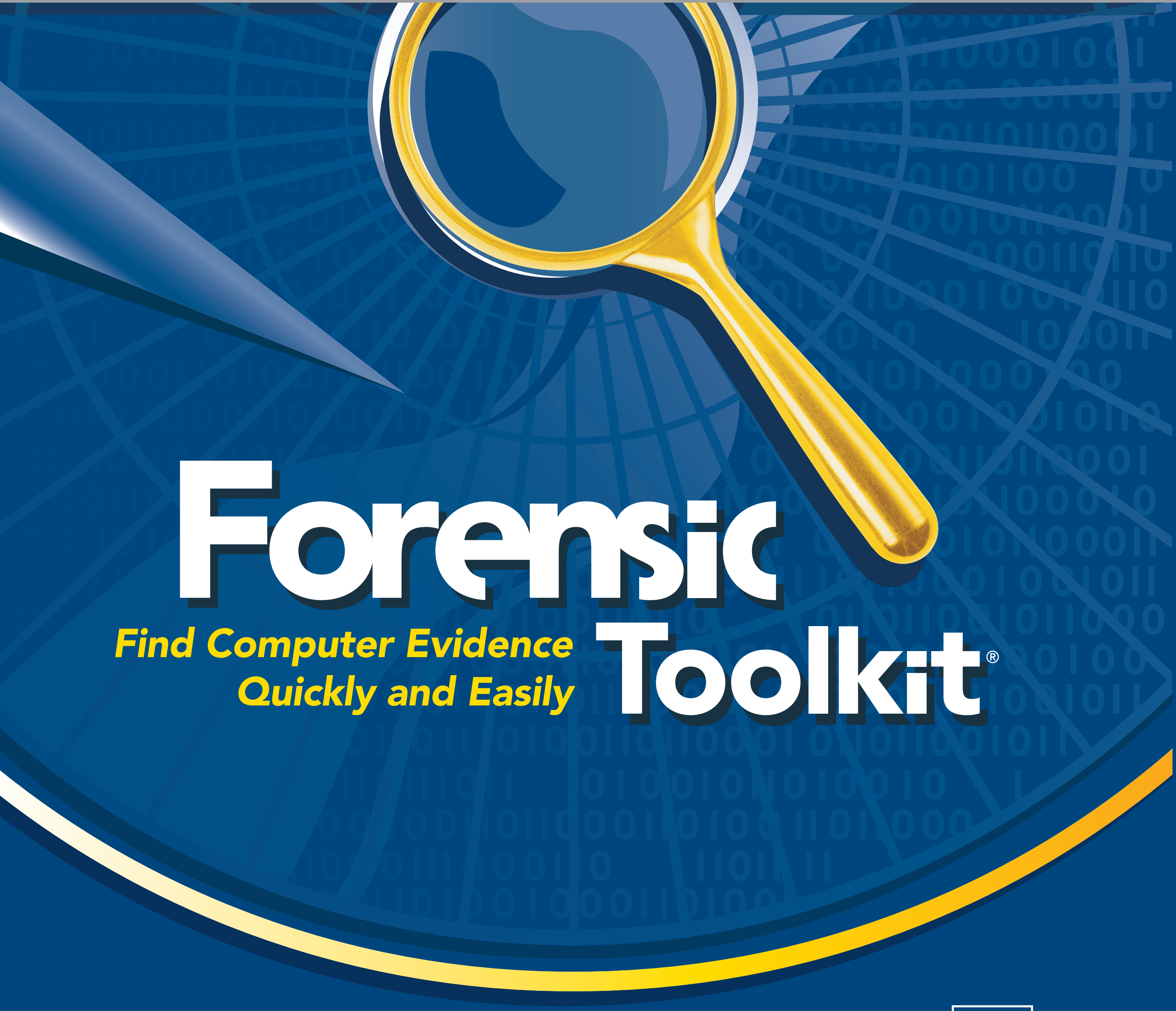
USER GUIDE

Find, Organize, & Analyze Computer Evidence



Forensic Toolkit®

Find Computer Evidence
Quickly and Easily

AccessData®

Legal Notices

AccessData Corp. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Corp. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, AccessData Corp. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, AccessData Corp. reserves the right to make changes to any and all parts of AccessData software, at any time, without any obligation to notify any person or entity of such changes.

You may not export or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Version 1.80.0
May 22, 2008

AccessData Corp.
384 South 400 West
Lindon, Utah 84042
U.S.A.
www.accessdata.com

AccessData Trademarks

Third-Party Trademarks

CONTENTS

Audience 2
Handling Evidence. 2
Role of Forensic Toolkit 3
Other AccessData Products 3
Password Recovery Software 4
FTK 2.0 4

Chapter 1 FTK Overview
The Big Picture. 6
Acquiring and Preserving the Evidence. 7
Analyzing the Evidence 8
Hashing 8
Known File Filter 9
Searching 9
Presenting the Evidence 10

Chapter 2 Installing the Forensic Toolkit
. . . . 11
System Requirements 12
Supported File Systems and Image Formats 13
System Preparation. 14
Basic Installation 15
Basic Install from CD 16
Basic Install from Downloadable Files 19
Upgrade Instructions 27
Upgrading from CD 27
Upgrading from Downloadable Files 28
Uninstalling 30

Chapter 3 Getting Started
Starting FTK 32

Using the Start Menu 32
Using the Command Line 32
Using the Case File 33
Using the Dongle 33
Using the FTK Startup Menu 33
Overview Window 34
Evidence and File Items. 35
File Status 36
File Category. 37
Explore Window 39
Graphics Window 40
E-mail Window 41
Search Window 42
Indexed Search 43
Live Search 44
Bookmark Window 45
Toolbar Components. 48
Viewer Toolbar 48
Tree List Toolbar 49
File List Toolbar. 50
File List Columns 51
FTK Imager 54
Using LicenseManager 55
Starting LicenseManager 56

Chapter 4 Starting a New Case

Starting a Case 60
Completing the New Case Form 61
Entering Forensic Examiner Information. 63
Selecting Case Log Options 64
Selecting Evidence Processes. 65
Refining the Case 69
Refining the Index 74
Managing Evidence. 78
Adding Evidence 78
Editing Evidence 81
Removing Evidence 81
Refining Evidence. 81
Reviewing Case Summary 88
Processing the Evidence 89

Backing Up the Case 90
Storing Your Case Files 90
Recovering Evidence from a System Failure 90
Backing Up Cases Automatically 91

Chapter 5 Working with Existing Cases

Opening an Existing Case 94
Opening an Existing Case from a Different Location 94
Opening a Case in Case Agent Mode (Read-only) 95
Using the Case Agent Mode Manager 95
Adding Evidence 99
Completing the Add Evidence Form 100
Selecting Evidence Processes. 101
Managing Evidence 103
Refining the Index 113
Reviewing Evidence Setup 117
Processing the Evidence 118
Viewing File Properties 119
General Info 120
File Source Info 121
File Content Info 122
Case-Specific Info 123
E-mail Info 125
Setting Up Multiple Temporary Files 126

Chapter 6 Processing Evidence

Using Bookmarks 128
Creating a Bookmark 128
Adding Files to a Bookmark 130
Removing a Bookmark 131
Creating Thumbnails 131
Importing KFF Hashes 132
Verifying Image Integrity 133
Using Analysis Tools 135
Using the Case Log. 137
Viewing the Case Log. 139
Adding Entries to the Case Log 140
Copying Information from FTK. 140
Exporting Files 143
About Recursive File Exporting 146

Exporting the Word List 147

Chapter 7 Searching a Case

Conducting a Live Search 149
Conducting an Indexed Search 154
Single-Term Searches 156
Multi-Term Searches 160
Importing Search Terms 163
Viewing Search Results 164
Reloading a Search Query 164
Wildcard Characters. 165
Indexed Search Options 167
Documenting Your Search Results. 170
Copying Search Results to the Clipboard 170
Using Copy Special to Document Search Results 171
Bookmarking Search Results 172

Chapter 8 Advanced Searching

Searching the Main Viewer. 176
Searching the File List Columns 176
Searching for Internet Keywords. 177
Viewing Internet Addresses. 178
Saving Internet Keyword Search Lists to the Case 179
Bookmarking Internet Keyword Search Items. 180

Chapter 9 Data Carving

Searching for Embedded and Deleted Files (Data Carving) 182
Data Carving Files During Evidence Processing in a New Case 183
Data Carving Files in an Existing Case 184
Adding Carved Files to the Case 186
Bookmarking Carved Files 187

Chapter 10 Using Filters

Applying an Existing Filter 190
Using The File Filter Manager 190
Modifying or Creating a Filter 196
Deleting a Filter. 197

Chapter 11 Searching the Registry

Starting Registry Viewer 200
Launching Registry Viewer as a Separate Application. 200

Launching Registry Viewer from FTK 200
Understanding the Registry Viewer Windows 201
The Full Registry Window 201
The Common Areas Window 202
The Report Window 203
Opening Registry Files 204
Opening a Registry File in Registry Viewer 204
Opening Registry Files within FTK 205
Obtaining Protected Registry Files Using FTK Imager 205
Working with Registry Evidence 206
Adding Keys to the Common Areas Window 207
Deleting Keys from the Common Areas Window 207
Adding Keys to the Report Window 207
Deleting Keys from the Report Window 208
Creating Registry Summary Reports 208
Using Pre-defined AccessData Templates 210
Creating Your Own Registry Report Templates 210
Changing RSR Settings in the FtkSettings.0.ini File 210
Searching for Specific Data 211
Generating a Report 213
Exporting a Word List 214
. . . . 215

Chapter 12 Decrypting EFS

Understanding EFS 218
Decrypting EFS Files and Folders 218
Windows 2000 and XP Systems Prior to SP1 218
Windows XP SP1 or Later 218
Viewing the Decrypted Files in FTK. 219

Chapter 13 Working with Reports

Creating a Report 222
Entering Basic Case Information 223
Managing Bookmarks 224
Selecting the Properties of Bookmarked Files 226
Managing Thumbnails 229
Selecting a File Path List 230
Selecting a File Properties List 232
Selecting the Properties of the File Properties List 233
Adding Supplementary Files and the Case Log 235

Selecting the Report Location 238
Viewing and Distributing a Report. 239
Updating a Report 241
Modifying a Report 242
Modifying a Report in the Same FTK Session 242
Modifying a Report in a Different FTK Session 243

Chapter 14 Customizing FTK
Customizing Fonts and Colors 245
Customizing Columns 249
Modifying the File Listing Database 251
Creating and Modifying Column Settings 252
Deleting Column Settings. 253
Changing the Viewer Settings 253
Changing Preferences 255
Date and Time Format Options 256
File Viewing Options 257
Case Log Options 257
Evidence Cache Size 259
Temporary File Folder 259
KFF Database Location 259
Post Processing Backup Location. 259
Show Reminder when Exporting or Creating a Report with Filter Active . 260
Show Startup Dialog. 260

Chapter 15 Managing Licenses
Managing Licenses with LicenseManager 263
Starting LicenseManager 264
LicenseManager Interface 264
The Installed Components Tab 265
The Licenses Tab 267
Opening and Saving Dongle Packet Files 269
Viewing Product Licenses 269
Adding and Removing Product Licenses 269
Managing Product Licenses on Isolated Machines 270
Adding a Product License to an Isolated Machine 271
Removing a Product License from an Isolated Machine 272
Updating Products 273
Checking for Product Updates 273
Downloading Product Updates 273

Purchasing Product Licenses 274
Sending a Dongle Packet File to Support. 274

Chapter 16 Troubleshooting

Chapter A FTK Recognized File Types
Document File Types 282
Spreadsheet File Types. 285
Database File Types 286
Graphic File Types 288
Multimedia File Types 290
E-mail Message Programs 290
Instant Messaging Programs. 291
Executable File Types 291
Archive File Types 291
Other Known File Types. 293

Chapter B Regular Expression Searching
Understanding Regular Expressions 296
Simple Regular Expressions 296
Complex Regular Expressions—Visa and MasterCard Numbers. 297
Predefined Regular Expressions. 300
Social Security Number 300
U.S. Phone Number 300
IP Address. 302
Going Farther with Regular Expressions 302
Locating More Information on Regular Expressions. 303
Common Operators 303

Chapter C Recovering Deleted Material
FAT 12, 16, and 32 306
NTFS 306
ext2 307
ext3 307

Chapter D Program Files

Chapter E Securing Windows Registry Evidence
Understanding the Windows Registry. 316
Additional Considerations 323
Registry Quick Find Chart 325
System Information. 325

Networking 327
User Data 328
User Application Data. 329

Chapter F dtSearch Requests

Words and Phrases 332
Wildcards (* and ?) 333
Natural Language Searching 333
Synonym Searching. 334
Fuzzy Searching 334
Phonic Searching 335
Stemming 335
Variable Term Weighting 335
AND Connector. 336
OR Connector 336
W/N Connector 336
NOT and NOT W/N 337
Numeric Range Searching 338

Chapter G Corporate Information

Subscriptions 341
Technical Support 341
Product Returns 342

PREFACE

Welcome to AccessData® Forensic Toolkit® (FTK®). FTK enables law enforcement and corporate security professionals to perform complete and thorough computer forensic examinations. FTK features powerful file filtering and search functionality and is recognized as the leading forensic tool for e-mail analysis.

This chapter contains the following sections:

- "Audience" on page 2
- "Handling Evidence" on page 2
- "Role of Forensic Toolkit" on page 3
- "Other AccessData Products" on page 3

Audience

The *Forensic Toolkit User Guide* is written for law enforcement and corporate security professionals with the following competencies:

- Basic knowledge of and training in forensic policies and procedures
- Basic knowledge of and experience with personal computers
- Familiarity with the fundamentals of collecting digital evidence
- Understanding of forensic images and how to acquire forensically sound images
- Experience with case studies and reports
- Familiarity with the Microsoft Windows environment

Handling Evidence

Computer forensics involves the acquisition, preservation, analysis, and presentation of computer evidence. This type of evidence is fragile and can easily, even inadvertently, be altered, destroyed, or rendered inadmissible as evidence. Computer evidence must be properly obtained, preserved, and analyzed to be accepted as reliable and valid in a court of law.

To preserve the integrity of case evidence, forensic investigators do not work on the original files themselves. Instead, they create an exact replica of the files and work on this image to ensure that the original files remain intact.

To verify the files they are working on have not been altered, investigators can compare a hash of the original files at the time they were seized with a hash of the imaged files used in the investigation. Hashing provides mathematical validation that a forensic image exactly matches the contents of the original computer.

Another important legal element in computer forensics is the continuity, or chain of custody, of computer evidence. The chain of custody deals with who has supervised, acquired, analyzed, and controlled the evidence. Forensic investigators must be able to account for all that has happened to the evidence between its point of acquisition or seizure and its eventual appearance in court.

There are many cases in which personnel trained in information technology have made incriminating computer evidence legally inadmissible because of their reckless or ill-conceived examinations. Only properly trained computer forensics specialists should obtain and examine computer evidence.

Role of Forensic Toolkit

When you acquire computer evidence, you can use FTK Imager™ to create an image of the source drives or files. You can also create a hash of the original image that you can later use as a benchmark to prove the validity of your case evidence. FTK Imager verifies that the image hash and the drive hash match when the image is created.

After you create the image and hash the data, you can then use FTK to perform a complete and thorough computer forensic examination and create a report of your findings.

For a big-picture view of FTK, see“FTK Overview” on page 5.

Other AccessData Products

In addition to FTK and FTK Imager, AccessData offers other industry-leading products.

Password Recovery Software

AccessData has been the leader in the field of commercial software decryption since 1987. AccessData has multiple tools available for password recovery:

- Password Recovery Toolkit™ (PRTK™) has a wide variety of individual password-breaking modules that can help you recover lost passwords.

  For more information about PRTK, the AccessData Website (http://www.accessdata.com).

- Distributed Network Attack® (DNA®) provides a new approach to recovering password-protected files. Rather than using a single machine, DNA uses machines across the network or across the world to conduct key space and dictionary attacks.

  For more information about DNA, the AccessData Website (http://www.accessdata.com).

FTK 2.0

The most comprehensive AccessData product for forensic investigation is FTK 2.0. It includes all the PRTK recovery modules, a 50-client license for DNA, and a one-year upgrade subscription for all of the included products. Any products and upgrades purchased in that year do not expire.

For more information about FTK 2.0, the AccessData Website (http://www.accessdata.com).

CHAPTER 1

FTK Overview

This chapter provides a big-picture overview of how Forensic Toolkit (FTK) can be used to acquire, preserve, analyze, and present computer evidence.

The chapter contains the following sections:

- "The Big Picture" on page 6
- "Acquiring and Preserving the Evidence" on page 7
- "Analyzing the Evidence" on page 8
- "Presenting the Evidence" on page 10

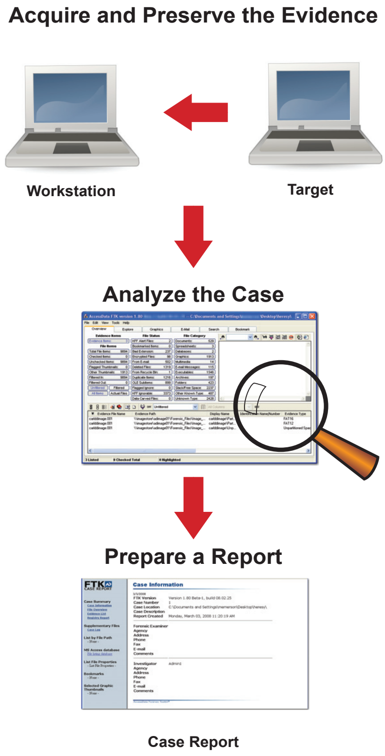
The Big Picture

The following are the basic steps taken during a forensic computer examination using FTK and FTK Imager:

1 Acquire and preserve the evidence.

2 Analyze the evidence.

3 Present computer evidence by creating a case report to document the evidence and investigation results.



The concepts behind each of these steps are discussed in the following sections.

Acquiring and Preserving the Evidence

For digital computer evidence to be valid, it must be preserved in its original form. There are two ways to achieve this: by creating an image of the suspect drive using hardware devices or by using software applications.

Hardware acquisition tools duplicate disk drives or allow read-only mode access to a hard drive. For more information about hardware tools, see “Industry and Third-Party Contacts” on page 321.

Software acquisition tools create a forensically sound image that makes no changes to the data or information on the suspect hard drive. The forensic image must be identical in every way to the original. As a rule, no changes to the evidence should be made.

FTK Imager is a software acquisition tool. It can be used to quickly preview evidence and, if the evidence warrants further investigation, create a forensically sound image of the disk. To prevent against accidental or intentional manipulation of evidence, FTK Imager makes a bit-by-bit duplicate image of the media. The forensic image is identical in every way to the original, including file slack and unallocated space or free space. For information about file slack and unallocated space, see the Glossary on page 343.

Analyzing the Evidence

To analyze the evidence, FTK uses a variety of tools, including hashing, the Known File Filter™ (KFF™) database, and searching.

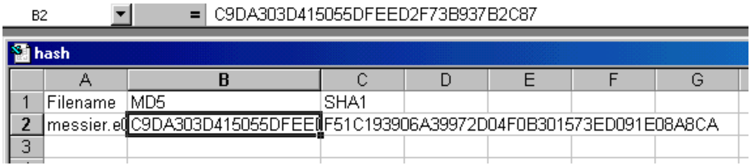
Hashing

Hashing a file or files refers to the process of generating a unique value based on a file's contents. Hash values are used to verify file integrity and identify duplicate and known files. (Known files are standard system files that can be ignored in your investigation as well as known illicit or dangerous files.)

Two hash functions are available in FTK and FTK Imager: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA-1). By default, FTK creates MD5 hashes.

The hashing options are selected automatically by FTK based on the KFF databases that are available. For more information about KFF, see "Known File Filter" on page 9.

The following graphic shows a sample file with a list of MD5 and SHA-1 hashes.



B2 = C9DA303D415055DFEED2F73B937B2C87

hash

	A	B	C	D	E	F	G
1	Filename	MD5	SHA1				
2	messier.e	C9DA303D415055DFEE	F51C193906A39972D04F0B301573ED091E08A8CA				
3							

Typically, you hash individual files to compare the results with a known database of hashes, such as KFF. However, you can also hash multiple files or an image to verify that the working copy is identical to the original.

You can create hashes with FTK Imager or FTK. For information on creating hashes with FTK, see "Selecting Evidence Processes" on page 65.

Known File Filter

KFF is an FTK utility that compares file hashes against a database of hashes from known files. The purpose of KFF is to eliminate ignorable files (such as known system and program files) or to alert you to known illicit or dangerous files. It also checks for duplicate files.

Files which contain other files, such as Zip and e-mail files with attachments, are called *container files*. When KFF identifies a container file as ignorable, FTK does not extract its component files.

When KFF is used, the evidence is separated into ignored files (such as system files) and evidence that you continue to examine.

KFF includes the HashKeeper database, which is updated periodically and is available for download on the FTK update page (http://www.accessdata.com). For information on defining the location of the KFF database, see "KFF Database Location" on page 259.

Searching

With FTK, you can conduct a live search or an indexed search.

A live search is a time-consuming process involving an item-by-item comparison with the search term. Live searches allow you to search non-alphanumeric characters and perform regular expression searches.

Note: Regular expressions are mathematical statements that describe a data pattern such as a credit card or social security number. Regular expression searches allow you to find data items that conform to the pattern described by the expression. FTK provides several pre-defined regular expressions such as U.S. phone number, U.K. phone number, credit card number, social security number, and IP address.

The indexed search uses the index file to find a search term. The index file contains all discrete words or number strings found in both the allocated and unallocated space in the case evidence.

FTK uses dtSearch as its index search engine. dtSearch, one of the leading search tools available, can quickly search gigabytes of text.

For more information on searching, see “Searching a Case” on page 149.

Presenting the Evidence

FTK presents computer evidence by creating a case report and case log to document the evidence and investigation results.

FTK uses the Report Wizard to create and modify reports. In the report, you can add bookmarks (information you selected during the examination), customize graphics references, select file listings, and include supplementary files and the case log. You can also export selected files with the report, such as bookmarked files and flagged graphics, so they are available with the report. The report is generated in HTML.

The case log assists in documenting and logging activities during the investigation and analysis of a case. This information can be used as part of a report or to identify what has occurred if you are assigned to an investigation in progress. The case log is created automatically by the FTK and is called ftk.log.

For information about creating a report, see “Working with Reports” on page 221.

CHAPTER 2

Installing the Forensic Toolkit

This chapter explains how to install and upgrade Forensic Toolkit (FTK). The chapter is divided into the following sections:

- "Supported File Systems and Image Formats" on page 13
- "System Preparation" on page 14
- "Basic Installation" on page 15
- "Upgrade Instructions" on page 27
- "Uninstalling" on page 30

System Requirements

The computer you install FTK on must meet the following minimum system requirements:

Hardware or Software	Minimum Requirement	Recommended Requirement
Operating System	Windows 2000, or XP	Windows 2000, XP, or 2003
Processor	2 GHz or faster Intel Pentium IV, AMD Athlon, or equivalent	Intel Core 2 Duo, or equivalent
RAM	512 MB	2 GB
Hard disk space	◆ 4 GB for program files ◆ Additional hard disk space for index storage	◆ 4 GB for program files ◆ Additional hard disk space for index storage
Monitor	SVGA (800 x 600)	XGA (1024 x 768) or higher resolution
USB Port	Dongle shipped with FTK	

For additional information about the space required for indexes, use this table to estimate the disk space required to index different sizes of data:

Evidence Size	Work Space	Index Size
8 GB	4 GB	2 GB
15 GB	7.5 GB	3.75 GB
30 GB	15 GB	7.5 GB
30+ GB	50% of the original	25% of the original

For more information, see “Conducting an Indexed Search” on page 154.

Supported File Systems and Image Formats

FTK can analyze the following types of file systems and image formats:

File Systems	FAT 12, FAT 16, FAT 32
	NTFS
	Ext2, Ext3
Hard Disk Image Formats	Encase
	SnapBack
	Safeback 2.0 and under
	Expert Witness
	Linux DD
	ICS
	Ghost (forensic images only)
	SMART
CD and DVD Image Formats	Alcohol (*.mds)
	CloneCD (*.ccd)
	ISO
	IsoBuster CUE
	Nero (*.nrg)
	Pinnacle (*.pdi)
	PlexTools (*.pxi)
	Roxio (*.cif)
	Virtual CD (*.vc4)

System Preparation

Before installing FTK, you should evaluate the workstation and its current software. A good understanding of the workstation and its configured devices will help ensure that FTK runs at its best.

Consider the following:

- Role of the workstation

  Determine if it will be used as a regular user workstation, a forensic analysis workstation, or a password recovery workstation.

- Access policy

  Identify where the workstation will be located, who can access the information, and when the cases can be worked on.

- Hardware and software requirements

  For the hardware and software requirements, see “System Requirements” on page 12.

- Application relationships

  Verify that the applications can work simultaneously. Do not run so many applications that you compromise overall performance.

- Network and Internet issues

  Determine if the workstation should be connected to a network or the Internet. Under normal circumstances, the forensic analysis workstation will not be connected to the Internet to avoid the possible tainting of evidence.

- System policies and procedures

  Check with your system administrator about any specific policies and procedures that may exist.

Basic Installation

You can install FTK from a CD or from downloadable files available on the AccessData Website (http://www.accessdata.com).

The installation is divided into three parts:

- Install the Forensic Toolkit: FTK 1.70.0 and later will install in locations separate from FTK 1.6 or earlier. Your older versions of FTK and their cases will not be affected by installing FTK 1.70.

  Warning: FTK 1.70.0 has an upgraded database, increasing the limit on how many items a case can contain. This enhancement, however, renders FTK 1.70.0 incompatible with earlier versions. Cases processed in earlier versions of FTK cannot be opened in FTK 1.70.0, and cases processed in 1.70.0 cannot be opened in earlier FTK versions.

  FTK Imager is now a separate installation.

- Install the Known File Filter Library: Installs the Known File Filter (KFF) database, a utility that compares file hashes in your case against a database of hashes for known system and program files as well as known illicit and contraband files.

  To preserve work done on earlier versions of FTK, your 1.70.0 KFF will be installed in the 1.70.0 directory without overwriting any previously installed KFFs. To economize disk space, you may choose to manually delete older versions of your KFF.

  To point any version of FTK to the new KFF, go to the Tools menu, then type in the path in the Preferences dialog.

  For additional information about KFF, see “Known File Filter” on page 9.

- Launch Dongle Driver Setup: Installs the driver for either the USB or parallel port dongle.

  The dongle is required to use FTK and it should be stored in a secure location when not in use.

Each part can be independently installed, although FTK and the dongle driver must be installed for FTK to work properly. If you want to eliminate ignorable and duplicate files, and be alerted of known illicit or contraband files, you need to install KFF.

For troubleshooting information on the FTK install, see “Troubleshooting” on page 275.

Basic Install from CD

The following sections review installing FTK, the dongle drivers, and KFF from CD.

Installing FTK from CD

To install FTK from CD:

1. Insert the CD into the CD-ROM drive and click **Install the Forensic Toolkit**.

   If auto-run is not enabled, select **Start**, and then **Run**. Browse to the CD-ROM drive and select **Autorun.exe**.

2. Click **Next** on the Welcome screen.
3. Select **I Accept the Terms of the License Agreement** and then click **Next**.
4. Designate the program directory by doing one of the following:
   - To accept the default directory, click **Next**. The default directory is c:\Program Files\AccessData\AccessData Forensic Toolkit\.
   - To specify a different directory, click **Browse**, select the location, and click **OK**.
5. Click **Next**.
6. Check the box to run FTK if you want it to automatically start after you complete the installation.

   If you check the box to run FTK but haven’t installed the dongle drivers, you will receive an error message and FTK will not start.

   If you run FTK but haven’t installed the KFF database, you will receive an error message at the end of the installation saying that the KFF Hash Library is not found and certain features will be disabled.

You can install the dongle drivers and KFF from the CD. For installation instructions, see "Installing the Dongle Driver from CD" on page 17 and "Installing KFF from CD" on page 18.

7 Check the box to run LicenseManager if you want it to automatically check for updates.

LicenseManager automatically checks the AccessData Website for software updates. For more information on LicenseManager, see "Managing Licenses" on page 263.

If LicenseManager is not installed, a warning is displayed. See "Installing LicenseManager from CD" on page 23 or "Installing LicenseManager from Downloadable Files" on page 26.

8 Click **Finish**.

Installing the Dongle Driver from CD

Installing the KEYLOK (green) Dongle Driver

1 Insert the CD into the CD-ROM drive and click **Launch Dongle Driver Setup**.

If auto-run is not enabled, select **Start**, and then **Run**. Browse to the CD-ROM drive and select **Autorun.exe**.

2 Click **Next** to install the driver.

3 If you have a USB dongle, verify that it is *not* plugged in. If you have a parallel port dongle, verify that it *is* plugged in.

Click **Next** after meeting the above conditions.

4 Designate the dongle driver directory by doing one of the following:

- To accept the default directory, click **Next**. The default directory is c:\Program Files\AccessData\Dongle Driver\.
- To specify a different directory, click **Browse**, select the location, and click **OK**.

5 Click **Next**.

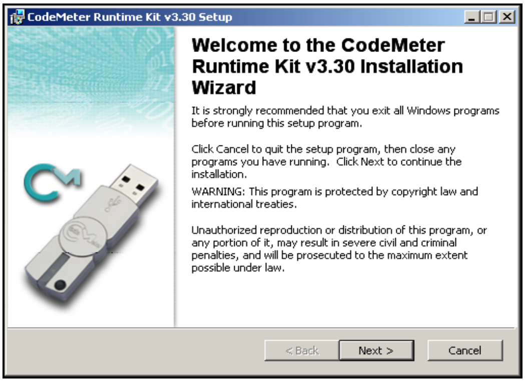
6 If you have a USB dongle, plug it in.

7 Click **Finish**.

Installing the CodeMeter CmStick Driver

If you are using the new CodeMeter CmStick (silver dongle), you need to install the WIBU CodeMeter Runtime 3.30 driver.

1 Install the WIBU CodeMeter Runtime 3.30 software for the CmStick. Click *Install CodeMeter Software* to launch the CodeMeter installation wizard, as displayed in the following figure.



Welcome to the CodeMeter Runtime Kit v3.30 Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

2 Follow the directions for installation, accepting all defaults, and click *Finish* to complete the installation.

Installing KFF from CD

To install KFF from CD:

1 Insert the CD into the CD-ROM drive and click **Install the Known File Filter Library**.

If auto-run is not enabled, select **Start**, and then **Run**. Browse to the CD-ROM drive and select **Autorun.exe**.

2 Click **Next** on the Welcome screen.

3 Select **I Accept the Terms of the License Agreement** and then click **Next**.

4 Designate the KFF directory by doing one of the following:

- To accept the default directory, click **Next**. The default directory is c:\Program Files\AccessData\AccessData Forensic Toolkit\Program\.
- To specify a different directory, click **Browse**, select the location, and click **OK**.

Important: If you install KFF to another directory, you must indicate the new location in FTK Preferences. For more information, see “KFF Database Location” on page 259.

5 Click **Next**.

6 Click **Finish**.

Basic Install from Downloadable Files

FTK downloadable files are available from the AccessData Website (http://www.accessdata.com).

To download the FTK program files:

1 Go to the AccessData downloads page.

2 Under Forensic Toolkit, click **Updates**.

3 Download the program files you would like to install.

If this is the first time you have installed FTK, download both FTK and the dongle driver. If you want to eliminate ignorable and duplicate files, and be alerted of known illicit or contraband files, you also need to download the KFF database.

the following sections for more information on installing FTK, the dongle drivers, and the KFF database from downloadable files.

Installing FTK from Downloadable Files

To install FTK from downloadable files:

1 On the Forensic Toolkit Download page, click **FTKInstall.exe**.

2 Save the FTK install file (FTKInstall-*version.exe*) to a temporary directory on your drive.

3 To launch the install program, go to the temporary directory and double-click the FTK install file (FTKInstall-*version.*exe).

4 Click **Install**.

5 Click **Next** on the Welcome screen.

6 Select **I Accept the Terms of the License Agreement** and then click **Next**.

7 Designate the program directory by doing one of the following:

- To accept the default directory, click **Next**. The default directory is c:\Program Files\AccessData\AccessData Forensic Toolkit\.
- To specify a different directory, click **Browse**, select the location, and click **OK**.

8 Click **Next**.

9 Check the box to run FTK if you want it to automatically start after you complete the installation.

If you check the box to run FTK but haven't installed the dongle drivers, you will receive an error message and FTK will not start.

If you run FTK but haven't installed the KFF database, you will receive an error message at the end of the installation saying that the KFF Hash Library is not found and certain features will be disabled.

You can install the dongle drivers and KFF from the downloadable files. For installation instructions, see "Installing the Dongle Drivers from Downloadable Files" on page 21.

10 Check the box to run LicenseManager if you want it to automatically check for updates.

LicenseManager automatically checks the AccessData Website for software updates. For more information on LicenseManager, see “Managing Licenses” on page 263.

If LicenseManager is not installed, a warning is displayed. See “Installing LicenseManager from CD” on page 23 or “Installing LicenseManager from Downloadable Files” on page 26.

11 Click **Finish**.

Installing the Dongle Drivers from Downloadable Files

Installing the KEYLOK (green) Dongle Driver

To install the dongle drivers from downloadable files:

1 On the Forensic Toolkit Download page, click the dongle drivers install.

2 Save the dongle install file (dongle.exe) to a temporary directory on your drive.

3 To launch the install program, go to the temporary directory and double-click the dongle install file (dongle.exe).

4 Click **Install**.

5 Click **Next** to install the driver.

6 If you have a USB dongle, verify that it is *not* plugged in. If you have a parallel port dongle, verify that it *is* plugged in.

7 Designate the dongle driver directory by doing one of the following:

- To accept the default directory, click **Next**. The default directory is c:\Program Files\AccessData\Dongle Driver\.
- To specify a different directory, click **Browse**, select the location, and click **OK**.

8 Click **Next**.

9 If you have a USB dongle, plug it in.

10 Click **Finish**.

Installing the CodeMeter CmStick Driver

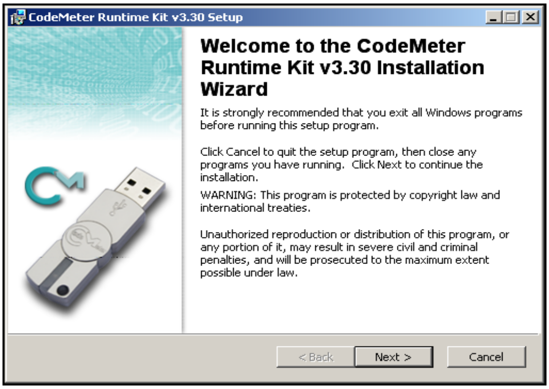
If you are using the new CodeMeter CmStick (silver dongle), you need to install the WIBU CodeMeter Runtime 3.30 driver.

1 On the Forensic Toolkit Download page, click the CodeMeter Runtime 3.30 install.

2 Save the dongle install file to a temporary directory on your drive.

3 To launch the install program, go to the temporary directory and double-click the dongle install file.

4 Install the WIBU CodeMeter Runtime 3.30 software for the CmStick. Click *Install CodeMeter Software* to launch the CodeMeter installation wizard, as displayed in the following figure.CodeMeter Installation Wizard



CodeMeter Runtime Kit v3.30 Setup

Welcome to the CodeMeter Runtime Kit v3.30 Installation Wizard

It is strongly recommended that you exit all Windows programs before running this setup program.

Click Cancel to quit the setup program, then close any programs you have running. Click Next to continue the installation.

WARNING: This program is protected by copyright law and international treaties.

Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

5 Follow the directions for installation, accepting all defaults, and click *Finish* to complete the installation.

Installing KFF from Downloadable Files

To install KFF from downloadable files:

1 On the Forensic Toolkit Download page, click **KFFInstall.exe**.

2 Save the KFF install file (kffinstall.exe) to a temporary directory on your drive.

3 To launch the install program, go to the temporary directory and double-click the KFF install file (kffinstall.exe).

4 Click **Next** on the Welcome screen.

5 Select **I Accept the Terms of the License Agreement** and then click **Next**.

6 Designate the KFF directory by doing one of the following:

- To accept the default directory, click **Next**. The default directory is c:\Program Files\AccessData\AccessData Forensic Toolkit\Program\.
- To specify a different directory, click **Browse**, select the location, and click **OK**.

Important: If you install KFF to another directory, you must indicate the new location in FTK Preferences. For more information, see “KFF Database Location” on page 259.

7 Click **Next**, then click **Finish**.

Installing LicenseManager from CD

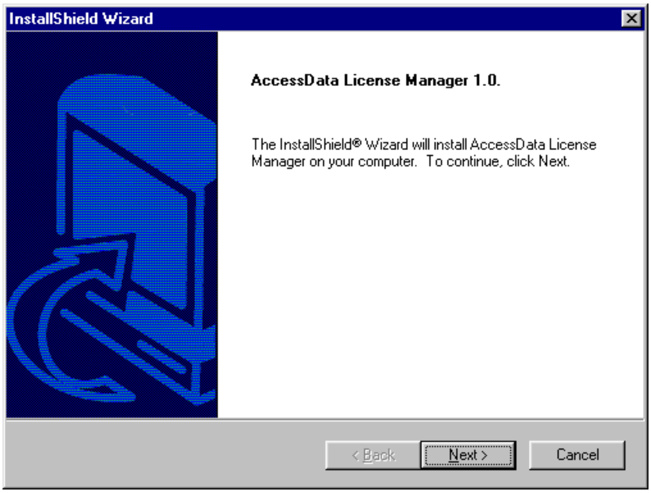
LicenseManager lets you manage product and license subscriptions using a dongle or dongle packet file. For more information, see “Using LicenseManager” on page 55.

To install LicenseManager:

1 Insert the CD into the CD-ROM drive and click **Install LicenseManager**.

If auto-run is not enabled, select **Start**, and then **Run**. Browse to the CD-ROM drive and select **Autorun.exe**.

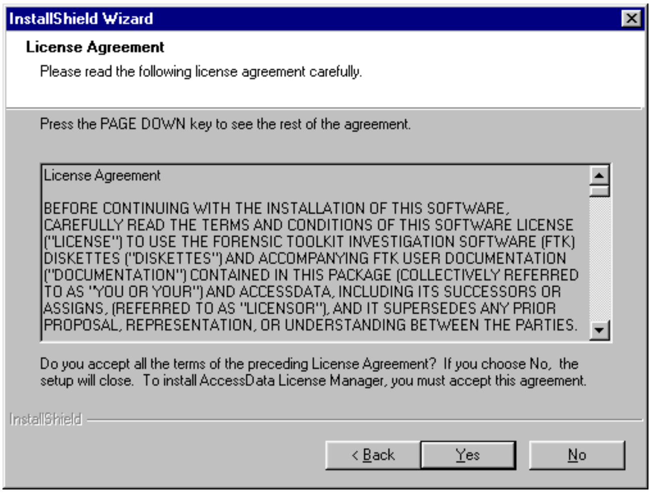
2 Click **Next** on the Welcome screen.



AccessData License Manager 1.0.

The InstallShield® Wizard will install AccessData License Manager on your computer. To continue, click Next.

3 Click **Yes** to accept the license agreement.



License Agreement

Please read the following license agreement carefully.

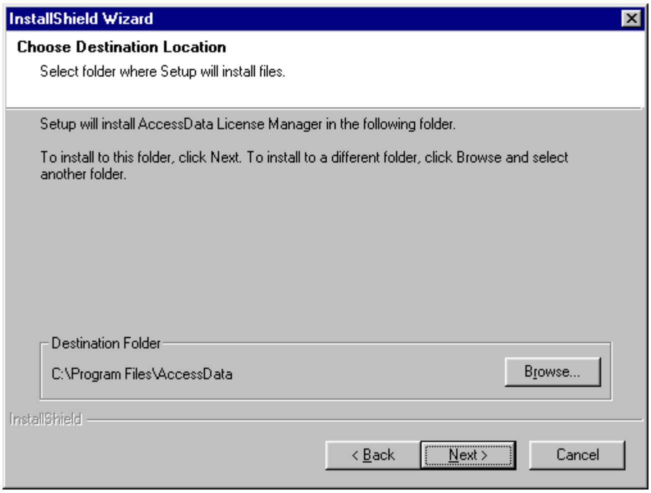
Press the PAGE DOWN key to see the rest of the agreement.

License Agreement

BEFORE CONTINUING WITH THE INSTALLATION OF THIS SOFTWARE, CAREFULLY READ THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE ("LICENSE") TO USE THE FORENSIC TOOLKIT INVESTIGATION SOFTWARE (FTK) DISKETTES ("DISKETTES") AND ACCOMPANYING FTK USER DOCUMENTATION ("DOCUMENTATION") CONTAINED IN THIS PACKAGE (COLLECTIVELY REFERRED TO AS "YOU OR YOUR") AND ACCESSDATA, INCLUDING ITS SUCCESSORS OR ASSIGNS, (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install AccessData License Manager, you must accept this agreement.

4 Designate the program directory:



InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

Setup will install AccessData License Manager in the following folder.

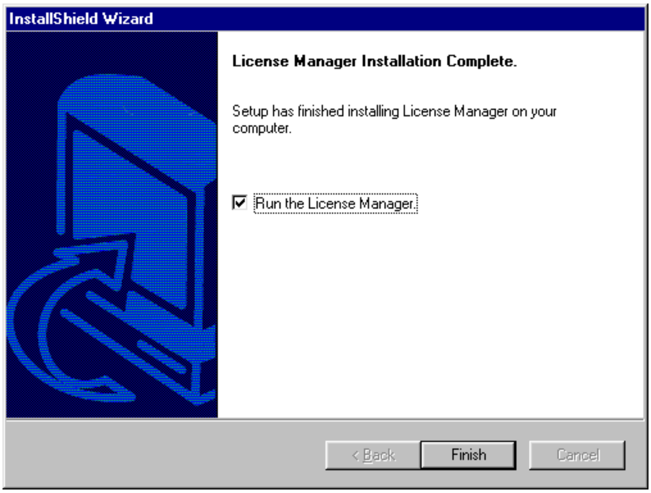
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\AccessData

- To accept the default directory, click **Next**. The default directory is C:\Program Files\AccessData\AccessData LicenseManager.
- To specify a different location, click **Browse**, select the location, click **OK**, and the click **Next**.

5 If you want to launch LicenseManager after completing the installation, select **Run LicenseManager**.



License Manager Installation Complete.

Setup has finished installing License Manager on your computer.

☑ Run the License Manager.

You can start LicenseManager later by clicking **Start**, then **Programs**, then **AccessData**, then **LicenseManager**, and then **LicenseManager**. You can also start LicenseManager in FTK, by clicking **Help**, and then **Launch LicenseManager**.

Installing LicenseManager from Downloadable Files

LicenseManager lets you manage product and license subscriptions using a dongle or dongle packet file. For more information, see “Using LicenseManager” on page 55.

To install LicenseManager:

1. Go to the AccessData download page (http://www.accessdata.com).
2. On the download page, click **LicenseManager**.
3. Save the dongle installation file (LicenseManager.exe) to a temporary directory on your drive.
4. To launch the installation program, go to the temporary directory and double-click the dongle installation file (LicenseManager.exe).
5. Click **Install**.

Follow the same instructions for installing from CD beginning with Step 2 on page 24.

Upgrade Instructions

You do not have to upgrade FTK and KFF at the same time. For example, you can upgrade to a newer version of FTK without upgrading the KFF database.

Important: You do not need to upgrade the dongle drivers unless notified by AccessData.

You can upgrade the version of FTK from a CD or from downloadable files available on the AccessData Website (http://www.accessdata.com).

To be notified via e-mail when FTK upgrades are available, go to the Update Notification page on the AccessData Website (http://www.accessdata.com).

For troubleshooting information on upgrading FTK, see “Troubleshooting” on page 275.

Upgrading from CD

Typically you will upgrade from downloadable files. If you want to upgrade from CD, contact AccessData. For contact information, see “Technical Support” on page 341.

Upgrading FTK from CD

To upgrade FTK from CD:

1. Insert the CD into the CD-ROM drive and click **Install the Forensic Toolkit**.

   If auto-run is not enabled, select **Start**, and then **Run**. Browse to the CD-ROM drive and select **Autorun.exe**.

2. Select **Install the Newer Version** and click **Next**.
3. Check the box to run FTK if you want it to automatically start after you complete the installation.
4. Check the box to run LicenseManager if you want it to automatically check for updates.

LicenseManager automatically checks the AccessData Website for software updates. For more information on LicenseManager, see “Managing Licenses” on page 263.

If LicenseManager is not installed, a warning is displayed. See “Installing LicenseManager from CD” on page 23 or “Installing LicenseManager from Downloadable Files” on page 26.

5 Click **Finish**.

Upgrading KFF from CD

If you have added your own hashes to the KFF database, see “Upgrading a Customized KFF” on page 30 for instructions on how to upgrade the KFF database without overwriting the hashes you have added.

If you have not customized the KFF library, simply re-install the KFF from CD.

To upgrade a basic KFF from CD:

1 Insert the CD into the CD-ROM drive and click **Install the Known File Filter Library**.

2 Select **Replace My KFF with This Version** and click **Next**.

3 Click **Finish**.

Upgrading from Downloadable Files

FTK downloadable files are available from the AccessData Website (http://www.accessdata.com).

To download the FTK program files:

1 Go to the AccessData downloads page.

2 Under Forensic Toolkit, click **Updates**.

3 Download the program files you would like to install.

Upgrading FTK from Downloadable Files

To upgrade FTK from downloadable files:

1 On the Forensic Toolkit Download page, click **FTKInstall.exe**.

2 Save the FTK install file (FTKInstall-*version*.exe) to a temporary directory on your drive.

3 To launch the install program, go to the temporary directory and double-click the FTK install file (FTKInstall-*version*.exe).

4 Click **Install**.

5 Click **Yes to All** to replace all files.

Note: Your custom column settings and filters are not overwritten.

6 In the install program, select **Install the Newer Version** and click **Next**.

7 Check the box to run FTK if you want it to automatically start after you complete the installation.

8 Check the box to run LicenseManager if you want it to automatically check for updates.

LicenseManager automatically checks the AccessData Website for software updates. For more information on LicenseManager, see “Managing Licenses” on page 263.

If LicenseManager is not installed, a warning is displayed. See “Installing LicenseManager from CD” on page 23 or “Installing LicenseManager from Downloadable Files” on page 26.

9 Click **Finish**.

Upgrading KFF from Downloadable Files

If you have customized the KFF library by adding your own hashes, you need to follow the instructions in “Upgrading a Customized KFF” on page 30. These instructions will prevent the overwriting of the hashes you have added.

If you have not customized the KFF library, simply re-install the KFF from the downloadable files.

To upgrade a basic KFF from downloadable files:

1 On the Forensic Toolkit Download page, click **KFFInstall.exe**.

2 Save the KFF install file (kffinstall.exe) to a temporary directory on your drive.

3 To launch the install program, go to the temporary directory and double-click the KFF install file (kffinstall.exe).

4 Select **Replace my KFF with This Version** and click **Next**.

5 Click **Finish**.

Upgrading a Customized KFF

To upgrade a customized KFF:

1 On the Forensic Toolkit Download page, click **kfflibrary.zip**.

2 Save kfflibrary.zip to a temporary directory on your drive.

3 Extract ADKFFLibrary.hdb to the temporary directory.

4 Open FTK.

5 Click **Tools**, and then **Import KFF Hashes.**

6 Browse to the ADKFFLibrary.hdb file located in your temporary directory and click **Open**.

The new and updated KFF files are added to your KFF library without overwriting your custom hashes.

Uninstalling

Use the Windows Add/Remove Programs utility to uninstall FTK, the dongle drivers, KFF database, and the LicenseManager.

CHAPTER 3

Getting Started

Before working in Forensic Toolkit (FTK), you should familiarize yourself with the FTK interface. The FTK interface contains six main windows, organized like tabbed pages, each with a particular focus or function. Most windows also contain a common toolbar and file list with columns.

Note: Viewing large items in their native applications is often faster than waiting for them to be rendered in an FTK viewer.

This chapter discusses the interface in the following sections:

- “Starting FTK” on page 32
- “Overview Window” on page 34
- “Explore Window” on page 39
- “Graphics Window” on page 40
- “E-mail Window” on page 41
- “Search Window” on page 42
- “Bookmark Window” on page 45
- “Toolbar Components” on page 48
- “File List Columns” on page 51
- “FTK Imager” on page 54
- “Using LicenseManager” on page 55

Starting FTK

After you complete the installation, you can start FTK from the Start menu, from the command line, or by double-click the case file.

Using the Start Menu

Select **Start**, then **Programs**, then **AccessData**, then **Forensic Toolkit**, and then **Forensic Toolkit,** or click the Forensic Toolkit shortcut on your desktop.

Using the Command Line

You can also start FTK from the command line by typing the following command:

***path_to_ftk_program_file*\ftk.exe**

Note: The default location for the FTK program is C:\Program Files\AccessData\AccessData Forensic Toolkit\Program\ftk.exe.

To start FTK with existing case, type the following command at the command line:

path_to_ftk_program_file*\ftk.exe /OpenCase *target_case_directory

If you want to preserve evidence in a case but still allow other investigators to look at the case, you can also start FTK in Case Agent Mode by typing the following command at the command line:

***path_to_ftk_program_file*\ftk.exe /CaseAgent**

If you want to open a specific case in Case Agent Mode, type the following command:

path_to_ftk_program_file*\ftk.exe /CaseAgent /OpenCase *target_case_directory

For more information on Case Agent Mode, see "Opening a Case in Case Agent Mode (Read-only)" on page 95.

Important: Close down any virus scanner while running FTK and processing evidence. Virus scanners can slow FTK performance significantly.

Using the Case File

FTK automatically launches the appropriate version for your case. Click the case file (name_of_case.ftk) in the case folder, and FTK will automatically open the case in the appropriate version.

If the correct version isn't found, an error message will display.

Using the Dongle

AccessData provides a parallel or USB dongle with FTK. The dongle is a security compliance device that you insert into the parallel or USB port during installation. It maintains your FTK licensing and subscription information and is required to use FTK. For information on installing the dongle drivers, see "Installing the Dongle Driver from CD" on page 17 or "Installing the Dongle Drivers from Downloadable Files" on page 21.

You can use the License Manager to monitor your FTK subscription. For more information, see "Using LicenseManager" on page 55.

Using the FTK Startup Menu

When you start FTK, the Simple Start menu appears with the following options:

- Start a new case

  For detailed information on starting a new case, see "Starting a New Case" on page 59.

- Open an existing case

  For detailed information on working with existing cases, see "Working with Existing Cases" on page 93.

- Preview evidence

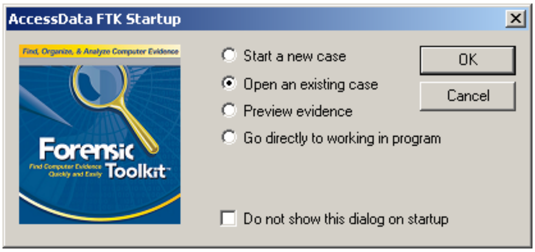
  This option opens FTK Imager. For more information, see "FTK Imager" on page 54.

- Go directly to working in program

This option opens FTK.

- Don't show this dialog on start-up again.

  Mark this option if you do not want the FTK Startup menu to appear when you start FTK.



AccessData FTK Startup

○ Start a new case
● Open an existing case
○ Preview evidence
○ Go directly to working in program

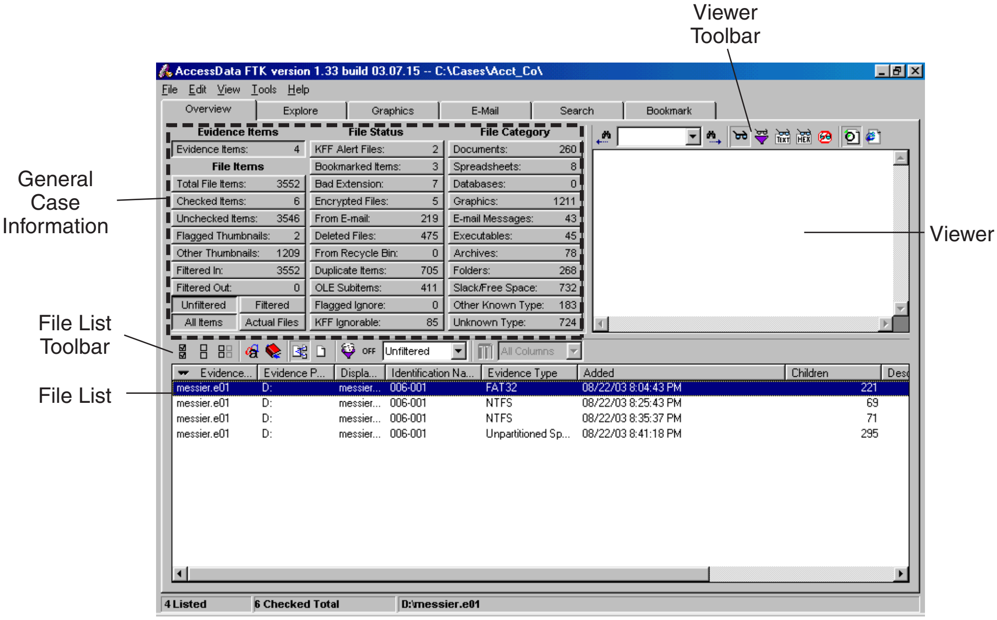
□ Do not show this dialog on startup

Find, Organize, & Analyze Computer Evidence
Forensic Toolkit
Find Computer Evidence Quickly and Easily
OK
Cancel

If you want the FTK Startup menu to appear after you have set it to not appear, click Tools, then Preferences, and then Show Startup Dialog.

Overview Window

The Overview window provides a general view of a case.



AccessData FTK version 1.33 build 03.07.15 -- C:\Cases\Acct_Co\

Evidence Items		File Status		File Category	
Evidence Items:	4	KFF Alert Files:	2	Documents:	260
File Items		Bookmarked Items:	3	Spreadsheets:	8
Total File Items:	3552	Bad Extension:	7	Databases:	0
Checked Items:	6	Encrypted Files:	5	Graphics:	1211
Unchecked Items:	3546	From E-mail:	219	E-mail Messages:	43
Flagged Thumbnails:	2	Deleted Files:	475	Executables:	45
Other Thumbnails:	1209	From Recycle Bin:	0	Archives:	78
Filtered In:	3552	Duplicate Items:	705	Folders:	268
Filtered Out:	0	OLE Subitems:	411	Slack/Free Space:	732
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	183
All Items	Actual Files	KFF Ignorable:	85	Unknown Type:	724

Evidence...	Evidence P...	Displa...	Identification Na...	Evidence Type	Added	Children	Desc
messier.e01	D:	messier...	006-001	FAT32	08/22/03 8:04:43 PM	221	
messier.e01	D:	messier...	006-001	NTFS	08/22/03 8:25:43 PM	69	
messier.e01	D:	messier...	006-001	NTFS	08/22/03 8:35:37 PM	71	
messier.e01	D:	messier...	006-001	Unpartitioned Sp...	08/22/03 8:41:18 PM	295	

4 Listed | 6 Checked Total | D:\messier.e01

You can how many items exist in various categories, view lists of items, and look at individual files.

Evidence and File Items

The statistics for each category are automatically listed. Click the category button to its associated file list.

Category	Description
Actual Files	Filters out parsed files and lists only actual files in the case. An actual file is one that existed on the original hard drive as a file: documents, zip files, executables, logs, etc. For example, a file extracted from a Zip archive is filtered out.
All Items	All items in the case. This includes files as well as embedded items such as e-mail attachments, files within Zip archives, and so forth.
Checked Items	All items that are checked in any of the FTK windows.
Evidence Item	A physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive.
File Item	Individual items added to the case such as text files, documents, graphics, OLE items, drive images, and so forth.
Filtered	Filters the items shown in the Overview window.
Filtered In	Files included by the current filter.
Filtered Out	Files excluded by the current filter.
Flagged Thumbnails	Graphics you have flagged. Flagged graphics appear with a green button in the thumbnail view in the Graphics window.
Other Thumbnails	Graphics that have not been flagged. These graphics appear with a red button in the thumbnail view in the Graphics window.
Total File Items	Total items in the case, which is not necessarily the number of files in the case because multiple items can be parsed out of one file. For example, a Zip archive can contain many items. Total File Items is the total items in the case unless Filtered is selected.

Category	Description
Unchecked Items	All items that are left unchecked.
Unfiltered	A filter that overrides normal filters. This filter is specific to the Overview window.

File Status

File Status covers a number of file categories that can alert you to problem files or help you narrow down a search.

The statistics for each category are automatically listed. Click the category button to the file list associated with it.

Category	Description
Bad Extension	Files with an extension that does not match the file type identified in the file header, for example, a GIF image renamed as graphic.txt.
Bookmarked Items	Files that you bookmarked in FTK.
Deleted Files	Complete files or folders recovered from slack or free space.
Duplicate Items	Any items that have an identical hash. Because the filename is not part of the hash, identical files may actually have different filenames. The primary item is the first one found by FTK.
Encrypted Files	Files that are encrypted or have a password. This includes files that have a read-only password; that is, they may be opened and viewed, but not modified by the reader. If the files have been decrypted with EFS and you have access to the user’s login password, you can decrypt these files. See “Decrypting EFS” on page 217.
Flagged Ignore	Files that are flagged to be ignored.
From E-mail	All e-mail related files including e-mail messages, archives, and attachments.
From Recycle Bin	Files retrieved from the Windows Recycle Bin.

Category	Description
KFF Alert Files	Files identified by the HashKeeper Website as contraband or illicit files.
KFF Ignorable	Files identified by the HashKeeper and NIST databases as common, known files such as program files.
OLE Subitems	Items or pieces of information that are embedded in a file, such as text, graphics, or an entire file. This includes file summary information (also known as metadata) included in documents, spreadsheets, and presentations.

File Category

File Category itemizes the files by function, for example, a word processing document, graphics, e-mail, executable (program file), or folder.

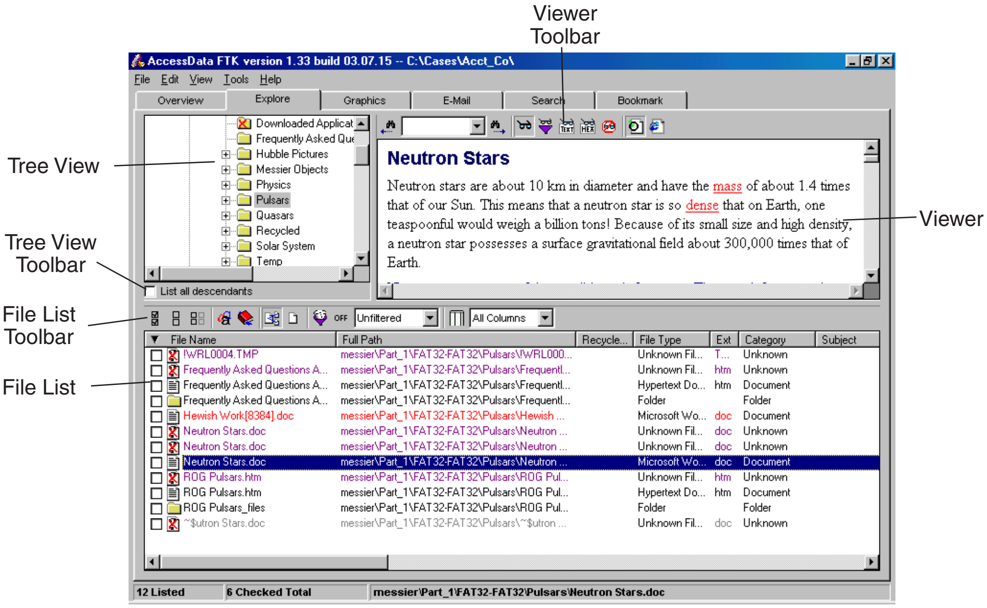
The statistics for each category are automatically listed. Click the category button to the file list associated with it.

Category	Description
Archives	Archive files include e-mail archive files, Zip, Stuffit,Thumbs.db thumbnail graphics, and other archive formats. For a complete list of archive file types recognized by FTK, see “Archive File Types” on page 291.
Databases	Includes databases from Access, Quicken, Microsoft Money, QuickBooks, and others. For a complete list of database file types recognized by FTK, see “Database File Types” on page 286.
Documents	Includes most word processing, HTML, WML, HDML, or text files. For a complete list of document file types recognized by FTK, see “Document File Types” on page 282.

