



AccessData®

# FTK®

FORENSIC TOOLKIT®



# *AccessData FTK 3.0*

## **LEGAL INFORMATION**

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.

© 2008 AccessData Corp. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

AccessData Corp.  
384 South 400 West  
Suite 200  
Lindon, Utah 84042  
U.S.A.

[www.accessdata.com](http://www.accessdata.com)

## ACCESSDATA TRADEMARKS

AccessData<sup>®</sup> is a registered trademark of AccessData Corp.

Distributed Network Attack<sup>®</sup> is a registered trademark of AccessData Corp.

DNA<sup>®</sup> is a registered trademark of AccessData Corp.

Forensic Toolkit<sup>®</sup> is a registered trademark of AccessData Corp.

FTK<sup>®</sup> is a registered trademark of AccessData Corp.

Password Recovery Toolkit<sup>®</sup> is a registered trademark of AccessData Corp.

PRTK<sup>®</sup> is a registered trademark of AccessData Corp.

Registry Viewer<sup>®</sup> is a registered trademark of AccessData Corp.

## DOCUMENTATION CONVENTIONS

In AccessData documentation, a greater-than symbol (>) is used to separate actions within a step. Where an entry must be typed in using the keyboard, the variable data is set apart using `[variable_data]` format.

A trademark symbol (®, ™, etc.) denotes an AccessData trademark. All third-party products are denoted with an (\*). Third-party trademarks and copyrights are the property of the trademark and copyright holders. AccessData claims no responsibility for the function or performance of third-party products.

## REGISTRATION

The AccessData product registration is tracked by the USB security device included with your purchase, and is managed by AccessData.

## SUBSCRIPTIONS

AccessData provides an annual licensing subscription with all new product purchases. The subscription allows you to download and install the latest product releases for your licensed products during the active license period. Following the initial licensing period, a subscription renewal is required annually for updating your products. You can renew your subscriptions through your AccessData Sales Representative.

Use LicenseManager to view your current registration information, to check for product updates and to download the latest product versions, where they are available for download. You can also visit our website, [www.accessdata.com](http://www.accessdata.com) anytime to find the latest releases of our products.

For more information, see Managing Licenses in your product manual or on the AccessData website.

## ACCESSDATA CONTACT INFORMATION

Your AccessData Sales Representative is your main contact with AccessData Corp. Also, listed below are the general AccessData telephone number and mailing address, and telephone numbers for contacting individual departments.

### MAILING ADDRESS AND GENERAL PHONE NUMBERS

You can contact AccessData in the following ways:

**TABLE Front-1 Mailing Address, Hours, and Department Phone Numbers**

---

Corporate Headquarters	AccessData Corp. 384 South 400 West Suite 200 Lindon, UT 84042 USA <b>Voice:</b> 801.377.5410 <b>Fax:</b> 801.377.5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales	<b>Voice:</b> 800.574.5199, option 1 <b>Fax:</b> 801.765.4370 <b>Email:</b> Sales@AccessData.com
Federal Sales	<b>Voice:</b> 800.574.5199, option 2 <b>Fax:</b> 801.765.4370 <b>Email:</b> Sales@AccessData.com
Corporate Sales	<b>Voice:</b> 801.377.5410, option 3 <b>Fax:</b> 801.765.4370 <b>Email:</b> Sales@AccessData.com

---

**TABLE Front-1 Mailing Address, Hours, and Department Phone Numbers**

---

Training	<b>Voice:</b> 801.377.5410, option 6 <b>Fax:</b> 801.765.4370 <b>Email:</b> Training@AccessData.com
Accounting	<b>Voice:</b> 801.377.5410, option 4

## TECHNICAL SUPPORT

You can contact AccessData Customer and Technical Support in the following ways:

---

**TABLE Front-2 AccessData Customer & Technical Support Contact Information**

---

Customer Service Hours:	Monday through Friday, 7:00 AM – 6:00 PM (MST)
Customer/Technical Support	<b>Voice:</b> 801.377.5410, option 5
Free technical support is available on all AccessData products.	<b>Voice:</b> 800.658.5199 (Toll-free North America) <b>Email:</b> Support@AccessData.com <b>Website:</b> <a href="http://www.AccessData.com/Support">http://www.AccessData.com/Support</a>

The Support website allows access to Discussion Forums, Downloads, Previous Releases, our Knowledgebase, a way to submit and track your “trouble tickets”, and in-depth contact information.

**Note:** All support inquiries are typically answered within one business day. If there is an urgent need for support, contact AccessData via phone during normal business hours.

## DOCUMENTATION

Please e-mail any typos, inaccuracies, or other problems you find with the documentation to:

**[documentation@accessdata.com](mailto:documentation@accessdata.com)**

## PROFESSIONAL SERVICES

The AccessData Professional Services staff comes with a varied and extensive background in digital investigations including law enforcement, counter-intelligence, and corporate security. Their collective experience in working with both government and commercial entities, as well as in providing expert testimony, enables them to provide a full range of computer forensic and eDiscovery services.

At this time, Professional Services provides support for sales, installation, training, and utilization of FTK. They can help you resolve any questions or problems you may have regarding FTK.

## **CONTACT INFORMATION FOR PROFESSIONAL SERVICES**

- Washington DC: 410.703.9237
- North America: 800.574.5199
- International: +1.801.377.5410

**Email:** [adservices@accessdata.com](mailto:adservices@accessdata.com)





# Table of Contents

<i>AccessData FTK 3.0</i> .....	<i>i</i>
<i>Legal Information</i> .....	<i>i</i>
<i>AccessData Trademarks</i> .....	<i>ii</i>
<i>Documentation Conventions</i> .....	<i>ii</i>
<i>Registration</i> .....	<i>ii</i>
<i>Subscriptions</i> .....	<i>ii</i>
<i>AccessData Contact Information</i> .....	<i>iii</i>
<i>Mailing Address and General Phone Numbers</i> .....	<i>iii</i>
<i>Technical Support</i> .....	<i>iv</i>
<i>Documentation</i> .....	<i>iv</i>
<i>Professional Services</i> .....	<i>iv</i>
<i>Contact Information for Professional Services</i> .....	<i>v</i>
<i>Table of Contents</i> .....	<i>vii</i>
<i>Chapter 1 Introduction to AccessData Products</i> .....	<i>1</i>
<i>Audience</i> .....	<i>1</i>
<i>Role of AccessData Forensic Investigation Tools</i> .....	<i>1</i>
<i>AccessData Forensic Products</i> .....	<i>2</i>
<i>AccessData eDiscovery</i> .....	<i>2</i>
<i>AccessData Enterprise</i> .....	<i>3</i>

<i>Forensic Toolkit</i> .....	3
<i>FTK Imager</i> .....	4
<i>Lab</i> .....	5
<i>Language Selector</i> .....	5
<i>Mobile Phone Examiner</i> .....	5
<i>Registry Viewer</i> .....	6
<i>SilentRunner</i> .....	6
<i>Password Discovery and File Decryption</i> .....	6
<i>DNA and PRTK</i> .....	6
<i>Features Overview</i> .....	7
<i>DNA and PRTK Add-Ons</i> .....	7
<i>Portable Office Rainbow Tables</i> .....	7
<i>Rainbow (Hash) Tables</i> .....	8
<i>TACC Unit</i> .....	9
<i>License Management</i> .....	9
<i>CodeMeter Runtime</i> .....	9
<i>LicenseManager</i> .....	10
<i>Chapter 2 AccessData Forensic Toolkit 3.0 Overview</i> .....	11
<i>Computer Forensic Investigation Overview</i> .....	11
<i>Acquiring the Evidence</i> .....	12
<i>Preserving the Evidence</i> .....	12
<i>Analyzing the Evidence</i> .....	12
<i>Indexing and Hashing</i> .....	12
<i>Searching</i> .....	14
<i>Bookmarking</i> .....	14
<i>Presenting Evidence</i> .....	14
<i>Managing Cases</i> .....	15
<i>Chapter 3 AccessData Forensic Toolkit Installation</i> .....	17
<i>Installation Information</i> .....	17
<i>Hardware Considerations</i> .....	18
<i>Estimating Hard Disk Space Requirements</i> .....	18
<i>Configuration Options</i> .....	19

<i>Installing FTK</i> .....	19
<i>Install CodeMeter</i> .....	20
<i>Install Oracle</i> .....	20
<i>Single Computer Installation</i> .....	21
<i>Install FTK</i> .....	21
<i>Install the Evidence Processing Engine</i> .....	22
<i>Install the KFF Library</i> .....	22
<i>Installing on Separate Computers</i> .....	22
<i>Additional Programs</i> .....	23
<i>Install Language Selector</i> .....	23
<i>Using Language Selector 2</i> .....	3
<i>Licensing</i> .....	24
<i>Chapter 4 The FTK 3.0 User Interface</i> .....	25
<i>About Evidence</i> .....	25
<i>Acquiring and Preserving Static Evidence</i> .....	25
<i>Acquiring and Preserving Live Evidence</i> .....	26
<i>Acquiring Remote Evidence</i> .....	26
<i>Create a Case</i> .....	26
<i>Open an Existing Case</i> .....	27
<i>Add Evidence</i> .....	27
<i>Work The Case</i> .....	27
<i>Identify Meaningful Evidence</i> .....	27
<i>Generate Reports</i> .....	28
<i>Moving Forward</i> .....	28
<i>Using the CodeMeter Stick</i> .....	29
<i>Starting FTK</i> .....	29
<i>Set Up the Application Administrator</i> .....	29
<i>Basics of The FTK 3.0 User Interface</i> .....	30
<i>Using the Case Manager Window</i> .....	30
<i>Case List</i> .....	33
<i>Create a New Case</i> .....	33
<i>Case Management</i> .....	33
<i>Backing Up the Case</i> .....	34

<i>Archiving a Case</i> .....	35
<i>Archive and Detach a Case</i> .....	35
<i>Attach a Case</i> .....	36
<i>Restore a Case</i> .....	36
<i>Delete a Case</i> .....	37
<i>Storing Case Files</i> .....	37
<i>The FTK User Interface</i> .....	37
<i>Undocking</i> .....	45
<i>Toolbar Components</i> .....	45
<i>File List Pane</i> .....	46
<i>File List Toolbar</i> .....	47
<i>File List View Right-Click Menu</i> .....	48
<i>QuickPicks Filter</i> 50	
<i>The Data Processing Status Screen</i> .....	51
<i>Chapter 5 Starting a New FTK 3.0 Case</i> .....	53
<i>Launch FTK</i> .....	53
<i>Assigning Roles</i> .....	56
<i>Creating a Case</i> .....	57
<i>Selecting Evidence Processing Options</i> .....	58
<i>Fuzzy Hashing</i> .....	63
<i>Creating a Fuzzy Hash Library</i> .....	64
<i>Selecting Fuzzy Hash Options During Initial Processing</i> .....	64
<i>Additional Analysis Fuzzy Hashing</i> .....	65
<i>Comparing Files Using Fuzzy Hashing</i> .....	67
<i>Viewing Fuzzy Hash Results</i> .....	67
<i>Selecting dtSearch* Text Indexing Options</i> .....	68
<i>Indexing a Case</i> .....	68
<i>dtSearch Indexing Space Requirements</i> .....	68
<i>New Case Indexing Options</i> .....	68
<i>Selecting Data Carving Options</i> .....	69
<i>Explicit Material Identification</i> .....	71
<i>Selecting Evidence Discovery Options</i> .....	72
<i>Creating the Custom File Identification File</i> .....	73

<i>Selecting Evidence Refinement (Advanced) Options</i> .....	74
<i>Refining Evidence by File Status/Type</i> .....	75
<i>Refining Evidence by File Date/Size</i> .....	77
<i>Selecting Index Refinement (Advanced) Options</i> .....	78
<i>Refining an Index by File Status/Type</i> .....	79
<i>Refining an Index by File Date/Size</i> .....	80
<i>Creating the Case</i> .....	82
<i>Adding Evidence to a New Case</i> .....	82
<i>Processing Evidence</i> .....	85
<i>Viewing Processed Items</i> .....	86
<i>The FTK User Interface</i> .....	86
<i>Chapter 6 Adding and Processing Static Evidence</i> .....	87
<i>Static Evidence vs. Remote Evidence</i> .....	87
<i>Acquiring and Preserving Static Evidence</i> .....	88
<i>Opening an Existing Case</i> .....	88
<i>Adding Evidence</i> .....	88
<i>Selecting a Language</i> .....	92
<i>Additional Analysis</i> .....	93
<i>Hashing</i> .....	96
<i>Data Carving</i> .....	97
<i>Data Carving Files When Processing a New Case</i> .....	97
<i>Data Carving Files in an Existing Case</i> .....	98
<i>The FTK User Interface</i> .....	98
<i>FTK Menus and Toolbars</i> .....	99
<i>Menu Bar Components</i> .....	99
<i>File Menu Options</i> .....	100
<i>Edit Menu Options</i> .....	107
<i>View Menu Options</i> .....	110
<i>Evidence Menu Options</i> .....	112
<i>Filter Menu Options</i> .....	112
<i>Tools Menu Options</i> .....	113
<i>Help Menu Options</i> .....	115
<i>Toolbar Components</i> .....	115

<i>QuickPicks Filter</i> .....	116
<i>File List Pane</i> .....	118
<i>File List Toolbar</i> .....	119
<i>Using Tabs</i> .....	120
<i>Chapter 7 Adding and Processing Remote Live Evidence</i> .....	121
<i>Acquiring and Preserving Remote Evidence</i> .....	121
<i>FTK Role Requirements</i> .....	122
<i>Acquiring Data Remotely</i> .....	122
<i>Provide Credentials</i> .....	123
<i>Remote Disk Management System (RDMS) Additional Information</i> .....	126
<i>RDMS Requirements for Manual Deployment</i> .....	126
<i>Utilizing the Agent</i> .....	126
<i>Chapter 8 Using Tabs to Explore &amp; Refine Evidence</i> .....	129
<i>Using Tabs to Explore and Refine Evidence</i> .....	129
<i>Explore Tab</i> .....	130
<i>Viewer Pane</i> .....	133
<i>Properties Tab</i> .....	134
<i>Hex Interpreter Tab</i> .....	137
<i>File Content Tab</i> .....	139
<i>Hex Tab</i> .....	139
<i>Text Tab</i> .....	141
<i>Filtered Tab</i> .....	142
<i>Natural Tab</i> .....	143
<i>Overview Tab</i> .....	144
<i>File Items Container</i> .....	144
<i>File Extension Container</i> .....	145
<i>File Category Container</i> .....	145
<i>File Status Container</i> .....	146
<i>Bookmark Container</i> .....	148
<i>Email Tab</i> .....	148
<i>Email Status Tree</i> .....	148
<i>Email Tree</i> .....	148

<i>Graphics Tab</i> .....	148
<i>Using Thumbnails</i> .....	149
<i>Moving the Thumbnails Pane</i> .....	149
<i>The Bookmarks Tab</i> .....	150
<i>Creating a Bookmark</i> .....	151
<i>Viewing Bookmark Information</i> .....	154
<i>Bookmarking Selected Text</i> .....	156
<i>Adding to an Existing Bookmark</i> .....	158
<i>Creating Email or Email Attachment Bookmarks</i> .....	159
<i>Adding Email and Email Attachments to Bookmarks</i> .....	160
<i>Moving a Bookmark</i> .....	162
<i>Deleting a Bookmark</i> .....	162
<i>Deleting Files from a Bookmark</i> .....	163
<i>Search Tabs</i> .....	163
<i>Live Search Tab</i> .....	163
<i>Index Search Tab</i> .....	164
<i>Volatile Tab</i> .....	165
<i>Creating Tabs</i> .....	165
<i>Chapter 9 Searching a Case</i> .....	175
<i>Conducting a Live Search</i> .....	175
<i>Customizing the Live Search Tab</i> .....	179
<i>Conducting a Pattern Search</i> .....	179
<i>Simple Pattern Searches</i> .....	180
<i>Complex Pattern Searches</i> .....	180
<i>Predefined Regular Expressions</i> .....	182
<i>Creating Custom Regular Expressions</i> .....	187
<i>Conducting Hex Searches</i> .....	188
<i>Conducting Text Searches</i> .....	188
<i>Conducting an Index Search</i> .....	189
<i>Search Terms</i> .....	191
<i>Search Criteria</i> .....	192
<i>Index Search Options</i> .....	192
<i>Documenting Search Results</i> .....	195

<i>Using Copy Special to Document Search Results</i> .....	196
<i>Bookmarking Search Results</i> .....	199
<i>Chapter 10 Using Filters</i> .....	205
<i>The Filter Toolbar</i> .....	205
<i>Using Filters</i> .....	206
<i>Predefined Filters</i> .....	206
<i>Customizing Filters</i> .....	209
<i>Creating a Filter</i> .....	209
<i>Refining a Filter</i> .....	209
<i>Exporting a Filter</i> .....	210
<i>Deleting a Filter</i> .....	210
<i>Using the Known File Filter</i> .....	211
<i>A Closer Look at the AccessData KFF Library</i> .....	211
<i>KFF Library Sources</i> .....	211
<i>Importing KFF Hashes</i> .....	213
<i>Exporting KFF Hashes</i> .....	215
<i>Understanding How the KFF Database is Used 2</i> .....	16
<i>Storing Hashes in the KFF Database</i> .....	216
<i>Creating Sets and Groups</i> .....	218
<i>Chapter 11 Decrypting EFS and Other Encrypted Files</i> .....	225
<i>Understanding EFS</i> .....	225
<i>Decrypting EFS Files and Folders</i> .....	226
<i>Decrypting Windows EFS Files</i> .....	227
<i>Understanding EFS</i> .....	227
<i>Windows 2000 and XP Systems Prior to SP1</i> .....	227
<i>Windows XP SP1 or Later</i> .....	228
<i>Viewing the Decrypted Files</i> .....	228
<i>Decrypting Domain Account EFS Files from Live Evidence</i> .....	228
<i>Decrypting Credential Files</i> .....	235
<i>Using an Offline Key Bundle</i> .....	236
<i>Using an Online Key Bundle</i> .....	236
<i>Decrypting Safeguard Utimaco Files</i> .....	238



<i>Decrypting SafeBoot Files</i> .....	239
<i>Decrypting Guardian Edge Files</i> .....	240
<i>Decrypting an Image Encrypted With PGP® Whole Disk Encryption (WDE)</i> .....	240
<i>About PGP® Corporation and PGP® Whole Disk Encryption</i> .....	241
<i>PGP® WDE Decryption in FTK 3.0</i> .....	241
<i>Chapter 12 Working with Reports</i> .....	245
<i>Creating a Report</i> .....	245
<i>Saving Your Settings</i> .....	246
<i>Entering Case Information</i> .....	247
<i>Managing Bookmarks in a Report</i> .....	249
<i>Managing Graphics in a Report</i> .....	251
<i>Selecting a File Path List</i> .....	253
<i>Adding a File Properties List</i> .....	254
<i>Registry Selections</i> .....	255
<i>Selecting the Report Output Options</i> .....	256
<i>Customizing the Formatting of Reports</i> .....	257
<i>Creating the Report</i> .....	259
<i>Viewing and Distributing a Report</i> .....	259
<i>Modifying a Report</i> .....	261
<i>Printing a Report</i> .....	261
<i>Chapter 13 Customizing the FTK Interface</i> .....	263
<i>Customizing Overview</i> .....	263
<i>The View Menu</i> .....	264
<i>The Tab Layout Menu</i> .....	265
<i>Moving View Panes</i> .....	265
<i>Creating Custom Tabs</i> .....	267
<i>Customizing File List Columns</i> .....	268
<i>Creating and Modifying Column Settings</i> .....	268
<i>Available Columns</i> .....	269
<i>Common Features</i> .....	269
<i>Disk Image Features</i> .....	271
<i>Email Features</i> .....	271

<i>Entropy Statistics</i> .....	274
<i>File Status Features</i> .....	275
<i>File System Features</i> .....	275
<i>DOS File Systems</i> .....	276
<i>ext2 File Systems</i> .....	277
<i>HFS File Systems</i> .....	277
<i>NTFS File Systems</i> .....	278
<i>Unix Security File Systems</i> .....	278
<i>Mobile Devices</i> .....	278
<i>Zip-specific Features</i> .....	279
<i>Temporary File Folder</i> .....	279
<i>Data Carving</i> .....	279
<i>Appendix A File Systems and Drive Image Formats</i> .....	281
<i>File Systems</i> .....	282
<i>Hard Disk Image Formats</i> .....	282
<i>CD and DVD Image Formats</i> .....	282
<i>Appendix B Recovering Deleted Material</i> .....	283
<i>EAT 12, 16, and 32</i> .....	283
<i>NTFS</i> .....	284
<i>ext2</i> .....	284
<i>ext3</i> .....	284
<i>HFS</i> .....	284
<i>Appendix C Program Files</i> .....	285
<i>Files and Folders for the Application</i> .....	285
<i>Files and Folders for the Database</i> .....	286
<i>Changing Registry Options</i> .....	286
<i>Appendix D Gathering Windows Registry Evidence</i> .....	287
<i>Understanding the Windows Registry</i> .....	287
<i>Windows 9x Registry Files</i> .....	288

<i>Windows NT and Windows 2000 Registry Files</i> .....	289
<i>Windows XP Registry Files</i> .....	290
<i>Possible Data Types</i> .....	292
<i>Additional Considerations</i> .....	293
<i>Seizing Windows Systems</i> 294	
Registry Quick Find Chart.....	294
<i>System Information</i> .....	295
<i>Networking</i> .....	296
<i>User Data</i> .....	296
<i>User Application Data</i> .....	297
<i>Appendix E Managing Security Devices and Licenses</i> .....	299
<i>NLS Support</i> .....	299
<i>Installing and Managing Security Devices</i> .....	299
<i>Installing the Security Device</i> .....	299
<i>Installing the CodeMeter Runtime Software</i> .....	300
<i>Installing Keylok Dongle Drivers</i> .....	305
<i>Installing LicenseManager</i> .....	308
<i>Managing Licenses with LicenseManager</i> .....	310
<i>Starting LicenseManager</i> .....	312
<i>The LicenseManager Interface</i> .....	314
<i>The Installed Components Tab 3</i> .....	14
<i>The Licenses Tab</i> .....	316
<i>Opening and Saving Dongle Packet Files</i> .....	319
<i>Adding and Removing Product Licenses</i> .....	320
<i>Remove a License</i> .....	320
<i>Add a License</i> .....	321
<i>Adding and Removing Product Licenses Remotely</i> .....	322
<i>Add a License Remotely</i> .....	322
<i>Remove a License Remotely</i> .....	323
<i>Updating Products</i> .....	325
<i>Check for Product Updates</i> .....	325
<i>Download Product Updates</i> .....	325
<i>Purchase Product Licenses</i> .....	326

*Send a Dongle Packet File to Support* ..... 326

*AccessData Glossary*..... 327

# *Chapter 1 Introduction to AccessData Products*

This chapter addresses the roles of the AccessData forensic investigation tools.

## **AUDIENCE**

AccessData forensic investigation software tools are intended for law enforcement officials and corporate security and IT professionals who need to access and evaluate the evidentiary value of files, folders, and computers.

In addition, law enforcement and corporate security professionals should possess the following competencies:

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

## **ROLE OF ACCESSDATA FORENSIC INVESTIGATION TOOLS**

AccessData provides world-class products to address every aspect and phase of computer forensics investigations, including evidence gathering and imaging, analysis

tools, password cracking and data decryption, and reporting. The following section provides insight into the various products available to address various needs and environments where digital evidence can be very useful. For more information on any of these products, please visit our website, [www.accessdata.com](http://www.accessdata.com).

**Note:** FTK 2+ and FTK 2+-based products require the CodeMeter Runtime Kit and Wibu CodeMeter USB device (CmStick). Some other AccessData products may still be run using the Keylok dongle and related dongle drivers.

## ACCESSDATA FORENSIC PRODUCTS

This section provides basic information about AccessData's forensic investigation products. The products are listed alphabetically, by product type.

## ACCESSDATA EDISCOVERY

AccessData eDiscovery is truly a landmark technology that virtually walks you through each and every step of the eDiscovery lifecycle. Fortune 500 companies are quickly turning to eDiscovery, because it is the only true custodian-based, end-to-end eDiscovery solution on the market today.

AccessData eDiscovery is a product designed to gather the data required to investigate a legal matter. eDiscovery is designed to allow the tracking of multiple legal matters and the groupings of their data, termed "collections." Each collection can contain human, share, or computer "custodians" (or combinations of the three) of data required for the legal matter. Filters can be designed to exclude or include specific types of files. The collection can be run across the entire network of a company or enterprise.

Furthermore, AD eDiscovery is by far the easiest to use with an intuitive dashboard that conveys the real-time status of all collection activities. True custodian data mapping, the ability to schedule and manage ongoing and periodic collections to better address ongoing litigation matters, as well as powerful processing and reporting are just a few of the reasons eDiscovery is the new revelation in the industry. Not only does it give you the power to address each phase of the process in-house, but it allows you to search and collect data from network shares, email servers, Documentum, SharePoint, Open Text, databases and other structured data repositories. This gives you a level of reach unmatched by any other e-discovery solution. Simply compare other solutions' capabilities to eDiscovery and you will see why so many people are switching.

For more information about eDiscovery, see the AccessData Web site at (<http://www.accessdata.com/Products/eDiscovery.aspx>).

## ACCESSDATA ENTERPRISE

AccessData Enterprise takes network-enabled digital investigations to the next level. AD Enterprise is a powerful, enterprise-scale investigative solution built on our industry-standard, court-validated FTK technology. With an integrated Oracle database on the back-end, true multi-processor support and robust processing capabilities, Enterprise provides the most powerful investigative solution on the market. It handles larger data sets than other investigative solutions and processes data at greater speeds. AccessData Enterprise delivers state-of-the-art incident response capabilities, deep dive analysis of both volatile and static data, as well as superior threat detection capabilities — all within an easy-to-use interface. A role-based permission system, an intuitive incident response console, secure batch remediation capabilities, unsurpassed searching and filtering, and comprehensive logging and reporting are just a few of the reasons Enterprise is quickly being adopted by Fortune 500 companies.

Enterprise gives visibility into data and systems across an enterprise network. It enables proactive or reactive location, preservation, and containment of confidential and personal data leakage, as well as address the most sensitive employee issues.

It optimizes incident response by enabling easy and quick deep analysis to determine the “who”, “what”, “when”, “where” and “how” of any given event and to zero-in on all affected machines. With the seamless integration of static and volatile data, examiners are able to analyze, collect, contain and report on any type of data.

For more information on Enterprise, see the AccessData Web site (<http://www.accessdata.com/Products/Enterprise.aspx>).

## FORENSIC TOOLKIT

AccessData Forensic Toolkit (FTK) provides award-winning technology that is used by law enforcement and corporate security professionals to filter, analyze, investigate, and report on acquired evidence.

FTK provides users with the ability to perform complete and thorough computer forensic examinations. FTK features powerful file filtering and search functionality. FTK customized filters allow you to sort through thousands of files so you can quickly find the evidence you need. FTK is recognized as the leading forensic tool for performing email analysis. In addition, outstanding bookmarking and reporting functions add to the power and usability of the product.

AccessData Forensic Toolkit is recognized around the world as the standard in computer forensic investigation technology. This court-validated platform delivers cutting edge analysis, decryption and password cracking all within an intuitive,

customizable and user-friendly interface. In addition, with FTK you have the option of utilizing a back-end database to handle large data sets. You get the benefit of best-of-breed technologies that can be expanded to meet your ever-changing needs. Known for its intuitive functionality, email analysis, customizable data views and stability, FTK is the smart choice for stand-alone forensic investigations.

For more information about FTK, or any other AccessData product, see the AccessData website at [www.accessdata.com](http://www.accessdata.com).

## FTK IMAGER

FTK Imager is an AccessData software evidence acquisition tool. It can quickly preview evidence and, if the evidence warrants further investigation, create a forensically sound image of the disk. It makes a bit-by-bit duplicate of the media, rendering a forensic image identical in every way to the original, including file slack, and unallocated and drive free space.

Imager performs the following tasks:

- Preview files and folders on local hard drives, network drives, floppy diskettes, Zip disks, CDs, DVDs, SD cards, and USB storage devices.
- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, DVDs, USB storage devices, and othes.
- Preview the contents of forensic images stored on the local computer or on a network drive.
- Export files and folders from forensic images.
- Generate hash reports for regular files and disk images (including files inside disk images.)

**Important:** When using Imager to create a forensic image of a hard drive, use a hardware-based write-blocking device as well. This ensures that the operating system does not alter the hard drive data while attached to the imaging computer.

Use Imager to create a hash of the original drive image that can be referenced later as a benchmark to prove the integrity of the case evidence. Imager verifies that the drive image hashes and the drive hash match when the drive image is created. Two hash functions are available in FTK Imager: Message Digest 5 (MD5), and Secure Hash Algorithm (SHA-1 & SHA -256).



After you create a drive image or custom image of the data, use FTK to perform a complete and thorough forensic examination and create a report of your findings.

## **LAB**

The AccessData Lab family of solutions enables labs of all sizes, facing an array of challenges, to work more effectively. Single person labs can radically speed up the processing of cases, utilizing the distributed processing in our FTK Pro solution. Labs that have expanded a little can extend the distributed processing capabilities of Pro, and add collaborative work and web-enabled case management. Finally large labs that either utilize a distributed workforce or would like to collaborate with attorneys, HR personnel or any other non-forensic investigators can step up to Lab, which adds powerful and intuitive web-based review. Regardless of the size, scope or mission of your lab, AccessData Lab has a solution that will meet your needs.

## **LANGUAGE SELECTOR**

AccessData Language Selector is a utility that allows you to choose a language codepage to view your cases in. Currently, FTK, Imager, and Registry Viewer are localized. FTK currently supports only English, so Language Selector is not included on the FTK installation discs. If you need Language Selector for the AccessData programs that support additional languages, download it from the AccessData website, [www.accessdata.com/support](http://www.accessdata.com/support). Select Downloads and find it in the list of Utilities.

