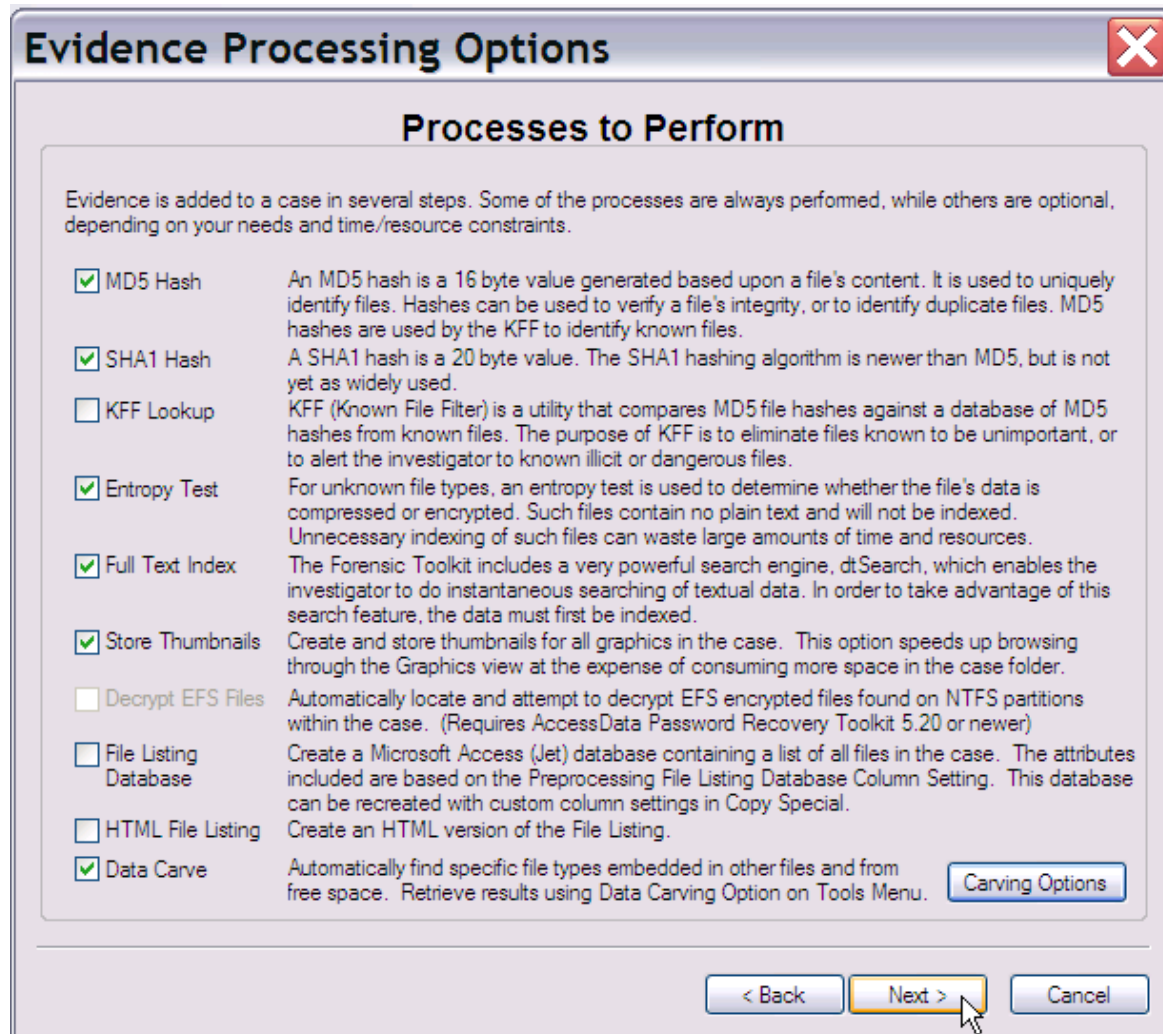
Make sure all of the options are checked and make sure “Automatically Add Carved Items to Case” is checked.

Click on “OK”





Click "Next"





FTK Demo

Leave the Refine Case window default, click "Next"



Leave the Refine Index window default, click "Next"

Refine Index - Default

In order to save time and resources, and/or to make searching more efficient, you may choose to exclude certain kinds of data from being indexed. Here, you can choose default settings that will apply to each evidence item that gets added to the case. To exclude items from being indexed, make any changes to the settings below. Note: any items that don't get indexed initially can be indexed later by clicking on "Analysis Tools" under the "Tools" menu item.