Category	Description
E-mail Message	Includes e-mail messages from Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail, and MSN. For a complete list of e-mail message file types recognized by FTK, see "E-mail Message Programs" on page 290.
Executables	Includes executables from Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats. For a complete list of executable file types recognized by FTK, see "Executable File Types" on page 291.
Folders	Folders or directories that are located in the evidence.
Graphics	Includes the standard graphic formats like .tif, .gif, .jpeg, and .bmp. For a complete list of graphic file types recognized by FTK, see "Graphic File Types" on page 288.
Multimedia	Includes the multimedia formats such as: MP3, Flash, QuickTime, WAV, and MIDI. **Important:** This feature may not place every multimedia type, including supported types, in the Multimedia container. You should still search for any known multimedia types. For a complete list of graphic file types recognized by FTK, see "Multimedia File Types" on page 290.
Other Known Type	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, link files, etc. For a complete list of other file types recognized by FTK, see "Other Known File Types" on page 293.
Slack/Free Space	Fragments of files that have not been completely overwritten.
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others. For a complete list of spreadsheet file types recognized by FTK, see "Spreadsheet File Types" on page 285.
Unknown Type	File types that FTK cannot identify.

Explore Window

The Explore window displays all the contents of the case files and drives.



Neutron Stars

Neutron stars are about 10 km in diameter and have the mass of about 1.4 times that of our Sun. This means that a neutron star is so dense that on Earth, one teaspoonful would weigh a billion tons! Because of its small size and high density, a neutron star possesses a surface gravitational field about 300,000 times that of Earth.

File Name	Full Path	Recycle...	File Type	Ext	Category	Subject
□ !WRL0004.TMP	messier\Part_1\FAT32-FAT32\Pulsars\!WRL000...		Unknown Fil...	T...	Unknown	
□ Frequently Asked Questions A...	messier\Part_1\FAT32-FAT32\Pulsars\Frequentl...		Unknown Fil...	htm	Unknown	
□ Frequently Asked Questions A...	messier\Part_1\FAT32-FAT32\Pulsars\Frequentl...		Hypertext Do...	htm	Document	
□ Frequently Asked Questions A...	messier\Part_1\FAT32-FAT32\Pulsars\Frequentl...		Folder		Folder	
□ Hewish Work[8384].doc	messier\Part_1\FAT32-FAT32\Pulsars\Hewish ...		Microsoft Wo...	doc	Document	
□ Neutron Stars.doc	messier\Part_1\FAT32-FAT32\Pulsars\Neutron ...		Unknown Fil...	doc	Unknown	
□ Neutron Stars.doc	messier\Part_1\FAT32-FAT32\Pulsars\Neutron ...		Unknown Fil...	doc	Unknown	
□ Neutron Stars.doc	messier\Part_1\FAT32-FAT32\Pulsars\Neutron ...		Microsoft Wo...	doc	Document	
□ ROG Pulsars.htm	messier\Part_1\FAT32-FAT32\Pulsars\ROG Pul...		Unknown Fil...	htm	Unknown	
□ ROG Pulsars.htm	messier\Part_1\FAT32-FAT32\Pulsars\ROG Pul...		Hypertext Do...	htm	Document	
□ ROG Pulsars_files	messier\Part_1\FAT32-FAT32\Pulsars\ROG Pul...		Folder		Folder	
□ ~$utron Stars.doc	messier\Part_1\FAT32-FAT32\Pulsars\~$utron ...		Unknown Fil...	doc	Unknown	

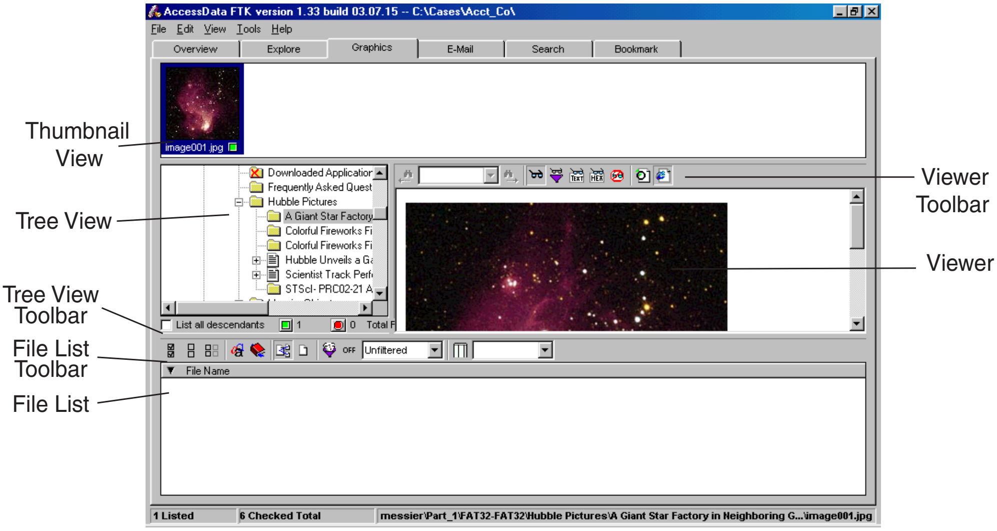
The Explore window contains the following:

- Tree view: Lists directory structure of each evidence item, similar to the way one would view directory structure in Windows Explorer. An evidence item is a physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive. The List All Descendants option on the Tree View toolbar displays all the currently selected folder's files in the File List.
- Viewer: Displays the contents of the currently selected file. The Viewer toolbar allows you to choose different view formats.
- File List: Displays information about a file, such as filename, file path, and file type.

For information about the toolbar options, see “Toolbar Components” on page 48. For information about the columns in the File List, see “File List Columns” on page 51.

Graphics Window

The Graphics window displays the case in photo-album style. Each graphic file is shown in a thumbnail view. If you select a graphic, it is displayed in the viewer.



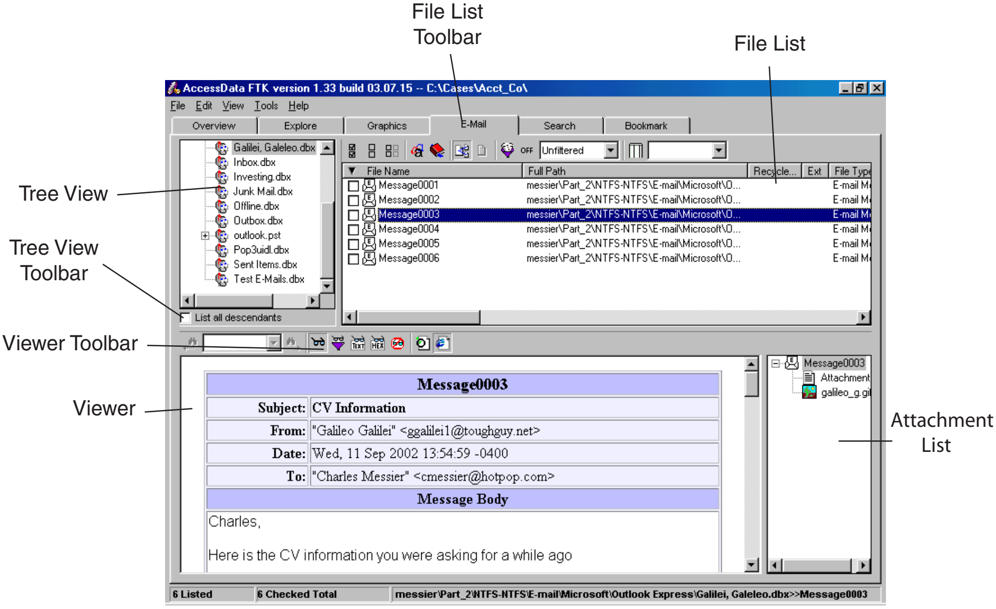
Beneath each thumbnail image is a button that can be clicked red or green. Flagging a graphic red or green is only relevant to the case report. When creating a report, you can choose to include all of the graphics in the case or only those graphics that are flagged green. To automatically mark all the thumbnails green, click the green button in the Tree View toolbar. Conversely, click the red button in the Tree View toolbar to automatically mark all the thumbnails red.

In the Graphics window, only graphic files appear in the File List. This simplifies the process of working with graphics.

For information about the toolbar options, see “Toolbar Components” on page 48. For information about the columns in the File List, see “File List Columns” on page 51.

E-mail Window

The E-mail window displays e-mail mailboxes, including Web e-mail, and their associated messages and attachments. The display is a coded HTML format. For the list of the supported e-mail applications, see "E-mail Message Programs" on page 290.



File Name	Full Path	Recycle...	Ext	File Type
□ Message0001	messier\Part_2\NTFS-NTFS\E-mail\Microsoft\O...			E-mail M
□ Message0002	messier\Part_2\NTFS-NTFS\E-mail\Microsoft\O...			E-mail M
□ Message0003	messier\Part_2\NTFS-NTFS\E-mail\Microsoft\O...			E-mail M
□ Message0004	messier\Part_2\NTFS-NTFS\E-mail\Microsoft\O...			E-mail M
□ Message0005	messier\Part_2\NTFS-NTFS\E-mail\Microsoft\O...			E-mail M
□ Message0006	messier\Part_2\NTFS-NTFS\E-mail\Microsoft\O...			E-mail M

Message0003	
Subject:	CV Information
From:	"Galileo Galilei" <ggalilei1@toughguy.net>
Date:	Wed, 11 Sep 2002 13:54:59 -0400
To:	"Charles Messier" <cmessier@hotpop.com>
Message Body	

Charles,

Here is the CV information you were asking for a while ago

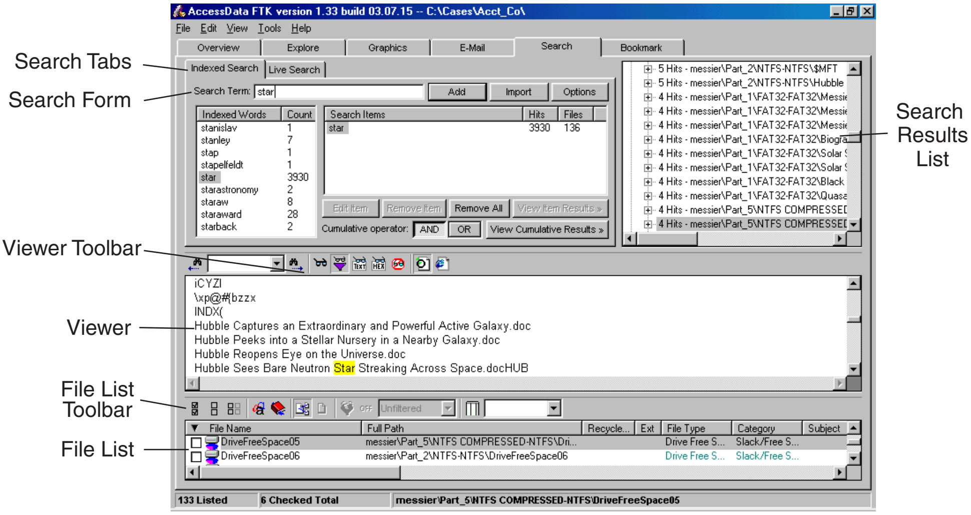
6 Listed | 6 Checked Total | messier\Part_2\NTFS-NTFS\E-mail\Microsoft\Outlook Express\Galilei, Galeleo.dbx>>Message0003

The File List references the subject line of the e-mail or the file attached to a message.

For information about the toolbar options, see "Toolbar Components" on page 48. For information about the columns in the File List, see "File List Columns" on page 51.

Search Window

Through the Search window, you can conduct an indexed search or a live search. An indexed search is fast. A live search is more flexible.



AccessData FTK version 1.33 build 03.07.15 -- C:\Cases\Acct_Co\

Search Term: star

Indexed Words	Count
stanislav	1
stanley	7
stap	1
stapelfeldt	1
star	3930
starastronomy	2
staraw	8
staraward	28
starback	2

Search Items	Hits	Files
star	3930	136

Cumulative operator:

```
5 Hits - messier\Part_2\NTFS-NTFS\$MFT
5 Hits - messier\Part_2\NTFS-NTFS\Hubble
4 Hits - messier\Part_1\FAT32-FAT32\Messie
4 Hits - messier\Part_1\FAT32-FAT32\Messie
4 Hits - messier\Part_1\FAT32-FAT32\Messie
4 Hits - messier\Part_1\FAT32-FAT32\Biogra
4 Hits - messier\Part_1\FAT32-FAT32\Solar S
4 Hits - messier\Part_1\FAT32-FAT32\Solar S
4 Hits - messier\Part_1\FAT32-FAT32\Black
4 Hits - messier\Part_1\FAT32-FAT32\Quasa
4 Hits - messier\Part_5\NTFS COMPRESSED
4 Hits - messier\Part_5\NTFS COMPRESSED
```

```
iCYZI
\xp@#|bzzx
INDX(
Hubble Captures an Extraordinary and Powerful Active Galaxy.doc
Hubble Peeks into a Stellar Nursery in a Nearby Galaxy.doc
Hubble Reopens Eye on the Universe.doc
Hubble Sees Bare Neutron Star Streaking Across Space.docHUB
```

File Name	Full Path	Recycle...	Ext	File Type	Category	Subject
□ DriveFreeSpace05	messier\Part_5\NTFS COMPRESSED-NTFS\Dri...			Drive Free S...	Slack/Free S...	
□ DriveFreeSpace06	messier\Part_2\NTFS-NTFS\DriveFreeSpace06			Drive Free S...	Slack/Free S...	

133 Listed | 6 Checked Total | messier\Part_5\NTFS COMPRESSED-NTFS\DriveFreeSpace05

The results of each search appear as a line item in the search results list. Click the plus icon (+) next to a search line to expand the search results. To view a specific item, select the file in the search results or file lists. All search terms are highlighted in the file. For information on searching, see “Searching a Case” on page 149.

For information about the toolbar options, see “Toolbar Components” on page 48. For information about the columns in the File List, see “File List Columns” on page 51.

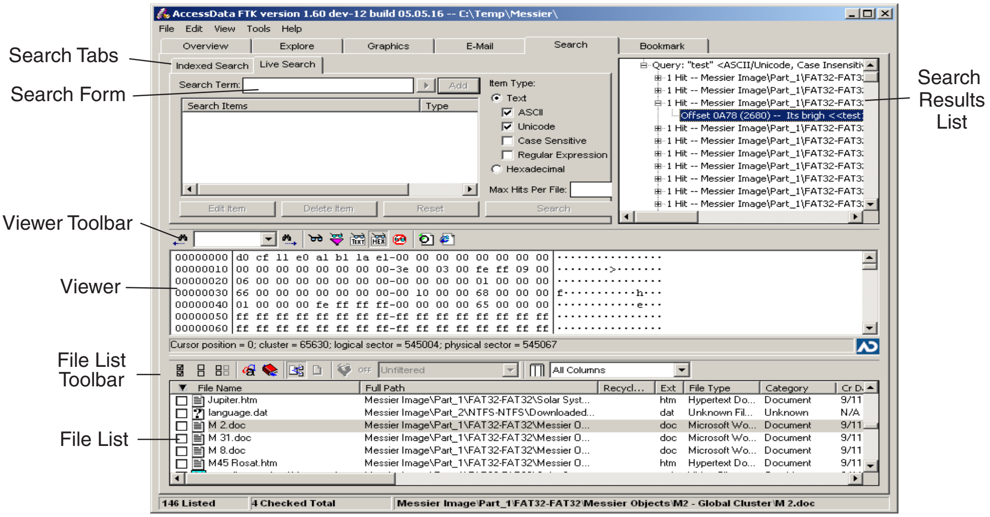
Indexed Search

The following table describes the interface options on the Indexed Search tab.

Interface Option	Description
Add	Adds the search term to Search Items. You can add multiple terms to one search.
Count	The number of times the indexed word is found in the case.
Cumulative Operator: And	This operator is specific to multi-term searches. FTK looks for items that contain all the search terms listed in the search list.
Cumulative Operator: Or	This operator is specific to multi-term searches. FTK looks for items that contain any of the search terms listed in the search list.
Edit Item	Allows you to edit the currently selected search term.
Files	The number of files the search term is found in.
Hits	The number of times the search term is found in the case.
Import	Imports search terms from text files.
Indexed Words	This column displays the index. When a search term is entered in the search field, this column scrolls to display the term in the index.
Options	Options that allow you to broaden or narrow the search.
Remove All	Removes all search terms from the search list.
Remove Item	Removes the currently selected search term from the search list.
Search Items	Lists the search terms.
Search Term field	The field in which you enter the term you want to search for.
View Cumulative Results	Initiates a multi-term search. For more information, see “Multi-Term Searches” on page 160.
View Item Results	Initiates a single term search. For more information, see “Single-Term Searches” on page 156.

Live Search

The following table describes the interface options on the Live Search tab.



```
Query: "test" <ASCII/Unicode, Case Insensiti
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
    Offset 0A78 (2680) --  Its brigh <<test
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
  1 Hit -- Messier Image\Part_1\FAT32-FAT3:
```

```
00000000 d0 cf 11 e0 a1 b1 1a e1-00 00 00 00 00 00 00 00 ................
00000010 00 00 00 00 00 00 00 00-3e 00 03 00 fe ff 09 00 ........>.......
00000020 06 00 00 00 00 00 00 00-00 00 00 00 01 00 00 00 ................
00000030 66 00 00 00 00 00 00 00-00 10 00 00 68 00 00 00 f...........h...
00000040 01 00 00 00 fe ff ff ff-00 00 00 00 65 00 00 00 ............e...
00000050 ff ff ff ff ff ff ff ff-ff ff ff ff ff ff ff ff ................
00000060 ff ff ff ff ff ff ff ff-ff ff ff ff ff ff ff ff ................
```

Cursor position = 0; cluster = 65630; logical sector = 545004; physical sector = 545067

	File Name	Full Path	Recycl...	Ext	File Type	Category	Cr D.
☐	Jupiter.htm	Messier Image\Part_1\FAT32-FAT32\Solar Syst...		htm	Hypertext Do...	Document	9/11
☐	language.dat	Messier Image\Part_2\NTFS-NTFS\Downloaded...		dat	Unknown Fil...	Unknown	N/A
☐	M 2.doc	Messier Image\Part_1\FAT32-FAT32\Messier O...		doc	Microsoft Wo...	Document	9/11
☐	M 31.doc	Messier Image\Part_1\FAT32-FAT32\Messier O...		doc	Microsoft Wo...	Document	9/11
☐	M 8.doc	Messier Image\Part_1\FAT32-FAT32\Messier O...		doc	Microsoft Wo...	Document	9/11
☐	M45 Rosat.htm	Messier Image\Part_1\FAT32-FAT32\Messier O...		htm	Hypertext Do...	Document	9/11

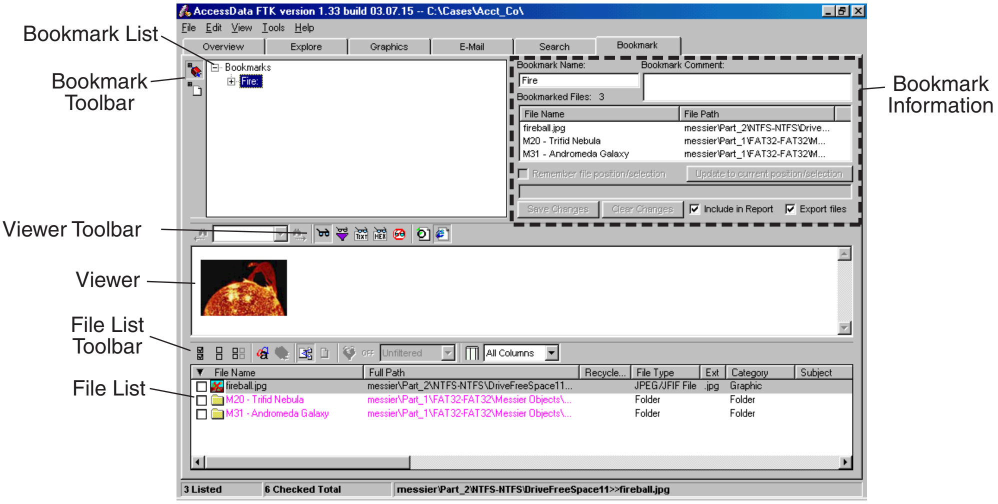
146 Listed | 4 Checked Total | Messier Image\Part_1\FAT32-FAT32\Messier Objects\M2 - Global Cluster\M 2.doc

Interface Option	Description
Add	Adds the search term to the search list. You can add multiple terms to one search.
ASCII	Searches any text in the same single-byte character set that your Windows version natively uses. For example, the English version of Windows uses the ISO 8859-1 character set; therefore, on English systems, you can find words in any ISO 8859-1 language. **Note:** For a listing of character sets used by common languages, visit http://www.w3.org/International/O-charset-lang.html.
Case Sensitive	Searches for the term exactly as it is typed in the Search Term field.
Delete Item	Deletes the currently selected search term from the search list.
Edit Item	Allows you to edit the currently selected search term.

Interface Option	Description
Hexadecimal	Searches in hexadecimal. It can be used to find embedded information that doesn't display in text.
Max Hits Per File	Lists the maximum number of search hits that will be returned in a search.
Regular Expression	Searches patterns in files, such as, any numbers that are in a phone number pattern. When selected, the arrow next to the Search Term field is activated. Clicking the arrow displays the predefined regular expressions and the option to edit the expressions. For regular expression syntax, see "Regular Expression Searching" on page 295.
Reset	Clears all search terms from the search list.
Search	Searches all files or filtered files (depending on what you select) for the terms listed in Search Items.
Search Items	Lists the search terms.
Search Term field	The field in which you enter the term you want to search for.
Text	Searches text.
Type	Lists what was selected under Item Type.
Unicode	Converts the ASCII/ISO 8859-1 text typed in the Search Term field to Unicode (the UCS-2 little endian form) and searches the Unicode version of the text. This search cannot be used to find Unicode text, because there is no way to type Unicode text in the Search Term field. So, while the Unicode search doesn't search any additional languages, it does let you find ASCII/ISO 8859-1 strings that are being stored in Unicode.

Bookmark Window

On the Bookmark window, you can view all the items you have bookmarked as important items in the case. You can also add comments and mark them for inclusion in the report. For more information about bookmarking, see “Using Bookmarks” on page 128.



Bookmark Name: Fire

Bookmark Comment:

Bookmarked Files: 3

File Name	File Path
fireball.jpg	messier\Part_2\NTFS-NTFS\Drive...
M20 - Trifid Nebula	messier\Part_1\FAT32-FAT32\M...
M31 - Andromeda Galaxy	messier\Part_1\FAT32-FAT32\M...

☐ Remember file position/selection

☑ Include in Report ☑ Export files

	File Name	Full Path	Recycle...	File Type	Ext	Category	Subject
☐	fireball.jpg	messier\Part_2\NTFS-NTFS\DriveFreeSpace11...		JPEG/JFIF File	.jpg	Graphic	
☐	M20 - Trifid Nebula	messier\Part_1\FAT32-FAT32\Messier Objects\...		Folder		Folder	
☐	M31 - Andromeda Galaxy	messier\Part_1\FAT32-FAT32\Messier Objects\...		Folder		Folder	

3 Listed | 6 Checked Total | messier\Part_2\NTFS-NTFS\DriveFreeSpace11>>fireball.jpg

The following table describes the interface options specific to the Bookmark window.

Interface Option	Description
Bookmark Comment	Displays comments included with a bookmark.
Bookmark Name	Displays the name given to a bookmark when it was created.
Bookmarked Files	Number of bookmarked files.
Clear Changes	Resets the Include in Report and Export Files settings in the current bookmark.
Export Files	If checked, the files included in the bookmark are exported when a report is generated.
File Path	Displays the paths of bookmarked files.
Filename	Displays the bookmarked files’ filenames.
Include in Report	If checked, includes the bookmark and its files in case reports.

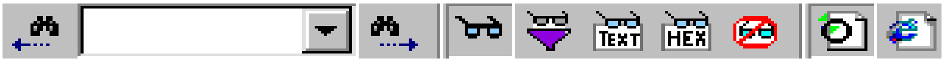
Interface Option	Description
Remember File Position/Selection	Remembers the highlighted text in the first bookmarked file and automatically highlights it when you return to the bookmark. The highlighted text also prints in the report. This option is disabled if there is more than one file in the bookmark.
Save Changes	Saves the Include in Report and Export Files settings for the current bookmark.
Update to Current Position/Selection	Use this option to change which text is highlighted in the bookmarked file. To change which text is highlighted in the bookmarked file: 1. Select the text you want highlighted when you return to the bookmark. 2. Click Update to Current Position/Selection. This option is disabled if there is more than one file in the bookmark.

For information about the toolbar options, see “Toolbar Components” on page 48. For information about the columns in the File List, see “File List Columns” on page 51.

Toolbar Components

The FTK interface contains several different toolbars. The following section lists the toolbars and their components.

Viewer Toolbar



The Viewer toolbar, shown above, appears in each window. The following table identifies and describes the toolbar components:

Component	Description
▼	In the text field, enter the text string you want to search for in the viewer. To initiate the search, click the Find Next ➡ or Find Previous button ⬅.
⬅	Searches backward in the current file. It highlights the previous instance of the search string in the viewer. This option does not search the previous file.
➡	Searches forward in the current file. It highlights the next instance of the search string in the viewer. This option does not search the next file.
👓	Displays the file in its native format. Typically, the file is viewed in Outside In (the viewer). However, FTK uses Internet Explorer to display HTML and graphics when possible.
▼	Displays the file in filtered text mode. Readable text is filtered out of binary files.
TEXT	Displays the file in the viewer in text format.
HEX	Displays the file in the viewer in hex format.

Component	Description
🚫	Disables the viewer.
	Displays the file in the Outside In viewer. Outside In can display 270 different file formats.
	Uses embedded Internet Explorer to view the file.

Tree List Toolbar

The Tree List toolbar appears in the Explore, Graphics, Email, and Bookmark windows. The components of the toolbar vary in each window.

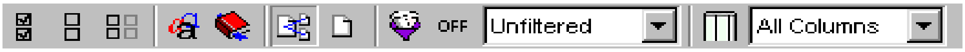
The following table lists and describes all components:

Component	Description
☑ List all descendants	This option appears in the Explore, Graphics, and E-mail windows. If checked, File List displays contents of all folders or directories.
🟩	This button is specific to the Graphics window. It marks all thumbnails green. When creating a report, you can choose to include all of the graphics in the case or only those graphics that are flagged green. The number next to the green button indicates how many thumbnails are marked.

●	This button is specific to the Graphics window. It marks all thumbnails red. When creating a report, you can choose to include all of the graphics in the case or only those graphics that are flagged green. The number next to the red button indicates how many thumbnails are excluded.
⊞	This button is specific to the Bookmark window. It displays bookmark names in the bookmark list. Bookmarked items are listed under their associated bookmark.
⊞	This button is specific to the Bookmark window. It displays the filenames of bookmarked items in the bookmark list. Each item lists its associated bookmark.

File List Toolbar

The File List toolbar appears in each window.



The following table identifies and describes the toolbar components:

Component	Description
☑ ☑	Checks all files in the current file list.
□ □	Unchecks all files in the current file list.
□□ □□	Unchecks all files in the case.
a	Opens a page to select colors and fonts for FTK categories. For more information about changing colors and fonts, see “Customizing Fonts and Colors” on page 245.

	Opens a page to create a new bookmark.
	Lists all items, including Zip contents, e-mail messages, and OLE streams.
	Lists only actual files.
	Opens File Filter Manager.
OFF	Displays “Off” if no file filter is active. Displays “On” if a file filter is active.
Unfiltered ▾	Drop-down list that contains different filters.
	Displays the File List column settings, including description of each column.
All Columns ▾	Drop-down list that contains different column views.

File List Columns

The following table describes all available columns in the File List. The columns you actually depend on what window and category you are in.

Hint: When viewing data in the File List, use the type-down control feature to locate the information you are looking for. Select the first item in the list and then type the first letter of the what you are searching for. FTK will move down the list to the first file containing that letter.

You can change which columns display, as well as the order of those columns. For more information, see “Customizing Columns” on page 249.

Column	Description
Acc Date	Date the file was last accessed
Alt Name	Item is an alternate name for an existing file in the case Usually, the alternate name refers to the MS-DOS filename (the 8.3 name) assigned to the file.
Attachment Info	E-mail attachment information
Badxt	Incorrect file extension
BCC	Blind carbon copy field in an e-mail message
Category	File category based on file type
CC	Carbon copy field in an e-mail message
Children	Number of files in the folder or archive
Cluster	The first cluster of the file
Cmp	Compressed file
Cr Date	Date and time the file was created **Note:** Date and time format options may be modified in FTK Preferences. For more information, see "Changing Preferences" on page 255.
Del	Deleted file
Descendants	Number of files in the folder or archive as well as its sub-folders
Dup	Duplicate file of another file in the case
Email Date	Date field in an e-mail message
Emailed	File from e-mail archive, either message or attachment
Enc	Encrypted or password-protected file
Ext	File extension
File Type	File type based on file content

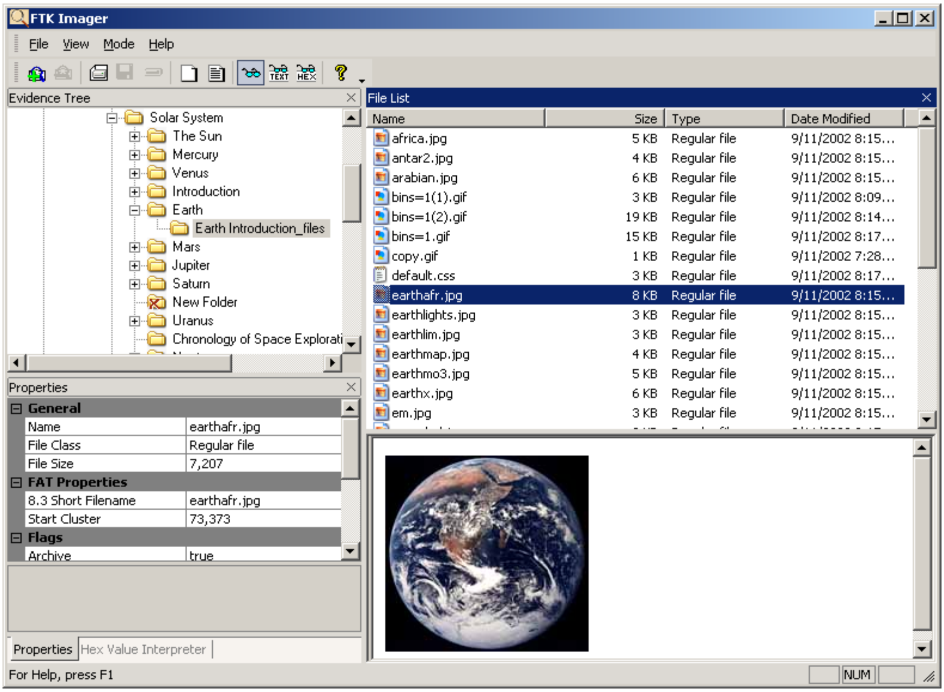
Column	Description
Filename	Filename without the path
From	From field in an e-mail message
Full Path	Full path of the file
Hash Set	Name of hash set containing matching hash
Header	File header (it only displays the first 8 bytes)
Hid	Hidden file
Idx	Indexed file
Item #	Unique item number
KFF	File matches a known file
L-Size	Logical file size; excludes file slack
MD5 Hash	MD5 (128-bit) hash of the data
Mod Date	Date and time the file was last modified
P-Size	Physical file size; includes file slack
Recyc	File recovered from the Recycle Bin
Recycle Bin Original Name	Full path of the file before it was sent to the Recycle Bin
RO	Read-only file
Sector	The logical sector (relative to the partition) where the file begins
SHA-1 Hash	SHA-1 (160-bit) hash of the data
Subject	E-mail subject
Sys	System file
To	To field in an e-mail message

FTK Imager

FTK Imager is a separate utility that is included with FTK. It allows you to

- Preview images and drives without having to add the evidence to the case.
- Create images.
- Convert images.
- Create hashes.
- View image, drive, file system, file and folder properties.

To open FTK Imager, select **File**, and then **FTK Imager**.



Name	Size	Type	Date Modified
africa.jpg	5 KB	Regular file	9/11/2002 8:15...
antar2.jpg	4 KB	Regular file	9/11/2002 8:15...
arabian.jpg	6 KB	Regular file	9/11/2002 8:15...
bins=1(1).gif	3 KB	Regular file	9/11/2002 8:09...
bins=1(2).gif	19 KB	Regular file	9/11/2002 8:14...
bins=1.gif	15 KB	Regular file	9/11/2002 8:17...
copy.gif	1 KB	Regular file	9/11/2002 7:28...
default.css	3 KB	Regular file	9/11/2002 8:17...
earthafr.jpg	8 KB	Regular file	9/11/2002 8:15...
earthlights.jpg	3 KB	Regular file	9/11/2002 8:15...
earthlim.jpg	3 KB	Regular file	9/11/2002 8:15...
earthmap.jpg	4 KB	Regular file	9/11/2002 8:15...
earthmo3.jpg	5 KB	Regular file	9/11/2002 8:15...
earthx.jpg	6 KB	Regular file	9/11/2002 8:15...
em.jpg	3 KB	Regular file	9/11/2002 8:15...

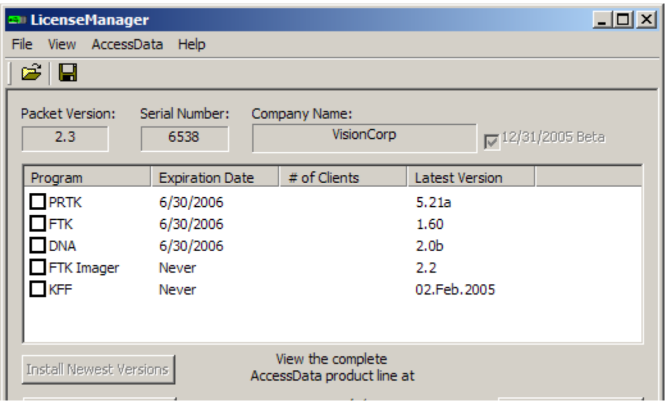
General	
Name	earthafr.jpg
File Class	Regular file
File Size	7,207
FAT Properties	
8.3 Short Filename	earthafr.jpg
Start Cluster	73,373
Flags	
Archive	true

Using LicenseManager

LicenseManager lets you manage product licenses on a dongle or in a dongle packet file.

With LicenseManager you can view license information, add or remove existing licenses to a dongle or dongle packet file, renew your subscription, purchase licenses, and send a dongle packet file to AccessData Technical Support. You can also check for product updates and download the latest product versions.

Note: While using many of the features in LicenseManager requires having an Internet connection, you can manage licenses in a dongle packet file for a dongle that resides on a machine where you do not want to connect to the Internet (because of the need for forensic soundness).



Packet Version: 2.3

Serial Number: 6538

Company Name: VisionCorp

☑ 12/31/2005 Beta

Program	Expiration Date	# of Clients	Latest Version
□ PRTK	6/30/2006		5.21a
□ FTK	6/30/2006		1.60
□ DNA	6/30/2006		2.0b
□ FTK Imager	Never		2.2
□ KFF	Never		02.Feb.2005

View the complete
AccessData product line at

LicenseManager displays dongle information (including packet version and serial number) and licensing information for such products as FTK, PRTK, DNA, and Registry Viewer. The licensing information provides the following:

- Name of the program
- Subscription expiration date
- Number of DNA clients (if any)
- Latest version of the program

Starting LicenseManager

To start LicenseManager, click **Help**, then **Launch LicenseManager,** or Click **Start**, then **Programs**, then **AccessData**, then **LicenseManager**, and then **LicenseManager**.

Note: LicenseManager.exe is located in the C:\Program Files\AccessData\Common Files\AccessData LicenseManager directory.

When you start LicenseManager, it reads licensing and subscription information from your dongle.

If you are using a dongle and LicenseManager either does not open or it displays the message "Dongle not Found."

- Make sure the dongle drivers are installed.

  For more information, see "Installing the Dongle Driver from CD" on page 17 or "Installing the Dongle Drivers from Downloadable Files" on page 21.
- Make sure the dongle is connected to the USB or parallel port.
- In LicenseManager, click **File**, then **Reload from Dongle**.

If you do not have a dongle installed, LicenseManager lets you manage licenses using a dongle packet file.

To open LicenseManager without a dongle installed:

1. Run LicenseManager by clicking **Start**, then **Programs**, then **AccessData**, then **LicenseManager**, and then **LicenseManager**.

   LicenseManager displays the message "Dongle not Found."
2. Click **OK** and browse for a dongle packet file to open.

When you start LicenseManager, you are prompted whether to check the update site for the latest product versions. You can also choose not to be prompted to check for updates when starting LicenseManager.

Note: If you disable displaying this prompt at startup, you cannot turn it back on. However, you can still check the update site for latest product versions by clicking **AccessData**, and then **Check for Updates**.

For more information about LicenseManager, see “Managing Licenses” on page 263.

CHAPTER 4

Starting a New Case

After you image the files or drives you want to examine, you are ready to start a new case. To simplify the process of starting a new case, Forensic Toolkit (FTK) uses the New Case Wizard.

The following sections review the options in the New Case Wizard:

- "Starting a Case" on page 60
- "Entering Forensic Examiner Information" on page 63
- "Completing the New Case Form" on page 61
- "Selecting Case Log Options" on page 64
- "Selecting Evidence Processes" on page 65
- "Refining the Case" on page 69
- "Refining the Index" on page 74
- "Managing Evidence" on page 78
- "Reviewing Case Summary" on page 88
- "Processing the Evidence" on page 89

Starting a Case

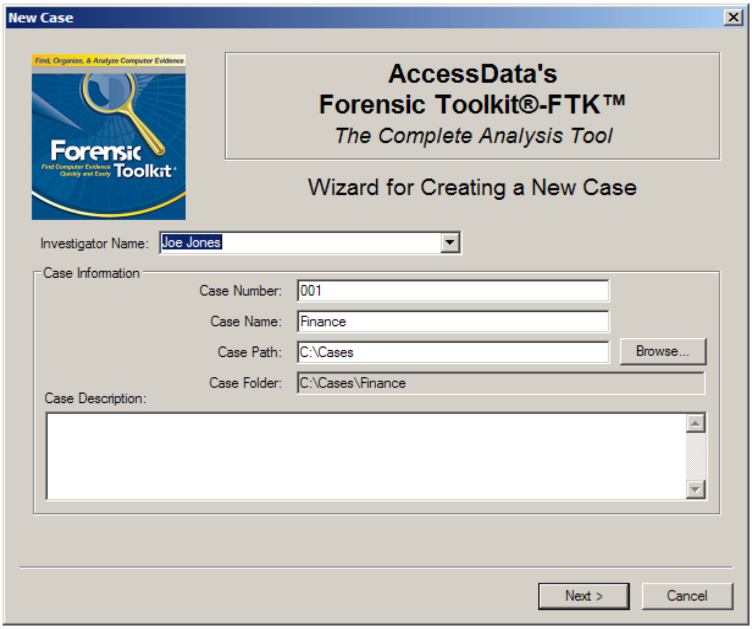
You access the New Case Wizard by selecting **File**, and then **New Case**. If this is your first time opening FTK or if you have chosen to always display the FTK Startup screen, select **Start a New Case** and click **OK**.

To start a new case, you must complete the following steps. Each step is discussed in detail in the following sections.

1. Enter basic case information.
2. Check what you want included in the case log.
3. Check the processes that you want run on the evidence.
4. Select the criteria for adding evidence to the case.
5. Select the criteria for creating the index.
6. Add the evidence.
7. Review your case selections.
8. Complete the wizard to launch the processing of evidence.

Completing the New Case Form

The New Case form provides fields for basic case information, such as the case name and its investigator.


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
Browse...
Next >
Cancel

Investigator Name: Joe Jones

Case Information

Case Number: 001

Case Name: Finance

Case Path: C:\Cases

Case Folder: C:\Cases\Finance

Case Description:

To provide the new case information:

1 In the **Investigator Name** field, type the name of the investigator.

  The drop-down list contains the name of investigators that have been entered in prior cases. If the investigator has worked on other cases in FTK, select the name from the list.

2 In the **Case Number** field, enter the case number for reference.

3 In the **Case Name** field, enter the name of the case.

The name cannot contain the following characters:

“ > ? / : \ | <

The case name also becomes the name of the folder where all case information will be stored.

4 Next to the **Case Path** field, click **Browse** to select the path where the evidence will be stored.

By default, all FTK cases are stored in that directory.

5 Verify that the **Case Folder** field lists the folder where you want the case to be stored.

Each case is stored in a separate folder and should be kept distinct from other cases.

The **Case Folder** field is based on the **Case Name** and **Case Path** fields. To make changes to the **Case Folder**, change the **Case Name** and **Case Path** fields.

6 (Optional) In the **Case Description** field, add information that will be helpful to the analysis of the case.

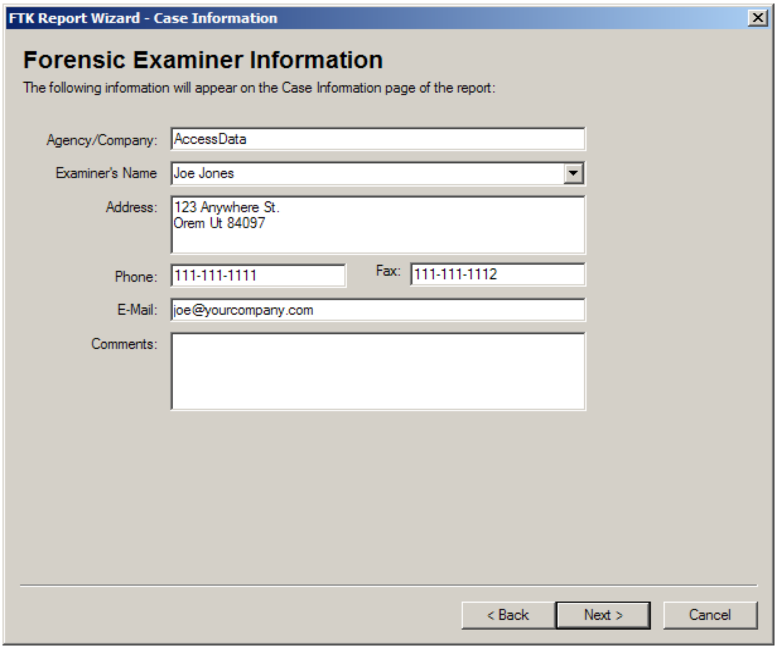
This field is particularly useful if several people work on the case.

This field is included in the report created at the end of the case investigation. For more information about the report, see “Working with Reports” on page 221.

7 Click **Next**.

Entering Forensic Examiner Information

The Forensic Examiner Information form allows you to enter information about the forensic examiner. This information then appears on the Case Information page of the report



FTK Report Wizard - Case Information

Forensic Examiner Information

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

Agency/Company: AccessData

Examiner's Name: Joe Jones

Address: 123 Anywhere St.
Orem Ut 84097

Phone: 111-111-1111

Fax: 111-111-1112

E-Mail: joe@yourcompany.com

Comments:

To provide the forensic examiner information:

1 In the **Agency/Company** field, type the name of the agency or company.

2 In the **Examiner's Name** field, type the name of the examiner.

The drop-down list contains the name of examiners that have been entered in prior cases. If the examiner has worked on other cases in FTK, select the name from the list.

3 In the **Address** field, enter the address for the agency/company.

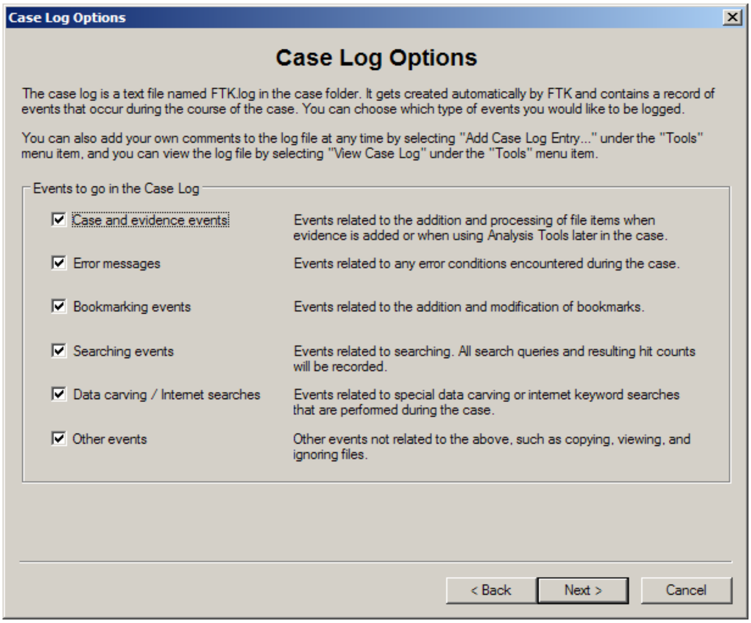
4 In the **Phone** field, enter the phone number for the agency/company.

5 In the **E-Mail** field, enter the examiner's e-mail address.

6 In the **Comments** field, enter any necessary comments.

Selecting Case Log Options

The Case Log Options form allows you to select which events you want FTK to log for the current case. FTK maintains a log file of FTK events such as bookmarking items, searches, and error messages for each case.



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

☑ 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.

The following table outlines the Case Log Options form:

Option	Description
Bookmarking Events	Events related to the addition and modification of bookmarks.
Case and Evidence Events	Events related to the addition and processing of file items when evidence is added or when using the Analysis Tools.
Data Carving/Internet Searches	Events related to data carving or Internet keyword searches that are performed during the case.

Option	Description
Error Messages	Events related to any errors encountered during the case.
Other Events	The following events: ◆ Copy special ◆ Exporting files ◆ Viewing items in the detached viewer ◆ Ignoring and unignoring files
Searching Events	All search queries and resulting hit counts.

The case log file is named ftk.log. This file is created automatically by FTK and is placed in the case folder, which is specified during the selection of the case name and case path.

The case log can be used as part of a report or to identify what has occurred on the case if you are assigned to an investigation in progress.

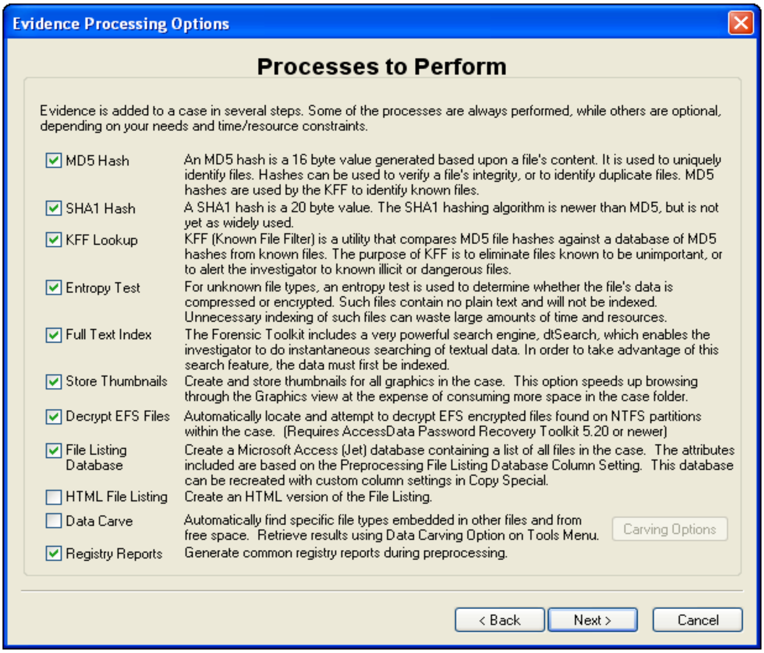
In the Case Log Options form:

1. Select what you want to include in the case log.
2. Click **Next**.

You can also add entries to the case log. For more information, see “Adding Entries to the Case Log” on page 140.

Selecting Evidence Processes

The Evidence Processing Options form allows you to select which processes you want to perform on the current evidence. You only need to select those processes that are relevant to the evidence you are adding to the case. For example, if your case is primarily a graphics case, there is no need to index the evidence.



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	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
☑ KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
☑ 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 this search feature, the data must first be indexed.
☑ 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.
☑ Registry Reports	Generate common registry reports during preprocessing.

Another factor that may determine which processes you select is time frame. If you are adding a large image to the case, it will take some time to create an index for that amount of information. If you are in a hurry, you can add the image to the case without creating the index. You can then return at a later time and index the image. For information on processing evidence after it is added to the case, see “Using Analysis Tools” on page 135.

The following table outlines the Evidence Processing Options form:

Process	Description
Data Carve	Carves data immediately after pre-processing. Select Carving Options and then select the file types you want to carve immediately. For more information on Data Carving, see “Data Carving” on page 181.
Decrypt EFS Files	Automatically locates and attempts to decrypt EFS encrypted files found on NTFS partitions with the case (requires Password Recovery Toolkit 5.20 or later). For more information on EFS, see “Decrypting EFS” on page 217.
Entropy Test	Determines if the data in unknown file types is compressed or encrypted. The compressed and encrypted files identified in the entropy test are not indexed.
File Listing Database	Creates a Microsoft Access (Jet) database containing a list of all files in the case. The attributes included are based on the Default File List Column Setting. This database can be recreated with custom column setting in Copy, and then Special.
Full Text Index	Indexes all keyboard-related characters in the case evidence. This process is the most time-consuming step in starting a new case. However, the index is required for data carving and Internet keyword searches. It also makes searching much more efficient. For more information about indexing, including disk space requirements, see “Conducting an Indexed Search” on page 154.
HTML File Listing	Creates an HTML version of the File Listing database.
KFF Lookup	Using a database of hashes from known files, this option eliminates ignorable files, checks for duplicate files, and alerts you to known illicit or dangerous files. For more information about Known File Filter (KFF), see “Known File Filter” on page 9.

Process	Description
MD5 Hash	Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. For more information about MD5 hashes, see “Message Digest 5” on page 344.
Registry Reports	Generates common registry reports. For more information about Registry Report Summaries, see “Creating Registry Summary Reports” on page 208.
SHA-1 Hash	Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. This is the only process not checked by default. If you want FTK to create SHA-1 hashes, you must check the box. For more information about SHA-1 hashes, see “Secure Hash Algorithm” on page 344.
Store Thumbnails	Creates and stores thumbnails for all graphics in the case. This process speeds up the browsing of graphics in the Graphics window. Each thumbnail is about 4 KB per graphic file.

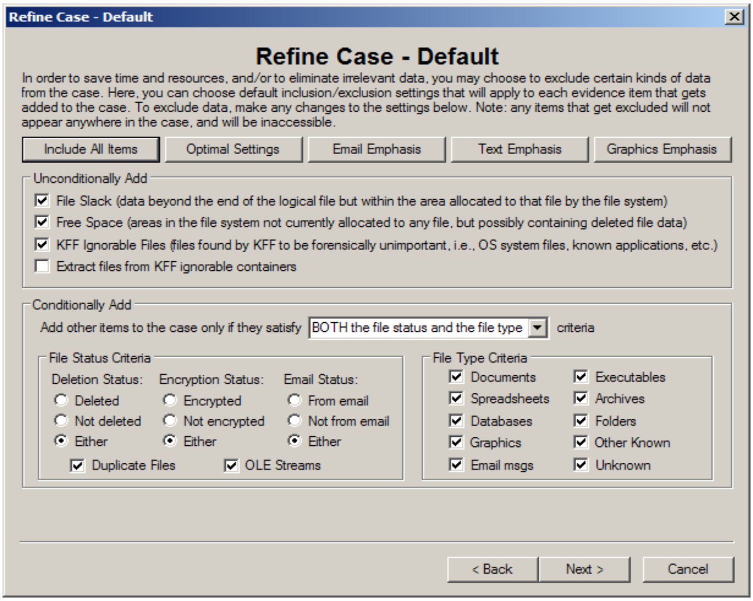
In the Evidence Processing Options form:

1 Select the processes that you want to be run on the evidence.

2 Click **Next**.

Refining the Case

The Refine Case form allows you to exclude certain kinds of data from the case.



Refine Case - Default

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

Unconditionally Add

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

Conditionally Add

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

File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
○ Deleted	○ Encrypted	○ From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	● Either

☑ Duplicate Files ☑ OLE Streams

File Type Criteria

☑ Documents	☑ Executables
☑ Spreadsheets	☑ Archives
☑ Databases	☑ Folders
☑ Graphics	☑ Other Known
☑ Email msgs	☑ Unknown

FTK contains five default exclusion templates:

- Include All Items
- Optimal Settings
- Email Emphasis
- Text Emphasis
- Graphics Emphasis

The default templates cannot be modified. However, you can modify the default template settings. Note that your settings cannot be saved for future use, so be sure to document any settings that you want to re-use.

AccessData strongly recommends that you include all items when adding evidence to a case.

Important: After data is excluded from an evidence item, you cannot go back and add it to the case. An evidence item is a physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive. FTK does not allow you to add the same evidence item more than once. If you discover that you need data that was previously excluded, you must create a new case. Consequently, AccessData strongly recommends that you use the Include All Items template unless you are absolutely certain that you will not need any of the excluded items.

The following tables outline the options in the Refine Case form:

Template Options

Template	Description
E-mail Emphasis	Includes only e-mail related files. Excludes file slack, free space, KFF ignorable files, duplicate files, OLE streams, executables, and folders. **Important:** Using the Data Carving feature, it is possible to retrieve graphics, documents and other files from file slack; therefore, you may not want to exclude file slack or unallocated space from your cases.
Graphics Emphasis	Excludes file slack, KFF ignorable files, duplicate files, OLE streams, executables, folders, and other file types such as audio and unknown files. **Important:** Using the Data Carving feature, it is possible to retrieve graphics, documents, and other files from file slack; therefore, you may not want to exclude file slack or unallocated space from your cases.
Include All Items	Includes all categories of files of any file status from any location in the image.
Optimal Settings	Created for smaller cases. Excludes KFF ignorable files, duplicate files, and executables.
Text Emphasis	Excludes KFF ignorable files, duplicate files, graphics, and executables.

Unconditionally Add Options

Option	Description
Extract Files from KFF Ignorable Containers	Files within KFF ignorable containers. **Note:** A container is a file that contains other files such as Zip files, e-mail archives, TAR files, and so forth. Containers that are flagged ignorable by the KFF include Windows .cab files and known DOOM level packs. Files that are extracted from containers have a double angle bracket (>>) in their path name. For example, c:\My Documents\letters.zip>>letter1.doc.
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 that could contain deleted file data.
KFF Ignorable Files	Files identified by the HashKeeper database as common, known files, such as program files.

File Status Criteria

Status	Description
Deletion Status	Allows you to exclude or include deleted items.
Duplicate Files	Allows you to include or exclude duplicate files.
Email Status	Allows you to include or exclude files associated with e-mail.
Encryption Status	Allows you to exclude or include encrypted or password-protected files.
OLE Streams	Allows you to include or exclude OLE elements embedded in a file.

File Type Criteria

Category	Description
Archives	Archive files include e-mail archive files, Zip, Stuffit,Thumbs.db thumbnail graphics, and other archive formats. For a complete list of archive file types recognized by FTK, see "Archive File Types" on page 291.
Databases	Includes databases from Access, Quicken, Microsoft Money, QuickBooks, and others. For a complete list of database file types recognized by FTK, see "Database File Types" on page 286.
Documents	Includes most word processing, HTML, WML, HDML, or text files. For a complete list of document file types recognized by FTK, see "Document File Types" on page 282.
E-mail Message	Includes e-mail messages from Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail, and MSN. For a complete list of e-mail message file types recognized by FTK, see "E-mail Message Programs" on page 290.
Executables	Includes executables from Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats. For a complete list of executable file types recognized by FTK, see "Executable File Types" on page 291.
Folders	Folders or directories located on the image.
Graphics	Includes the standard graphic formats like .tif, .gif, .jpeg, and .bmp. For a complete list of graphic file types recognized by FTK, see "Graphic File Types" on page 288.
Other Recognized	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, etc. For a complete list of other file types recognized by FTK, see "Other Known File Types" on page 293.

File Type Criteria

Category	Description
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others. For a complete list of spreadsheet file types recognized by FTK, see “Spreadsheet File Types” on page 285.
Unknown	File types that FTK cannot identify.

In the Refine Case form:

1 Select the default template that you want to use.

See the "Template Options" table on page 70.

Each template has different pre-defined settings; however, you can modify any of the default settings by selecting different options in the Refine Case form.

2 To modify the default options:

2a Select which items you want to unconditionally add to the case.

See the "Unconditionally Add Options" table on page 71.

Important: To use the data carving feature, you must add file slack and free space. For more information, see “Data Carving” on page 181.

2b From the drop-down list, indicate whether you want to add items that satisfy BOTH the File Status and File Type criteria or items that satisfy EITHER the File Status or File Type criteria.

2c Select the File Status criteria.

See the "File Status Criteria" table on page 71.

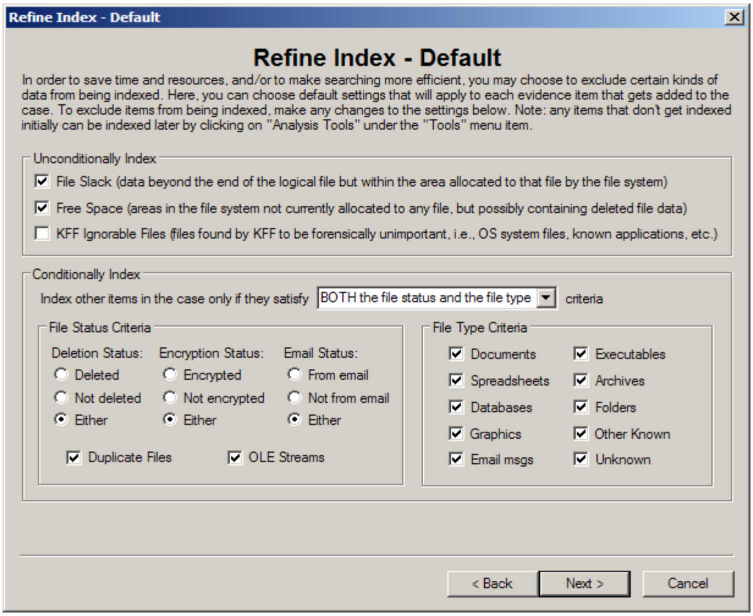
2d Select the File Type criteria.

See the "File Type Criteria" table on page 72.

3 Click **Next**.

Refining the Index

The Refine Index form allows you to specify types of data that you do not want to index. You might choose to exclude data to save time and resources and to increase searching efficiency.



Refine Index - Default

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:
○ Deleted	○ Encrypted	○ From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	● Either

☑ Duplicate Files ☑ OLE Streams

File Type Criteria

☑ Documents	☑ Executables
☑ Spreadsheets	☑ Archives
☑ Databases	☑ Folders
☑ Graphics	☑ Other Known
☑ Email msgs	☑ Unknown

Important: AccessData strongly recommends that you use the default index settings.

Indexing can be quite time-consuming. However the index is required for data carving and Internet keyword searches. It also makes searching much more efficient. Generally AccessData recommends that you accept the default index settings to create the most efficient index possible.

The index file is generated after the creation of a case; however, an evidence item can actually be indexed at any time. An evidence item is a physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive. For more information about indexing an evidence item, see "Using Analysis Tools" on page 135.

The index file contains all discrete words or number strings found in both the allocated and unallocated space in the case evidence.

After an evidence item is indexed, it is merged into the existing index and can no longer be removed from the case. For more information about indexing, see “Conducting an Indexed Search” on page 154.

The following tables outline the options in the Refine Index form:

Unconditionally Index Options

Option	Description
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 that could contain deleted file data.
KFF Ignorable Files	Files identified by the HashKeeper database as common, known files, such as program files.

File Status Criteria

Status	Description
Deletion Status	Allows you to exclude or include deleted items.
Encryption Status	Allows you to exclude or include encrypted or password-protected files.
Email Status	Allows you to include or exclude files associated with e-mail.
Duplicate Files	Allows you to include or exclude duplicate files.
OLE Streams	Allows you to include or exclude OLE elements embedded in a file.

File Type Criteria

Category	Description
Archives	Archive files include e-mail archive files, Zip, Stuffit,Thumbs.db thumbnail graphics, and other archive formats. For a complete list of archive file types recognized by FTK, see “Archive File Types” on page 291.
Databases	Includes databases from Access, Quicken, Microsoft Money, QuickBooks, and others. For a complete list of database file types recognized by FTK, see “Database File Types” on page 286.
Documents	Includes most word processing, HTML, WML, HDML, or text files. For a complete list of document file types recognized by FTK, see “Document File Types” on page 282.
E-mail Message	Includes e-mail messages from Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail, and MSN. For a complete list of e-mail message file types recognized by FTK, see “E-mail Message Programs” on page 290.
Executables	Includes executables from Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats. For a complete list of executable file types recognized by FTK, see “Executable File Types” on page 291.
Folders	Folders and directories.
Graphics	Includes the standard graphic formats like .tif, .gif, .jpeg, and .bmp. For a complete list of graphic file types recognized by FTK, see “Graphic File Types” on page 288.
Other Recognized	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, etc. For a complete list of other file types recognized by FTK, see “Other Known File Types” on page 293.