## **MOBILE PHONE EXAMINER**

Mobile Phone Examiner is an AccessData program that reads and images data from cell phones and cell phone data card readers. It can run as a standalone program or as an add-on to FTK.

When run as a standalone, it reads and images the data. You then would add the image file to a case in FTK.

When installed on a machine that also has FTK installed, the phone or device can be detected when adding new evidence, and the data, when imaged, is automatically added to the current FTK case.

## **REGISTRY VIEWER**

AccessData Registry Viewer<sup>®</sup> allows you to view the contents of Windows operating system registry files. Unlike Windows Registry Editor, which only displays the registry of the current system, Registry Viewer lets you examine registry files from any Windows 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.

## **SILENTRUNNER**

SilentRunner enables you to answer the difficult question of “What happened?” in the aftermath of a security incident by tackling the complicated tasks of capturing, analyzing and visualizing network data. It is a passive network monitoring solution that visualizes network activity by creating a dynamic picture of communication flows, swiftly uncovering break-in attempts, weaknesses, abnormal usage, policy violations and misuse, and anomalies — before, during and after an incident. Operating like a surveillance camera, SilentRunner can play back events from thousands of communications to validate system threats and investigate security breaches. This dramatically enhances your ability to identify offenders, determine root cause, and mitigate the recurrence of the same security incident. In addition, it helps monitor infractions to regulatory controls and policy violations, providing supporting reports for auditing requirements and contributing to your ability to demonstrate compliance.

## **PASSWORD DISCOVERY AND FILE DECRYPTION**

AccessData offers two superior programs for file decryption and password discovery. In addition, AccessData offers add-ons that provide impressive enhancements to the speed of these applications.

## **DNA AND PRTK**

DNA and PRTK have essentially the same program interface and they work essentially the same way. Both programs analyzes file signatures to find encryption types and determine which recovery modules to use.

DNA and PRTK perform recoveries on protected files using various methods, including decryption and dictionary attacks. For difficult password key values, PRTK performs dictionary attacks using various types of dictionaries, including the Golden Dictionary

(containing previously recovered passwords), as well as Biographical, Custom User, and Default dictionaries.

## FEATURES OVERVIEW

DNA and PRTK perform the following basic functions:

- Hash files  
Hashing a file uses an algorithm that creates a unique hash value for a file, allowing verification that the contents of a file remain unchanged. When a file is added to PRTK or DNA for key or password recovery, it is hashed. When the key or password is recovered, the file is automatically hashed again to verify that the file itself has remained unchanged. This is particularly helpful to law enforcement personnel who need to verify that a file has not been changed while recovering a password.
- Recover passwords  
PRTK can recover the password to files created in many popular industry applications by using a variety of methods, including several types of dictionaries used within profiles, in combination with rules to achieve the desired results. PRTK can also recover multi-lingual passwords.
- Generate reports  
You can now print job information reports for password recovery jobs in .PDF format.
- Open encrypted files

You can use recovered keys or passwords to open recovered files, if the applications the files originated from are available and installed on a computer you have access to. Recovered files can be copied or moved to any location.

## DNA AND PRTK ADD-ONS

The following add-ons are available to enhance the power and speed of password-cracking with PRTK and/or DNA:

### PORTABLE OFFICE RAINBOW TABLES

Rainbow Tables are also pre-computed, brute-force attacks. AccessData Portable Office Rainbow Tables (PORT) are different from the full Hash tables set. A statistical analysis is done on the file itself to determine the available keys. This takes far less

space than the Hash Tables, but also takes somewhat more time and costs a small percentage in accuracy.

As previously stated, a system set at 40-bit encryption has one trillion keys available. A brute-force attack of 500,000 keys per second would take approximately 25 days to exhaust the key space combinations of a single file using a single 3 Ghz Pentium 4 computer. With Portable Office Rainbow Tables, you can decrypt 40-bit encrypted files Microsoft Word or Excel files, usually in seconds, minutes, or hours, rather than days or weeks, depending on the power of the system you are using. DNA and PRTK seamlessly integrate with PORT

### **Product Features**

- 40-bit encrypted files decrypted in 5 minutes on average
- One table available: MS Word & Excel (MS Office)
- Completely portable, fits on your laptop
- 98.6% accuracy for MS Office Word and Excel files.

PORT for Word and Excel takes only about 3.7 GB of disc space. It is shipped on a single DVD. You can carry it with you! Indispensable for on-site acquisitions and investigations.

## **RAINBOW (HASH) TABLES**

Rainbow Tables are pre-computed, brute-force attacks. In cryptography, a brute-force attack is an attempt to recover a cryptographic key or password by trying every possible key combination until the correct one is found. How quickly this can be done depends on the size of the key, and the computing resources applied.

A system set at 40-bit encryption has one trillion keys available. A brute-force attack of 500,000 keys per second would take approximately 25 days to exhaust the key space combinations using a single 3 GHz Pentium 4 computer. With a Rainbow Table, because all possible keys in the 40-bit keyspace are already calculated, file keys are found in a matter of seconds-to-minutes; far faster than by other means. DNA and PRTK seamlessly integrate with Rainbow Tables.

### **Product Features**

Three Rainbow Tables Hash Sets are available:

- MS Office Word and Excel
- Acrobat PDF

- Windows LAN Hash

Each hash set takes nearly 3TB of disk space.

AccessData RainbowTables hash sets for Windows LAN Hash ship with their own user-interface program, and that is the one that should be used for LAN Hash files. The Rainbow Tables has sets for MS Office and Acrobat PDF, as well as the Portable Office Rainbow Tables, (PORT) all run with AccessData Rainbow Tables stand-alone user-interface program. Check for the latest version of **RainbowTables.exe** on the AccessData Website, [www.AccessData.com](http://www.AccessData.com).

## TACC UNIT

The Tableau TACC1441 Hardware Accelerator (TACC) is a specialized product that reduces the dictionary-based password recovery times of PRTK and DNA. The TACC accelerator performs massively parallel, high-speed computations of cipher-keys, yielding a dramatic increase in the number of passwords per second that each host computer generates. This results in a greater number of successful attacks in a significantly shorter amount of time. For more information, contact your AccessData sales representative, or contact Tableau, LLC; [www.tableau.com](http://www.tableau.com).

## LICENSE MANAGEMENT

The following products aid in the management of your AccessData product licenses and license security devices. For more detailed information regarding licenses, LicenseManager, and license security devices, see “Appendix E Managing Security Devices and Licenses” on page 299.

## CODEMETER RUNTIME

The CodeMeter Runtime Kit is a program that is designed to work with the Wibu CodeMeter (CmStick) so AccessData programs can verify license information stored on the CmStick. It must be installed prior to connecting the CmStick. The CmStick and CodeMeter Runtime Kit software must be fully installed prior to running LicenseManager. Either a CmStick, or a Keylok dongle with a current license is required to fully utilize AccessData products. CodeMeter Runtime can be installed and running on the same machine with the AccessData Dongle Drivers, but both hardware devices cannot be connected to the same machine at the same time.

## LICENSEMANAGER

AccessData LicenseManager lets you manage product and license subscriptions stored on your Wibu CodeMeter CmStick or Keylok dongle USB license security device. LicenseManager communicates directly with AccessData's license server, so when license renewals take place, the information is readily and immediately accessible for download to your license device.

LicenseManager checks for the newest releases of your installed products, and also tells you when your license is near expiration.

# *Chapter 2 AccessData Forensic Toolkit 3.0 Overview*

Welcome to AccessData<sup>®</sup> (AD) Forensic Toolkit<sup>®</sup> (FTK<sup>®</sup>). 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 a leading forensic tool.

## **COMPUTER FORENSIC INVESTIGATION OVERVIEW**

This section provides a synopsis of how FTK perfectly suits the needs of the computer forensic investigator. FTK 3.0 can be used to acquire, preserve, analyze, and present digital evidence. This section also covers how to manage a case with FTK. For information on acquiring and preserving evidence, and beginning case analysis, see “Chapter 5 Starting a New FTK 3.0 Case” on page 53.

Any forensic digital examination requires these basic steps:

1. Acquire — identify and secure the evidence.
2. Preserve — create and store a forensic image of the evidence.
3. Analyze — create a case in a program that provides the tools to properly investigate the evidence.
4. Present — create a case report to document and synthesize the investigation results of the case from the evidence.
5. Manage — Back-up (archive), restore, and delete cases and evidence.

## ACQUIRING THE EVIDENCE

The basics of acquiring evidence is discussed in “Chapter 1 Introduction to AccessData Products” on page 1. In most cases, use AccessData FTK Imager to acquire exact duplicates of electronic evidence, particularly when evidence is not part of your local network. Some aspects of acquiring evidence is dependent on local or federal law. Be aware of those requirements prior to acquiring the evidence.

FTK 3.0 enables you to acquire live remote evidence from computers on your network. See “Chapter 6 Adding and Processing Static Evidence” on page 87, and “Chapter 7 Adding and Processing Remote Live Evidence” on page 121 for more detailed information.

## PRESERVING THE EVIDENCE

Preserving the evidence is accomplished both in the method of acquisition and the storage of the acquired data. Creating an exact replica of the original source is critical in forensic investigations. Keeping that replica safe from any source of corruption or unauthorized access involves both physical and electronic security. Once a case is created and the evidence is added to it, the case becomes just as critical.

## ANALYZING THE EVIDENCE

Prior to analyzing evidence that has been acquired and preserved, you must have a forensic investigation software program installed, and a case created.

Once you have FTK 3.0 installed and a case created, you are ready to add evidence for analysis. Evidence to be added to FTK can include images of hard drives, floppy drives, CDs and DVDs, portable media such as USB drives, and/or live (unimaged data from any common source.

Defining evidence for analysis uses features such as indexing, hashing, searching, and utilizing the Known File Filter (KFF) database. Bookmarking your findings improves your efficiency in the analysis process.

## INDEXING AND HASHING

When you are preparing to create a case, or add evidence to an existing case, you have options for creating an index of the data and for creating hashes of all files contained in the data as it is added to the case.



Indexing is simply the process of creating an index, or a searchable list of the discrete words, or strings of characters in a case. The index instantaneously provides results. However, it is sometimes necessary to use a live search to find things not contained in the index, and thus an index search cannot find.

Hashing a file or files refers to the process of using an algorithm to generate 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 can be standard system files that can be ignored in the investigation or they can be files known to contain illicit or dangerous materials. Ignore and alert statuses provide the investigator with valuable information at a glance.)

Three hash functions are available in FTK: Message Digest 5 (MD5) and Secure Hash Algorithms 1 and 256 (SHA-1 and SHA-256).

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

*File List View Showing Generated Hashes*

Name	Item #	Extension	Path	Category	P-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
[root]	1006		fastbloc.E01/Partition 1...	Folder	16.00 KB	9EAE67547454...	FB01D05764A...	BEEAA200A8AE7810...	n/a	n/a	n/a
[unallocated space]	1008		fastbloc.E01/Partition 1...	Folder	n/a				n/a	n/a	n/a
FAT1	1010		fastbloc.E01/Partition 1...	Meta	n/a	18A827FDD0A86...	EASF8FC3247...	CD04D9F9EECC658E98...	n/a	n/a	n/a
FAT2	1011		fastbloc.E01/Partition 1...	Meta	n/a	18A827FDD0A86...	EASF8FC3247...	CD04D9F9EECC658E98...	n/a	n/a	n/a
file system slack	1009		fastbloc.E01/Partition 1...	File Sys...	n/a	0F34380931126...	60CAC8F3D72...	5F70BF18A08600701...	n/a	n/a	n/a
VER	1007		fastbloc.E01/Partition 1...	Meta	n/a	E805D20FF9A8...	C479FC8543C...	FD782188BD463060...	n/a	n/a	n/a

Typically, individual file hashes (each file is hashed as it is indexed and added to a case) compare the results with a known database of hashes, such as the KFF. However, you can also hash multiple files or a disk image to verify that the working copy is identical to the original. Hashes can be generated with FTK Imager and with FTK. For information on creating hashes with FTK, see “Creating a Case” on page 57

## UTILIZING THE KNOWN FILE FILTER DATABASE

The Known File Filter (KFF) is an AccessData utility used to compare file hashes in a case against a database of hashes from files known to be ignorable (such as known system and program files), or those with alert status (such as known contraband or illicit material). The KFF allows quick elimination or pinpointing of these files during an investigation.

Files which contain other files, such as ZIP, CAB, and email files with attachments, are called container files. When KFF identifies a container file as ignorable or alert; the component files are not extracted.

KFF includes the HashKeeper database, which is updated periodically and is available for download on the AccessData Support website. For more information on the KFF, see “Using the Known File Filter” on page 211 “Using the Known File Filter” on page 211

## **SEARCHING**

As stated earlier, FTK can conduct live or index searches of the acquired images.

A live search is an item-by-item comparison with the search term, and can be very time-consuming. Live searches allow you to search non-alphanumeric characters and to perform pattern searches, such as regular expressions and hex values.

The indexed search uses an index file containing discrete words or number strings found in both the allocated and unallocated space in the case evidence. The investigator can choose to generate an index file during preprocessing.

AccessData products use dtSearch, one of the leading search tools available, in the index search engine. dtSearch can quickly search gigabytes of text.

For more information on searching, see “Chapter 9 Searching a Case” on page 175.

## **BOOKMARKING**

As important data is identified from the evidence in the case, bookmarking that data enables you to quickly find and refer to it, add to it, and attach related files, even files that are not processed into the case. These files are called “supplementary files.” Bookmarks can be included in reports at any stage of the investigation and analysis.

## **PRESENTING EVIDENCE**

AccessData FTK presents digital evidence by creating a case report containing the evidence and investigation results in a readable, accessible format.

Use the report wizard to create and modify reports. A report can include bookmarks (information selected during the examination), customized graphic references, and

selected file listings. Selected files, such as bookmarked files and graphics, can be exported to make them available with the report. The report can be generated in several file formats, including HTML and PDF and can be generated in multiple formats simultaneously.

For information about creating a report, see “Creating a Report” on page 245.

## MANAGING CASES

As you work with cases, it is a best practice to backup the cases and the evidence. Backup of evidence files is as easy as copying them to a secure location and media. Backup of cases can be more complicated, but equally important in the case of a crash or other catastrophic data loss.

Backup of a case requires the same amount of drive space as the case itself. This is an important consideration when planning your network resources for investigations.

This version includes three new case management features: Archive, Archive and Detach, and Attach. These allow you a wider focus of control over your cases



# *Chapter 3 AccessData Forensic Toolkit Installation*

This chapter details the steps for the installation of the required components for the operation of AccessData Forensic Toolkit (FTK) 3.0.

Additional AccessData programs are available to aid in processing cases. For more information, see “AccessData Forensic Products” on page 2.

## **INSTALLATION INFORMATION**

As with the AccessData FTK 2.3 version, FTK 3.0 can be installed with any one earlier version of 2.x remaining on the same computer at the same time. Installation paths will differ slightly from previous versions and registry entries will also be different. This means you may not have to uninstall your earlier version of FTK 2.x and thus may not have to convert cases to the newer version to maintain compatibility with the database.

This chapter details the steps for the installation of the required components for the operation of AccessData FTK 3.0. The following components are required to run FTK:

- CodeMeter 3.30a Runtime software for the CodeMeter Stick;
- A CodeMeter Stick.
- Oracle 10g Database
- FTK 3.0 Program
- Evidence Processing Engine

These additional programs are available to aid in processing cases:

- FTK Known File Filter (KFF) Library
- AccessData Registry Viewer
- AccessData LanguageSelector
- AccessData LicenseManager

## HARDWARE CONSIDERATIONS

The more powerful the available hardware, the faster FTK can analyze and prepare case evidence. Larger evidence files require more processing time than smaller evidence files. While the components can be installed on a single workstation, it is recommended to install them on separate workstations in order to make more hardware resources available to each.

The ideal configuration uses two workstations connected by a Gigabit ethernet connection. The Oracle database can be installed on a separate computer, or on the same computer as the FTK Program. If the KFF is installed, it must be installed on the same computer as the Oracle database. Ideally, the CodeMeter Runtime 3.30a software, LanguageSelector, and LicenseManager should be installed on the computer with the FTK Program.

To further maximize performance, AccessData recommends the following:

- For both the single- and separate-workstation configurations, install Oracle to a large hard disk drive that Oracle can use exclusively.
- Do not run other applications on these machines that will compete with FTK or the Oracle database for hardware resources.

## ESTIMATING HARD DISK SPACE REQUIREMENTS

The FTK Program requires a minimum of 500 megabytes of disk space for installation, although 5 gigabytes is recommended. Oracle, where images are stored, requires a minimum of 6 gigabytes (5 gigabytes for the basic installation) and additional room for case processing. Additional space is required for cases and case data.

**Important:** If disk space depletes while processing a case, the case data is erased.

To estimate the amount of hard drive space needed, apply these suggested factors:

- Data: every 500,000 items require one gigabyte of space in the Oracle storage location.
- Index: every 100 megabytes of text in the evidence requires 20 megabytes of space for processing in the case storage folder.

## CONFIGURATION OPTIONS

FTK can be set up in three different configurations, each with its own benefits and advantages. The three configurations listed below are represented in the graphic following:

- FTK and Oracle 10g can be installed on separate boxes or on the same box. If both are installed on the same box, it is recommended that Oracle be installed either on a separate drive, or on a separate partition from FTK.
- If a compatible Oracle 10g database is already installed, you may be able to use it with FTK. The installer runs a check for compatibility.

**Note:** AccessData recommends that you turn off firewalls and anti-virus software during installation.

If installation is being done using remote desktop to Server 2003, the remote connection needs to be established using the `/admin` or `/console` commands.

- Single Machine
- Separate Machines with a new Oracle install
- Separate Machines with an existing Oracle install

**Note:** AccessData recommends that you turn off firewalls and anti-virus software during installation.

## INSTALLING FTK

To install FTK 3, follow these steps:

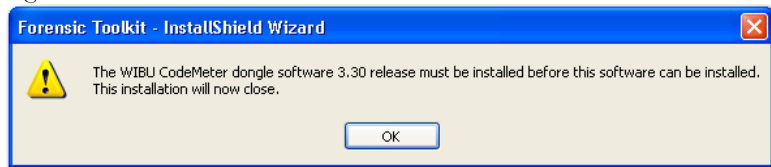
1. Insert the FTK 3.0 DVD into the drive.
2. Click *Install Forensic Toolkit 3.0*.

## INSTALL CODEMETER

Install the WIBU CodeMeter Runtime v3.30a software for the CodeMeter Stick. Click *Install CodeMeter Software* to launch the CodeMeter installation wizard. Follow the directions for installation, accepting all defaults, and click *Finish* to complete the installation.

If the user attempts to install FTK 3.0 before installing the CodeMeter v3.30a software and the Wibu CmStick, a message similar to the following error message will be displayed.

Figure 3-1 CodeMeter Error



**Note:** To remedy, click *OK*, then cancel the FTK 3.0 install. Install CodeMeter Runtime 3.30a software, and connect the CmStick. Then restart FTK 3.0 installation.

## INSTALL ORACLE

FTK must link to an Oracle database. If a compatible one already exists in the network or domain (with sufficient space for storage and processing) it can be leveraged for use with FTK. If no Oracle database exists, it must be installed either on the same computer as the FTK Program within the same network or domain, or a separate computer.

If you are not using a network with a domain controller, you can still use FTK. Check the AccessData Knowledge Base on the AccessData website, [www.accessdata.com](http://www.accessdata.com). Click *Support > Knowledge Base*, then search for the desired topic. One suggested search may be for “mirrored local accounts”.

1. Launch the installer.
2. Click *Next* and follow the prompts.
3. Read and accept the license agreement, and click *Next*.
4. Choose the Destination folder. Click *Next*.
5. Choose the setup type to use. Most users will choose *Typical*.



- 5a. If you choose *Custom*, type the SYS password into the text box, then click *I agree to remember this password and keep it safe* indicating you understand the risks. Click *Next*.

**Important** AccessData has no method of recovering lost SYS account passwords.

6. Wait for the installer to configure the installation.

7. Select the installation drive letter.

**Note:** Select the appropriate drive where Oracle will reside, separate from all other programs.

8. Click *Install*.

9. Wait for the installation and configuration to finish.

**Note:** This step can take up to forty minutes.

10. Click *Finish* to finalize the Oracle installation process, and return to the main menu.

## SINGLE COMPUTER INSTALLATION

The FTK Program can be installed on the same computer as the installed Oracle database.

### INSTALL FTK

From the FTK 3.0 New Install screen, perform the steps displayed in the following figure.

1. Click *Install FTK 3.0*

2. Click *Next*.

3. Read and accept the AccessData License Agreement.

4. Click *Next*.

5. Select the location for the FTK components.

**Note:** If another directory is desired instead of the default, click *Browse* to navigate to or create the folder using the Windows *Browse* functionality.

6. Click *Next*.

7. Click *Install* to continue with the installation.

8. Follow the prompts on the screens that follow.

9. When the installation is completed successfully mark the *View Readme* box to open the *Readme* file when you finalize the installation. Otherwise, click *Finish*.

## INSTALL THE EVIDENCE PROCESSING ENGINE

The Evidence Processing Engine is now installed separately. To install it, follow these steps:

1. From the FTK 3 Installer Autorun Main Menu, click *Install Engine*.
2. Read and accept the License Agreement. Click *Next*.
3. Accept the default Destination Folder, or specify one of your choice. Click *Next*.
4. Click *Install* on the Ready to Install screen.
5. Click *Next* to continue the installation.
6. Click *Finish* when the installation is completed successfully.

## INSTALL THE KFF LIBRARY

The FTK KFF Library can be installed to help shorten the investigation time on the case. The KFF Library must be installed on the same volume as the Oracle database. To perform step 4 and install the KFF, perform the following steps from the Install New FTK window, as displayed in the following figure.

1. Click *Install KFF Library*
2. Click *Next*.
3. Accept the KFF license agreement.
4. Click *Next*.
5. Allow installation to progress.
6. When the screen indicates a successful installation, click *Finish* to finalize the installation.
7. Click *Back to Main Menu* to return to the Main Menu and make other selections.

## INSTALLING ON SEPARATE COMPUTERS

FTK 3.0 can be installed on two separate computers. The table explains the recommended order for the installation tasks.

**TABLE 3-1**

---

Step	Machine	Task
1	Oracle	Install Oracle
2	FTK	Install CodeMeter

**TABLE 3-1**

---

Step	Machine	Task
3	FTK	Install FTK 3
4	FTK	Install Evidence Processing Engine
5	FTK	Run FTK to initialize the database
6	Oracle	Install KFF

## ADDITIONAL PROGRAMS

To change to another supported language other than the default English (United States) that ships with FTK, LanguageSelector must be installed.

## INSTALL LANGUAGE SELECTOR

To install Language Selector follow these steps:

1. From the FTK 3.0 Autorun Main Menu, click *Install Other Products*, then click *Install Language Selector*
2. The Language Selector Installer runs. Click *Next* to continue
3. Read and accept the License Agreement. Click *Next* to continue..
4. Click *Finish*.

## USING LANGUAGE SELECTOR

Run Language Selector by clicking *Start > All Programs > AccessData > Language Selector > Language Selector*.

**OR**

Click the Language Selector Icon on your desktop:



Language Selector has a very simple interface.

Click the *Select Languages* dropdown to select the language to use. Languages to choose from are as follows:

**TABLE 3-2 Language Selector Supported Languages**

---

- |                             |                                     |
|-----------------------------|-------------------------------------|
| • Chinese (Simplified, PRC) | • Japanese (Japan)                  |
| • Dutch (Netherlands)       | • Korean (Korea)                    |
| • English (United States)   | • Portuguese (Brazil)               |
| • French (France)           | • Russian (Russia)                  |
| • German (Germany)          | • Spanish (Spain, Traditional Sort) |
| • Italian (Italy)           |                                     |

The Products supporting this language text box indicates the products that will be affected by the language selection.

The File menu contains two choices:

- Select Language
- Exit

The Help menu contains one choice:

- About

## LICENSING

If licenses need to be managed, LicenseManager must be installed. For more information on LicenseManager, see “Appendix E Managing Security Devices and Licenses” on page 299.

Also, make sure the current versions of any other programs required for the investigation are installed, including AccessData Registry Viewer, and AccessData Password Recovery Toolkit, or AccessData Distributed Network Attack.

# *Chapter 4 The FTK 3.0 User Interface*

Before using AccessData Forensic Toolkit, an understanding of the basic features and general flow of a case is helpful. This chapter focuses on the basics. The chapters that follow give more detail.

## **ABOUT EVIDENCE**

### **ACQUIRING AND PRESERVING STATIC EVIDENCE**

For digital evidence to be valid, it must be preserved in its original form. The evidence image must be forensically sound, in other words, identical in every way to the original.

Two types of tools can do this: hardware acquisition tools and software acquisition tools.

- Hardware acquisition tools duplicate, or clone, disk drives and allow read-only access to the hard drive. They do not necessarily use a CPU, and are often hand-held.
- Software acquisition tools also create a disk image and in addition, give you a choice regarding the file format, the compression level where available, and the size of the data segments to use.

**Important:** Use a write-blocking device when using software tools, because some operating systems, such as Windows, make changes to the drive as it reads the data to be imaged.

FTK Imager is a software acquisition tool. It can quickly preview evidence and, if the evidence warrants further investigation, create a forensically sound image of the evidence drive or source. It makes a bit-by-bit duplicate of the media, rendering a forensic disk image identical in every way to the original, including file slack and unallocated or free space.

New with this release: FTK can now see and preview evidence on CDs and DVDs.

## ACQUIRING AND PRESERVING LIVE EVIDENCE

You can collect evidence from a live machine when you must. It is important to be aware of the data compromises you will face in such a situation, however sometimes there is no other choice. One such example is when the suspect drive is encrypted and you must acquire the image in-place while the machine is running. Another example is when imaging a RAID array; it must be live to be properly acquired.

For more information on acquiring and imaging “live” evidence gathered remotely from outside of your network, see “Chapter 6 Adding and Processing Static Evidence” on page 87

## ACQUIRING REMOTE EVIDENCE

FTK now provides additional tools to acquire live evidence in a different way. Using FTK you can gather many types of active information from network computers, including information in RAM, and Drive data. In addition, using Remote Drive Management System (RDMS), you can mount any drive through a mapping, and browse its contents, then make a custom image of what you find. This type of evidence is known as remote evidence. These features are discussed in-depth in “Chapter 7 Adding and Processing Remote Live Evidence” on page 121.

## CREATE A CASE

1. From the Case Management window, click *Case > New*.
2. Specify the evidence options to apply to the evidence by clicking Detailed Options in the New Case Options window.
3. Mark *Open the Case*, then click *OK*.
4. Wait while the case is being created. When case creation is complete, FTK opens and the Manage Evidence dialog opens.

## OPEN AN EXISTING CASE

After cases are created, it is likely that you will need to shut down the case and the program and return to it in the future. To do so,

1. Run FTK.
2. In the Case Management screen, highlight and double-click the case to open it.  
**Note:** If you attempt to open a case you have not been assigned to, you will receive a message saying, “You have not been assigned to work on this case.” This is because you must be authenticated to open the case.

## ADD EVIDENCE

To add evidence to any case, do the following:

1. Click *Add*.
2. Select the type of evidence to add, then click *OK*.
3. Type an ID or Name associated with the case, and a description if you wish.
4. Select the timezone for the original location of the selected evidence.
5. Select a language if other than English.
6. Click *OK*.
7. The Data Processing Status window appears and indicates the progress of the evidence processing. When a process is complete, the bar turns green. When all processes represented are green, the evidence processing is complete and you can begin working in the case.

**Note:** You can close the Data Processing Status window. Processing will continue until it is complete. To view the Data Processing Status window at any time, click *View > Progress Window*.

## WORK THE CASE

Use FTK’s tools and features to effectively locate evidence.

### IDENTIFY MEANINGFUL EVIDENCE

The purpose of FTK is to help investigators to identify meaningful evidence and to make that evidence available to the appropriate parties in an easy-to-understand medium.

The beginning of the evidence defining process involves the hashing of the data added to a case. Another key to easily finding meaningful evidence is the indexing of case

data. Through these two functions, FTK provides the foundation for successful investigation and analysis.

Use Index and live searching, and filtering, including using the Known File Filter Library (KFF) to isolate the information you are looking for. The results can then be bookmarked and added to the report that summarizes the findings in the case.

Use the tabs to view basic evidence groups, and to get an idea where best to look for the evidence you seek. In addition, you can run searches for specific words, names, email addresses and so forth from the index, or you can run live searches. Look through thumbnails of graphics, and look through emails and attachments. Narrow your search to look through specific document types, or to look for items by status, or by file extension. You can dig into the registry files to find websites visited, and the passwords for those sites. The possibilities are nearly endless.

As you find items of interest, you can:

- Create Labels to see them easily in a sorted File List view.
- Use searches and filters to find helpful items.
- Create Bookmarks so you can easily group the items by topic, and then find those items again, and to make the bookmarked items easy to add to reports.
- Export files as necessary for password cracking or decryption, then add them back as evidence.
- Add external files, that are not otherwise part of the case, to bookmarks as supplemental files.

## GENERATE REPORTS

When you feel you have exhausted the resources within the case and are ready to create your report, you can include your bookmarks, graphics, emails, documents, and registry evidence. They can be arranged in the way that works best for you, or for your audience.

A report can be generated in several formats to make it more useful to your audience.

## MOVING FORWARD

The remainder of this chapter provides basics of the Case Management window and its options.



For more detailed information about features and how they are used, see “Chapter 5 Starting a New FTK 3.0 Case” on page 53.