Unconditionally Index

- File Slack (data beyond the end of the logical file but within the area allocated to that file by the file system)
- Free Space (areas in the file system not currently allocated to any file, but possibly containing deleted file data)
- KFF Ignorable Files (files found by KFF to be forensically unimportant, i.e., OS system files, known applications, etc.)

Conditionally Index

Index other items in the case only if they satisfy **BOTH the file status and the file type** criteria

File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
<input type="radio"/> Deleted	<input type="radio"/> Encrypted	<input type="radio"/> From email
<input type="radio"/> Not deleted	<input type="radio"/> Not encrypted	<input type="radio"/> Not from email
<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either	<input checked="" type="radio"/> Either

Include Duplicate Files OLE Streams

File Type Criteria

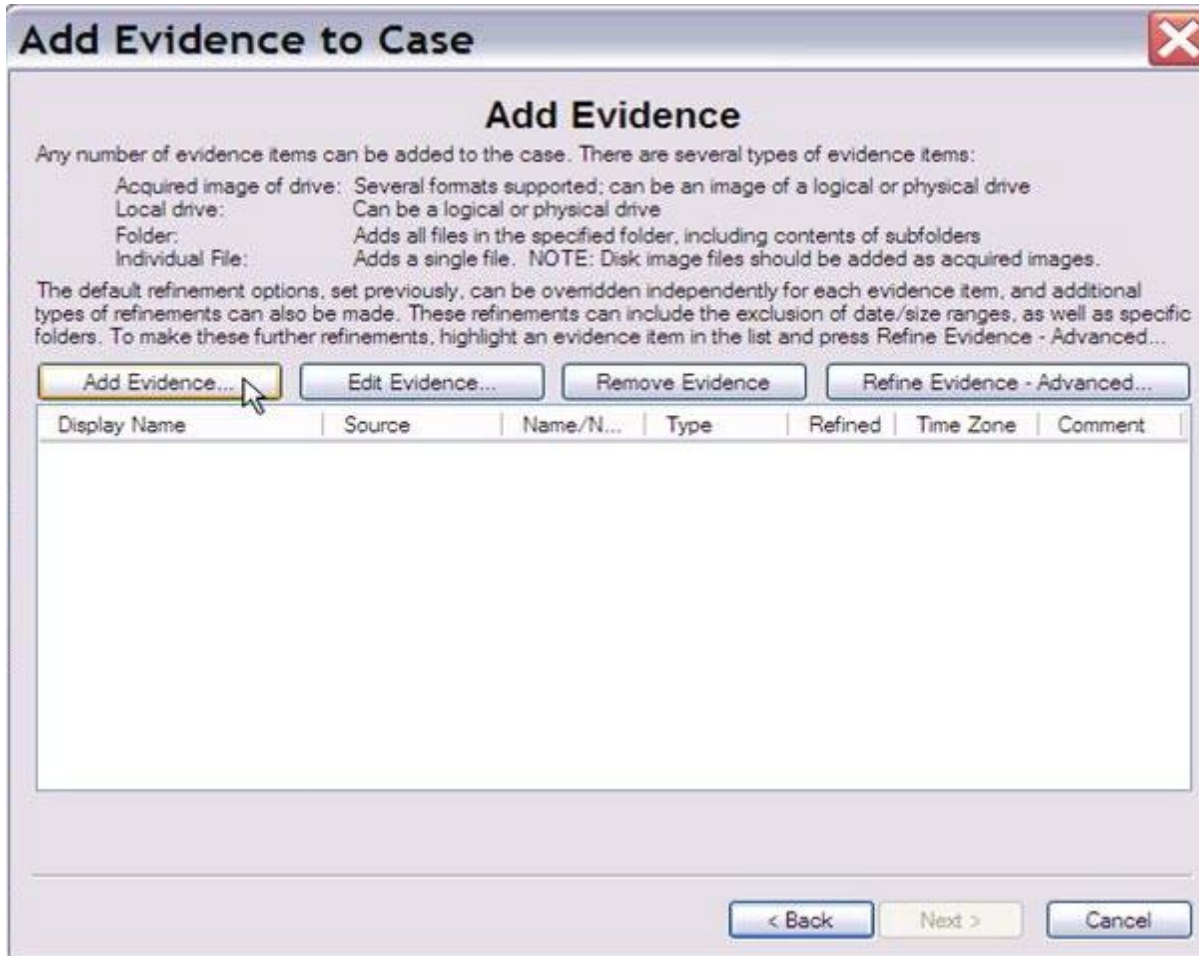
- Documents
- Executables
- Spreadsheets
- Archives
- Databases
- Folders
- Graphics
- Other Known
- Multimedia
- Unknown
- Email msg