File Type Criteria

Category	Description
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others. For a complete list of spreadsheet file types recognized by FTK, see “Spreadsheet File Types” on page 285.
Unknown	File types that FTK cannot identify.

The Refine Index form has pre-defined settings; however, you can modify the default settings by selecting different options in the Refine Index form.

To modify the default index settings in the Refine Index form:

1 Select the types of files that you want to index.

1a Select which items you want to unconditionally index.

See the "Unconditionally Index Options" table on page 75.

Important: To use the data carving feature, you must index file slack and free space. For more information, see “Data Carving” on page 181.

1b From the drop-down list, indicate whether you want to index items that satisfy *both* the File Status and File Type criteria or items that satisfy *either* the File Status or File Type criteria.

1c Select the File Status criteria.

See the "File Status Criteria" table on page 75.

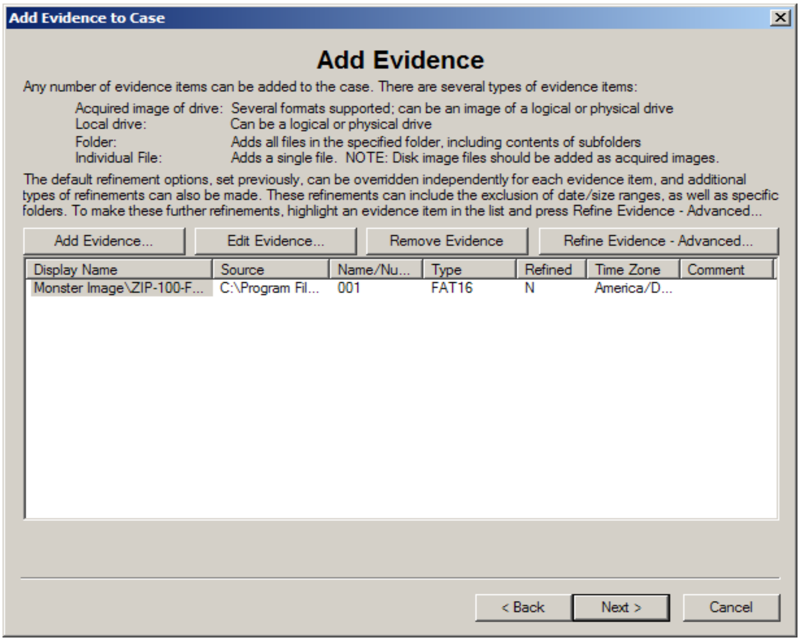
1d Select the File Type criteria.

See the "File Type Criteria" table on page 76.

2 Click **Next**.

Managing Evidence

As your investigation progresses, you will want to edit the information you entered for your evidence. Evidence is managed through the Add Evidence forms.



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...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
Monster Image\ZIP-100-F...	C:\Program Fil...	001	FAT16	N	America/D...	

The Add Evidence form allows you to perform the following functions:

- Add evidence.
- Remove evidence.
- Edit basic information about the evidence.
- Create parameters for adding evidence to the case.

The following sections review each function.

Adding Evidence

Evidence added during the same session of the New Case Wizard is created as part of one complete case. For example, you can add evidence from multiple floppies, a ZIP disk, and a hard drive.

Note: To protect the integrity of case evidence, all items are added as read-only.

You can add the same evidence item to multiple cases. An evidence item is a physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive.

To add evidence to the case:

1 In the Add Evidence Case form, click **Add Evidence**.

2 Select one of the following evidence types and click **Continue**:

Evidence Type	Description
Acquired Image of Drive	A forensic image of a logical or physical drive. If the image is segmented, select the first segment. **Important:** All the image segments must be placed in a single directory for FTK to process them properly. For a list of supported image formats, see “Supported File Systems and Image Formats” on page 13. When you add evidence using this type, you can successfully move the evidence later if necessary.
Contents of a Folder	A specific folder, any accompanying sub-folders, and files. The contents of a folder are always added in logical form; that is, they do not include file slack or deleted files. When you add evidence using this type, you should find a a permanent location for this folder because this evidence cannot be moved later.

Evidence Type	Description
Individual File	A specific file. Individual files are always added in a logical form; that is, they do not include file slack. **Note:** If you export an encrypted file for decryption, you can use this option to add the decrypted file back to the case. When you add evidence using this type, you should find a a permanent location for this folder because this evidence cannot be moved later.
Local Drive	A logical or physical drive. If you are running FTK on Windows NT, 2000, or XP, make sure that you are logged in on an account with administrative rights.

3 Browse to and select the evidence.

If you add an unidentified evidence item that is larger than 25 MB, it will be chunked into 25 MB pieces.

4 In the Evidence Information form, enter the following information and click **OK**:

Information Field	Description
Comment	Optional area for any additional information or clarification.
Evidence Display Name	The name used in FTK for the evidence item.
Evidence Identification Name/Number	The unique name or number by which this item will be known in the case.
Evidence Location	The same location that you selected when you added this item. If you move the item during the investigation, FTK will prompt you for the new location of the evidence when you load the case.

Information Field	Description
Local Evidence Time Zone	The time zone associated with the evidence. Local Evidence Time Zone is enabled when the evidence item is on the FAT file system. NTFS images store the created, accessed, and modified times in Universal Coordinated Time (UTC) (previously known as GMT or Greenwich Mean Time).

The information and the evidence item is added to the File List. The file format and any refinements are also listed. For information about refining case evidence, see “Refining Evidence” on page 81.

Editing Evidence

The Edit Evidence option allows you to modify the information you entered in the Evidence Information form.

To modify the evidence information for a particular item:

1 Select an evidence item in the File List.

2 Click **Edit Evidence**.

3 Modify the information in the Evidence Information form.

4 Click **OK**.

Removing Evidence

You can remove an item from the File List in the Add Evidence form only. You cannot remove an item from your case after it has been processed.

Refining Evidence

The Refine Evidence-Advanced option allows you to exclude specific data from an individual evidence item.

Note: You cannot refine evidence items after they are added to the case. This has to be done while adding the item.

AccessData strongly recommends that you include all items when adding evidence to a case.

Important: After data is excluded from an evidence item, you cannot go back and add it to the case. FTK does not allow you to add the same evidence item more than once. If you discover that you need data that was previously excluded, you must create a new case. Consequently, AccessData strongly recommends that you use include all items unless you are absolutely certain that you will not need any of the excluded items.

To refine case evidence:

1. Select the evidence item in the File List.
2. Click **Refine Evidence-Advanced**.

   The Refine Case-Advanced menu is organized into three windows:

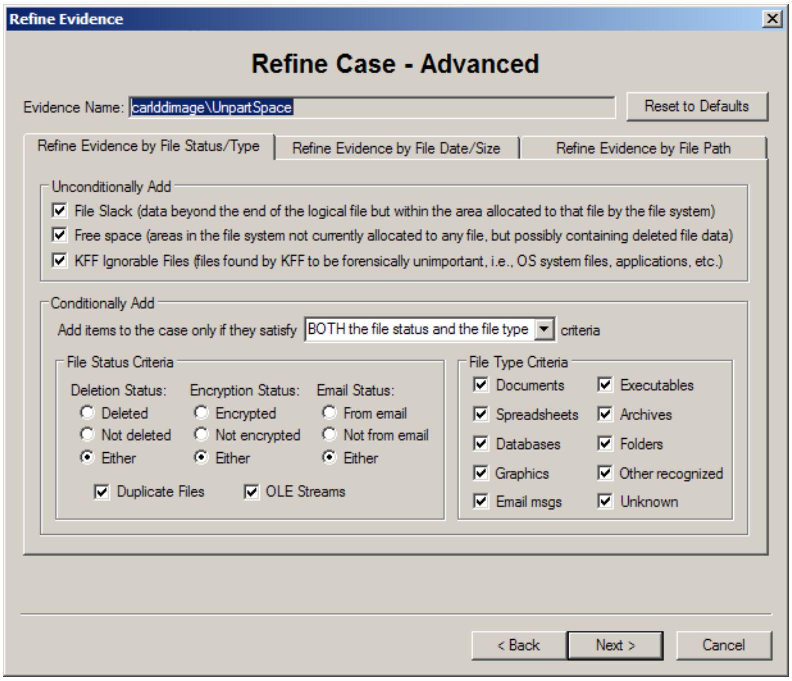
   - Refine Evidence by File Status/Type
   - Refine Evidence by File Date/Size
   - Refine Evidence by File Path
3. Click the corresponding tab to access each window.
4. Define the refinements you want for the current evidence item.

   If you want to reset the menu to the default settings, click **Reset to Defaults**.
5. Click **Next**.

The following sections review each window in the Refine Evidence-Advanced menu.

Refining Evidence—File Status/Type

The following tables outline the options in the Refine Evidence by File Status/Type window:


Refine Evidence
Refine Case - Advanced
Reset to Defaults
Refine Evidence by File Status/Type
Refine Evidence by File Date/Size
Refine Evidence by File Path
< Back
Next >
Cancel

Evidence Name: carlddimage\UnpartSpace

Unconditionally Add

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

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

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

Conditionally Add

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

File Status Criteria

Deletion Status: ○ Deleted ○ Not deleted ● Either

Encryption Status: ○ Encrypted ○ Not encrypted ● Either

Email Status: ○ From email ○ Not from email ● Either

☑ Duplicate Files ☑ OLE Streams

File Type Criteria

☑ Documents ☑ Executables
☑ Spreadsheets ☑ Archives
☑ Databases ☑ Folders
☑ Graphics ☑ Other recognized
☑ Email msgs ☑ Unknown

Unconditionally Add Options

Option	Description
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 that could contain deleted file data.
KFF Ignorable Files	Files identified by the HashKeeper database as common, known files, such as program files.

File Status Criteria

Status	Description
Deletion Status	Allows you to include or exclude deleted items.
Encryption Status	Allows you to include or exclude encrypted or password-protected files.
Email Status	Allows you to include or exclude files associated with e-mail.
Duplicate Files	Allows you to include or exclude duplicate files.
OLE Streams	Allows you to include or exclude OLE elements embedded in a file.

File Type Criteria

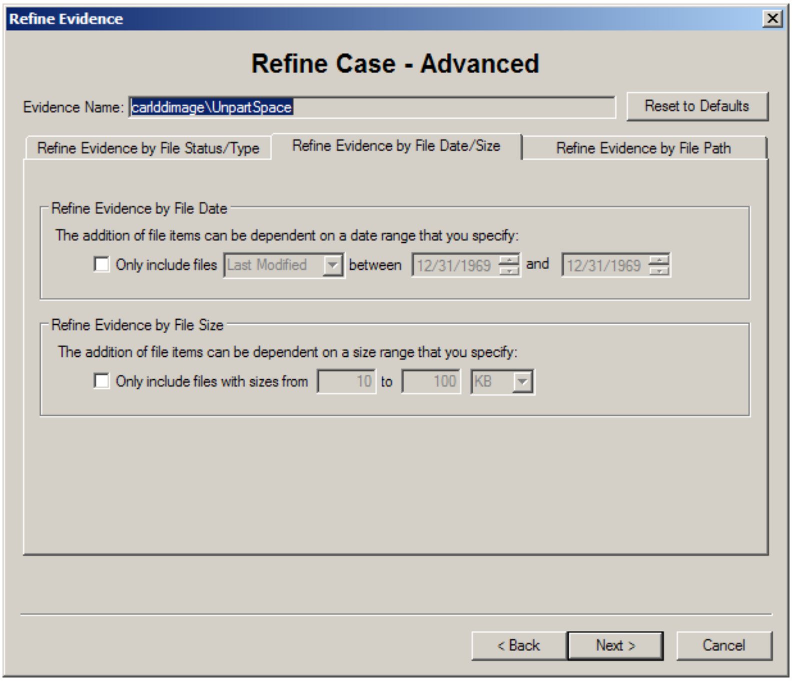
Category	Description
Archives	Archive files include e-mail archive files, Zip, Stuffit,Thumbs.db thumbnail graphics, and other archive formats. For a complete list of archive file types recognized by FTK, see “Archive File Types” on page 291.
Databases	Includes databases from Access, Quicken, Microsoft Money, QuickBooks, and others. For a complete list of database file types recognized by FTK, see “Database File Types” on page 286.
Documents	Includes most word processing, HTML, WML, HDML, or text files. For a complete list of document file types recognized by FTK, see “Document File Types” on page 282.
E-mail Message	Includes e-mail messages from Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail, and MSN. For a complete list of e-mail message file types recognized by FTK, see “E-mail Message Programs” on page 290.

File Type Criteria

Category	Description
Executables	Includes executables from Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats. For a complete list of executable file types recognized by FTK, see "Executable File Types" on page 291.
Folders	Folders and directories.
Graphics	Includes the standard graphic formats like .tif, .gif, .jpeg, and .bmp. For a complete list of graphic file types recognized by FTK, see "Graphic File Types" on page 288.
Other Recognized	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, etc. For a complete list of other file types recognized by FTK, see "Other Known File Types" on page 293.
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others. For a complete list of spreadsheet file types recognized by FTK, see "Spreadsheet File Types" on page 285.
Unknown	File types that FTK cannot identify.

Refining Evidence—File Date/Size

The following table outlines the options in the Refine Evidence by File Date/Size window:



Refine Evidence
Refine Case - Advanced
Reset to Defaults
Refine Evidence by File Status/Type
Refine Evidence by File Date/Size
Refine Evidence by File Path
Refine Evidence by File Date
Refine Evidence by File Size
< Back
Next >
Cancel

Evidence Name: carlddimage\UnpartSpace

The addition of file items can be dependent on a date range that you specify:

□ Only include files Last Modified between 12/31/1969 and 12/31/1969

The addition of file items can be dependent on a size range that you specify:

□ Only include files with sizes from 10 to 100 KB

Refine Evidence by File Date/Size

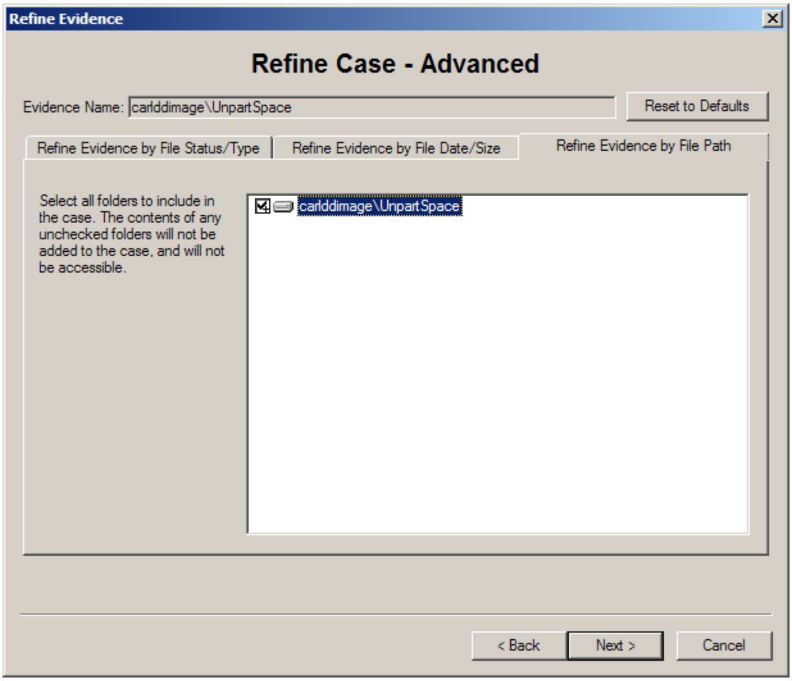
Exclusion	Description
Refine Evidence by File Date	Check to make the addition of evidence items dependent on a date range that you specify. To refine evidence by file date: 1. From the drop-down list, select **Created**, **Last Modified**, or **Last Accessed**. 2. In the two date fields, enter the beginning and ending dates that you want.

Refine Evidence by File Date/Size

Exclusion	Description
Refine Evidence by File Size	Check to make the addition of evidence items dependent on a file size that you specify. To refine evidence by file size: 1. In the two size fields, enter the minimum and maximum sizes that you want. 2. In the drop-down list, select **Bytes**, **KB**, or **MB**.

Refining Evidence—File Path

In the Refine Evidence by File Path window, mark the folders that you want to add to the case. The contents of any folders that are not marked will not be added to the case.


Refine Evidence
Refine Case - Advanced
Reset to Defaults
Refine Evidence by File Status/Type
Refine Evidence by File Date/Size
Refine Evidence by File Path
< Back
Next >
Cancel

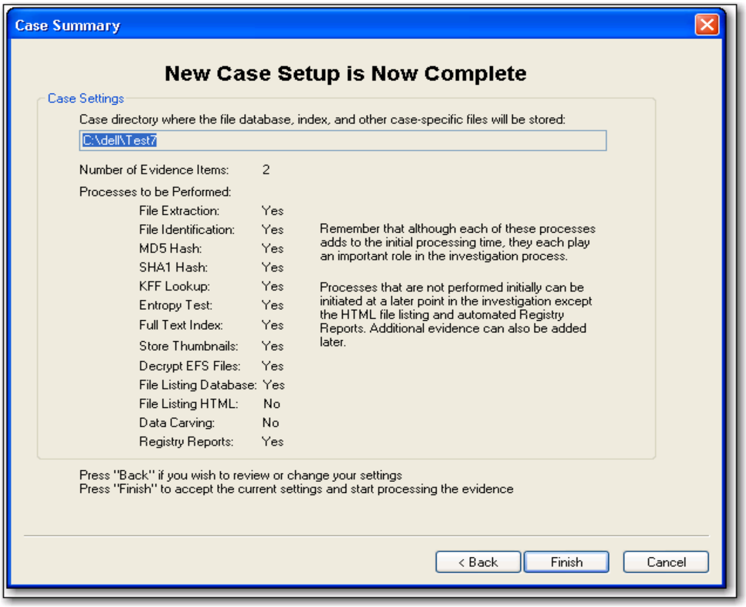
Evidence Name: carlddimage\UnpartSpace

Select all folders to include in the case. The contents of any unchecked folders will not be added to the case, and will not be accessible.

☑ carlddimage\UnpartSpace

Reviewing Case Summary

The Case Summary form allows you to review the evidence directory, number of evidence items, and evidence processes that you selected during the New Case Wizard.



New Case Setup is Now Complete

Case Settings

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

C:\dell\Test7

Number of Evidence Items: 2

Processes to be Performed:

File Extraction:	Yes
File Identification:	Yes
MD5 Hash:	Yes
SHA1 Hash:	Yes
KFF Lookup:	Yes
Entropy Test:	Yes
Full Text Index:	Yes
Store Thumbnails:	Yes
Decrypt EFS Files:	Yes
File Listing Database:	Yes
File Listing HTML:	No
Data Carving:	No
Registry Reports:	Yes

Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.

Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing and automated Registry Reports. Additional evidence can also be added later.

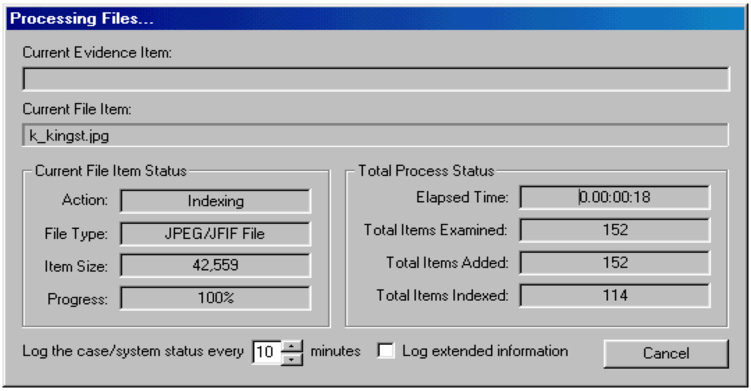
Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence

If you want to change or review any selections, click **Back** to return to the appropriate form. After you make your changes, click **Next** to return to the Case Summary form.

To accept the current settings and start the processing of the evidence, click **Finish**.

Processing the Evidence

After you click Finish, the Processing Files form appears and displays the status of the processes you selected in the wizard.



Processing Files...

Current Evidence Item:

Current File Item: k_kingst.jpg

Current File Item Status

Action: Indexing

File Type: JPEG/JFIF File

Item Size: 42,559

Progress: 100%

Total Process Status

Elapsed Time: 0.00:00:18

Total Items Examined: 152

Total Items Added: 152

Total Items Indexed: 114

Log the case/system status every 10 minutes

□ Log extended information

The Processing Files form allows you to select the interval for system status entries in the case log. You can also choose to log extended information. Extended information includes information about file identification, indexing, hashing, and rendering graphic thumbnails for each evidence item.

The time required to complete the processes depends on the size of the evidence, the processor type, and the amount of available RAM. Because of the complexity and variance of evidence items, it is not possible to predict how much time it will take to execute and perform the various processes. However, as a benchmark statistic, a Pentium 1 system running at 133 Mhz with 128 MB of RAM will take 115 minutes to process a 500 MB image. A Pentium 4 system running at 1.6 Ghz with 256 MB of RAM will take eight minutes to process the same 500 MB image.

The forensic workstation is heavily taxed while the evidence is being processed. Therefore, AccessData strongly recommends that you exit all other programs so that no other applications or processes are competing for system resources during file processing.

Backing Up the Case

You can back up your case at any time during your evidence processing. In addition, you will be asked to back up the case before exiting FTK.

To back up the case manually, click **File**, and then **Backup Case** and then select an empty directory where you want the backup to be created. Subsequent backups will be made to this directory unless another directory is specified.

Storing Your Case Files

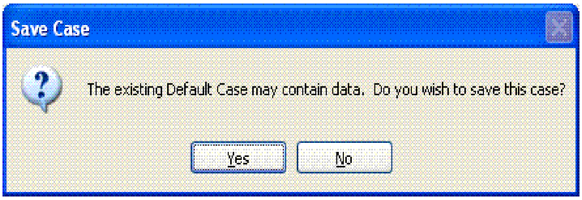
Storing your case file and evidence on the same drive substantially taxes you processors' throughput. Your system slows as it saves and reads huge files. For desktop systems in laboratories, you can increase your processors' speed by saving evidence files to a separate server.

If you are taking the case out of the lab, you may choose to compromise some processor speed for the convenience of having your evidence and case on the same drive.

Recovering Evidence from a System Failure

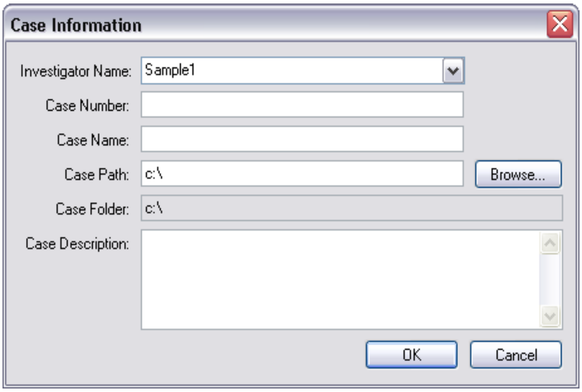
Processed data from which you gather evidence is saved in the DefaultCase folder. This folder is intended to be temporary, and will be erased each time you start an FTK session. You must save data you are processing to a named case folder to avoid being erased each time you start the program.

Do not process evidence without starting a case to which you can save it. If you have processed evidence outside of a case, and FTK closes before you save it, you will be prompted to save the evidence to a file.



The existing Default Case may contain data. Do you wish to save this case?

Click Yes to open the Case Information dialog, and name the data you want to save.



Case Information

Investigator Name: Sample1

Case Number:

Case Name:

Case Path: c:\

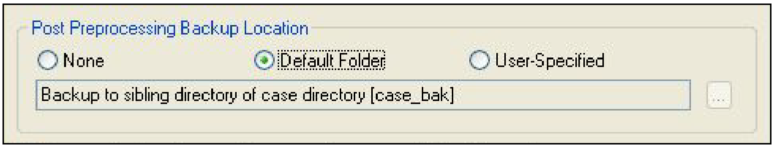
Case Folder: c:\

Case Description:

Click No to exit FTK. The data will be deleted.

Backing Up Cases Automatically

The FTK program can automatically backup a case following preprocessing. The backup is saved in a directory named after the case that's running, but with "_bak" appended to the case name. For example, if you were processing a case saved on c:\casefiles\case1\etc., your automatic backup would be created in the directory c:\casefiles\case1_bak\etc.



Post Preprocessing Backup Location

○ None ● Default Folder ○ User-Specified

Backup to sibling directory of case directory [case_bak]

The automatic backup feature creates backups for the case on which you're currently working. To speed up the copying process, the backup does not include the Thmbldx directory.

A successful backup will complete without any notice other than a log entry. If the automatic backup fails, a message box will pop up notifying you, and details of the failure will be entered in the case log.

For more information, see “Post Processing Backup Location” on page 259.

CHAPTER 5

Working with Existing Cases

In working with cases, you might need to open an existing case, add evidence, or view the file properties.

This chapter contains the following information:

- "Opening an Existing Case" on page 94
- "Adding Evidence" on page 99
- "Opening a Case in Case Agent Mode (Read-only)" on page 95
- "Viewing File Properties" on page 119
- "Setting Up Multiple Temporary Files" on page 126

Opening an Existing Case

You can open an existing case from FTK or from the command line.

To open an existing case from FTK:

1 In Forensic Toolkit (FTK), select **File**, and then **Open Case**.

Or if you have chosen to always display the FTK Startup screen, select **Open an Existing Case** and click **OK**.

2 Select the case you want to open.

Remember, all case files are named case.ftk. The case.ftk file for each case is stored in the applicable case folder.

To open an existing case from the command line, type the following command at the command line:

```
path_to_ftk_program_file\ftk.exe /OpenCase target_case_directory
```

Opening an Existing Case from a Different Location

If you have processed a case, then move the files to another location, FTK will prompt you to redirect the program to the new path.

Important: Do not add the processed evidence to FTK; the program will reprocess the data.

To open an existing case from a different location:

1 Start the FTK program, and select Open an Existing Case. The FTK program will not find the case data in the old location, and will prompt you to browse to the new location.

2 Click **OK** to browse to the new location, and then choose the case file. The FTK program will prompt you to make this new path the permanent path for this case.

3 Click **Yes**. The FTK program will automatically open the case from that location.

Opening a Case in Case Agent Mode (Read-only)

You can open a case in Read-only mode so that evidence cannot be added or deleted. This is called Case Agent Mode. When FTK is in Case Agent Mode, the following occurs:

- No evidence can be added to the case.
- No items flagged with Ignore Status are displayed, including items within bookmarks.
- The Flagged Ignore container is always empty.
- The evidence item numbers displayed in the Overview window may not reflect the available files because files flagged with an Ignore Status are not displayed.
- The Ignore Status flag cannot be removed.
- A new case cannot be created from this case.
- The live search does not show files flagged with the Ignore Status.
- Index Search results does not display hits in files flagged with the Ignore Status.

  Note: The hit count displays the total hits; however the Results window does not display hits in ignored files. Therefore the number of hits in the Results window may be different than the total number of hits reported when you enter the search term.

To open FTK in Case Agent Mode, type the following command:

***path_to_ftk_program_file*\ftk.exe /CaseAgent**

If you want to open a specific case in Case Agent Mode, type the following command:

path_to_ftk_program_file*\ftk.exe /CaseAgent /OpenCase *target_case_directory

Note: The default location for the FTK program is C:\Program Files\AccessData\AccessData Forensic Toolkit\Program\ftk.exe.

Using the Case Agent Mode Manager

Case Agent Mode Manager has been enhanced to give forensic examiners more control over the FTK features that will be available to forensic investigators for a given FTK case. This feature set is configured by the forensic examiner in the Case Mode Manager.

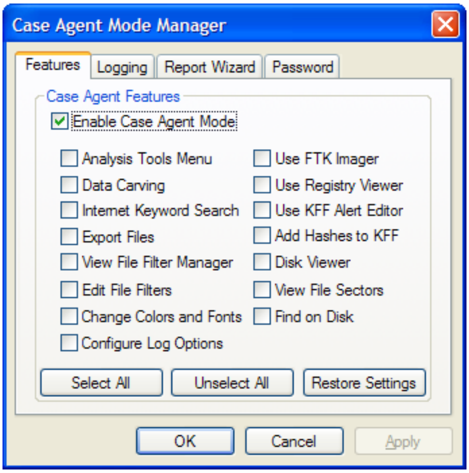
Case Agent Mode Manager has the following features:

- Password Protection: Case Agent Mode Manager is password-protected so that forensic examiners can control what FTK features forensic investigators have access to. If you administer FTK, you have the password needed to set these settings. If you are a forensic investigator using FTK, Case Agent Mode Manager has been customized for your work environment and it is unnecessary for you to access this tool.
- Reports: As the forensic examiner and FTK administrator, you can select to include the registry viewer reports, case log, all bookmarks, export all bookmarked files, exporting thumbnails of bookmarked graphics and listing certain file properties for bookmarks.
- Filters: An investigator using FTK in Case Agent Mode is not permitted to create custom filters. When an investigator creates a report or exports a report when a filter is applied, a warning will prompt him that he may be excluding important information due to the filter.
- Case Log Options: Case Agent Mode Manager allows you to determine which events are included in the case log while in Case Agent Mode. By default, Bookmarking Events, Searching Events, and Special Searches are selected.

To set Case Agent settings:

1. Start FTK in Case Agent Mode.
2. Select **Tools**, and then **Case Agent Mode Manager**.

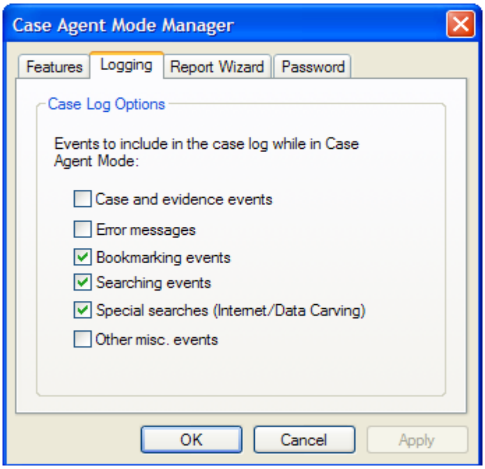
3 From the Features tab, select the FTK tools that will be available when FTK is in Case Agent Mode.



☑ Enable Case Agent Mode

□ Analysis Tools Menu
□ Data Carving
□ Internet Keyword Search
□ Export Files
□ View File Filter Manager
□ Edit File Filters
□ Change Colors and Fonts
□ Configure Log Options
□ Use FTK Imager
□ Use Registry Viewer
□ Use KFF Alert Editor
□ Add Hashes to KFF
□ Disk Viewer
□ View File Sectors
□ Find on Disk

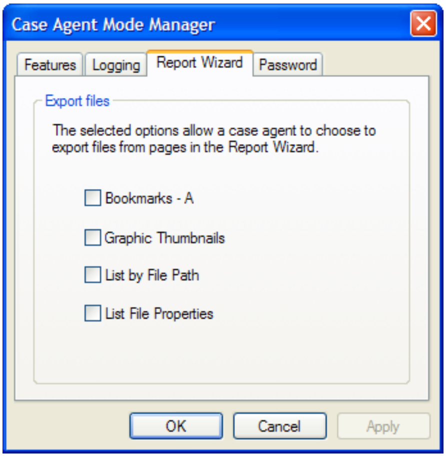
4 From the Logging tab, select the events to include in the case log when FTK is in Case Agent Mode.



Events to include in the case log while in Case Agent Mode:

□ Case and evidence events
□ Error messages
☑ Bookmarking events
☑ Searching events
☑ Special searches (Internet/Data Carving)
□ Other misc. events

5 From the Report Wizard tab, select what Report Wizard options will be available to the investigator when FTK is in Case Agent Mode.



The selected options allow a case agent to choose to export files from pages in the Report Wizard.

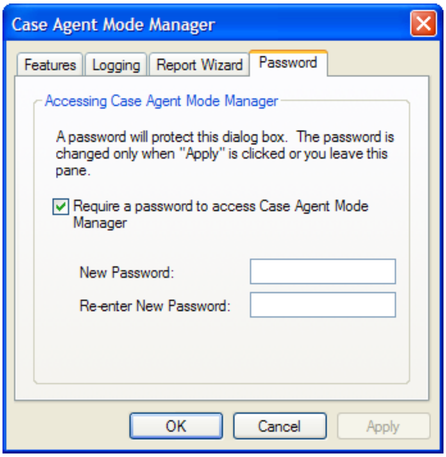
□ Bookmarks - A

□ Graphic Thumbnails

□ List by File Path

□ List File Properties

6 From the Password tab, set the password for the Case Agent Mode Manager. When you start Case Agent Mode Manager the next time, this is the password that will be used.



A password will protect this dialog box. The password is changed only when "Apply" is clicked or you leave this pane.

☑ Require a password to access Case Agent Mode Manager

New Password:

Re-enter New Password:

7 Click **Apply**.

Adding Evidence

During the case investigation, you might need to add a file, folder, drive, or image to a case. FTK uses the Add Evidence Wizard to add evidence to a case.

> **Note:** When adding large evidence images such as large email archives, you should set up the Temporary Files Manager settings before adding the large evidence images so that FTK can divide large images in to several folders to meet Microsoft folder limitations. For more information, see “Setting Up Multiple Temporary Files” on page 126.

You can add the same evidence item to multiple cases. Remember to use your organization’s policies and procedures in working with existing cases.

To add evidence to a case, you must complete the following steps. Steps 3–7 are discussed in detail in the following sections.

1 Open the case to which you want to add evidence. Click **File**, and then **Open**. Select the case.ftk file for the appropriate case.

   For more information on opening a case, see “Opening an Existing Case” on page 94.

2 Click **File**, and then **Add Evidence**. The Add Evidence Wizard opens.

3 Enter the investigator’s name.

4 Check the processes that you want run on the evidence.

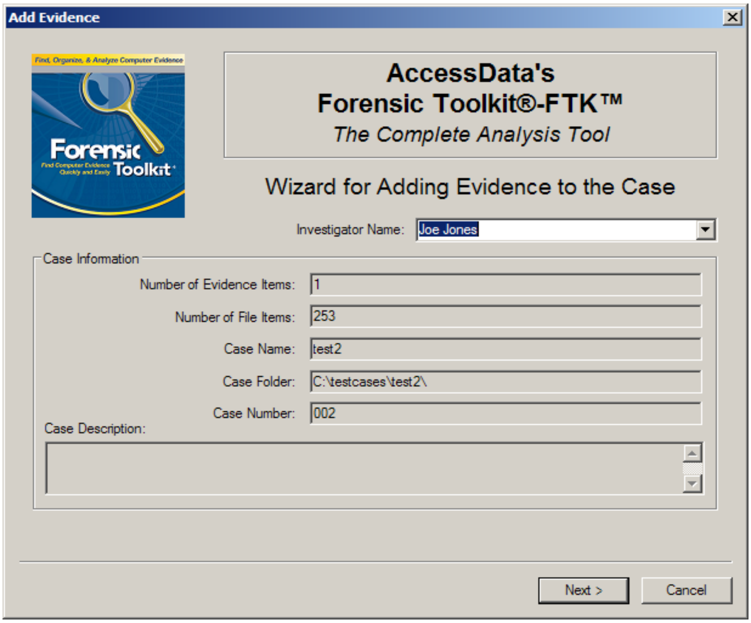
5 Add the evidence.

6 Review your evidence selections.

7 Complete the wizard to launch the processing of evidence.

Completing the Add Evidence Form

The Add Evidence form provides information about the case investigator and other case basics. The Case Information and Description fields contain the data that you entered when you created the case. The only field you can modify in this wizard is the investigator's name.



Add Evidence

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

Wizard for Adding Evidence to the Case

Investigator Name: Joe Jones

Case Information

Number of Evidence Items: 1

Number of File Items: 253

Case Name: test2

Case Folder: C:\testcases\test2\

Case Number: 002

Case Description:

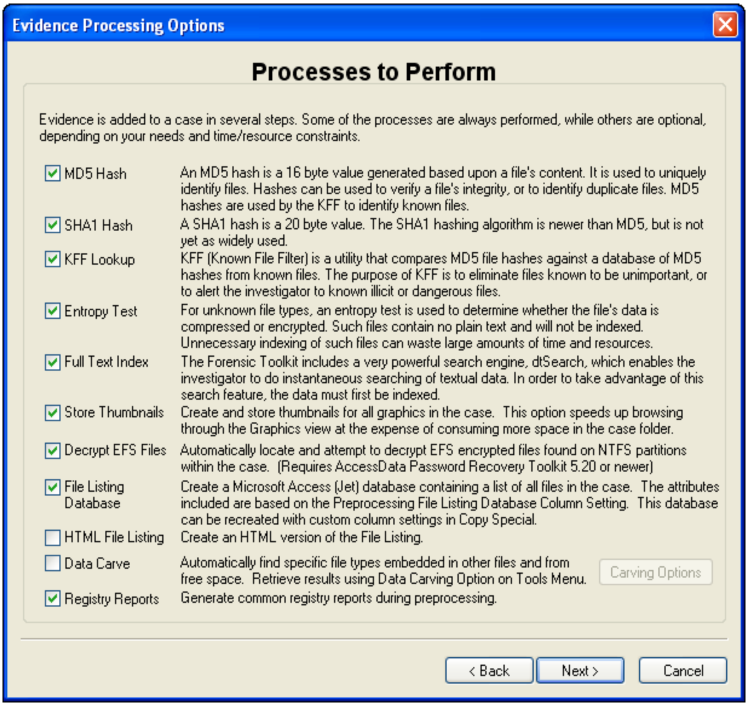
Find, Organize, & Analyze Computer Evidence
Forensic Toolkit
Find Computer Evidence Quickly and Easily
Next >
Cancel

In the **Investigator Name** field, type the name of the investigator.

The drop-down list contains the names of investigators that have been entered in prior cases. If the investigator has worked on other cases in FTK, select the name from the list.

Selecting Evidence Processes

The Evidence Processing Options form allows you to specify how you want the evidence processed. These processes can shape the scope of your analysis and the outcome of your case.



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	A SHA1 hash is a 20 byte value. The SHA1 hashing algorithm is newer than MD5, but is not yet as widely used.
☑ KFF Lookup	KFF (Known File Filter) is a utility that compares MD5 file hashes against a database of MD5 hashes from known files. The purpose of KFF is to eliminate files known to be unimportant, or to alert the investigator to known illicit or dangerous files.
☑ 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 this search feature, the data must first be indexed.
☑ 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.
☑ Registry Reports	Generate common registry reports during preprocessing.

Many factors can affect which processes you decide to select. For example, if you have specific information available, you may not need to perform a full text index. Or, if you know that compression or encryption are not used, you may not need an entropy test.

The following table outlines the Evidence Processing Options form:

Process	Description
Data Carve	Carves data immediately after pre-processing. The data carve is then accessed when the Data Carve option is selected. To select the type of file to carve, click Carving Options.
Decrypt EFS Files	Automatically locates and attempts to decrypt EFS encrypted files found on NTFS partitions within the case. Using this option requires AccessData Password Recovery Toolkit 5.20 or later to decrypt files.
Entropy Test	Determines if the data in unknown file types is compressed or encrypted. The compressed and encrypted files identified in the entropy test are not indexed.
File Listing Database	Creates a Microsoft Access database containing a list of all files in the case. The attributes included in the database are based on the Default File List Column Setting. You can recreate the database with custom column settings by selecting Copy, and then Special.
Full Text Index	Indexes all keyboard-related characters in the case evidence. This process is the most time-consuming step in adding evidence to a case. However, the index is required for data carving and Internet keyword searches. It also makes searching much more efficient. For more information about indexing, including disk space requirements, see “Conducting an Indexed Search” on page 154.
HTML File Listing	Creates an HTML version of the File Listing database.
KFF Lookup	Using a database of hashes from known files, this option eliminates ignorable files (such as known system and program files), checks for duplicate files, and alerts you to known illicit or dangerous files. For more information about KFF, see “Known File Filter” on page 9.

Process	Description
MD5 Hash	Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. For more information about MD5 hashes, see “Message Digest 5” on page 344.
Registry Reports	Generates common registry reports during preprocessing.
SHA-1 Hash	Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. This process is not checked by default. If you want FTK to create SHA-1 hashes, you must check the box. For more information about SHA-1 hashes, see “Secure Hash Algorithm” on page 344.
Store Thumbnails	Creates and stores thumbnails for all graphics in the case. This process speeds up the browsing of graphics in the Graphics window. Each thumbnail is about 4 KB per graphic file, so verify that you have space available. This process is not checked by default. If the evidence item is a graphic and you want to store its thumbnail, you must check the box.

In the Evidence Processing Options form:

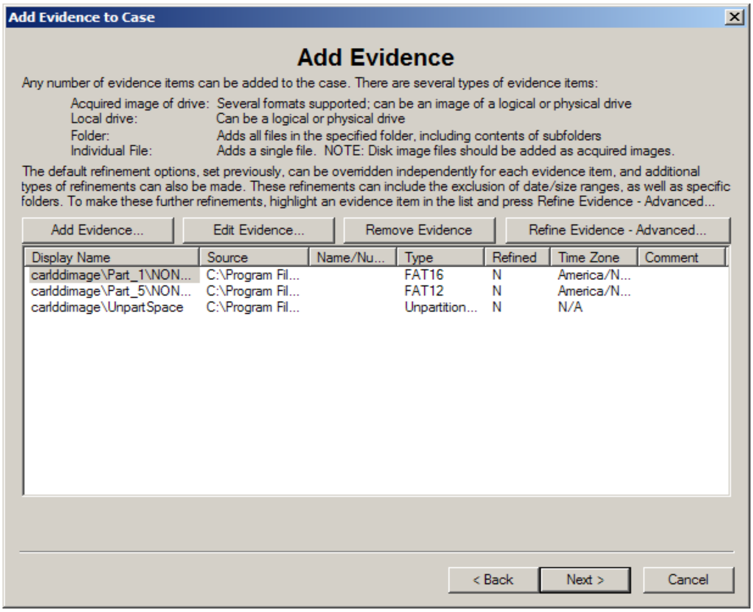
1. Select the processes that you want to be run on the evidence.
2. Click **Next**.

Managing Evidence

The Add Evidence form allows you to select the following functions:

- Add evidence.
- Remove evidence.

- Edit basic information about the evidence.
- Create parameters for adding evidence to the 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...

Display Name	Source	Name/Nu...	Type	Refined	Time Zone	Comment
carlddimage\Part_1\NON...	C:\Program Fil...		FAT16	N	America/N...	
carlddimage\Part_5\NON...	C:\Program Fil...		FAT12	N	America/N...	
carlddimage\UnpartSpace	C:\Program Fil...		Unpartition...	N	N/A	

The following sections review each function.

Adding Evidence

Evidence added during the same session of the New Case Wizard is created as part of one complete case. For example, you can add evidence from multiple floppies, a ZIP disk, and a hard drive.

Note: To protect the integrity of case evidence, all items are added as read-only.

You can add the same evidence item to multiple cases.

To add evidence to the case:

1 In the Add Evidence to Case form, click **Add Evidence**.

2 Select one of the following evidence types and click **Continue**:

Evidence Type	Description
Acquired Image of Drive	A forensic image of a logical or physical drive. If the image is segmented, select the first segment. **Important:** All the image segments must be placed in a single directory for FTK to process them properly. For a list of supported image formats, see “Supported File Systems and Image Formats” on page 13.
Contents of a Folder	A specific folder, any accompanying sub-folders, and files. The contents of a folder are always added in logical form; that is, they do not include file slack or deleted files.
Individual File	A specific file. Individual files are always added in a logical form; that is, they do not include file slack. **Note:** If you export an encrypted file for decryption, you can use this option to add the decrypted file back to the case.
Local Drive	A logical or physical drive. If you are running FTK on Windows NT, 2000, or XP, make sure that you are logged in on an account with administrative rights.

3 Browse to and select the evidence.

If you add an unidentified evidence item that is larger than 25 MB, it will be chunked into 25 MB pieces.

4 In the Evidence Information form, enter the following information and click **OK**:

Information Field	Description
Evidence Location	The same location that you selected when you added this item. If you move the item during the investigation, FTK will prompt you for the new location of the evidence when you load the case.

Information Field	Description
Evidence Display Name	The name used in FTK for the evidence item.
Evidence Identification Name/Number	The unique name or number by which this item will be known in the case.
Comment	Optional area for any additional information or clarification.
Local Evidence Time Zone	Select the time zone for the evidence item. Local Evidence Time Zone is enabled when the evidence item is on the FAT file system. NTFS images store the created, accessed, and modified times in Universal Coordinated Time (UTC) (previously known as GMT or Greenwich Mean Time).

The information and the evidence item is added to the File List. The file format and any refinements are also listed. For information about refining case evidence, see "Refining Evidence" on page 107.

Editing Case Evidence

The Edit Evidence option allows you to modify the information you entered in the Evidence Information form.

To modify the Evidence Information for a particular item:

1. Select an evidence item in the File List.
2. Click **Edit Evidence**.
3. Modify the information in the Evidence Information form.
4. Click **OK**.

Removing Case Evidence

The Remove Evidence option allows you to remove an evidence item from the File List.

Important: You can remove an item only from the File List in the Add Evidence form. You cannot remove an item after it has been processed.

To remove an evidence item from the File List, click **Remove Evidence**.

Refining Evidence

The Refine Evidence-Advanced option allows you to exclude specific data from an individual evidence item.

Note: You cannot refine evidence items once they are added to the case. This must be done while adding the item.

AccessData strongly recommends that you include all items when adding evidence to a case.

Important: After data is excluded from an evidence item, you cannot go back and add it to the case. FTK does not allow you to add the same evidence item more than once. If you discover that you need data that was previously excluded, you must create a new case. Consequently, AccessData strongly recommends that you use include all items unless you are absolutely certain that you will not need any of the excluded items.

To refine case evidence:

1. Select the evidence item in the File List.
2. Click **Refine Evidence-Advanced**.

   The Refine Case-Advanced menu is organized into three windows:

   - Refine Evidence by File Status/Type
   - Refine Evidence by File Date/Size
   - Refine Evidence by File Path
3. Click the corresponding tab to access each window.

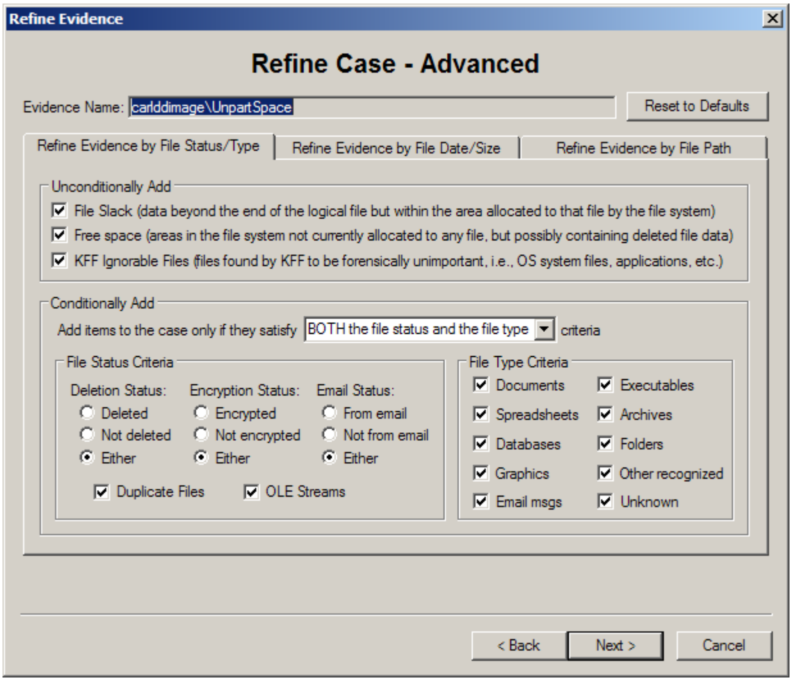
4 Define the refinements you want for the current evidence item.

If you want to reset the menu to the default settings, click **Reset to Defaults**.

5 Click **Next**.

The following sections review each window in the Refine Evidence-Advanced menu.

Refining Evidence by File Status/Type



Refine Evidence

Refine Case - Advanced

Evidence Name: carlddimage\UnpartSpace

Reset to Defaults
Refine Evidence by File Status/Type
Refine Evidence by File Date/Size
Refine Evidence by File Path

Unconditionally Add

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

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

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

Conditionally Add

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

File Status Criteria

Deletion Status: ○ Deleted ○ Not deleted ● Either

Encryption Status: ○ Encrypted ○ Not encrypted ● Either

Email Status: ○ From email ○ Not from email ● Either

☑ Duplicate Files ☑ OLE Streams

File Type Criteria

☑ Documents ☑ Executables

☑ Spreadsheets ☑ Archives

☑ Databases ☑ Folders

☑ Graphics ☑ Other recognized

☑ Email msgs ☑ Unknown

The following tables outline the options in the Refine Evidence by File Status/Type window:

Unconditionally Add Options

Option	Description
File Slack	Data beyond the end of the logical file but within the area allocated to that file by the file system.

Unconditionally Add Options

Option	Description
Free Space	Areas in the file system not currently allocated to any file but that could contain deleted file data.
KFF Ignorable Files	Files identified by the HashKeeper database as common, known files, such as program files.

File Status Criteria

Status	Description
Deletion Status	Allows you to include or exclude deleted items.
Duplicate Files	Allows you to include or exclude duplicate files.
Email Status	Allows you to include or exclude files associated with e-mail.
Encryption Status	Allows you to include or exclude encrypted or password-protected files.
OLE Streams	Allows you to include or exclude OLE elements embedded in a file.

File Type Criteria

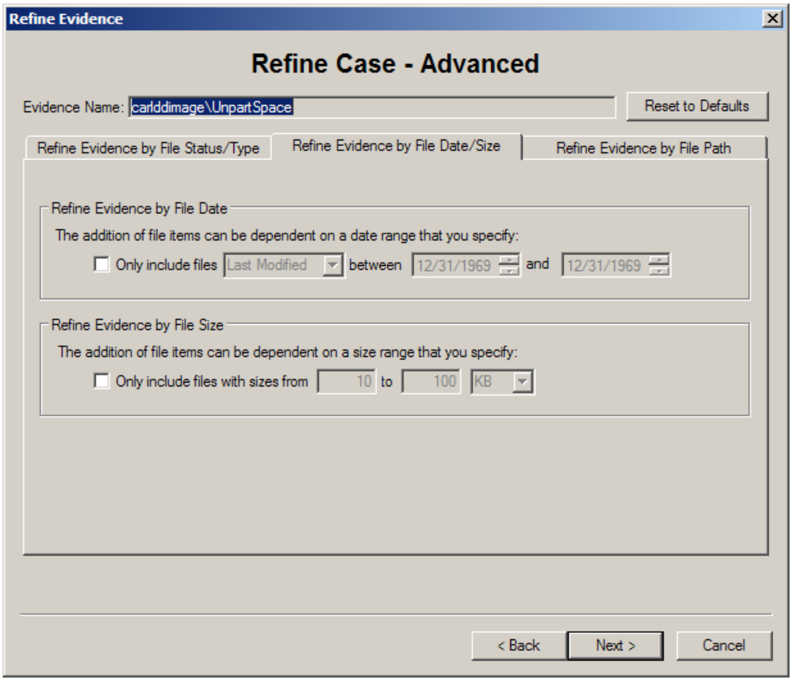
Category	Description
Archives	Archive files include e-mail archive files, Zip, Stuffit,Thumbs.db thumbnail graphics, and other archive formats. For a complete list of archive file types recognized by FTK, see “Archive File Types” on page 291.
Databases	Includes databases from Access, Quicken, Microsoft Money, QuickBooks, and others. For a complete list of database file types recognized by FTK, see “Database File Types” on page 286.
Documents	Includes most word processing, HTML, WML, HDML, or text files. For a complete list of document file types recognized by FTK, see “Document File Types” on page 282.

File Type Criteria

Category	Description
E-mail Message	Includes e-mail messages from Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail, and MSN. For a complete list of e-mail message file types recognized by FTK, see “E-mail Message Programs” on page 290.
Executables	Includes executables from Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats. For a complete list of executable file types recognized by FTK, see “Executable File Types” on page 291.
Folders	Folders and directories.
Graphics	Includes the standard graphic formats like .tif, .gif, .jpeg, and .bmp. For a complete list of graphic file types recognized by FTK, see “Graphic File Types” on page 288.
Other Recognized	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, etc. For a complete list of other file types recognized by FTK, see “Other Known File Types” on page 293.
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others. For a complete list of spreadsheet file types recognized by FTK, see “Spreadsheet File Types” on page 285.
Unknown	File types that FTK cannot identify.

Refining Evidence by File Date/Size

The following table outlines the options in the Refine Evidence by File Date/Size window:


Refine Evidence
Reset to Defaults
Refine Evidence by File Status/Type
Refine Evidence by File Date/Size
Refine Evidence by File Path
< Back
Next >
Cancel

Refine Case - Advanced

Evidence Name: carlddimage\UnpartSpace

Refine Evidence by File Date

The addition of file items can be dependent on a date range that you specify:

□ Only include files Last Modified between 12/31/1969 and 12/31/1969

Refine Evidence by File Size

The addition of file items can be dependent on a size range that you specify:

□ Only include files with sizes from 10 to 100 KB

Refine Evidence by File Date/Size

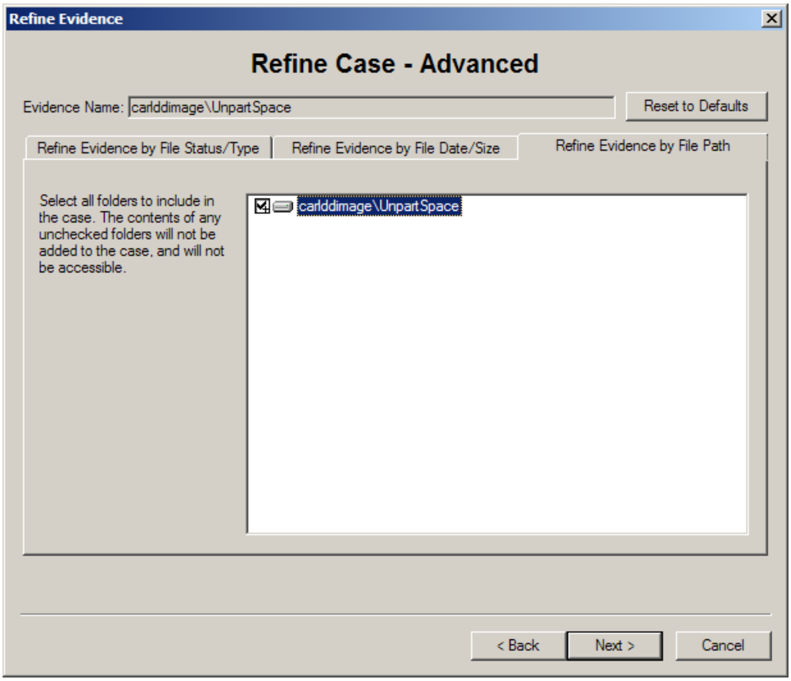
Exclusion	Description
Refine Evidence by File Date	Check to make the addition of evidence items dependent on a date range that you specify. To refine evidence by file date: 1. From the drop-down list, select **Created**, **Last Modified**, or **Last Accessed**. 2. In the two date fields, enter the beginning and ending dates that you want.

Refine Evidence by File Date/Size

Exclusion	Description
Refine Evidence by File Size	Check to make the addition of evidence items dependent on a file size that you specify. To refine evidence by file size: 1. In the two size fields, enter the minimum and maximum sizes that you want. 2. In the drop-down list, select **Bytes**, **KB**, or **MB**.

Refining Evidence by File Path

In the Refine Evidence by File Path window, mark the folders that you want to add to the case. The contents of any folders that are not marked will not be added to the case.



Refine Evidence

Refine Case - Advanced

Evidence Name: carlddimage\UnpartSpace

Select all folders to include in the case. The contents of any unchecked folders will not be added to the case, and will not be accessible.

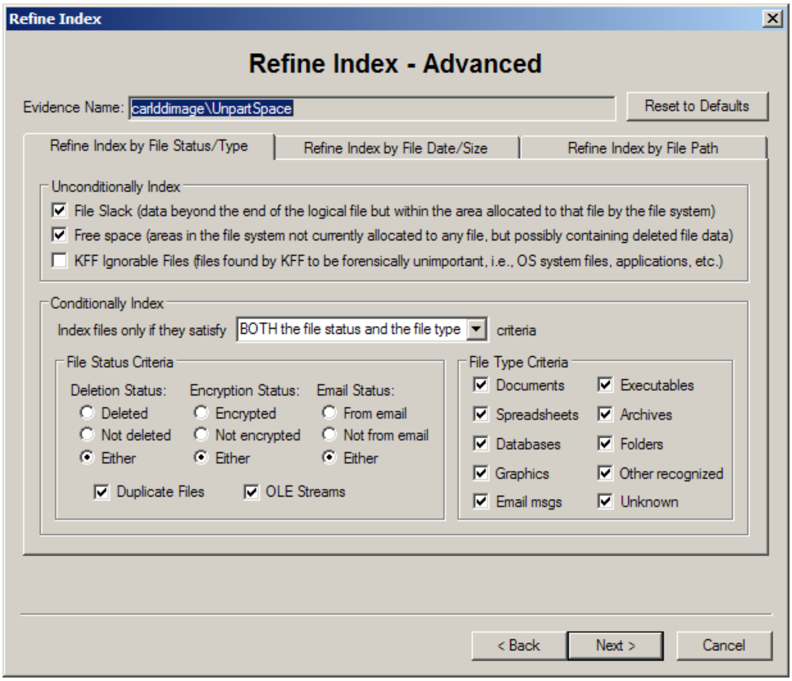
☑ carlddimage\UnpartSpace

Reset to Defaults
Refine Evidence by File Status/Type
Refine Evidence by File Date/Size
Refine Evidence by File Path
< Back
Next >
Cancel

Refining the Index

When you click **Next** in the Refine Case-Advanced form, FTK brings up the Refine Index-Advanced form.

Note: The Refine Index-Advanced form only appears when you click **Next** in the Refine Case-Advanced form. It does not appear if you simply click **Next** in the Add Evidence form.



Refine Index - Advanced

Evidence Name: carlddimage\UnpartSpace

Reset to Defaults
Refine Index by File Status/Type
Refine Index by File Date/Size
Refine Index by File Path

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, applications, etc.)

Conditionally Index

Index files only if they satisfy BOTH the file status and the file type criteria

File Status Criteria

Deletion Status:	Encryption Status:	Email Status:
○ Deleted	○ Encrypted	○ From email
○ Not deleted	○ Not encrypted	○ Not from email
● Either	● Either	● Either

☑ Duplicate Files ☑ OLE Streams

File Type Criteria

☑ Documents	☑ Executables
☑ Spreadsheets	☑ Archives
☑ Databases	☑ Folders
☑ Graphics	☑ Other recognized
☑ Email msgs	☑ Unknown

The Refine Index form allows you to specify types of data that you do not want to index. You might choose to exclude data to save time and resources and to increase searching efficiency.

Important: AccessData strongly recommends that you use the default index settings.

Indexing can be quite time-consuming. However the index is required for data carving and Internet keyword searches. It also makes searching much more efficient. Generally AccessData recommends that you accept the default index settings to create the most efficient index possible.

The index file is generated after the creation of a case; however, an evidence item can actually be indexed at any time. For more information about indexing an evidence item, see “Using Analysis Tools” on page 135.

The index file contains all discrete words or number strings found in both the allocated and unallocated space in the case evidence.

After an evidence item is indexed, it is merged into the existing index and can no longer be removed from the case. For more information about indexing, see “Conducting an Indexed Search” on page 154.

The following tables outline the options in the Refine Index form:

Unconditionally Index Options

Option	Description
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 that could contain deleted file data.
KFF Ignorable Files	Files identified by the HashKeeper database as common, known files, such as program files.

File Status Criteria

Status	Description
Deletion Status	Allows you to include or exclude deleted items.
Duplicate Files	Allows you to include or exclude duplicate files.
Email Status	Allows you to include or exclude files associated with e-mail.
Encryption Status	Allows you to include or exclude encrypted or password-protected files.
OLE Streams	Allows you to include or exclude OLE elements embedded in a file.