## USING THE CODEMETER STICK

AccessData provides a WIBU-SYSTEM AG\*USB CodeMeter\* Stick security license device with FTK. The CodeMeter Stick (or CmStick) is a security compliance license device. Insert the CmStick into the USB port prior to installation. It maintains your product licensing and subscription information, and is required by FTK.

You can use the LicenseManager application to monitor your product subscription. For more information, see “Appendix E Managing Security Devices and Licenses” on page 299.

**Note:** FTK versions 2.0 and above do not work with the KEYLOK (green) dongle used with FTK 1.x.

## STARTING FTK

After you complete the installation, start FTK by selecting *Start > Programs > AccessData > Forensic Toolkit > FTK 3.0*, or by selecting the Forensic Toolkit shortcut on the desktop.



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

## SET UP THE APPLICATION ADMINISTRATOR

On first launch, an Application Administrator must be created to manage the database. The Add New User dialog box opens automatically. The first added user is the Application Administrator, with rights for both database management and case administration. The Application Administrator can add new users to the database to administer cases (Case Administrator) or review cases (Case Reviewer) they are assigned to, as needed. Click *Database > Add User* to open the Add New User dialog. The following figure displays the Add New User dialog.

Figure 4-1 Add New User Dialog

The screenshot shows a dialog box titled "Add New User". It has a blue title bar with a close button in the top right corner. The dialog contains the following fields and controls:

- User Name:** A text box containing "Bond".
- Full Name:** A text box containing "James Bond".
- Password:** A text box containing "\*\*\*".
- Verify Password:** A text box containing "\*\*\*".
- Role:** A dropdown menu with "Case Administrator" selected. A list of roles is visible: "Application Administrator", "Case Administrator", and "Case Reviewer".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

Complete the fields to assign a new user a role and a password. Every field is required. Click *OK* to save the new user and close the dialog.

## BASICS OF THE FTK 3.0 USER INTERFACE

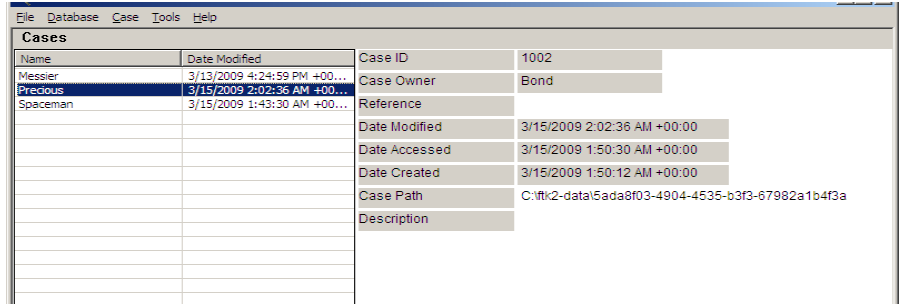
This section discusses the features of the AccessData FTK 3.0 interface that are common throughout the program.

### USING THE CASE MANAGER WINDOW

AccessData FTK cases are managed from a central database. The following figure displays the Case Manager window.

The Case Manager Window is the first screen that opens when FTK 3.0 is started. FTK case and database administration is done from the Case Manager window. The following figure displays the Case Manager window.

*Case Manager Window* After logging into FTK, the Case Management window appears



with the following menus:

**TABLE 4-1 Case Manager Menus**

- |        |            |
|--------|------------|
| • File | • Database |
| • Case | • Tools    |
| • Help |            |

The following tables show the available Case Manager menu options.

**TABLE 4-2 Case Manager File Menu**

Option	Description
Exit	Exits and closes FTK.

**TABLE 4-3 Case Manager Database Menu**

Option	Description
Log In	Opens the authentication dialog for users to log into the database.
Log Out	Logs out the currently authenticated user without closing FTK.
Administer Users	Manage user accounts. Options are: <ul style="list-style-type: none"> <li>• Add User: provide User Name, Role (Options are Application Administrator, Case Administrator, or Case Reviewer), Full Name, and Password. Application Administrator role can only be created or assigned by an Application Administrator.</li> <li>• Change Password: Provide and confirm the new password for the selected user.</li> <li>• Disable User: Click to disable the selected user account.</li> <li>• Show Disabled: Mark to display all disabled user accounts.</li> </ul>

The Application Administrator can change Users' roles, in addition to the options listed above.

**TABLE 4-3 Case Manager Database Menu**

---

<b>Option</b>	<b>Description</b>
Manage KFF	Opens the KFF Admin dialog. Edit or delete existing defined groups or defined sets, or add new groups; import or export a selected group or set.
Session Management	Opens the Manage DB Sessions dialog. Click <i>Refresh</i> to update the view of current sessions. Click <i>Terminate</i> to end sessions that are no longer active.
Change my Password	Opens a Change Password dialog for the currently authenticated user. Provide original password, type new password, and type it again to confirm the change.

**TABLE 4-4 Case Manager Case Menu**

---

<b>Option</b>	<b>Description</b>
New	Start a new case with the logged-in user as the Case Administrator. Case Reviewers cannot create a new case.
Open	Opens the highlighted case with its included evidence.
Assign Users	Allows the Application Administrator or the Case Administrator to adjust or control the rights of other users to access a particular case.
Backup	Opens a dialog for specifying names and locations for backup of selected cases. Options are: <ul style="list-style-type: none"><li>• Backup</li><li>• Archive</li><li>• Archive and Detach</li></ul>
Restore	Opens a Windows Explorer instance for locating and restoring a selected, saved case. Options are: <ul style="list-style-type: none"><li>• Restore an archived case</li><li>• Attach an archived and detached case</li></ul>
Delete	Deletes the selected case. Pop-up appears to confirm deletion.
Copy from FTK 2.2	Copy a case from FTK 2.2 into the FTK 3.0 database.

**TABLE 4-5 Case Manager Tools Menu**

---

<b>Option</b>	<b>Description</b>
Preferences	Opens Preferences dialog. Options are: <ul style="list-style-type: none"><li>• Choose temporary file path</li><li>• Choose network security device location. Provide IP address and port.</li></ul>

**TABLE 4-6 Case Manager Help Menu**

---

<b>Option</b>	<b>Description</b>
User Guide	Opens this User Guide in PDF format. The manual is formatted for two-sided printing.
About	Provides version and build information, copyright and trademark information about FTK, and other copyright and trade acknowledgements.

## CASE LIST

The Case List in the Case Manager lists all cases that are available to the currently authenticated user. For each case, in the right side of the screen opposite the Case List, information for the highlighted case is listed. Refer to “Case Manager” on page 54 to see the details. Case File, Description File, and Description (of the case) are determined by either the Application Administrator or the Case Administrator.

## CREATE A NEW CASE

When a case is created, the user who creates it becomes that case’s Administrator. To create a new case, click *Case > New* from the Case Manager window.

For more information about creating a new case, see “Chapter 5 Starting a New FTK 3.0 Case” on page 53.

## CASE MANAGEMENT

Case management includes creating new cases, as well as performing backup, archive, detach, restore and attach functions for cases, deleting cases from the database, and managing case and evidence files.

Case management tasks are performed from the Case Manager.

**Note:** Multiple user names in a case are correctly automatically assigned to Original User Names when a case is Archived, or Archived and Detached, and then restored. They can now also be reassigned if necessary.

## BACKING UP THE CASE

If a case is prematurely or accidentally deleted, or if it becomes corrupted, it can be restored from the previous backup.

Backup your case from the Case Manager window.

When you backup a case, FTK copies case information and database files (but not evidence) to a chosen folder. Keep copies of your drive images and other evidence independent of the backed-up case. Individual files and folders processed into the case are converted to an .AD1 (custom content) image and stored in the case folder.

**Important:** Case administrators back up cases and must maintain and protect the library of backups against unauthorized restoration, because the user who restores an archive becomes the case administrator.

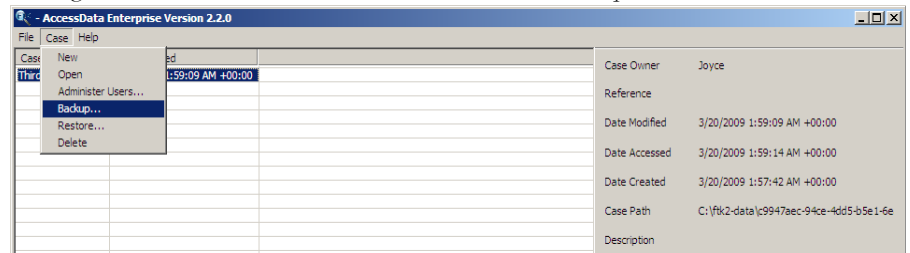
**Note:** FTK does not compress the backup file. A backed-up case requires the same amount of space as the database plus the case folder together.

To back up a case perform the following steps:

1. In the Case Manager window, select the case to backup.
2. Click *Case > Backup*,

**OR**

.Right-click on the case in the Cases list, and click *Backup*.



3. Select a Backup folder location on a drive with enough space to hold both the database and the case folder.
4. Enter a filename indicating the relationship to the original, and click *Save*.

**Note:** Each case you backup should have its own backup folder to ensure all data is kept together and not overwritten by another case backup. In addition, it is recommended that

backups be stored on a separate drive or system from the case, to reduce space consumption and to reduce the risk of total loss in the case of catastrophic failure (drive crash, etc.).

## ARCHIVING A CASE

When work on a case is completed and it is no longer necessary to access it, that case can be archived.

Archive copies that case's Oracle database tablespace file to the case folder. Look for filename DB *fn*. Archive keeps up to four backups, DB f0, DB f1, DB f2, and DB f3.

To Archive a case, do the following:

1. In the Case Manager, click *Case > Backup > Archive*.  
A message box displays informing you that the case is being archived. The box closes automatically when the archive is complete.

To view the resulting list of files, do the following:

1. Open the FTK 3 cases folder.
2. Find and open the sub-folder for the archived case.
3. Find and open the sub-folder for the archive (DB *fn*).
4. You may view the file names as well as Date modified, Type, and Size.

## ARCHIVE AND DETACH A CASE

When work on a case is not complete but it must be accessible from a different computer, archive and detach that case.

Archive and Detach copies that case's Oracle database tablespace file to the case folder, then deletes it from the Oracle database. This prevents two people from making changes to the case at the same time, preserving the integrity of the case, and the work that has been done on it.

To Archive and Detach a case do the following:

1. In the Case Manager, click *Case > Backup > Archive and Detach*.  
The case is archived.

2. You will see a notice informing you that the specified case will be removed from the database. Click *OK* to continue, or *Cancel* to abandon the removal and close the message box.
3. If you click *OK*, the Please Wait box appears while the Detach is in progress. The box closes when the Detach is complete.

To view the resulting list of files, do the following:

1. Open the FTK 3 cases folder.
2. Find and open the sub-folder for the archived case.
3. Find and open the sub-folder for the archive (DB *fn*).

You may view the file names as well as Date modified, Type, and Size.

## ATTACH A CASE

Attaching a case is different from Restoring a case. Restore a case from a backup to its original location, in the event of corruption or other data loss. Attach a case to the same or a different machine/database than the one where it was archived and detached from.

The Attach feature copies that case's Oracle database tablespace file into the Oracle database on the local machine.

**Note:** The Oracle database must be compatible and contain the FTK schema.

To attach a detached case:

1. Click *Case > Restore > Attach*.
2. Browse to and select the case folder to be attached.
3. Click *OK*.

## RESTORE A CASE

If a case is prematurely or accidentally deleted, or it becomes corrupted it can be restored from the backup.

To restore a case:

1. In the Case Manager window, click *Case > Restore*.

**OR**



- Right-click on the case to restore, and click *Restore*.
2. Browse to and select the Backup folder to be restored.
  3. Click *OK*.

## DELETE A CASE

To delete a case from the database:

1. In the Case Manager window, highlight the folder of case to delete from the database.
2. Click *Case > Delete*.

### OR

- Right-click on the folder of the case to delete, and click *Delete*.
3. Click *Yes* to confirm deletion.

## STORING CASE FILES

Storing case files and evidence on the same drive substantially taxes the processors' throughput. The system slows as it saves and reads huge files. For desktop systems in laboratories, increase the processing speed by saving evidence files to a separate server. For more information, see the "Configuration Options" on page 19.

If taking the case off-site, you can choose to compromise some processor speed for the convenience of having your evidence and case on the same drive.

## THE FTK USER INTERFACE

The FTK interface contains a menu bar, toolbars, main tabs, each tabbed page having a specific focus. Most tabs also contain a common toolbar and file list with customizable columns.

When a case is created and assigned a user, the Case window opens with the following menus:

- File
- Edit
- View
- Evidence
- Filter

- Tools
- Help

The following tables show the available options from the FTK User Interface menus.

**TABLE 4-7 File Menu**

---

<b>Option</b>	<b>Description</b>
Export	<p>Exports selected files and associated evidence to a designated folder. File Options are:</p> <ul style="list-style-type: none"><li>• Append Item number to filename</li><li>• Append extension to filename if bad/absent</li><li>• Expand containers (email archives, email attachments, etc)</li><li>• Save HTML view (if available)</li><li>• Export emails as MSG</li></ul> <p>Choose <i>File-&gt;Export</i> to display the Export dialog. The dialog provides a way to select the output format. If an email message is selected, the .msg format will be enabled. Click <i>Save</i> to initiate writing the message to disk. The name of the email item will be used as the name of the file. For duplicates, the file names will have an “(1).msg”, “(2).msg”, “(3).msg”, ..., extension to the end of the name.</p> <ul style="list-style-type: none"><li>• Export directory as file</li><li>• Export children</li><li>• Include original path</li><li>• Export slack space as files</li></ul> <p><i>Items to Include</i> Options are:</p> <ul style="list-style-type: none"><li>• All checked</li><li>• All Listed</li><li>• All Highlighted</li><li>• All</li></ul> <p>Select the destination base path by typing it in or clicking <i>Browse</i>.</p>
Export to Image	<p>Exports one or more files as an AD1 image to a storage destination. Options are:</p> <ul style="list-style-type: none"><li>• Add, Edit, or Remove desitnation.</li><li>• Verify images after they are created.</li><li>• Precalculate progress statistics.</li><li>• Add image to case when completed.</li></ul> <p>Click <i>Start</i> to create image.</p>

---

Option	Description
Export File List Info	<p data-bbox="686 256 1338 314">Exports selected file information to files formatted as the Column List in .csv, .tsv, and .txt formats.</p> <p data-bbox="686 326 1338 354">File List items to export Options are:</p> <ul data-bbox="708 371 868 499" style="list-style-type: none"> <li data-bbox="708 371 868 399">• All highlighted</li> <li data-bbox="708 404 868 432">• All checked</li> <li data-bbox="708 437 868 465">• Currently listed</li> <li data-bbox="708 470 868 498">• All</li> </ul> <p data-bbox="686 510 1338 567">Choose Columns options can be selected from the drop-down list, or click Column Settings to define a custom column setting.</p> <p data-bbox="686 579 1338 713"><b>Note:</b> If you try to export File List info to part of a network/folder/etc. where you do not have rights, the dialog and process will seem successful, but the file isn't actually exported and sent anywhere. MS Windows Vista will popup an error message. XP is unable to do so. Be sure to verify that the exported information is sent to a place where you have rights.</p> <p data-bbox="686 725 1338 748"><b>Note:</b> The File List loads more quickly in version 3.0 than in the past.</p>
Export Word List	<p data-bbox="686 760 1338 817">Exports the discrete words from the registry as a text file from which a dictionary for PRTK can be created. Options are:</p> <ul data-bbox="708 835 839 961" style="list-style-type: none"> <li data-bbox="708 835 839 862">• Select All</li> <li data-bbox="708 868 839 895">• Deselect All</li> <li data-bbox="708 900 839 928">• Export</li> <li data-bbox="708 933 839 961">• Cancel</li> </ul>
Report	<p data-bbox="686 973 1338 1031">Opens the Report Options dialog for creating a case report. For more information, see “Creating a Report” on page 245.</p>
Close	<p data-bbox="686 1043 1338 1071">Closes the Case window and returns to the Case Manager window.</p>
Exit	<p data-bbox="686 1083 1338 1111">Closes both the Case and Case Manager windows.</p>

**Note:** The Tree and Search views are exclusive settings, meaning that you can use only one of these views per pane. For more information on using the View menu see, “The View Menu” on page 264.

**TABLE 4-8 Edit Menu**

---

<b>Option</b>	<b>Description</b>
Copy Special	Duplicates information about the object copied as well as the object itself, and places the copy in the clipboard. Options are: <ul style="list-style-type: none"><li>• Columns (Select the columns to include, or click Column Settings to define a new column setting)</li><li>• Include header row</li><li>• File List items to copy<ul style="list-style-type: none"><li>• All Highlighted</li><li>• All Checked</li><li>• Currently listed</li><li>• All</li></ul></li></ul> Click <i>OK</i> to copy or <i>Cancel</i> to cancel.

**TABLE 4-9 View Menu**

---

<b>Option</b>	<b>Description</b>
Refresh	Reloads the current view.
Filter Bar	Inserts the filter toolbar into the current tab. These features are available also from the Filter menu.
TimeZone Display	Opens the Time Zone Display dialog. Select a time zone for viewing the evidence, then click <i>OK</i> .
Thumbnail Size	Selects the size of the thumbnails displayed from the Graphics tab. Select from: <ul style="list-style-type: none"><li>• Large-default</li><li>• Medium</li><li>• Small</li><li>• Tiny</li></ul>

**TABLE 4-9 View Menu**

---

<b>Option</b>	<b>Description</b>
Tab Layout	Manages tab settings: the user can lock an existing setting, add and remove settings, save settings one tab at a time or all at once. The user can also restore previous settings. or reset them to the default settings. These options are in the following list: <ul style="list-style-type: none"><li>• Lock</li><li>• Add (create a new tab -- provide a name, then click <i>OK</i>.)</li><li>• Remove</li><li>• Save</li><li>• Save All Layouts</li><li>• Restore</li><li>• Reset to Default</li></ul>
File Content Tabs Switching	Choose Automatic or Manual switching of tabs based on the file content.
Explore Tree	Displays the Explore Tree in the upper-left pane.
Graphics Tree	Displays the Graphics Tree in the upper-left pane.
Overview Tree	Displays the Overview Tree in the upper-left pane.
Email Tree	Displays the Email Tree in the upper-left pane.
Bookmark Tree	Displays the Bookmark pane in the upper-left pane.
Indexed Searches	Displays the Index Search Results pane in the upper-left pane.
Live Searches	Displays the Live SearchResults pane in the upper-left pane.
Bookmark Information	Inserts the Bookmark Information pane into the current tab.
File List	Inserts the File List pane into the current tab. <b>Note:</b> The File List loads more quickly now than in previous versions.
File Content	Inserts the File Content pane into the current tab.
Email Attachments	Displays the attachments to email objects found in the case Displays from any tab. Selectable if it applies in the active tab.
Properties	Inserts the Object Properties pane into the current tab view.
Hex Value Interpreter	Displays a pane that provides an interpretation of Hex values selected from the Hex View pane.
Thumbnails	Displays a pane containing thumbnails of all graphics found in the case.
Progress Window	Opens the Progress dialog, from which you can monitor tasks and/or cancel them.

**TABLE 4-9 View Menu**

Option	Description
--------	-------------

**TABLE 5-10 Evidence Menu**

Add/Remove	<p>Opens the Manage Evidence dialog, used to add and remove evidence. From Manage Evidence, choose from the following</p> <ul style="list-style-type: none"> <li>• Refinement Options</li> <li>• Language Setting</li> <li>• Choose the local time zone for this evidence</li> <li>• Select Case KFF Options</li> </ul>
Add Remote Data	<p>Collect remote data from another computer on the network. Provide the following:</p> <ul style="list-style-type: none"> <li>• Remote IP or Address</li> <li>• Remote Port</li> </ul> <p>Select any or all of the following:</p> <ul style="list-style-type: none"> <li>• Physical Drives</li> <li>• Logical Drives</li> <li>• Memory Analysis</li> </ul> <p>Click <i>OK</i> or <i>Cancel</i>.</p>
Additional Analysis	<p>Opens the Additional Analysis dialog with many of the same processing options available when the evidence was added. Allows the user to reprocess using options not selected previously. For more information, see “Additional Analysis” on page 93.</p>

**TABLE 4-10 Filter Menu**

Option	Description
New	Opens the Filter Definition dialog to define a filter. This feature is also available from the Filter toolbar.
Duplicate	Duplicates a selected filter. Use the duplicate as a basis for a new filter. This feature is also available from the Filter toolbar.
Delete	Deletes a selected filter. This feature is also available from the Filter toolbar.
On	Applies the global filter to the application. The file list changes color to indicate that the filter is applied. This feature is also available from the Filter toolbar.
Import	Opens the system file manager allowing the user to import a pre-existing filter. Filter files are in .XML format. This feature is also available from the Filter toolbar.

**TABLE 4-10 Filter Menu**

---

<b>Option</b>	<b>Description</b>
Export	Opens the system file manager allowing the user to save a filter. This feature is also available from the Filter toolbar.
Tab Filter	Allows the selection of a filter to apply to a current tab.

**TABLE 4-11 Tools Menu**

---

<b>Option</b>	<b>Description</b>
KFF	Known File Filter (KFF) sets and groups can be managed, archived, and cleared. The following menu option is available: <ul style="list-style-type: none"><li>• Manage</li></ul>
Fuzzy Hash	Allows you to <ul style="list-style-type: none"><li>• Find Similar Files</li><li>• Manage Library</li></ul>
Decrypt Files	Decrypts EFS and Office files passwords that matched those entered.
Credant Decryption	Opens the Credant Decryption dialog where you enter the decryption information. See “Decrypting Credant Files” on page 235, for more information.
Verify Image Integrity	Generates hash values of the disk image file for comparison.
Disk Viewer	Opens a viewer that allows you to see and search evidence items.
Other Applications	Opens other AccessData tools to complement the investigational analysis: <ul style="list-style-type: none"><li>• Imager</li><li>• PRTK</li><li>• Registry Viewer</li><li>• LicenseManager</li><li>• Language Selector</li></ul>
Final Carve Processing	Provides a means to manually carve for data from the hex view of files.
Execute SQL	Provides the ability to execute SQL scripts directly from FTK. You can type a script in, or browse to and execute a saved script.



**TABLE 4-12 Help Menu**

Option	Description
User Guide	Provides a link to theFTK 3.0 User Guide.
About	Provides information about the current FTK release.

## UNDOCKING

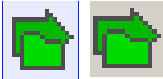




The File List, Properties/Hex Interpreter, and File Content panes can be undocked and moved around the screen, even outside the FTK window. For information on undocking moving, and customizing your FTK window view, see “Chapter 13 Customizing the FTK Interface” on page 263.

## TOOLBAR COMPONENTS






The FTK interface provides a toolbar for applying QuickPicks and filters to the case. The following section lists the toolbars and their components.

The following table shows the available components of the toolbar.

**TABLE 4-13 Toolbar Components**

Component	Description
	Turns the QuickPicks filter on or off. The QuickPicks filter is used in the Explore tab to populate the file list with only items the investigator wishes to analyze. When active, or ON, the QuickPicks button is light blue. When inactive, or OFF, the background is gray
	Turns the filter on or off. Filtered data is shown in a colored pane to indicate that it is filtered.
	Applies the selected filter. A drop-down menu lists defined filters.
	Opens the filter definition dialogue to define the rules of the current filter, or allows the creation of a new one.
	Deletes the selected filter.

**TABLE 4-13** Toolbar Components

Component	Description
	Creates a new filter.
	Creates a copy of the selected filter.
	Imports the selected filter from an XML file.
	Exports the selected filter to an XML file.
	Locks the movable panes in the application, making them immovable. When the lock is applied, the blue box turns grey..

## FILE LIST PANE










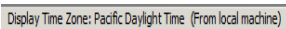
The File List pane lists the files selected from the Evidence Items pane. In this pane the user can choose which columns to display, as well as the order of those columns, create bookmarks, create labels, copy or export file lists.

When viewing data in the File List, use the type-down control feature to locate sought information. When the list is sorted by name, select an item in the list, then type the first letter of the desired file. FTK will move down the list to the first file beginning with that letter. For more information, see “Customizing File List Columns” on page 268.




## FILE LIST TOOLBAR

The File List pane includes a toolbar containing these buttons for managing the File List:

**TABLE 4-14 File List Toolbar**

Component	Description
	Checks all of the files in the current list.
	Unchecks all of the files in the current list.
	Unchecks all of the files in the current case.
	Opens Create New Bookmark dialog box.
	Opens Manage Labels dialog box.
	Export File List allows the user to save selected files to another folder.
	Opens Copy Special dialog box.
	Opens the Column Settings dialog box.
	<p>Sets the columns to a specific selection from the list of defined column sets. Defaults are:</p> <ul style="list-style-type: none"> <li>• Email</li> <li>• File Listing</li> <li>• Normal (default)</li> <li>• Reports: File Path Section</li> <li>• Reports: Standard</li> </ul>
	Displays the selected time zone from the local machine.

**TABLE 4-14 File List Toolbar**

Component	Description
	Leave query running when switching tabs (May affect performance of other tabs).
	Cancel retrieving row data. This is not a pause button. To retrieve row data after clicking Cancel, you must begin again. There is no way to pause and restart the retrieval of row data.
	Indicates Processing activity.

## FILE LIST VIEW RIGHT-CLICK MENU

When you right-click on any item in the File List view, a menu with the following options appears. Some options are enabled or disabled, depending on the tab you are in, the evidence that exists in the case, the item you have selected, or whether bookmarks have been created.

**TABLE 4-15 File List View Right-Click Menu Options**

Option	Description
Open	Opens the selected file.
Launch in Content Viewer	Launches the file in the Content Viewer, formerly known as Detached Viewer.
Open With	Opens the file. Choose either Internet Explorer or an External Program
Create Bookmark	Opens the Create New Bookmark dialog for creating a new bookmark.
Add to Bookmark	Opens the Add to Bookmark dialog for selecting an existing bookmark to add files to.
Remove from Bookmark	Removes a file from a bookmark. From the Bookmarks tab, open the bookmark containing the file to be removed, then select the file. Right-click and select <i>Remove from Bookmark</i>
Manage Labels	Opens the Manage Labels dialog. Create or Delete a label, or apply labels to files.
Review Labels	Opens the Label Information dialog to display all labels assigned to the selected file or files.

**TABLE 4-15 File List View Right-Click Menu Options**

<b>Option</b>	<b>Description</b>
Add Decrypted File	Right-click and select Add Decrypted File. Opens the Add Decrypted File dialog. Browse to and select the file to add to the case, click <i>Add</i> .
View File Sectors	Opens a hex view of the selected file. Type in the file sector to view and click <i>Go To</i> .
Find on Disk	Opens the FTK Disk Viewer and shows where the file is found in the disk/file structure.  <b>Note:</b> Find on disk feature won't find anything under 512 B physical size. Files smaller than 1500 bytes may reside in the MFT and do not have a start cluster. Find on disk depends on that to work. This is working as designed
Add to Fuzzy Hash Library	Opens Select Fuzzy Hash Group dialog. Click the drop-down list to select the Fuzzy hash group to add to. The Fuzzy Hash group must already have been created.
Find Similar Files	Opens the Search for Similar Files dialog. The selected file's hash value is displayed. Click From File to see the filename the hash is from. The Evidence items to search box shows all evidence items in the case. Mark which ones to include in the search. Select the Minimum match similarity you prefer, and click <i>Search</i> or <i>Cancel</i> .
Open in Registry Viewer	Opens a registry file in AccessData's Registry Viewer. Choose SAM, SOFTWARE, SYSTEM, SECURITY, or NTUSER.dat.
Export	Opens the Export dialog with all options for file export, and a destination path selection.
Export to image	Opens the Create Custom Content Image dialog.
Export File List Info	Opens the Save As dialog. Choose *.txt, *.tsv, or *.csv. Default name is FileList.txt.
Copy Special	Opens the Copy Special dialog.
Check All Files	Check-marks all files in the case.
Uncheck all Files in Current List	Unchecks all files in the current list.
Uncheck All Files in Case	Unchecks all files in the case.
Change "Flag as Ignorable" Status	Change Flag Status of all files as either Ignorable or Not Ignorable according to Selection Options.
Change "Flag as Privileged" Status	Change Flag Status of all files as either Privileged or Not Privileged according to Selection Options.

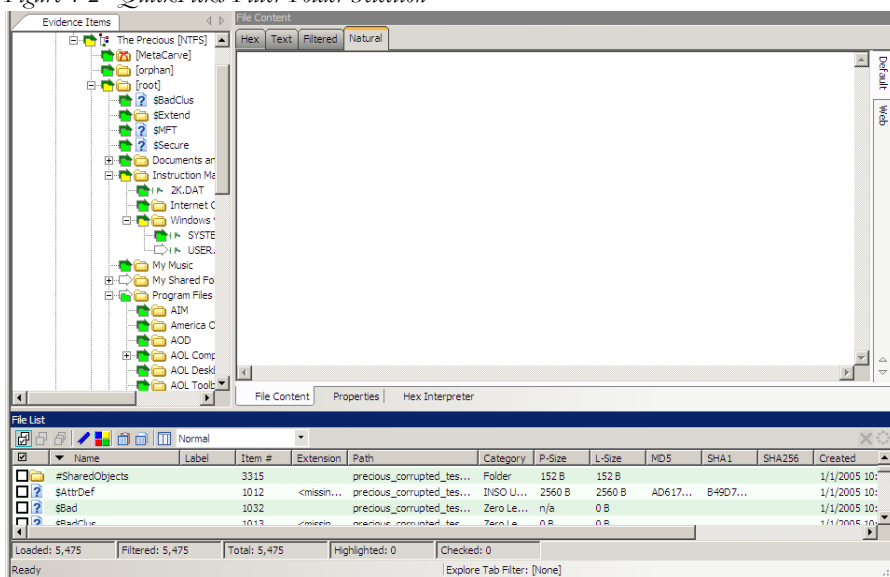
**TABLE 4-15 File List View Right-Click Menu Options**

Option	Description
Re-assign File Category	Change File Category assignment. See File Categories under Overview Tab.
View This Item In a Different List	Changes the File List view from the current tab to that of the selected tab from the pop-out.