< Back **Next** Cancel



FTK Demo

In the Add Evidence window click on “Add Evidence”

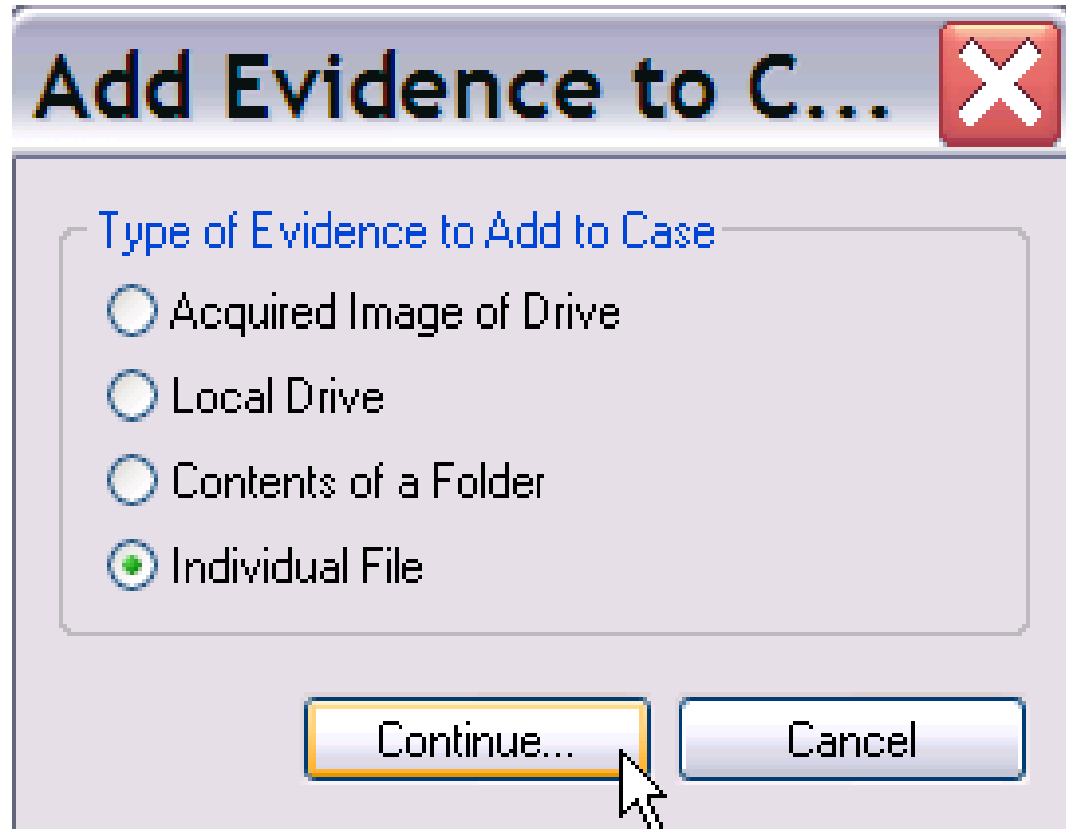




FTK Demo

We want to add an "Individual File", the RAM dump file.