File Type Criteria

Category	Description
Archives	Archive files include e-mail archive files, Zip, Stuffit,Thumbs.db thumbnail graphics, and other archive formats. For a complete list of archive file types recognized by FTK, see "Archive File Types" on page 291.
Databases	Includes databases from Access, Quicken, Microsoft Money, QuickBooks, and others. For a complete list of database file types recognized by FTK, see "Database File Types" on page 286.
Documents	Includes most word processing, HTML, WML, HDML, or text files. For a complete list of document file types recognized by FTK, see "Document File Types" on page 282.
E-mail Message	Includes e-mail messages from Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail, and MSN. For a complete list of e-mail message file types recognized by FTK, see "E-mail Message Programs" on page 290.
Executables	Includes executables from Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats. For a complete list of executable file types recognized by FTK, see "Executable File Types" on page 291.
Folders	Folders and directories.
Graphics	Includes the standard graphic formats like .tif, .gif, .jpeg, and .bmp. For a complete list of graphic file types recognized by FTK, see "Graphic File Types" on page 288.
Other Recognized	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, etc. For a complete list of other file types recognized by FTK, see "Other Known File Types" on page 293.

File Type Criteria

Category	Description
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others. For a complete list of spreadsheet file types recognized by FTK, see “Spreadsheet File Types” on page 285.
Unknown	File types that FTK cannot identify.

The Refine Index form has pre-defined settings; however, you can modify the default settings by selecting different options in the Refine Index form.

In the Refine Index form:

1 To modify the default index settings, select the types of files that you want to index.

1a Select which items you want to unconditionally index.

See the "Unconditionally Index Options" table on page 114.

Important: To use the data carving feature, you must index file slack and free space. For more information, see “Data Carving” on page 181.

1b From the drop-down list, indicate whether you want to index items that satisfy BOTH the File Status and File Type criteria or items that satisfy EITHER the File Status or File Type criteria.

1c Select the File Status criteria.

See the "File Status Criteria" table on page 114.

1d Select the File Type criteria.

See the "File Type Criteria" table on page 115.

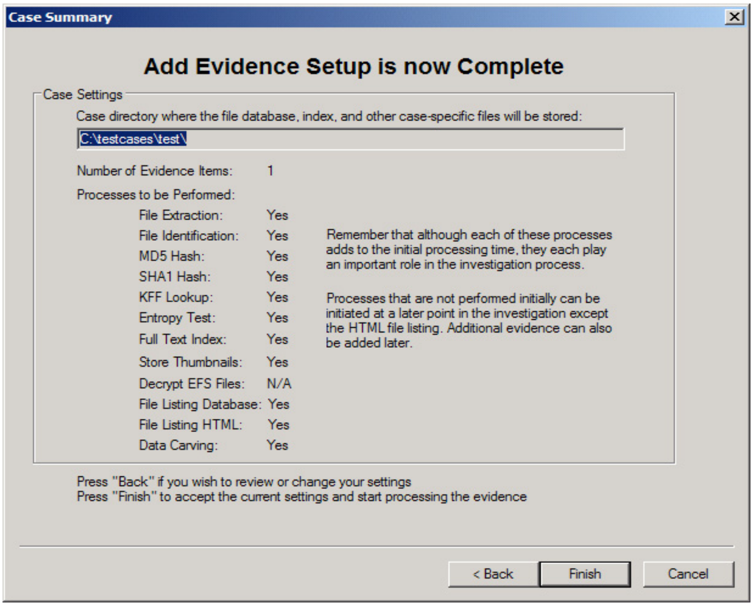
2 Click **Next**.

When you click **Next**, FTK returns you to the Add Evidence form.

3 Click **Next** in the Add Evidence form.

Reviewing Evidence Setup

The Case Summary form allows you to review the number of evidence items and evidence processes that you selected during the Add Evidence Wizard.



Add Evidence Setup is now Complete

Case Settings

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

C:\testcases\test\

Number of Evidence Items: 1

Processes to be Performed:

File Extraction:	Yes
File Identification:	Yes
MD5 Hash:	Yes
SHA1 Hash:	Yes
KFF Lookup:	Yes
Entropy Test:	Yes
Full Text Index:	Yes
Store Thumbnails:	Yes
Decrypt EFS Files:	N/A
File Listing Database:	Yes
File Listing HTML:	Yes
Data Carving:	Yes

Remember that although each of these processes adds to the initial processing time, they each play an important role in the investigation process.

Processes that are not performed initially can be initiated at a later point in the investigation except the HTML file listing. Additional evidence can also be added later.

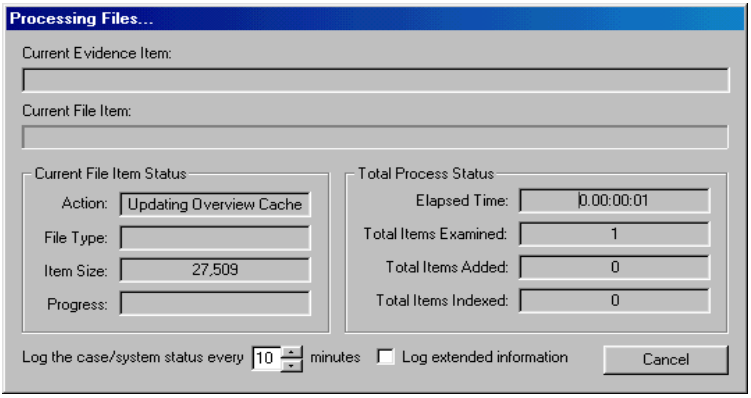
Press "Back" if you wish to review or change your settings
Press "Finish" to accept the current settings and start processing the evidence

If you want to change or review any selections, click **Back** to return to the appropriate form. After you make your changes, click **Next** to return to the Case Summary form.

To accept the current settings and start the processing of the evidence, click **Finish**.

Processing the Evidence

After you click Finish, the Processing Files form appears and displays the status of the processes you selected in the wizard.



Processing Files...

Current Evidence Item:

Current File Item:

Current File Item Status

Action:	Updating Overview Cache
File Type:	
Item Size:	27,509
Progress:	

Total Process Status

Elapsed Time:	0.00:00:01
Total Items Examined:	1
Total Items Added:	0
Total Items Indexed:	0

Log the case/system status every 10 minutes □ Log extended information

The Processing Files form allows you to select the interval for system status entries in the case log. You can also choose to log extended information. Extended information includes information about file identification, indexing, hashing, and rendering graphic thumbnails for each evidence item.

The time required to complete the processes depends on the size of the evidence, the processor type, and the amount of available RAM. Because of the complexity and variance of evidence items, it is not possible to predict how much time it will take to execute and perform the various processes. However, as a benchmark statistic, a Pentium 1 system running at 133 Mhz with 128 MB of RAM will take 115 minutes to process a 500 MB image. A Pentium 4 system running at 1.6 Ghz with 256 MB of RAM will take eight minutes to process the same 500 MB image.

The forensic workstation is heavily taxed while the evidence is being processed. Therefore, AccessData strongly recommends that you exit all other programs so that no other applications or processes are competing for system resources during file processing.

Viewing File Properties

To view a file's properties:

1 Highlight a file in the File List.

2 Select **Tools**, and then **File Properties**.

The File Properties menu is organized into five information windows:

- General
- File Source
- File Content
- Case-specific
- E-mail (appears only when viewing file properties for e-mail messages and attachments)

Click on the corresponding tab to access each window. Each window contains the following file information:

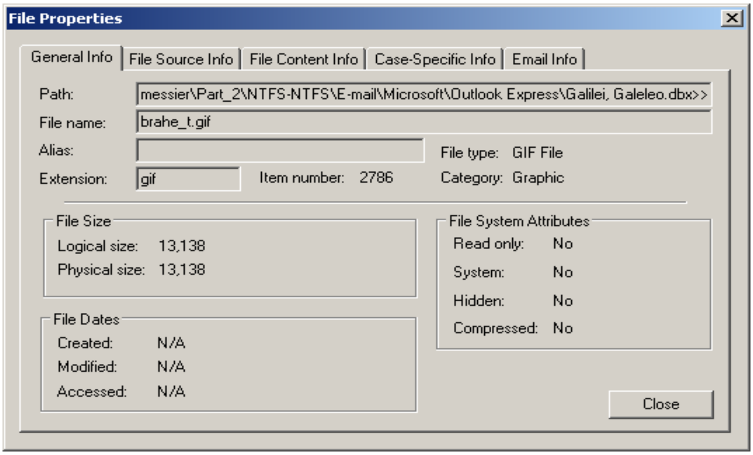
Property	Description
Alias	Typically, this field indicates the name and path of a recycled file before it was recycled. Recycled files are usually renamed to "Dc1", "Dc2", etc.
Category	The item's file type category. File type categories are Documents, Spreadsheets, Databases, Graphics, Email Message, Executables, Archives, Folders, Other Recognized, and Unknown.
Extension	The file extension.
File Type	The file type, such as an HTML file or a Microsoft Word 98 document. FTK uses the file header to identify each item's file type.
Filename	The name of the file.
Item Number	The unique number assigned to the item.

Property	Description
Path	The full file path.

The unique information in each window is discussed in the following sections.

General Info

On the General Info window, you can view the following information:



Path: messier\Part_2\NTFS-NTFS\E-mail\Microsoft\Outlook Express\Galilei, Galeleo.dbx>>
File name: brahe_t.gif
Alias:
Extension: gif
Item number: 2786
File type: GIF File
Category: Graphic

File Size
Logical size: 13,138
Physical size: 13,138

File Dates
Created: N/A
Modified: N/A
Accessed: N/A

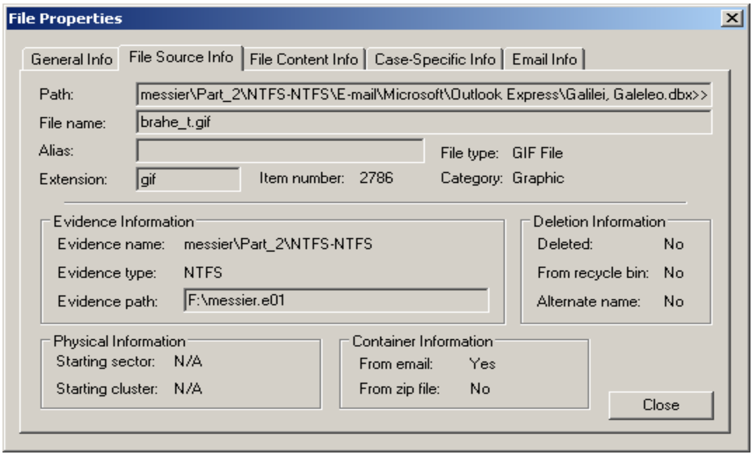
File System Attributes
Read only: No
System: No
Hidden: No
Compressed: No

Property	Description
Accessed	The date that the file was last accessed.
Compressed	Yes or No, depending on if the file is a compressed file.
Created	The date that the file was created.
Hidden	Yes or No, depending on if the file is a hidden file.
Logical Size	The logical file size. This value excludes file slack.
Modified	The date that the file was last modified.
Physical Size	The physical file size. This value includes file slack.

Property	Description
Read Only	Yes or No, depending on if the file is flagged read-only.
System	Yes or No, depending on if the file is a system file.

File Source Info

On the File Source Info window, you can view the following information:



Path: messier\Part_2\NTFS-NTFS\E-mail\Microsoft\Outlook Express\Galilei, Galeleo.dbx>>
File name: brahe_t.gif
Alias:
File type: GIF File
Extension: gif
Item number: 2786
Category: Graphic

Evidence Information
Evidence name: messier\Part_2\NTFS-NTFS
Evidence type: NTFS
Evidence path: F:\messier.e01

Deletion Information
Deleted: No
From recycle bin: No
Alternate name: No

Physical Information
Starting sector: N/A
Starting cluster: N/A

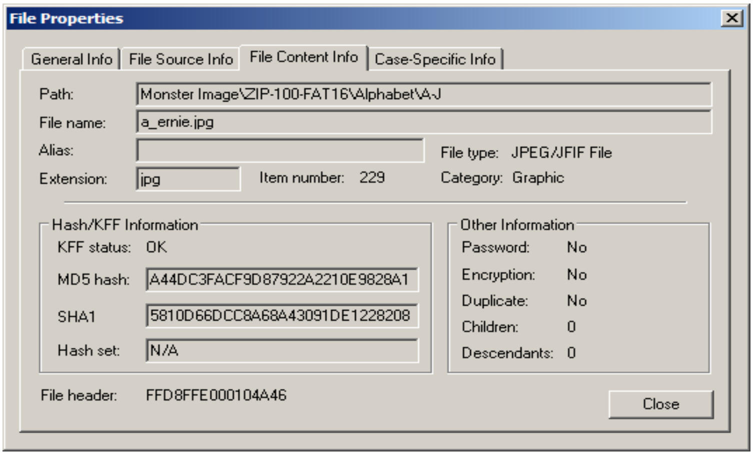
Container Information
From email: Yes
From zip file: No

Property	Description
Alternate Name	Yes or No, depending on if a copy of an existing file has been given an alternate name. Usually, the alternate name refers to the MS-DOS filename (the 8.3 name) assigned to the file.
Deleted	Yes or No, depending on if the file was deleted.
Evidence Name	Name of the evidence item that the file belongs to.
Evidence Path	The full path that FTK uses to access the evidence files.
Evidence Type	The type of evidence item the file belongs to. For an acquired image or drive, this field identifies the associated file system (for example, FAT16, FAT32, or NTFS). Otherwise, it indicates if the evidence is an individual file or the contents of a folder.

Property	Description
From E-mail	Yes or No, depending on if the item is an e-mail item such as a message, archive, or attachment.
From Recycle Bin	Yes or No, depending on if the file was recovered from the Recycle Bin.
From Zip File	Yes or No, depending on if the file is from a Zip file.
Starting Cluster	The first cluster of the file.
Starting Sector	The logical sector (relative to the partition) where the file begins.

File Content Info

On the File Content Info window, you can view the following information:



Path: Monster Image\ZIP-100-FAT16\Alphabet\A-J

File name: a_ernie.jpg

Alias:

File type: JPEG/JFIF File

Extension: jpg

Item number: 229

Category: Graphic

Hash/KFF Information

KFF status: OK

MD5 hash: A44DC3FACF9D87922A2210E9828A1

SHA1 5810D66DCC8A68A43091DE1228208

Hash set: N/A

Other Information

Password: No

Encryption: No

Duplicate: No

Children: 0

Descendants: 0

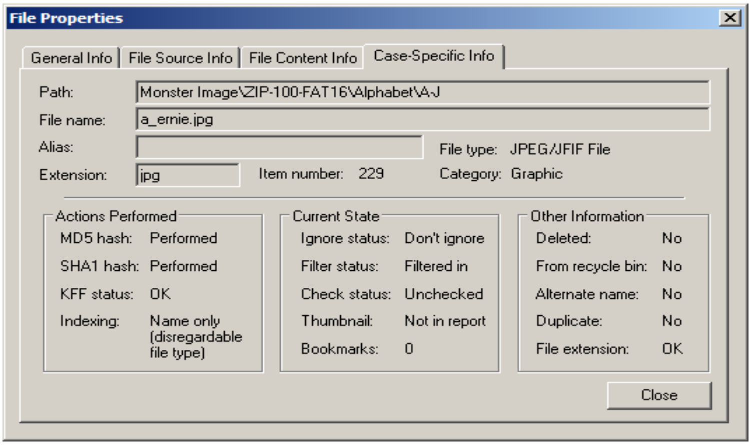
File header: FFD8FFE000104A46

Property	Description
Children	The number of files in the folder or archive.
Descendants	The number of files and descendants in the folder or archive.
Duplicate	Yes or No, depending on if another file matches the current file’s hash.
Encryption	Yes or No, depending on if the file is encrypted.

Property	Description
File Header	The first 8 bytes of the file header.
Hash Set	The name of the hash set that contains a matching hash.
KFF Status	Indicates if the file is identified by the KFF as an illicit or contraband file.
MD5 Hash	The MD5 (16 bytes) hash of the file, if performed.
Password	Yes or No, depending on if the file has a password. This includes files that have a read-only password; that is, they may be opened and viewed, but not modified by the reader.
SHA-1 Hash	The SHA-1 (20 bytes) hash of the file, if performed.

Case-Specific Info

On the Case-Specific Info window, you can view the following information:



Path: Monster Image\ZIP-100-FAT16\Alphabet\A-J

File name: a_ernie.jpg

Alias:

File type: JPEG/JFIF File

Extension: jpg

Item number: 229

Category: Graphic

Actions Performed

MD5 hash:	Performed
SHA1 hash:	Performed
KFF status:	OK
Indexing:	Name only (disregardable file type)

Current State

Ignore status:	Don't ignore
Filter status:	Filtered in
Check status:	Unchecked
Thumbnail:	Not in report
Bookmarks:	0

Other Information

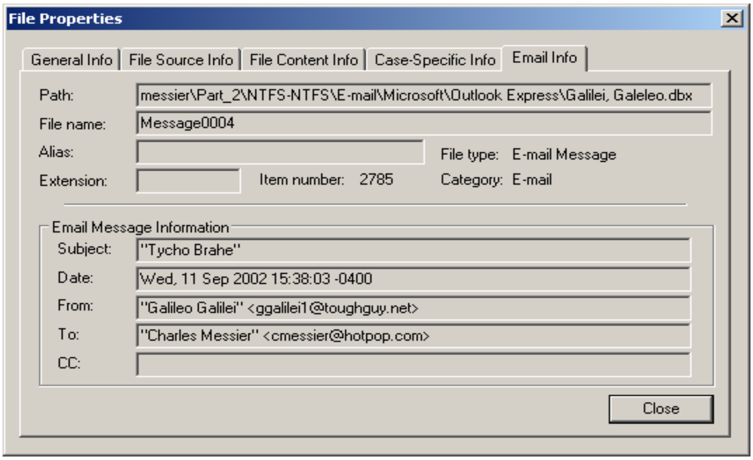
Deleted:	No
From recycle bin:	No
Alternate name:	No
Duplicate:	No
File extension:	OK

Property	Description
Alternate Name	Yes or No, depending on if a copy of an existing file has been given an alternate name. Usually, the alternate name refers to the MS-DOS filename (the 8.3 name) assigned to the file.

Property	Description
Bookmarks	Displays the number of bookmarks the item belongs to.
Check Status	Indicates if the item is currently checked in the File List.
Deleted	Yes or No, depending on if the item was deleted.
Duplicate	Yes or No, depending on if another file matches the current file's hash.
File Extension	Indicates if the file extension matches the file header.
Filter Status	Indicates if the item is currently filtered in or out.
From Recycle Bin	Yes or No, depending on if the item was recovered from the Recycle Bin.
Ignore Status	Indicates if the item is currently flagged to be ignored.
Indexing	Displays the type of indexing that was performed on the item. The available options are as follows: ◆ Full indicates that the evidence item was fully indexed. ◆ Name Only indicates that only the filename was indexed because the file type is one that FTK does not index, such as graphics. ◆ Not Yet indicates that you disabled indexing when you added the evidence item to the case.
KFF Status	Indicates if the file is identified by KFF as an illicit or contraband file.
MD5 Hash	Indicates if an MD5 hash was performed.
SHA-1 Hash	Indicates if an SHA-1 hash was performed.
Thumbnail	If the item is a graphics file, this property indicates if the item is included in the report. If the item is flagged green, the Thumbnail property reads "In Report." If the item is marked red, the Thumbnail property reads "Not in Report."

E-mail Info

The E-mail Info tab only appears in the File Properties menu if you are viewing e-mail messages or attachments.



Path: messier\Part_2\NTFS-NTFS\E-mail\Microsoft\Outlook Express\Galilei, Galeleo.dbx
File name: Message0004
Alias:
File type: E-mail Message
Extension:
Item number: 2785
Category: E-mail

Email Message Information
Subject: "Tycho Brahe"
Date: Wed, 11 Sep 2002 15:38:03 -0400
From: "Galileo Galilei" <ggalilei1@toughguy.net>
To: "Charles Messier" <cmessier@hotpop.com>
CC:

The information in the E-mail Info window varies, depending on if you are viewing an e-mail message or an attachment.

If you are viewing an e-mail message, the E-mail Info window displays the following information:

- The message subject
- The date the message was sent
- Who sent the message
- Who received the message
- The copied recipients

If you are viewing an e-mail attachment, the E-mail Info window indicates the attachment's corresponding mailbox file and message.

Setting Up Multiple Temporary Files

When FTK processes large evidence images, particularly those containing large e-mail archives, it requires significant disk space for creating and using temporary files. If the drive containing FTK's current temp folder fills to capacity while FTK is processing evidence, FTK will pause and prompt you to choose one (or more) alternate drives where temp files can be written. Temp files are deleted immediately after their use. Any stray files in the temp area are deleted when FTK is relaunched.

If you are adding large evidence to a case, you can select a location for the temp files prior to adding the large evidence files using the Temporary Files Manager.

1. Click **Tools**, and then **Preferences**.
2. In the **Temporary File Folder** area, click the **Browse** button.
3. Click the **Folder** button, and then select the folder.

   The path and folder name appear in the Temporary Files Areas In Order of Use list. Folders are used in the order listed here.
4. To change the order of use, select the folder and click the Up or Down arrows to change the order.
5. Click **OK**.

CHAPTER 6

Processing Evidence

After you add evidence to a case, you can process it by bookmarking and exporting files that are relevant to the case, verifying the image integrity, analyzing the evidence, and so forth.

This chapter contains the information that you need to process your case. It includes the following:

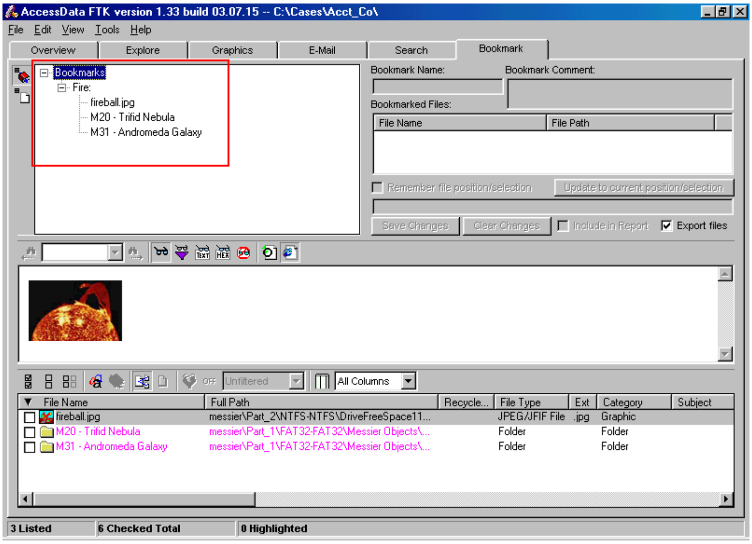
- "Using Bookmarks" on page 128
- "Creating Thumbnails" on page 131
- "Importing KFF Hashes" on page 132
- "Verifying Image Integrity" on page 133
- "Using Analysis Tools" on page 135
- "Using the Case Log" on page 137
- "Adding Entries to the Case Log" on page 140
- "Copying Information from FTK" on page 140
- "Exporting Files" on page 143
- "Exporting the Word List" on page 147

Using Bookmarks

A bookmark contains a group of files that you want to reference in your case.

Bookmarks help organize the case evidence by grouping related or similar files. For example, you can create a bookmark of graphics that contain similar images.

The Bookmark window lists all bookmarks that have been created in the current case, as shown below:



□ Remember file position/selection

□ Include in Report ☑ Export files

File Name	Full Path	Recycle...	File Type	Ext	Category	Subject
□ fireball.jpg	messier\Part_2\NTFS-NTFS\DriveFreeSpace11...		JPEG/JFIF File	.jpg	Graphic	
□ M20 - Trifid Nebula	messier\Part_1\FAT32-FAT32\Messier Objects\...		Folder		Folder	
□ M31 - Andromeda Galaxy	messier\Part_1\FAT32-FAT32\Messier Objects\...		Folder		Folder	

3 Listed | 6 Checked Total | 0 Highlighted

Creating a Bookmark

To create a bookmark:

1 Select **Tools**, and then **Create Bookmark**.

The Create New Bookmark form appears.

2 In the Bookmark Name field, enter the name of the bookmark.

3 (Optional) In the Bookmark Comment field, enter comments about the bookmark or its contents.

4 Click one of the following to specify which files to add to the bookmark:

Option	Description
All Checked Items	All items checked in all file lists. You can check files in multiple lists.
All Currently Listed Items	All items in the current file list.
All Highlighted Items	All items highlighted in the current file list. Items remain highlighted only as long as the same window is displayed.

5 If you want FTK to remember the highlighted text in the first file and automatically highlight it for you when you return to the bookmark, check **Remember File Position/Selection**. (The highlighted text will also print in the report.)

Note: This option is disabled if there is more than one file in the bookmark.

6 Check **Include in Report** to include the bookmark in the report.

7 If you choose to include the bookmark in the report, you can check **Export** to export the bookmark's files with the report.

8 Click **OK**.

Adding Files to a Bookmark

To add files to a bookmark:

1. In a file list, highlight the file that you want to add to the bookmark.

   Shift+click to select multiple contiguous files.

   Ctrl+click to select multiple discontiguous files.

2. Right-click and select **Add to Bookmark**.

   The Add Files to Bookmark form appears and displays the filename and full path of the file you selected.

3. Do one of the following:

   - To add to the last-used bookmark, go to Step 4.

     For convenience, FTK remembers the last-used bookmark. You can add several files to the bookmark without having to select the bookmark.

   - To select a different bookmark or select several bookmarks, select the bookmarks to add the file to in the Bookmark Name column.

     Shift+click to select multiple contiguous bookmarks.

     Ctrl+click to select multiple discontiguous bookmarks.

     The Bookmark Comment column displays the comments entered when the bookmark was created.

4. Click **OK**.

You can add checked files, highlighted files, and currently listed files to the last-accessed bookmark without having to select the bookmark from the Bookmark Name column. When you select additional files to add to a bookmark, FTK defaults to the last-accessed bookmark.

Removing a Bookmark

You can remove both a bookmark and individual files within bookmarks.

To remove a bookmark or an individual file:

1 In the Bookmark window, expand the bookmark list and highlight the bookmark or file that you want to remove.

2 To remove a bookmark, right-click and select **Delete Bookmark**.

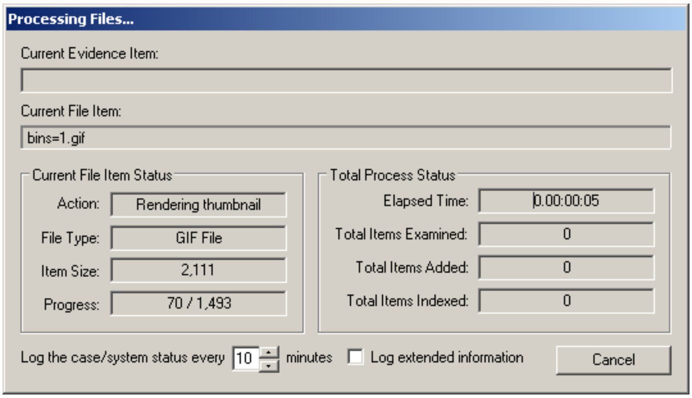
3 To remove a file, right-click and select **Remove This File From the Bookmark**.

Creating Thumbnails

If you did not check the **Store Thumbnails** box when you added graphic files to the case, thumbnails aren't created before the graphics are viewed.

Thumbnails can be created spontaneously the first time graphics are viewed, but the creation of the thumbnail slows the display of the graphic. To create the thumbnails after you have added the graphics to the case, click **Tools**, and then **Prerender Thumbnails**.

The Prerender Thumbnails Processing Files form lists each graphic as it is being processed and reflects the overall process status.



Processing Files...

Current Evidence Item:

Current File Item: bins=1.gif

Current File Item Status

Action: Rendering thumbnail

File Type: GIF File

Item Size: 2,111

Progress: 70 / 1,493

Total Process Status

Elapsed Time: 0.00:00:05

Total Items Examined: 0

Total Items Added: 0

Total Items Indexed: 0

Log the case/system status every 10 minutes

□ Log extended information

The Processing Files form also allows you to designate the interval at which you want the prerendering events logged to the case log. You can also choose to log extended information.

Note: The extended information includes information about file identification, indexing, hashing, and rendering graphic thumbnails for each evidence item.

Completing the processes may take some time, depending on the size of the evidence, the processor type, and the amount of available RAM.

Importing KFF Hashes

Using the Import KFF Hashes feature, you can import hashes from other databases or update the KFF database.

Note: The HashKeeper database is updated periodically and is available for download on the FTK update page (http://www.accessdata.com). For specific instructions on updating the KFF database, see “Upgrading a Customized KFF” on page 30.

To import hashes to the KFF database:

1. Click **Tools**, and then **Import KFF Hashes**.
2. Browse to and select one of the following file types:
   - AccessData Hash Database (.hdb)
   - FTK Imager Hash List (.csv)
   - Hashkeeper Hash Set (.hke, hke.txt)
3. Designate the hash set’s KFF Status as either Alert or Ignore.
4. When finished, click OK.

   The imported hash set is merged into the existing hash set and saved. Duplicate hashes are overwritten.

Verifying Image Integrity

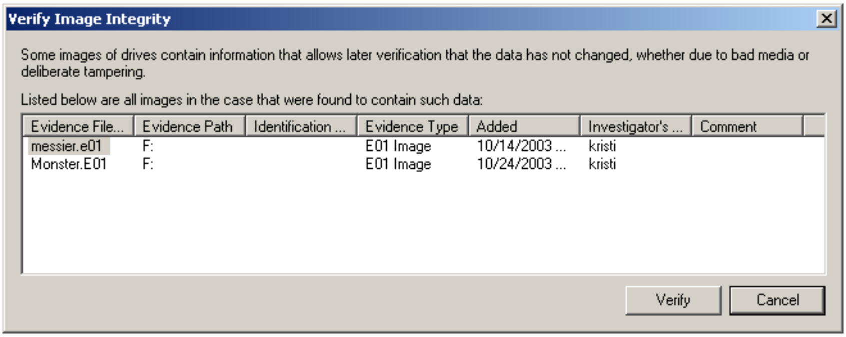
An image can be altered due to bad media or deliberate tampering. To validate the integrity of your case evidence, FTK allows you to determine if an image has changed from the original acquired image. This feature only works with images that store the hash within the image itself, such as EnCase and SMART images.

To verify an image's integrity, FTK generates an hash of the current file and compares that to the hash of the original acquired image.

To verify that an image has not changed:

1 Select **Tools**, and then **Verify Image Integrity**.

The Verify Image Integrity menu appears.



Some images of drives contain information that allows later verification that the data has not changed, whether due to bad media or deliberate tampering.

Listed below are all images in the case that were found to contain such data:

Evidence File...	Evidence Path	Identification ...	Evidence Type	Added	Investigator's ...	Comment
messier.e01	F:		E01 Image	10/14/2003 ...	kristi	
Monster.E01	F:		E01 Image	10/24/2003 ...	kristi	

The Verify Image Integrity form contains the following information:

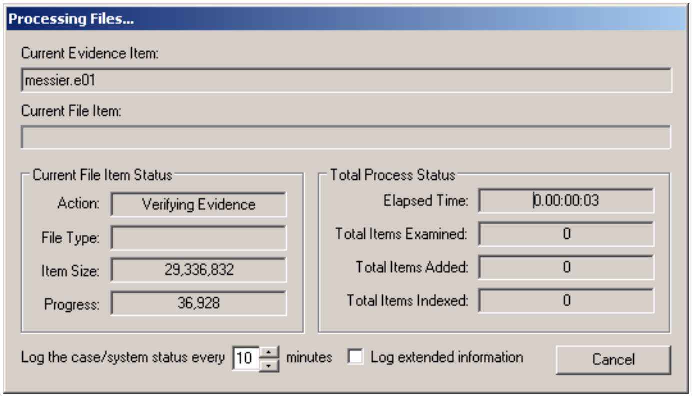
Column	Description
Added	Date when image was added to the case.
Comment	Additional information entered about the image when it was added to the case.
Evidence filename	The name of the image.

Column	Description
Evidence Path	The full path FTK uses to access the image file.
Evidence Type	The image format.
Identification	The evidence number that was entered when the image was added to the case.
Investigator's Name	The investigator assigned to the case.

2 In the **Evidence Filename** column, select the image and click **Verify**.

3 Click **Yes** to confirm.

The Processing Files form appears and displays the status of the verification.



Processing Files...

Current Evidence Item: messier.e01

Current File Item:

Current File Item Status

Action: Verifying Evidence

File Type:

Item Size: 29,336,832

Progress: 36,928

Total Process Status

Elapsed Time: 0.00:00:03

Total Items Examined: 0

Total Items Added: 0

Total Items Indexed: 0

Log the case/system status every 10 minutes □ Log extended information

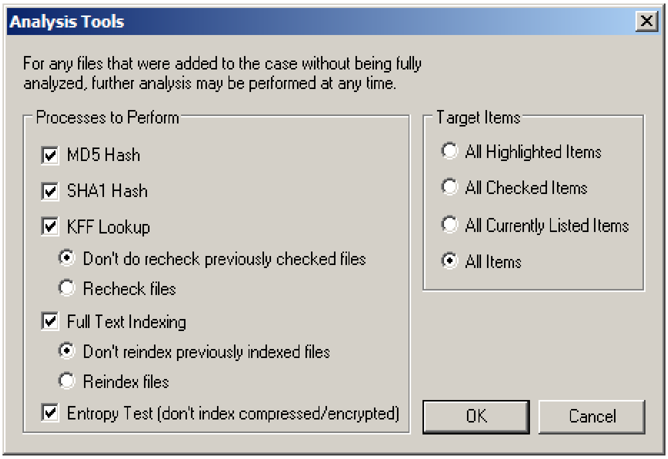
The Processing Files form reflects the overall process status. The Processing Files form also allows you to designate the interval at which you want the verification events logged to the case log. You can also choose to log extended information.

Note: The extended information includes information about file identification, indexing, and hashing.

Completing the processes may take some time, depending on the size of the evidence, the processor type, and the amount of available RAM.

Using Analysis Tools

If any evidence item is added to the case without being fully analyzed, you can run analysis processes at a later time. The Analysis Tools form allows you to generate hashes, compare hashes to the KFF database, or index files.



Analysis Tools

For any files that were added to the case without being fully analyzed, further analysis may be performed at any time.

Processes to Perform

- ☑ MD5 Hash
- ☑ SHA1 Hash
- ☑ KFF Lookup
  - ● Don't do recheck previously checked files
  - ○ Recheck files
- ☑ Full Text Indexing
  - ● Don't reindex previously indexed files
  - ○ Reindex files
- ☑ Entropy Test (don't index compressed/encrypted)

Target Items

- ○ All Highlighted Items
- ○ All Checked Items
- ○ All Currently Listed Items
- ● All Items

The following tables outline the options in the Analysis Tools menu:

Processes to Perform

Process	Description
Entropy Test	Determines if the data in unknown file types is compressed or encrypted. The compressed and encrypted files identified in the entropy test are not indexed.

Processes to Perform

Process	Description
Full Text Indexing	Indexes all keyboard-related characters in the case evidence. This process is a time-consuming step. However, the index is required for data carving and Internet keyword searches. It also makes searching much more efficient. If you do not want to re-index items that have already been indexed, select **Don’t Re-index Previously Indexed Files**. If you want to re-index all items in the case, select **Re-index Files**. For more information about indexing, including disk space requirements, see “Conducting an Indexed Search” on page 154.
KFF Lookup	Using a database of hashes from known files, this option eliminates ignorable files (such as known system or program files), checks for duplicate files, and alerts you to known illicit or dangerous files. If you do not want to recheck items that have already been checked, select **Don’t Recheck Previously Selected Files**. If you want to recheck all items in the case, select **Recheck Files**. For more information about KFF, see “Known File Filter” on page 9.
MD5 Hash	Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. For more information about MD5 hashes, see “Message Digest 5” on page 344.
SHA-1 Hash	Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. This is the only process not checked by default. If you want FTK to create SHA-1 hashes, you must check the box. For more information about SHA-1 hashes, see “Secure Hash Algorithm” on page 344.

Target Items

Items to be Analyzed	Description
All Checked Items	All items checked in all file lists. You can check files in multiple lists.
All Currently Listed Items	All items highlighted in the current file list. Items remain highlighted only as long as the same window is displayed.
All Highlighted Items	All items highlighted in the current file list. Items remain highlighted only as long as the same window is displayed.
All Items	All items checked in all file lists. You can check files in multiple lists.

To run these processes:

1. Select **Tools**, and then **Analysis Tools**.
2. Check the processes you want to perform.
3. Select the files to process.
4. Click **OK**.

The Processing Files form appears and displays the status of the processes.

Using the Case Log

The case log documents activities that occur on the case during its investigation and analysis. The case log file, ftk.log, is automatically created in the case folder when you start a new case.

The contents of the case log depends on what you checked when you used the New Case Wizard. The Case Log Options form in the New Case Wizard allows you to determine which of the following events you want to record in the case log.

Option	Description
Bookmarking Events	Events related to the addition and modification of bookmarks.
Case and Evidence Events	Events related to the addition and processing of file items when evidence is added or when using the Analysis Tools at a later time.
Data Carving/Internet Searches	Events related to data carving or Internet keyword searches performed during the case.
Error Messages	Events related to any error conditions encountered during the case.
Other Events	The following events: ◆ Using copy special feature ◆ Exporting files ◆ Viewing items in the detached viewer ◆ Ignoring and unignoring files
Searching Events	All search queries and resulting hit counts.

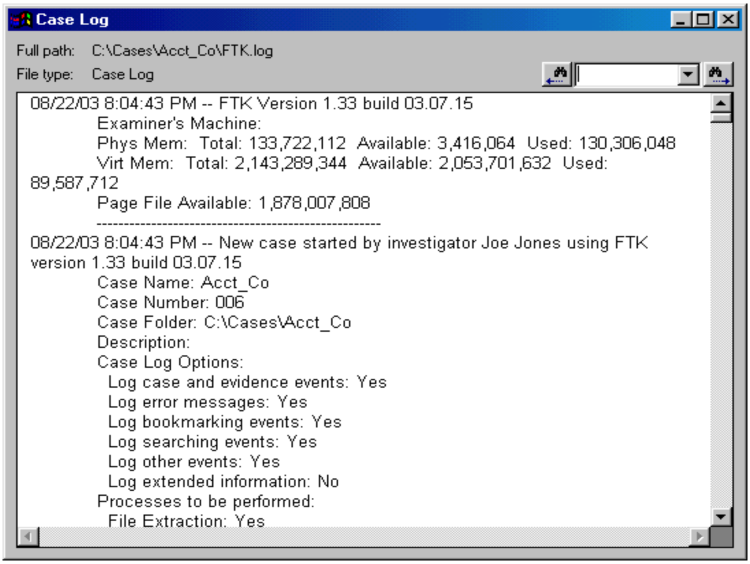
The case log also reflects the examiner's if that information is available. If no examiner's name is available, the investigator's name appears as the person who started the case.

For more information about defining which events are logged to the case log, see "Selecting Case Log Options" on page 64.

In addition to specific events, the case log can contain user entries. You can manually add information to the case log. For more information, see "Adding Entries to the Case Log" on page 140.

The case log can be used to identify what has occurred on the case and it can be included in a case report. For information on viewing the case log, see "Viewing the Case Log" on page 139. For information on including the case log in a report, see "Adding Supplementary Files and the Case Log" on page 235.

Viewing the Case Log



Full path: C:\Cases\Acct_Co\FTK.log

File type: Case Log

```
08/22/03 8:04:43 PM -- FTK Version 1.33 build 03.07.15
          Examiner's Machine:
          Phys Mem:  Total: 133,722,112  Available: 3,416,064  Used: 130,306,048
          Virt Mem:  Total: 2,143,289,344  Available: 2,053,701,632  Used:
89,587,712
          Page File Available: 1,878,007,808
          --------------------------------------------------
08/22/03 8:04:43 PM -- New case started by investigator Joe Jones using FTK
version 1.33 build 03.07.15
          Case Name: Acct_Co
          Case Number: 006
          Case Folder: C:\Cases\Acct_Co
          Description:
          Case Log Options:
            Log case and evidence events: Yes
            Log error messages: Yes
            Log bookmarking events: Yes
            Log searching events: Yes
            Log other events: Yes
            Log extended information: No
          Processes to be performed:
            File Extraction: Yes
```

To view the case log:

1 Select **Tools**, and then **View Case Log**.

2 You can search for an event using the following options:

Option	Description
▼	In the text field, enter the string that you want to search for in the case log.
🔍←	Highlights the previous instance of the search string in the case log. Searches backward in the current file.
🔍→	Highlights the next instance of the search string in the viewer. Searches forward in the current file.

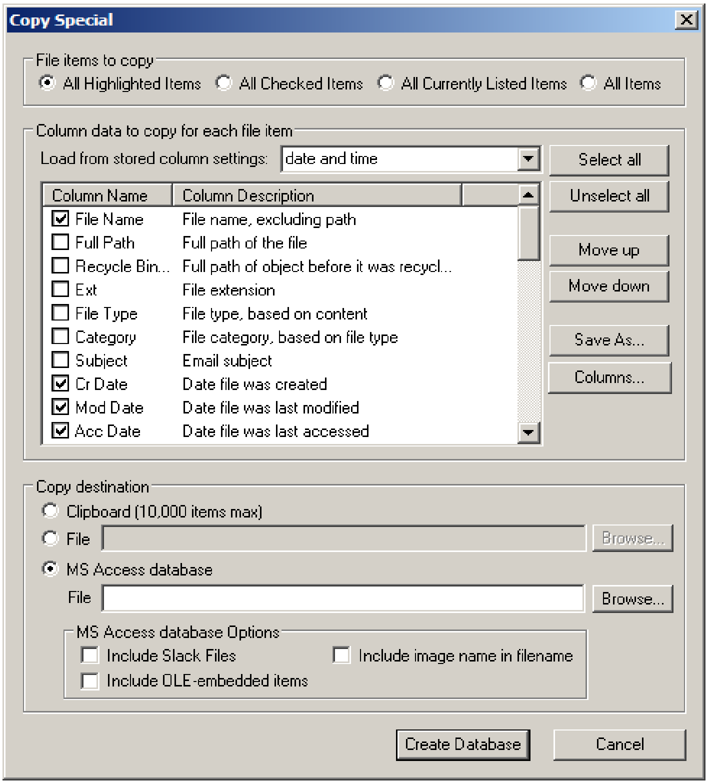
Adding Entries to the Case Log

During the case investigation and analysis, you can manually add information to the case log (ftk.log). You can add any information that you want included in the audit trail.

To add an entry to the case log:

1. Select **Tools**, and then **Add Case Log Entry**.
2. In the **Investigator's Name** field, enter the name of the investigator or select the name from the drop-down list.
3. In the Case Log Entry field, enter the information that you want to add.
4. Click **OK**.

Copying Information from FTK



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: date and time

Column Name	Column Description
☑ File Name	File name, excluding path
□ 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 modified
☑ Acc Date	Date file was last accessed

Copy destination

○ Clipboard (10,000 items max)

○ File

● MS Access database

File

MS Access database Options

□ Include Slack Files □ Include image name in filename

□ Include OLE-embedded items

The Copy Special form allows you to copy information about the files in your case. The file information can include any column item, such as filename, file path, file category and so forth. The data is copied in a tab-delimited format.

In addition, the information about the files contained in the case can be exported to an MS Access Database that lists all the files in the case. The MS Access Database export can be customized to include slack files, image names, and OLE-embedded items. MS Access Databases can be sorted in ascending or descending order by date.

Note: If you want to copy the actual items, use the Export Files feature. For more information about exporting, see "Exporting Files" on page 143.

To copy file information:

1 In the file list on any window, select the files that you want to copy information about.

2 Select **Edit**, and then **Copy Special**.

3 In the **File Items to Copy** list, select one of the following:

Item	Description
All Checked Items	All items checked in all file lists. You can check files in multiple lists.
All Currently Listed Items	All items in the current file list.
All Highlighted Items	All items highlighted in the current file list. Items remain highlighted only as long as the same window is displayed.
All Items	All items in the case.

4 In the **Load from Stored Column Settings** drop-down list, select the template that contains the file information that you want to copy.

5 If you want to define a new column settings template:

5a Check or uncheck the Column Names, depending on which ones you want to include in the setting.

You can click **Select All** or **Unselect All** to mark or unmark all the columns.

5b To change the order in which the columns appear in the File List, select a column name and click **Move Up** or **Move Down**.

5c To create a new column setting, click **Save As**, enter a name in the field, and click **OK**.

6 If you want to modify an existing template:

6a Click **Columns**.

6b Select the column setting you want to modify.

6c Modify the Column Settings form.

6d Click **Save**, and then **Close**.

For more information about the Column Settings form, see "Customizing Columns" on page 249.

7 Under **Copy Destination**, select one of the following:

Destination	Description
Clipboard	Copies the selected data to the Windows Clipboard where it can be copied to another Windows application, such as an Excel spreadsheet. The maximum number of evidence items that can be copied is 10,000.
File	Copies information to a file. The default filename is ftkfileinfo.txt. Browse to and select the location for the information file.

Destination	Description
MS Access Database	Creates an MS Access Database File based on the selected data. Browse to and select the location for the database file, then select the MS Access database Options including: ◆ Include Slack Files ◆ Include OLE-embedded items ◆ Include image name in filename

8 Do one of the following:

For Clipboard and general File copies, click **Copy**.

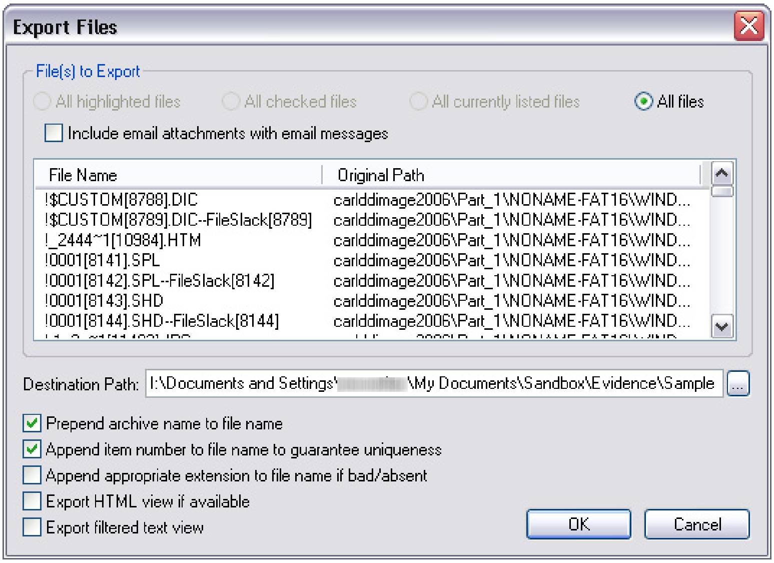
For MS Access Database copies, click **Create Database**.

Exporting Files

FTK allows you to export any evidence item. Files can be exported for additional processing or distribution to other parties. For example, encrypted files may be exported so you can decrypt them using Password Recovery Toolkit (PRTK).

Similarly, registry files may be exported so you can analyze them using the Registry Viewer. (Neither PRTK or Registry Viewer can read files within an image.)

The FTK program exports files in raw format, but includes an HTML view when it's available for that file.



Export Files

File(s) to Export

○ All highlighted files ○ All checked files ○ All currently listed files ● All files

□ Include email attachments with email messages

File Name	Original Path
!$CUSTOM[8788].DIC	carlddimage2006\Part_1\NONAME-FAT16\WIND...
!$CUSTOM[8789].DIC--FileSlack[8789]	carlddimage2006\Part_1\NONAME-FAT16\WIND...
!_2444~1[10984].HTM	carlddimage2006\Part_1\NONAME-FAT16\WIND...
!0001[8141].SPL	carlddimage2006\Part_1\NONAME-FAT16\WIND...
!0001[8142].SPL--FileSlack[8142]	carlddimage2006\Part_1\NONAME-FAT16\WIND...
!0001[8143].SHD	carlddimage2006\Part_1\NONAME-FAT16\WIND...
!0001[8144].SHD--FileSlack[8144]	carlddimage2006\Part_1\NONAME-FAT16\WIND...

Destination Path: I:\Documents and Settings\[redacted]\My Documents\Sandbox\Evidence\Sample

☑ Prepend archive name to file name
☑ Append item number to file name to guarantee uniqueness
□ Append appropriate extension to file name if bad/absent
□ Export HTML view if available
□ Export filtered text view

Note: Bookmarked files and graphics can be automatically exported with reports. For more information about exporting files with a report, see "Creating a Report" on page 222.

You can export folders while maintaining the original directory structure (Recursive File Export) or not.

To manually export files without maintaining the directory structure:

1 Select **File**, and then **Export Files**.

2 Select the files to export.

Target Item	Description
All Checked Files	All items checked in all file lists. You can check files in multiple lists.
All Currently Listed Files	All items in the current file list.

Target Item	Description
All Files	All items in the case. All files includes parsed and extracted items like the contents of a zip file, or the messages from an email archive, or OLE streams that are part of Office docs, anything that didn't have it's own entry in Windows Explorer.
All Highlighted Files	All items highlighted in the current file list. Items remain highlighted only as long as the same window is displayed.

The filenames and paths are displayed.

3 If you want to export e-mail attachments, check **Include Email Attachments With Email Messages**.

4 In the Destination Path field, browse to and select the location where you want to export the files.

The default path is the \case_folder\Report\Export\ directory.

5 If you want to add the archive name to the filename, check **Prepend Archive Name to filename**.

6 If you want to add the item number after the filename, check **Append Item Number to filename to Guarantee Uniqueness**.

7 If you want to add an appropriate extension to a file that is missing an extension or has a bad extension, check **Append Appropriate Extension to filename if Bad/Absent**.

8 To export the file in the same formatting as seen in the FTK program, check **Export HTML View if Available**. Some files may not be available in this view.

9 To export files in which readable text is filtered out of binary files, check **Export Filtered Text View**.

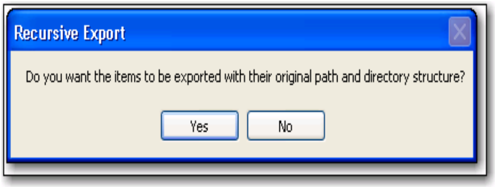
10 Click OK.

To manually export files while maintaing the directory structure:

1 Select and highlight the files to export.

2 **Right-click** the files and then select **Recursive File Export**.

3 Select the destination for these files. The Recursive Export dialog opens.



Recursive Export

Do you want the items to be exported with their original path and directory structure?

4 If you want to include the path of the exported file, click **Yes**.

The recursive path will include everything from image name down to the file or folder itself. If the path is too long, the file will still be dropped into the destination directory specified.

It will not truncate long file paths to make them fit. You will get a case log entry indicating that the file name was too long and the destination path was not created.

Recursive exported files have a Unique Item ID number appended to the filename to prevent them overwriting files with similar names.

About Recursive File Exporting

In versions of FTK before 1.80, the Recursive File Export function allows users to export a folder with all of its children and descendants. FTK 1.80 includes new functionality that allows users to also export upwardly or outwardly, rebuilding the original folder structure from the root of the image down to the selected file or folder, then exporting the descendants of the selected file or folder.

If the original path of the exported file is longer than that allowed by Windows, FTK will not be able to export it. In this case, FTK will notify the user and add an entry to the case log. This problem can often be avoided by exporting to a location near the root of the destination drive.

Exporting the Word List

If you are using PRTK, you can export the case index to use as a dictionary in the password recovery process.

To export the word list:

1 Select **Tools**, and then **Export Word List**.

2 Select the file and location that you want to write the word list to.

The default filename is *case_name*.txt.

3 To add registry files, click **Add Files** and then select the registry files to add to the word list.

This option is only available if you are using PRTK version 5.21a or later and you have Registry Viewer installed.

4 Click **Save**.

CHAPTER 7

Searching a Case

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. Forensic Toolkit (FTK) provides both live and indexed searches.

This chapter contains the information that allows you to successfully search your case evidence:

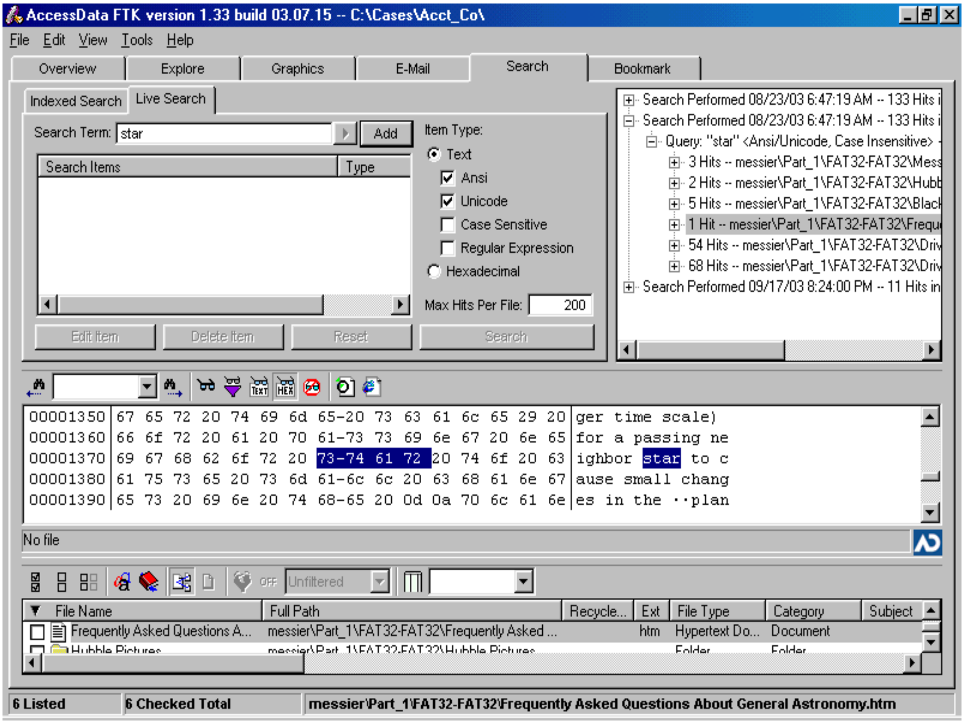
- "Conducting a Live Search" on page 149
- "Conducting an Indexed Search" on page 154
- "Documenting Your Search Results" on page 170

In addition to basic searches, you can also do several types of advanced searches. See "Advanced Searching" on page 175 and "Data Carving" on page 181 for more information.

Conducting a Live Search

The live search is a time-consuming process involving an item-by-item comparison with the search term. A live search is flexible because it can find patterns of non-alphanumeric characters.

Live search also supports regular expression searches. Regular expressions are mathematical statements that describe a data pattern such as a credit card or social security number. Regular expression searches allow you to find data items that conform to the pattern described by the expression. For more information about regular expressions and syntax, see “Regular Expression Searching” on page 295.



AccessData FTK version 1.33 build 03.07.15 -- C:\Cases\Acct_Co\

Search Term: star

Item Type:
● Text
☑ Ansi
☑ Unicode
□ Case Sensitive
□ Regular Expression
○ Hexadecimal

Max Hits Per File: 200

```
⊞ Search Performed 08/23/03 6:47:19 AM -- 133 Hits i
⊟ Search Performed 08/23/03 6:47:19 AM -- 133 Hits i
   ⊟ Query: "star" <Ansi/Unicode, Case Insensitive> -
      ⊞ 3 Hits -- messier\Part_1\FAT32-FAT32\Mess
      ⊞ 2 Hits -- messier\Part_1\FAT32-FAT32\Hubb
      ⊞ 5 Hits -- messier\Part_1\FAT32-FAT32\Black
      ⊞ 1 Hit -- messier\Part_1\FAT32-FAT32\Frequ
      ⊞ 54 Hits -- messier\Part_1\FAT32-FAT32\Driv
      ⊞ 68 Hits -- messier\Part_1\FAT32-FAT32\Driv
⊞ Search Performed 09/17/03 8:24:00 PM -- 11 Hits in
```

```
00001350 67 65 72 20 74 69 6d 65-20 73 63 61 6c 65 29 20 ger time scale)
00001360 66 6f 72 20 61 20 70 61-73 73 69 6e 67 20 6e 65 for a passing ne
00001370 69 67 68 62 6f 72 20 73-74 61 72 20 74 6f 20 63 ighbor star to c
00001380 61 75 73 65 20 73 6d 61-6c 6c 20 63 68 61 6e 67 ause small chang
00001390 65 73 20 69 6e 20 74 68-65 20 0d 0a 70 6c 61 6e es in the ··plan
```

Unfiltered

File Name	Full Path	Recycle...	Ext	File Type	Category
□ Frequently Asked Questions A...	messier\Part_1\FAT32-FAT32\Frequently Asked ...		htm	Hypertext Do...	Document
□ Hubble Pictures	messier\Part_1\FAT32-FAT32\Hubble Pictures			Folder	Folder

6 Listed | 6 Checked Total | messier\Part_1\FAT32-FAT32\Frequently Asked Questions About General Astronomy.htm

AccessData recommends live searching only if you do not have time to index the evidence.

To perform a live search:

1 In the **Search** window, click **Live Search**.

2 In the Search Term field, enter the term you want to search for.

   You can also enter a regular expression in this field if the **Regular Expression** box is checked. For more information about regular expressions and syntax, see “Regular Expression Searching” on page 295.

3 In the **Item Type** column, specify if you want FTK to search in **Text** or **Hexadecimal**.

If you select **Text**, check any of the following search criteria:

Text Search Criteria

Criteria	Description
ASCII	Searches any text in the same single-byte character set that your Windows version natively uses. For example, the English version of Windows uses the ISO 8859-1 character set; therefore, on English systems, you can find words in any ISO 8859-1 language. **Note:** For a listing of character sets used by common languages, visit http://www.w3.org/International/O-charset-lang.html.
Case Sensitive	Searches for text matching the case (uppercase or lowercase) of the search string. If unchecked, FTK ignores case when searching a term.
Regular Expression	Searches patterns in files, such as any numbers that are in a phone number pattern. If you select **Regular Expression**, the arrow next to the **Search Term** field is activated. Click the arrow and select one of the following predefined regular expressions: ◆ U.S. Phone Number ◆ U.K. Phone Number ◆ Credit Card Number ◆ Social Security Number ◆ IP Address Click **Edit Expressions** to edit the expressions in a text editor. For more information about regular expressions and syntax, see “Regular Expression Searching” on page 295.

Text Search Criteria

Unicode	Converts the ASCII/ISO 8859-1 text typed in the Search Term field to Unicode (the UCS-2 little endian form) and searches the Unicode version of the text. This search cannot be used to find Unicode text because there is no way to type Unicode text in the Search Term field. So although the Unicode search doesn't search any additional languages, it does let you find ASCII/ISO 8859-1 strings that are being stored in Unicode.

4 Click **Add** to add the search term to the Search Items column.

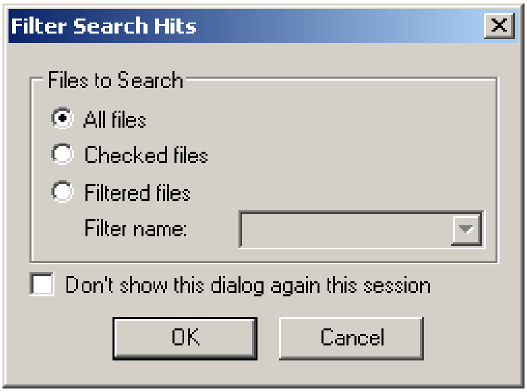
You can add as many terms as you want to the Search Items column. FTK searches for all terms listed in this column.

After a term is added to the search list, you can click **Edit Item** to modify the term or **Delete Item** to remove the term. Click **Reset** to clear the search list.

5 In the Max Hits Per File field, enter the maximum number of times you want a search hit to be listed per file. The default is 200.

6 Click **Search**.

The Filter Search Hits dialog appears.



Filter Search Hits

Files to Search

● All files

○ Checked files

○ Filtered files

Filter name:

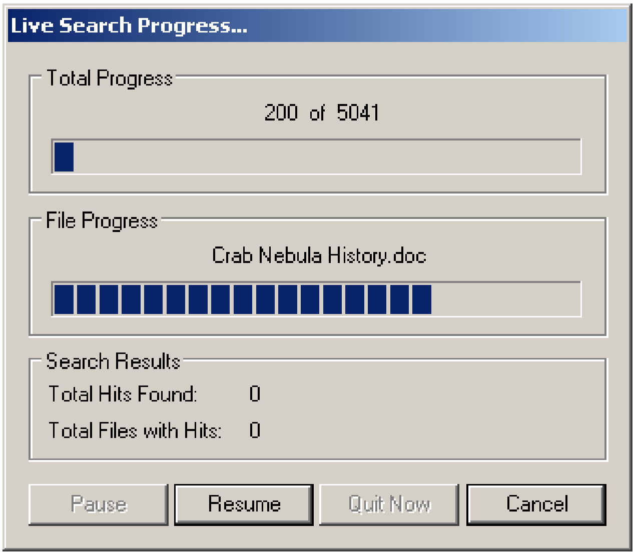
□ Don't show this dialog again this session

7 In the Filter Search Hits dialog, select one of the following:

Option	Description
All Files	Search all the files in the case. All files includes parsed and extracted items like the contents of a zip file, or the messages from an email archive, or OLE streams that are part of Office docs; anything that didn't have it's own entry in Windows Explorer.
Checked Files	Search the checked files in the Explore, Graphics, E-Mail, or Bookmark windows.
Filtered Files	Search files selected by a filter. Select the filter from the drop-down list. For information on creating a filter, see "Modifying or Creating a Filter" on page 196.