## QUICKPICKS FILTER

The QuickPicks feature is a type of filter that allows the selection of multiple folders and files in order to focus analysis on specific content. The following figure represents the Explore Evidence Items tree with a partially selected set of folders and sub-folders using the QuickPicks feature.

*Figure 4-2 QuickPicks Filter Folder Selection*

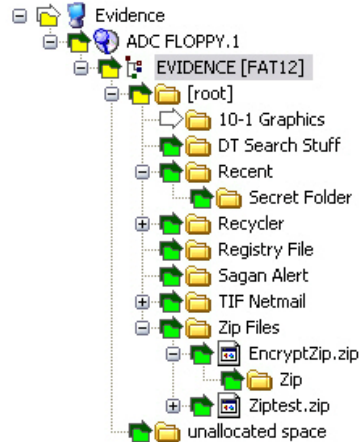


The QuickPicks filter simultaneously displays open and unopened descendent containers of all selected tree branches in the File List at once. The colors of the compound icons indicate whether descendents are selected.

The icons are a combination of an arrow, representing the current tree level, and a folder, representing any descendent.

The icons' colors indicate the levels and descendent selected. Green means all are selected, yellow means some are selected, and white means none are selected.

Figure 4-3



In the illustration above, the decedent folder 10-1 Graphics is unselected. Its arrow icon is white.

The folder icons for the folders above item “10-1 Graphics” are yellow to indicate that not all descendent folders are selected. The top-most level item “Evidence” has a white arrow icon, indicating that it is not selected, and a yellow folder icon, indicating that some of its descendent folders are not selected.

The folder icon for “DT Search Stuff” is green, indicating that all contents of the folder have been selected.

## THE DATA PROCESSING STATUS SCREEN

Also known as the Progress Dialog, the Data Processing Status screen reports the status of any processing that is being done on the evidence in the case. Whenever the user processes an evidence item or runs additional analysis, the Progress Dialog gives an estimation of how tasks are progressing.

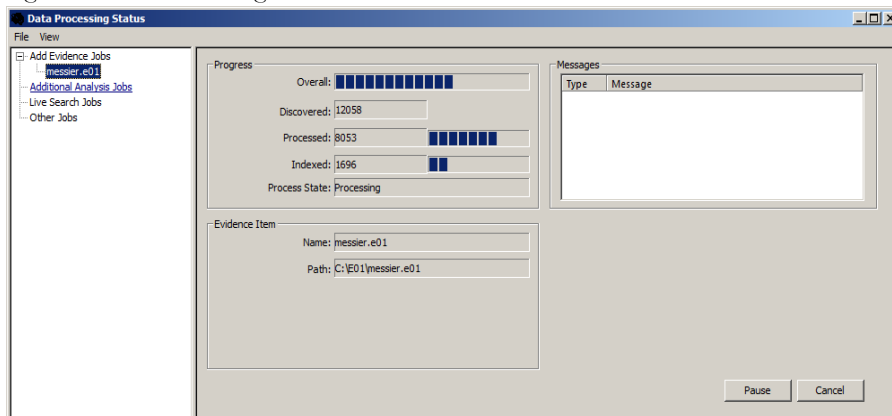
The Progress Dialog can be opened by clicking View > Progress Window. In FTK 3.0, the Progress Window has changed.

There are four views to choose from, depending on the type of job(s) that are running:

- Add Evidence Jobs
- Additional Analysis Jobs
- Live Search Jobs
- Other Jobs

Click on the type of job to expand the list of that job type. Click on an individual job to see its status, as indicated in the following figure:

Figure 4-4 Data Processing Status



Different information is displayed for each job type. The evidence item currently being reported on is listed by its Name and Path location. Task activity is shown by a blue bar. Tasks are measured by:

**TABLE 4-16 Data Processing Status Task Measurements**

- |                              |                   |
|------------------------------|-------------------|
| • Overall progress           | • Processed State |
| • Number of items Indexed    | • Finished        |
| • Number of items Processed  | • Static          |
| • Number of items Discovered | • Processing      |



# Chapter 5 Starting a New FTK 3.0 Case

This chapter explains how to create a new AccessData FTK case.

## LAUNCH FTK

After FTK is installed, launchFTK by doing the following:

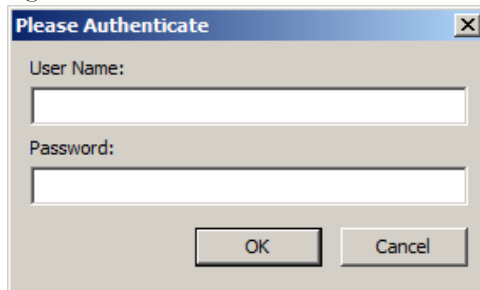
1. Click *Start > All Programs > AccessData > Forensic Toolkit > FTK 3.0*, or click the *FTK 3.0* icon on the desktop:



**Note:** Please note that it may take a few moments forFTK to run. This is because it is also launching the Oracle database.

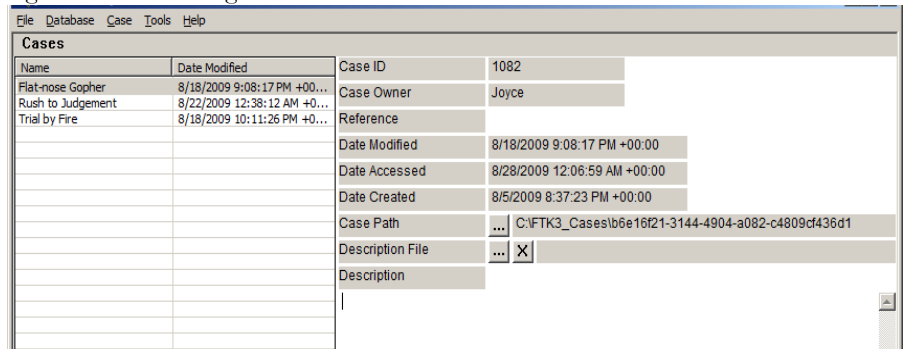
2. Log in to FTK 3.0 providing your username and the case-sensitive password. The first person to log in to FTK upon complete installation is the Application Administrator.

Figure 5-1 Please Authenticate



A successful login brings up the Case Management window, as in the following figure:

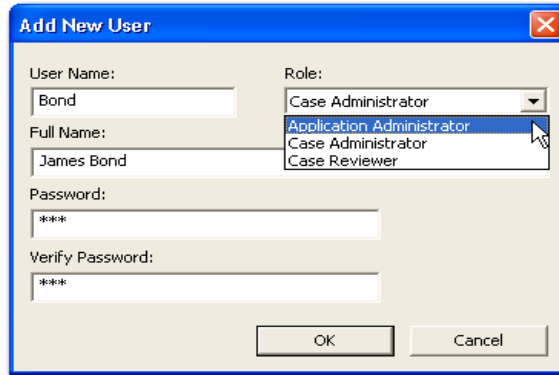
Figure 5-2 Case Manager



The Case Manager menus are discussed in detail in “Basics of The FTK 3.0 User Interface” on page 30.

The Application Administrator can add additional users from the Case Management window. The following steps can be used by the Application Administrator to set up new users as needed.

3. Click *Database > Administer Users > Add User* to open the Add New User dialog



4. Enter a username.
5. Enter the full name of the user as it is to appear in reports.
6. Assign a role to limit or increase database and Administrative access
7. Enter a password.
8. Verify the password.
9. Click *OK* to save the new user and close the dialog.

The following table gives information on the fields available in the Add New User dialog.

**TABLE 5-1 Add New User Information Fields**

Field	Description
User Name	Enter the name by which the user is known in program logs and other system information.
Role	Assign rights to the user name: <ul style="list-style-type: none"> <li>• <b>Application Administrator:</b> can perform all types of tasks, including adding and managing users.</li> <li>• <b>Case Administrator:</b> can process data and change settings to FTK, although only the application administrator can add new users.</li> <li>• <b>Case Reviewer:</b> cannot create cases; can only process cases.</li> </ul>
Full Name	Enter the full name of the user as it is to appear on case reports.
Password	Enter and verify a password for this user.

10. After completing the dialog, the log in prompt returns again for a login name and password for the newly created user to login. The Case Management window shows

the name you just created, indicating that the user can login, view and modify cases within that database.

## ASSIGNING ROLES

New users require a role, or a set of permissions to perform specific sets of actions.

### APPLICATION ADMINISTRATOR

An Application Administrator has permissions to all areas of the program and can create and manage users..

### CASE ADMINISTRATOR

A Case Administrator can perform all of the tasks an Application Administrator can perform, with the exception of creating and managing users.

### CASE REVIEWER

The following tasks are unavailable to a user having the Case Reviewer role:

**TABLE 5-2 Permissions Denied Case Reviewer Users**

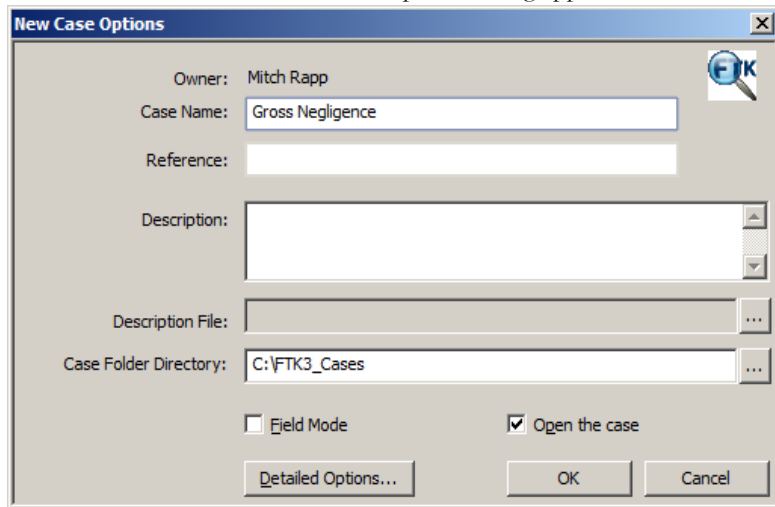
---

• Create, Add, or Delete cases	• Use FTK Imager
• Administer Users	• Use Registry Viewer
• Data Carve	• Use PRTK
• Manually data carve	• Use Find on Disk
• Assign Users to cases	• Use the Disk Viewer
• Add Evidence	• View file sectors
• Access Credant Decryption from the Tools Menu	• Define, Edit, Delete, Copy, Export, or Import Filters
• Decrypt Files from the Tools Menu	• Export files or folders
• Mark or View Items Flagged as “Ignorable” or “Privileged.”	• Access the Additional Analysis Menu
• Manage the KFF	• Backup or Restore Cases
• Manage Fuzzy Hash	• Add a Database
• Enter Session Management	

## CREATING A CASE

FTK stores each case in an Oracle database, and allows case administration as each new case is created. When an authorized user creates a case, that user becomes that case's administrator. To start a new case from the Case Manager window, do the following:

1. Launch FTK 3.0 and login. This opens the Case Management window.
2. Click *Case > New*. The New Case Options dialog appears.



3. Enter a name for the case in the Case Name field.
4. Enter any optional specific reference information in the *Reference* field.
5. Enter an optional short description of the case in the *Description* field.
6. If you wish to specify a different location for the case, click the *Browse* button: ...

**Note:** If the [drive]:\ftk3\_Cases folder is not set as shared, an error occurs during case creation.

7. If you wish to create the case in Field Mode, mark the Field Mode box. Field Mode disables the Detailed Options button when creating a case.

The screenshot shows the 'New Case Options' dialog box. The 'Owner' field is set to 'Joyce'. The 'Case Name' field contains the text 'Rush to Judgement'. The 'Reference' field is empty. The 'Description' field is a large, empty text area. The 'Attached File' field is empty, with a browse button (...). The 'Case Folder Directory' field is set to 'C:\FTK3\_Cases', also with a browse button (...). At the bottom of the dialog, there are two checked checkboxes: 'Field Mode' and 'Open the case'. Below these checkboxes are three buttons: 'Detailed Options...', 'OK', and 'Cancel'.

8. In addition to disabling Detailed Options, Field Mode bypasses file signature analysis and the Oracle database communication queue. These things vastly speed the processing.
- Note:** The Job Processing screen always shows 0 for Queued when Field Mode is enabled, because items move directly from Active Tasks to Completed.
9. If you wish to open the case as soon as it is created, mark *Open the case*.
  10. If you do not select Field Mode, click *Detailed Options* to specify how you wish the evidence to be treated as it is processed and added to the case. The case creation steps are continued in the following section.
  11. When the case is defined and Detailed Options are selected, click *OK* to create the new case.

## SELECTING EVIDENCE PROCESSING OPTIONS

The Evidence Processing options allow selection of processing tasks to perform on the current evidence. Select only those tasks that are relevant to the evidence being added to the case.

After processing, the Evidence Processing options selected for this case can be found in the case log. You can also view them by clicking *Evidence > Add/Remove*. Double-click on any of the evidence item to open the Refinement Options dialog.

Some pre-processing options require others to be selected. For example:

- Data Carving depends on Expand
- KFF depends on MD5 hashing
- Flag Duplicates depends on MD5 hashing
- Indexing depends on identification
- Flag bad extension depends on file signature analysis.

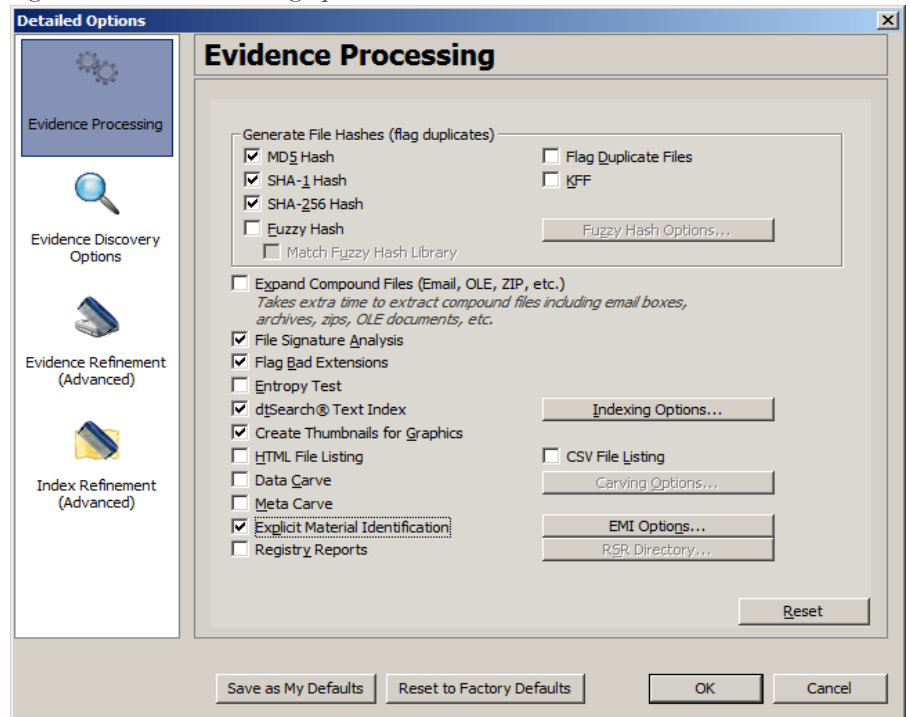
The following figure represents the detailed options dialog. Different processing options can be selected and un-selected depending on the specific requirements of the case.

At the bottom of every Refinement Options selection screen you will find five buttons:

- **Reset:** resets the current settings to the currently defined defaults.
- **Save as My Defaults:** saves current settings as the default for the current user.
- **Reset to Factory Defaults:** Resets current settings to the factory defaults.
- **OK:** accepts current settings without saving for future use.
- **Cancel:** cancels the entire Detailed Options dialog without saving settings or changes, and returns to the New Case Options dialog.

If you choose not to index in the Processing Options page, but later find a need to index the case, click *Evidence > Additional Analysis*. Choose *All Items*, and check *dtSearch\** *Index*.

Figure 5-3 Evidence Processing Options



**Note:** Another factor that may influence which processes to select is your schedule. If you disable indexing, it shortens case processing time. The case administrator can return at a later time and index the case if needed.

12. Click *Detailed Options* to choose settings for the case.
  - 12a. Click the *Evidence Processing* icon in the left pane, and select the processing options to run on the evidence. For more information, see “Selecting Evidence Processing Options” on page 58.

**Note:** Select File Listing Database here in pre-processing to create an MDB database of the evidence files.

- 12b. Click the *Evidence Discovery* icon to specify the location of the File Identification File, if one is to be used. For more information, see “Evidence Discovery Options” on page 73.
  - 12c. Click the *Evidence Refinement (Advanced)* icon to select the custom file identification file to use on this case. For more information, see “Selecting Evidence Discovery Options” on page 72.



- 12d. Click the *Index Refinement (Advanced)* icon to select which types of evidence to not index. For more information, see “Selecting Evidence Refinement (Advanced) Options” on page 74.
13. Click *OK*.
14. When you are satisfied with your evidence refinement options, Click *OK* to continue to the Evidence Processing screen.

The following table outlines the Evidence Processing options:

**TABLE 5-3 Evidence Processing Options**

Process	Description
MD5 Hash	<p>Creates a digital fingerprint using the Message Digest 5 algorithm, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</p> <p>For more information about MD5 hashes, see “Message Digest 5” on page 337.</p>
SHA-1 Hash	<p>Creates a digital fingerprint using the Secure Hash Algorithm-1, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files.</p> <p>For more information about SHA hashes, see “Secure Hash Algorithm” on page 340.</p>
SHA-256 Hash	<p>Creates a digital fingerprint using the Secure Hash Algorithm-256, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. SHA-256 is a hash function computed with 32-bit words, giving it a longer digest than SHA-1.</p> <p>For more information about SHA hashes, see “Secure Hash Algorithm” on page 340.</p>
Fuzzy Hash	<p>Fuzzy hashes are hash values that can be compared to determine how similar two pieces of data are. Traditional cryptographic hashes can only tell if two bitstreams are identical; fuzzy hashes can tell how similar two bitstreams to each other. The similarity value is expressed as a value 0-100, where 0 is not similar and 100 is almost identical. If selected, click <i>Fuzzy Hash Options</i> to make file size limitations and Fuzzy Hash Group(s) selections, and choose whether to <i>Match fuzzy hash library</i>.</p>

**Note:** The Hash fields in the case may be empty for files carved from unallocated space

**TABLE 5-3 Evidence Processing Options**

---

<b>Process</b>	<b>Description</b>
Flag Duplicate Files	Identifies files that are found more than once in the evidence. This is done by comparing file hashes.
KFF	<p>Using a database of hashes from known files, this option flags insignificant files as ignoreable files and flags known illicit or dangerous files as alert files, alerting the examiner to their presence in the case.</p> <p>Both AD KFF Alert and AD KFF Ignore groups are selected by default. If you have custom groups and you want them to be enabled, specify them under the Case KFF Options.</p> <p>For more information about Known File Filter (KFF), see “Using the Known File Filter” on page 211.</p>
Expand Compound Files	Automatically opens and processes the contents of compound files such as .ZIP, email, and OLE files.
File Signature Analysis	
Flag Bad Extensions	Identifies files whose types do not match their extensions, based on the file header information.
Entropy Test	<p>Identifies files that are compressed or encrypted.</p> <p>Compressed and encrypted files identified in the entropy test are not indexed.</p>
dtSearch* Text Index	<p>Stores the words from evidence in an index for quick retrieval. Additional space requirement is approximately 25% of the space required for all evidence in the case.</p> <p>Click <i>Indexing Options</i> for extensive options for indexing the contents of the case.</p> <p>New in FTK 3.0: Generated text that is the result of a formula in a document or spreadsheet is indexed, and can be filtered.</p>
Generate Thumbnails for Graphics	<p>Creates thumbnails for all graphics in a case.</p> <p><b>Note:</b> Thumbnails are always .jpg format, regardless of the original graphic file type.</p>
HTML File Listing	Creates an HTML version of the File Listing in the case folder.
CSV File Listing	The File Listing Database is now created in .CSV format instead of an MDB file and can be added to Microsoft Access.

**TABLE 5-3 Evidence Processing Options**

---

<b>Process</b>	<b>Description</b>
Data Carve	Carves data immediately after pre-processing. Click <i>Carving Options</i> , then select the file types to carve. Uses file signatures to identify deleted files contained in the evidence. All available file types are selected by default.  For more information on Data Carving, see “Selecting Data Carving Options” on page 69.
Meta Carve	Carves deleted directory entries and other metadata. The deleted directory entries often lead to data and file fragments that can prove useful to the case, that could not be found otherwise.
Explicit Material Identification	Click EMI Options to specify the EMI threshold for suspected explicit material found in the case.
Registry Reports	Creates RSR reports from case content automatically. Click RSR Directory to specify the location of the RSR Templates. When creating a report, click the RSR option in the Report Wizard to include the RSR reports requested here.

## FUZZY HASHING

Fuzzy hashing is a tool which provides the ability to compare two distinctly different files and determine a fundamental level of similarity. This similarity is expressed as score from 1-100. The higher the score reported the more similar the two pieces of data. A score of 100 would indicate that the files are close to identical. Alternatively a score of 0 would indicate no meaningful common sequence of data between the two files.

Traditional forensic hashes (MD5, SHA-1, SHA-256, etc.) are useful to quickly identify known data and to ensure that files have been forensically preserved. However, these types of hashes cannot indicate how closely two non-identical files match. This is when fuzzy hashing is useful.

In AccessData applications fuzzy hashes are organized into a library. This library is very similar in concept to the AccessData KFF library. The fuzzy hash library contains of a set of hashes for known files that can be compared to evidence files in order to determine if there are any files which may be relevant to a case. Fuzzy hash libraries are organized into groups. Each group contains a set of hashes and a threshold. The group threshold is a number the investigator chooses, to indicate how closely an evidence item must match a hash in the group to be considered a match and to be included as evidence.

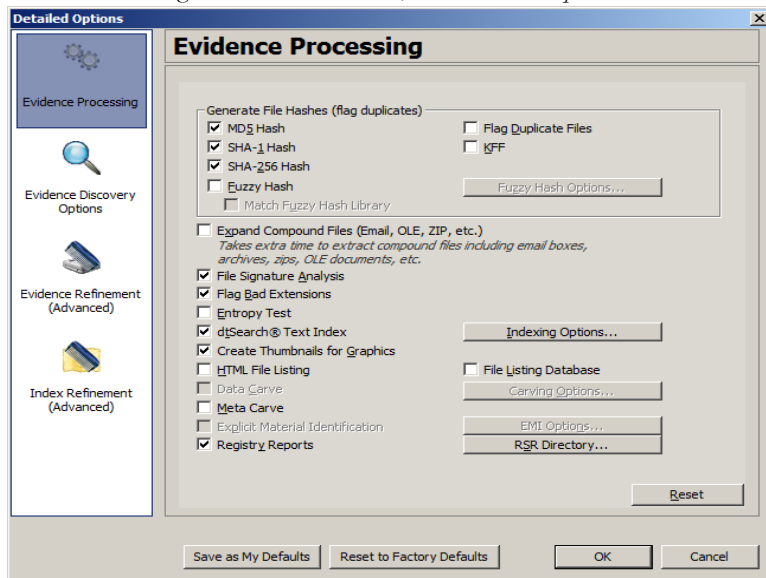
## CREATING A FUZZY HASH LIBRARY

There are two ways to create a fuzzy hash library. The first way is to drag and drop a file, or files, from a disk into the Fuzzy Hash Library screen. The second way is to right click on the file and select, *Add to Fuzzy Hash Library*. To access the Fuzzy Hash Library screen go to *Tools > Fuzzy Hash > Manage Library*.

## SELECTING FUZZY HASH OPTIONS DURING INITIAL PROCESSING

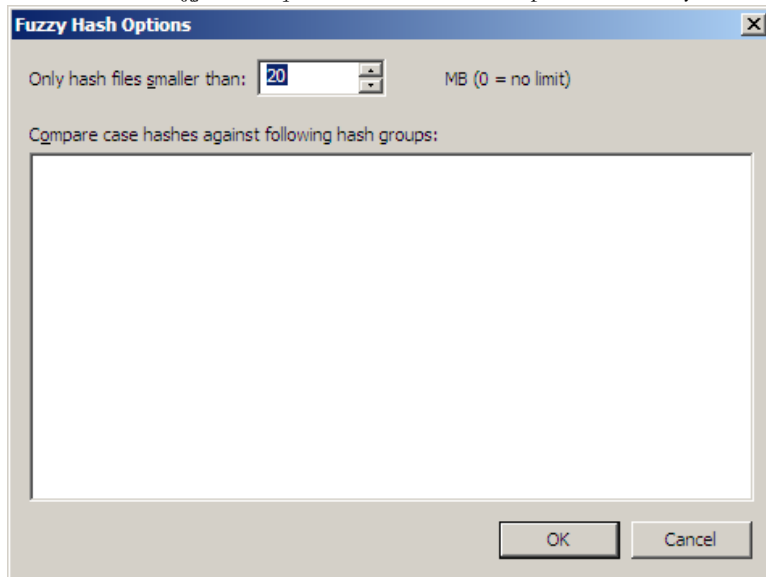
Follow these steps to initialize fuzzy hashing during initial processing or when adding additional evidence to a case:

1. After choosing to create a new case, click *Detailed Options*.



2. Select *Fuzzy Hash*.
  - 2a. (Optional) If FTK already refers to a fuzzy hash library, you can select to match the new evidence against the existing library by selecting *Match Fuzzy Hash Library*.

2b. Click *Fuzzy Hash Options* to set additional options for fuzzy hashing.



2c. Set the size limit of files to hash. The size defaults to 20 MB, 0 indicates no limit.

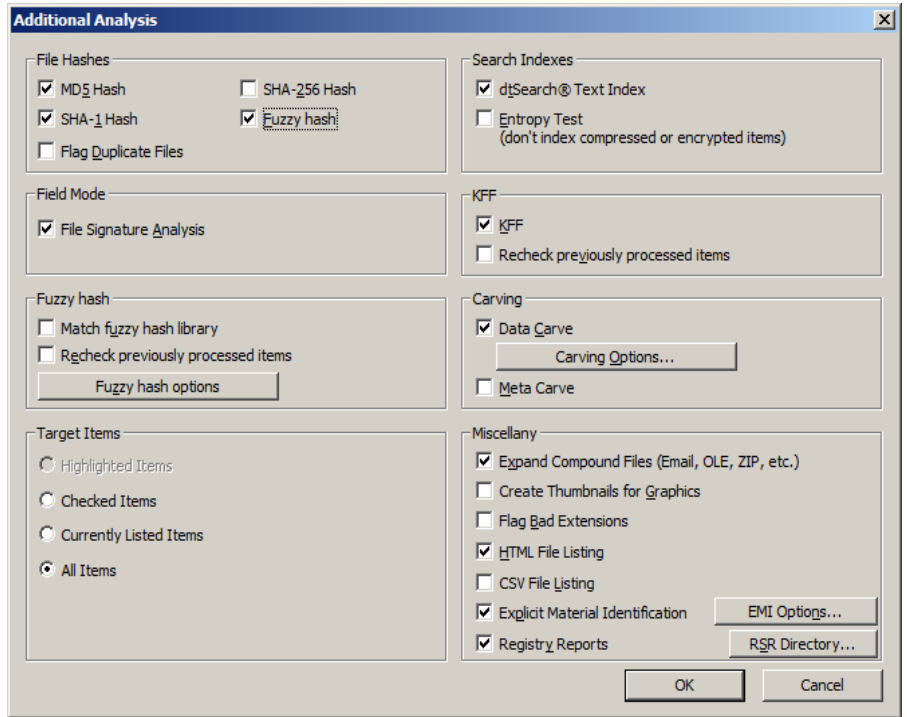
2d. Click *OK* to set the value.

3. Select *OK* to close the detailed options dialog.

## ADDITIONAL ANALYSIS FUZZY HASHING

Fuzzy hashing can also be initialized on data already processed into the case by performing the following steps:

1. Click *Evidence > Additional Analysis*.

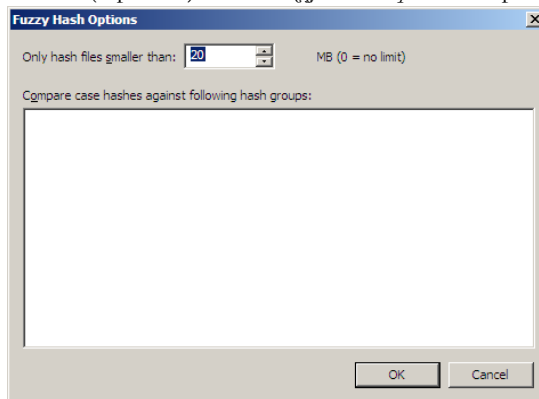


2. Select *Fuzzy Hash*.

3. (Optional) Select if the evidence needs to be matched against the fuzzy hash library.

3a. Mark *Fuzzy Hash* under File Hashes. This activates the Fuzzy Hash options.

3b. (Optional) Click *Fuzzy Hash Options* to open the Fuzzy Hash Options dialog.



- 3c. Set the file size limit on the files to be hashed.
- 3d. If you have created or imported other hash groups, select the ones to use from the list of hash groups.
- 3e. Click *OK*.
4. Click *OK* to close the Additional Analysis dialog and begin the fuzzy hashing.

## COMPARING FILES USING FUZZY HASHING

To compare a file to another file or group of files go to *Tools > Fuzzy Hash > Find Similar Files*. This option allows you to select a file hash to compare against. You can specify the minimum match similarity that you want in this screen. This screen can also be accessed by right clicking on a file and selecting *Find Similar Files*.