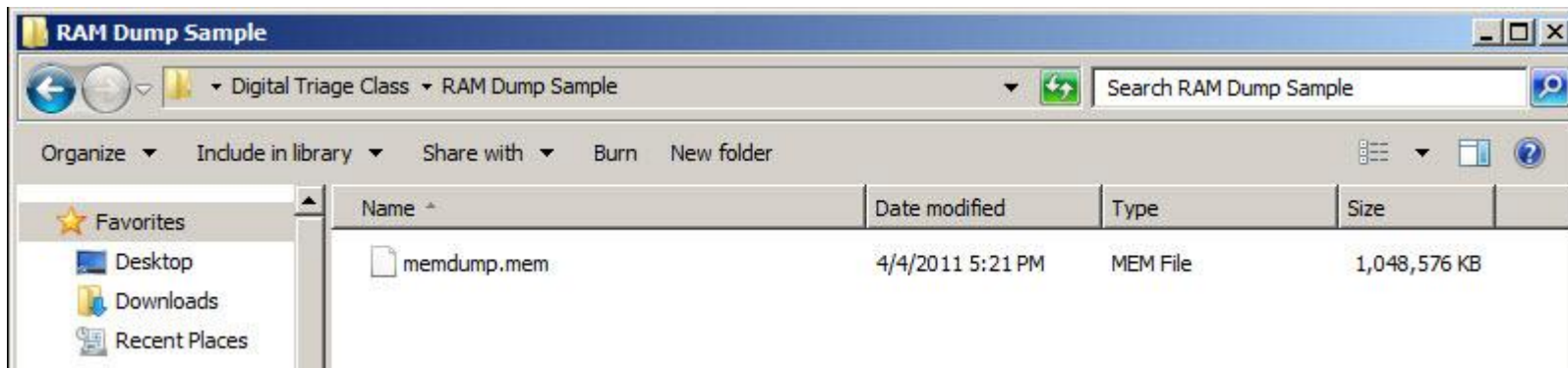
Click "Individual File", then "Continue".





FTK Demo

Navigate to the Digital Triage Class folder then click on the memdump.mem file.





FTK Demo

Click on "OK"

The screenshot shows a dialog box titled "Evidence Information" with a close button (X) in the top right corner. The dialog contains the following fields:

- Evidence Location:** A text box containing the path "C:\Documents and Settings\CArmstrong\Desktop\CoreDump\Co".
- Evidence Display Name:** A text box containing "CoreDump".
- Evidence Identification Name/Number:** An empty text box.