8 Click **OK**.

The Live Search Progress dialog displays the progress of the search. You can choose to pause, resume, or cancel the search.


Live Search Progress...

Total Progress

200 of 5041

File Progress

Crab Nebula History.doc

Search Results

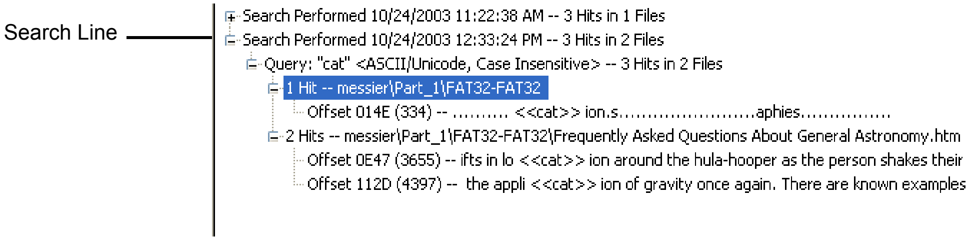
Total Hits Found: 0

Total Files with Hits: 0

9 Click **View Results** to the results.

When the search is complete, the search is added to the search results list. The results of each search appear as separate line items in the search results list.

10 Select the search results you want to in the search or file lists.



```
⊞ Search Performed 10/24/2003 11:22:38 AM -- 3 Hits in 1 Files
⊟ Search Performed 10/24/2003 12:33:24 PM -- 3 Hits in 2 Files
   ⊟ Query: "cat" <ASCII/Unicode, Case Insensitive> -- 3 Hits in 2 Files
      ⊟ 1 Hit -- messier\Part_1\FAT32-FAT32
           Offset 014E (334) -- ......... <<cat>> ion.s.......................aphies...............
      ⊟ 2 Hits -- messier\Part_1\FAT32-FAT32\Frequently Asked Questions About General Astronomy.htm
           Offset 0E47 (3655) -- ifts in lo <<cat>> ion around the hula-hooper as the person shakes their
           Offset 112D (4397) --  the appli <<cat>> ion of gravity once again. There are known examples
```

Click the plus icon (+) next to a search line to expand the search results. Individual search results are listed in the search and file lists. To view a specific item, select the file in the search results or file lists. All search results are highlighted in the file.

If this search does not display the needed information, you can conduct several types of advanced searches. See “Advanced Searching” on page 175 and “Data Carving” on page 181 for more information.

Conducting an Indexed Search

The indexed search uses the index file to find the search term. Evidence items may be indexed when they are first added to the case or at a later time. For more information about indexing an evidence item, see “Using Analysis Tools” on page 135.

The index file contains all discrete words or number strings found in both the allocated and unallocated space in the case evidence. It does not capture spaces or symbols, including the following:

. , : ; " ’ ~ ! @ # $ % ^ & = + .

Note: The at symbol (@) can be included in Internet keyword searches. For more information, see “Searching for Internet Keywords” on page 177.

FTK uses the search engine, dtSearch, to perform all indexed searches. For more information on performing searches using dtSearch, see “dtSearch Requests” on page 331. For a listing of the wildcard characters that may be used with dtSearch, see “Wildcard Characters” on page 165.

In addition to performing searches within the case, you can also use the index as a dictionary for password recovery processes in the Password Recovery Toolkit (PRTK). You can export the index by selecting **Tools**, and then **Export Word List**.

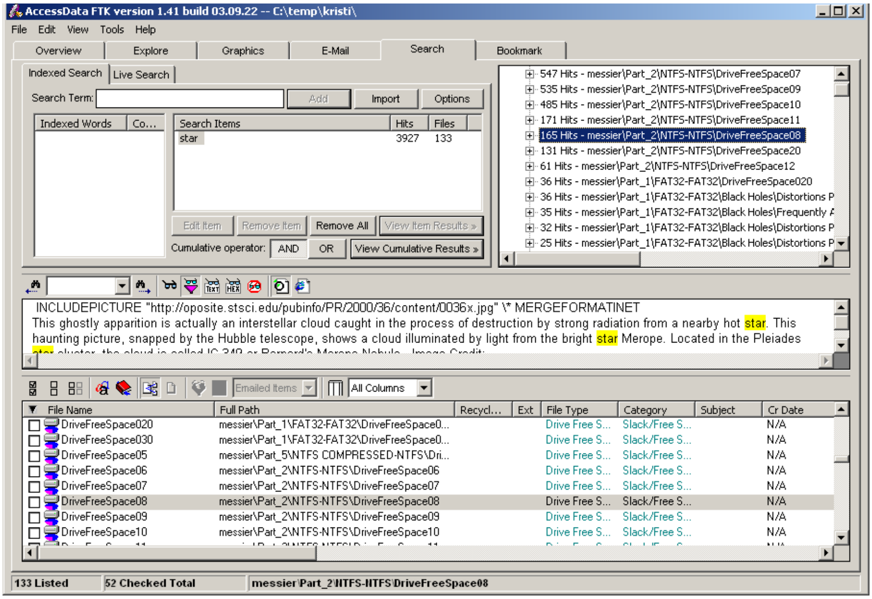
All evidence should be indexed so that the index is accurate and complete. To index evidence when it is added to the case, check the **Full Text Index** box on the Evidence Processing Options form. To index evidence after it is added to the case, select **Tools**, then **Analysis Tools**, and then **Full Text Indexing**.

To generate the index file, FTK requires free space equivalent to approximately 50% of the total size of your evidence files. After they are generated, the index files are typically 25% of the total size of your evidence files.

The following table illustrates the disk space required to index different sizes of data:

Evidence Size	Work Space	Index Size
8 GB	4 GB	2 GB
15 GB	7.5 GB	3.75 GB
30 GB	15 GB	7.5 GB
30+ GB	50% of the original	25% of the original

Single-Term Searches



Search Items	Hits	Files
star	3927	133

```
547 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace07
535 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace09
485 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace10
171 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace11
165 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace08
131 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace20
61 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace12
36 Hits - messier\Part_1\FAT32-FAT32\DriveFreeSpace020
36 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Distortions P
35 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Frequently A
32 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Distortions P
25 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Distortions P
```

INCLUDEPICTURE "http://oposite.stsci.edu/pubinfo/PR/2000/36/content/0036x.jpg" * MERGEFORMATINET
This ghostly apparition is actually an interstellar cloud caught in the process of destruction by strong radiation from a nearby hot star. This haunting picture, snapped by the Hubble telescope, shows a cloud illuminated by light from the bright star Merope. Located in the Pleiades

File Name	Full Path	Recycl...	Ext	File Type	Category	Subject	Cr Date
□ DriveFreeSpace020	messier\Part_1\FAT32-FAT32\DriveFreeSpace0...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace030	messier\Part_1\FAT32-FAT32\DriveFreeSpace0...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace05	messier\Part_5\NTFS COMPRESSED-NTFS\Dri...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace06	messier\Part_2\NTFS-NTFS\DriveFreeSpace06			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace07	messier\Part_2\NTFS-NTFS\DriveFreeSpace07			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace08	messier\Part_2\NTFS-NTFS\DriveFreeSpace08			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace09	messier\Part_2\NTFS-NTFS\DriveFreeSpace09			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace10	messier\Part_2\NTFS-NTFS\DriveFreeSpace10			Drive Free S...	Slack/Free S...		N/A

133 Listed | 52 Checked Total | messier\Part_2\NTFS-NTFS\DriveFreeSpace08

To perform a single-term indexed search:

1 In the **Search** window, click **Indexed Search**.

2 In the Search Term field, enter the term you want to search for, including any wildcard characters.

  Note: For a listing of supported wildcard characters, see “Wildcard Characters” on page 165. For more information about supported search requests, see “dtSearch Requests” on page 331.

  As you type your search term in the field, the **Indexed Words** list scrolls to match the term. The **Count** column displays the number of times each indexed word is found in the case.

3 Click **Add** to add the search term to the search list.

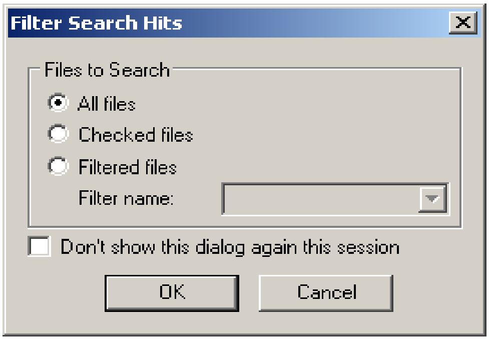
  The Search Items column displays the number of hits and the number of files that contain the search term. When a term is added to the search list, you can click **Edit Item** to modify the term or **Remove Item** to remove the term.

4 To refine the search, click **Options**.

For more information on the options in this menu, see “Indexed Search Options” on page 167.

5 In the **Search Items** column, select the index term you want to search.

6 Click **View Item Results** to initiate the search. The Filter Search Hits dialog appears.



Filter Search Hits

Files to Search

● All files

○ Checked files

○ Filtered files

Filter name:

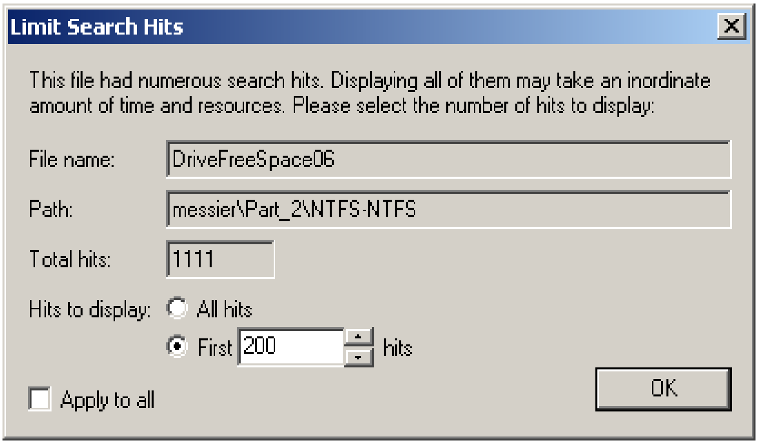
□ Don't show this dialog again this session

7 In the Filter Search Hits dialog, select one of the following:

Option	Description
All Files	Search all the files in the case. All files includes parsed and extracted items like the contents of a zip file, or the messages from an email archive, or OLE streams that are part of Office docs; anything that didn't have it's own entry in Windows Explorer.
Checked Files	Search the checked files in the Explore, Graphics, E-Mail, or Bookmark windows.
Don't show this dialog again this session	Disables the Filter Search Hits dialog for the current session. When you restart FTK or load another case, the Filter Search Hits dialog reappears. If you want the Filter Search Hits dialog to reappear in the current session, check **Show Filter Search Hits Dialog for Each Session** in the Search Options dialog. For more information, see **"Indexed Search Options" on page 167**.
Filtered Files	Search files selected by a filter. Select the filter from the drop-down list. For information on creating a filter, see "Modifying or Creating a Filter" on page 196.

8 Click **OK**.

If FTK locates more than 200 kits, the Limit Search Hits dialog appears. You can limit the number of search hits that are highlighted per file.



Limit Search Hits

This file had numerous search hits. Displaying all of them may take an inordinate amount of time and resources. Please select the number of hits to display:

File name: DriveFreeSpace06

Path: messier\Part_2\NTFS-NTFS

Total hits: 1111

Hits to display: ○ All hits

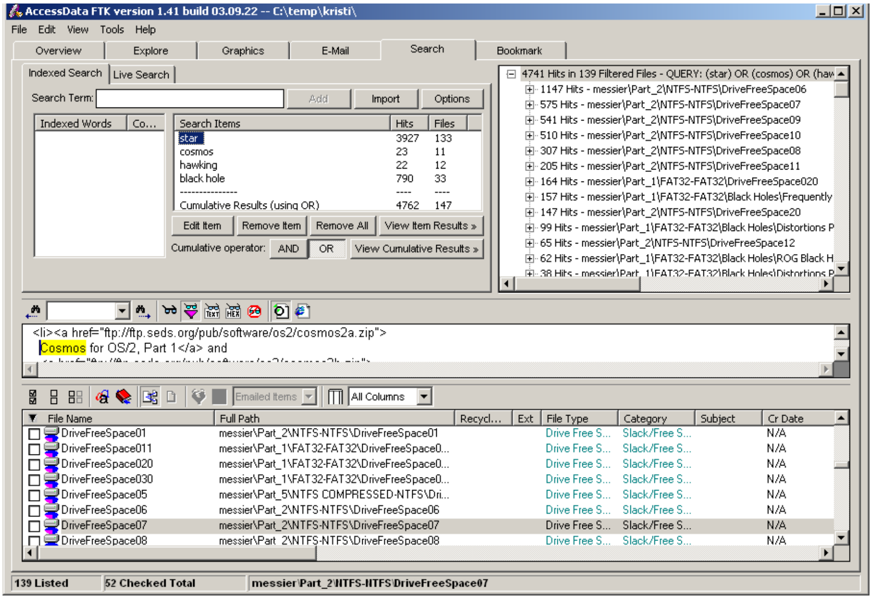
● First 200 hits

□ Apply to all

9 Select the number of search hits to display per file. Check **Apply to All** to use your settings for all files.

When the single item search is complete, the query is added to the query list. (Each query is listed separately.)

Multi-Term Searches



Search Term:

Indexed Words	Co...

Search Items	Hits	Files
star	3927	133
cosmos	23	11
hawking	22	12
black hole	790	33
---------------	----	----
Cumulative Results (using OR)	4762	147

Cumulative operator: OR

```
4741 Hits in 139 Filtered Files - QUERY: (star) OR (cosmos) OR (haw
   1147 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace06
   575 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace07
   541 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace09
   510 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace10
   307 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace08
   205 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace11
   164 Hits - messier\Part_1\FAT32-FAT32\DriveFreeSpace020
   157 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Frequently
   147 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace20
   99 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Distortions P
   65 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace12
   62 Hits - messier\Part_1\FAT32-FAT32\Black Holes\ROG Black H
   38 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Distortions P
```

```
<li><a href="ftp://ftp.seds.org/pub/software/os2/cosmos2a.zip">
 Cosmos for OS/2, Part 1</a> and
```

File Name	Full Path	Recycl...	Ext	File Type	Category	Subject	Cr Date
□ DriveFreeSpace01	messier\Part_2\NTFS-NTFS\DriveFreeSpace01			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace011	messier\Part_1\FAT32-FAT32\DriveFreeSpace0...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace020	messier\Part_1\FAT32-FAT32\DriveFreeSpace0...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace030	messier\Part_1\FAT32-FAT32\DriveFreeSpace0...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace05	messier\Part_5\NTFS COMPRESSED-NTFS\Dri...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace06	messier\Part_2\NTFS-NTFS\DriveFreeSpace06			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace07	messier\Part_2\NTFS-NTFS\DriveFreeSpace07			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace08	messier\Part_2\NTFS-NTFS\DriveFreeSpace08			Drive Free S...	Slack/Free S...		N/A

139 Listed | 52 Checked Total | messier\Part_2\NTFS-NTFS\DriveFreeSpace07

To perform a multi-term indexed search:

1 In the **Search** window, click **Indexed Search**.

2 In the Search Term field, enter a term you want to search for, including any wildcard characters.

   Note: For a listing of supported wildcard characters, see “Wildcard Characters” on page 165. For more information about supported search requests, see “dtSearch Requests” on page 331.

   As you type your search term in the field, the **Indexed Words** list scrolls to match the term. The **Count** column displays the number of times the indexed word is found in the case.

3 Click **Add** to add a search term to the search list.

   The Search Items column lists the terms you have added to the search. It also displays the number of hits and the number of files that contain each search term as well as the cumulative results for all search terms.

After a term is added to the search list, you can click **Edit Item** to modify the term or **Delete Item** to remove the term.

4 To refine the search, click **Options**.

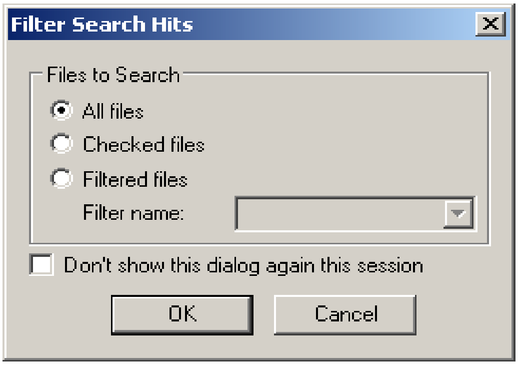
For more information on the options in this menu, see "Indexed Search Options" on page 167.

5 Define your search operators.

5a Click **And** to search for items containing all the terms.

5b Click **Or** to search for items containing any of the terms.

6 Click **View Cumulative Results** to initiate the search. The Filter Search Hits dialog appears.



Filter Search Hits

Files to Search

● All files

○ Checked files

○ Filtered files

Filter name:

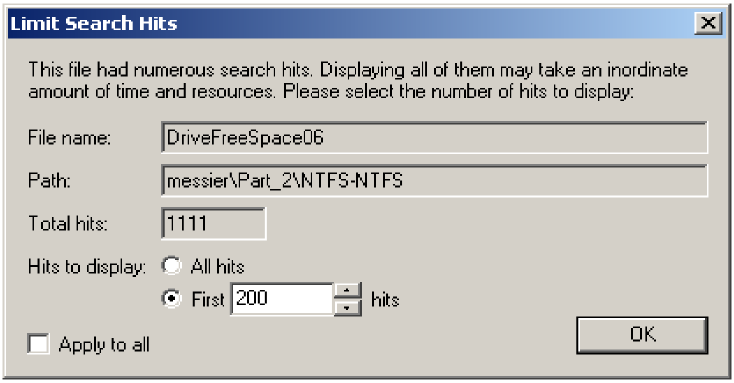
□ Don't show this dialog again this session

7 In the Filter Search Hits dialog, select one of the following:

Option	Description
All Files	Search all the files in the case. All files includes parsed and extracted items like the contents of a zip file, or the messages from an email archive, or OLE streams that are part of Office docs; anything that didn't have it's own entry in Windows Explorer.
Checked Files	Search the checked files in the Explore, Graphics, E-Mail, or Bookmark windows.
Don’t show this dialog again this session	Disables the Filter Search Hits dialog for the current session. When you restart FTK or load another case, the Filter Search Hits dialog reappears. If you want the Filter Search Hits dialog to reappear in the current session, check **Show Filter Search Hits Dialog for Each Session** in the Search Options dialog. For more information, see **“Indexed Search Options” on page 167**.
Filtered Files	Searches filtered files. Select the filter from the drop-down list. For information on creating a filter, see “Modifying or Creating a Filter” on page 196.

8 Click **OK**.

If FTK locates more than 200 kits, the Limit Search Hits dialog appears. You can limit the number of search hits that are highlighted per file.


Limit Search Hits

This file had numerous search hits. Displaying all of them may take an inordinate amount of time and resources. Please select the number of hits to display:

File name: DriveFreeSpace06

Path: messier\Part_2\NTFS-NTFS

Total hits: 1111

Hits to display: ○ All hits
● First 200 hits

□ Apply to all

9 Select the number of search hits to display per file. Check **Apply to All** to use your settings for all files.

When the cumulative search is complete, the query is added to the search results list. (Each query is listed separately.)

Importing Search Terms

In addition to individually adding index terms to the search list, you can also import search terms from text files. This is a quick and easy way to add multiple search terms to your indexed search list.

Note: Text files containing search terms must only have one search term per line.

To import search terms:

1 In the **Search** window, click **Indexed Search**.

2 Click **Import**.

3 Select the text file containing the search terms.

Important: The text file must only contain one search term per line.

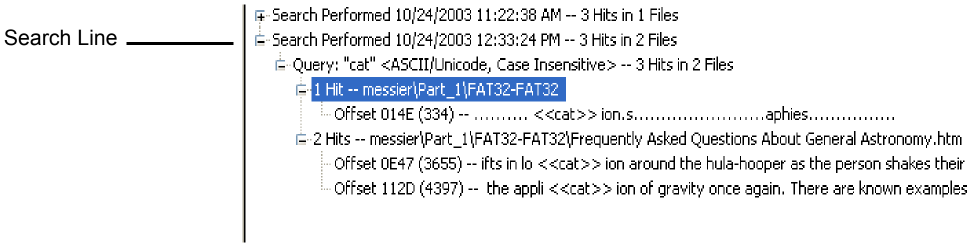
4 Select **Yes** or **No** to display terms that have zero hits.

The terms are added to the search list.

Viewing Search Results

When you complete either a single term search or a multi-term search, the results of each search appear as separate line items in the search results list.

For more information on searching, see "Single-Term Searches" on page 156 or "Multi-Term Searches" on page 160.



```
⊞ Search Performed 10/24/2003 11:22:38 AM -- 3 Hits in 1 Files
⊟ Search Performed 10/24/2003 12:33:24 PM -- 3 Hits in 2 Files
   ⊟ Query: "cat" <ASCII/Unicode, Case Insensitive> -- 3 Hits in 2 Files
      ⊟ 1 Hit -- messier\Part_1\FAT32-FAT32
         Offset 014E (334) -- .......... <<cat>> ion.s........................aphies...............
      ⊟ 2 Hits -- messier\Part_1\FAT32-FAT32\Frequently Asked Questions About General Astronomy.htm
         Offset 0E47 (3655) -- ifts in lo <<cat>> ion around the hula-hooper as the person shakes their
         Offset 112D (4397) --  the appli <<cat>> ion of gravity once again. There are known examples
```

Click the plus icon (+) next to a search line to expand the search results. Individual search results are listed in the search and file lists.

To view a specific item, select the file in the search results or file lists. All search results are highlighted in the file.

Reloading a Search Query

After you perform an indexed search, the search terms are removed from the search list. However, it is possible to reload the search terms from any query.

To reload a query:

1. Select the query in the search results list.
2. Right-click and select **Reload Search Query** from the quick menu.

   All the search terms for the selected query are added to the search list.

You can reload multiple queries at a time.

Wildcard Characters

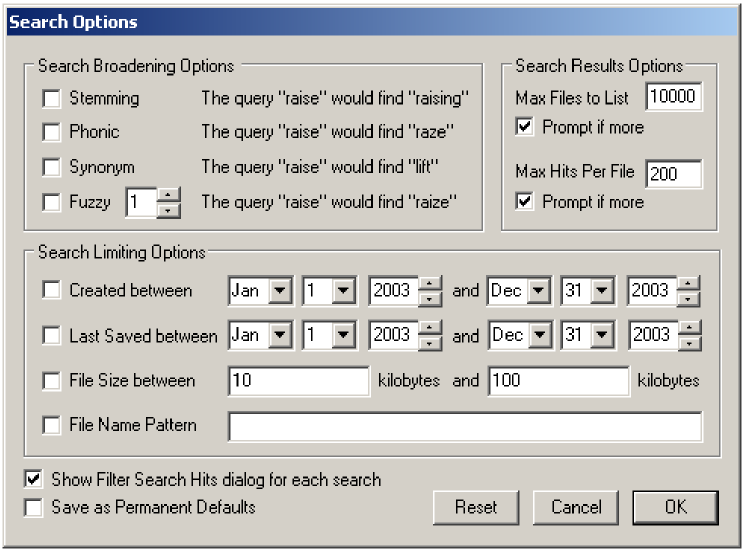
dtSearch supports the following wildcard characters for indexed searches:

Wildcard	Description
?	Matches any single character. For example, “appl?” matches “apply” or “apple.”
	Matches any number of characters. For example, “appl” matches “application.”
~	Matches words that contain the same root. This is called stemming. For example, “apply~” matches “apply”, “applies”, and “applied.” You can also select stemming by clicking Options and checking the appropriate box.
%	Matches words that have similar spellings. This is called a fuzzy search. For example, “ba%nana” matches “banana” and “bananna.” You can also select a fuzzy search by clicking Options and checking the appropriate box.
#	Matches words that sound the same. This is called a phonic search. For example, “#smith” matches “smith” and “smythe.” You can also select a phonic search by clicking Options and checking the appropriate box.
&	Matches words that have similar meaning. This is called a synonym search. For example, “fast&” matches “quick.” You can also select a synonym search by clicking Options and checking the appropriate box.
~~	Matches a numeric range. For example, “12~~24” matches “18.”

Wildcard	Description
:	Matches variable term weighting, for example, “apple:4 w/5 pear:1.” “w/5” means within five words.

Indexed Search Options

When you are conducting an indexed search, you can use the Options menu to refine the search.


Search Options

Search Broadening Options

- □ Stemming — The query "raise" would find "raising"
- □ Phonic — The query "raise" would find "raze"
- □ Synonym — The query "raise" would find "lift"
- □ Fuzzy 1 — The query "raise" would find "raize"

Search Results Options

- Max Files to List: 10000
- ☑ Prompt if more
- Max Hits Per File: 200
- ☑ Prompt if more

Search Limiting Options

- □ Created between Jan 1 2003 and Dec 31 2003
- □ Last Saved between Jan 1 2003 and Dec 31 2003
- □ File Size between 10 kilobytes and 100 kilobytes
- □ File Name Pattern

☑ Show Filter Search Hits dialog for each search

□ Save as Permanent Defaults

The following tables review the individual search options:

Search Broadening Options

Option	Description
Fuzzy	Words that have similar spellings, such as *raise* and *raize.* Click the arrows to increase or decrease the number of letters in a word that can be different from the original search term.
Phonic	Words that sound the same, such as *raise* and *raze.*
Stemming	Words that contain the same root, such as *raise* and *raising.*
Synonym	Words that have similar meanings, such as *raise* and *lift.*

Search Limiting Options

Option	Description
Created Between	Beginning and ending dates for the creation of a file. 1. Check the box. 2. In the date fields, enter the beginning and ending dates that you want to search.
File Size Between	Minimum and maximum file sizes, specified in KB. 1. Check the box. 2. In the size fields, enter the minimum and maximum size in KB of the files that you want to search.
Filename Pattern	Limits the search to files that match the filename pattern. The pattern can include “?” to match a single character or “*” to match zero or more characters. For example, if you set the filename pattern to “?b”, only files whose second letter is “b” are searched. To enter a filename pattern: 1. Check the box. 2. In the field, enter the filename pattern.
Last Saved Between	Beginning and ending dates for the last time a file was saved. 1. Check the box. 2. In the date fields, enter the beginning and ending dates that you want to search.

Search Results Options

Option	Description
Max Files To List	Maximum number of files that are listed in the results. The default is 10,000 and the maximum is 32,767. (The results are displayed in the search results list.) You can change the maximum number in the field. If you want to be prompted if there are more files than the specified maximum, check the box.
Max Hits Per File	Maximum number of hits per file. The default is 200. You can change the maximum number in the field. If you want to be prompted if there are more hits than the specified maximum, check the box.

Miscellaneous Options

Option	Description
Save as Permanent Defaults	Saves the current settings as your default search options. These options are applied to all searches.
Show Filter Search Hits Dialog for Each Search	Displays the Filter Search Hits dialog every time you perform a search. If this option is not selected, the default values are assumed for every search. This is the default option; however, if you check **Don't Show This Dialog Again This Session** in the Filter Search Hits dialog, the Filter Search hits dialog does not appear again until you select this option again. See page 158 for more information on the Filter Search Hits dialog.

When you select any options on the Search Option dialog, the Search Options button turns red to indicate that non-default options are applied. If you save these selections as the new permanent defaults, the button returns to its original color.

Documenting Your Search Results

The following sections review the ways you can document the results of your Indexed and Live searches:

- "Copying Search Results to the Clipboard" on page 170
- "Using Copy Special to Document Search Results" on page 171
- "Bookmarking Search Results" on page 172

Copying Search Results to the Clipboard

When you right-click in the search results list, the quick menu displays the following options:

- Copy to Clipboard (including all hits)
- Copy to Clipboard (visible information only)

Copy to Clipboard (including all hits) copies all the information for all the searches to the clipboard. This means that even if a search line is not expanded, the results of that search are copied to the clipboard.

Copy to Clipboard (visible information only) only copies the currently viewed information to the clipboard. This means that search results are not copied to the clipboard unless the search line is expanded.

After the information is copied to the clipboard, it can be pasted into a text editor or word processing program and saved. Then this information can be added to the case report as an supplementary file. For more information, see "Adding Supplementary Files and the Case Log" on page 235.

Using Copy Special to Document Search Results

The Copy Special feature allows you to copy specific information about files to the clipboard or a file.

To copy information about the files in your search results:

1 In the search results list, highlight the search you want to document.

2 Select **Edit**, and then **Copy Special**.

3 In the **File Items to Copy** list, select **All Highlighted Items**.

4 In the **Load from Stored Column Settings** drop-down list, select the template that contains the file information that you want to copy.

5 If you want to define a new column settings template:

5a Check or uncheck the Column Names, depending on which ones you want to include in the setting.

You can click **Select All** or **Unselect All** to mark or unmark all the columns.

5b To change the order that the columns appear in the File List, select a column name and click **Move Up** or **Move Down**.

5c To create a new column setting, click **Save As**, enter a name in the field, and click **OK**.

6 If you want to modify an existing template:

6a Click **Columns**.

6b Select the column setting you want to modify.

6c Modify the Column Settings form.

6d Click **Save**, and then **Close**.

For more information about the Column Settings form, see “Customizing Columns” on page 249.

7 Under **Copy Destination**, select one of the following:

Destination	Description
Clipboard	Copies the selected data to the Windows Clipboard where it can be copied to another Windows application, such as an Excel spreadsheet. The maximum number of evidence items that can be copied is 10,000.
File	Copies information to a file. The default filename is ftkfileinfo.txt. Browse to and select the location for the information file.
MS Access Database	Creates an MS Access Database File based on the selected data. Browse to and select the location for the database file, then select the MS Access database Options including: ◆ Include Slack Files ◆ Include OLE-embedded items ◆ Include image name in filename

8 Do one of the following:

For Clipboard and general File copies, click **Copy**. For MS Access Database copies, click **Create Database**.

Bookmarking Search Results

To keep track of the files that were returned in a particular search, you can bookmark the search results. You can create a bookmark from the search results list or the file list.

To create a bookmark from the search results list:

1 Select the search you want to bookmark.

2 Right-click and select **Bookmark Search Query Result** from the quick menu.

3 In the Create New Bookmark form, enter the following:

Interface	Description
Apply Bookmark To	Displays the filename and path of the bookmarked file.
Bookmark Comment	Information you want to document about the bookmark.
Bookmark Name	The name of the bookmark.
Export Files	If checked, the files included in the bookmark are exported when a report is generated.
Include In Report	If checked, includes the bookmark and its files in case reports.
Remember File Position/Selection	Remembers the highlighted text in the first bookmarked file, and automatically highlights it when you return to the bookmark. The highlighted text also prints in the report. This option is available only if the first file in a bookmark is selected.

4 Click **OK**.

To create a bookmark from the file list:

1 Select the files you want to include in the bookmark.

2 Click the bookmark icon or right-click and select **Create Bookmark** from the quick menu.

3 In the Create New Bookmark form, enter the following:

Interface	Description
Apply Bookmark To	Displays the filename and path of the bookmarked file.
Bookmark Comment	Information you want to document about the bookmark.
Bookmark Name	The name of the bookmark.
Export Files	If checked, the files included in the bookmark are exported when a report is generated.
Include In Report	If checked, includes the bookmark and its files in case reports.

Interface	Description
Remember File Position/Selection	Remembers the highlighted text in the bookmarked file and automatically highlights it when you return to the bookmark. The highlighted text also prints in the report. This option is available only if the first file in a bookmark is selected.

4 Click **OK**.

The bookmark now appears in the Bookmark window.

CHAPTER 8

Advanced Searching

Forensic Toolkit (FTK) includes several advanced search features, such as searching file list columns and for Internet keywords.

This chapter contains the following information about advanced searching:

- “Searching the Main Viewer” on page 176
- “Searching the File List Columns” on page 176
- “Searching for Internet Keywords” on page 177

Searching the Main Viewer

If you want to search the file currently displayed in the main viewer, you can use the following options in the viewer toolbar:

Note: These options are only available when viewing text-based items.

Option	Description
▭▾	In the text field, enter the string that you want to search for in the currently displayed item.
🔍←	Highlights the previous instance of the search string in the viewer. Searches backward in the current file. Does not search the previous file.
🔍→	Highlights the next instance of the search string in the viewer. Searches forward in the current file. Does not search the next file.

Searching the File List Columns

You can search for a term, such as a filename, in the File List. To search for a term:

1. Select **Edit**, and then **Find File in List**.
2. In the Find What field, enter the term that you want to find.
3. In the **Column** drop-down list, select the columns to search.
4. Click **Find Next**.

   The first match is highlighted in the File List.
5. Continue to click **Find Next** to locate all matches.

Searching for Internet Keywords

The Internet keyword search finds Internet keywords, such as *http*, *www*, *com*, *net*, and *org*. You can search for both URL and e-mail related strings.

Important: Evidence items must be indexed before you can perform an Internet keyword search.

The following table outlines the URL search options:

URL Option	Description
http://...	Searches for text that starts with *http://.*
www. ...	Searches for text that starts with *www.*
... .com	Searches for text that ends with .com.
... .org	Searches for text that ends with .org.
... .net	Searches for text that ends with .net.
... .[empty field]	Searches for text that ends with the domain name that you enter in the box.

The following table outlines the e-mail address search options:

E-mail Address Option	Description
...@... .com	Searches for e-mail address that ends with.com.
...@... .org	Searches for e-mail address that ends with .org.
...@... .net	Searches for e-mail address that ends with .net.
...@... .[empty field]	Searches for e-mail address that ends with the domain name that you enter in the box.

To search for Internet keywords:

1 Select **Tools**, and then **Internet Keyword Search**.

2 Select the URL-related strings you want to search.

3 Select the e-mail related strings you want to search.

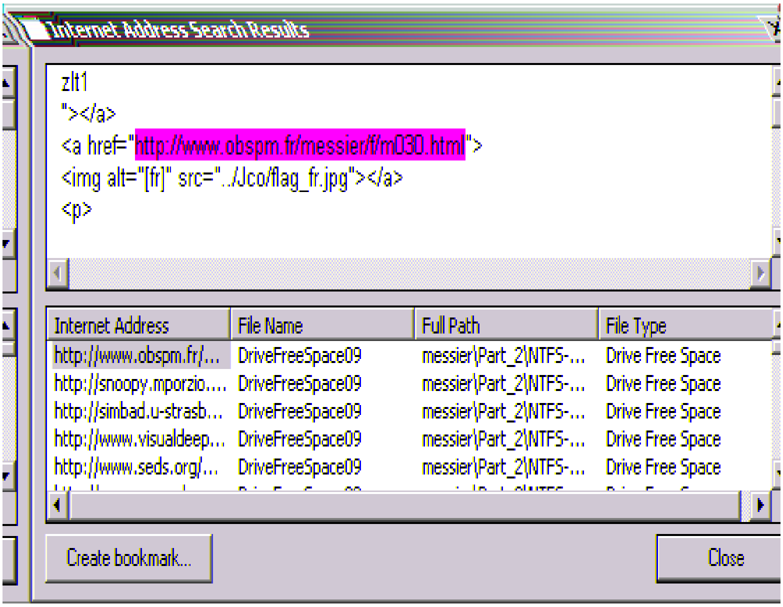
Because the index only captures discrete words, you cannot search for full e-mail addresses, such as john@abc.com. You must search for discrete components within the e-mail address.

You can check options in both the **URL** and **E-mail** columns.

4 Click **OK**.

Viewing Internet Addresses

When the process is complete, the detached viewer appears with the Internet address search results.



```
zlt1
"></a>
<a href="http://www.obspm.fr/messier/f/m030.html">
<img alt="[fr]" src="../Jco/flag_fr.jpg"></a>
<p>
```

Internet Address	File Name	Full Path	File Type
http://www.obspm.fr/...	DriveFreeSpace09	messier\Part_2\NTFS-...	Drive Free Space
http://snoopy.mporzio....	DriveFreeSpace09	messier\Part_2\NTFS-...	Drive Free Space
http://simbad.u-strasb...	DriveFreeSpace09	messier\Part_2\NTFS-...	Drive Free Space
http://www.visualdeep...	DriveFreeSpace09	messier\Part_2\NTFS-...	Drive Free Space
http://www.seds.org/...	DriveFreeSpace09	messier\Part_2\NTFS-...	Drive Free Space

The Internet Search Results window contains the following information:

Column	Description
File Type	The type of file, for example, an e-mail message or an unknown file type.
Filename	The filename. When a filename is not recoverable, the file is listed with a default name.
Full Path	The full path of the file.
Internet Address	Displays the full Internet address that contains the keyword being searched for.

To view an item, select the Internet address you want to examine. The item containing the Internet address appears in the viewer with the address highlighted.

You can save the entire list of Internet keywords or you can bookmark specific Internet addresses and save them to your case. See “Saving Internet Keyword Search Lists to the Case” on page 179 and “Bookmarking Internet Keyword Search Items” on page 180.

Saving Internet Keyword Search Lists to the Case

If you want to save an Internet Keyword Search List to the case:

1. In the Internet Search Results window, click **Add List to Evidence**.
2. Click **OK.**

The list is saved as an HTML file to the *case_name*\Attach folder. FTK names the file using the following date and time format: `Web Scan YYYYMMDD-HHMMSS.htm.`

For example, `Web Scan 20040421-205740.htm.`

The file is also added to the case and can be viewed in the Documents container in the Overview window.

Bookmarking Internet Keyword Search Items

If you want to bookmark an item containing Internet keywords:

1. Select an Internet Address.
2. Click **Create Bookmark**.
3. In the **Create New Bookmark** form, enter the following:

Interface	Description
Bookmark Name	The name of the bookmark.
Bookmark Comment	Any additional information about the bookmark and file.
Apply Bookmark To	Displays filename and path of the bookmarked file.
Remember File Position/Selection	Remembers the highlighted text in the bookmarked file and automatically highlights it when you return to the bookmark. The highlighted text also prints in the report. This option is available only if the first file in a bookmark is selected.
Include In Report	If checked, includes the bookmark and its files in case reports.
Export Files	If checked, the files included in the bookmark are exported when a report is generated.

4. Click **OK**.

CHAPTER 9

Data Carving

Data carving is the ability to locate files that have been deleted or that are embedded in other files.

This chapter contains the information that allows you to successfully locate deleted or embedded files:

- “Searching for Embedded and Deleted Files (Data Carving)” on page 182
- “Adding Carved Files to the Case” on page 186
- “Bookmarking Carved Files” on page 187

Searching for Embedded and Deleted Files (Data Carving)

Because embedded items and deleted files contain information that may be helpful in forensic investigations, Forensic Toolkit (FTK) simplifies the process of recovering these items and adding them to the case.

The data carving feature allows you to search for items, such as graphics embedded in other files. It also allows you to recover previously deleted files located in unallocated space.

To recover embedded or deleted files, FTK searches the index for specific file headers. When it finds a file header for a recognized file type, FTK carves the file's associated data. FTK can find any embedded or deleted item as long as the file header still exists.

You can data carve the following file types:

Interface	Description
AOL/AIM Buddy Lists	Searches for embedded AOL or AIM buddy lists.
BMP Files	Searches for embedded or deleted BMP files.
Enhanced WIndows Metafiles (EMF)	Searches for deleted EMF files.
GIF Files	Searches for embedded or deleted GIF files.
HTML Files	Searches for embedded HTML files.
JPEG Files	Searches for embedded or deleted JPEG files, even JPEG files embedded in other JPEG files.
OLE Archive Files (Office Documents)	Searches for any embedded Microsoft Office document, such as PowerPoint slide shows, Excel spreadsheets, and Word doc files.
PDF Files	Searches for embedded PDF files.

Data carving can be done either during evidence processing (when a new case is added) or it can be done in an existing case.

Versions of FTK before 1.80 used an index granularity of 4 characters when indexing unknown file types. FTK 1.80 can be set to use an index granularity of 3 or 2 characters for unknown file types. Lowering the index granularity will sometimes make it possible for FTK to carve more .bmp, .png, and .emf files, at the cost of increased pre-processing time. To lower the index granularity, change the value of the IndexGranularity entry in the [Global] section of the FtkSettings.0.ini file to 3 or 2.

Note: Make any change to the .ini file while FTK is closed. If FTK is open when a change is made, closing FTK will rewrite the old setting to the file and the change will not be saved.

Data Carving Files During Evidence Processing in a New Case

You can select to data carve when a case is added by selecting Data Carve in the Process to Perform Screen during the New Case Wizard. FTK carves data immediately after pre-processing. Select Carving Options and then select the file types you want to carve immediately.

Important: Full-text indexing must be enabled in order to the Data Carve option.

For more information, see “Selecting Evidence Processes” on page 65.

When you select to data carve when creating a new case, FTK creates a cache for the carved data. If data is located, the cache is saved.

To access the cache:

1. Select **Tools**, and then **Data Carving**.
2. Check the file types to carve.

   You can click **Select All** or **Select None** to speed up the selection process.
3. Click **OK**.

When the process is complete, the detached viewer appears with the data carving results. A message appears if no data was located.

Data Carving Files in an Existing Case

When FTK finds embedded or previously deleted items, it displays them in a detached viewer. You can then review the items and determine if you want to add them back into the case.

Important: Evidence items must be indexed before the data carving feature is available.

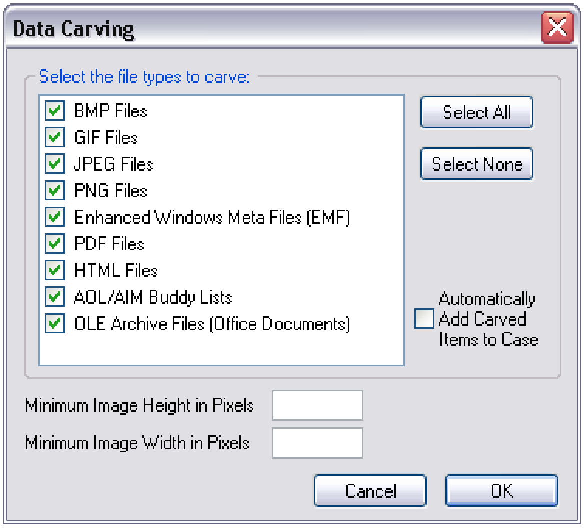
The results of the data carving search are temporarily saved in the case cache directory. Each file type has its own temporary file, such as PDF_cache.dat and JPEG_cache.dat.

To search for embedded and deleted files:

1 Select **Tools**, and then **Data Carving**.

2 Check the file types to carve.

You can click **Select All** or **Select None** to speed up the selection process.



Data Carving

Select the file types to carve:

☑ BMP Files
☑ GIF Files
☑ JPEG Files
☑ PNG Files
☑ Enhanced Windows Meta Files (EMF)
☑ PDF Files
☑ HTML Files
☑ AOL/AIM Buddy Lists
☑ OLE Archive Files (Office Documents)

☐ Automatically Add Carved Items to Case

Minimum Image Height in Pixels

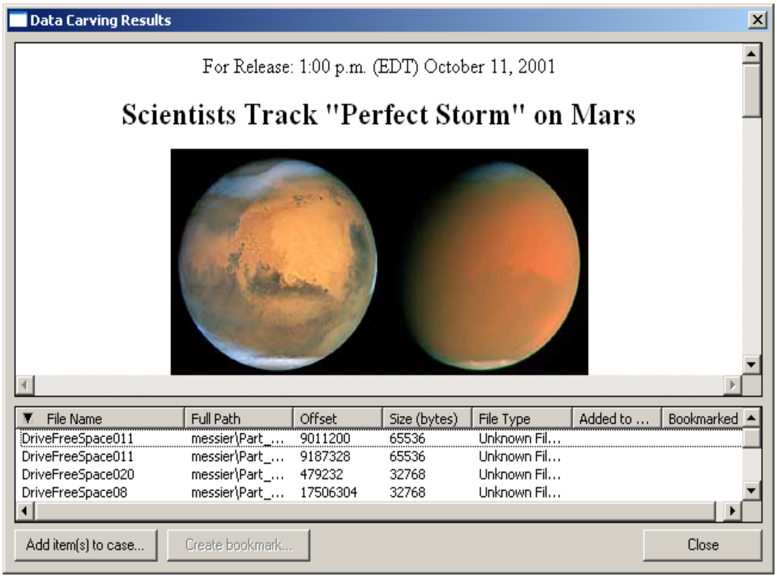
Minimum Image Width in Pixels

3 (Optional) Check the **Automatically Add Carved Items to Case** option. The the Minimum Image Size fields activate.

3a Specify a minimum size in pixels in which to display images. The program will question you about minimum sizes over 480 pixels.

4 Click **OK**.

When the process is complete, the detached viewer appears with the data carving results.



For Release: 1:00 p.m. (EDT) October 11, 2001

Scientists Track "Perfect Storm" on Mars

File Name	Full Path	Offset	Size (bytes)	File Type	Added to ...	Bookmarked
DriveFreeSpace011	messier\Part_...	9011200	65536	Unknown Fil...		
DriveFreeSpace011	messier\Part_...	9187328	65536	Unknown Fil...		
DriveFreeSpace020	messier\Part_...	479232	32768	Unknown Fil...		
DriveFreeSpace08	messier\Part_...	17506304	32768	Unknown Fil...		

The Data Carving Results window contains the following information:

Column	Description
Added to Case As	The item’s filename when it is added back to the case.
Bookmarked	Indicates if the file is bookmarked.
File Type	The file type, such as GIF or PDF.

Column	Description
Filename	The filename. When a filename cannot be recovered, FTK generates a filename based on the item's location.
Full Path	The full path of the file.
Offset	The logical position of the file in the evidence item.
Size (Bytes)	The size (in bytes) of the embedded file.

Adding Carved Files to the Case

To add a carved file to the case:

1. Select the files you want to add to the case.

   You can Shift+click to select multiple contiguous files. or Ctrl+click to select multiple discontiguous files.

2. Click **Add Items to Case**.
3. Click **Yes** to accept the default name.

   or

   Click **No**, enter a different name, and click **OK**.

After a file is added to a case, FTK will not find it in subsequent data carving procedures. In other words, there is no redundancy. If a file is identified as case evidence, the data carving feature ignores it. The data carving feature only looks for files that are not individually identified in the body of evidence.

Bookmarking Carved Files

After the files are added to the case, they are moved into their associated categories, such as documents or graphics, and are not distinguished from any other file. Therefore, if you want to track files that were retrieved using the data carving feature, you can create a bookmark.

To bookmark a carved file:

1 Select the files you want to include in the bookmark and click **Create Bookmark**.

Files must be added to the case before they can be bookmarked. See "Adding Carved Files to the Case" table on page 186.

2 In the Create New Bookmark form, enter the following:

Interface	Description
Apply Bookmark To	Displays the filename and path of the bookmarked file.
Bookmark Comment	Information you want to document about the bookmark.
Bookmark Name	The name of the bookmark.
Export Files	If checked, the files included in the bookmark are exported when a report is generated.
Include In Report	If checked, includes the bookmark and its files in case reports.
Remember File Position/Selection	Remembers the highlighted text in the bookmarked file and automatically highlights it when you return to the bookmark. The highlighted text also prints in the report. This option is available only if the file has text to select (such as an HTML file or Word), and only if the first file in a bookmark is selected.

3 Click **OK**.

CHAPTER 10

Using Filters

If you want to minimize the number of evidence items to examine, you can apply an existing filter or create a customized filter to exclude unwanted items. Forensic Toolkit (FTK) allows you to filter your case evidence by file status, type, size, and date parameters.

This chapter contains the information that allows you to successfully filter your case evidence:

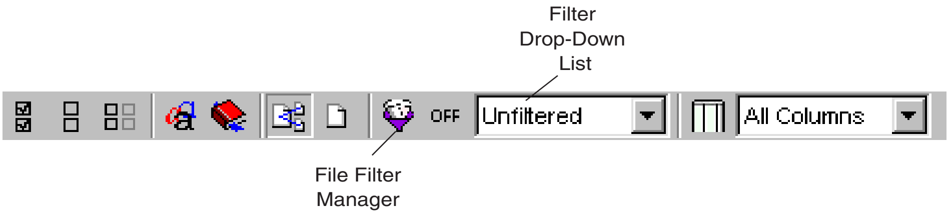
- "Applying an Existing Filter" on page 190
- "Using The File Filter Manager" on page 190
- "Modifying or Creating a Filter" on page 196
- "Deleting a Filter" on page 197

Applying an Existing Filter

FTK contains the following predefined filters:

Filter	Description
E-mailed Items	Shows e-mail items such as e-mail messages, archive files, and attachments.
Encrypted Files	Shows encrypted files that are possibly in all file types.
Graphic Files	Only shows graphic files.
KFF Alert Files	Shows KFF alert files that are possibly in all file types.
No Deleted	Hides deleted items.
No Duplicates	Hides duplicate items.
No Ignorable	Hides duplicate items, KFF ignorable files, and files that were flagged ignorable.
No OLE	Hides items or pieces of information that were embedded in a file, such as text, graphics, or an entire file.
Unfiltered	Displays all items in the case.

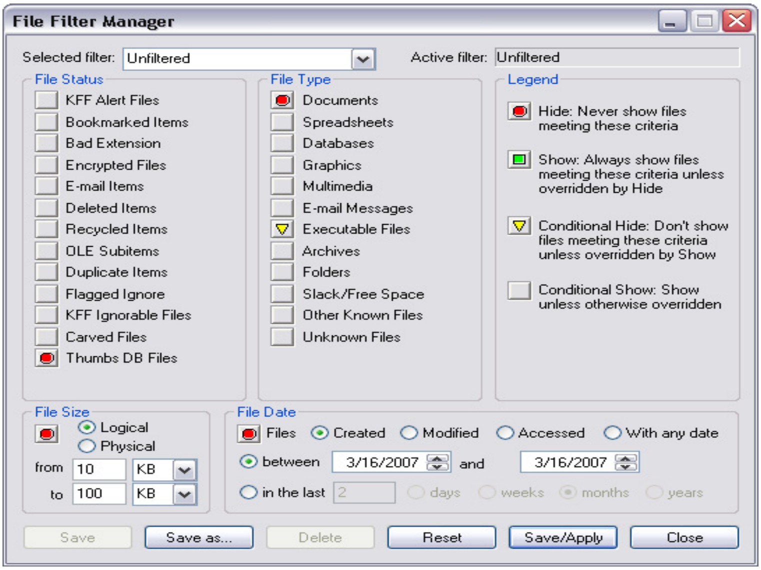
To apply an existing filter, use the Filter drop-down list on the File List toolbar, shown below:



Using The File Filter Manager

The File Filter Manager allows you to create or modify file filters. To access this menu, select **View**, and then **File Filter**

Manager or click the File Filter Manager icon on the File List toolbar.



File Filter Manager

Selected filter: Unfiltered

Active filter: Unfiltered

File Status
- □ KFF Alert Files
- □ Bookmarked Items
- □ Bad Extension
- □ Encrypted Files
- □ E-mail Items
- □ Deleted Items
- □ Recycled Items
- □ OLE Subitems
- □ Duplicate Items
- □ Flagged Ignore
- □ KFF Ignorable Files
- □ Carved Files
- 🟥 Thumbs DB Files

File Type
- 🟥 Documents
- □ Spreadsheets
- □ Databases
- □ Graphics
- □ Multimedia
- □ E-mail Messages
- ▽ Executable Files
- □ Archives
- □ Folders
- □ Slack/Free Space
- □ Other Known Files
- □ Unknown Files

Legend
- 🟥 Hide: Never show files meeting these criteria
- 🟩 Show: Always show files meeting these criteria unless overridden by Hide
- ▽ Conditional Hide: Don't show files meeting these criteria unless overridden by Show
- □ Conditional Show: Show unless otherwise overridden

File Size
- 🟥 ● Logical ○ Physical
- from 10 KB
- to 100 KB

File Date
- 🟥 Files ● Created ○ Modified ○ Accessed ○ With any date
- ● between 3/16/2007 and 3/16/2007
- ○ in the last 2 ○ days ○ weeks ● months ○ years

The following sections review the categories in the File Filter Manager menu:

- "Legend" on page 192
- "File Status" on page 192
- "File Type" on page 193
- "File Size" on page 195
- "File Date" on page 195

Legend

The Legend identifies the individual filter settings that can be selected for each item. Click an item in the Legend to apply the setting to all items in the File Status and File Type columns.

The following table reviews the available filter settings:

Icon	Description
🔴	Hide: Never shows files meeting selected criteria. If you click this icon in the Legend column, all file statuses and types are marked Hide.
🟩	Show: Always shows files meeting selected criteria unless overridden by Hide. If you click this icon in the Legend column, all file statuses and types are marked Show.
▽	Conditional Hide: Doesn’t show files meeting selected criteria unless overridden by Show. If you click this icon in the Legend column, all file statuses and types are marked Conditional Hide.
□	Conditional Show: Shows selected criteria unless otherwise overridden. If you click this icon in the Legend column, all file statuses and types are marked Conditional Show.

File Status

The following table outlines the file status categories you can use to filter items in FTK.

Item buttons toggle between filter settings; simply click an item button multiple times to rotate through the filter settings.

Category	Description
Bad Extension	Files with an extension that does not match the file type identified in the file header, for example, a GIF image renamed as graphic.txt.

Category	Description
Bookmarked Items	Files that you bookmarked in FTK.
Deleted Files	Complete files or folders recovered from slack or free space.
Duplicate Items	Any items that have an identical hash. Because the filename is not part of the hash, identical files may actually have different filenames. The primary item is the first one found by FTK. The secondary item is any file that has an identical hash of the primary item.
Encrypted Files	Files that are encrypted or have a password. This includes files that have a read-only password. Files with a read-only password may be opened and viewed, but not modified by the reader.
Flagged Ignore	Files that you flagged to ignore.
From E-mail	Files that were embedded in an e-mail message, such as an attachment.
From Recycle Bin	Files derived from the recycled/recycler file structure.
KFF Alert Files	Files identified by the current hash set as illicit or contraband files.
KFF Ignorable	Files identified by the HashKeeper database as common, known files, such as program files.
OLE Subitems	Items or pieces of information that were embedded in a file, such as text, graphics, or an entire file.

File Type

The following table outlines the file types you can use to filter items in FTK.

Item buttons toggle between filter settings; simply click an item button multiple times to rotate through the filter settings.

Category	Description
Archives	Archive files include e-mail archive files, Zip, Stuffit,Thumbs.db thumbnail graphics, and other archive formats. For a complete list of archive file types recognized by FTK, see "Archive File Types" on page 291.
Databases	Includes databases from Access, Quicken, Microsoft Money, Quickbooks, and others. For a complete list of database file types recognized by FTK, see "Database File Types" on page 286.
Documents	Includes most word processing, HTML, WML, HDML, or text files. For a complete list of document file types recognized by FTK, see "Document File Types" on page 282.
E-mail Messages	Includes e-mail messages from Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail, and MSN. For a complete list of e-mail message file types recognized by FTK, see "E-mail Message Programs" on page 290.
Executable Files	Includes executables from Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats. For a complete list of executable file types recognized by FTK, see "Executable File Types" on page 291.
Folders	Folders and directories.
Graphics	Includes the standard graphic formats like .tif, .gif, .jpeg, and .bmp. For a complete list of graphic file types recognized by FTK, see "Graphic File Types" on page 288.
Other Known Files	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, etc. For a complete list of other file types recognized by FTK, see "Other Known File Types" on page 293.

Category	Description
Slack/Free Space	Fragments of files that have not been completely overwritten.
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others. For a complete list of spreadsheet file types recognized by FTK, see “Spreadsheet File Types” on page 285.
Thumbs.db Files	Files used in Microsoft Windows to store caches for Windows Explorer's thumbnail view.
Unknown Files	File types that FTK cannot identify.

File Size

To filter items by file size:

- You define the file size range you want to use to filter items.
- You determine if you want to measure file size using the logical or physical file size. Logical file size is the size of the file itself. Physical file size is the size of the clusters occupied by the file; that is, it includes the file and the file slack.

File Date

FTK allows you to filter items by a specific range of file dates or by a specific number of days, weeks, months, or years.

Because the operating system tracks multiple dates for a given item, FTK allows you to filter on different types of file dates. The following table identifies which file dates you can use to filter items in FTK:

Option	Description
Accessed	The date the file was last accessed.
Created	The date the file was created.

Option	Description
Modified	The date the file was last modified.
With Any Date	Any date.

Modifying or Creating a Filter

Custom file filters are saved in the FtkFileFilters.ini file. This file is located in the \AccessData\AccessData Forensic Toolkit\Program\ directory.

Note: You can access your custom file filters on other machines by copying the FtkFileFilters.ini file to the computer's \AccessData\AccessData Forensic Toolkit\Program\ directory. This will, however, overwrite the custom file filters on the target machine. (This does not impact the default file filters.)

To modify or create a filter:

1 Select **View**, and then **File Filter Manager**.

or

Click the File Filter Manager icon on the File List toolbar.

2 In the **Selected Filter** drop-down list, enter the name of your new filter.

or

Select the filter that you want to modify.

3 To filter by file status and type:

3a Click the button for each **File Status** item to rotate through the available filter settings.

See page 192 for an explanation of each file status.

3b Click the button for each **File Type** item to rotate through the available filter settings.

See page 193 for an explanation of each file type.

3c You can also click a filter setting in the Legend to unilaterally apply the setting to all items in the File Type and File Status columns.

4 To filter by file size:

4a Click the **File Size** button to rotate through the available filter settings.

4b Determine if you want to measure file size using the **Logical** or **Physical** file size.

Logical file size is the size of the file itself. Physical file size is the size of the clusters occupied by the file; that is, it includes the file and the file slack.

4c In the **From** field, select the minimum file size.

4d In the **To** field, select the maximum file size.

4e To filter by file date:

4f Click the **File Date** button to rotate through the available filter settings.

4g Select which file date you want to use to filter items.

See page 195 for an explanation of each file date.

4h Select **Between** and enter the beginning and ending dates.

or

Select **In The Last**, enter the number in the box, and select **Days**, **Weeks**, **Months**, or **Years**.

5 If you are modifying an existing filter, click **Save/Apply**.

or

If you are creating a new filter, click **Save As**, enter the name, and click **OK**.

Deleting a Filter

You can delete a filter if you no longer need it.

To delete a filter:

1 Select **View**, and then **File Filter Manager**.

or

Click the Filter Manager icon on the File List toolbar.

2 In the **Selected Filter** drop-down list, select the filter that you want to delete.

3 Click **Delete**.

CHAPTER 11

Searching the Registry

The Windows Registry allows the Windows operating system to control hardware, software, user information, and the overall functionality of the Windows interface. Unlike Windows Registry Editor, which only displays the current system's registry, Registry Viewer lets you examine registry files from any system. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor.

This chapter contains the information that allows you to successfully search the registry for additional evidence to build your case evidence:

- "Starting Registry Viewer" on page 200
- "Understanding the Registry Viewer Windows" on page 201
- "Opening a Registry File in Registry Viewer" on page 204
- "Working with Registry Evidence" on page 206
- "Creating Registry Summary Reports" on page 208
- "Generating a Report" on page 213
- "Exporting a Word List" on page 214

Detailed information on Registry Viewer functionality is available in the Registry Viewer help. Click **Help**, and then **Help Topics**.

Starting Registry Viewer

You can run Registry Viewer as a separate application or you can launch it directly within Forensic Toolkit (FTK).

Launching Registry Viewer as a Separate Application

To run Registry Viewer as a separate application, select **Start**, then **Programs**, then **AccessData**, and then **Registry Viewer**, and then **Registry Viewer**.

Launching Registry Viewer from FTK

Integrating Registry Viewer with FTK allows you to seamlessly view registry files and create registry reports from within FTK. Any created reports are saved by default in the current FTK case file.

Integration also allows you to extract and open registry files on the fly from hard drive images. FTK automatically creates a temporary registry file from the image and opens it in Registry Viewer; after you're finished, FTK deletes the temporary file.

To run Registry Viewer from FTK:

1. In FTK, open an existing case by selecting **File**, and then **Open Case**.

   Or if you have chosen to always display the FTK Startup screen, select **Open an Existing Case** and click **OK**.

2. Select the case you want to open.
3. Select **File**, and then **Registry Viewer** to open Registry Viewer.
4. Select the registry file you want to view and then click **View File**.

Note: If you have located registry files in the case in FTK, you can right-click on a file and then select **View in Registry Viewer**. Registry Viewer automatically launches.

Understanding the Registry Viewer Windows

Registry Viewer has three viewing windows to help you obtain and report important registry information. All windows contain a hex viewer that displays a selected key's values in hexadecimal format.

Note: For more information on the files that comprise the registry, see "Securing Windows Registry Evidence" on page 315.