## VIEWING FUZZY HASH RESULTS

To view the fuzzy hash results in FTK, several pre-defined column settings can be selected in the Column Settings field under the Common Features category. Those settings are: Fuzzy Hash, Fuzzy Hash blocksize, Fuzzy Hash library group, Fuzzy Hash library score, and Fuzzy Hash library status.

The following table shows the column settings and the description of each:

**TABLE 5-4 Fuzzy Hash Column Settings**

Column Setting	Description
Fuzzy Hash blocksize	Dictates which fuzzy hash values can be used to compare against a file. Fuzzy hashes can only be compared to another fuzzy hash value which is half the fuzzy hash value, equal to the actual fuzzy hash value, or two times the fuzzy hash value.
Fuzzy Hash Library Group	The highest matching group value for a file. To find all of the library groups which have been used to compare a file against, double click on the value in column settings.
Fuzzy Hash	The actual fuzzy hash value given to a file.

**TABLE 5-4 Fuzzy Hash Column Settings**

---

<b>Column Setting</b>	<b>Description</b>
Fuzzy Hash Library Score	The value of the highest group score a file has been compared against. To find all of the library scores, double click on the value in the column settings.
Fuzzy Hash Library Status	Set to either alert or ignore, which is similar to the KFF alert or ignore settings.

## SELECTING DTSEARCH\* TEXT INDEXING OPTIONS

### INDEXING A CASE

All evidence should be indexed to aid in searches. Index evidence when it is added to the case by checking the dtSearch Text Index box on the Evidence Processing Options dialog, or index after the fact by clicking and specifying indexing options.

Another factor that can determine which processes to select is schedule. Time restraints may not allow for all tasks to be performed initially. For example, if you disable indexing, it shortens the time needed to process a case. You can return at a later time and index the case if needed.

### DTSEARCH INDEXING SPACE REQUIREMENTS

To estimate the space required for a dtSearch Text index, plan on approximately 25% of the space needed for each case's evidence.

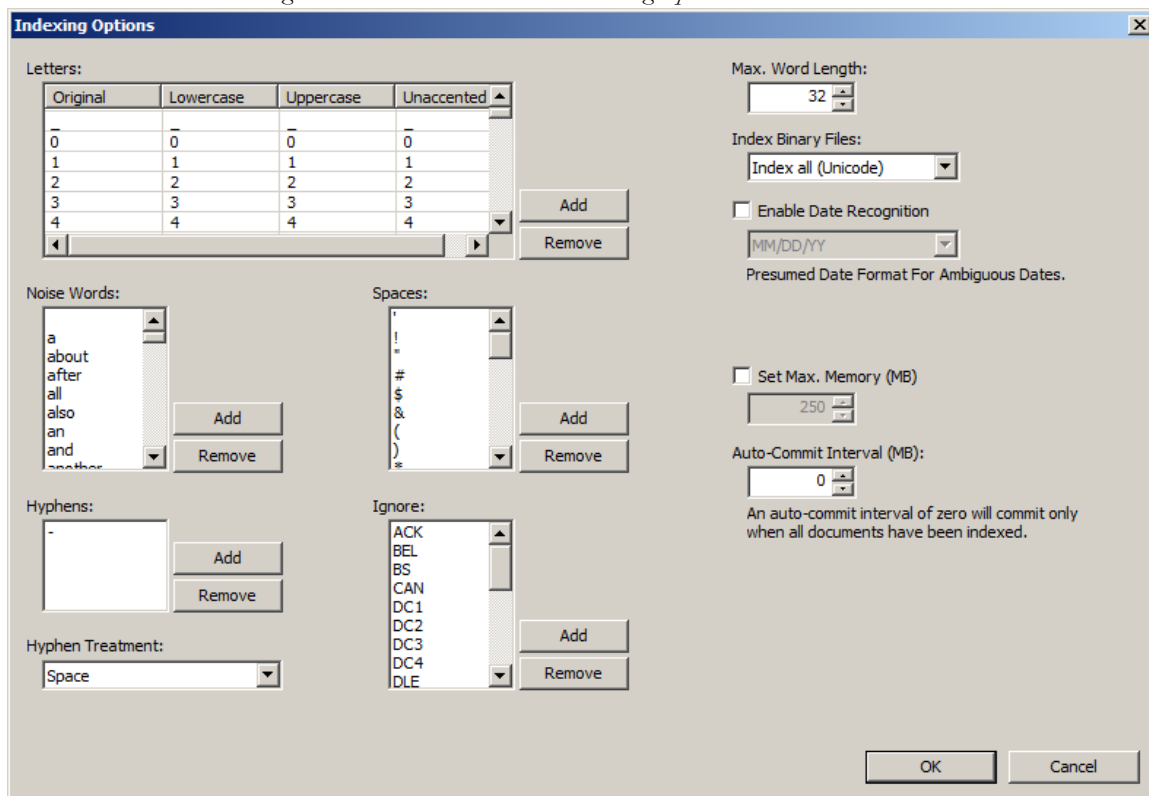
### NEW CASE INDEXING OPTIONS

This new feature gives you almost complete control over what goes in your case index. These options can be selected to apply globally from Case Management by clicking *Tools > Create Options File* to bring up the Detailed Options dialog. In the Evidence Processing screen, mark the *dtSearch Text Index* box, then click *Indexing Options* to bring up the Indexing Options screen shown in the figure below.

**Note:** Search terms for pre-processing options support only ASCII characters.



Figure 5-4 *dtSearch Text Index: Indexing Options*



To adjust these options for a single case, in Case Management, click *Case > New > Detailed Options*. Again, in the Detailed Options: Evidence Processing dialog, mark the *dtSearch Text Index* box, then click *Indexing Options* to bring up the Indexing Options screen shown in the figure above.

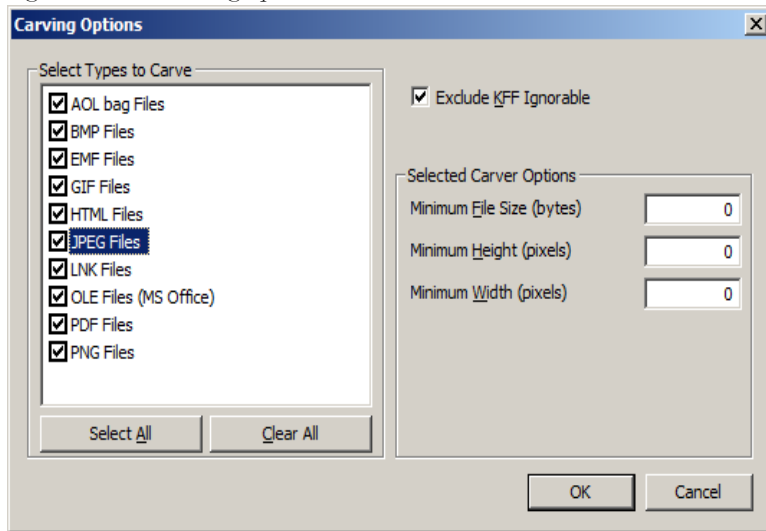
**Note:** The Indexing Options dialog does not support some Turkish characters.

For more detailed information regarding the Indexing Options dialog, see “Chapter 9 Searching a Case” on page 175.

## SELECTING DATA CARVING OPTIONS

Data Carving gives you the choice of which file types to carve, as seen in the following figure:

Figure 5-5 Data Carving Options



When you select to carve data, choose which types of data to carve according to the information below:

1. Select *Data Carve*.
2. Click *Carving Options*.
3. Select the types of files you want carved.
  - Click *Select All* to select all file types to be carved.
  - Click *Clear All* to unselect all file types.
  - Click on individual file types to toggle either selected or unselected.
- Note:** It may help to be aware of the duplicate files and the number of times they appear in an evidence set to determine intent.
4. Define the optional limiting factors to be applied to each file:
  - Define the minimum byte file size for the selected type.
  - Define the minimum pixel height for graphic files.
  - Define the minimum pixel width for graphic files
5. Click *OK*.

## EXPLICIT MATERIAL IDENTIFICATION

New in this version of FTK, Explicit Material Identification reads all graphics in a case and assigns each one a score according to what it interprets as being possible pornography.

When you add evidence to a case, in the *Detailed Options > Evidence Processing* dialog, select Explicit Material Identification to activate EMI Options. The four EMI Options are profiles that indicate the type of filtering each one does.

According to LTU Technologies, “Porn filtering rates pictures according to the presence or absence of pornographic or adult-related content. Successfully filtered pictures are issued a score between 0 and 100 (0 being non-pornographic or “clean” content, 100 being clearly pornographic content). A score above 100 indicates that no decision could be taken (see chapter 3.3). Users of the software then specify their own acceptance threshold limit for images they consider inappropriate.” Negative scores indicate an error in processing the file, or some other error.

Porn scores can be roughly interpreted as follows:

- 0 to 100 = CLEAN to PORN
- -1 = File not found
- -2 = License error
- -3 = Wrong file format
- -4 = No match found
- -5 = Folder not found
- -6 = Unknown error
- -7 = Cannot load Image (e.g, corrupt image)
- -8 = Not enough information
- -9 = Face detection profile path is null
- -10 = Can't open face detection directory
- -11 = Face detection file not found
- -12 = Input classifier not initialized
- -13 = Init profile failed
- -14 = File path is empty
- -16 = Image data is empty
- -17 = Null matching handle

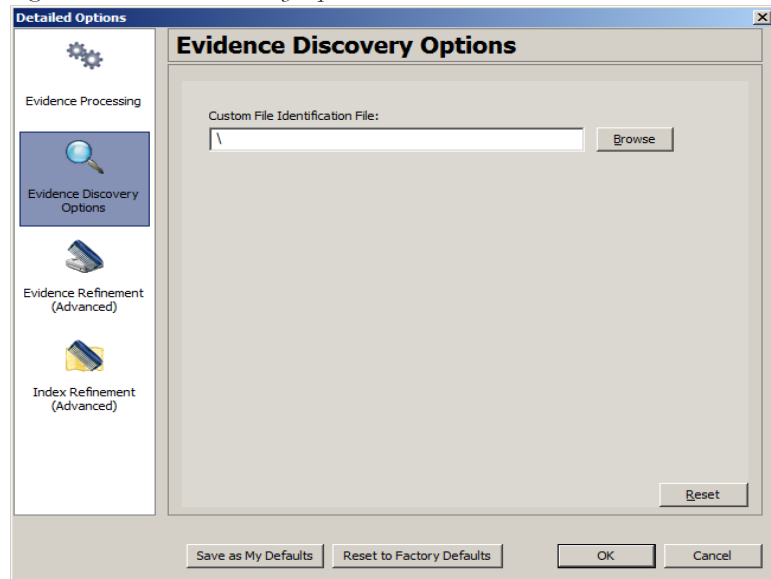
- -18 = Missing retrieval result
- -100 = Unsupported file format.
- -101 = Unsupported black & white image.
- -102 = Unsupported grayscale image.
- -103 = Unsupported monochrome image.
- -1000 = Unknown error.
- -1001 = LTU score function threw an exception.
- -1002 = LTU score function threw an exception.

## SELECTING EVIDENCE DISCOVERY OPTIONS

The Custom File Identification file is a text file that overrides the file types assigned by FTK during preprocessing. With this file, FTK can assign custom file types to specific files.

The Evidence Discovery Options dialog lets you select the Custom File Identification file to apply to new case. This file is stored elsewhere on the system, and the location is determined by the user. The following figure represents the Evidence Discovery Options window in the detailed options dialog. The location can be browsed to, by clicking *Browse*, or reset to the root drive folder by clicking *Reset*.

Figure 5-6 Evidence Discovery Options



## CREATING THE CUSTOM FILE IDENTIFICATION FILE

The Custom File Identification file, or Custom Identifier, creates the new branch “File Category\User Types” on the Overview tab, under which the new file type assignments appear.

The Custom File Identification file can be created in a text editor or similar utility. Each line in the file represents a custom file type assignment. The general format is:

`name, description, category[, offset:value [| offset:value]* ] +`

For example, the line,

```
"MyGIF", "Tim's GIF", "Graphics", 0:"47 49 46 38 37" | 0:"47 49 46 38 39"
```

creates a branch called “MyGIF” under “File Category\User Types.” The offset:value rules in this case look for the string “GIF87” or “GIF89” at offset 0.

The following table describes the parameters for Custom File Identification files:

**TABLE 5-5 Custom File Identification File Parameters**

---

Parameter	Description
Name	The file type displayed in the Overview Container tree branch. It also appears in the Category column.
Description	Accompanies the Overview Container's tree branch name.
Category	The Overview Container tree branch under which the file would normally appear relative to "File Category\user types\".
Offset	A decimal representation of the offset into the file (the first byte of the file is 0). This allows you to find and verify data in a hex view.
Value	An even number of hex bytes or characters with arbitrary white space.

**Note:** You must use at least one offset:value pair (hence the [...]+), and use zero or more OR-ed offset:value pairs (the [...]\*). All of the offset:value conditions in an OR-ed group are OR-ed together, then all of those groups are AND-ed together.

For example, the following line creates a branch called "MyGIF" under "File Category\User Types." The offset:value rules in this case look for the string "GIF87" or "GIF89" at offset 0.

```
"MyGIF", "Tim's GIF", "Graphics",0:"47 49 46 38 37"|0:"47 49 46 38 39".
```

## SELECTING EVIDENCE REFINEMENT (ADVANCED) OPTIONS

The Evidence Refinement Options dialogs allow you to specify how the evidence is sorted and displayed. The Evidence Refinement (Advanced) option allows you to exclude specific data from being added to the case when found in an individual evidence item type.

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

**Important:** After data is excluded from an evidence item in a case, the same evidence cannot be added back into the case to include the previously excluded evidence. If data that was previously excluded is found necessary, the user must remove the related evidence item from the case,

then add the evidence again, using options that will include the desired data.

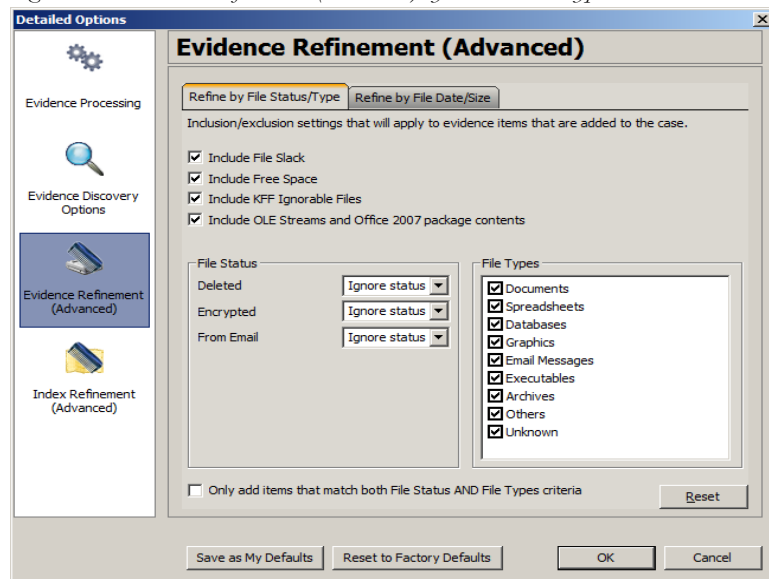
Use the following steps for refining case evidence:

1. Click the *Evidence Refinement (Advanced)* icon in the left pane.  
The Evidence Refinement (Advanced) menu is organized into two dialog tabs:
  - *Refine Evidence by File Status/Type*
  - *Refine Evidence by File Date/Size*
2. Click the corresponding tab to access each dialog.
3. Set the needed refinements for the current evidence item.
4. To reset the menu to the default settings, click *Reset*.
5. To accept the refinement options you have selected and specified, click *OK*.

## REFINING EVIDENCE BY FILE STATUS/TYPE

Refining evidence by file status and type allows you to focus on specific files needed for a case.

Figure 5-7 *Evidence Refinement (Advanced) by File Status/Type*



The following table outlines the options in the Refine Evidence by File Status/Type dialog:

**TABLE 5-6 Refine by File Status/Type Options**

<b>Options</b>	<b>Description</b>
Include File Slack	Mark to include file slack space in which evidence may be found.
Include Free Space	Mark to include unallocated space in which evidence may be found.
Include KFF Ignorable Files	(Recommended) Mark to include files flagged as ignorable in the KFF for analysis
Deleted	Specifies the way to treat deleted files. Options are: <ul style="list-style-type: none"> <li>• Ignore Status</li> <li>• Include Only</li> <li>• Exclude</li> </ul> Defaults to “Ignore Status.”
Encrypted	Specifies the way to treat encrypted files. Options are: <ul style="list-style-type: none"> <li>• Ignore Status</li> <li>• Include Only</li> <li>• Exclude</li> </ul> Defaults to “Ignore Status.”
From Email	Specifies the way to treat email files. Options are: <ul style="list-style-type: none"> <li>• Ignore Status</li> <li>• Include Only</li> <li>• Exclude</li> </ul> Defaults to “Ignore Status.”
Include OLE Streams	Includes Object Linked or Embedded (OLE) files found within the evidence.
File Types	Specifies which types of files to include and exclude
Match using both File Type and File Status criteria	Applies selected criteria from both File Status and File Types tabs to the refinement.

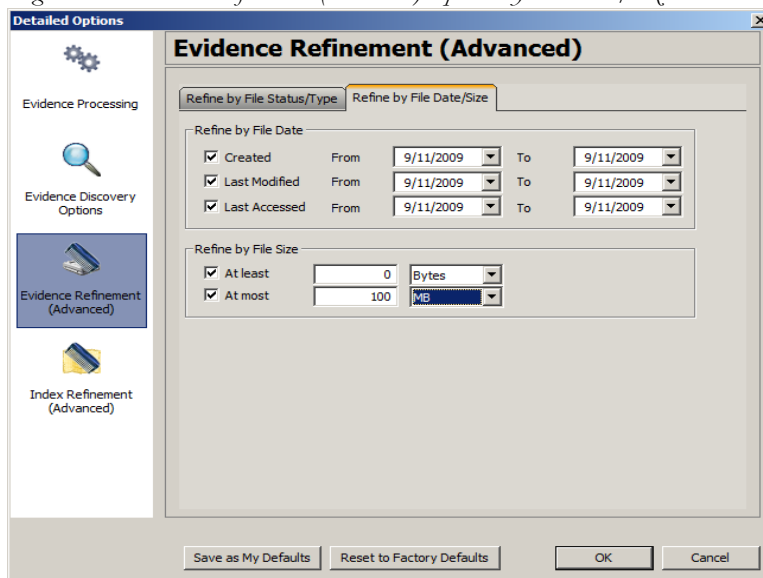


## REFINING EVIDENCE BY FILE DATE/SIZE

Refine evidence further by making the addition of evidence items dependent on a date range or file size that you specify. However, once in the case, filters can also be applied to accomplish this.

The following figure shows an example of the options in the Evidence Refinement (Advanced) page:

Figure 5-8 Evidence Refinement (Advanced) Options by File Date/Size



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

**TABLE 5-7 Refine by File Date/Size Options**

---

<b>Exclusion</b>	<b>Description</b>
Refine Evidence by File Date	To refine evidence by file date: <ol style="list-style-type: none"><li>1. Check <i>Created</i>, <i>Last Modified</i>, and/or <i>Last Accessed</i>.</li><li>2. In the two date fields for each date type selected, enter beginning and ending date ranges.</li></ol>
Refine Evidence by File Size	To refine evidence by file size: <ol style="list-style-type: none"><li>1. Check <i>At Least</i> and/or <i>At Most</i> (these are optional settings).</li><li>2. In the corresponding size box(es), specify the applicable file size.</li><li>3. In the drop-down lists, to the right of each, select <i>Bytes</i>, <i>KB</i>, or <i>MB</i>.</li></ol>

## SELECTING INDEX REFINEMENT (ADVANCED) OPTIONS

The Index Refinement (Advanced) feature allows you to specify types of data that you do not want to index. You may choose to exclude data to save time and resources, or to increase searching efficiency.

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

To refine an index, in the Detailed Options dialog perform the following steps:

1. Click *Index Refinement (Advanced)* in the left pane.

The Index Refinement (Advanced) menu is organized into two dialog tabs:

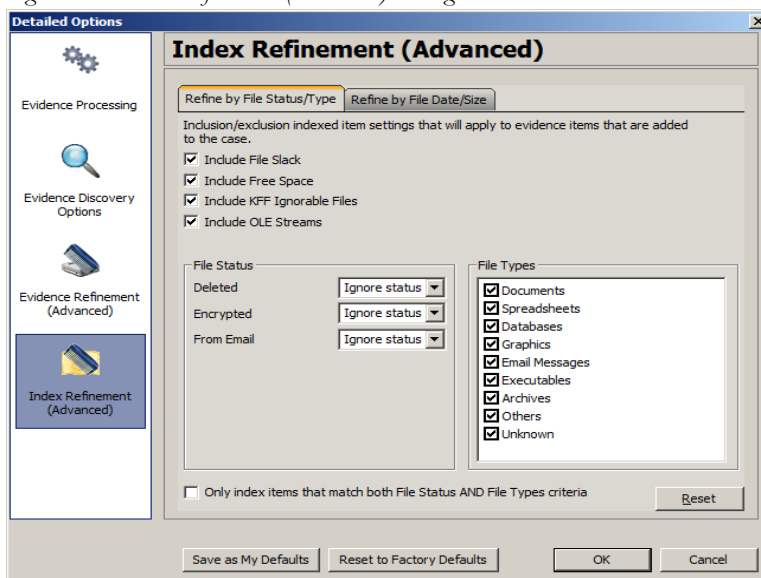
  - *Refine Index by File Status/Type*
  - *Refine Index by File Date/Size*
2. Click the corresponding tab to access each dialog.
3. Define the refinements you want for the current evidence item.
4. Click *Reset* to reset the menu to the default settings.
5. Click *OK* when you are satisfied with the selections you have made.

## REFINING AN INDEX BY FILE STATUS/TYPE

Refining an index by file status and type allows the investigator to focus attention on specific files needed for a case through a refined index defined in a dialog as contained in the following figure.

At the bottom of the two Index Refinement tabs you can choose to mark the box for *Only index items that match both File Status AND File Types criteria*, if that suits your needs.

Figure 5-9 Index Refinement (Advanced) Dialog



The following table outlines the Refine the Index by File Status/Type dialog options:

**TABLE 5-8 Refine Index by File Status/Type Options**

Options	Description
Include File Slack	Mark to include free space between the end of the file footer, and the end of a sector, in which evidence may be found.
Include Free Space	Mark to include both allocated (partitioned) and unallocated (unpartitioned) space in which evidence may be found.
Include KFF Ignorable Files	Mark to include files flagged as ignorable in the KFF for analysis.

**TABLE 5-8 Refine Index by File Status/Type Options**

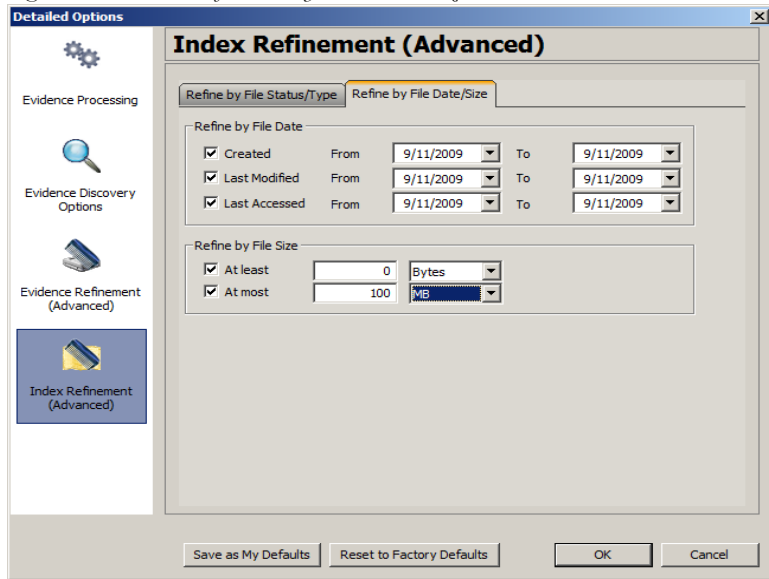
---

<b>Options</b>	<b>Description</b>
Deleted	Specifies the way to treat deleted files. Options are: <ul style="list-style-type: none"><li>• Ignore status</li><li>• Include only</li><li>• Exclude</li></ul>
Encrypted	Specifies the way to treat encrypted files. Options are: <ul style="list-style-type: none"><li>• Ignore status</li><li>• Include only</li><li>• Exclude</li></ul>
From Email	Specifies the way to treat email files. Options are: <ul style="list-style-type: none"><li>• Ignore status</li><li>• Include only</li><li>• Exclude</li></ul>
Include OLE Streams	Includes Object Linked or Embedded (OLE) files found within the evidence.
File Types	Specifies types of files to include and exclude.
Match using both File Type and File Status criteria	Applies selected criteria from both File Status and File Types tabs to the refinement.

## **REFINING AN INDEX BY FILE DATE/SIZE**

Refine index items dependent on a date range or file size you specify, as displayed in the following figure:

Figure 5-10 Index Refinement by File Date/Size



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

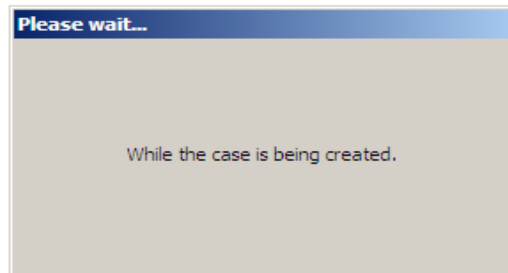
**TABLE 5-9 Refine Index by File Date/Size Options**

Exclusion	Description
Refine Index by File Date	To refine index content by file date: <ol style="list-style-type: none"> <li>1. Select <i>Created</i>, <i>Last Modified</i>, or <i>Last Accessed</i>.</li> <li>2. In the date fields, enter beginning and ending dates within which to include files.</li> </ol>
Refine Index by File Size	To refine evidence by file size: <ol style="list-style-type: none"> <li>1. Click in either or both of the size selection boxes.</li> <li>2. In the two size fields for each selection, enter minimum and maximum file sizes to include.</li> <li>3. In the drop-down lists, select whether the specified minimum and maximum file sizes refer to <i>Bytes</i>, <i>KB</i>, or <i>MB</i>.</li> </ol>

## CREATING THE CASE

When you have finished selecting all the initial case options, you are ready to create the case. No evidence has been added to the case yet. Click *OK > OK* to begin case creation. FTK indicates that it is creating the case and asks you to please wait.

Figure 5-11 Please Wait While the Case is Being Created.



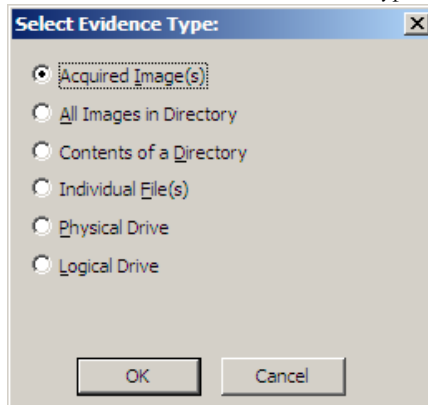
## ADDING EVIDENCE TO A NEW CASE

When case creation is complete, the Manage Evidence dialog appears. Evidence items added here will be processed using the options you selected in pre-processing.

**Note:** You can repeat this process as many times as you need to, for the number of evidence items and types you wish to add.

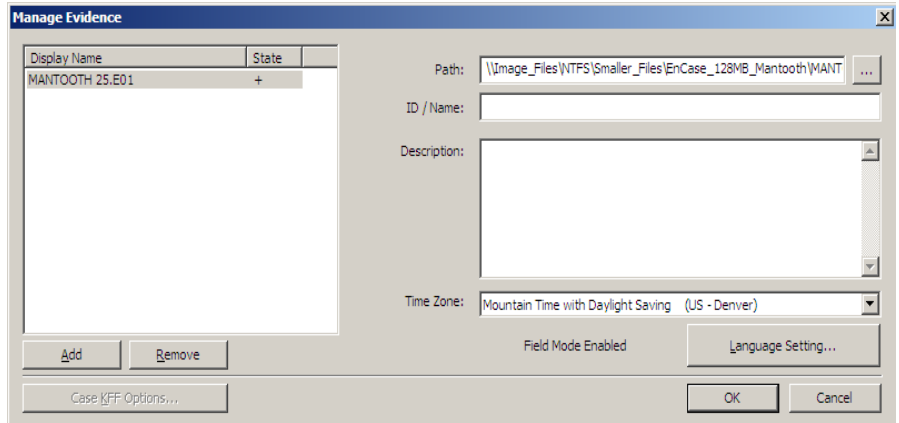
To add evidence to a case, do the following:

1. Click *Add*. The Select Evidence Type dialog appears.



2. Select the type of evidence item(s) to add to the case at this time.

3. Click *OK*.
4. Browse to the evidence item(s) to add. Select the item(s). Click *Open*.
5. If you are in Field Mode the Manage Evidence dialog will indicate Field Mode below the Time Zone Selection, and you will not be able to specify any detailed evidence options. You will still be able to change the Language Setting however, as shown in the figure below:



If you are not creating this case in Field Mode, the Detailed Options button will be available. Click *Detailed Options* to override settings that were previously selected for evidence added to this case. If you do not click *Detailed Options* here, the options that were specified when you created the case will be used.

6. Complete the Manage Evidence dialog based on information in the following table:

**TABLE 5-10 Manage Evidence Options**

Option	Description
Add	Opens the Select Evidence Type dialog. Click to select the evidence type, and a Windows Explorer instance will open, allowing you to navigate to and select the evidence you choose
Remove	Displays a caution box and asks if you are sure you want to remove the selected evidence item from the case. Removing evidence items that are referenced in bookmarks and reports will remove references to that evidence and they will no longer be available. Click <i>Yes</i> to remove the evidence, or click <i>No</i> to cancel the operation.
Display Name	The filename of the evidence being added.