- Comment:** A large empty text area.
- Local Evidence Time Zone:** A dropdown menu currently showing "Choose time zone for evidence ...".

At the bottom of the dialog are two buttons: "OK" and "Cancel".



FTK Demo

In the Add Evidence Window, Click "Next"

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...

Buttons: Add Evidence..., Edit Evidence..., Remove Evidence, Refine Evidence - Advanced...

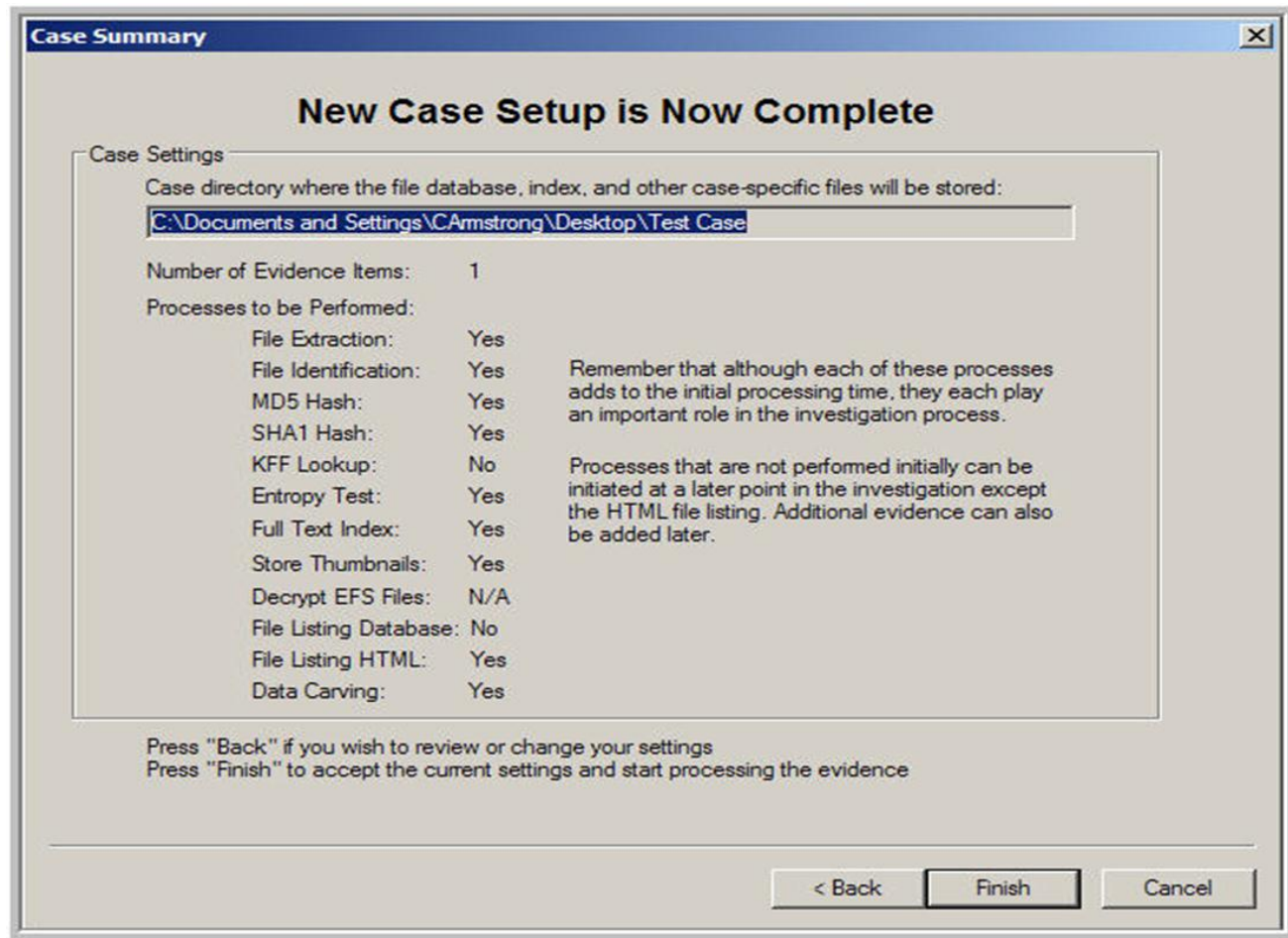
Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
CoreDump	C:\Documents...		Individual f...	N	N/A	