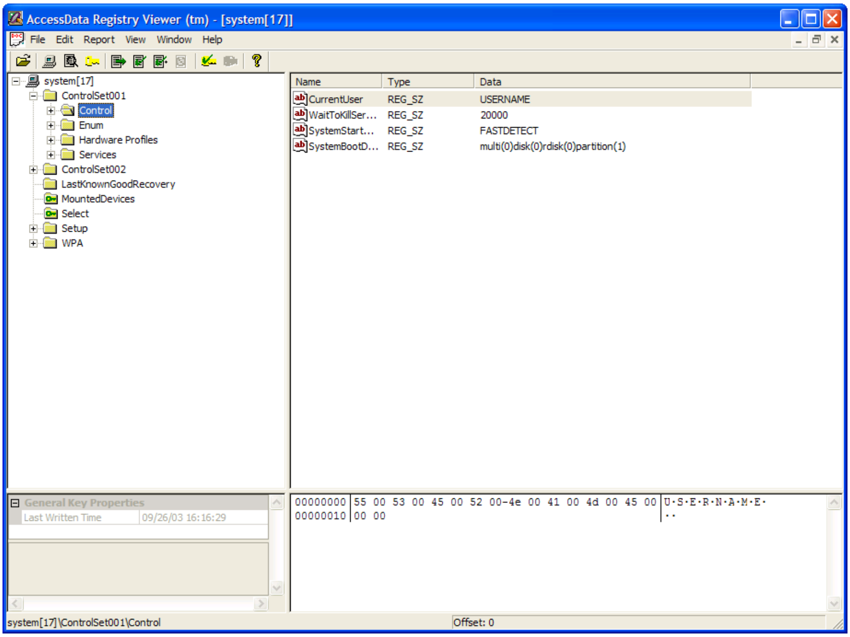
The Full Registry Window

The Full Registry window shows all the contents of a registry file. From this window, you can select a keys or subkeys to add to a report. Registry Viewer opens one file at a time.

Note: You can extend the Registry Viewer by dragging it to the right so that you can the entire registry path.

To view the Full Registry window, select **View**, and then **Full Registry** or click the button on the toolbar to open the Full Registry window

.



Name	Type	Data
CurrentUser	REG_SZ	USERNAME
WaitToKillSer...	REG_SZ	20000
SystemStart...	REG_SZ	FASTDETECT
SystemBootD...	REG_SZ	multi(0)disk(0)rdisk(0)partition(1)

Last Written Time 09/26/03 16:16:29

```
00000000 55 00 53 00 45 00 52 00-4e 00 41 00 4d 00 45 00 U·S·E·R·N·A·M·E·
00000010 00 00                                            ··
```

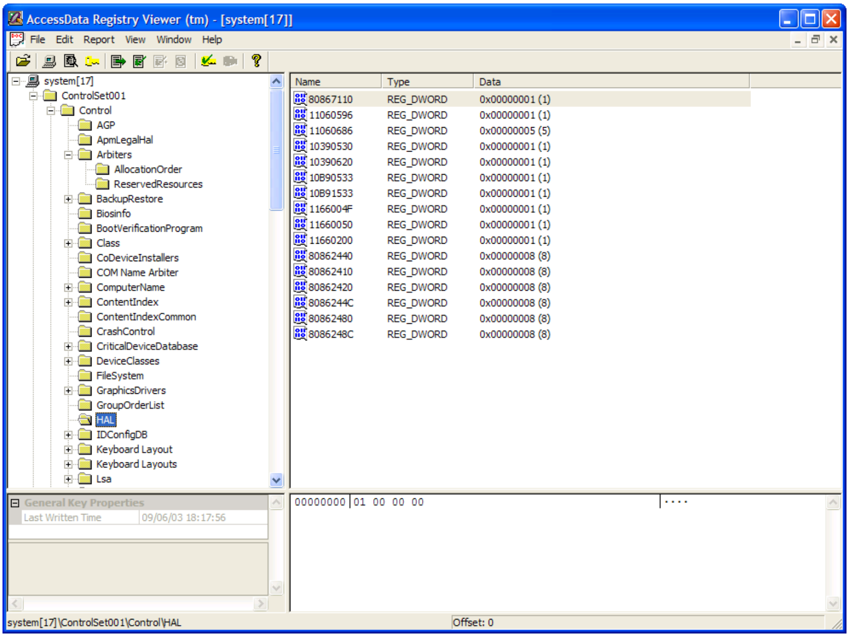
system[17]\ControlSet001\Control

Offset: 0

The Common Areas Window

The Common Areas window helps you quickly access those areas of a registry file most likely to contain important information.

To view the Common Areas window, select **View**, and then **Common Areas** from the menu or click the button on the toolbar.



Name	Type	Data
80867110	REG_DWORD	0x00000001 (1)
11060596	REG_DWORD	0x00000001 (1)
11060686	REG_DWORD	0x00000005 (5)
10390530	REG_DWORD	0x00000001 (1)
10390620	REG_DWORD	0x00000001 (1)
10B90533	REG_DWORD	0x00000001 (1)
10B91533	REG_DWORD	0x00000001 (1)
1166004F	REG_DWORD	0x00000001 (1)
11660050	REG_DWORD	0x00000001 (1)
11660200	REG_DWORD	0x00000001 (1)
80862440	REG_DWORD	0x00000008 (8)
80862410	REG_DWORD	0x00000008 (8)
80862420	REG_DWORD	0x00000008 (8)
8086244C	REG_DWORD	0x00000008 (8)
80862480	REG_DWORD	0x00000008 (8)
8086248C	REG_DWORD	0x00000008 (8)

Last Written Time 09/06/03 18:17:56

```
00000000 01 00 00 00                                ....
```

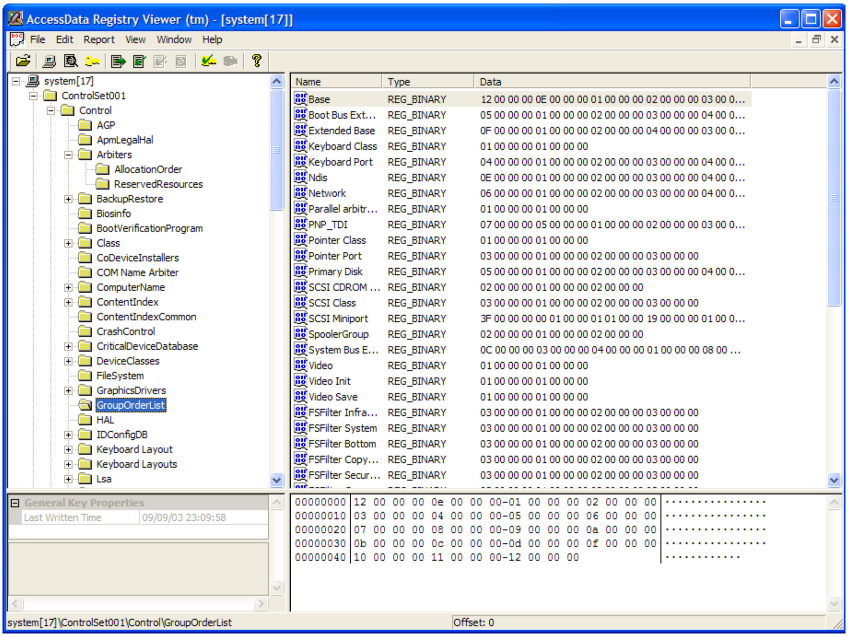
system[17]\ControlSet001\Control\HAL   Offset: 0

Unlike the Full Registry window, which displays all the contents of a registry file, the Common Areas window only shows those keys that commonly contain information of forensic interest such as usernames, passwords, browser history, and so forth. Of course, the various files that make up the registry each contain different information; therefore, the keys that appear by default in the Common Areas window depend upon which registry file you open.

The Report Window

The Report window displays the selected keys, allowing you to print only relevant information. After you have finished adding keys, you can generate a printable HTML report file containing all the selected keys and their associated information. If you integrate Registry Viewer with FTK, Registry Viewer uses the case report location defined in FTK as the default location for the generated report.

To view the Report window, select **View**, and then **Report** from the menu, or click the button on the toolbar.



Name	Type	Data
Base	REG_BINARY	12 00 00 00 0E 00 00 00 01 00 00 00 02 00 00 00 03 00 0...
Boot Bus Ext...	REG_BINARY	05 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 0...
Extended Base	REG_BINARY	0F 00 00 00 01 00 00 00 02 00 00 00 04 00 00 00 03 00 0...
Keyboard Class	REG_BINARY	01 00 00 00 01 00 00 00
Keyboard Port	REG_BINARY	04 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 0...
Ndis	REG_BINARY	0E 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 0...
Network	REG_BINARY	06 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 0...
Parallel arbitr...	REG_BINARY	01 00 00 00 01 00 00 00
PNP_TDI	REG_BINARY	07 00 00 00 05 00 00 00 01 00 00 00 02 00 00 00 03 00 0...
Pointer Class	REG_BINARY	01 00 00 00 01 00 00 00
Pointer Port	REG_BINARY	03 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00
Primary Disk	REG_BINARY	05 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 0...
SCSI CDROM ...	REG_BINARY	02 00 00 00 01 00 00 00 02 00 00 00
SCSI Class	REG_BINARY	03 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00
SCSI Miniport	REG_BINARY	3F 00 00 00 00 01 00 00 01 01 00 00 19 00 00 00 01 00 0...
SpoolerGroup	REG_BINARY	02 00 00 00 01 00 00 00 02 00 00 00
System Bus E...	REG_BINARY	0C 00 00 00 03 00 00 00 04 00 00 00 01 00 00 00 08 00 ...
Video	REG_BINARY	01 00 00 00 01 00 00 00
Video Init	REG_BINARY	01 00 00 00 01 00 00 00
Video Save	REG_BINARY	01 00 00 00 01 00 00 00
FSFilter Infra...	REG_BINARY	03 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00
FSFilter System	REG_BINARY	03 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00
FSFilter Bottom	REG_BINARY	03 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00
FSFilter Copy...	REG_BINARY	03 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00
FSFilter Secur...	REG_BINARY	03 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00

General Key Properties	
Last Written Time	09/09/03 23:09:58

```
00000000 12  00  00  00  0e  00  00  00-01  00  00  00  02  00  00  00 ················
00000010 03  00  00  00  04  00  00  00-05  00  00  00  06  00  00  00 ················
00000020 07  00  00  00  08  00  00  00-09  00  00  00  0a  00  00  00 ················
00000030 0b  00  00  00  0c  00  00  00-0d  00  00  00  0f  00  00  00 ················
00000040 10  00  00  00  11  00  00  00-12  00  00  00                 ············
```

system[17]\ControlSet001\Control\GroupOrderList

Offset: 0

Opening Registry Files

Registry Viewer allows you to open and view archived Windows registry files.

Note: Registry Viewer cannot open active Windows registry files.

The following sections review different ways to open Windows registry files:

- "Opening a Registry File in Registry Viewer" on page 204
- "Opening Registry Files within FTK" on page 205
- "Obtaining Protected Registry Files Using FTK Imager" on page 205

Opening a Registry File in Registry Viewer

To open a registry file in Registry Viewer:

1. Select **File**, and then **Open** or click the 📂 button.

   Note: Registry Viewer cannot open registry files within an image. You must export registry files from an image before they can be opened in Registry Viewer.

2. Select the registry file and then click **Open**.

   Or

   You can open a recently used file by selecting **File**, and then ***filename*** from the menu.

The file opens in the Full Registry Window.

You can open only one registry file at a time in Registry Viewer. If you want to open another file, you must first close the current file or run a second instance of Registry Viewer. You can run multiple instances of Registry Viewer.

Opening Registry Files within FTK

To open a registry file from FTK,

1 Click **File**, and then **Registry Viewer**.

FTK opens a Registry File List that includes all the registry files in the current body of evidence.

Note: If the registry files are part of an image file, FTK automatically exports the registry files to a temporary registry file so they can be viewed in Registry Viewer. When you are finished, FTK deletes the temporary registry file.

2 Double-click a file in the Registry File List to open it in Registry Viewer.

Or

Click **View File**.

You can also open registry files in FTK as follows:

1 Select an individual registry file in the file list.

2 Right-click, then select **Registry Viewer** from the quick menu.

Obtaining Protected Registry Files Using FTK Imager

The Windows operating system does not allow you to copy or save live registry files. Therefore, users have had to image their hard drive and then extract the registry files or boot their computer from a boot disk and copy the registry files from the inactive drive.

FTK Imager provides a much easier solution. It bypasses the Windows operating system and allows you to copy registry files underneath the Windows file lock.

To obtain the protected registry files using FTK Imager:

1 Launch FTK Imager.

2 Click **File**, and then **Obtain Protected Files**, or click the button on the toolbar.

3 Designate a destination directory and file options, then click **OK**.

4 FTK Imager exports the selected files to the designated location.

5 Add the files to the case in FTK (see “Adding Evidence” on page 99).

6 To open the registry files, click **File**, and then **Registry Viewer**

or

Right-click on a registry file in the file list, then select **Registry Viewer**.

Working with Registry Evidence

You can add keys to the Common Areas and Report windows. This section reviews how to manage keys within Registry Viewer:

- “Adding Keys to the Common Areas Window” on page 207
- “Deleting Keys from the Common Areas Window” on page 207
- “Adding Keys to the Report Window” on page 207
- “Deleting Keys from the Report Window” on page 208

Adding Keys to the Common Areas Window

Once you add a key to the Common Areas window, Registry Viewer keeps track of each key you add, remembering them between registry files and between sessions.

To add a key to the Common Areas window

1. Select **View, and then Full Registry** or click the 🖥 button on the toolbar to open the Full Registry window.
2. In the registry tree, locate and select the key you want to add.
3. From the menu, select **Edit**, and then **Add to Common Areas** or click the ✓ button on the toolbar to add the selected key to Common Areas window.

Deleting Keys from the Common Areas Window

To delete keys from the Common Areas Window:

1. In the registry tree, locate and select the key you want to delete.
2. From the menu, select **Edit**. and then **Remove from Common Areas** or click the 🚫 button on the toolbar to remove the selected key from Common Areas window.

Adding Keys to the Report Window

The Report window displays only those keys that you select to be added to a report. Registry Viewer lets you select keys in the Full Registry and Common Areas windows and add them to the Report window.

Note: Keys added to the Report window are not saved between sessions or between registry files. To save a record of this information, you must generate a report file before closing the registry file or exiting Registry Viewer.

To add keys to the Report window:

1. In the registry tree, locate and select the key you want to add.
2. From the menu, select **Report**, and then **Add to Report with Children** or click the button to add the selected key and all its subkeys to the Report window.

Keys that have been added to a report are denoted by a checked folder icon in the Full Registry and Common Areas windows.

After a report has been generated, it can be added to a case in FTK. When FTK reports are generated, the Registry Viewer reports can be included by checking the **Include Registry Viewer Reports** box in the Report Wizard's Report Location window.

Deleting Keys from the Report Window

To remove a key from the Report window:

1. In the Report window, locate and select the key you want to remove.
2. From the menu, select **Report**, and then **Remove from Report** or click the button on the toolbar.

Creating Registry Summary Reports

You can create Registry Summary Reports (RSRs) in FTK 1.80. An RSR file is simply a template list of desired registry key/value locations, along with section headings. FTK can use these templates to quickly generate reports, saving a significant amount of time in cases where the keys/values you are reporting are in a static location.

FTK creates registry reports for the following Registry Files:

- NTuser.dat
- SAM
- Security
- Software

- System

To create RSRs, select the **Registry Reports** check box in the Evidence Processing Options (Processes to Perform) window when you set up your case (see “Selecting Evidence Processes” on page 65).

Note: If you would like this check box to be selected by default, see “Changing RSR Settings in the FtkSettings.0.ini File” on page 210.

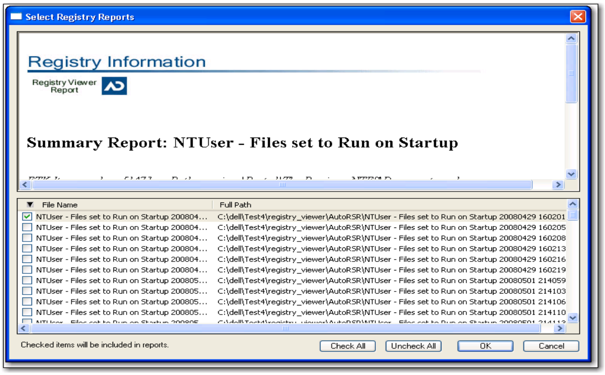
If you want to add additional RSRs to your case, or if you didn’t select the **Registry Reports** check box when you set up the case, you can still create or add new RSRs by clicking **Tools** and then **Preliminary Registry Reports**.

Note: This does not replace exiting files, but adds new files with new filenames.

A series of report dialogs (one for each RSR) indicates that the RSRs are being created.

If you would like to preview the RSRs and add them to your case report, do the following:

1 From the Menu bar, click **Tools** and then **Select Registry Reports**.



Summary Report: NTUser - Files set to Run on Startup

	File Name	Full Path
☑	NTUser - Files set to Run on Startup 200804...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080429 160201
□	NTUser - Files set to Run on Startup 200804...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080429 160205
□	NTUser - Files set to Run on Startup 200804...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080429 160208
□	NTUser - Files set to Run on Startup 200804...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080429 160213
□	NTUser - Files set to Run on Startup 200804...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080429 160216
□	NTUser - Files set to Run on Startup 200804...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080429 160219
□	NTUser - Files set to Run on Startup 200805...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080501 214059
□	NTUser - Files set to Run on Startup 200805...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080501 214103
□	NTUser - Files set to Run on Startup 200805...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080501 214106
□	NTUser - Files set to Run on Startup 200805...	C:\dell\Test4\registry_viewer\AutoRSR\NTUser - Files set to Run on Startup 20080501 214110

Checked items will be included in reports.

2 Select the RSRs you want to include in your report.

A check appears in the box next to the selected reports.

If you have modified your .ini file to add RSRs as evidence items to every new case (see “Changing RSR Settings in the FtkSettings.0.ini File” on page 210). These items are automatically included in the Registry Reports section of the case report.

The highlighted report appears in the View pane.

3 Click **OK**.

Using Pre-defined AccessData Templates

AccessData provides a list of registry report template files. The RSR files available from AccessData have been collected from both internal and external sources. Each of these files has been reviewed by AccessData for basic functionality only. Since every investigation varies, Accessdata cannot guarantee that these templates will report on the information you are targeting. AccessData recommends that you review the RSR files intended output prior to using it in a case or relying on it as the basis for any professional opinion.

Creating Your Own Registry Report Templates

In addition to the template set that comes with the program, FTK can also use custom registry report templates that you have created in Registry Viewer (see "Changing RSR Settings in the FtkSettings.0.ini File" on page 210). The filename of a custom template must begin with the registry file type (for example, NTUser, Software, System, etc.) and have a .rsr extension.

Changing RSR Settings in the FtkSettings.0.ini File

You can make the following changes to RSR settings in the FtkSettings.0.ini file:

- Select the Registry Reports check box by default in the Evidence Processing Options window.
- Add Registry Summary Reports as evidence items to every new case.

- Change the default directory for RSRs.

To Change RSR settings in the FtkSettings.0.ini file, do the following:

1 Close FTK.

2 Browse to the \Program Files\AccessData\AccessData Forensic Toolkit 1.80.0\Program\FtkSettings.0.ini (configuration) file.

3 Open the file with a text editor.

4 Scroll to the [Global] section near the end of the file.

5 Change the settings:

To	Do this
Select the Registry Reports check box by default in the Evidence Processing Options form.	Change PreprocessRegistryFiles=0 to PreprocessRegistryFiles=1
Add Registry Summary Reports as evidence items to every case.	Change AddRegistryReportsToCase=0 to AddRegistryReportsToCase=1
Change the default location for RSRs.	Change RVRSRDirectory= to RVRSRDirectory=[default directory path]

6 Save and close the FtkSettings.0.ini file.

Searching for Specific Data

Registry Viewer lets you perform live searches for specific information in a registry file.

Note: Registry Viewer performs searches in the currently open window. Therefore, if you want to search the entire registry file, you must search from the Full Registry window. Likewise, if you want to search only in common areas, you must search from the Common Areas window, and so forth.

To search for specific data:

1 Open the window that contains the keys you want to search.

1a To open the Full Registry window, select **View**, and then **Full Registry** from the menu or click the button on the toolbar.

1b To open the Report window, select **View**, and then **Report** from the menu or click the button on the toolbar.

1c To open the Common Areas window, select **View**, and then **Common Areas** from the menu or click the button on the toolbar.

2 From the menu, select **Edit**, and then **Find**.

3 The Find dialog appears.

4 In the Find What field, enter the text string you want to search for.

5 Select the registry file areas you want to search.

5a Check the **Keys** box to search for the specified string in all key names.

5b Check the **Values** box to search for the specified string in all value names.

5c Check the **Data** box to search for the specified string in all value data.

6 Check the **Match Whole String Only** box to only find data that matches the entire specified string.

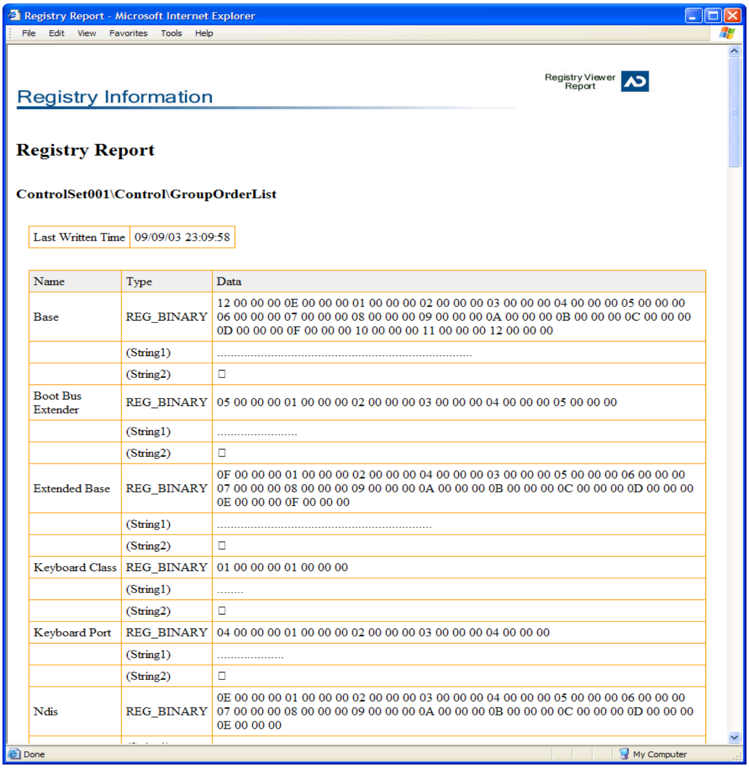
7 Click **Find Next** to search for the specified string.

8 When Registry Viewer finds a match to the specified string, it expands the registry tree and highlights the matching data.

9 To search for the next instance of the specified string, select **Edit**, and then **Find** from the menu and click **Find Next** again.

Generating a Report

After you have finished adding keys to the Report window, you can generate a printable HTML report file containing all the selected keys and their associated information.


Registry Report - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Registry Viewer Report
Done
My Computer

Registry Information

Registry Report

ControlSet001\Control\GroupOrderList

Last Written Time	09/09/03 23:09:58

Name	Type	Data
Base	REG_BINARY	12 00 00 00 0E 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0A 00 00 00 0B 00 00 00 0C 00 00 00 0D 00 00 00 0F 00 00 00 10 00 00 00 11 00 00 00 12 00 00 00
	(String1)	....
	(String2)	□
Boot Bus Extender	REG_BINARY	05 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00
	(String1)	....
	(String2)	□
Extended Base	REG_BINARY	0F 00 00 00 01 00 00 00 02 00 00 00 04 00 00 00 03 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0A 00 00 00 0B 00 00 00 0C 00 00 00 0D 00 00 00 0E 00 00 00 0F 00 00 00
	(String1)	....
	(String2)	□
Keyboard Class	REG_BINARY	01 00 00 00 01 00 00 00
	(String1)	....
	(String2)	□
Keyboard Port	REG_BINARY	04 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00
	(String1)	....
	(String2)	□
Ndis	REG_BINARY	0E 00 00 00 01 00 00 00 02 00 00 00 03 00 00 00 04 00 00 00 05 00 00 00 06 00 00 00 07 00 00 00 08 00 00 00 09 00 00 00 0A 00 00 00 0B 00 00 00 0C 00 00 00 0D 00 00 00 0E 00 00 00

To generate a report file,

1. From the menu, select **Report**, and then **Generate Report** or click the button on the toolbar.
2. The Create Report dialog appears.
3. In the Report Title field, enter a name for the report file.
4. In the Report Location field, enter the location where you want to save the report file or click **Browse** to navigate to the desired location.

5 Check the **View Report When Created** box to automatically open the newly-created report file (*.htm) in your Internet browser.

6 Click **OK** to generate the report file.

Registry Viewer uses the case report location defined in FTK as the default location for the generated report.

Exporting a Word List

Registry Viewer lets you create and export a word list containing all the strings in a registry file. The word list can then be used in PRTK as a dictionary for decoding passwords and pass phrases.

When you export a word list, Registry Viewer searches the registry file for key values that are stored as strings. Each string it finds is exported into a text file as a separate line. Thus the resulting file contains a list of every string value in the registry.

If you save or copy the word list file into the PRTK dictionary folder (\AccessData\Dictionaries), PRTK automatically adds it to its list of available user-defined dictionaries. PRTK can then use each line in the file as a possible password or pass phrase in a password recovery operation. For more information on PRTK user dictionaries or on password recovery, the *Password Recovery Toolkit User Guide*.

To export a word list:

1 From the menu, select **Report**, and then **Export Word List.**

2 The Export Word List dialog appears.

3 In the Filename field, enter a name for the word list file. The file (*.txt) is saved in plain-text format.

4 In the Path field, enter the location where you want to save the word list file or click **Browse** to navigate to the desired directory location.

5 The default path for word list files is \AccessData\Registry Viewer.

6 Click **OK** to export the word list.

CHAPTER 12

Decrypting EFS

Windows 2000 and XP Professional include the ability to encrypt files and folders. Forensic Toolkit (FTK) can break the file encryption so that additional evidence can be uncovered.

This chapter contains the information that allows you to understand the Encrypting File System (EFS) and how FTK breaks the encryption:

- "Understanding EFS" on page 218
- "Decrypting EFS Files and Folders" on page 218
- "Viewing the Decrypted Files in FTK" on page 219

Understanding EFS

EFS is built in to Windows 2000 and Windows XP Professional. It is not supported in Windows XP Home Edition.

EFS can be used to encrypt files or folders. EFS files or folders can be viewed only by the user who encrypted them or by the user who is the authorized Recovery Agent. When the user logs in, encrypted files and folders are seamlessly decrypted and the files are automatically displayed.

Note: There are certain files that cannot be encrypted, including system files, NTFS compressed files, and files in the C:\Windows_System_Root and its subdirectories.

Decrypting EFS Files and Folders

When evidence is added to a case and Decrypt EFS Files is selected in the New Case Wizard, FTK launches PRTK and decrypts EFS files.

The following sections review the requirements to decrypt EFS files on Windows 2000 and XP systems.

Windows 2000 and XP Systems Prior to SP1

FTK automatically decrypts EFS files on Windows 2000 systems and Windows XP systems prior to Service Pack 1. Simply select the Decrypt EFS Files option when adding evidence to a case and FTK will launch PRTK and decrypt the EFS files.

Windows XP SP1 or Later

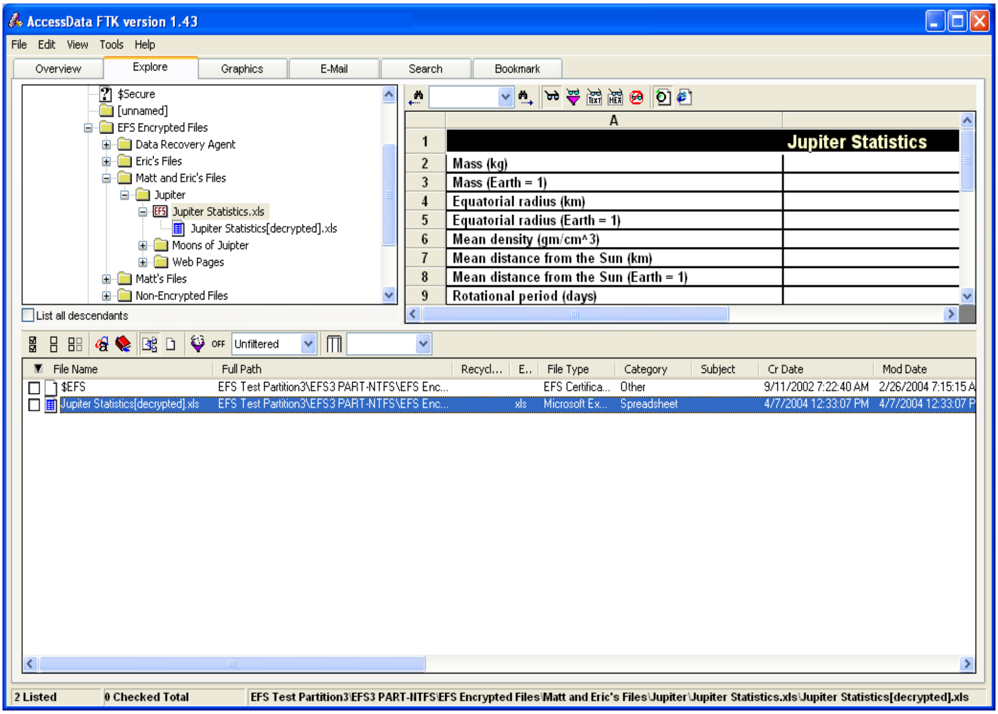
For Windows XP systems with Service Pack 1 or later, FTK needs the user's or Recovery Agent's password before it can decrypt EFS files.

Depending on what version of PRTK you have, there are different steps that need to be followed to decrypt EFS files.

The *Password Recovery Toolkit User Guide* associated with the version of PRTK that you are running contains a chapter entitled "Specialized Password Recoveries." This chapter includes information on recovering EFS files. Follow the steps in this section to decrypt the files.

Viewing the Decrypted Files in FTK

The decrypted information is displayed in the Explore window. The decrypted file is displayed as a subitem below the encrypted file, the metadata is displayed, and the full path name is displayed, including a note that shows that the file is decrypted.



	A	
1		Jupiter Statistics
2	Mass (kg)	
3	Mass (Earth = 1)	
4	Equatorial radius (km)	
5	Equatorial radius (Earth = 1)	
6	Mean density (gm/cm^3)	
7	Mean distance from the Sun (km)	
8	Mean distance from the Sun (Earth = 1)	
9	Rotational period (days)	

File Name	Full Path	Recycl...	E..	File Type	Category	Subject	Cr Date	Mod Date
□ $EFS	EFS Test Partition3\EFS3 PART-NTFS\EFS Enc...			EFS Certifica...	Other		9/11/2002 7:22:40 AM	2/26/2004 7:15:15 A
□ Jupiter Statistics[decrypted].xls	EFS Test Partition3\EFS3 PART-NTFS\EFS Enc...		xls	Microsoft Ex...	Spreadsheet		4/7/2004 12:33:07 PM	4/7/2004 12:33:07 P

2 Listed | 0 Checked Total | EFS Test Partition3\EFS3 PART-NTFS\EFS Encrypted Files\Matt and Eric's Files\Jupiter\Jupiter Statistics.xls\Jupiter Statistics[decrypted].xls

For example, if you have a decrypted file named Jupiter Statistics.xls, then *Jupiter Statistics[decrypted].xls* is listed as a child of Jupiter Statistics.xls in the File List.

CHAPTER 13

Working with Reports

After you complete the case investigation, you can create a report that summarizes the relevant evidence of the case. The final report is in HTML format and is viewable in a standard Web browser.

This chapter contains the following sections about reports:

- "Creating a Report" on page 222
- "Viewing and Distributing a Report" on page 239
- "Updating a Report" on page 241
- "Modifying a Report" on page 242

Creating a Report

You create a report with the Report Wizard. You access the Report Wizard by selecting **File**, and then **Report Wizard**.

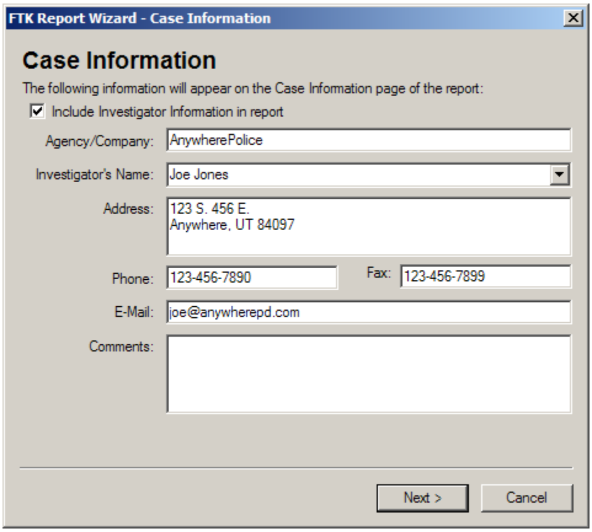
To create a report:

1. Enter basic case information.
2. Decide how to handle bookmarks.
3. Select the properties of bookmarks.
4. Decide how to handle graphic thumbnails.
5. Decide if you want a file path list.
6. Decide if you want a file properties list.
7. Select the properties of the file properties list.
8. Add supplementary files and the case log.
9. Add the Registry Viewer report or a custom graphic to the report and select the report location.

Most of the steps are optional. Each step is discussed in detail in the following sections.

Entering Basic Case Information

The Case Information form provides fields for basic case information, such as the investigator and the organization that analyzed the case.



Case Information

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

☑ Include Investigator Information in report

Agency/Company: AnywherePolice

Investigator's Name: Joe Jones

Address: 123 S. 456 E.
Anywhere, UT 84097

Phone: 123-456-7890

Fax: 123-456-7899

E-Mail: joe@anywherepd.com

Comments:

To provide basic case information:

1. If you want to include the investigator information, check the **Include Investigator Information in Report** box.
2. In the Agency/Company field, enter the name of the organization that analyzed the case.
3. In the **Investigator Name** field, type the name of the investigator.

   The drop-down list contains the name of investigators that have been entered in prior cases. If the investigator has worked on other cases in FTK, select the name from the list.
4. In the **Address** field, enter the investigator’s address.
5. In the **Phone** field, enter the investigator’s phone number.
6. In the **Fax** field, enter the investigator’s fax number.

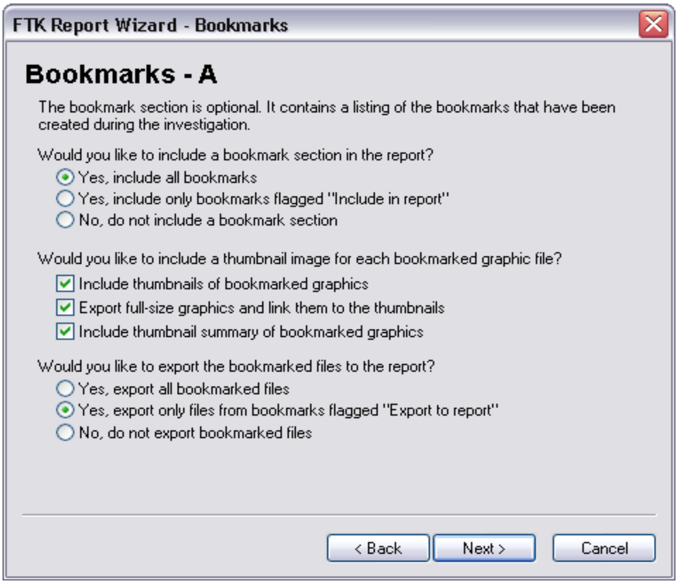
7 In the **E-mail** Address field, enter the investigator’s e-mail address.

8 In the **Comments** field, enter the comments pertinent to the report.

9 Click **Next**.

Managing Bookmarks

The Bookmarks-A form allows you to create a section in the report that lists the bookmarks that were created during the case investigation. You can also choose to not create a bookmark section.



FTK Report Wizard - Bookmarks

Bookmarks - A

The bookmark section is optional. It contains a listing of the bookmarks that have been created during the investigation.

Would you like to include a bookmark section in the report?

- ● Yes, include all bookmarks
- ○ Yes, include only bookmarks flagged "Include in report"
- ○ No, do not include a bookmark section

Would you like to include a thumbnail image for each bookmarked graphic file?

- ☑ Include thumbnails of bookmarked graphics
- ☑ Export full-size graphics and link them to the thumbnails
- ☑ Include thumbnail summary of bookmarked graphics

Would you like to export the bookmarked files to the report?

- ○ Yes, export all bookmarked files
- ● Yes, export only files from bookmarks flagged "Export to report"
- ○ No, do not export bookmarked files

The following sections explain the options in the Bookmarks-A form:

Would you like to include a Bookmark section in the report?

Option	Description
Yes, Include All Bookmarks	Includes all bookmarks listed in the Bookmark window. **Note:** This option overrides individual bookmark settings.
Yes, Include Only Bookmarks Marked "Include In Report"	Includes only bookmarks that are specifically marked to include in the report. When you create a bookmark, you can check to include it in the report. If you decide later to include the bookmark in the report, you can check the box in the Bookmark window.
No, Do Not Include a Bookmark Section	Does not include bookmarks in the Bookmark section of the report. **Note:** This option overrides individual bookmark settings. A bookmark header still appears on the report; although, there is no content beneath the header.

Would you like to include a thumbnail image for each bookmarked graphic file?

Option	Description
Include Thumbnails of Bookmarked Graphics	Includes a thumbnail for each bookmarked graphic under the Bookmarked Graphics section.
Export Full-Size Graphics and Link Them to the Thumbnails	Exports the bookmarked graphic files to the Report\Export\ directory. Also includes a thumbnail for each bookmarked graphic in the report that links to the full-size file. You cannot select this option unless you also choose to include the thumbnails. If you choose to not include a bookmark section, you can still select this option to export the graphic files.
Include Thumbnail Summary of Bookmarked Graphic	Displays each graphic bookmark as a thumbnail and path under the Bookmarked Graphics section.

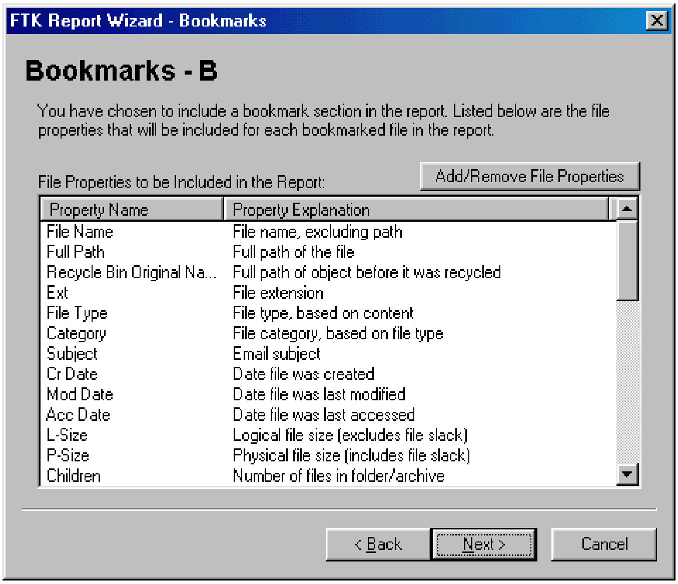
Would you like to export the bookmarked files to the report?

Option	Description
Yes, Export All Bookmarked Files	Exports all bookmarked files to the Report\Export\ directory. **Note:** This option overrides individual bookmark settings.
Yes, Export Only Files from Bookmarks Marked "Export to Report"	Exports only bookmarked files that are checked to export. When you create a bookmark, you can check it to export its files. If you decide later to export the bookmarked files, you can check the box in the Bookmark window.
No, Do Not Export Bookmarked Files	Does not export bookmarked files, even if they are checked to be exported. **Note:** This option overrides individual bookmark settings.

10 Click **Next**.

Selecting the Properties of Bookmarked Files

The Bookmarks-B form allows you to select which file properties to include for each bookmarked file. If you chose to not include a bookmark section, this form does not appear in the wizard.



You have chosen to include a bookmark section in the report. Listed below are the file properties that will be included for each bookmarked file in the report.

File Properties to be Included in the Report:

Property Name	Property Explanation
File Name	File name, excluding path
Full Path	Full path of the file
Recycle Bin Original Na...	Full path of object before it was recycled
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 modified
Acc Date	Date file was last accessed
L-Size	Logical file size (excludes file slack)
P-Size	Physical file size (includes file slack)
Children	Number of files in folder/archive

In the Bookmarks-B form:

1 Review the file properties to be included in the report.

The scrolling list contains the property name and explanation for each file property. For more information about the file properties, see “File List Columns” on page 51.

2 If you want to modify the file property list, click **Add/Remove File Properties**.

3 In the **Load from Stored Column Settings** drop-down list, select the template that contains the file information that you want to include in the Bookmark section of the report.

4 If you want to define a new column settings template:

4a Check or uncheck the Column Names, depending on which ones you want to include in the setting.

You can click **Select All** or **Unselect All** to mark or unmark all the columns.

4b To change the order in which the columns appear in the File List, select a column name and click **Move Up** or **Move Down**.

4c To create a new column setting, click **Save As**, enter a name in the field, and click **OK**.

5 If you want to modify an existing template:

5a Click **Columns**.

5b Select the column setting you want to modify.

5c Modify the Column Settings form.

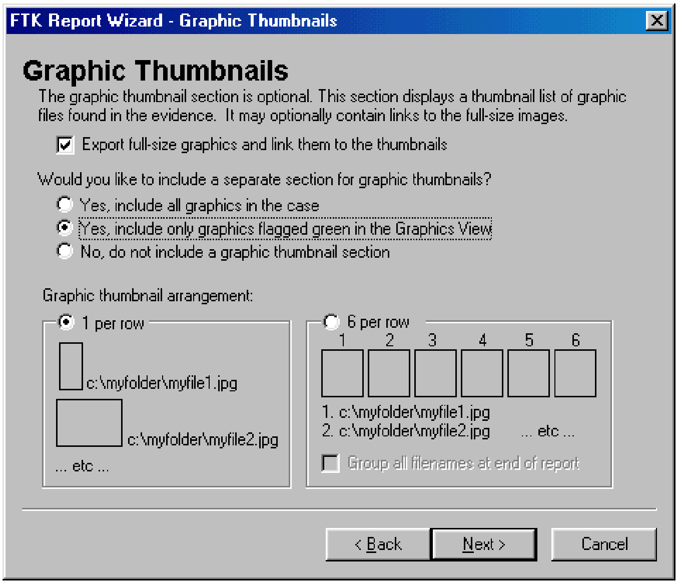
5d Click **Save**, then **Close**, and then **OK**.

For more information about the Column Settings form, see “Customizing Columns” on page 249.

6 Click **Next**.

Managing Thumbnails

The Graphic Thumbnails form allows you to create a section in the report that displays thumbnail images of the case graphics.



FTK Report Wizard - Graphic Thumbnails

Graphic Thumbnails

The graphic thumbnail section is optional. This section displays a thumbnail list of graphic files found in the evidence. It may optionally contain links to the full-size images.

☑ Export full-size graphics and link them to the thumbnails

Would you like to include a separate section for graphic thumbnails?

○ Yes, include all graphics in the case
● Yes, include only graphics flagged green in the Graphics View
○ No, do not include a graphic thumbnail section

Graphic thumbnail arrangement:

● 1 per row
○ 6 per row

☐ Group all filenames at end of report

The following tables outline the options in the Graphic Thumbnails form:

Would you like to include a separate section for graphic thumbnails?

Option	Description
Yes, Include all Graphics in the Case	Includes thumbnails for every graphic in the case.
Yes, Include Only Graphics Flagged Green in the Graphics View	Includes thumbnails only for the graphics that are marked green in the Thumbnail view of the Graphics window.
No, Do Not Include a Graphic Thumbnail Section	Does not include thumbnails for the graphics that are included in the report.

Arrangement	Description
Export Full-Size Graphics and Link Them to the Thumbnails	If you include a Graphic Thumbnails section in the report, this option allows you to export and link to the thumbnails' associated graphic files.

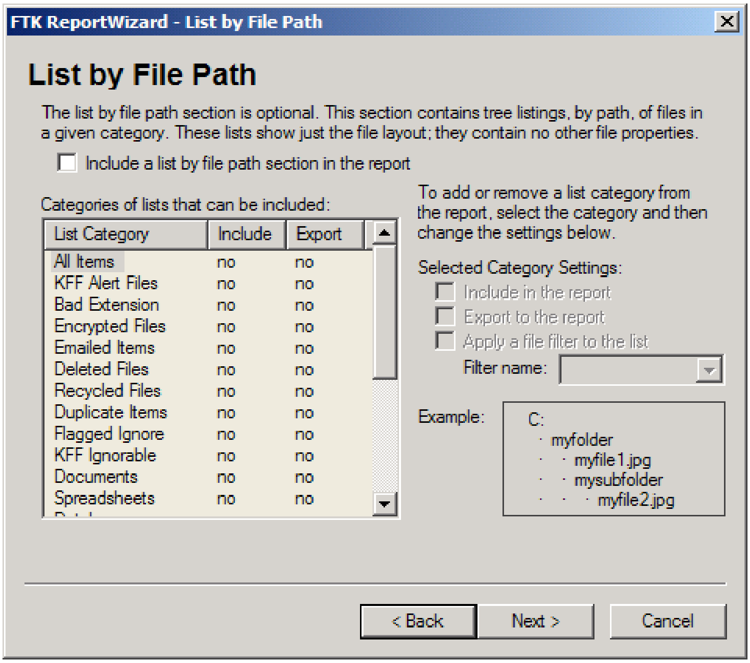
Graphic Thumbnails Arrangement

Arrangement	Description
1 Per Row	Displays thumbnails in one column. The file paths and names are displayed next to the thumbnail.
6 Per Row	Displays thumbnails in six columns. If you want to group all the file paths and names together, check the Group All Filenames at End of Report box. If you do not check this box, each file path and name is displayed next to its thumbnail.

7 Click **Next**.

Selecting a File Path List

The List by File Path form allows you to create a section in the report that lists the file paths of files in selected categories. The List by File Path section simply displays the files and their file paths; it does not contain any additional information. However, you can export and link to the files in the File Path list by checking the Export to the Report box.



FTK ReportWizard - List by File Path

List by File Path

The list by file path section is optional. This section contains tree listings, by path, of files in a given category. These lists show just the file layout; they contain no other file properties.

□ Include a list by file path section in the report

Categories of lists that can be included:

List Category	Include	Export
All Items	no	no
KFF Alert Files	no	no
Bad Extension	no	no
Encrypted Files	no	no
Emailed Items	no	no
Deleted Files	no	no
Recycled Files	no	no
Duplicate Items	no	no
Flagged Ignore	no	no
KFF Ignorable	no	no
Documents	no	no
Spreadsheets	no	no

To add or remove a list category from the report, select the category and then change the settings below.

Selected Category Settings:

□ Include in the report

□ Export to the report

□ Apply a file filter to the list

Filter name:

Example:

```
C:
 · myfolder
 ·  · myfile1.jpg
 ·  · mysubfolder
 ·  ·  · myfile2.jpg
```

In the List by File Path form:

1 If you want to include the list, check the **Include a List by File Path Section in the Report** box.

If you do not want to include the list, click **Next**.

2 If you want to include the MS Access database in the report, check the **Include MS Access database in report** box.

3 In the **Categories of Lists that Can Be Included** list, select which file categories to include in the list.

For more information about the categories, see “Getting Started” on page 31. Check the **Include in the Report** box.

The **Include** column of the selected categories changes to “YES.”

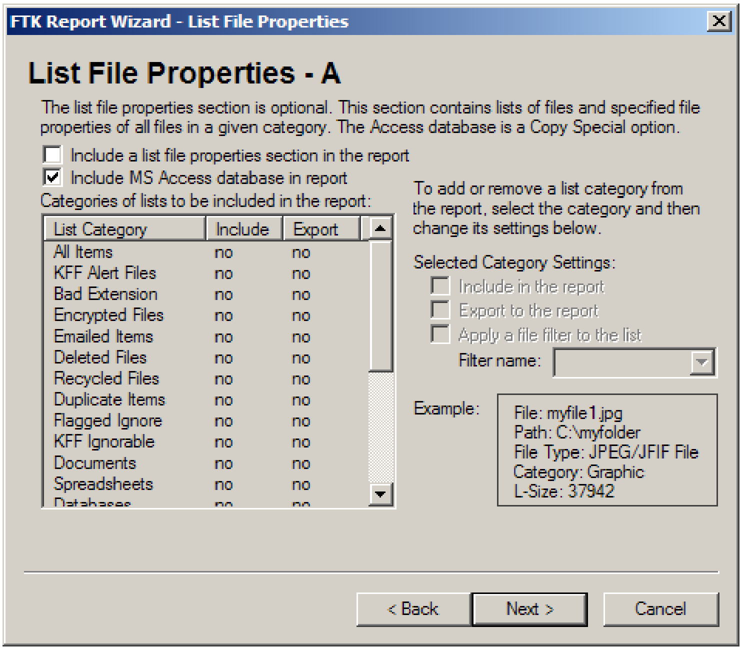
4 If you want to export and link to the files in the File Path list, check the **Export to the Report** box.

5 If you want to use a filter to manage which files appear in the File Path list, check the **Apply a File Filter to the List** box and select the filter from the **Filter Name** drop-down list.

6 Click **Next**.

Selecting a File Properties List

The List File Properties-A form allows you to create a section in the report that lists file properties for files in selected categories.



FTK Report Wizard - List File Properties

List File Properties - A

The list file properties section is optional. This section contains lists of files and specified file properties of all files in a given category. The Access database is a Copy Special option.

☐ Include a list file properties section in the report

☑ Include MS Access database in report

Categories of lists to be included in the report:

List Category	Include	Export
All Items	no	no
KFF Alert Files	no	no
Bad Extension	no	no
Encrypted Files	no	no
Emailed Items	no	no
Deleted Files	no	no
Recycled Files	no	no
Duplicate Items	no	no
Flagged Ignore	no	no
KFF Ignorable	no	no
Documents	no	no
Spreadsheets	no	no
Databases	no	no

To add or remove a list category from the report, select the category and then change its settings below.

Selected Category Settings:

☐ Include in the report

☐ Export to the report

☐ Apply a file filter to the list

Filter name:

Example:

File: myfile1.jpg
Path: C:\myfolder
File Type: JPEG/JFIF File
Category: Graphic
L-Size: 37942

Note: You designate which file properties will be listed for each file in the next step of the wizard.

In the List File Properties form:

1 If you want to include the list, check the **Include a List File Properties Section in the Report** box.

If you do not want to include the list, click **Next**.

2 If you want to include an MS Access database, check the **Include MS Access database in Report** box.

3 In the **Categories of Lists to Be Included in the Report** list, select which file categories to include in the list.

For more information about the categories, see "Getting Started" on page 31.

4 Check the **Include in the Report** box.

The **Include** column of the selected categories changes to "YES."

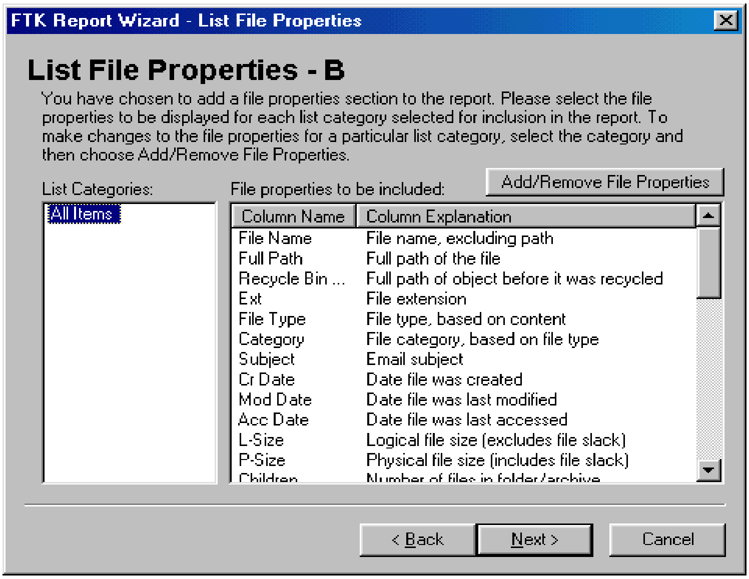
5 If you want to export and link to the files in the File Properties list, check the **Export to the Report** box.

6 If you want to use a filter to manage which files appear in the File Properties list, check the **Apply a File Filter to the List** box and select the filter from the **Filter Name** drop-down list.

7 Click **Next**.

Selecting the Properties of the File Properties List

The List File Properties-B form allows you to select which file properties are displayed for files in the categories specified in the previous form. This form only appears if you chose to create the List File Properties section in the report.


FTK Report Wizard - List File Properties
Add/Remove File Properties
< Back
Next >
Cancel

List File Properties - B

You have chosen to add a file properties section to the report. Please select the file properties to be displayed for each list category selected for inclusion in the report. To make changes to the file properties for a particular list category, select the category and then choose Add/Remove File Properties.

List Categories:

All Items

File properties to be included:

Column Name	Column Explanation
File Name	File name, excluding path
Full Path	Full path of the file
Recycle Bin ...	Full path of object before it was recycled
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 modified
Acc Date	Date file was last accessed
L-Size	Logical file size (excludes file slack)
P-Size	Physical file size (includes file slack)
Children	Number of files in folder/archive

In the List File Properties-B form:

1 From the **List Categories** column, select the category that you want to specify file properties for and review the properties listed for it.

You can specify different file properties for each category.

2 In the **Load from Stored Column Settings** drop-down list, select the template that contains the file information that you want to include in the report.

3 If you want to define a new column settings template:

3a Check or uncheck the Column Names, depending on which ones you want to include in the setting.

You can click **Select All** or **Unselect All** to mark or unmark all the columns.

3b To change the order in which the columns appear in the File List, select a column name and click **Move Up** or **Move Down**.

3c To create a new column setting, click **Save As**, enter a name in the field, and click **OK**.

4 If you want to modify an existing template:

4a Click **Columns**.

4b Select the column setting you want to modify.

4c Modify the Column Settings form.

4d Click **Save**, then **Close**, and then **OK**.

For more information about the Column Settings form, see "Customizing Columns" on page 249.

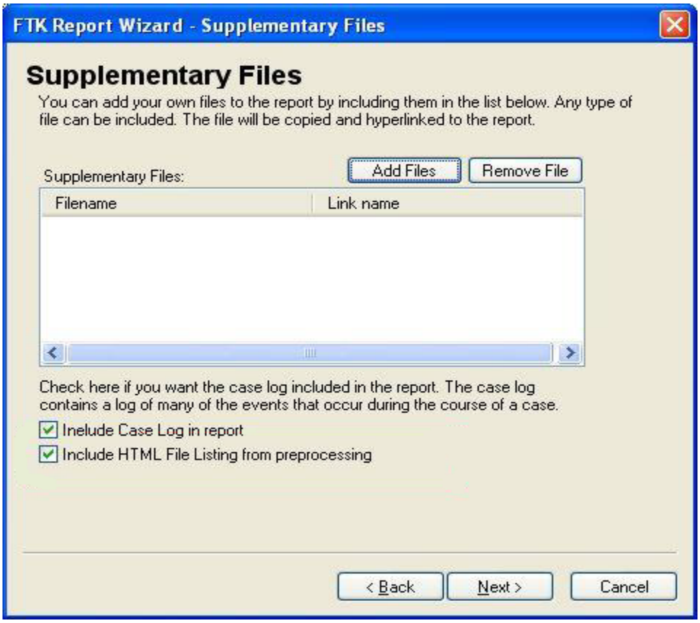
5 Click **Next**.

Note: If the exported item has a bad or missing extension and FTK is able to determine the correct extension, FTK appends the correct extension to the exported file. The description of the file in the report is unchanged, but the actual exported file and the link in the report to the exported file have the correct extension appended. The person viewing the report clicks the link to have Windows detect the correct application with which to open the exported file.

Adding Supplementary Files and the Case Log

The Supplementary Files form allows you to add files such as hash lists or search results to the report.

You can also add the case log to the report. The case log documents activities that occur on the case during its investigation and analysis.



FTK Report Wizard - Supplementary Files

Supplementary Files

You can add your own files to the report by including them in the list below. Any type of file can be included. The file will be copied and hyperlinked to the report.

Supplementary Files:

Filename	Link name

Check here if you want the case log included in the report. The case log contains a log of many of the events that occur during the course of a case.

☑ Include Case Log in report

☑ Include HTML File Listing from preprocessing

In the Supplementary Files form:

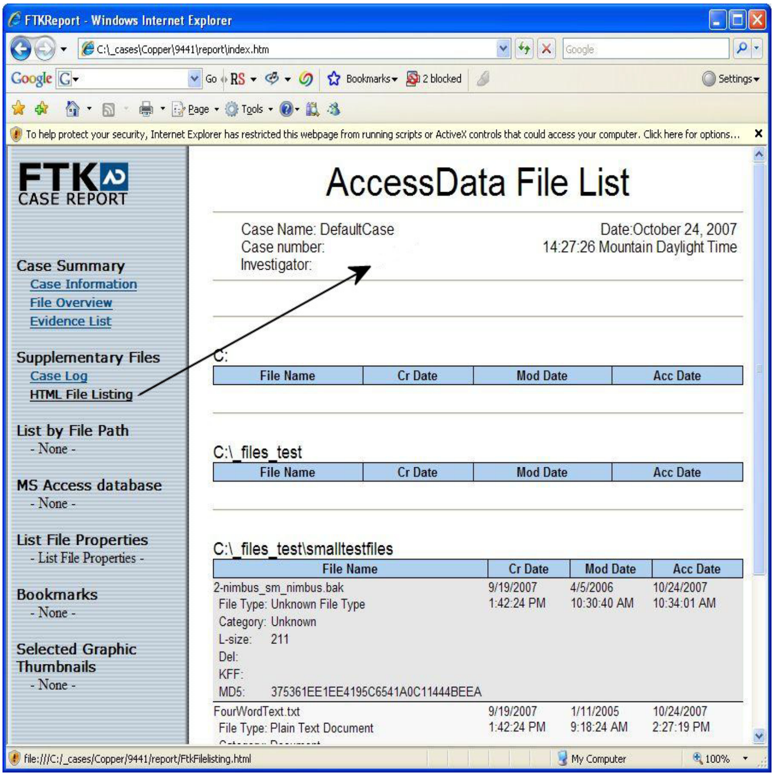
1 If you want to add an supplementary file, click **Add Files** and browse to the file you want to include in the report.

Files listed in the Supplementary Files window are copied to the report folder so they are available within the report.

2 If you want to remove a file, select the file in the Supplementary Files window and click **Remove File**.

3 If you want to add the case log to the report, check the **Include Case Log in Report** box.

4 If you created an HTML file list in preprocessing, you can add it to your reports.


FTKReport - Windows Internet Explorer
C:_cases\Copper\9441\report\index.htm
Google
Go
RS
Bookmarks
2 blocked
Settings
Page
Tools
To help protect your security, Internet Explorer has restricted this webpage from running scripts or ActiveX controls that could access your computer. Click here for options...
FTK
CASE REPORT
file:///C:/_cases/Copper/9441/report/FtkFilelisting.html
My Computer
100%

Case Summary
- Case Information
- File Overview
- Evidence List

Supplementary Files
- Case Log
- HTML File Listing

List by File Path
- None -

MS Access database
- None -

List File Properties
- List File Properties -

Bookmarks
- None -

Selected Graphic Thumbnails
- None -

AccessData File List

Case Name: DefaultCase
Case number:
Investigator:

Date:October 24, 2007
14:27:26 Mountain Daylight Time

C:

File Name	Cr Date	Mod Date	Acc Date

C:_files_test

File Name	Cr Date	Mod Date	Acc Date

C:_files_test\smalltestfiles

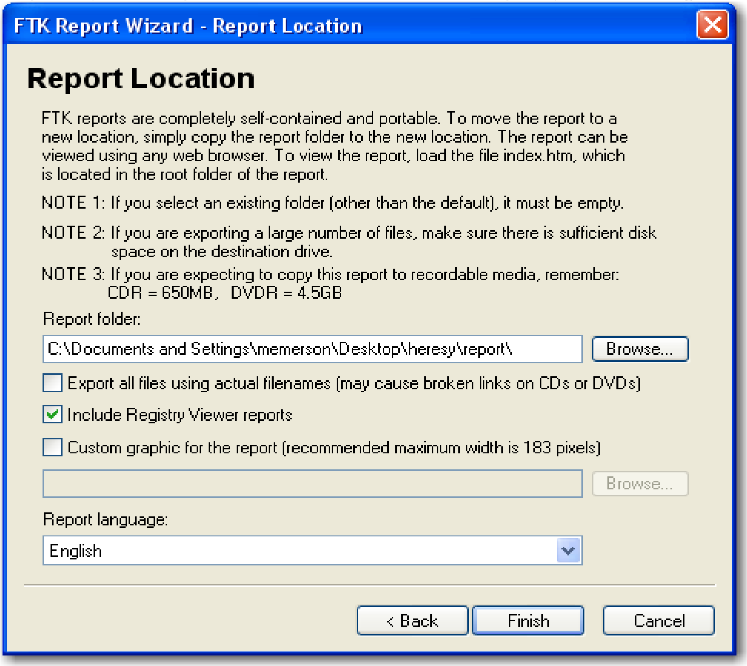
File Name	Cr Date	Mod Date	Acc Date
2-nimbus_sm_nimbus.bak File Type: Unknown File Type Category: Unknown L-size: 211 Del: KFF: MD5: 375361EE1EE4195C6541A0C11444BEEA	9/19/2007 1:42:24 PM	4/5/2006 10:30:40 AM	10/24/2007 10:34:01 AM
FourWordText.txt File Type: Plain Text Document	9/19/2007 1:42:24 PM	1/11/2005 9:18:24 AM	10/24/2007 2:27:19 PM

5 Click **Next**.

Note: The case log is best viewed through a text editor capable of large files.