**TABLE 5-10 Manage Evidence Options**

---

<b>Option</b>	<b>Description</b>
State	<p>The State of the evidence item:</p> <ul style="list-style-type: none"><li>• “ ” (empty) indicates that processing is complete.</li><li>• “+” indicates the item is to be added to the case</li><li>• “-” indicates the item is to be removed from the case.</li><li>• “*” indicates the items is processing.</li><li>• “!” Indicates there was a failure in processing the item.</li></ul> <p>If you click Cancel from the Add Evidence Dialog, the state is ignored and the requested processing will not take place.</p> <p><b>Note:</b> If the State field is blank and you think the item is still processing, from any tab view, click <i>View &gt; Progress Window</i> to verify.</p>
Path	<p>The full pathname of the evidence file.</p> <p><b>Note:</b> Use universal naming convention (UNC) syntax in your evidence path for best results.</p>
ID/Name	The optional ID/Name of the evidence being added.
Description	The options description of the evidence being added. This can be the source of the data, or other description that may prove helpful later.
Time Zone	The time zone of the original evidence. Select a time zone from the drop-down list.
Language Setting	Select the code page for the language to view the case in. The Language Selection dialog contains a drop-down list of available code pages. Select a code page and click <i>OK</i> .
Case KFF Options	Opens the KFF Admin box for managing KFF libraries, groups, and sets for this case.
Refinement Options	<p>Displays the Refinement Options for Evidence Processing. This dialog has limited options compared to the Refinement Options selectable prior to case creation. You cannot select Save as My Defaults, nor can you select <i>Reset</i> to reset these options to the Factory Defaults.</p> <p>Select the options to apply to the evidence being added, then click <i>OK</i> to close the dialog.</p>

7. When you are satisfied with the evidence options selected, click *OK*.



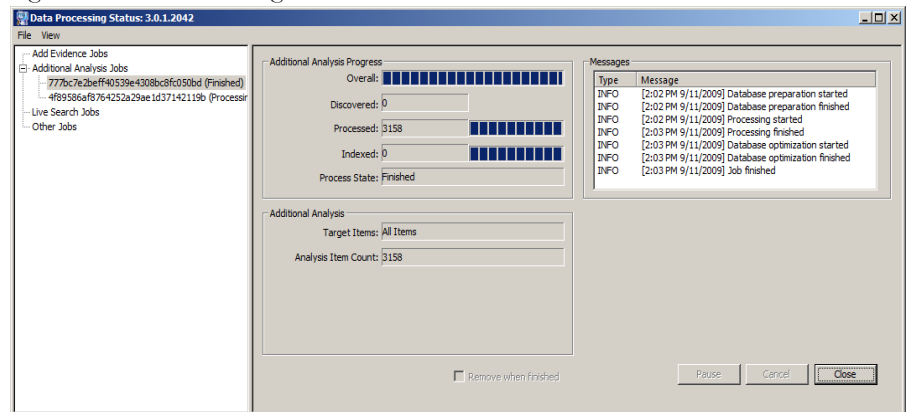
## PROCESSING EVIDENCE

When all evidence has been added and all options have been chosen, click *OK*. The Data Processing Status window appears and processing begins.

As you watch the Data Processing Status progress and complete, if you compare the numbers in the Data Processing Status screen with the numbers shown in *Overview tab > Case Overview > File Category*, for example, you may notice that the numbers are not the same. If there is a difference, the numbers in the case are accurate; the numbers in the Data Processing Screen on the progress bar items are not.

FTK shows the Data Processing Status screen similar to that shown in the following figure:

Figure 5-12 Data Processing Status: Finished



Each task is listed individually on the left. A blue progress bar measures percentage complete by a ratio, or simply by a moving bar as each task progresses. When the task is complete, the Process State shows Finished.

- Click the different Job types to see other tasks or jobs that have been created, and their status.
- Click *Remove when finished* to remove a task or job from the list when it is complete.
- Click *Close* to close the Data Processing Status Dialog.
- Click the *Close* button to close the Data Processing Status Window. This closes only the display and does not cancel any current tasks.

## VIEWING PROCESSED ITEMS

It is not necessary to wait for the program to finish processing the case to begin viewing data. The metadata—the information about the evidence—can be viewed in several modes before the disk image has completed processing.

**Important:** Do not attempt to do any search prior to processing completion. You can view processed items from the tabbed views, but searching during indexing may corrupt the index and render the case useless.

## THE FTK USER INTERFACE

When a case has been created, before evidence has been added you will see the FTK User Interface. The FTK User Interface is described in detail in Chapter 5. For more information, see “Chapter 6 Adding and Processing Static Evidence” on page 87.

# Chapter 6 Adding and Processing Static Evidence

After creating a case in AccessData Forensic Toolkit (FTK) Case Manager, open the case. Investigate the case by running searches, bookmarking, exporting relevant files when necessary, verifying the drive image integrity, identifying meaningful evidence, and performing other tasks. For more information regarding creating a new case, see “Chapter 5 Starting a New FTK 3.0 Case” on page 53.

## STATIC EVIDENCE VS. REMOTE EVIDENCE

Static evidence describes evidence that has been captured *to an image* before being added to the case.

Live evidence describes data that is acquired in-person *to an image* from a machine that is running. For example, a suspect’s computer—whether because a password is not known, or to avoid the suspect’s knowing that he or she is under suspicion—may be imaged live if the computer has not yet been or will not be confiscated.

Remote evidence describes data that is acquired from remote live computers belonging to the FTK network after the case has been created. That evidence is added directly to the case as it is acquired.

This chapter covers working with static evidence. For more information regarding acquisition and utilization of remote evidence, see “Chapter 7 Adding and Processing Remote Live Evidence” on page 121.

## ACQUIRING AND PRESERVING STATIC EVIDENCE

For digital evidence to be valid, it must be preserved in its original form. The evidence image must be forensically sound, in other words, identical in every way to the original.

Two types of tools can do this: hardware acquisition tools and software acquisition tools.

- Hardware acquisition tools duplicate, or clone, disk drives and allow read-only access to the hard drive. They do not necessarily use a CPU, and are often hand-held.
- Software acquisition tools also create a disk image and in addition, give you a choice regarding the file format, the compression level where available, and the size of the data segments to use.

**Important:** Use a write-blocking device when using software tools, because some operating systems, such as Windows, make changes to the drive as it reads the data to be imaged.

**Important:** If the Mozilla Firefox directory is added as evidence while in use, history, downloads, etc are identified as zero-length files.

FTK Imager is a software acquisition tool. It can quickly preview evidence and, if the evidence warrants further investigation, create a forensically sound image of the evidence drive or source. It makes a bit-by-bit duplicate of the media, rendering a forensic disk image identical in every way to the original, including file slack and unallocated or free space.

## OPENING AN EXISTING CASE

Open an existing case from FTK Case Manager. To open an existing case, perform the following steps:

1. Log on to FTK 3.0.
2. Double-click on the case you want to open, or highlight the case and click *Case > Open*.

## ADDING EVIDENCE

After setting up a case, evidence must be added to it for processing. After evidence has been added, you can perform some processing tasks that were not performed initially. You can also add more evidence to the case after the initial processing of evidence is

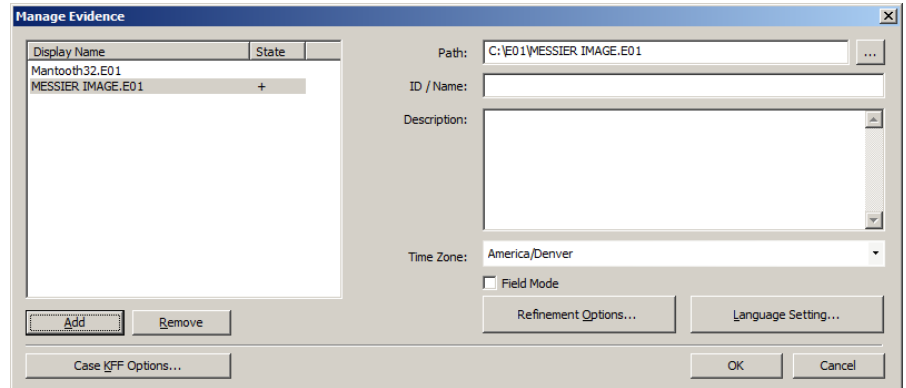
complete. Additional evidence files and images can be added and processed later, if needed.

**Note:** After processing, the Evidence Processing selected options can be found in the case log. You can also view them by clicking Evidence > Add/Remove. Double-click on any of the evidence item to open the Refinement Options dialog.

To add static evidence (an exact image, or “snapshot” of electronic data found on a hard disk or other data storage device) to an existing case, select *Evidence > Add/Remove* from the menu bar and continue as shown below.

**Note:** Use universal naming convention (UNC) syntax in your evidence path for best results.

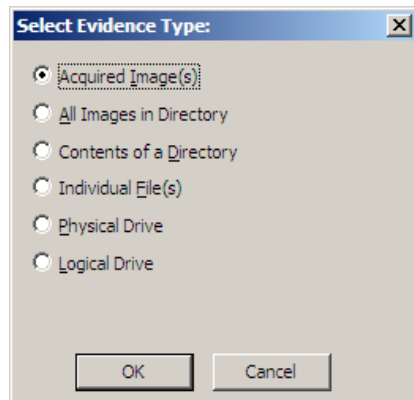
Figure 6-1 Managing Evidence



To add new evidence to the case perform the following steps.

**Note:** To remove evidence from the list either before processing, or after it has been added to the case, select the evidence item in the list, then click *Remove*.


1. Click *Add* to choose the type of evidence items to add into a new case.



**Note:** Evidence taken from any physical source that is removable, whether it is a “live” drive or an image, will become inaccessible to the case if the drive letters change or the evidence-bearing source is moved. Instead, create a disk image of this drive, save it either locally, or to the drive you specified during installation, then add the disk image to the case. Otherwise, be sure the drive will be available whenever working on the case.

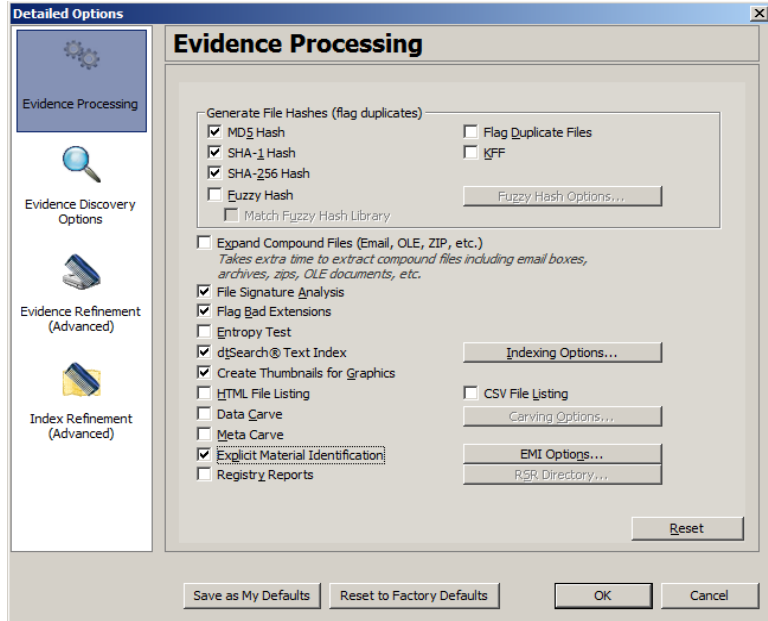
2. Mark the type of evidence to add, then click *OK*.
3. Browse to and select the evidence item from the stored location.
4. Click *OK*.

**Note:** Folders and files not contained in an image when added to the case will be imaged in the AD1 format and stored in the case folder. If you select AD1 as the image type, you can add these without creating an image from the data.

- 4a. (Optional) Click the Browse button  at the end of the Path field to browse to another path.
5. Fill in the ID/Name field with any specific ID or Name data applied to this evidence for this case.
6. Use the Description field to enter an optional description of the evidence being added.
7. Select the Time Zone of the evidence where it was seized in the Time Zone field. This is required to save the added evidence.  
After selecting an Evidence Type, and browsing to and selecting the evidence item, the selected evidence displays under Display Name. The Status column shows a plus (+) symbol to indicate that the file is being added to the case.
8. Click *Refinement Options* to open the Refinement Options dialog with a set similar to the Refinement Options set at case creation. Refinement Options are much the same as Detailed Options. For this reason, only the main Refinement Options

screen is included here. For more extensive information, see “Chapter 5 Starting a New FTK 3.0 Case” on page 53.

Figure 6-2 Refinement Options for Adding Evidence After Case Creation



The sections available are:

- Evidence Processing
- Evidence Refinement (Advanced)
- Index Refinement (Advanced)

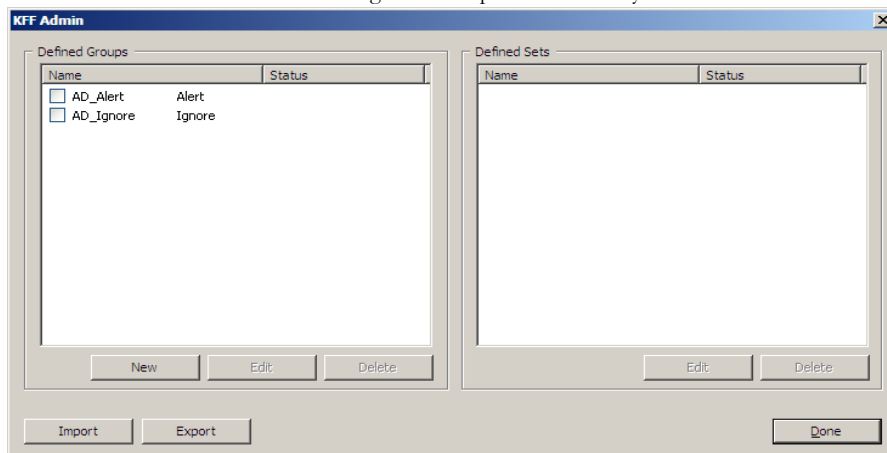
For more information on Evidence Processing options, see “Selecting Evidence Processing Options” on page 58.

For more information on Evidence Refinement (Advanced) options, see “Selecting Evidence Refinement (Advanced) Options” on page 74.

For more information on Index Refinement (Advanced), see “Selecting Index Refinement (Advanced) Options” on page 78.

9. Click *OK* to accept the settings and to exit the Manage Evidence dialog.
10. Select the *KFF Options* button to display the KFF Admin dialog.

**Note:** The AD Alert and the AD Ignore Groups are selected by default.



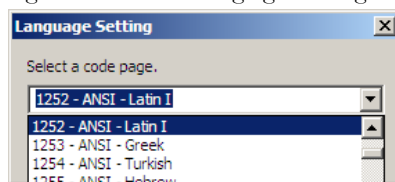
See “Using the Known File Filter” on page 211 for detailed information about the KFF.

11. Click *Done* to accept settings and return to the Manage Evidence dialog.
12. Click *Language Settings* to select the codepage for the language to be used for viewing the evidence. More detail is given in the following section.
13. Click *OK* to add and process the evidence.

## SELECTING A LANGUAGE

If you are working with a case including evidence in another language, or you are working with a different language OS, click *Language Settings* from the Manage Evidence dialog.

Figure 6-3 Select a Language CodePage Setting



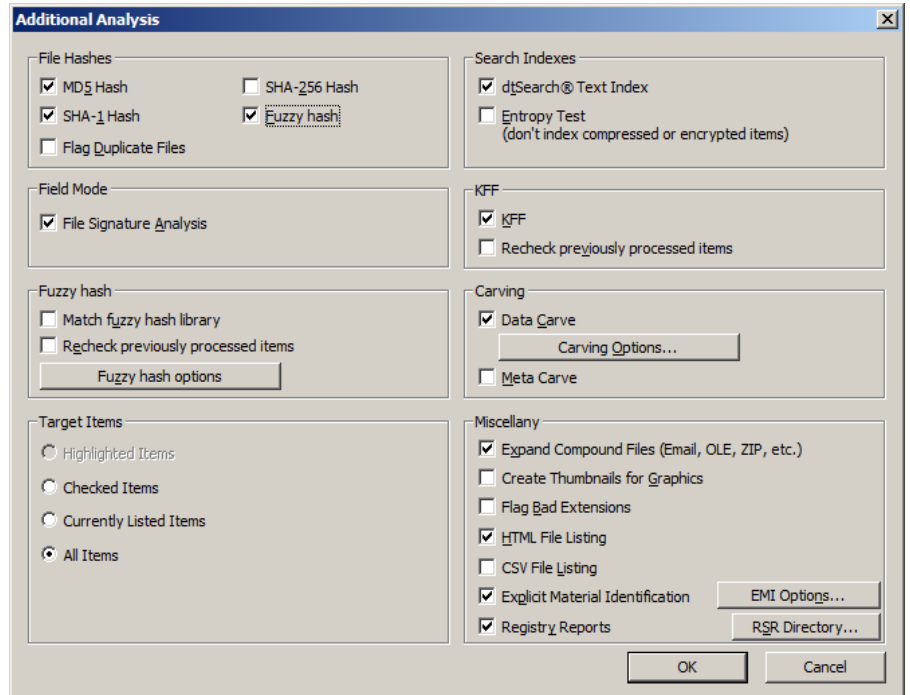
The Language Setting dialog appears, allowing you to select a code page from a drop-down list. When the setting is made, click *OK*.



## ADDITIONAL ANALYSIS

After evidence has been added to a case and processed, you may wish to perform other analysis tasks. To further analyze selected evidence, click *Evidence > Additional Analysis*. The following figure represents the Additional Analysis dialog.

Figure 6-4 *Additional Analysis Dialog*



Most of the tasks available during the initial evidence processing remain available with Additional Analysis. Specific items can also be targeted. Multiple processing tasks can be performed at the same time.

Make your selections based on the information in the table below. Click *OK* when you are ready to continue.

**TABLE 6-1 Additional Analysis Options**

Field	Description
File Hashes	<p>These options create file hashes for the evidence. The Options are:</p> <ul style="list-style-type: none"> <li>• <b>MD5 Hash:</b> This hash option 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 (“Message Digest 5” on page 337).</li> <li>• <b>SHA-1 Hash:</b> This hash option 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 (see “Secure Hash Algorithm” on page 340).</li> <li>• <b>SHA-256:</b> This hash option 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 (see “Secure Hash Algorithm” on page 340).</li> <li>• <b>Fuzzy Hash:</b> Mark to enable Fuzzy Hash options, described below. For more information on Fuzzy Hashes, see “Fuzzy Hashing” on page 63.</li> <li>• <b>Flag Duplicates:</b> Mark to flag duplicate files. This applies to all files in the case, regardless of the Target Items selected</li> </ul> <p><b>Note:</b> A blank hash field appears for unallocated space files, the same as if the files had not been hashed at all. To notate in the hash field the reason for it being blank would slow the processing of the evidence into the case.</p>
Search Indexes	<p>Choose <i>dtSearch® Index</i> to create a dtSearch index that enables index searches. Marking <i>dtSearch Index</i> activates the Entropy Test check box.</p> <p><b>Note:</b> Select <i>Entropy Test</i> to exclude compressed or encrypted items from the index.</p>
Field Mode	<p>Choose to do File Signature Analysis, which is not normally done in Field Mode.</p> <p><b>Note:</b> The Job Processing screen will always show 0 for Queued when Field Mode is enabled, because items move directly from Active Tasks to Completed.</p> <p><b>Note:</b> In addition to disabling <i>Detailed Options</i>, Field Mode bypasses file signature analysis and the Oracle database communication queue. These things vastly speed the processing.</p>
KFF	<p><b>KFF:</b> Filters targeted files in the KFF. Select KFF to filter targeted files in the KFF. When KFF is selected, the user can select to Recheck previously processed items when searching for new information, or when a KFF group is added or changed.</p>

**TABLE 6-1 Additional Analysis Options**

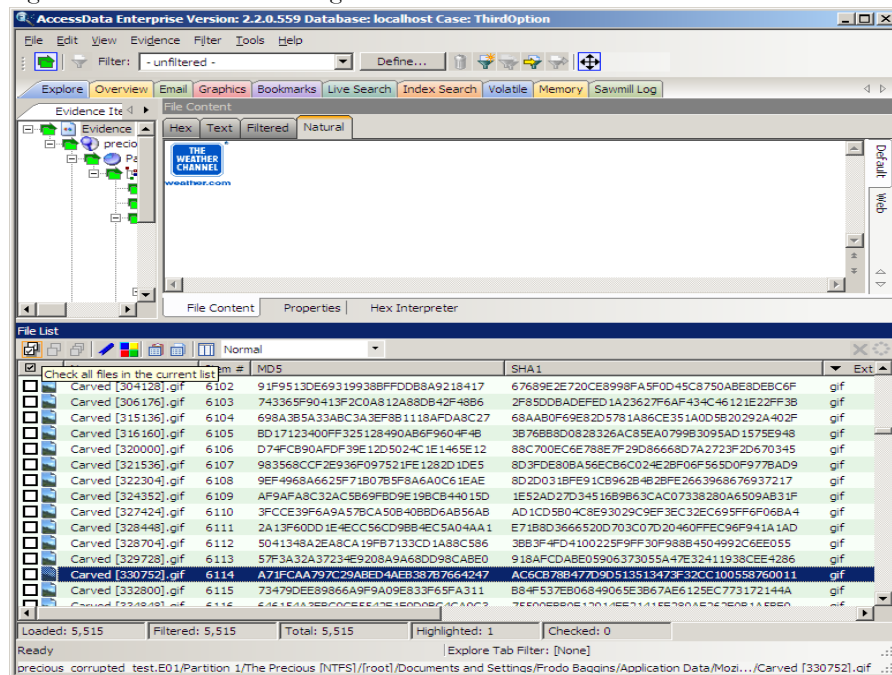
<b>Field</b>	<b>Description</b>
Fuzzy Hashing	<p>Choose either <i>Fuzzy Hash</i>, or both <i>Fuzzy Hash</i> and <i>Match Fuzzy Hash Library</i>; marking Fuzzy Hash activates Match Fuzzy Hash Library.</p> <p>Click <i>Fuzzy Hash Options</i> to select Fuzzy Hash groups, and specify file limitations for matching. For more information on Fuzzy Hashes, see “Fuzzy Hashing” on page 63.</p>
Carving	<p>Choose to run the MetaCarve process, and if you also choose Expand Compound Files under Miscellany, you can also choose to run Data Carving, and select which Carving Options to use.</p>
Target Items	<p>Select the items on which to perform the additional analysis. Highlighted, and Checked items will be unavailable if no items in the case are highlighted or checked. The following list shows the available options:</p> <ul style="list-style-type: none"><li>• <b>Highlighted Items:</b> Performs the additional analysis on the items highlighted in the File List pane when you select Additional Analysis.</li><li>• <b>Checked Items:</b> Performs the additional analysis on the checked evidence items in the File List pane when you select Additional Analysis.</li><li>• <b>Currently Listed Items:</b> Performs the additional analysis on all the evidence items currently listed in the File List pane when you select Additional Analysis.</li><li>• <b>All Items:</b> Performs the additional analysis on all evidence items in the case.</li></ul>
Miscellany	<ul style="list-style-type: none"><li>• <b>Expand Compound Files (Email, OLE, Zip, etc.):</b> expands and indexes files that contain other files.</li><li>• <b>Generate Thumbnails:</b> Generates thumbnails for graphic files found in the evidence. Thumbnails are always .JPG format, regardless of the original graphic format.</li><li>• <b>Flag Bad Extensions:</b> Flags files that have extensions that do not match the file headers.</li><li>• <b>HTML File Listing:</b> Generate a list of files contained in the case, in HTML format.</li><li>• <b>Explicit Material Identification:</b> Enables EMI Options button. EMI license is purchased separately. This item will be disabled unless the license is detected on your CmStick.</li><li>• <b>Registry Reports:</b> Enables Registry Summary Reports (RSRs) to be used directly from Registry Viewer if it is installed. Specify the location of any RSR templates you have saved or downloaded from the AccessData website.</li></ul>

# HASHING

Hashing a file refers to the process of generating a unique value based on a file's contents. Use hash values to verify file integrity and to identify duplicate files as well as "known" files

Known files include standard system and program files that can be flagged as "ignorable", as well as known illicit or dangerous files for which program alerts call the attention of the investigator if found in the case. More details are given in the table above. The following figure shows the hash values for files in the File List view.

Figure 6-5 File List View Showing the Hashes Column



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

You can also use hashes to eliminate data from your case, once you identify files not interesting, or pertinent, to the case. Export the hash list for those files and add them to your KFF, then reprocess the case. Despite the time required, this technique proves highly effective when necessary.

## DATA CARVING

AccessData FTK has the ability to carve data. Data carving is the process of locating files and objects that have been deleted or that are embedded in other files.

Because embedded items and deleted files can contain information that may be helpful in forensic investigations, FTK simplifies the process of recovering these items and adding them to the case.

The data carving feature allows the recovery of previously deleted files located in unallocated space. Users can also carve directory entries to find information about data or metadata.

**Note:** You can manually carve for any file type for which you have the correct header/footer/file length information, then save that file and add it to the case.

To recover embedded or deleted files, FTK searches the case evidence for specific file headers. Using the data from a file header for a recognized file type, FTK determines the length of that file, or looks for the file footer, and “carves” the associated data, then saves it as a distinct file. A child object is created with a name reflecting the type of object carved and its offset into the parent object’s data stream. FTK can find any embedded or deleted item as long as the file header still exists.

Data carving can be done when adding evidence to a case, or by clicking *Evidence > Additional Analysis > Data Carve* from within a case. You can search all items for the following file types:

**TABLE 6-2 Recognized File Types for Data Carving**

---

• AOL Bag Files	• LNK Files
• BMP Files	• OLE Archive Files (Office Documents)
• EMF Files	• PDF Files
• GIF Files	• PDF Files
• HTML Files	• PNG Files
• JPEG Files	

You can set additional options to refine the data carving process for the selected file types.

### DATA CARVING FILES WHEN PROCESSING A NEW CASE

Choose to data carve when a case is created by following these steps:

1. Selecting *Data Carve* in CaseManager  
Click *Case > New > Detailed Options*.
2. In the Evidence Processing dialog select *Expand Compound Files* to enable *Data Carve*.
3. Click *Data Carve*.
4. Click *Carving Options*.
5. Mark the file types to carve.
6. Click *OK*.

For more information, see “Selecting Evidence Processing Options” on page 58.

## DATA CARVING FILES IN AN EXISTING CASE

Data carving can be performed on previously processed data.

To data carve files in an existing case:

1. From the *Evidence > Additional Analysis*.
2. In the Evidence Processing dialog select *Expand Compound Files* to enable *Data Carve*.
3. Check *Data Carve*.
4. Click *Carving Options*.
5. Set the data carving options to use.
6. Click *OK* to close the Carving Options dialog.
7. Select the target items to carve data from.
8. Click *OK*.

The carved objects and files are automatically added to the case, and can be searched, bookmarked, and organized along with the existing files. For more information, see “Chapter 8 Using Tabs to Explore & Refine Evidence” on page 129.

## THE FTK USER INTERFACE

The FTK user interface is comprised of several components. There is a Menu Bar, a ToolBar, UI Tabs, and various panes. The user interface has many customizable features. For example, Tab views can be customized, to suit your needs. For more information on customizing the FTK3.0 user interface, see “Chapter 13 Customizing the FTK Interface” on page 263.

# FTK MENUS AND TOOLBARS

The FTK user interface is comprised of several components. Common throughout the interface is a Menu Bar, a Toolbar and a Tab bar. Wherever a File List pane is found, there is also a File List ToolBar. These elements are discussed in this section.

## MENU BAR COMPONENTS

When a case is created and assigned a user, the FTK Case window opens with the following menus:

**TABLE 6-3 FTK 3.0 Menu Bar Items**

---

• File	• Filter
• Edit	• Tools
• View	• Help
• Evidence	

The following tables show the available options from the FTK 3.0 user interface window menus. Details on some items are found below the table in which they are introduced.

## FILE MENU OPTIONS

**TABLE 6-4 FTK3.0 File Menu**

---

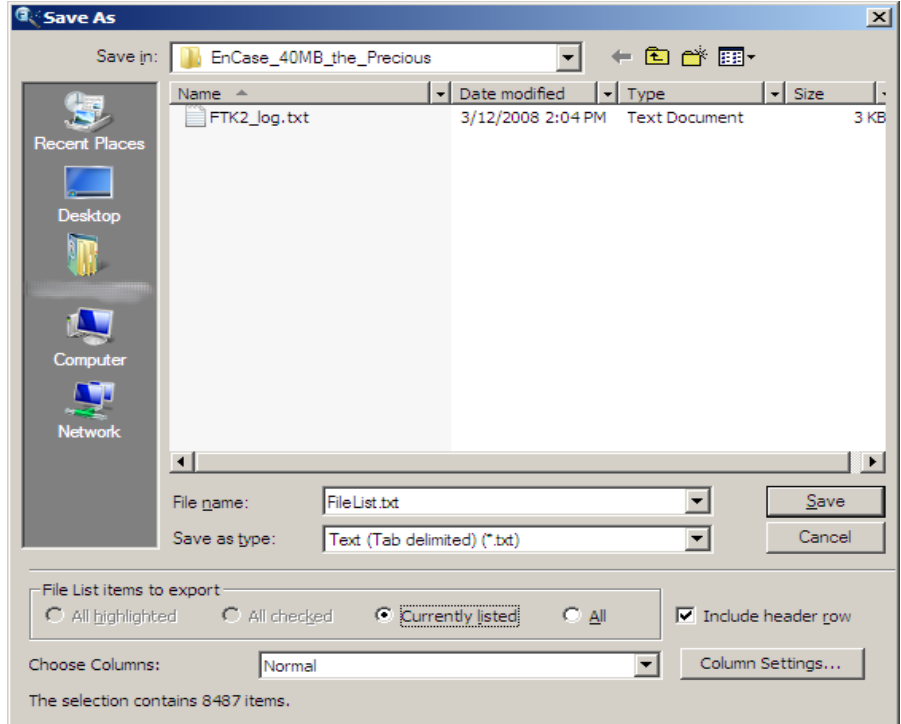
<b>Option</b>	<b>Description</b>
Export	Exports selected files and associated evidence to a designated folder.
Export to Image	Exports one or more files as AD1 files to a storage destination.
Export File List Info	Exports selected file information to files formatted as the Column List in <b>.csv</b> , <b>.tsv</b> , and <b>.txt</b> formats.
Export Word List	Exports the index as a text file from which a dictionary for PRTK can be created.
Report	Opens the Report Options window for creating a case report.
Volatile Data Report	Opens a report of the Volatile Data that has been collected in this case.
Close	Closes the FTK Window and returns to the Case Management window.
Exit	Closes both the FTK and Case Management windows.