Buttons: < Back, Next >, Cancel



FTK Demo

Click "Finish" and FTK Demo will start carving the data from the RAM dump.





This may take a while.

Processing Files...

Current Evidence Item:
C:\Documents and Settings\CArmstrong\Desktop\CoreDump\CoreDump.dd

Current File Item:
C:\Documents and Settings\CArmstrong\Desktop\CoreDump\CoreDump.dd

Current File Item Status	Total Process Status
Action: Hashing and Entropy Test	Elapsed Time: 0:00:00:04
File Type: Unknown File Type	Total Items Examined: 1
Item Size: 1,064,103,936	Total Items Added: 0
Progress: 229,580,800	Total Items Indexed: 0

Log the case/system status every minutes Log extended information



FTK Demo

When FTK is finished, the RAM dump file will show up as an Evidence File.

The screenshot shows the AccessData FTK 1.71 DEMO VERSION interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu bar are tabs for Overview, Explore, Graphics, E-Mail, Search, and Bookmark. The main window is divided into several sections:

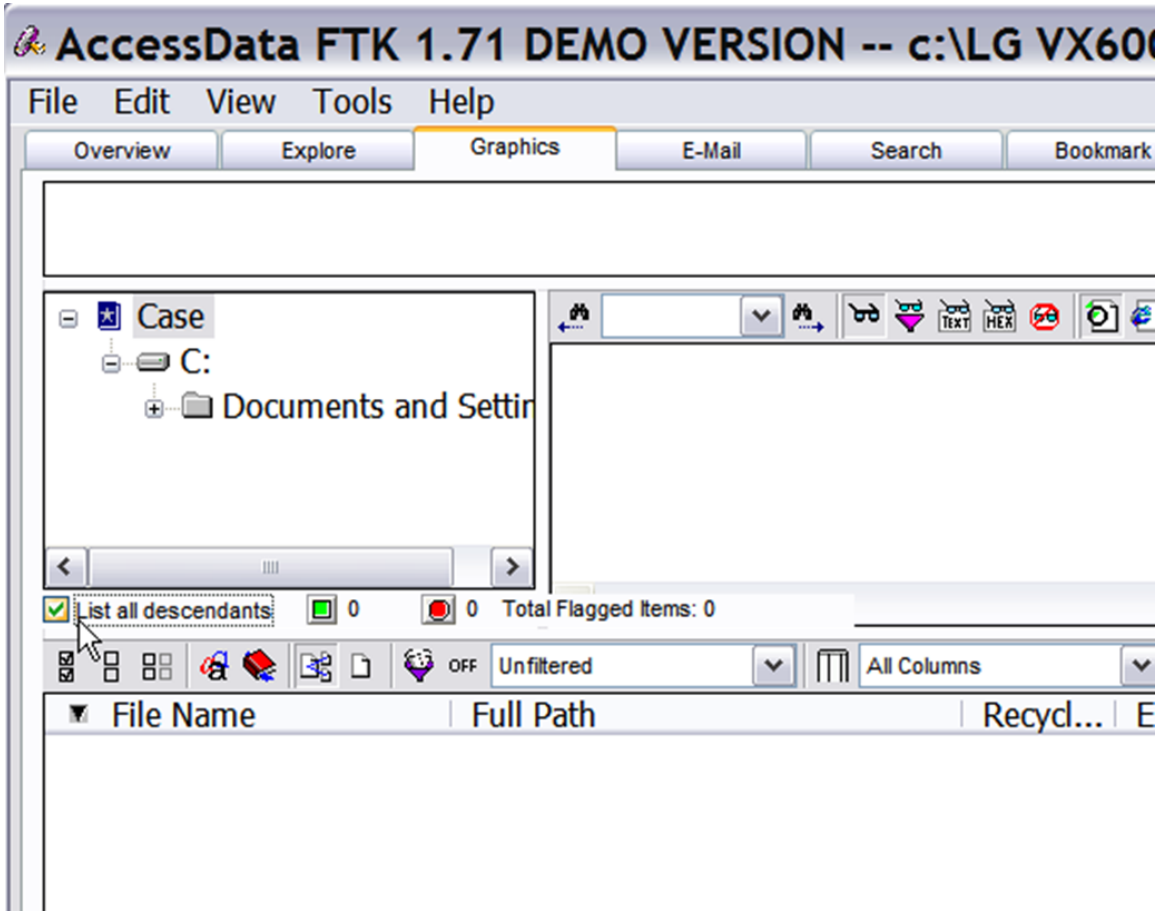
- Evidence Items:** A summary table showing counts for various file categories.
- File Status:** A table showing counts for file status categories.
- File Category:** A table showing counts for file category categories.
- Table:** A table listing evidence files with columns: Evidence File Name, Evidence Path, Display Name, Identification Name/Number, Evidence Type, Added, Children, Descendants, and Investigator's Name.

Evidence File Name	Evidence Path	Display Name	Identification Name/Number	Evidence Type	Added	Children	Descendants	Investigator's Name
CoreDump.dd	C:\Documents and Settings\CArmstrong\Desktop\...	CoreDump		Individual file	9/23/2008 9:34:51 AM			Test

At the bottom of the window, there is a status bar showing: 1 Listed, 0 Checked Total, 0 Highlighted.



FTK Demo



To view results, click on the heading, in this case "Graphics" then click on "List all descendants"



FTK Demo

Review the results by scrolling down the list.

The screenshot displays the AccessData FTK 1.71 DEMO VERSION interface. The top menu bar includes File, Edit, View, Tools, and Help. Below the menu is a toolbar with icons for Overview, Explore, Graphics, E-Mail, Search, and Bookmark. The main window is divided into three panes: Evidence Items, File Status, and File Category. The Evidence Items pane shows a summary of 662 total file items, including 558 thumbnails and 662 unchecked items. The File Status pane shows 0 KFF Alert Files, 0 Bookmarked Items, 0 Bad Extension, 0 Encrypted Files, 0 From E-mail, 0 Deleted Files, 0 From Recycle Bin, 0 Duplicate Items, 0 OLE Subitems, 0 Filtered Ignore, 0 KFF Ignorable, and 621 Data Carved Files. The File Category pane shows 63 Documents, 0 Spreadsheets, 0 Databases, 558 Graphics, 0 Multimedia, 0 E-mail Messages, 0 Executables, 0 Archives, 0 Folders, 0 Slack/Free Space, 0 Other Known Type, and 41 Unknown Type. The main pane shows a list of file items with columns for File Name, Full Path, Recycle Bin, Ext, File Type, Category, Subject, Cr Date, Mod Date, Acc Date, and L-Size. The list contains 58 items, all of which are BMP files located in the C:\Documents and Settings\CArmstrong\Desktop\0001\ directory. The status bar at the bottom indicates 588 Listed, 0 Checked Total, and 0 Highlighted.