Selecting the Report Location

The Report Location form allows you to select the location of the report. You can also add a customized graphic, such as the logo of your organization, and include Registry Viewer reports.



Report Location

FTK reports are completely self-contained and portable. To move the report to a new location, simply copy the report folder to the new location. The report can be viewed using any web browser. To view the report, load the file index.htm, which is located in the root folder of the report.

NOTE 1: If you select an existing folder (other than the default), it must be empty.

NOTE 2: If you are exporting a large number of files, make sure there is sufficient disk space on the destination drive.

NOTE 3: If you are expecting to copy this report to recordable media, remember: CDR = 650MB, DVDR = 4.5GB

Report folder: C:\Documents and Settings\memerson\Desktop\heresy\report\

□ Export all files using actual filenames (may cause broken links on CDs or DVDs)

☑ Include Registry Viewer reports

□ Custom graphic for the report (recommended maximum width is 183 pixels)

Report language: English

Note: For more information on Registry Viewer, see “Securing Windows Registry Evidence” on page 315.

In the Report Location form:

1 In the **Report Folder** field, browse to and select the location for the report folder.

  The default location is the *case_name*\report\ directory. The report consists of several files with default filenames. If you select a different directory, the directory must be empty.

  If you are exporting a large number of files, make sure that there is sufficient drive space in the destination directory.

2 If you have created registry reports in Registry Viewer or FTK, check the **Include Registry Viewer Reports** box to include those reports in your FTK case report. This

includes any Registry Summary Reports (RSRs) you have created and selected in FTK.

3 If you want to include a custom graphic in the report, check the **Custom Graphic for the Report** box. Click **Browse** to select the graphic from the directory tree.

The graphic appears at the top of the report's left frame.

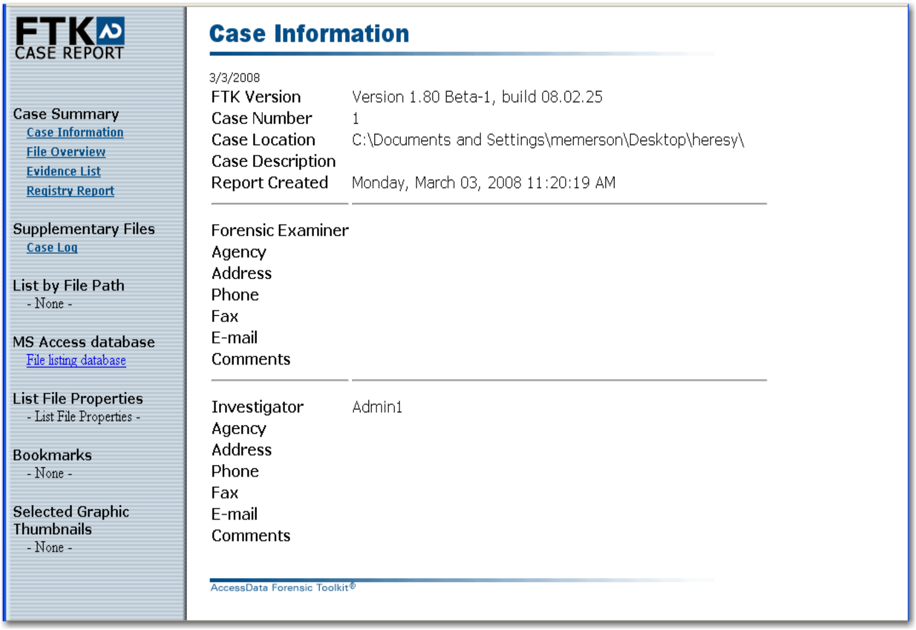
The recommended maximum width of the graphic is 183 pixels.

4 Select the language for the report from the Report Language drop-down list.

5 Click **Finish**.

Viewing and Distributing a Report

The report contains the information that you selected in the Report Wizard. An example of the main page of the report (index.htm) is shown above. When bookmarked for inclusion in the report, files appear in both raw data format and in HTML format depending on the file type. A link also allows any RSRs you created to be viewed by clicking on the **Registry Report** link.



Case Information

3/3/2008

FTK Version	Version 1.80 Beta-1, build 08.02.25
Case Number	1
Case Location	C:\Documents and Settings\memerson\Desktop\heresy\
Case Description	
Report Created	Monday, March 03, 2008 11:20:19 AM

Forensic Examiner	
Agency	
Address	
Phone	
Fax	
E-mail	
Comments	

Investigator	Admin1
Agency	
Address	
Phone	
Fax	
E-mail	
Comments	

AccessData Forensic Toolkit®

To view the report in FTK:

- Immediately after creating the report, click **Yes** to view the report.
- Select **File**, and then **View Report**. Browse to and select the \case_name\\report\\ directory.

To view the report outside FTK, you can browse to the Report directory and open index.htm in your Web browser.

To disseminate the report, you must include all the files within the case Report directory. To view the report, users can simply open index.htm in their browsers.

If you are distributing the report via CD, copy the contents of the Report directory and burn the files to the root of the CD. This allows you to leverage the FTK report autorun. The autorun automatically launches the report's main page (index.htm) in the user's default browser when the CD is read on a Windows computer.

Note: The Windows computer must be configured to automatically execute autorun files.

Updating a Report

If you have already created a report and then modify the case in any way, such as adding an evidence item, you need to update the report.

When you update the report, only sections you originally included in the Report Wizard will be updated. For example, if you add a graphic to the case and you chose to add a thumbnail of all graphics in the Report Wizard, the update will add only the thumbnail of the new graphic.

To update a report, select **File**, and then **Update Report**. You can select Update Report only if a report has been created.

If you want to change the sections that you included in the report, see "Modifying a Report" on page 242.

Modifying a Report

If you want to change any of the selections that you made in the Report Wizard, you can modify the report.

You can modify reports in the same FTK session, or from a different FTK session.

Note: To be in the same FTK session means that you haven't closed the case, you haven't exited FTK, and you haven't turned off the computer.

Each option is discussed in the following sections.

Modifying a Report in the Same FTK Session

If you are in the same FTK session as the initial report creation, your report settings are still listed in the Report Wizard. You can modify the report by changing your listed selections.

To modify the report:

1. Select **File**, and then **Report Wizard**.
2. Make the changes that you want as you complete the wizard.

   For instructions on using the wizard, see "Creating a Report" on page 222.
3. On the Report Location form, click **Finish** to overwrite the existing report with the new version.

   If you want to keep the existing report and create a new report, browse to and select a different report folder. You cannot simply rename the report file and keep it in the same directory because you cannot define the filenames.

Modifying a Report in a Different FTK Session

If you are in a different FTK session from that in which the report was created, you need to create a new report. The existing Report Wizard settings are not listed by default.

To modify the report:

1 Select **File**, and then **Report Wizard**.

2 Complete the wizard.

For instructions on using the wizard, see "Creating a Report" on page 222.

3 On the Report Location form, click **Finish** if you want to overwrite the existing report with the new version.

If you want to keep the existing report and create a new report, browse to and select a different report folder.

CHAPTER 14

Customizing FTK

You can customize certain parts of the Forensic Toolkit (FTK) interface. You can also change some default settings, such as the temporary file location.

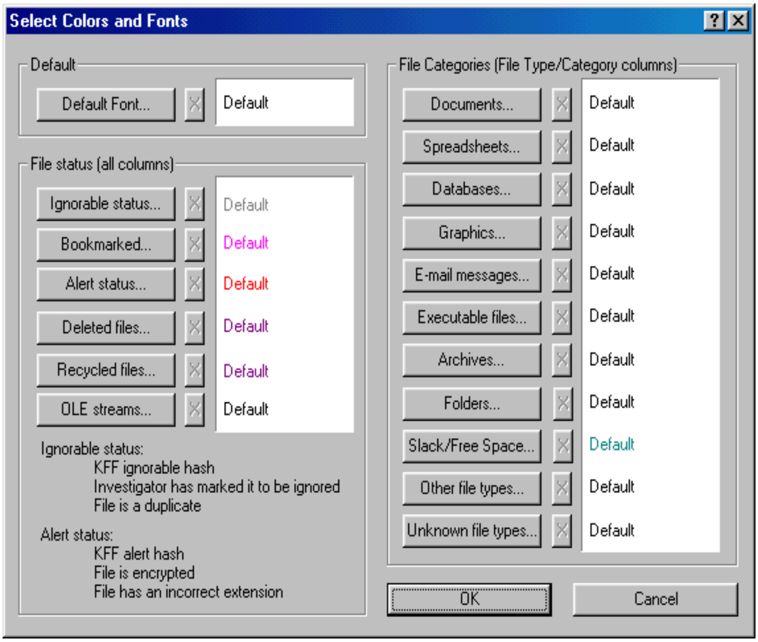
The customization features are discussed in the following sections:

- "Customizing Fonts and Colors" on page 245
- "Customizing Columns" on page 249
- "Changing the Viewer Settings" on page 253
- "Changing Preferences" on page 255

Customizing Fonts and Colors

The Select Colors and Fonts form allows you to customize the fonts and font colors used to designate file status or file categories. Changing the font or color of a file status or category is an easy way to flag files of interest.

The FTK font selections are hierarchical, so some selections override others. Items at the top of the form have the highest priority while items at the bottom of the form have the lowest priority.

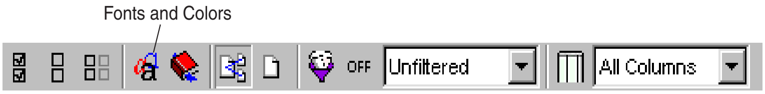


Ignorable status:
- KFF ignorable hash
- Investigator has marked it to be ignored
- File is a duplicate

Alert status:
- KFF alert hash
- File is encrypted
- File has an incorrect extension

All color and font settings are saved in the ftksettings.ini file, located in the \AccessData\AccessData Forensic Toolkit\Program\ directory.

You can select the colors and fonts by clicking on the following icon on the File List toolbar, shown below:



The following tables outline the file status and categories to which you can assign custom fonts and colors:

File Status	Description
Alert Status	Files that are a KFF alert hash or encrypted or that have an incorrect extension.
Bookmarked	Files that you bookmarked in FTK.
Deleted Files	Complete files or folders recovered from slack or free space.
Ignorable Status	Files that are a KFF ignorable hash or a duplicate file or that are marked ignorable.
OLE Streams	Items or pieces of information, such as text or graphics, that were embedded in a file or an entire file.
Recycled Files	Files retrieved from the Windows recycled/recycler file structure.

Category	Description
Archives	Archive files include e-mail archive files, Zip, Stuffit,Thumbs.db thumbnail graphics, and other archive formats. For a complete list of file types recognized by FTK, see “Archive File Types” on page 291.
Databases	Includes databases from Access, Quicken, Microsoft Money, QuickBooks, and others. For a complete list of database file types recognized by FTK, see “Database File Types” on page 286.

Category	Description
Documents	Includes most word processing, HTML, WML, HDML, or text files. For a complete list of document file types recognized by FTK, see "Document File Types" on page 282.
E-mail Messages	Includes e-mail messages from Outlook, Outlook Express, AOL, Netscape, Yahoo, Earthlink, Eudora, Hotmail, and MSN. For a complete list of e-mail message file types recognized by FTK, see "E-mail Message Programs" on page 290.
Executable Files	Includes executables from Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats. For a complete list of executable file types recognized by FTK, see "Executable File Types" on page 291.
Folders	Folders and directories.
Graphics	Includes the standard graphic formats like .tif, .gif, .jpeg, and .bmp. For a complete list of graphic file types recognized by FTK, see "Graphic File Types" on page 288.
Other File Types	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, etc. For a complete list of other file types recognized by FTK, see "Other Known File Types" on page 293.
Slack/Free Space	Fragments of files that have not been completely overwritten.
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, Quattro Pro, and others. For a complete list of spreadsheet file types recognized by FTK, see "Spreadsheet File Types" on page 285.
Unknown File Types	File types that FTK cannot identify.

To customize the fonts and colors used to display file status or category:

1 Select **View**, and then **Colors and Fonts**, or click the Colors and Fonts icon on the File List toolbar.

2 To change the default font:

   2a Click **Default Font**.

   2b In the **Font** dialog, select the font options you want to use as the general default display.

   2c Click **OK**.

3 To change the font or color for a specific file status or category:

   3a Click the file status or category button.

   3b In the **Font** dialog, select the font options you want to use to display the current file status or category.

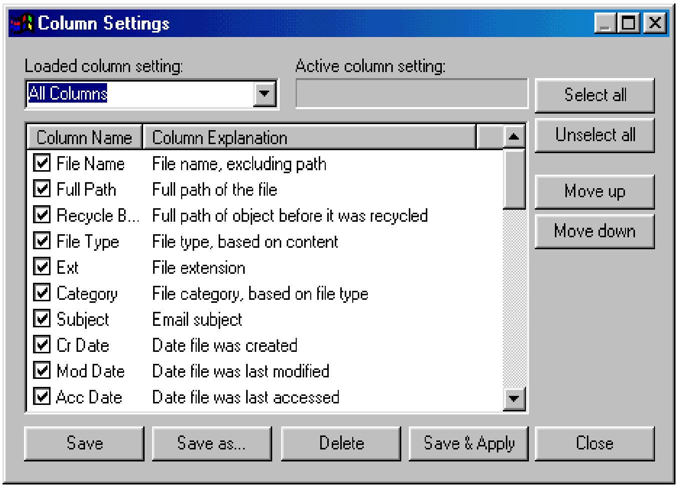
4 To reset the display font for any option, click the **X** button next to the option.

5 Click **OK**.

Customizing Columns

The Column Settings form allows you to modify existing column settings or create new column settings. Column settings define what information is displayed in the File List, and in what order it is displayed. Column settings also define what file information appears in the Bookmark and List File Properties sections of case reports.

The File List properties also create a Microsoft Access (JET) database containing the files of the case. The attributes included are based on the column settings you choose.



Loaded column setting: All Columns

Active column setting:

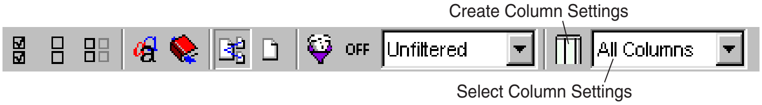
Column Name	Column Explanation
☑ File Name	File name, excluding path
☑ Full Path	Full path of the file
☑ Recycle B...	Full path of object before it was recycled
☑ File Type	File type, based on content
☑ Ext	File extension
☑ Category	File category, based on file type
☑ Subject	Email subject
☑ Cr Date	Date file was created
☑ Mod Date	Date file was last modified
☑ Acc Date	Date file was last accessed

Using custom column settings, you can narrow the information provided in the File List and case reports. For example, if you are analyzing e-mail, you can choose to only display columns that are relevant to e-mail.

Custom column settings are saved in the ftkcolumnsettings.ini file, located in the \AccessData\AccessData Forensic Toolkit\Program\ directory.

Note: You can access your custom column settings on other machines by copying the ftkcolumnsettings.ini file to the computer’s \AccessData\AccessData Forensic Toolkit\Program\ directory. This will, however, overwrite the custom column settings on the target machine. (This does not impact the default column settings.)

You can create and apply column settings by clicking on the following icons on the File List toolbar, shown below:



Note: You can apply a different column setting in each window.

The column setting "Preprocessing File Listing Database Column Setting" is available when you select the **File Listing Database** option from the Processes to Perform dialog in the evidence wizard. With this setting, you can modify your columns and then return to your default set.

To return to the default set of values, delete the entry from the column settings manager, and restart FTK. The Default File List Column Settings entry is applied again.

Modifying the File Listing Database

The Microsoft Access (Jet) database containing a list of only actual files in the case, or files that existed on the original hard drive as files: documents, zip files, executables, logs, etc.

You can expand the File Listing database to contain all files in the case, or those items parsed and extracted such as the contents of a zip file, or the messages from an email archive, or OLE streams that are part of Office docs; anything that didn't have it's own entry in Windows Explorer.

To increase the files listed in the File Listing database, you must shut down the FTK program, and then edit the FtkSettings.0.ini file:

1. Open the FtkSettings.0.ini file, and find the [Global] section.
2. In the [Global] section, find the PreprocessListsAllFiles key, and then set the value from 0 to 1.
3. Save the changes, and restart FTK.

The new File Listing database and the HTML version will now include all files.

Important: The File Listing database file's size will increase substantially.

Creating and Modifying Column Settings

To modify or create a column setting:

1 Select **View**, and then **Column Settings**, or click on the Column Settings icon in the File List toolbar.

Note: You cannot access the Column Settings form when viewing Evidence Items in the Overview window.

2 In the **Loaded Column Setting** drop-down list, select the column setting that you want to modify, or select the column setting that you want to use as a baseline for your new column setting.

3 Mark the columns that you want to display in the File List.

You can click **Select All** or **Unselect All** to quickly mark or unmark all the columns.

4 Select a column name and click **Move Up** or **Move Down** to change the order that the columns appear in the File List.

5 Save your column setting:

5a To save your changes to an existing column setting, click **Save**.

5b To save your changes and immediately apply a column setting, click **Save and Apply**.

Note: You can also apply the column setting from the Column Setting drop-down list on the File List toolbar.

5c To create a new column setting, click **Save As**, enter the column setting name, and click **OK**.

6 Click **Close**.

Deleting Column Settings

To delete a column setting:

1 Select **View**, and then **Column Settings**, or click on the Column Settings icon in the File List toolbar.

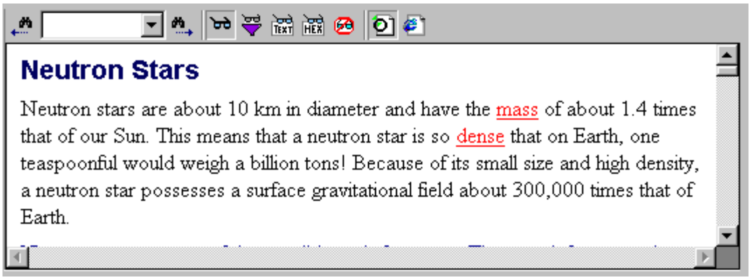
Note: You cannot access the Column Settings form when viewing Evidence Items in the Overview window.

2 In the **Loaded Column Setting** drop-down list, select the column setting that you want to delete.

3 Click **Delete**, and then **Close**.

Changing the Viewer Settings

By default, the main viewer in FTK is set to view items as if they were in their native application. However, you can change the default to view items in hex, raw (text), or filtered views. You can also turn off the viewer to speed up FTK performance because it can be time-consuming to load large files in the viewer.



Neutron Stars

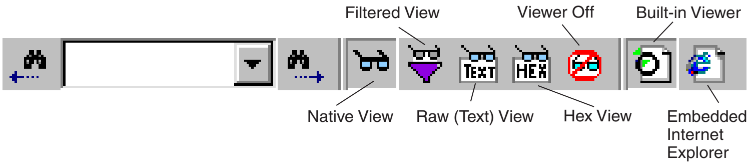
Neutron stars are about 10 km in diameter and have the mass of about 1.4 times that of our Sun. This means that a neutron star is so dense that on Earth, one teaspoonful would weigh a billion tons! Because of its small size and high density, a neutron star possesses a surface gravitational field about 300,000 times that of Earth.

To change the viewer settings, select **View**, and then **Viewer** and select one of the following:

Setting	Description
Built-in Viewer	Displays the file using the Outside In Viewer (built-in viewer).
Filtered View	Displays the file in filtered text mode. Readable text is filtered out of binary files.
Hex View	Displays the file in the viewer in hex format.

Setting	Description
Internet Explorer	Uses embedded Internet Explorer to view the file.
Native View	Displays the file in the viewer as if in native format.
Raw View	Displays the file in the viewer in text format.
Viewer Off	Disables the viewer.

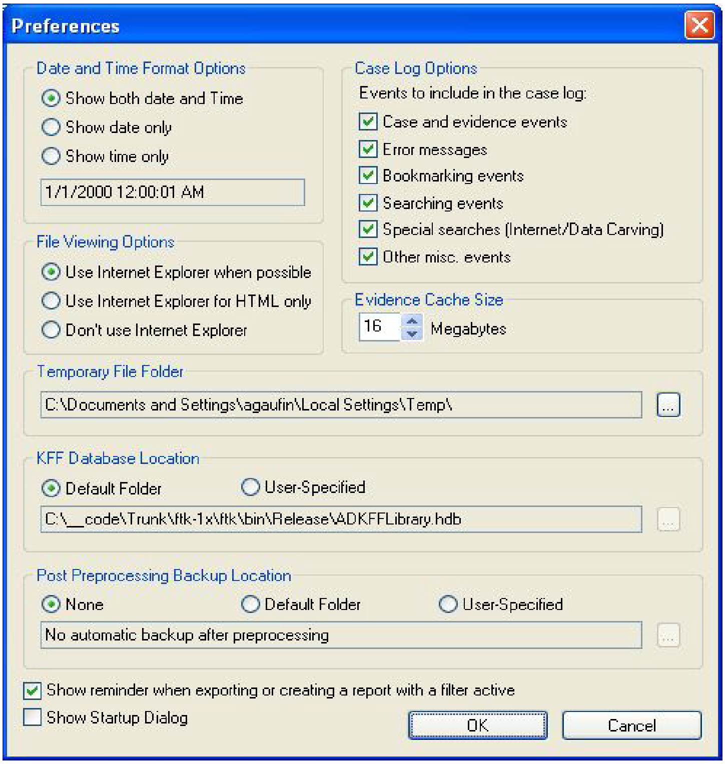
To change the view, you can also click on the appropriate icon in the Viewer toolbar, shown below:



Changing Preferences

To change FTK Preferences, click **Tools**, and then **Preferences**.

On the Preferences form, you can change various options, such as how the date and time are displayed for evidence items or the location of a temporary file folder.



Preferences

Date and Time Format Options

● Show both date and Time
○ Show date only
○ Show time only

1/1/2000 12:00:01 AM

Case Log Options

Events to include in the case log:

☑ Case and evidence events
☑ Error messages
☑ Bookmarking events
☑ Searching events
☑ Special searches (Internet/Data Carving)
☑ Other misc. events

File Viewing Options

● Use Internet Explorer when possible
○ Use Internet Explorer for HTML only
○ Don't use Internet Explorer

Evidence Cache Size

16 Megabytes

Temporary File Folder

C:\Documents and Settings\agaufin\Local Settings\Temp\

KFF Database Location

● Default Folder ○ User-Specified

C:\__code\Trunk\ftk-1x\ftk\bin\Release\ADKFFLibrary.hdb

Post Preprocessing Backup Location

● None ○ Default Folder ○ User-Specified

No automatic backup after preprocessing

☑ Show reminder when exporting or creating a report with a filter active

☐ Show Startup Dialog

Preference settings are saved in the ftksettings.ini file. This file is located in the \AccessData\AccessData Forensic Toolkit\Program\ directory.

The following sections review the options on the Preferences form.

Date and Time Format Options

The Date and Time Format Options determines what information FTK provides in evidence items' time and date fields.

The following table outlines the available options:

Option	Description
Show Both Date and Time	Displays both date and time (such as the creation and modification dates and times) for an evidence item in the appropriate file list columns.
Show Date Only	Displays only the date (such as the creation and modification dates) for an evidence item in the appropriate file list columns. Select this option if you only need to view the evidence dates.
Show Time Only	Displays only time (such as the creation and modification times) for an evidence item in the appropriate file list columns. You may select this option if the evidence is primarily from one day and you are investigating the times.

File Viewing Options

The File Viewing Options determines how FTK uses Internet Explorer to view files.

The following table outlines the available options:

Option	Description
Don’t Use Internet Explorer	Doesn’t display any evidence items in the embedded Internet Explorer viewer.
Use Internet Explorer for HTML Only	Displays HTML files in the embedded Internet Explorer viewer.
Use Internet Explorer When Possible	Displays evidence items in an embedded Internet Explorer viewer if the item can be displayed in a browser. This option is good for animated graphics.

Case Log Options

The Case Log Options determine what items are included in the case log.

The following table outlines the available options:

Option	Description
Bookmarking Events	Events related to the addition and modification of bookmarks.
Case and Evidence Events	Events related to adding and processing file items when evidence is added or related to using the Analysis Tools at a later time.
Error Messages	Events related to any error conditions encountered during the case.
Other Misc Events	The following events: ◆ Using the copy special feature ◆ Exporting files ◆ Viewing items in the detached viewer ◆ Ignoring and unignoring files
Searching Events	All search queries and resulting hit counts.

Option	Description
Special Searches	Events related to data carving or Internet keyword searches performed during the case.

Creating a Mini Log

You can create a log file with fewer entries than the more comprehensive FTK.log file. This smaller log contains:

- Added Bookmarks
- Addition to Bookmarks
- Case Closings
- Case Loadings
- Case Path
- Case Start
- Case Title
- Data CarveExported Files
- Deleted Bookmarks
- Examiner's Name
- FTK Version
- Internet Keyword Search
- Investigator's Name
- KFF Databases
- List Bookmarked Files
- List Bookmarked Terms
- List Search Terms
- Live Search Terms
- Search Terms

To create a mini log file, you must shut down the FTK program, and then edit the FtkSettings.0.ini file:

1. Open the FtkSettings.0.ini file, and find the [Global] section.
2. In the [Global] section, find the CreateMiniLog key, and then set the value from 0 to 1.
3. Save the changes, and restart FTK.

The new mini log will be generated with the regular FTK log, and saved in the same directory.

Evidence Cache Size

The evidence cache increases performance when viewing case files on a local drive. This setting determines how much RAM is allocated for the evidence cache.

Temporary File Folder

The temporary file folder stores temporary files, including files extracted from Zip and e-mail archives. The folder is also used as scratch space during text filtering and indexing. FTK frequently uses the temporary file folder.

KFF Database Location

By default, the KFF database (ADKFFLibrary.hdb) installs to the FTK program folder (\AccessData\AccessData Forensic Toolkit\Program\). If you install the KFF database to another location, you must specify where to find it.

The following table outlines the available options:

Location	Description
FTK Program Folder	The KFF database is placed in the same directory as the FTK program. This is the default setting.
User-Specified	Browse to and select the location for the KFF database.

Post Processing Backup Location

The FTK program can automatically backup a case following preprocessing. The backup is saved in a directory named after the case directory, but with “_bak” appended to the case name.

You can use the default location to store your backup, or you can select another location.

Option	Description
None	Does not make a backup automatically.
Default Folder	Makes a backup automatically, and saves it to a sibling folder with "_bak" appended to the case name.
User-Specified	Makes a backup automatically, and saves it to the location specified with "_bak" appended to the case name.

Important: To speed up the copying process, the backup does not include the Thmbldx directory.

Show Reminder when Exporting or Creating a Report with Filter Active

If you want to display a remider that there is an active filter applied to the case when you are exporting or creating a report, check the **Show Reminder When Exporting or Creating a Report with a Filter Active** box.

Show Startup Dialog

If you want the Startup dialog box to appear each time that you open FTK, check the **Show Startup Dialog** box.

The Startup dialog includes the following options:

Option	Description
Do Not Show This Dialog on Startup	Disables the Startup dialog box on all subsequent openings of FTK.
Go Directly to Working in Program	Opens FTK with no case loaded.
Open an Existing Case	Opens a window to browse to and select the *case*.ftk file for the case that you want to work on.
Preview Evidence	Launches FTK Imager.

Option	Description
Start a New Case	Starts the New Case Wizard.

CHAPTER 15

Managing Licenses

This chapter acquaints you with the LicenseManager interface and describes how to manage licenses and update products using LicenseManager.

The chapter is divided into the following sections:

- "Managing Licenses with LicenseManager" on page 263
- "LicenseManager Interface" on page 264
- "Managing Product Licenses on Isolated Machines" on page 270
- "Updating Products" on page 273
- "Purchasing Product Licenses" on page 274

Managing Licenses with LicenseManager

LicenseManager lets you manage product licenses on a dongle or in a dongle packet file.

With LicenseManager, you can view license information, add or remove existing licenses to a dongle or dongle packet file, renew subscriptions, purchase licenses, and send a dongle packet file to AccessData support. You can also check for product updates and download the latest product versions.

LicenseManager displays dongle information (including packet version and serial number) and licensing information for such products as FTK, PRTK, DNA, and Registry Viewer.

The licensing information provides the following:

- Name of programs

- Versions of programs
- Subscription expiration date
- Number clients

Starting LicenseManager

LicenseManager.exe is located in the C:\Program Files\AccessData\Common Files\AccessData LicenseManager directory. When you start LicenseManager, it reads licensing and subscription information from your dongle.

From the Tools menu, click **LicenseManager**. The LicenseManager program opens.

If you are using a dongle, and LicenseManager either does not open or display the message, Dongle Not Found:

- Make sure the dongle drivers are installed.
- Make sure the dongle is connected to the USB port.

If you do not have a dongle installed, LicenseManager lets you manage licenses using a dongle packet file.

To open LicenseManager without a dongle installed:

1. From the Tools menu, click **LicenseManager**.

   LicenseManager displays the message: “Dongle not Found.”

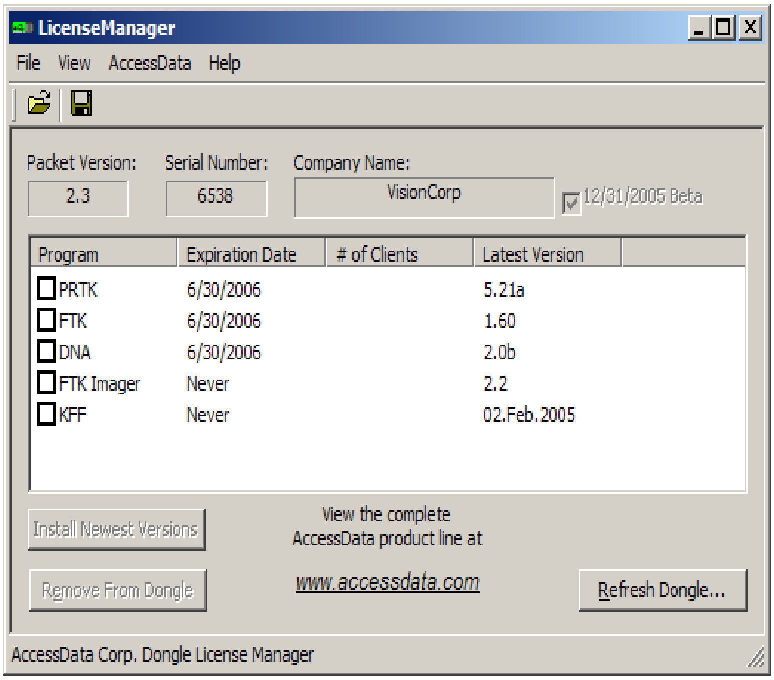
2. Click **OK**, then browse for a dongle packet file to open.

LicenseManager Interface

The LicenseManager interface consists of two tabs that organize the options in the LicenseManager window: the Installed Components tab, and the Licenses tab.

The Installed Components Tab

The Installed Components tab lists the AccessData programs installed on your machine.



LicenseManager
File View AccessData Help

Packet Version: 2.3

Serial Number: 6538

Company Name: VisionCorp

☑ 12/31/2005 Beta

Program	Expiration Date	# of Clients	Latest Version
□ PRTK	6/30/2006		5.21a
□ FTK	6/30/2006		1.60
□ DNA	6/30/2006		2.0b
□ FTK Imager	Never		2.2
□ KFF	Never		02.Feb.2005

Install Newest Versions
View the complete AccessData product line at
Remove From Dongle
www.accessdata.com
Refresh Dongle...
AccessData Corp. Dongle License Manager

From the Installed Components tab, you can the following information:

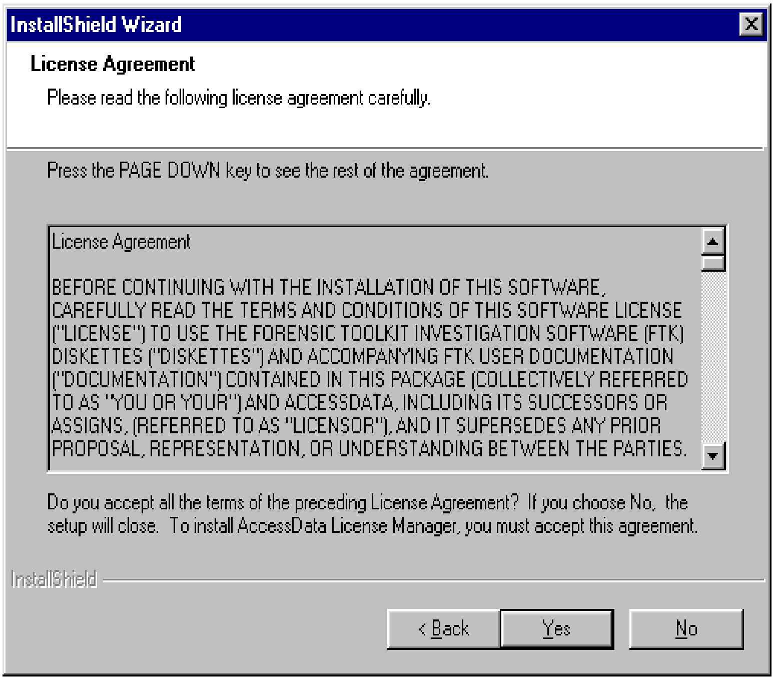
Item	Description
Program	Shows a list of AccessData products installed on the host.
Installed Version	Shows the version of each AccessData product installed on the host.
Newest Version	Shows the latest version available of each AccessData product installed on the host.
Product Notes	Displays notes and information about the product selected in the product window

Item	Description
AccessData Link	Brings up the AccessData product page from which you can learn more about AccessData products.
Install Newest Button	Installs the newest version of the programs checked in the product window.
Newest Button	Downloads a list of AccessData's available products and their latest versions.

Use the Installed Components tab to manage your AccessData products and stay up to date on new releases.

The Licenses Tab

The Licenses tab displays dongle information for the current dongle packet file and licensing information for available AccessData products.



License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

License Agreement

BEFORE CONTINUING WITH THE INSTALLATION OF THIS SOFTWARE, CAREFULLY READ THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE ("LICENSE") TO USE THE FORENSIC TOOLKIT INVESTIGATION SOFTWARE (FTK) DISKETTES ("DISKETTES") AND ACCOMPANYING FTK USER DOCUMENTATION ("DOCUMENTATION") CONTAINED IN THIS PACKAGE (COLLECTIVELY REFERRED TO AS "YOU OR YOUR") AND ACCESSDATA, INCLUDING ITS SUCCESSORS OR ASSIGNS, (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install AccessData License Manager, you must accept this agreement.

The Licenses tab provides the following information:

Column	Description
Program	Shows the AccessData products for which you own a license.
Expiration	Shows the date on which your current license expires.
Status	Shows these statuses: ◆ None: the product license isn't currently owned ◆ Days Left: displays when less than 31 days remain ◆ Never: you own the license permanently

Column	Description
Name	Shows the name of additional parameters or information a product requires for its license.
Value	Shows the values of additional parameters or information a product requires for its license.
Show Unlicensed Checkbox	When checked, the License window displays products for which you don't currently own a license.

You can perform the following license management in the License tab:

Button	Function
Remove License	Removes a license from the Licenses window.
Reload Dongle	Click to start the program reading the dongle attached to your machine (Release Dongle).
Refresh Dongle	Loads the information from the Licenses window to the dongle.
Release Dongle	Click to stop the program reading the dongle attached to your machine, much like Windows' Safely Remove Hardware feature. Click this button before removing a dongle.
Open Packet File	Opens Windows Explorer, allowing you to navigate to a .pkt file containing your license information.
Save to File	Opens Windows Explorer, allowing you to save a .pkt file containing your license information.
Finalize Removal	Removes any licenses you checked in the Licenses window.
View Registration Info	Displays an HTML page with your Dongle number and other license information.
Add Existing License	Allows you to associate a new license to your dongle, and download it from AccessData.
Purchase License	Brings up the AccessData product page from which you can learn more about AccessData products.

Opening and Saving Dongle Packet Files

You can open or save dongle packet files using LicenseManager.

To open a dongle packet file:

1. From the Licenses tab, click **Open Packet File**.
2. Browse for a dongle packet file to open, then click **Open**.

To save a dongle packet file:

1. From the Licenses tab, click **Save to File**.
2. Specify the folder and name of the .pkt file, then click **Save**.

Note: When started, LicenseManager attempts to read licensing and subscription information from your dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file.

Viewing Product Licenses

LicenseManager lets you view product license information for products registered (or associated) with your dongle or dongle packet file.

To view product licenses that are associated with a dongle, click **Reload from Dongle**.

To view all available product licenses that are or can be associated with a dongle (according to Website database), click **View Registration Info**.

To synchronize your dongle with the product license information in the AccessData Website database, click **Refresh Dongle**.

Adding and Removing Product Licenses

On a computer with an Internet connection, LicenseManager lets you add or remove available product licenses on a dongle.

To add, or “associate,” a product license:

1. From the Licensing tab, click **Add Existing License**.

2. On the Website page, select the product license you want to add. After an update file downloads and installs, click **OK**.
3. Click **Yes** when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”

To remove, or “unassociate,” a product license, check the program licenses you want to remove, and then click **Finalize Removal**.

The message, “Removal of licenses from dongle (your dongle number) was successful” is displayed.

Managing Product Licenses on Isolated Machines

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer that does not have an Internet connection, such as a lab computer.

When you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, then physically move the dongle back to the original computer. However, if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

To remotely add or remove product licenses, you must transfer the dongle packet file to a computer with an Internet connection so you can open the dongle packet file and add or remove product licenses. You must then copy and run the update file on the original computer where the dongle resides.

To remotely move a product license from one dongle to another dongle, first remove the product license from the dongle packet file to a computer with an Internet connection, copy and update the file on the computer where the dongle you want to change resides, then add the unassociated product license to the other dongle.

Adding a Product License to an Isolated Machine

To add (associate) a product license:

1 On the computer where the dongle resides:

1a Click **Reload from Dongle** in the Licenses tab to read the dongle license information.

1b Save the dongle packet file to the local machine.

2 Copy the dongle packet file to a computer with an Internet connection.

3 On the computer with an Internet connection:

3a Open the copied dongle packet file in LicenseManager.

3b Click **Add Existing License**. Do not answer the prompt; complete instead the process to add a product license on the Website page.

3c Click **Yes** when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”

When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file (an executable).

4 After the update file is downloaded, copy the update file to the computer where the dongle resides:

5 On the computer where the dongle resides:

5a Run the update file.

5b Click **Reload From Dongle** in the Licenses tab to verify the product license has been added to the dongle.

Note: On the computer with an Internet connection, click **View**, and then **Registration Info** in LicenseManager to license information for associated and unassociated product licenses.

Removing a Product License from an Isolated Machine

To remove (unassociate) a product license:

1 On the computer where the dongle resides:

1a Click **Reload from Dongle** in the Licenses tab to read the dongle license information.

1b Save the dongle packet file to the local machine.

2 Copy the file to a computer with an Internet connection.

3 On the computer with an Internet connection:

3a Open the copied dongle packet file in LicenseManager.

3b Select the product license you want to unassociate, then click **Remove License**.

3c When prompted to remove the selected license from the dongle, click **Yes**.

When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.

3d Save the update file to the local machine.

4 After the update file is downloaded, copy the update file to the computer where the dongle resides.

5 On the computer where the dongle resides:

5a Run the update file.

5b Click **Reload From Dongle** in the Licenses tab to verify the product license is removed from the dongle.

5c Save the dongle packet file to the local machine.

6 Copy the file to a computer with an Internet connection.

7 On the computer with an Internet connection:

7a Open the copied dongle packet file in LicenseManager.

7b Click **Finalize Removal**.

On the computer with an Internet connection, click **Registration Info** in License Manager to license information for associated and unassociated product licenses.

Updating Products

You can use LicenseManager to check for product updates and download the latest product versions.

For more information on the general features of the subscription service, the AccessData Website (http://www.accessdata.com).

Checking for Product Updates

When checking for updates, LicenseManager checks for an updated version of LicenseManager. If there is one, a prompt appears. When prompted whether to update LicenseManager, click Yes to download and install the latest product version of LicenseManager, or click No to update product version information for the products listed in the LicenseManager window.

To check for product updates, click **Newest** from the Installed Components tab.

To determine whether you have the latest version of a product, check for updates, and then compare the product version with the latest version number listed in the Products window.

Downloading Product Updates

To download a product update:

1. Ensure that LicenseManager displays the latest product information.
2. Check the programs you want to download, and then click **Install Newest**.

3. When prompted, click **Yes** to download the latest install program of the product.
4. Follow the installation wizard to install the product update.

Purchasing Product Licenses

You can use LicenseManager to link to the AccessData website where you can purchase products.

To purchase a product, click **Purchase Licenses** from the Licenses tab.

Note: Once a product has been purchased and appears in the AccessData Website database, you can add the product license to a dongle or dongle packet file by clicking **Refresh Dongle**.

Sending a Dongle Packet File to Support

Send a dongle packet file *only* when specifically directed to do so by AccessData support.

To send a dongle packet file, e-mail a dongle packet file to support@accessdata.com.

CHAPTER 16

Troubleshooting

This chapter contains solutions to the following commonly asked questions:

Problem	Cause	Action
I installed Forensic Toolkit (FTK) on a new machine and my dongle is not working.	The dongle driver is not installed on the new machine.	Install the dongle driver on the new machine. For information on installing the dongle driver, see "Installing the Dongle Driver from CD" on page 17 or "Installing the Dongle Drivers from Downloadable Files" on page 21.
I downloaded the latest version of FTK on a new machine, but I cannot find the dongle drivers.	The dongle driver is a separate download.	On the FTK Download page, click the link to download the dongle drivers. For information on installing the dongle drivers, see "Installing the Dongle Drivers from Downloadable Files" on page 21.

Problem	Cause	Action
FTK cannot find the KFF library.	The KFF database file, ADKFFLibrary.hdb, is not in the same directory as ftk.exe.	1. Search the computer drive for ADKFFLibrary.hdb. 2. After finding ADKFFLibrary.hdb, copy it into the same directory as ftk.exe. By default, this directory is \AccessData\AccessData Forensic Toolkit\Program. If you want to keep KFF in a different directory: 1. In FTK, select **Tools**, and then **Preferences**. 2. In the **KFF Database Location** list, select **User-Specified** and browse to the location of ADKFFLibrary.hdb.
FTK isn't extracting the files from a compressed drive.	FTK cannot currently extract files from drives encrypted or compressed with programs like Double Space or Stacker.	Uncompress the drive before adding it to FTK.

Problem	Cause	Action
FTK shuts down when it adds segmented image files to a case.	The segments are not in the same directory.	To put the segments in the same directory: 1. Verify that all the image files are in one directory. 2. In FTK, click **File**, and then **Add Evidence**. 3. On the **Add Evidence to Case** form, click **Add Evidence** and select the acquired image of the drive. 4. Select **Acquired Image of Drive** and then select the first image segment. The other segments are automatically added.
I was looking at some evidence not assigned to a case when my system crashed. Can I recover that evidence?	Evidence is saved in a default case folder until you save it with a specific name. This folder is intended to be temporary, and will be erased when you start a new session of FTK.	Before you start another session of FTK, rename or move the default case folder. When you start FTK again, browse to the newly named case folder, and open the DefaultCase.ftk file. You should then save the data.

Problem	Cause	Action
FTK cannot find the evidence when opening a case. If the case is opened anyway, the evidence isn't viewable.	FTK must always have access to the evidence files in order to display them. When evidence is added to FTK, the filenames, file types, and search information are the only items recorded in the case file (the index). When the evidence is moved, the way the evidence was added to the case affects whether or not it is viewable. Evidence that was added as an Acquired Image can be moved successfully and remains viewable. Evidence that was added as Contents of a Folder or Individual File should not be moved and will not be viewable if moved. See “Adding Evidence” on page 78.	To view the evidence, keep the evidence in its original location or, when opening a case, browse to and select the new location.

Problem	Cause	Action
FTK doesn't show any attachments for e-mails.	The List All Descendants box in the Tree View toolbar must be checked in order to display attachments. Also, a filter that is applied to the File List may be filtering out the attachments.	Check the **List All Descendants** box in the Tree View toolbar. Make sure a filter is not filtering out attachments in the File List. To view the properties of a filter: 1. Click **View**, and then **File Filter Manager**. 2. In the **Selected Filter** drop-down list, select the filter you want to check. 3. Review and change any necessary selections. For more information about the File Filter Manager, see "Using The File Filter Manager" on page 190.
There are several ftkcrash*value*.txt files in my \AccessData\AccessData Forensic Toolkit\Program\ directory.	ftkcrash*value*.txt files are the FTK crash logs. If FTK crashes, it creates a crash file in the program directory.	The contents of the crash files can be useful to AccessData Technical Support in determining what happened on your system.

APPENDIX A

FTK Recognized File Types

This appendix lists the different file types that are recognized by Forensic Toolkit (FTK). The file type is a string in the document header that identifies the program used to create the document. FTK looks at the document headers to identify the file types.

Because of the large number of recognized files types, use the Search function in the document viewer to quickly find what you are looking for.

This appendix is divided into the following sections:

- "Document File Types" on page 282
- "Spreadsheet File Types" on page 285
- "Database File Types" on page 286
- "Graphic File Types" on page 288
- "Executable File Types" on page 291
- "Archive File Types" on page 291
- "Other Known File Types" on page 293

Document File Types

7-Bit Text

Acrobat Portable Document Format (PDF)

Ami Pro Document

Ami Pro Snapshot

Ami Professional

AreHangeul

CEO Word

CEO Write

CHTML (Compact HTML)

Cyrillic (Ansi 1251)

Cyrillic (KOI8-R)

DEC DX 3.0 and lower

DEC DX 3.1

DisplayWrite 4

DisplayWrite 5

Enable Word Processor 3.x

Enable Word Processor 4.x

Excel 2000 Save As... HTML

FTDF

Hana

HDML (Handheld Device Markup Language)

HTML - Central European

HTML - Chinese Big5

HTML - Chinese EUC

HTML - Chinese GB

HTML - CSS

HTML - Cyrillic (KOI8-R)

HTML - Japanese EUC

HTML - Japanese ShiftJIS

HTML - Korean Hangul

HTMLAG

HTMLWCA

Hypertext Document

IBM DCA/RFT

IBM FFT

IBM Writing Assistant

IchiTaro 3

IchiTaro 4

IchiTaro 8

Interchange File Format Text File

Interleaf

Interleaf (Japanese)

JustWrite 1

JustWrite 2

Legacy

Legacy Clip

Lotus Manuscript 1

Lotus Manuscript 2

Lotus screen snapshot

MacWrite II

Mass 11

Mass 11 (Vax)

Matsu 4

Matsu 5

Microsoft Windows Write

Microsoft Word 1 Document

Microsoft Word 2 Document

Microsoft Word 2000 Document

Microsoft Word 3 Document (Mac)

Microsoft Word 4 Document (DOS)

Microsoft Word 4 Document (Mac)

Microsoft Word 5 Document (DOS)

Microsoft Word 5 Document (Japanese)

Microsoft Word 5 Document (Mac)

Microsoft Word 6 Document

Microsoft Word 6 Document (DOS)

Microsoft Word 6 Document (Mac)

Microsoft Word 7 Document

Microsoft Word 8 Document (Mac)

Microsoft Word 97 Document

Microsoft Word Document

Microsoft Works (Windows)

Microsoft Works 1

Microsoft Works 2

Microsoft Works 2 (Mac)

MIFF

MIFF 3

MIFF 3 (Japanese)

MiFF 4

MIFF 4 (Japanese)

MIFF 5

MIFF 5 (Japanese)

MIFF 5.5

MIFF 6

MIFF 6 Japanese

MS Works/Win 3 (Windows)

MS Works/Win 4

MultiMate 3.6

MultiMate 4

MultiMate Advantage II

MultiMate Note

Navy DIF

OfficeWriter

P1

PC File 5.0 - Letter

Perfect Works 1

PFS: First Choice 2.0

PFS: First Choice 3.0

PFS: WRITE A

PFS: WRITE B

Pocket Word

PowerPoint 2000 Save As... HTML

Professional Write 1

Professional Write 2

Professional Write PLUS

Professional Write PLUS Clip

Q&A Write

Q&A Write 3

Rainbow

Rich Text Format

Rich Text Format (Japanese)

Samna

Signature

SmartWare II

Sprint

StarOffice Writer 5.2

TotalWord

Unicode Text Document

vCard Electronic Business Card

Volkswriter

Wang

WangIWP

WML - Chinese Big 5

WML - Chinese EUC

WML - Chinese GB

WML - CSS

WML - Cyrillic 1251

WML - Cyrillic KOI8

WML - Japanese EUC

WML - Japanese JIS

WML - Japanese Shift JIS

WML - Korean Hangul

WML - Latin 2

Word 2000 Save As... HTML

WORDMARC

WordPad

WordPerfect 4 Document

WordPerfect 4.2

WordPerfect 5

WordPerfect 5 Asian

WordPerfect 5 Mac

WordPerfect 6.0

WordPerfect 6.0 Asian

WordPerfect 6.0 Asian (Enh)

WordPerfect 6.0 (Enh)

WordPerfect 6.0 Mac

WordPerfect 6.0 Mac (Enh)

WordPerfect 6.1

WordPerfect 6.1 Asian

WordPerfect 6.1 Asian (Enh)

WordPerfect 6.1 (Enh)

WordPerfect 6.1 Mac

WordPerfect 6.1 Mac (Enh)

WordPerfect 7

WordPerfect 7 Asian

WordPerfect 7 Asian (Enh)

WordPerfect 7 (Enh)

WordPerfect 7 Mac

WordPerfect 7 Mac (Enh)

WordPerfect 8

WordPerfect 8 Asian

WordPerfect 8 Asian (Enh)

WordPerfect 8 (Enh)

WordPerfect 8 Mac

WordPerfect 8 Mac (Enh)

WordPerfect 9

WordPerfect 9 (Enh)

WordPerfect 9 Mac (Enh)

WordPerfect 9 Mac

WordPerfect Document

Word Pro Document

Word Pro 96 Document

Word Pro 97 Document

WordStar 4 and lower

WordStar 5

WordStar 5.5

WordStar 6

WordStar 7

WordStar 2000

WordStar for Windows

WPF Encrypt

WPF Unknown

WPS Plus

WWrite ChineseBig5

WWrite ChineseGB

WWrite Hangeul

WWrite Shift-JIS

XHTMLB

XML

XyWrite / Nota Bene

Spreadsheet File Types

1-2-3 1.A Document

1-2-3 2.0 Document

1-2-3 2.01 Document

1-2-3 3.0 Document

1-2-3 4.0 Document

1-2-3 97 Document

1-2-3 Document

1-2-3 Japanese Document

1-2-3 Seal Document

CEO Spreadsheet

Enable SpreadSheet

First Choice (Spreadsheet)

Generic WKS format

Lotus 1-2-3 2 (FRM)

Lotus 1-2-3 6

Lotus 1-2-3 9

Lotus 1-2-3 OS/2 2

Lotus 1-2-3 OS/2 Chart

Lotus Symphony 1.0 Document

Mac Works 2 (SS)

Microsoft Excel 2 Worksheet

Microsoft Excel 2000 Worksheet

Microsoft Excel 3 Workbook

Microsoft Excel 3 Worksheet

Microsoft Excel 4 Workbook

Microsoft Excel 4 Workbook (Mac)

Microsoft Excel 4 Worksheet

Microsoft Excel 4 Worksheet (Mac)

Microsoft Excel 5 Worksheet (Mac)

Microsoft Excel 7 Worksheet

Microsoft Excel 97 Worksheet

Microsoft Excel Worksheet

Microsoft Multiplan 4.*x*

Mosaic Twin

MS Works Spreadsheet

MS Works/Win 3 (SS)

MS Works/Win 4 (SS)

MS Works/Win Spreadsheet

PFS Plan

PlanPerfect File

Quattro Pro 4

Quattro Pro 7.0 Graph

Quattro Pro 9 for Windows

Quattro Pro Notebook

Quattro Pro Notebook 1.0

Quattro Pro Notebook 1.0J

Quattro Pro Notebook 3.0 (DOS)

Quattro Pro Notebook 4.0 (DOS)

Quattro Pro Notebook 5.0

Quattro Pro Notebook 5.5 (DOS)

Quattro Pro Notebook 6.0

Quattro Pro Notebook 7.0

Quattro Pro Notebook 8.0

Smart SpreadSheet

SuperCalc 5

VP Planner

Database File Types

Access 2 File

Access 2 System File

Access 2000 File

Access 2000 System File

Access 7 File

Access 7 System File

ACT 1 File

ACT 1.1 File

ACT 2 File

ACT 3 File

Approach 96 File

Approach 97 File

Ascend File

CEO Database

DataEase 4.*x*

DataPerfect File

DBase II File

DBase III File

DBase IV/V File

First Choice (Database)

Framework III

Mac Works 2 (DB)

Microsoft Project98

Microsoft Works (DB)

MS Jet 2 Database

MS Jet 3 Database

MS Jet 4 Database

MS Jet Database

MS Money 1 File

MS Money 2 File

MS Money 2000 File

MS Money 3 File

MS Money 4 File

MS Money 5 File

MS Money 98 File

MS Money File

MS Works Database

MS Works/Win 3 (DB)

MS Works/Win 4 (DB)

MS Works/Win Database

Organizer 1.1 File

Organizer 2 File

Organizer 3 File

Organizer 4 File

Quicken 5 File

Quicken 6 File

Quicken 98 File

Quicken 99 File

Paradox 3

Paradox 3.5

Paradox 4

Paradox Database File

Paradox Script File

Q&A Database

Quickbooks 2 File

Quickbooks 2000 File

Quickbooks 3.1 File

Quickbooks 5 File

Quickbooks 6 File

Quickbooks 99 File

Quickbooks File

Quicken 2000 File

Quicken 2001 File

Quicken 3 File

Quicken 4 File

Quicken File

RBase 5000

RBase File 1

RBase File 3

RBase V

Reflex 2.0 Database

Smart DataBase

Graphic File Types

Acrobat Portable Document Format (Mac)

Adobe Illustrator

Adobe Photoshop File

Ami Professional Draw

Animated Cursor

Animatic Film File

Animation

AOL Art Files version 3.0

Apple Quicktime File

AutoCAD Drawing Exchange File

AutoCAD Drawing Interchange (DXF-ASCII)

AutoCAD Drawing Interchange (DXF-Binary

AutoCAD DWG 12

AutoCAD DWG 13

AutoCAD Native Drawing Format (DWG)

AutoCAD Native Drawing Format 14 (DWG)

Autodesk 3D Studio File

Autodesk Animator File

AutoShade (RND)

Bentley Microstation DGN

Bitmap File

CALS Raster File Format

Candy 4

CAS Fax File

CCITT Group 3

Computer Graphic Metafile

ComputerEyes Raw Data File

Corel Draw 2

Corel Draw 3

Corel Draw 4

Corel Draw 5

Corel Draw 6

Corel Draw 7

Corel Draw 8

Corel Draw 9

Corel Draw Clipart

Cursor

Cyber Paint Sequence File

DrawPerfect File

Dual PowerPoint 95/97

DXB

Encapsulated PostScript (EPS)

Enhanced Windows Metafile

Excel 3 Chart

Excel 4 Chart

Excel 5 Chart

Excel Chart

Framemaker

Freelance

Freelance 96

GEM Bitmap (IMG)

GEM IMG File

GEM Metafile

GIF File

Graphic File

Hanako 1

Hanako 2

Harvard Graphics

Harvard Graphics 2.*x* Chart

Harvard Graphics 3.*x* Chart

Harvard Graphics Presentation

Hewlett Packard Graphics Language

HP Gallery

IBM Graphics Data Format (GDF)

IBM Picture Interchange Format

Icon

IGES Drawing

Intel Digital Video File

JiNG File (JPEG Network Graphics)

JPEG File Interchange Format

JPEG/JFIF File

Kodak Flash Pix (FPX)

Kodak Photo CD

Lotus PIC

Lotus screen snapshot

Macintosh Picture 1

Macintosh Picture 2

MAC-Paint File

Micrografx Designer (DRW)

Micrografx File

MIFFG

MiNG File (Multiple-image Network Graphics)

Multi-page PCX (DCX)

NEOChrome Animation File

OS/2 PM Metafile

OS/2 Warp Bitmap

Paintshop Pro (PSP)

PCPAINT File

PCX Paintbrush File

PiNG File (Portable Network Graphics)

Portable Bitmap (PBM)

Portable Graymap (PGM)

Portable Pixmap (PPM)

PostScript

PowerPoint 2000

PowerPoint 3

PowerPoint 3 (Mac)

PowerPoint 4

PowerPoint 4 (Mac)

PowerPoint 7

PowerPoint 97/98

Progressive JPEG

Sun Raster File

Targa File

TIFF File

Video Clip

Visio 2000

Visio 4

Visio 5

Windows DIB

Windows Icon

Windows Metafile

WordPerfect Graphic (WPG)

WordPerfect Graphic File

WordPerfect MAC SOFT Graphics

WP Presentations

WP Presentations 7

XBM - X-Windows Bitmap

XPM - X-Windows Pixmap

XWD - X-Windows Dump

Multimedia File Types

AIFF

ASF

Audio Director

AVI

Flash

MIDI

MP3

MP4

QuickTime

SMUS

WAV

WM

WMA

WMV

8SVX

E-mail Message Programs

FTK handles e-mail messages differently than other categories. FTK recognizes the source of the e-mail messages based on e-mail archives and special headers.

Note: FTK includes extended support for AOL including buddy lists, global settings, user history, URL history, thumbnail extraction, and address book extraction.

The following are supported e-mail applications:

- AOL
- Earthlink
- Eudora
- Hotmail
- MSN E-mail
- Netscape
- Outlook
- Outlook Express
- Yahoo

Instant Messaging Programs

FTK can recover instant messaging chat logs and additional information such as buddy lists.

The following are supported instant messaging applications:

AOL Instant Messenger	Yahoo Messenger

Executable File Types

Executable File	NT Executable File
Executable File (COM)	OS/2 Executable File
JavaScript	Windows VxD Executable File

Archive File Types

File Type	Additional Information
ARC Archive	Identified but not extracted by FTK.
BestCrypt GOST/BLOWFISH	Identified but not extracted by FTK.
BestCrypt GOST/DES	Identified but not extracted by FTK.
BestCrypt GOST/GOST	Identified but not extracted by FTK.
BestCrypt GOST/TWOFISH	Identified but not extracted by FTK.
BestCrypt GOST/Unknown	Identified but not extracted by FTK.
BestCrypt SHA/BLOWFISH	Identified but not extracted by FTK.
BestCrypt SHA/DES	Identified but not extracted by FTK.
BestCrypt SHA/GOST	Identified but not extracted by FTK.
BestCrypt SHA/TWOFISH	Identified but not extracted by FTK.
BestCrypt SHA/Unknown	Identified but not extracted by FTK.