### EXPORT FILE LIST INFO

The Export File List Info dialog, as displayed in the following figure, provides the copy special options with the ability to save the information to a file. This file can be saved in **.tsv**, **.txt**, or **.csv** format. Text files of this sort are **.txt** files that displayed in a text editor program like Notepad. Files saved in **.tsv** or **.csv** display in the default spreadsheet program.



Figure 6-6 Export File List Info Dialog



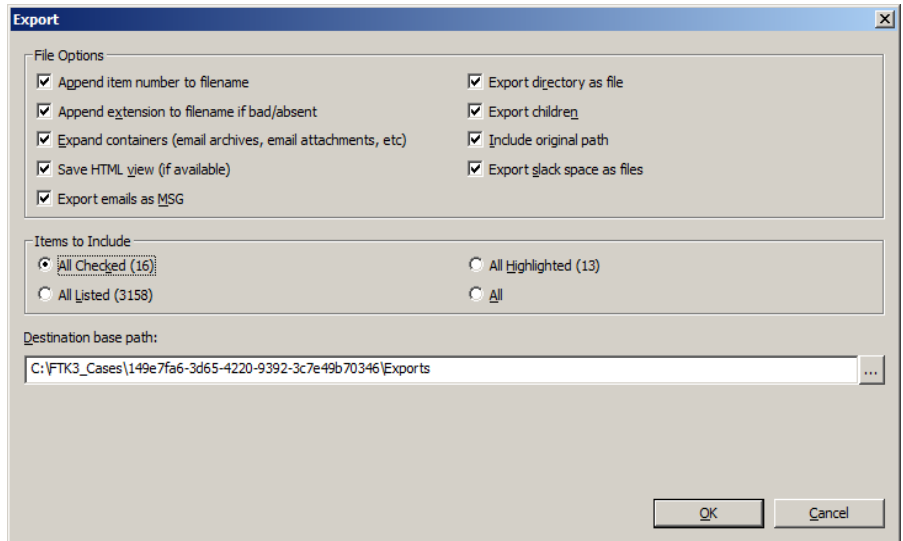
To export a list containing column headings and other information from the File List perform the following steps:

1. Select *File > Export File List Info*, or click *Export File List* on the File List pane, or right-click on a file in the File List pane and select *Export File List Info*.
2. Select the File List Items to Export. Choose from *All Highlighted*, *All Checked*, *All Listed*, or *All*,
3. Choose whether to include a header row in the exported file.
4. From the *Choose Columns* dropdown, select the column template to use.  
Click *Column Settings* to customize a column template to use for this export.
5. Specify the filename for the exported information.
6. Choose a file type for the exported file.
7. Browse to and select the destination folder for the exported file.
8. Click *Save*.

## EXPORTING FILES

FTK allows the export of files found in the investigation. Files can be exported for additional processing or for distribution to other parties. For example, encrypted files can be exported to decrypt using Password Recovery Toolkit (PRTK). Similarly, registry files can be exported to analyze them using the Registry Viewer. (Neither PRTK nor Registry Viewer can read files within a drive image.) The following figure represents the Export dialog.

Figure 6-7 Export Dialog



To export files do the following:

1. Click *File > Export*, or right click on a file in the File List pane and choose *Export*.
2. Select the export options you want from the Export dialog based on the table below.

**TABLE 6-5** Export Files Dialog Options

Option	Description
Append Item number to Filename	Appends the FTK unique File ID to a filename.
Append extension to filename if bad/absent	Adds the extension to a filename if it is bad or missing, based on the file's header information.
Expand containers (email archives, email attachments, etc.)	Expands container-type files and exports their contents.

**TABLE 6-5 Export Files Dialog Options**

---

<b>Option</b>	<b>Description</b>
Save HTML view (if available)	If a file can be exported and saved in HTML format, it will be done.
Export emails as MSG	Exports emails to MSG format for broader compatibility.
Export directory as file	Creates a file containing the binary data of the directory being exported.
Export children	Exports all child files of a parent folder.
Include original path	Includes the full path from the root to the file; maintains folder structure for exported files.
Export slack space as files	Exports slack space from files and saves it as files for easier viewing.

3. Select the Items to Include based on the following table:

**TABLE 6-6 Export Files Selection Options**

---

<b>Target Item</b>	<b>Description</b>
All Checked	All items checked in all file lists. You can check files in multiple lists.
All Listed	All items in the current file list.
All Highlighted	All items highlighted in the current file list. Items remain highlighted only as long as the same tab is displayed.
All	All items in the case.

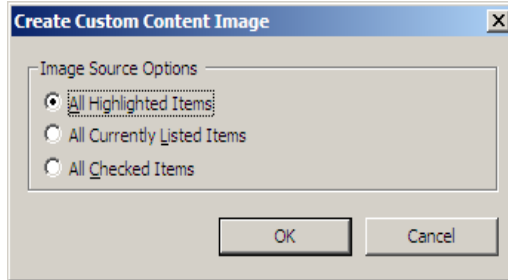
Each item displays its filename and path.

4. In the Destination Path field, browse to and select the export file location. The default path is `[Drive]:\case_folder\Report\Export\`.
5. Click *OK* to begin the export.

## **EXPORTING TO IMAGE**

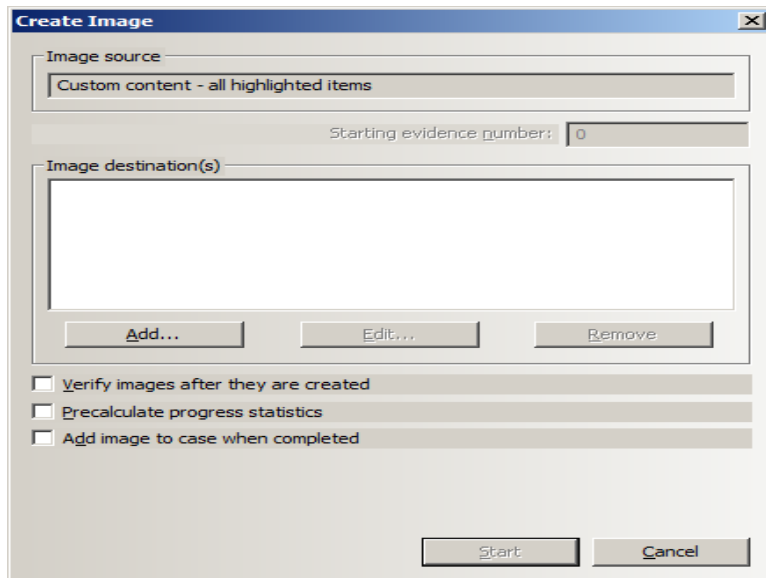
You can export selected files to an AccessData Custom Content Image (.AD1). To do so, follow these steps:

1. Click *File > Export to Image*.



2. Select the Image Source for your AD1 file.

3. Click *OK*.



4. In the Create Image Dialog, click *Add*. This brings up the Select Image Destination dialog.

5. Verify the Image Source.

6. Specify the Image destination. This opens a new dialog box, Select Image Destination.

6a. Specify Evidence Item information:

**Select Image Destination**

**Evidence Item Info**

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

**Destination**

Image Destination Type:

Image Destination

Relative to:  This machine  Remote source machine

Folder:

Username (DOMAIN\User):

Password:

Image Filename (Excluding Extension)

Image Fragment Size (MB)   
For Raw and E01 formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest)

6b. Case Number

6c. Evidence Number

6d. Unique Description

6e. Examiner

6f. Notes

6g. Select the Image Destination Type. Default is AD1.

6h. Specify the Image Destination.

6i. Image can be saved locally or remotely.

6j. Specify the path for the image on the target machine.

- 6k. If the file will be saved remotely, specify the Domain and Username required to access that machine.
- 6l. Specify the password of the user on the remote machine
- 6m. Specify a filename for the image, but do not include an extension.
- 6n. Specify the Image Fragment Size in MB. RAW and E01 format file types can be saved in a single segment by specifying 0 in the *Image Fragment Size* box.
- 6o. Specify the compression level to use.
- 6p. Click *OK* to close this dialog and return to the Create Image dialog.
7. Choose whether to *Verify Images after they are created*.
8. Choose whether to *Precalculate progress statistics*. This gives you an estimate of the progress of the task as it is running.
9. Choose whether to *Add image to case when completed*.
10. Specify the *Time Zone* of the evidence.
11. When you are satisfied that the information you have provided is accurate, click *OK*.
12. Select the processing options you wantSpecify the *Time Zone* of the evidene.
13. Click *Start* to begin the image creation, or click *Cancel* to return to the main FTK 3.0 user interface window.

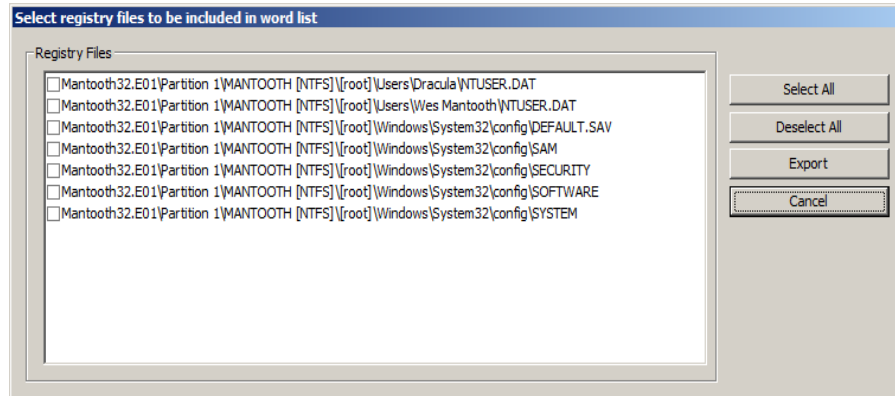
## EXPORTING THE WORD LIST

The contents of the case index can be exported to use as the basis for a custom dictionary to aid in the password recovery process.

**Important:** You must have indexed the case to export the word list. If you have not done so, click *Evidence > Additional Analysis*. In the Additional Analysis dialog, under Search Indexes, mark the *dtSearch Index* check box, then click *OK*.

When the index is complete, you can export the word list by doing the following:

1. Select *File > Export Word List*.



2. Select the Registry Keys to export to the word list.
3. Click *Export*.
4. Select the filename and location for the exported word list. Click *Browse Folders* to select the folder location for the wordlist file.  
The default filename is **Ftk2WordList.txt**. If you intend to use the wordlist as the basis for a custom dictionary in DNA or PR1TK, it is a good idea to name the wordlist by the casename. For example, **ADEE3.0\_PreciousWordList.txt**
5. Click *Save*.

## EDIT MENU OPTIONS

**TABLE 6-7 FTK 3.0 Edit Menu**

Option	Description
Copy Special	Duplicates information about the object copied as well as the object itself, and places the copy in the clipboard.

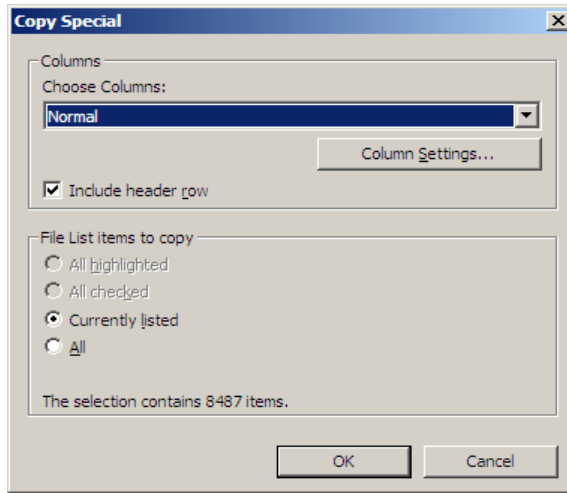
## COPYING INFORMATION FROM FTK

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

To copy file information perform the following steps:

1. In the File List on any tab, select the files that you want to copy information about.

2. Select *Edit > Copy Special*, click the *Copy Special* button on the file list pane, or right-click the file in the file list and click *Copy Special*.



3. In the Copy Special dialog, select from the options based on the following table:

**TABLE 6-8 Copy Special Dialog Options**

Item	Description
Choose Columns	From the drop-down, select the column template to use, or click <i>Column Settings</i> to create a custom template.
Include header row	Mark box to include a header row that uses the column headings you selected. Leave box empty to export the data with no header row.
All Highlighted	All items highlighted in the current file list. <b>Note:</b> Items remain highlighted only as long as the same tab is displayed.
All Checked	All items checked in all file lists. You can check files in multiple lists. Checked items remain checked until you uncheck them.
Currently Listed	All items in the current file list.
All	All items in the case. <b>Note:</b> Selecting All Items can create a very large TSV or .CSV file, and can exceed the 10,000 item capacity of the clipboard.

4. In the Choose Columns drop-down list, select the column template that contains the file information that you want to copy.
5. To define a new column settings template click *Column Settings* to open the Column Settings manager.
  - 5a. Create the column settings template you need.



5b. Click *Save* to save the changes.

5c. Close the Column Settings manager.

5d. Select the new columns setting template from the drop-down list.

For more information about Column Settings, see “Creating and Modifying Column Settings” on page 268.

6. Click *OK* to initiate the Copy Special task.

## VIEW MENU OPTIONS

**TABLE 6-9 FTK 3.0 View Menu**

Option	Description
Refresh	Reloads the current view.
Filter Bar	Inserts the filter toolbar into the current tab. These features are available also from the Filter menu.
Timezone Display	Opens the Time Zone Display dialog.
Thumbnail Size	Selects the size of the thumbnails displayed from the Graphics tab. Select from: <ul style="list-style-type: none"> <li>• Large-default</li> <li>• Small</li> <li>• Medium</li> <li>• Tiny</li> </ul>
Tab Layout	Manages tab settings: the user can lock an existing setting, add and remove settings, save settings one tab at a time or all at once. The user can also restore previous settings, or reset them to the default settings. These options are in the following list: <ul style="list-style-type: none"> <li>• Lock</li> <li>• Save All Layouts</li> <li>• Add</li> <li>• Restore</li> <li>• Remove</li> <li>• Reset to Default</li> <li>• Save</li> </ul>
File List Columns	Specifies how to treat the current File List Options are: <ul style="list-style-type: none"> <li>• Save As Default</li> <li>• Reset to Factory Default</li> <li>• SaveAll as Default</li> <li>• Reset All To Factory Default</li> </ul>
File Content Tabs Switching	Specifies the behavior of file content when a different tab is selected. Options are: <ul style="list-style-type: none"> <li>• Auto</li> <li>• Manual</li> </ul>
Explore Tree	Displays the Explore Tree in the upper-left pane.
Graphics Tree	Displays the Graphics Tree in the upper-left pane.
Overview Tree	Displays the Overview Tree in the upper-left pane.
Email Tree	Displays the Email Tree in the upper-left pane.
Bookmark Tree	Displays the Bookmark pane in the upper-left pane.
Indexed Searches	Displays the Index Search Results pane in the upper-left pane.
Live Searches	Displays the Live Search Results pane in the upper-left pane.
Bookmark Information	Adds the Bookmark Information pane into the current tab.

**TABLE 6-9 FTK 3.0 View Menu**

---

<b>Option</b>	<b>Description</b>
File List	Adds the File List pane into the current tab.
File Content	Adds the File Content pane into the current tab.
Email Attachments	Displays the attachments to email object found in the case. Available only in the Email and Overview tabs.
Properties	Inserts the Object Properties pane into the current tab view.
Hex Value Interpreter	Displays a pane that provides an interpretation of Hex values selected from the Hex View pane.
Thumbnails	Displays a pane containing thumbnails of all graphics found in the case.
Progress Window	Opens the Progress dialog, from which you can monitor tasks and/or cancel them.

The tree and search views are exclusive settings, meaning that you can use only one tree view per tab pane, and only one search view per tab pane.

## EVIDENCE MENU OPTIONS

**TABLE 6-10 FTK 3.0 Evidence Menu**

---

<b>Option</b>	<b>Description</b>
Add/Remove	Opens the Manage Evidence dialog, used to add and remove evidence.
Add Remote Data	Opens the Add Remote Data dialog from which you can remotely access volatile, memory, and/pr drive data and add it to the case.
Import Memory Dump	Opens the Import Memory Dump File dialog which allows you to select memory dumps from other case files or remote data acquisitions, and import them into the current case.
Additional Analysis	Opens the Additional Analysis dialog with many of the same processing options available when the evidence was added. Allows the user to reprocess using options not selected the previous time.

## FILTER MENU OPTIONS

**TABLE 6-11 FTK 3.0 Filter Menu**

---

<b>Option</b>	<b>Description</b>
New	Opens the Filter Definition dialog to define a filter. This feature is also available from the Filter toolbar.
Duplicate	Duplicates a selected filter. This feature is also available from the Filter toolbar.
Delete	Deletes a selected filter. This feature is also available from the Filter toolbar.
On	Applies the global filter to the application. The File List changes color to indicate that the filter is applied. This feature is also available from the Filter toolbar.
Import	Opens the system file manager allowing the user to import a pre-existing filter. This feature is also available from the Filter toolbar.
Export	Opens the System File Manager allowing the user to save a filter. This feature is also available from the Filter toolbar.  <b>Note:</b> The name of the filter cannot have any special or invalid characters or the export will not work.
Tab Filter	Allows the selection of a filter to apply in the current tab.

## TOOLS MENU OTIONS

**TABLE 6-12 FTK 3.0 Tools Menu**

Option	Description
KFF	Known File Filter (KFF) sets and groups can be managed, archived, and cleared. The following menu option is available: <ul style="list-style-type: none"><li>• Manage: Opens the KFF Admin dialog.</li></ul>
Fuzzy Hash	Options are: <ul style="list-style-type: none"><li>• Find Similar Files</li><li>• Manage Fuzzy Hash Library</li></ul>
Decrypt Files	Decrypts EFS and Microsoft Office files passwords that match those added to the password list.
Credant Decryption	Opens the tools for Credant* decryption. Credant is a third party encryption tool that encrypts files, folders, partitions, or entire disks.
Verify Image Integrity	Generates hash values of the disk image file for comparison.
Disk Viewer	Opens a viewer that allows you to see and search evidence items.
Other Applications	Opens other AccessData tools to complement the investigational analysis: <ul style="list-style-type: none"><li>• Imager</li><li>• LicenseManager</li><li>• PRTK</li><li>• Language Selector</li><li>• Registry Viewer</li></ul>
Unmount Agent	Allows you to unmount an agent from a remote machine
Final Carve Processing	
Execute SQL	Provides the ability to execute an SQL script from within FTK.
Launch 'oradjuster.exe'	Launches the OrAdjuster utility to optimize memory use for Oracle.

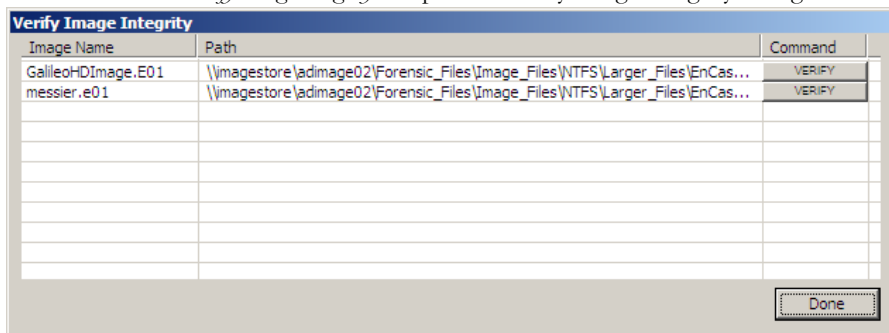
### VERIFYING DRIVE IMAGE INTEGRITY

A drive image can be altered or corrupted due to bad media, bad connectivity during image creation, or by deliberate tampering. This feature works with file types that store the hash within the drive image itself, such as EnCase and SMART images.

To verify an evidence image's integrity, FTK generates a hash of the current file and allows you to compare that to the hash of the originally acquired drive image.

To verify that a drive image has not changed, do the following steps:

1. Select *Tools > Verify Image Integrity* to open the Verify Image Integrity dialog.

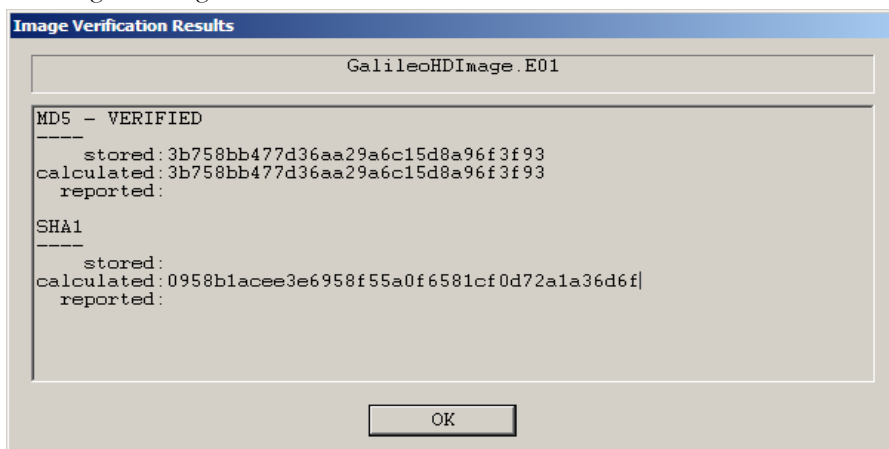


In case the image file does not contain a stored hash, FTK can calculate one. The Verify Image Integrity dialog provides the following information:

**TABLE 6-13 Verify Image Integrity**

Column	Description
Image Name	Displays the filename of the evidence image to be verified.
Path	Displays the path to the location of the evidence image file.
Command	Click <i>Verify</i> to begin hashing the evidence image file.

2. Click either *Calculate*, or *Verify* according to what displays in the Command column, to begin hashing the evidence file.



The Progress Dialog appears and displays the status of the verification. If the image file has a stored hash, when the verification is complete, the dialog shows and compares

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

## HELP MENU OPTIONS

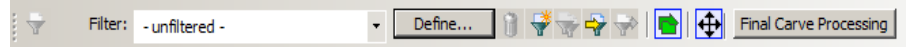
**TABLE 6-14 FTK3.0 Help Menu**

Option	Description
User Guide	Provides a link to the FTK 3.0 User Guide.
About	Provides information about the current FTK release.

## TOOLBAR COMPONENTS






The FTK interface provides a toolbar for applying QuickPicks and filters to the case. The following section lists the toolbars and their components.

*Figure 6-8 FTK Filter Toolbar*




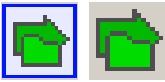

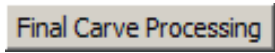


The following table shows the available components of the toolbar.

**TABLE 6-15 Toolbar Components**

Component	Description
	Turns the selected filter on or off. Filtered data is shown in a colored pane to indicate that it is filtered.
	Applies the selected filter. A drop-down menu lists defined filters.
	Opens the filter definition dialogue to define the rules of the current filter, or allows the creation of a new one.
	Deletes the selected filter
	Creates a new filter

**TABLE 6-15** Toolbar Components

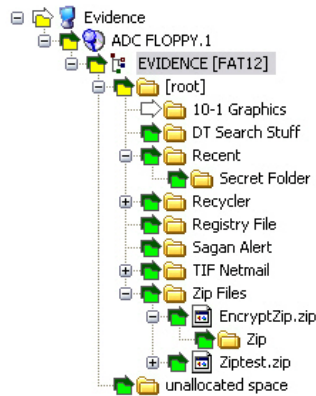
Component	Description
	Creates a copy of the selected filter
	Imports the selected filter from an XML file
	Exports the selected filter to an XML file
	Turns Quick Picks On or Off. The white background and blue border indicates QuickPicks is On. The gray background and lack of a border indicates QuickPicks is Off.
	Locks the movable panes in the application, making them immovable. When the lock is applied, the blue box turns grey.
	Final Carve Processing processes the data that you have selected and saved to files, and adds them to the case.

## QUICKPICKS FILTER

The QuickPicks feature is a type of filter that allows the selection of multiple folders and files in order to focus analysis on specific content. The following figure represents the Explore Evidence Items tree with a partially selected set of folders and sub-folders using the QuickPicks feature.







Figure 6-9 QuickPicks Filter Folder Selection



The QuickPicks filter simultaneously displays open and closed descendent containers of all selected tree branches in the File List at once. The colors of the compound icons indicate whether descendents are selected.

The icons are a combination of an arrow, representing the current tree level, and a folder, representing any descendent.

TABLE 6-16 QuickPicks Icons

Icon	Description
	A dark green arrow behind a bright green folder means all descendents are selected.
	a dark green arrow behind a yellow folder means that although the folder itself is not selected, some of its descendents are selected.
	a white arrow with no folder means neither that folder, nor any of its descendents is selected.
	A white arrow behind a bright green folder means tht all descendents are selected, but the folder is not.

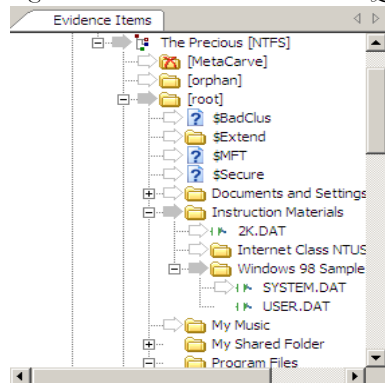
In the illustration above, the decendent folder 10-1 Graphics is unselected. Its arrow icon is white.

The folder icons for the folders above item “10-1 Graphics” are yellow to indicate that not all descendent folders are selected. The top-most level item “Evidence” has a white arrow icon, indicating that it is not selected, and a yellow folder icon, indicating that some of its descendent folders are not selected.

The folder icon for “DT Search Stuff” is green, indicating that all contents of the folder have been selected.

When QuickPicks is turned off, the tree view displays as shown in the figure below:

*Figure 6-10 Evidence Items List with QuickPicks Off*



## FILE LIST PANE

The File List pane lists the files available in the current tabbed view. In this pane the user can choose which columns to display, as well as the order of those columns, create bookmarks, create labels, copy or export file lists. The File List pane is displayed by default in all default tabs.










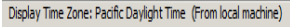
When viewing data in the File List, use the type-down control feature to locate specific files. When the list is sorted by name, select an item in the list, then type the first letter of the desired file. FTK will move down the list to the first file beginning with that letter. The more letters you type, the closer the match will be to the file you are looking for.

For more information, see “Customizing File List Columns” on page 268.

## FILE LIST TOOLBAR




The File List pane includes a toolbar containing these buttons for managing the File List:

**TABLE 6-17 File List Toolbar**

Component	Description
	Checks all of the files in the current list.
	Unchecks all of the files in the current list.
	Unchecks all of the files in the current case.
	Opens Create New Bookmark dialog box.
	Opens Manage Labels dialog box.
	Opens Copy Special dialog box.
	Opens the Export File List, allowing the user to save selected files to another folder.
	Opens the Column Settings dialog box.
	<p>Sets the displayed columns to a specific set from the following list</p> <ul style="list-style-type: none"> <li>• Normal (Default)</li> <li>• Email</li> <li>• File Listing</li> <li>• Normal (default)</li> <li>• Reports: File Path Section</li> <li>• Reports: Standard</li> </ul>
	Displays the selected time zone from the local machine.

**TABLE 6-17 File List Toolbar**

---

<b>Component</b>	<b>Description</b>
	Leave query running when switching tabs (May affect performance of other tabs).
	Cancel retrieving row data. This is not a pause button. To retrieve row data after clicking <i>Cancel</i> , you must begin again. There is no way to pause and restart the retrieval of row data.
	Indicates processing activity.

## USING TABS

The FTK2.x user interface is organized into tabbed pages to make organization and navigation easier. For a detailed description of the FTK 3 tabbed pages, see “Chapter 8 Using Tabs to Explore & Refine Evidence” on page 129.

# *Chapter 7 Adding and Processing Remote Live Evidence*

You can add more types of evidence to an FTK case than you could in the past. FTK can utilize various types of static images, such as .001, .E01, .S01, and .AD1. In addition, FTK can now acquire remote live evidence from network computers. Adding and using remote evidence is covered in this chapter. For more information regarding adding static evidence to a case, see “Chapter 6 Adding and Processing Static Evidence” on page 87.

## **ACQUIRING AND PRESERVING REMOTE EVIDENCE**

Using FTK Imager, you can create a static forensic image of evidence from a “live” machine when you must. It is important to be aware of the data compromises you will face in such a situation, such as file stamps being inaccurate, or data changing while the image is being collected; however sometimes there is no other choice. One such example is when the suspect drive is encrypted and you must acquire the image in-place while the machine is running. Another example is when imaging a RAID array; it must be live to be properly acquired.