File Name	Full Path	Recycle Bin	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size
BMP_10306149[10].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_10306149[10].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:26 PM	
BMP_10840720[31].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_10840720[31].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:29 PM	19
BMP_11523210[29].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_11523210[29].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:29 PM	
BMP_12354141[24].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_12354141[24].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:29 PM	
BMP_1242813[40].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_1242813[40].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:32 PM	3,552
BMP_12914772[41].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_12914772[41].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:32 PM	
BMP_13597197[11].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_13597197[11].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:27 PM	3,618
BMP_14055100[13].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_14055100[13].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:27 PM	39
BMP_14157501[15].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_14157501[15].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:28 PM	3,552
BMP_1418378[26].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_1418378[26].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:29 PM	
BMP_14683798[14].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_14683798[14].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:28 PM	18
BMP_15028749[43].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_15028749[43].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:32 PM	
BMP_15891200[32].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_15891200[32].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:30 PM	
BMP_16015444[33].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_16015444[33].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:31 PM	
BMP_16201581[37].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_16201581[37].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:31 PM	3,421
BMP_17550277[13].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_17550277[13].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:27 PM	3,421
BMP_17603328[46].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_17603328[46].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:33 PM	
BMP_18031494[24].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_18031494[24].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:29 PM	21
BMP_18232458[41].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_18232458[41].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:32 PM	
BMP_1852104[39].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_1852104[39].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:32 PM	
BMP_18669633[15].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_18669633[15].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:28 PM	
BMP_18813309[36].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_18813309[36].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:31 PM	3,618
BMP_19333185[32].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_19333185[32].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:30 PM	
BMP_19333505[32].bmp	C:\Documents and Settings\CArmstrong\Desktop\0001\BMP_19333505[32].bmp		bmp	Bitmap File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:30 PM	



FTK Demo

An example of images and partial images found in RAM

The screenshot displays the AccessData FTK 1.71 DEMO VERSION interface. The main window shows a grid of image thumbnails, many of which are labeled with file names such as JPEG_15937E, JPEG_16252E, JPEG_16396E, JPEG_17494C, JPEG_18264C, JPEG_18974E, JPEG_19996E, JPEG_20066E, JPEG_20540E, JPEG_20729E, JPEG_20955E, JPEG_21225E, JPEG_21227E, JPEG_21358E, JPEG_21448E, JPEG_21495E, JPEG_21524E, JPEG_22048E, JPEG_22050E, JPEG_22704E, JPEG_22880E, JPEG_23732E, JPEG_23764E, JPEG_23859E, JPEG_24071E, and JPEG_24793E. The thumbnails include various images: portraits of men and women, a weather map, a laptop, a car, and some abstract patterns. A 'Display Error' icon is also visible. Below the thumbnails, a file list is shown with columns for File Name, Full Path, Recycle Bin, Ext, File Type, Category, Subject, Cr Date, Mod Date, Acc Date, and L-Size. The file list contains entries for JPEG files with their respective paths and sizes. The status bar at the bottom indicates '558 Listed' and '0 Checked Total'.

File Name	Full Path	Recycle Bin	Ext	File Type	Category	Subject	Cr Date	Mod Date	Acc Date	L-Size
JPEG_16252926[29].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:37 PM	644
JPEG_16396288[33].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:38 PM	3
JPEG_17494016[34].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:38 PM	2
JPEG_18264064[33].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:38 PM	35
JPEG_18974574[31].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:37 PM	6
JPEG_19996672[46].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:39 PM	47
JPEG_20066304[32].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:38 PM	3
JPEG_20540832[37].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:38 PM	
JPEG_20729856[46].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:39 PM	32
JPEG_20955136[31].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:37 PM	203
JPEG_21225472[37].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:38 PM	
JPEG_21227520[37].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:38 PM	
JPEG_21358544[32].jpg	C:\Documents and Settings\CArmstrong\Desktop\...		jpg	JPEG/JFIF File	Graphic		9/3/2008 12:01:04 PM	8/28/2008 6:36:34 AM	9/3/2008 12:11:38 PM	92



FTK Demo

Conducting a "Search"

- Click on the "Search" tab
- Enter the search term in the "Search Term" field
- Click on "Add"
- Click on "View Cumulative Results"
- Results will show up in the right hand panel, and can be viewed in the lower panel



Questions?

Questions ?