File Type	Additional Information
BestCrypt Unknown Key Generation	Identified but not extracted by FTK.
CAB Archive	Identified but not extracted by FTK.
E-mail Archive	
GZIP Archive	Identified but not extracted by FTK.
Jetico BestCrypt Container	Identified but not extracted by FTK.
MS Exchange/Outlook	
Old Format PGP Secret Key Ring	Identified but not extracted by FTK.
OLE Archive	
OLE Embedded Object	
OLE Embedded Storage Container	
Outlook Express 5 Archive	
Outlook Express Archive	
PGP Disk 4.0 File	Identified but not extracted by FTK.
PGP Disk File	Identified but not extracted by FTK.
PGP Secret Key Ring	Identified but not extracted by FTK.
PK Zip Archive	
Self-Extracting Zip Archive	
Stuffit Archive	Identified but not extracted by FTK.
Thumb.db Thumbnail Graphics	
UNIX TAR Archive	Identified but not extracted by FTK.
Zip Archive	

Other Known File Types

8 Bit Sample Voice

Access File

Access System File

AccessData Recovery 5.0 Biographical Data

AccessData Recovery 5.0 Biographical Dictionary

AccessData Recovery 5.0 Dictionary

AccessData Recovery 5.0 Hard Drive Dictionary

AccessData Recovery 5.0 Password Data

AccessData Recovery 5.0 Profile Data

AccessData Recovery 5.0 Status Report

ACT File

Address Book Entry

Appointment

Approach

Audio Clip

Audio Director

Audio Flash

Contact Information

Drive Free Space

Email Folder

Encapsulated PostScript File

Envoy

Envoy 7

Escher

File Slack

File System Slack

Help File

ICF

Internet Cookie File

Internet Explorer Link Files

Journal Entry

LZH Compress

Microsoft Office Binder

MIDI Sequence

MPEG Version 1.0

MPEG Version 2.0

MPEG Version 2.5

QuickFinder

Sample Music

Scheduler File

Self-Extracting LZH

Shortcut FileSticky Note

Task

UNIX Compress

Wave Sound

Win95 Screensaver Settings

Windows Clipboard File

Windows Swap File

WordPerfect 4.2 (Vax)

WordPerfect Application Resource Library

WordPerfect Block File

WordPerfect Calculator

WordPerfect Calendar

WordPerfect Character Map

WordPerfect Column Block

WordPerfect Dictionary

WordPerfect Dictionary – Rules

WordPerfect Display Resource File

WordPerfect Equation Resource

WordPerfect External Spell Code Module

WordPerfect External Spell Dictionary

WordPerfect File Manager

WordPerfect Graphic Driver

WordPerfect Help File

WordPerfect Hyph Lex Module

WordPerfect Hyphenation Code Module

WordPerfect Hyphenation Data Module

WordPerfect InForms 1

WordPerfect Install Options

WordPerfect Keyboard Definition

WordPerfect Macro Editor

WordPerfect Macro File

WordPerfect Macro Resource

WordPerfect Mouse Driver

WordPerfect Notebook

WordPerfect Office

WordPerfect Overlay File

WordPerfect Printer

WordPerfect Printer Q Codes

WordPerfect Printer Resource File

WordPerfect Program Editor

WordPerfect Rectangular Block

WordPerfect Rhymer Pronunciation

WordPerfect Rhymer Word File

WordPerfect Scheduler

WordPerfect Setup File

WordPerfect Shell

WordPerfect Spell Code Module – Rules

WordPerfect Spell Code Module – Word List

WordPerfect Thesaurus

WordPerfect Unix Setup File

WordPerfect Vax Keyboard Definition

WordPerfect Vax Setup

APPENDIX B

Regular Expression Searching

Regular expressions allow forensics analysts to search through large quantities of text information for patterns of data such as the following:

- Telephone Numbers
- Social Security Numbers
- Computer IP Addresses
- Credit Card Numbers

This data can be extracted because it occurs in known patterns. For example, credit card numbers are typically sixteen digits in length and are often stored in the following pattern or format: xxxx–xxxx–xxxx–xxxx.

This appendix explains the following:

- “Understanding Regular Expressions” on page 296
- “Predefined Regular Expressions” on page 300
- “Going Farther with Regular Expressions” on page 302

Understanding Regular Expressions

Forensics analysts specify a desired pattern by composing a regular expression. These patterns are similar to arithmetic expressions that have operands, operators, sub-expressions, and a value. For example, the following table identifies the mathematical components in the arithmetic expression, 5/((1+2)*3):

Component	Example
Operands	5, 1, 2, 3
Operators	/, ( ), +, *
Sub-Expressions	(1+2), ((1+2)*3)
Value	Approximately 0.556

Like the arithmetic expression in this example, regular expressions have operands, operators, sub-expressions, and a value. How these expressions are created and used is explained using simple expressions followed by more complex regular expressions.

Note: Unlike arithmetic expressions which can only have numeric operands, operands in regular expressions can be any characters that can be typed on a keyboard, such as alphabetic, numeric, and symbolic characters.

Simple Regular Expressions

A simple regular expression can be made up entirely of operands. For example, the regular expression *dress* causes the search engine to return a list of all files that contain the sequence of characters *d r e s s*. The regular expression *dress* corresponds to a very specific and restricted pattern of text, that is, sequences of text that contain the sub-string *dress*. Files containing the words “dress,” “address,” “dressing,” and “dresser,” are returned in a search for the regular expression *dress*.

The search engine searches left to right. So in searching the regular expression *dress,* the search engine opens each file and scans its contents line by line, looking for a *d,* followed by an *r,* followed by an *e,* and so on.

Complex Regular Expressions—Visa and MasterCard Numbers

Operators allow regular expressions to search patterns of data rather than specific values. For example, the operators in the following expression enables the FTK's search engine to find all Visa and MasterCard credit card numbers in case evidence files:

\<((\d\d\d\d)[\–]){3}\d\d\d\d\>

Without the use of operators, the search engine could look for only one credit card number at a time.

Note: The credit card expression discussion in this section is included in FTK and is used here primarily for the explanation of advanced regular expressions.

The following table identifies the components in the Visa and MasterCard regular expression:

Component	Example
Operands	*d,* \–, spacebar space
Operators	\d, \, <, ( ), [ ], {3}, \>
Sub-Expressions	(\d\d\d\d), ((\d\d\d\d)[\–])
Value	Any sequence of sixteen decimal digits that is delimited by three hyphens and bound on both sides by non-word characters (xxxx–xxxx–xxxx–xxxx).

As the regular expression search engine evaluates an expression in left-to-right order, the first operand it encounters is the backslash less-than combination (\<). This combination is also known as the begin-a-word operator. This operator tells the search engine that the first character in any search hit immediately follows a non-word character such as white space or other word delimiter.

Tip: A precise definition of non-word characters and constituent-word characters in regular expressions is difficult to find. Consequently, experimentation by FTK users may be the best way to determine if the forward slash less-than (\<) and forward slash greater-than (\>) operators help find the data patterns relevant to a specific searching task. The hyphen and the period are examples of valid delimiters or non-word characters.

The begin-a-word operator illustrates one of two uses of the backslash character (\), often called the escape character: the modification of operands and the modification of operators. On its own, the left angle bracket (<) would be evaluated as an operand, requiring the search engine to look next for a left angle bracket character. However, when the escape character immediately precedes the (<), the two characters are interpreted together as the begin-a-word operator by the search engine. When an escape character precedes a hyphen (–) character, which is normally considered to be an operator, the two characters (\–) require the search engine to look next for a hyphen character and not apply the hyphen operator (the meaning of the hyphen operator is discussed below).

The next operator is the parentheses ( ). The parentheses group together a sub-expression, that is, a sequence of characters that must be treated as a group and not as individual operands.

The next operator is the \ *d*. This operator, which is another instance of an operand being modified by the escape character, is interpreted by the search engine to mean that the next character in search hits found may be any decimal digit character from *0–9*.

The square brackets ([ ]) indicate that the next character in the sequence must be one of the characters listed between the brackets or escaped characters. In the case of the credit card expression, the backslash-hyphen-spacebar space ([\-*spacebar space*]) means that the four decimal digits must be followed by a hyphen or a spacebar space.

Next, the *{3}* means that the preceding sub-expression must repeat three times, back to back. The number in the curly brackets ({ }) can be any positive number.

Finally, the forward slash greater-than combination (\>), also know as the end-a-word operator, means that the preceding expression must be followed by a non-word character.

Other Variations on the Same Expression

Sometimes there are ways to search for the same data using different expressions. It should be noted that there is no one-to-one correspondence between the expression and the pattern it is supposed to find. Thus the preceding credit card regular expression is not the only way to search for Visa or MasterCard credit card numbers. Because some regular expression operators have related meanings, there is more than one way to compose a regular expression to find a specific pattern of text. For instance, the following regular expression has the same meaning as the preceding credit card expression:

```
\<((\d\d\d\d)(\-| )){3}\d\d\d\d\>
```

The difference here is the use of the pipe, (|) or union operator. The union operator means that the next character to match is either the left operand (the hyphen) or the right operand (the spacebar space). The similar meaning of the pipe (|) and square bracket ([ ]) operators give both expressions equivalent functions.

In addition to the previous two examples, the credit card regular expression could be composed as follows:

```
\<\d\d\d\d(\-| )\d\d\d\d(\-| )\d\d\d\d(\-| )\d\d\d\d\>
```

This expression explicitly states each element of the data pattern, whereas the {3} operator in the first two examples provides a type of mathematical shorthand for more succinct regular expressions.

Predefined Regular Expressions

FTK provides the following predefined regular expressions:

- U.S. Social Security Numbers
- U.S. Phone Numbers
- U.K. Phone Numbers
- IP Addresses
- Visa and MasterCard Numbers

The Social Security Number, U.S. Phone Number, and IP Address expressions are discussed in the following sections.

Note: The U.K. Phone Number expression is similar enough to the U.S. Phone Number that it does not warrant a separate discussion.

Social Security Number

The regular expression for Social Security numbers follows a relatively simple pattern:

```
\<\d\d\d[\– ]\d\d[\– ]\d\d\d\d\>
```

This expression reads as follows: find a sequence of text that begins with three decimal digits, followed by a hyphen or spacebar space. This sequence is followed by two more decimal digits and a hyphen or spacebar space, followed by four more decimal digits. This entire sequence must be bounded on both ends by non-word characters.

U.S. Phone Number

The regular expression for U.S. phone numbers is more complex:

```
((\<1[\–\. ])?(\(|\<)\d\d\d[\)\.\–/ ] ?)?\<\d\d\d[\.\– ]\d\d\d\d\>
```

This expression demonstrates that regular expressions can be used to find more complex data patterns than simple credit card and Social Security number patterns.

The first part of the above expression,
`((\<1[\–\. ])?(\(|\<)\d\d\d[\)\.\–/ ] ?)?`,
means, in effect, that an area code may or may not precede the

seven digit phone number. This meaning is achieved through the use of the question mark (?) operator. This operator requires that the sub-expression immediately to its left appear exactly zero or one times in any search hits. Therefore, the U.S. Phone Number expression finds telephone numbers with or without area codes.

This expression also indicates that if an area code is present, a number one (1) may or may not precede the area code. This meaning is achieved through the sub-expression (\<1[\–\.])?, which says that if there is a “1” before the area code, it will follow a non-word character and be separated from the area code by a delimiter (period, hyphen, or spacebar space).

The next sub-expression, (\(|\<)\d\d\d[\)\.\–/] ?, specifies how the area code must appear in any search hits. The \(|\<) requires that the area code begin with a left parenthesis or other delimiter. (Note that the left parenthesis is, of necessity, escaped.) The initial delimiter is followed by three decimal digits, then another delimiter—namely, a right parenthesis, a period, a hyphen, a forward slash, or a spacebar space. Lastly, the question mark (?) means that there may or may not be one spacebar space after the final delimiter.

The latter portion of this expression, \<\d\d\d[\.\–]\d\d\d\d\>, requests a seven-digit phone number with a delimiter (period, hyphen, or spacebar space) between the third and fourth decimal digit characters. Note that typically, the period is an operator. It means that the next character in the pattern can be any valid character. To specify an actual period (.), the character must be escaped (\ .). The backslash period combination is included in the expression to catch phone numbers delimited by a period character.

IP Address

An IP address is a 32-bit value that uniquely identifies a computer on a TCP/IP network, including the Internet. Currently, all IP addresses are represented by a numeric sequence of four fields separated by the period character. Each field can contain any number from 0 to 255. The following regular expression locates IP addresses:

```
\<[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\.[1-2]?[0-9]?[0-9]\>
```

The IP Address expression requires the search engine to find a sequence of data with four fields separated by periods (.). The data sequence must also be bound on both sides by non-word characters.

Note that the square brackets ([ ]) still behave as a set operator, meaning that the next character in the sequence can be any one of the values specified in the square brackets ([ ]). Also note that the hyphen (–) is not escaped; it is an operator that expresses ranges of characters.

Each field in an IP address can contain up to three characters. Reading the expression left to right, the first character, if present, must be a *1* or a *2*. The second character, if present, can be any value *0–9*. The square brackets ([ ]) indicate the possible range of characters and the question mark (?) indicates that the value is optional; that is, it may or may not be present. The third character is required; therefore, there is no question mark. However, the value can still be any number *0–9*.

Going Farther with Regular Expressions

You can begin building your own regular expressions by experimenting with the default expressions in FTK. You can modify the default expressions to fine-tune your data searches or to create your own expressions.

Locating More Information on Regular Expressions

The World Wide Web contains many other reference materials and tutorials for regular expression searching. For example, the Website http://www.regular-expressions.info/ provides a regular expression for finding e-mail addresses. Keep in mind, however, that there is some variation among the search engines. Some of them differ in expression syntax, i.e., in the way that they form and use operands and operators.

Tip: Regular expression operators are often referred to as metacharacters in the regular expression literature.

http://www.boost.org/libs/regex/syntax.htm#syntax for a definitive reference on the syntax employed by Regex++, the regular expression search engine bundled with FTK.

Note: The regular expression search engine used by FTK is called Regex++. It was created by Dr. John Maddock, a contributor to www.boost.org.

Common Operators

The following is a list of common operators:

Operator	Description
+	Matches the preceding sub-expression one or more times. For example, "ba+" will find all instances of "ba," "baa," "baaa," and so forth; but it will not find "b."
$	Matches the end of a line.
*	Matches the preceding sub-expression zero or more times. For example, "ba*" will find all instances of "b," "ba," "baa," "baaa," and so forth.
?	Matches the preceding sub-expression zero or one times.
[]	Matches any single value within the square brackets. For example, "ab[xyz]" will find "abx," "aby," and "abz." A hyphen (-) specifies ranges of characters with the brackets. For example, "ab[0-3]" will find "ab0," "ab1," "ab2," and "ab3." You can also specify case specific ranges such as [a-r], or [B-M].
[^ftk]	Matches any character except those bound by the [^ and the].

Operator	Description
\<	Matches the beginning of a word. In other words, the next character in any search hit must immediately follow a non-word character.
\>	Matches the end of a word.
|	Matches either the sub-expression on the left or the right. For example, A|u will requires that the next character in a search hit be “A” or “u.”
\d	Matches any decimal digit.
\l	Matches any lowercase letter.
\s	Matches any white space character such as a space or a tab.
\u	Matches any uppercase letter.
\w	Matches any whole word.
^	Matches the start of a line.
{*n*,*m*}	Matches the preceding sub-expression at least *n* times, but no more than *m* times.
{*n*}	Matches the preceding sub-expression *n* times.

APPENDIX C

Recovering Deleted Material

Forensic Toolkit (FTK) finds deleted files on the supported file systems by their file header. This appendix discusses how deleted files are recovered on the following file systems:

- "FAT 12, 16, and 32" on page 306
- "NTFS" on page 306
- "ext2" on page 307
- "ext3" on page 307

FAT 12, 16, and 32

When parsing FAT directories, FTK identifies deleted files by their names. In a deleted file, the first character of the 8.3 filename is replaced by the hex character 0xE5.

The file's directory entry provides the files's starting cluster (*C*) and size. From the size of the file and the starting cluster, FTK computes the total number of clusters (*N*) occupied by the file.

FTK then examines the File Allocation Table (FAT) and counts the number of unallocated clusters starting at *C* (*U*). FTK then assigns the recovered file [min (*N*, *U*)] clusters starting at *C*.

If the deleted file was fragmented, the recovered file is likely to be incorrect and incomplete because the information that is needed to find subsequent fragments was wiped from the FAT system when the file was deleted.

FTK uses the long filename (LFN) entries, if present, to recover the first letter of the deleted file's short filename. If the LFN entries are incomplete or absent, FTK uses an exclamation mark ("!") as the first letter of the filename.

FTK does not search the volume free space for deleted directories that have been orphaned. An orphaned directory is a directory whose parent directory or whose entry in its parent directory has been overwritten.

NTFS

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.

ext2

FTK searches to find inodes that are marked deleted. The link count is zero and the deletion timestamp is nonzero.

For each deleted inode, FTK processes the block pointers as it does for a normal file and adds blocks to the deleted file. However, if an indirect block is marked allocated or references an invalid block number, the recovered file is truncated at that point because the block no longer contains a list of blocks for the file that FTK is attempting to recover.

FTK does not recover the filenames for files deleted on ext2 systems. Instead, deleted files are identified by inode number because ext2 uses variable-length directory entries organized in a linked list structure. When a file is deleted, its directory entry is unlinked from the list, and the space it occupied becomes free to be partially or completely overwritten by new directory entries. There is no reliable way to identify and extract completely deleted directory entries.

ext3

FTK does not support recovering deleted files from ext3 volumes because ext3 zeroes out a file's indirect block pointers when it is deleted.

APPENDIX D

Program Files

The following table identifies key program files, their functions, and their locations.

Filename	Directory Location	Function
cache folder	Located in the case folder defined by the user when creating the case.	This folder is used to store FTKINDEX files that direct Forensic Toolkit (FTK) on where to find items within a disk image. They do not contain any actual data from the disk image. The folder should not be moved or deleted. If you delete any of these files, it may render FTK unable to open the associated disk image.
case.ftk	The case folder defined by the user when creating the case.	All case files are named *case*.ftk. The *case*.ftk file for each case is stored in the applicable case folder.
case.idx	The case folder defined by the user when creating the case.	All case index files are named *case*.idx. The *case*.idx file for each case is stored in the applicable case folder.
efs folder	Located in the case folder defined by the user when creating the case.	This folder is used to store the keys for decrypting EFS files. This folder may not exist if Password Recovery Toolkit (PRTK) is not installed or if there are no EFS files in the case. For more information, see "Decrypting EFS" on page 217.

Filename	Directory Location	Function
ftk.log	The case folder defined by the user when creating the case.	ftk.log is the case log for the specified case.
ftk.log	The case folder defined by the user when creating the case.	The case log file. When you create a new case, FTK automatically creates the ftk.log file. The case log documents activities that occur on the case during its investigation and analysis. When creating a new case, you define which events you want FTK to log for the current case. You can also manually add any information that you want included in the audit trail. The case log can be included in reports to identify what has occurred on the case.
ftkcolumnsettings.ini	\AccessData\AccessData Forensic Toolkit\Program	Custom column settings are saved in the ftkcolumnsettings.ini file. You can access your custom column settings on other machines by copying the ftkcolumnsettings.ini file to the computer's \AccessData\AccessData Forensic Toolkit\Program\ directory. This will, however, overwrite the custom column settings on the target machine. (This does not impact the default column settings.) For more information, see "Creating and Modifying Column Settings" on page 252.
ftkcrash*nvalue*.txt	\AccessData\AccessData Forensic Toolkit\Program	ftkcrash*value*.txt files are the FTK crash logs. If FTK crashes, it creates a crash file in the program directory. The contents of the crash files can be useful to AccessData Technical Support in determining what happened on your system.

Filename	Directory Location	Function
ftkfilefilters.ini	\AccessData\AccessData Forensic Toolkit\Program	Custom file filters are saved in the ftkfilefilters.ini file. You can access your custom file filters on other machines by copying the ftkfilefilters.ini file to the computer's \AccessData\AccessData Forensic Toolkit\Program\ directory. This will, however, overwrite the custom file filters on the target machine. (This does not impact the default file filters.) For more information, see "Modifying or Creating a Filter" on page 196.
ftkfileinfo.txt	The case folder selected by the user during a Copy Special procedure.	If the user selects **File** as a copy destination during a Copy Special procedure, the file information is copied to the ftkfileinfo.txt file.
ftksettings.ini	\AccessData\AccessData Forensic Toolkit\Program	The ftksettings.ini file contains the following settings: ◆ Preference ◆ Default case ◆ Default report ◆ Default export ◆ Indexed search options ◆ Default column ◆ Default file filters ◆ Color and font ◆ Log and File Listing size For more information, see "Customizing Fonts and Colors" on page 245 and "Changing Preferences" on page 255.
index folder	Located in the case folder defined by the user when creating the case.	This folder is used to store the dtSearch text index files. The folder should not be moved or deleted.

Filename	Directory Location	Function
LicenseManager.exe	\AccessData\AccessData Forensic Toolkit\Program	With LicenseManager you can view license information, add or remove existing licenses to a dongle or dongle packet file, renew your subscription, purchase licenses, and send a dongle packet file to AccessData Technical Support. You can also check for product updates and download the latest product versions. For more information, see "Using LicenseManager" on page 55.
regexlist.ini	\AccessData\AccessData Forensic Toolkit\Program	All regular expressions are saved in the regexlist.ini file. Four regular expressions are provided by default: ◆ U.S. Phone Number ◆ U.K. Phone Number ◆ Credit Card Number ◆ Social Security Number ◆ IP Address When you select the **Edit Expressions** option in the Live Search form, the regexlist.ini file is opened in Notepad. From Notepad, you can create, modify, or delete expressions from the regexlist.ini file.

Filename	Directory Location	Function
registryviewer.exe	\AccessData\AccessData Forensic Toolkit\Program	Registry Viewer allows you to view the contents of Windows operating system registry files. Unlike Windows Registry Editor, which only displays the current system's registry, Registry Viewer lets you examine registry files from any system. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor. For more information, see "Searching the Registry" on page 199.
ThumbIdx folder	Located in the case folder defined by the user when creating the case.	This folder is used to store prerendered thumbnails. The folder should not be moved or deleted. For more information, see "Creating Thumbnails" on page 131.

APPENDIX E

Securing Windows Registry Evidence

This appendix contains information about the Windows Registry and what information can be gathered for evidence.

This appendix includes the following sections:

- "Understanding the Windows Registry" on page 316
- "Registry Quick Find Chart" on page 325

Understanding the Windows Registry

For forensic work, registry files are particularly useful because they can contain important information such as

- Usernames and passwords for programs, e-mail, and Internet sites.
- A history of Internet sites accessed, including date and time.
- A record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.).
- Lists of recently accessed files (e.g., documents, images, etc.).
- A list of all programs installed on the system.

Registry Viewer allows you to view the contents of Windows operating system registries. Unlike the standard Windows Registry Editor, which only displays the current system's registry, Registry Viewer lets you examine registry files from any system. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor.

The files that make up the registry differ depending on the version of Windows. The tables below list the registry files for each version of Windows, along with their locations and the information they contain.

The following table describes each item on the Windows 9*x* registry files:

Filename	Location	Contents
system.dat	\Windows	◆ Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet Websites, e-mail passwords for Microsoft Outlook or Outlook Express, and a record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed. ◆ All installed programs, their settings, and any usernames and passwords associated with them ◆ System settings
user.dat	\Windows **Note:** If there are multiple user accounts on the system, each user has a user.dat file located in \Windows\profiles\user account	◆ MRU (Most Recently Used) list of files. MRU Lists maintain a list of files so users can quickly re-access files. Registry Viewer allows you to examine these lists to what files have been recently used and where they are located. Registry Viewer lists each program's MRU files in order from most recently accessed to least recently accessed. ◆ User preference settings (desktop configuration, etc.

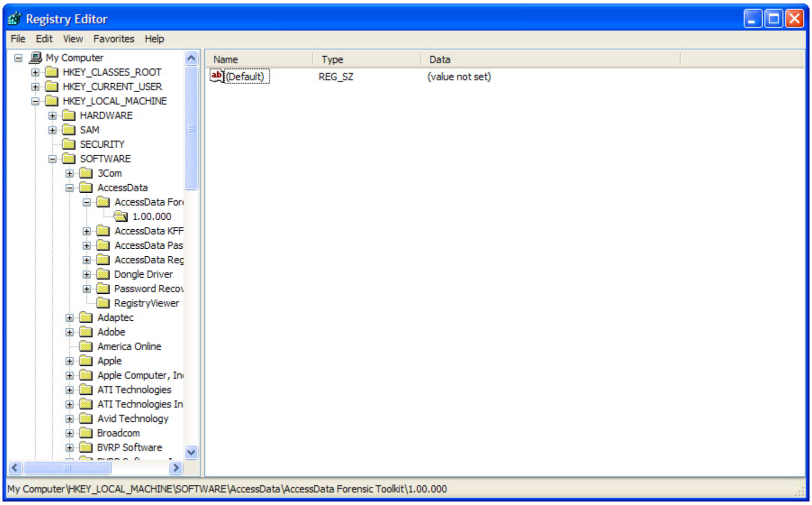
The following table describes each item on the Windows NT and 2000 registry files:

Filename	Location	Contents
Default	\Winnt\system32\config	System settings
ntuser.dat	\Documents and Settings\user account **Note:** If there are multiple user accounts on the system, each user has an ntuser.dat file.	◆ Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet Websites, e-mail passwords for Microsoft Outlook or Outlook Express, and a record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed. ◆ All installed programs, their settings, and any usernames and passwords associated with them ◆ User preference settings (desktop configuration, etc.)
SAM	\Winnt\system32\config	User account management and security settings
Security	\Winnt\system32\config	Security settings
Software	\Winnt\system32\config	All installed programs, their settings, and any usernames and passwords associated with them
System	\Winnt\system32\config	System settings

The following table describes each item on the Windows XP registry files:

Filename	Location	Contents
ntuser.dat	\Documents and Settings\user account **Note:** If there are multiple user accounts on the system, each user has an ntuser.dat file.	◆ Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet Websites, e-mail passwords for Microsoft Outlook or Outlook Express, and a record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.), including the time and date when they were performed. ◆ All installed programs, their settings, and any usernames and passwords associated with them ◆ User preference settings (desktop configuration, etc.)
Default	\Winnt\system32\config	System settings
SAM	\Winnt\system32\config	User account management and security settings
Security	\Winnt\system32\config	Security settings
Software	\Winnt\system32\config	All installed programs, their settings, and any usernames and passwords associated with them
System	\Winnt\system32\config	System settings

When you open one of the above files in Registry Viewer, a registry tree appears in the left pane of the Full Registry window. The tree is organized in a hierarchical structure, similar in appearance to the folder and file structure of the Windows file system.



Name	Type	Data
(Default)	REG_SZ	(value not set)

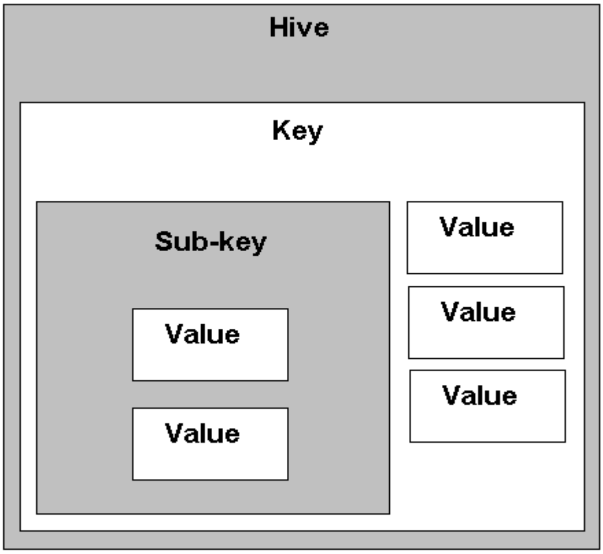
My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\AccessData Forensic Toolkit\1.00.000

Each registry entry, denoted by a folder icon, is called a *key*. Some keys contain *subkeys*, which may in turn contain other subkeys.

This is how Windows presents the registry to you and the applications that use it; however, this structure only exists while Windows is running. When you boot your machine, Windows pulls information from the system to create this virtual representation of the registry.

When you select a key, the top right pane displays the key's value(s) or the information associated with that key. Each value has a name and a data type, followed by a representation of the value's data. The data type tells you what kind of data the value contains as well as how it is represented. For example, values of the REG_BINARY type contain raw binary data and are displayed in hexadecimal format.

The logical registry is organized into the following way:



A hive is a discrete body of keys, subkeys, and values that is rooted at the top of the registry hierarchy. On Windows 9*x* systems, the registry hives are as follows:

HKEY_CLASSES_ROOT (HKCR)

HKEY_CURRENT_USER (HKU)

HKEY_LOCAL_MACHINE (HKLM)

HKEY_USERS (HKCU)

HKEY_CURRENT_CONFIG (HKCC)

HKEY_KYN_DATA (HKDD)

HKEY_LOCAL_MACHINE and HKEY_USERS are the root hives. They contain information that is used to create the HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, AND HKEY_CURRENT_CONFIG hives.

HKEY_LOCAL_MACHINE is generated at startup from the System.dat file and contains all the configuration information for the local machine. For example, it might have one configuration if the machine is docked, and another if the machine is not docked. Based on the machine state at startup, the information in HKEY_LOCAL_MACHINE is used to generate HKEY_CURRENT_CONFIG and HKEY_CLASSES_ROOT.

HKEY_USERS is generated at startup from the system User.dat files and contains information for every user on the system.

Based on who logs in to the system, the information in HKEY_USERS is used to generate HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, and HKEY_CLASSES_ROOT.

Keys and sub-keys are used to divide the registry tree into logical units off the root.

When you select a key, Registry Editor displays the key's values; that is, the information associated with that key. Each value has a name and a data type, followed by a representation of the value's data. The data type tells you what kind of data the value contains as well as how it is represented. For example, values of the REG_BINARY type contain raw binary data and are displayed in hexadecimal format.

The following table lists the possible data types:

Data Type	Name	Description
REG_BINARY	Binary Value	Raw binary data. Most hardware component information is stored as binary data and is displayed in hexadecimal format.
REG_DWORD	DWORD Value	Data represented by a number that is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in binary, hexadecimal, or decimal format. Related values are DWORD_LITTLE_ENDIAN (least significant byte is at the lowest address) and REG_DWORD_BIG_ENDIAN (least significant byte is at the highest address).
REG_EXPAND_SZ	Expandable String Value	A variable-length data string. This data type includes variables that are resolved when a program or service uses the data.

Data Type	Name	Description
REG_FULL_RESOURCE_DESCRIPTOR	Binary Value	A series of nested arrays deigned to store a resource list used by a physical hardware device. This data is displayed in hexadecimal format as a Binary Value.
REG_LINK	Link	A Unicode string naming a symbolic link.
REG_MULTI_SZ	Multi-String Value	A multiple string. Values that contain lists or multiple values in a format that people can read are usually this type. Entries are separated by spaces, commas, or other marks.
REG_NONE	None	Data with no particular type. This data is written to the registry by the system or applications and is displayed in hexadecimal format as a Binary Value.
REG_QWORD	QWORD Value	Data represented by a number that is a 64-bit integer.
REG_RESOURCE_LIST	Binary Value	A series of nested arrays designed to store a resource list used by a hardware device driver or one of the physical devices it controls. This data is detected by the system and is displayed in hexadecimal format as a Binary Value.
REG_RESOURCE_ REQUIREMENTS_LIST	Binary Value	A series of nested arrays designed to store a device driver's list of possible hardware resources it or one of the physical devices it controls can use. This data is detected by the system and is displayed in hexadecimal format as a Binary Value.
REG_SZ	String Value	A fixed-length text string.

Additional Considerations

If there are multiple users on a single machine, you must be aware of the following issues when conducting a forensic investigation:

- If there are individual profiles for each user on the system, you need to locate the User.dat file for the person who proceeds you.
- If all the users on the system are using the same profile, everyone's information is stored in the same User.dat file. Therefore, you will have to find other corroborating evidence because you cannot associate evidence in the User.dat file with a specific user profile.
- On Windows 9*x* systems, the User.dat file for the default user is used to create the User.dat files for new user profiles. Consequently, the User.dat files for new profiles can inherit a lot of junk.

To access the Windows registry from an image of the suspect's drive, you can do any of the following:

- Boot the suspect's image to view his or her registry in Registry Editor.
- Mount a restored image as a drive, launch Registry Editor at the command line from your processing machine, export the registry files from the restored image, then view them in a third-party tool.

  Note: The problem with this method is that you can only view the registry as text. Registry Editor displays everything in ASCII so you can't hex or binary values in the registry.

  - Export the registry files from the image and view them in a third-party tool.
  - Use AccessData Registry Viewer! Registry Viewer seamlessly integrates with FTK so you can view registry files within the image and generate reports.

Registry Viewer shows everything you normally in live systems using the Windows Registry Editor. However, unlike Registry Editor and other tools that use the Windows API, Registry Viewer decrypts protected storage information so you can view values in the Protected Storage System Provider key (PSSP). Registry Viewer also shows information that is normally hidden in null-terminated keys.

Information stored in the registry—Internet Messenger sessions, Microsoft Office MRU lists, usernames and passwords for Internet Websites accessed through Internet Explorer, and so forth—are temporarily stored in HKEY_CURRENT_USER. When the user closes an application or logs out, the hive's cached information is pulled out of memory and written to the user's corresponding User.dat file.

Passwords and MRU lists are not saved unless these options are enabled.

Important: Because normal seizure procedures require that you not alter the suspect machine in any way, you must be able to articulate why you closed any active applications before pulling the plug on the suspect's computer.

Registry Quick Find Chart

The following charts discuss common locations where you can find data of forensic interest in the registry.

- "System Information" on page 325
- "Networking" on page 327
- "User Data" on page 328
- "User Application Data" on page 329

System Information

Current Control Set	System	Select	Identifies the which control set is current.
Dynamic Disk	System	ControlSetXXX\Services\DMIO\Boot Info\Primary Disk Group	Identified the most recent dynamic disk mounted in the system.
Event Logs	System	ControlSetXXX\Services\Eventlog	Location of Event logs.
Information	File	Location	Description
Last User Logged In	Software	Microsoft\Windows NT\CurrentVersion\Winlogon	Last user logged in - can be local or domain account.

Logon Banner Message	Software	Microsoft\Windows\Current Version\Policies\System\Legal NoticeText	This is a banner that users must click through to log on to a system.
Logon Banner Message	Software	Microsoft\Windows\Current Version\Policies\System\Legal NoticeCaption	User defined data.
Logon Banner Title	Software	Microsoft\Windows\Current Version\Policies\System\Legal NoticeCaption	User defined data.
Mounted Devices	System	MountedDevices	Database of current and prior mounted devices that received a drive letter.
O\S Version	Software	Microsoft\Windows NT\ CurrentVersion	
Pagefile	System	ControlSetXXX\Control\ Session Manager\Memory Management	Location, size, set to wipe, etc.
Product ID	Software	Microsoft\Windows NT\ CurrentVersion	
Registered Organization	Software	Microsoft\Windows NT\ CurrentVersion	This information is entered during installation, but can be modified later.
Registered Owner	Software	Microsoft\Windows NT\ CurrentVersion	This information is entered during installation, but can be modified later.
Run	Software	Microsoft\Windows\Current Version\Run	Programs that appear in this key run automatically when the system boots.
Shutdown Time	System	ControlSetXXX\Control\Windows	System shutdown time.
Time Zone	System	ControlSet001(or002)\Control\ TimeZoneInformation\Standard Name	This information is entered during installation, but can be modified later.

Networking

Information	File	Location	Description
Map Network Drive MRU	ntuser.dat	Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	Most recently used list mapped network drives.
TCP\IP data	System	ControlSetXXX\Services\TCPIP\Parameters	Domain, hostname data.
TCP\IP Settings of a Network Adapter	System	ControlSetXXX\Services\ *adapter*\Parameters\TCPIP	IP address, gateway information.
Default Printer	ntuser.dat	Software\Microsoft\Windows NT\CurrentVersion\Windows	Current default printer.
Default Printer	ntuser.dat	\printers	Current default printer.
Local Users	SAM	Domains\Account\Users\Names	Local account security identifiers.
Local Groups	SAM	Domains\Builtin\Aliases\Names	Local account security identifiers.
Profile list	Software	Microsoft\Windows NT\CurrentVersion\ProfileList	Contain user security identifier (only users with profile on the system).
Network Map	ntuser.dat		

User Data

Information	File	Location	Description
Run	ntuser.dat	Software\Microsoft\Windows\ CurrentVersion\Run	Programs that appear in this key run automatically when the user logs on.
Media Player Recent List	ntuser.dat	Software\Microsoft\Media Player\Player\ RecentFileList	This key contains the user's most recently used list for Windows Media Player.
O\S Recent Docs	ntuser.dat	Software\Microsoft\Windows\ CurrentVersion\Explorer\ RecentDocs	MRU list pointing to shortcuts located in the recent directory.
Run MRU	ntuser.dat	\Software\Microsoft\Windows\ CurrentVersion\Explorer\RunMRU	MRU list of commands entered in the “run” box.
Open And Save As Dialog Boxes MRU	ntuser.dat	\Software\Microsoft\Windows\ CurrentVersion\Explorer\ ComDlg32	MRU lists of programs\files opened with or saved with the “open” or “save as” dialog box(es).
Current Theme	ntuser.dat	Software\Microsoft\Windows\ CurrentVersion\Themes	Desktop theme\wallpaper.
Last Theme	ntuser.dat	Software\Microsoft\Windows\ CurrentVersion\Themes\Last Theme	Desktop theme\wallpaper.
File Extensions\ Program Association	ntuser.dat	Software\Microsoft\Windows\ CurrentVersion\Explorer\ FileExts	Identifies associated programs with file extensions.

User Application Data

Information	File	Location	Description
Word User Info	ntuser.dat	Software\Microsoft\office\ *version*\Common\UserInfo	This information is entered during installation, but can be modified later.
Word Recent Docs	ntuser.dat	Software\Microsoft\office\ *version*\Common\Data	Microsoft word recent documents.
IE Typed URL's	ntuser.dat	Software\Microsoft\Internet Explorer\TypedURLs	Data entered into the URL address bar.
IE Auto-Complete Passwords	ntuser.dat	\Software\Microsoft\ Internet Explorer\IntelliForms	Web page auto complete passwords -Encrypted values.
IE Auto-Complete Web Addresses	ntuser.dat	\Software\Microsoft\Protected Storage System Provider	lists Web pages wherein autocomplete was utilized.
IE Default Download Directory	ntuser.dat	Software\Microsoft\Internet Explorer	Default download directory when utilizing Internet Explorer.
Outlook Temporary Attachment Directory	ntuser.dat	Software\Microsoft\office\ *version*\Outlook\Security	Location where attachments are stored when opened from outlook.
AIM	ntuser.dat	Software\America Online\AOL Instant Messenger\CurrentVersion\ Users\username	IM contacts, file transfer information, etc.
Word User Info	ntuser.dat	Software\Microsoft\office\ *version*\Common\UserInfo	This information is entered during installation, but can be modified later.
ICQ	ntuser.dat	\Software\Mirabilis\ICQ\*	IM contacts, file transfer information, etc.

MSN Messenger	ntuser.dat	Software\Microsoft\MSN Messenger\ListCache\.NET MessngerService*	IM contacts, file transfer information, etc.
Kazaa	ntuser.dat	Software\Kazaa\*	Configuration, search, download, IM data, etc.
Yahoo	ntuser.dat	Software\Yahoo\Pager\Profiles\*	IM contacts, file transfer information, etc.
Google Client History	ntuser.dat	Software\Google\NavClient\1.1\History	
Adobe	ntuser.dat	Software\Adobe\*	Acrobat, Photo deluxe, etc.

APPENDIX F

dtSearch Requests

Note: The following text is taken from DT Software, Inc. (Copyright 1991–1997 DT Software, Inc. www.dtsearch.com).

dtSearch supports two types of search requests: natural language, and Boolean.

A natural language search is any sequence of text, like a sentence or a question. After a natural language search, dtSearch sorts retrieved documents by their relevance to your search request.

A Boolean search request consists of a group of words or phrases linked by

connectors such as AND and OR that indicate the relationship between them.

For example:

- apple AND pear   Both words must be present
- apple OR pear   Either word can be present
- apple w/5 pear   "Apple" must occur within five words of "pear"
- apple NOT w/5 pear "Apple" must not occur within five words of "pear"
- apple AND NOT pear Only "apple" must be present
- name CONTAINS smith The field name must contain "smith"

If you use more than one connector, you should use parentheses to indicate precisely for what you want to search.

For example, apple AND pear OR orange juice could mean (apple and pear) or orange, or it could mean apple and (pear or orange).

Words such as “if” and “the,” or noise words, are ignored in searches. Search terms may include the following special characters:

? Matches any single character. For example: appl? matches “apply” or “apple.”

* Matches any number of characters. For example: appl* matches “application.”

~ Stemming. For example: apply~ matches “apply,” “applies,” “applied.”

% Fuzzy search. For example: ba%nana matches “banana,” “bananna.”

# Phonic search. For example: #smith matches “smith,” “smythe.”

& Synonym search. For example: fast& matches “quick.”

~~ Numeric range. For example: 12~~24 matches 18.

: Variable term weighting. For example: apple:4 w/5 pear:1

Words and Phrases

You do not need to use any special punctuation or commands to search for a phrase. Simply enter the phrase the way it ordinarily appears. You can use a phrase anywhere in a search request.

For example: apple w/5 fruit salad

If a phrase contains a noise word, dtSearch will skip over the noise word when searching for it.

For example: a search for “statue of liberty” would retrieve any document containing the word “statue,” any intervening word, and the word “liberty.”

Punctuation inside of a search word is treated as a space.

For example:

• “can't” would be treated as a phrase consisting of two words: “can” and “t”

• “1843(c)(8)(ii)” would become “1843 c 8 ii” (four words)

Wildcards (* and ?)

A search word can contain the wildcard characters asterisk (*) and question mark(?). A question mark in a word matches any single character, and an asterisk matches any number of characters. The wildcard characters can be in any position in a word.

For example:

• appl* would match “apple,” “application,” etc.

• *cipl* would match “principle,” “participle,” etc.

• appl? would match “apply” and “apple,” but not “apples.”

• ap*ed would match “applied,” “approved,” etc.

Use of the asterisk (*) wildcard character near the beginning of a word will slow searches.

Natural Language Searching

A natural language search request is any combination of words, phrases, or sentences. After a natural language search, dtSearch sorts retrieved documents by their relevance to your search request. Weighting of retrieved documents takes into account

• The number of documents in which each word in your search request appears (the more documents a word appears in, the less useful it is in distinguishing relevant from irrelevant documents)

• The number of times each word in the request appears in the documents

- The density of hits in each document; noise words and search connectors like NOT and OR are ignored

Synonym Searching

Synonym searching finds synonyms of a word in a search request.

For example, a search for “fast” would also find “quick.”

You can enable synonym searching for all words in a request, or you can enable synonym searching selectively by adding the ampersand (&) character after certain words in a request.

For example: fast& w/5 search.

Fuzzy Searching

Fuzzy searching will find a word even if it is misspelled.

For example, a fuzzy search for “apple” will find “appple.”

Fuzzy searching can be useful when you are searching text that may contain typographical errors. There are two ways to add fuzziness to searches:

1. Enable fuzziness for all of the words in your search request. You can adjust the level of fuzziness from 1 to 10.

2. You can also add fuzziness selectively using the percentage (%) character. The number of percentage characters you add determines the number of differences dtSearch will ignore when searching for a word. The position of the percentage characters determines how many letters at the start of the word have to match exactly.

For example:

- ba%nana will find words that begin with ba and have at most one difference between it and banana.

- b%%anana will find words that begin with b and have at most two differences between it and banana.

Phonic Searching

Phonic searching looks for a word that sounds like the word you are searching for and begins with the same letter.

For example, a phonic search for “Smith” will also find “Smithe” and “Smythe.”

To ask dtSearch to search for a word phonically, put a pound sign (#) in front of the word in your search request.

For example: #smith, #Johnson

You can also check the Phonic searching box in the search form to enable phonic searching for all words in your search request. Phonic searching is somewhat slower than other types of searching and tends to make searches over-inclusive, so it is usually better to use the pound symbol to do phonic searches selectively.

Stemming

Stemming extends a search to cover grammatical variations on a word.

For example:

- “fish” would also find “fishing.”
- “applied” would also find “applying,” “applies,” and “apply.”

There are two ways to add stemming to your searches:

1. Check the Stemming box in the search form to enable stemming for all of the words in your search request. Stemming does not slow searches noticeably and is almost always helpful in making sure you find what you want.

2. If you want to add stemming selectively, add a tilde (~) at the end of words that you want stemmed in a search.

For example: apply~

Variable Term Weighting

When dtSearch sorts search results after a search, by default all words in a request count equally in counting hits. However, you can change this by specifying the relative weights for each term in your search request.

For example: apple:5 and pear:1 would retrieve the same documents as “apple” and “pear” but dtSearch would weigh “apple” five times as heavily as “pear” when sorting the results.

In a natural language search, dtSearch automatically weights terms based on an analysis of their distribution in your documents. If you provide specific term weights in a natural language search, these weights will override the weights dtSearch would otherwise assign.

AND Connector

Use the AND connector in a search request to connect two expressions, both of which must be found in any document retrieved.

For example:

- “apple pie” and “poached pear” would retrieve any document that contained both phrases.

- (apple or banana) and (pear w/5 grape) would retrieve any document that contained either “apple” or “banana,” and contained “pear” within five words of “grape.”

OR Connector

Use the OR connector in a search request to connect two expressions, at least one of which must be found in any document retrieved.

For example: “apple pie” or “poached pear” would retrieve any document that contained “apple pie,” “poached pear,” or both.

W/N Connector

Use the W/N connector in a search request to specify that one word or phrase must occur within a number of words of the other.

For example:

- “apple w/5 pear” would retrieve any document that contained “apple” within five words of “pear.”
- (apple or pear) w/5 banana
- (apple w/5 banana) w/10 pear
- (apple and banana) w/10 pear

Some types of complex expressions using the W/N connector will produce ambiguous results and should not be used.

For example:

- (apple and banana) w/10 (pear and grape)
- (apple w/10 banana) w/10 (pear and grape)

In general, at least one of the two expressions connected by W/N must be a single word or phrase or a group of words and phrases connected by OR.

For example:

- (apple and banana) w/10 (pear or grape)
- (apple and banana) w/10 orange tree

dtSearch uses two built in search words to mark the beginning and end of a file: xfirstword and xlastword. The terms are useful if you want to limit a search to the beginning or end of a file.

For example: “apple w/10 xlastword” would search for apple within ten words of the end of a document.

NOT and NOT W/N

Use NOT in front of any search expression to reverse its meaning. This allows you to exclude documents from a search.

For example: apple sauce AND NOT pear

NOT standing alone can be the start of a search request.

For example: “NOT pear” would retrieve all documents that did not contain “pear.”

If NOT is not the first connector in a request, you need to use either AND or OR with NOT.

For example:

- apple OR NOT pear
- NOT (apple w/5 pear)

The NOT W/ ("not within") operator allows you to search for a word or phrase not in association with another word or phrase.

For example: apple not w/20 pear

Unlike the W/ operator, NOT W/ is not symmetrical. That is, apple not w/20 pear is not the same as pear not w/20 apple. In the apple not w/20 pear request, dtSearch searches for apple and excludes cases where apple is too close to pear. In the pear not w/20 apple request, dtSearch searches for pear and excludes cases where pear is too close to apple.

Numeric Range Searching

A numeric range search is a search for any numbers that fall within a range. To add a numeric range component to a search request, enter the upper and lower bounds of the search separated by two tildes (~~).

For example: apple w/5 12~~17 would find any document containing “apple” within five words of a number between 12 and 17.

Numeric range searches only work with positive integers. A numeric range search includes the upper and lower bounds (so 12 and 17 would be retrieved in the above example).

For purposes of numeric range searching, decimal points and commas are treated as spaces, and minus signs are ignored.

For example: –123,456.78 would be interpreted as: 123 456 78 (three numbers).

Using alphabet customization, the interpretation of punctuation characters can be changed.

For example: 123,456.78 would be interpreted as 12345678.

APPENDIX G

Corporate Information

This appendix contains information about AccessData and its products.

This appendix includes the following sections:

- "Subscriptions" on page 341
- "Technical Support" on page 341
- "Product Returns" on page 342

Subscriptions

A yearly subscription is now offered on all AccessData software. A subscription is good for one year from the date of purchase.

The AccessData subscription service allows you to download updates from the AccessData Website at any time.

For more information on the general features of the subscription service, the AccessData Website (http://www.accessdata.com).

Technical Support

AccessData offers free technical support on all of its software from 8:00 a.m. to 5:30 p.m. MST.

The following table identifies the different ways to receive technical support.

Phone	Long distance: 1-800-658-5199 Local: 1-801-377-5410
Fax	1-801-377-5426
Website	http://www.accessdata.com ◆ Product-specific FAQs that list common questions and their quick fixes. ◆ Online Support Form to submit for support. All support inquiries are typically answered within 24 hours. If there is an urgent need for support, contact AccessData via phone. ◆ Forensic Bulletin Board provides a forum to share questions and answers with other AccessData users.
E-mail	support@accessdata.com

Product Returns

AccessData has a strict return policy because of the nature of the products. The return policy of AccessData follows directly along with the license agreement. If the utility is unopened and AccessData has not sent an electronic copy of the program, it can be returned at any time within 30 days of purchase. Otherwise, no returns will be accepted unless the product is found to be defective.

GLOSSARY

Cluster

Fixed-length blocks that store files. Each cluster is assigned a unique number by the computer operating system.

Evidence Item

A physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive.

File Item

A file in the case. An evidence item can contain multiple file items. A file item can contain multiple file items, such as a Zip file that can contain many file items.

File Slack

Unused space. Operating systems store files in fixed-length blocks called *clusters*. Because few files are a size that is an exact multiple of the cluster size, there is typically unused space between the end of the file and the end of the last cluster used by that file.

Hashing

Generating a unique alphanumeric value based on a file's contents. The alphanumeric value can be used to prove that a file copy has not been altered in any way from the original. It is statistically impossible for an altered file to generate the same hash number.

Message Digest 5

A 128-bit digital fingerprint based on a file's content that was designed by Ron Rivest of RSA. Message Digest 5 (MD5) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a *hash* or *digest*. The number is derived from the input in such a way that it is computationally infeasible to derive any information about the input from the hash. It is also computationally infeasible to find another file that will produce the same output.

MD5 hashes are used by the KFF to identify known files.

Secure Hash Algorithm

A 160-bit digital fingerprint based on a file's content that was designed by the National Institute of Standards and Technology (NIST). Secure Hash Algorithm (SHA) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a *hash* or *digest*. The number is derived from the input in such a way that it is computationally infeasible to derive any information about the input from the hash. It is also computationally infeasible to find another file that will produce the same output.

FTK uses SHA-1. The KFF library contains some A hashes.

Sector

During a low-level format, hard disks are divided into tracks and sectors. The tracks are concentric circles around the disk and the sectors are segments within each circle. For example, a formatted disk might have 40 tracks, with each track divided into 10 sectors.

Physical sectors are relative to the entire drive. Logical sectors are relative to the partition.

Thumbnail

Smaller size version of graphic image.

Unallocated Space

All the clusters on a drive that are not currently assigned to a file. Also called *free space*. Some of these clusters may still contain data from files that were deleted but have not yet been overwritten by other files.

INDEX

A

acquiring evidence 7
Add Evidence Wizard 99
adding
  carved files 186
  entries to case log 140
  evidence 78, 99, 103
  files to bookmark 130
  Internet Keyword Search List to case 179
  keys to the Common Areas window 207
  keys to the Report window 207
Analysis Tools 135
analyzing evidence 8
applying existing filter 190
archive file types 291
audience 2
audit files, including in report 235

B

backing up case 90
bookmark
  adding files to 130
  carved files 187
  creating 128
  explanation of 128
  export files to report 224
  including in report 224
  Internet keywords 180
  removing 131
  selecting properties for report 226
  window 45

C

carved files
  adding 64, 67, 102, 183, 186
  bookmarking 187
  in existing case 184
case
  advanced searching 175, 181
  entering information in a report 223
  opening existing 94
  processing of 89
  processing of evidence 65, 101, 137
  searching 149, 199
  starting 60
Case Agent Mode 32, 95
Case Agent Mode Manager 95
case log 137
  adding entries to 140
  including in report 235
  sample of 139
  selecting content of 64, 257
  viewing 139
case preferences 255
case.ftk 94, 99, 260, 309, 311, 313
changing viewer settings 253
colors, customizing 245
columns, customizing 249
Common Areas window
  adding keys 207
  deleting keys 207
common operators in regular expressions 303
competencies 2
complex regular expression 297
compressed drive, files not extracted from 276
Copy Special 140, 141, 171
copying information from FTK 140

creating
- bookmark 128
- filter 196
- report 222

credit card number, searching 295, 297
customizing
- colors and fonts 245
- column settings 249

D

data carving 182
- adding files to a new case 64, 67, 102, 183
- in existing case 184

database file types 286
decrypted files
- automatically locating 67, 102
- EFS 217
- viewing 219

deleted material
- recovering 305
- searching for 182

deleting
- filter 197
- keys from the Common Areas window 207
- keys from the Report window 208

Distributed Network Attack (DNA) 4
document file types 282
Dongle 33
dongle driver
- installing from CD 17
- installing from downloadable files 21

dongle packet file
- opening and saving 269
- sending to support 273

Dongle Viewer 55
dongleviewer.exe 312, 313
dtSearch 9, 155

E

editing evidence 81
EFS 217
- decrypting files 67, 102, 218
- understanding 218
- viewing decrypted files 219

e-mail
- attachments not shown 279
- file types 290
- searching for address 177
- window 41

embedded files, searching for 182
evidence
- acquiring 7
- adding 78, 99, 103
- analyzing 8
- editing 81
- excluding 69
- excluding from index 74, 113
- FAT 121
- handling of 2
- not found 278
- not viewable 278
- NTFS 121
- presenting 10
- preserving 2, 7
- previewing 54
- processing at later time 135
- processing of 65, 101, 118, 137
- refining 83
- removing 81

evidence cache size 259
evidence items 35
examiner information, entering 63
excluding
- evidence 69
- evidence from index 74, 113

executables file types 291
explore window 39
exporting
- bookmarked files to report 224
- files 143
- index 155
- registry files 147
- word list 147
- word list in Registry Viewer 214

extracting files from compressed drive 276

F

FAT 121, 306
file category 37

File Filter Manager 190
file items 35
file list
columns 51
including in report 230
searching columns 176
toolbar 50
file listing database 67, 102, 141, 143, 172, 231
file properties
in report 232, 233
viewing 119
file status 36
file systems 13
file types
archive 291
database 286
document 282
e-mail message 290
executables 291
graphic 288
instant messages message 291
known 293
list of recognized 281
spreadsheet 285
files, exporting 143
filter
applying an existing 190
creating 196
deleting 197
modifying 196
using 189
Filter Search Hits dialog 153
fonts, customizing 245
forensic examiner information, entering 63
FTK Imager 54
opening a registry file 205
overview of 7
ftk.log 310
ftkcolumnsettings.ini 250, 310
ftkcrash files 310
ftkfilefilters.ini 196, 279, 311
ftkfileinfo.txt 311
ftksettings.ini 246, 256, 311

G

generating a report in Registry Viewer 213
graphics
file types 288
searching for 182
window 40

H

handling evidence 2
hardware acquisition tools 7
hardware requirements for index 155
hash
databases of 9, 132
importing KFF 132
overview of 8
sample of 8
Hashing 2
HashKeeper database 9, 132
HTML file listing 67, 102

I

image
adding segments to 277
formats 13
verifying integrity of 133
importing KFF hashes 132
index
contents of 154
selecting 65, 101, 137
indexed search 43
conducting 154
installing
dongle driver from CD 17
dongle driver from downloadable files 21
FTK from CD 16
FTK from downloadable files 19
KFF from CD 18
KFF from downloadable files 22
LicenseManager from CD 23
LicenseManager from downloadable files 26
preparation for 14
troubleshooting 275
instant message
file types 291

interface, understanding 31
Internet address
  viewing 178
Internet keywords 177
  adding list to case 179
  bookmarking 180
IP address, searching 295, 302

K

key program files 309
KFF
  see Known File Filter
Known File Filter 9
  installing from CD 18
  installing from downloadable files 22
  location of 259
  upgrading basic from CD 28
  upgrading basic from downloadable files 29
  upgrading customized from downloadable files 30
  upgrading from CD 28
  upgrading from downloadable files 29

L

LicenseManager 55
  adding and removing licenses 269
  installing from CD 23
  installing from downloadable files 26
  interface 264
  managing licenses with 263
  opening and saving dongle packet files 269
  purchasing licenses 274
  removing licenses remotely 270
  sending packet to support 273
  starting 264
  updating products 273
  using 263
  viewing licenses with 269
licenses
  adding and removing 269
  purchasing 274
  viewing 269
live search 44
  conducting 149
local evidence time zone 81, 106

M

managing licenses 263
marking thumbnail 40
MD5
  see Message Digest 5
Message Digest 5 8
  selecting 65, 101, 137
Microsoft Access database
  creating 67, 102, 143
  exporting files to 141
  including in report 231
  search results 172
Mini Log 258
modifying
  filter 196
  report 242

N

New Case Wizard 60
NTFS 13, 81, 218, 306
  decrypt EFS files 67, 102
  evidence type 121
  local time zone 106

O

obtaining protected files 205
online support 342
opening existing case
  in Case Agent Mode 32, 95
  with FTK 94
overview of FTK 6
overview window 34

P

partition
  evidence item 35, 74, 343
  FAT 306
  NTFS 13, 67, 81, 102, 106, 121, 306
password protection in Case Agent Mode 96
password recovery 4
Password Recovery Toolkit 155

overview of 4
preferences 255
Prerender Thumbnails 131
presenting evidence 10
preserving evidence 2, 7
previewing evidence 54
processing
case 89
evidence 118
evidence at later time 135
product
updating 273
product returns 342
program files 309
protected files, obtaining 205
PRTK
see Password Recovery Toolkit

R

recovering
deleted material 305
passwords 4
regexlist.ini 312
registry file
opening with FTK Imager 205
Registry Viewer 199, 316
adding keys to Common Areas window 207
deleting keys from the Common Areas window 207
exporting word list 214
generating a report 213
main window 201
Report window 207, 208
searching for specific data 211
starting 200
regular expression
common operators 303
complex 297
explanation of 295
predefined 300
simple 296
using 149
removing
bookmark 131
evidence 81
report
creating 222
entering case information 223
file list in 230
including audit files in 235
including bookmarks in 224
including case log in 235
including graphic thumbnails in 229
including list of file properties in 232, 233
modifying 242
overview of 10
sample of 239
selecting bookmarked file properties 226
selecting location of 238
updating 241
viewing 239
Report window
adding keys 207
deleting keys 208
Report Wizard 222
requirements
hardware for index 155
requirements, minimum and recommended 12
returns, product 342

S

search window 42
searching
conducting indexed 154
conducting live 149
credit card number 295, 297
defining limits of 157, 161
deleted material 182
e-mail address 177
embedded files 182
file list columns 176
graphics 182
importing terms 163
in viewer 176
interface of indexed 43
interface of live 44
Internet keywords 177
IP address 295, 302
main viewer 176

overview of 9
Registry Viewer for data 211
regular expressions 295
reloading query 164
social security number 295, 300
telephone number 295, 300
viewing results 164
Windows Registry 199
with wildcards 165
Secure Hash Algorithim
selecting 65, 101, 137
securing registry evidence 315
segmented images, adding to case 277
setting multiple temp files 126
SHA-1
see Secure Hash Algorithim
simple regular expression 296
social security number, searching for 295, 300
software acquisition tools 7
spreadsheet file types 285
starting
case 60
case in Case Agent Mode 32, 95
FTK 32
LicenseManager 56
Registry Viewer 200
Startup Dialog box 260
subscription, product 341
support
online 342
receiving technical 341
system
preparation 14
requirements 12

T

technical support 341
telephone number, searching for 295, 300
temp files, setting up multiple 126
thumbnail
creating 65, 101, 131
including in report 229
marking 40
thumbnails
prerender 131
time zone 81, 106
toolbar
file list 50
tree list 49
viewer 48
tree list toolbar 49
troubleshooting 275

U

U.K. telephone number, searching for 300
U.S. telephone number, searching for 300
updating report 241
upgrading
basic KFF from CD 28
basic KFF from downloadable files 29
customized KFF from downloadable files 30
FTK from CD 27
FTK from downloadable files 28
KFF from CD 28
KFF from downloadable files 29
user competencies 2
using
File Filter Manager 190
filter 189

V

verifying image integrity 133
viewer
changing settings of 253
searching 176
toolbar 48
viewing
case log 139
EFS files 219
file properties 119
Internet address 178
report 239
Windows Registry 199

W

wildcards 165
window
bookmark 45
e-mail 41

explore 39
graphics 40
overview 34
Registry Viewer main window 201
Registry Viewer Report window 207, 208
search 42
Windows Registry
file types 316
searching 199
securing evidence 315
viewing 199
Windows 9x file types 317
Windows NT and 2000 file types 318
Windows XP file types 319
word list
exporting in FTK 147
exporting in Registry Viewer 214
workstation, preparing 14