FTK 3 can now acquire live evidence remotely from Agent machines on the network. You can specify by IP address which machine to acquire data from, and you can choose to acquire data from Physical Drives, Logical Drives, or Memory (RAM) for Analysis. You can acquire remote data from only one machine at a time.

The installation of this feature is discussed in-depth in the installation chapter. The use of it is explained here. Types of Remote Information

## FTK ROLE REQUIREMENTS

To use Remote Data Acquisition in FTK 3, meet the following requirements:

- FTK 3 must be installed using a current license.
- You must have the Application Administrator or Case Administrator role to be able to access the Add Remote Evidence dialog.
- You must have Administrator rights on the remote machine you wish to acquire data from.
- You must have an FTK Agent. on the target computer.

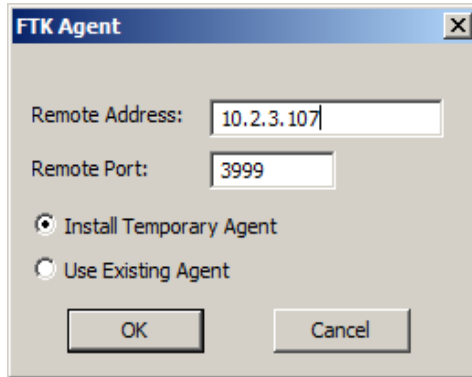
## ACQUIRING DATA REMOTELY

Remote Data Acquisition is accomplished through a new feature called Remote Disk Management System (RDMS). RDMS gives examiners the ability to acquire a forensic image of the physical or logical drive(s), acquire a non-proprietary image of memory , and forensically mount the physical devices or logical volumes on the examiners machine from a single live system. SSL is used to ensure communication between the agent and examiner is protected using either a self signed certificate or one signed by a Certificate Authority (CA).

Because FTK's ability to acquire data remotely is so tightly integrated with RDMS, the two are covered here together. Thus the differentiation between the two features may be vague. For a more specific discussion of the RDMS, see the RDMS Quick Start Guide.

To acquire remote live data in FTK, you can use an existing Agent, such as from FTK, on the remote machine. If no Agent exists on the remote machine, a Temporary Agent can be “pushed” to the remote machine, or you can manually install an agent using self-signed certificates, or certificates signed by a Certificate Authority (CA). To push a Temporary Agent, do the following:

1. From the Case UI, click *Evidence > Add Remote Data*.



2. Enter the IP Address of the Remote Machine.
3. Ensure that a port is designated. The default port is 3999. Use this port unless it is already in use and produces an error or conflict. If there is a conflict, select another port that is not in use.
4. Choose *Install a Temporary Agent*,
5. Click *OK*.

## PROVIDE CREDENTIALS

When *Install Temporary Agent* is selected, the *Credentials* dialog opens. The *Credentials* dialog stores a list of all the sets of credentials to try when connecting to a remote machine.

1. In the Credentials dialog, enter the credentials required to authenticate to the remote machine:



- 1a. Enter the Domain name, if the network uses a Domain Controller. If installing in a workgroup, or non-domain network, enter the IP address of the workgroup machine, or the local host name using the syntax: *[machinename\username]*.
- 1b. Enter the Username, that is, the name assigned to the user account having Admin rights on the remote computer.
- 1c. Password of the user account name given above.
- 1d. Confirm the password.
- 1e. Click *Add* to add this set of credentials to the list in the box.
- 1f. Click *Add* to create additional sets of credentials.

**OR**

Click *Remove* to remove a set of credentials from the list.

- 1g. Click *OK*.

**Note:** On XP systems, Simple File Sharing must be turned off for Temporary Agent deployment.

2. In the Remote Data dialog, select which type(s) of data to acquire. There are three options, each has its own dialog with options and requirements. Options are:



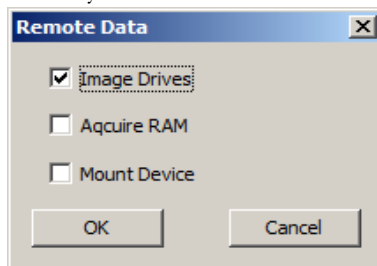
- **Image Drives:** Creates an E01 image of the selected drive. You are given a list of the drives on the remote system. This list includes the Drive, all Partitions, and other devices, such as memory cards that are connected. There is no drive preview available. Output is to .E01, using only default options.

**Note:** This options consumes a large amount of bandwidth, and is slow.

- **Acquire RAM:** Allows you to acquire the memory contents from the target machine. RAM data is viewable from the Volatile tab in FTK. You will be prompted for a filename to save the RAM data to. You specify the base name and FTK provides the extension.

**Note:** Mark Page File to also acquire the data in page files on the remote computer. This is the only way you will see the contents of the page file.

- **Mount device:** Mounts and connects to a device on the remote computer. You can then map to that device, and browse the contents in Windows Explorer. You are given a list of remote devices to map to. For the selected item on the left, the available information about that device is displayed on the right. While this is live data, it reads from the disk, not from the cache. This means that if there is activity on the screen while you are viewing the mounted device data, you will not see it.



- 2a. Make your selections from any or all of the Remote Data options during your session.
- 2b. Click *OK*
3. The Remote Data acquisition job begins and the Data Processing Status window opens. Acquire Remote Data jobs are displayed under Other Jobs.

Once you disconnect from the remote system, the Agent stays “alive” for approximately five minutes before self-deleting. In addition, if you do not disconnect from the remote system, the Agent will complete its assigned tasks and when there are no running tasks, it will also self-delete after about five minutes. To avoid waiting for the FTKEgent to expire, kill the FTKEgent in Task Manager on the Target machine.

Once disconnected, you must push the agent again to establish a new connection and acquire additional data, or follow the directions that follow to create a Manual

Deployment with either a self-signed certificate, or one from a Certificate Authority (CA).

## REMOTE DISK MANAGEMENT SYSTEM (RDMS) ADDITIONAL INFORMATION

In FTK 3.0 AccessData offers a new feature called Remote Disk Management System (RDMS). It gives examiners the ability to acquire a forensic image of the physical or logical drive(s), acquire a non-proprietary image of memory, and forensically mount the physical devices or logical volumes on the examiners machine from a single live system. SSL is used to ensure communication between the agent and examiner is protected using either a self signed certificate or one signed by a Certificate Authority (CA).

### RDMS REQUIREMENTS FOR MANUAL DEPLOYMENT

- FTK 3 installed with a license
- Either a self signed certificate or a CA signed certificate if you want to use the manual deployment on a thumb drive.
- FTK agent
- Admin privileges on the target node
- Network connectivity to the target node

### UTILIZING THE AGENT

There are two different agent deployment methods:

- **Auto Deployment:** Using the one time agent where FTK deploys the agent with a onetime certificate. This method was discussed in the previous Add Remote Data discussion.
- **Manual Deployment:** Using the agent binary (FTKagent.exe) and pre-created certificate running on the target machine.

Assuming FTK 3 is installed and you want be able to leverage both the manual and automatic agent deployment methods, complete the following:

**Note:** You only need to create one cert of keys

1. Create the certificates. The **certman** utility, which ships with FTK 3, can create a self-signed certificate or the certificates needed for an existing self signed certificate.

2. Create a new folder on your examiner machine for example **C:\Agent** (it can be called anything).
3. Copy the **certman** utility from **C:\Program Files\AccessData\Forensic Toolkit\3.0\bin** to the **C:\Agent**
4. Copy the **FTKagent.exe** from **C:\Program Files\AccessData\Forensic Toolkit\3.0\bin** to the **C:\Agent**
5. Create the certificates to be used during manual deployment.

To create a self signed certificate, do the following:

1. Open a command box and type the following command line:  
**Certman -n [name of issuer] [base name of cert]**

Example:

```
Certman -n DellComputer.domainname.com InvestigatorCert
```

Which generates the following certificates:

```
InvestigatorCert.crt <public>
```

```
InvestigatorCert.p12 <private>
```



# *Chapter 8 Using Tabs to Explore & Refine Evidence*

Changing tabs helps the investigation team to explore and refine evidence. The following sections look at each of the tabs in more detail.

## **USING TABS TO EXPLORE AND REFINE EVIDENCE**

The FTK interface contains nine main tabs and there may be other optional tabs if their correlating product is installed, each with a specific focus. Most tabs also contain a common toolbar and file list with customizable columns.

Changing tabs helps the investigator to explore and refine evidence. The following lists the nine default tabs of FTK.

**TABLE 8-1 FTK UI Main Tabs**

---

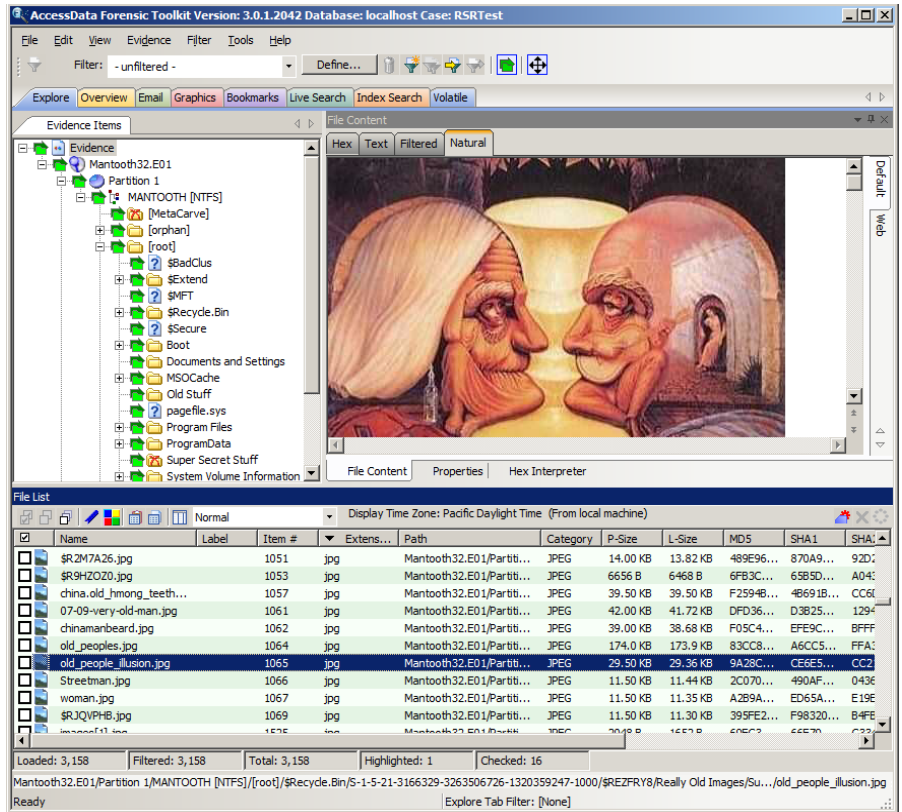
• Explore Tab	• Live Search Tab
• Overview Tab	• Index Search Tab
• Email Tab	• Volatile Tab
• Graphics Tab	• Sawmill Tab (When installed)
• Bookmarks Tab	• Mobile Phone Examiner (When installed)

The following pages contain more details for each tab. You can also create additional, customized tabs to meet your needs.

## EXPLORE TAB

The Explore tab displays all the contents of the case evidence files and drives as the original user would have seen them. The following figure displays the FTK window with the Explore Tab selected showing the path from the Evidence to the root (boot partition) in the Evidence Items tree.





The Explore tab contains the following panes:

**TABLE 8-2 Explore Tab Panes**

Pane	Description
Explorer Tree Pane	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 drive, as well as any file, folder, or image of a drive.
File List	Displays case files and pertinent information about files, such as filename, file path, file type and many more properties as defined in the current filter.

**Note:** The File List loads more quickly now than in previous versions.



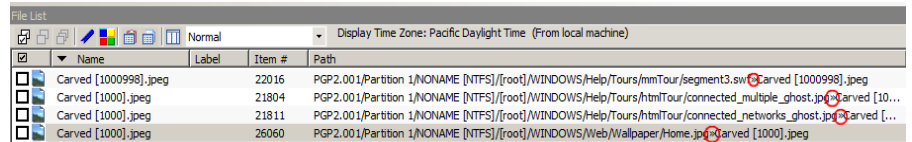
**TABLE 8-2 Explore Tab Panes**

Pane	Description
Viewer Pane	<p>Displays the contents of the currently selected file from the File List. The Viewer toolbar allows the choice of different view formats. Choices are:</p> <ul style="list-style-type: none"> <li>• File Content Tab                             <ul style="list-style-type: none"> <li>The File content tab has a Default tab and a Web tab for each of the following tabbed views:                                     <ul style="list-style-type: none"> <li>•HexTab</li> <li>•Text Tab</li> <li>•Filtered Tab</li> <li>•Natural Tab</li> </ul> </li> </ul> </li> <li>• Properties Tab</li> <li>• Hex Interpreter Tab</li> </ul>

**Note:** The Find on Disk feature (in File List view, right-click an item) won't find anything under 512 B physical size. Files smaller than 1500 bytes may reside in the MFT and do not have a start cluster. Find on disk depends on the start cluster information to work.

**Note:** In the File List view of any tab, a much-greater-than symbol (>>) now denotes that the path is not an actual path, but that the file came from another file or source, such as a zipped, compressed, or linked (OLE) file, or that it was carved. This is displayed in the figure below:

*Figure 8-2 File List View Showing Virtual Path to Files From Another Source*



## VIEWER PANE

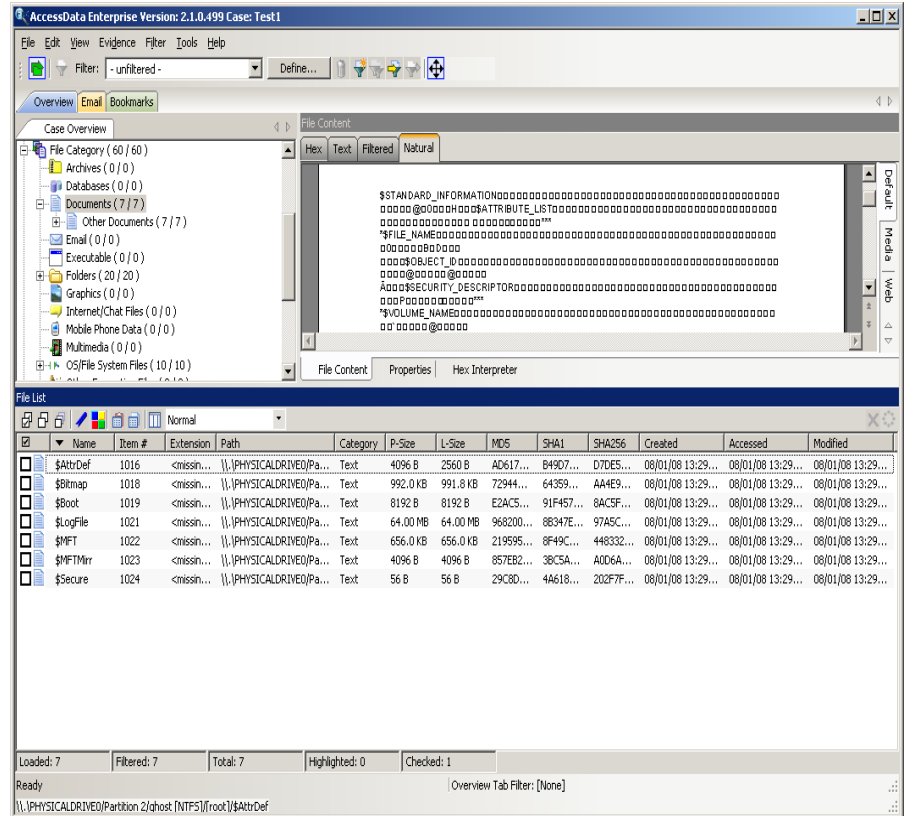
The Viewer pane now contains the File Content, Properties, and Hex Interpreter tabs, at the bottom of the pane. The File Content, Properties, and Hex Interpreter tabs default to the bottom left of the File Content pane in any program tab where it is used.

The three tabs can be re-ordered by clicking on a tab and dragging-and-dropping it to the position in the linear list where you want it. Click any of these tabs to switch between them. The information displayed applies to the currently selected file in the File List pane.

## PROPERTIES TAB

The Properties tab displays information about a selected file. The following figure displays the information contained in the Properties tab. This information corresponds to the file selected in the File List pane.

Figure 8-3 Properties Pane



The following table highlights the components of the Properties pane:

**TABLE 8-3 Properties Pane Components**

<b>Option</b>	<b>Description</b>
Name	The filename of the selected file.
Item Number	The arbitrary number assigned to the item by FTK 3.0 during case processing.
File Type	The type of selected file, such as an HTML file or a Microsoft Word 98 document.
Path	The file header is used to identify each item's file type. The path from the evidence source down to the selected file.
General Info	General information about the selected file: <b>File Size:</b> Lists the size attributes of the selected file as follows: <ul style="list-style-type: none"> <li>• Physical size of the file, including file slack</li> <li>• Logical size of the file, excluding file slack.</li> </ul> <b>File Dates:</b> Lists the Dates and Times of the following activities for that file on the imaged source system: <ul style="list-style-type: none"> <li>• Created</li> <li>• Last accessed</li> <li>• Last modified</li> </ul> <b>Note:</b> All dates are listed in UTC time.
File Attributes	The attributes of the file: <b>General:</b> <ul style="list-style-type: none"> <li>• <b>Actual File:</b> True if an actual file; False if derived from an actual file.</li> <li>• <b>From Recycle Bin:</b> True if the file was found in the Recycle Bin. False otherwise.</li> <li>• <b>Start Cluster:</b> Start cluster of the file on the disk</li> <li>• <b>Compressed:</b> True if compressed. False otherwise.</li> <li>• <b>Original Name:</b> Path and filename of the original file.</li> <li>• <b>Start Sector:</b> Start sector of the file on the disk.</li> <li>• <b>File has been examined for slack:</b> True if the file has been examined for slack. False otherwise.</li> <li>• <b>File has been examined for carving:</b> True if the file has been examined for carving. False otherwise.</li> </ul>

**TABLE 8-3 Properties Pane Components**

Option	Description
	<p data-bbox="686 326 851 352"><b>DOS Attributes:</b></p> <ul data-bbox="708 369 1329 647" style="list-style-type: none"> <li data-bbox="708 369 1329 421">• <b>Hidden:</b> True if Hidden attribute was set on the file. False otherwise.</li> <li data-bbox="708 439 1253 465">• <b>System:</b> True if this is a DOS system file. False otherwise.</li> <li data-bbox="708 482 1019 508">• <b>Read Only:</b> True or False value</li> <li data-bbox="708 526 1290 578">• <b>Archive:</b> True if Read Only attribute was set on the file. False otherwise.</li> <li data-bbox="708 595 1315 647">• <b>8.3 Name:</b> Name of the file in the <b>DOS 8.3</b> naming convention, such as [<i>filename.ext</i>]</li> </ul> <p data-bbox="686 664 1193 716"><b>Verification Hashes:</b> True if Verification hashes exist. False otherwise.</p> <p data-bbox="686 734 879 760"><b>NTFS Information</b></p> <ul data-bbox="708 777 1329 1359" style="list-style-type: none"> <li data-bbox="708 777 1300 829">• <b>NTFS Record Number:</b> The number of the file in the NTFS MFT record.</li> <li data-bbox="708 847 1222 873">• <b>Record Date:</b> UTC time and date record was created.</li> <li data-bbox="708 890 1329 1003">• <b>Resident:</b> True if the item was Resident, meaning it was stored in the MFT and the entire file fit in the available space. False otherwise. (If false, the file would be stored FAT fashion, and its record would be in the \$I30 file in the folder where it was saved.)</li> <li data-bbox="708 1020 982 1046">• <b>Offline:</b> True or False value</li> <li data-bbox="708 1064 976 1090">• <b>Sparse:</b> True or False value</li> <li data-bbox="708 1107 1300 1159">• <b>Temporary:</b> True if the item was a temporary file, False otherwise.</li> <li data-bbox="708 1177 1290 1229">• <b>Owner SID:</b> The Windows-assigned security identifier of the owner of the object.</li> <li data-bbox="708 1246 1329 1298">• <b>Owner Name:</b> Name of the owner of that file on the source system.</li> <li data-bbox="708 1315 1290 1367">• <b>Group SID:</b> The Windows-assigned security identifier of the group that the owner of the object belongs to.</li> </ul>
File Content Info	<p data-bbox="686 1376 1286 1402">The content information and verification information of the file:</p> <ul data-bbox="708 1420 1329 1519" style="list-style-type: none"> <li data-bbox="708 1420 1268 1446">• <b>MD5 Hash:</b> The MD5 (16 bytes) hash of the file (default).</li> <li data-bbox="708 1463 1296 1489">• <b>SHA-1 Hash:</b> The SHA-1 (20) bytes hash of the file (default).</li> <li data-bbox="708 1506 1329 1519">• <b>SHA-256 Hash:</b> the SHA-256 (32bytes) hash of the file (default).</li> </ul>

**TABLE 8-3 Properties Pane Components**

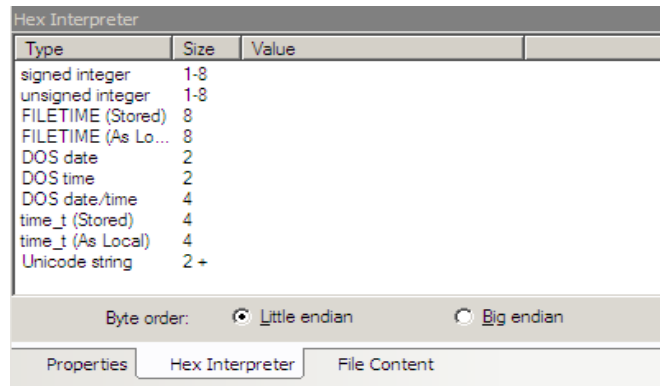
Option	Description
Fuzzy hash	Lists the following Fuzzy Hash information <ul style="list-style-type: none"><li>• Hash</li><li>• Fuzzy Hash Block Size</li></ul>

The information displayed in the Properties tab is file-type-dependent, so the selected file determines what displays. Additional information, if available and depending on file type, also displays.

## HEX INTERPRETER TAB

The Hex Interpreter tab interprets hexadecimal values selected in the Hex tab viewer on the File Content tab in the Viewer pane into decimal integers and possible time and date values as well as unicode strings.

*Figure 8-4 The Hex Interpreter Tab*



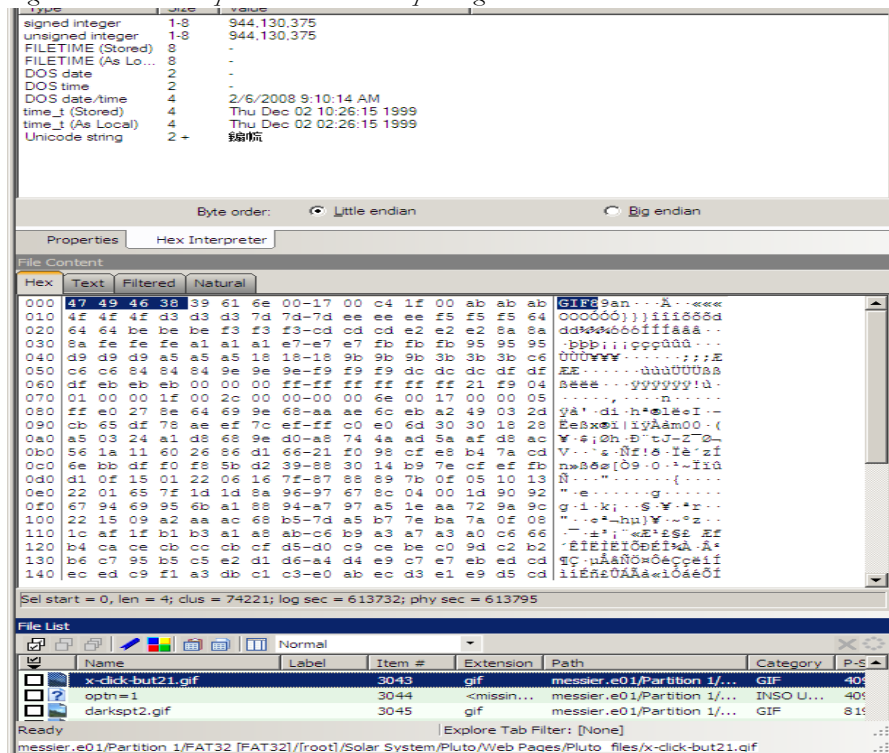
The Hex tab displays file contents in hexadecimal format. Use this view together with the Hex Interpreter pane.

This feature is most useful if the investigator is familiar with the internal code structure of different file types, and knows exactly where to look for specific data patterns or for time and date information.

The following figure shows the Hex tab selected, with a portion of the code selected and interpreted in the Hex Interpreter pane.

**Note:** The bar symbol indicates that the character in that font is not available, or that an unassigned space is not filled.

Figure 8-5 Hex Interpreter Tab and Corresponding File Content Pane Hex View Tab



To convert hexadecimal values do the following:

1. Highlight one to eight contiguous bytes of hexadecimal code in the *File Content pane* > *File Content tab viewer* > *Hex tab*. (Select two or more bytes for the Unicode string, depending on the type of data you wish to interpret and view.)
2. Switch to the Hex Interpreter tab at the bottom of the *File Content Viewer* > *Hex tab*, or open it next to, or below the *File Content tab* > *Hex tab* view.
3. The possible valid representations, or interpretations, of the selected code automatically display in the Hex Value Interpreter.

Little-endian and big-endian refer to which bytes are most significance in multi-byte data types, and describe the order in which a sequence of bytes is stored in a computer's

memory. Microsoft Windows generally runs as Little Endian, because it was developed on and mostly runs on Intel-based, or Intel-compatible machines.

In a big-endian system, the most significant bit value in the sequence is stored first (at the lowest storage address). In a little-endian system, the least significant value in the sequence is stored first. These rules apply when reading from left to right, as we do in the English language. As a rule, Intel based computers store data in a little-endian fashion, where RISC-based systems such as Macintosh, store data in a big-endian fashion. This would be fine, except that a) AccessData's products image and process data from both types of machines, and b) there are many applications that were developed on one type of system, and are now "ported" to the other system. You can't always just apply one rule and automatically know which it is.

FTK 3.0 uses Little-endian as the default setting. If you view a data selection in the Hex Interpreter and it does not seem right, try choosing *Big endian* to see if the data displayed makes more sense.

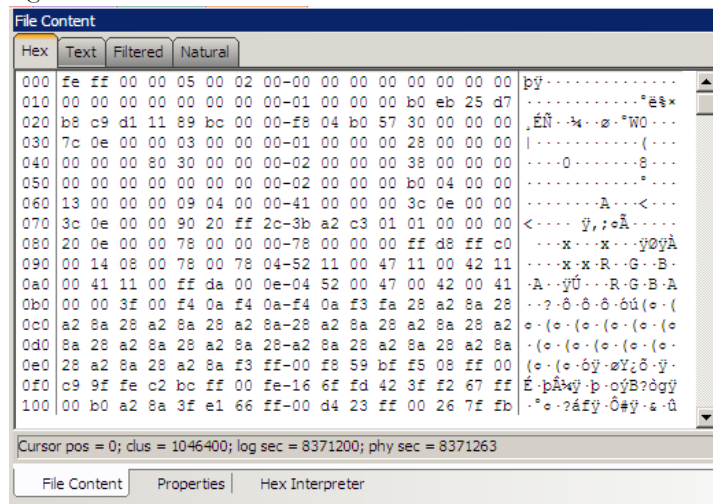
For further information on using the Hex Interpreter pane, see "Hex Interpreter Tab" on page 137.

## **FILE CONTENT TAB**

### **HEX TAB**

The Hex tab shows the file content in Hex view. It is different from the Hex Interpreter tab at the bottom of the screen, which was shown in the previous section in this chapter.

Figure 8-6 The File Content Hex View Tab.



**Note:** The bar symbol indicates that the character font is not available, or that an unassigned space is not filled.

The following table lists the available options and their descriptions:

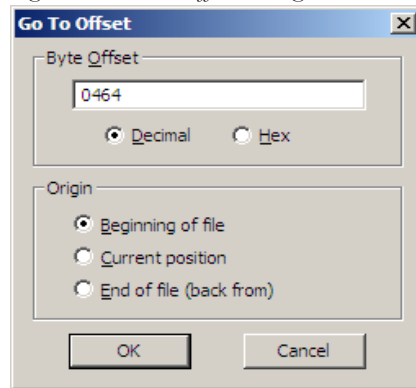
**TABLE 8-4 File Content Hex View Right-click Menu Options**

- |                  |                                 |
|------------------|---------------------------------|
| • Select all     | • Show decimal offsets          |
| • Copy text      | • Show text only                |
| • Copy hex       | • Fit to windows                |
| • Copy Unicode   | • Save current settings         |
| • Copy raw data  | • Got to offset                 |
| • Save Selection | • Save selection as carved file |

Click *Save selection as carved file* to manually carve data from files, and the Go to Offset dialog to specify offset amounts and origins. Click *OK* to close Go To Offset dialog.



Figure 8-7 Go to Offset Dialog

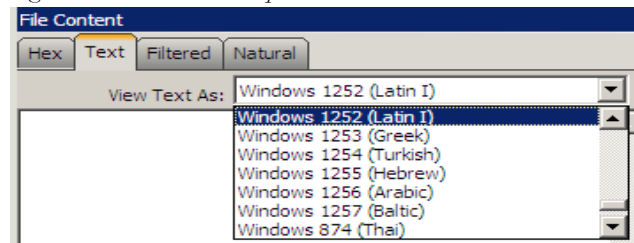


After Go to Offset has taken you to the desired offset, select the Hex data you wish to save as a separate file to add to your case, perhaps in a bookmark. Right-click and select *Save Selection as Carved File* from the menu. Name the file and click OK.

## TEXT TAB

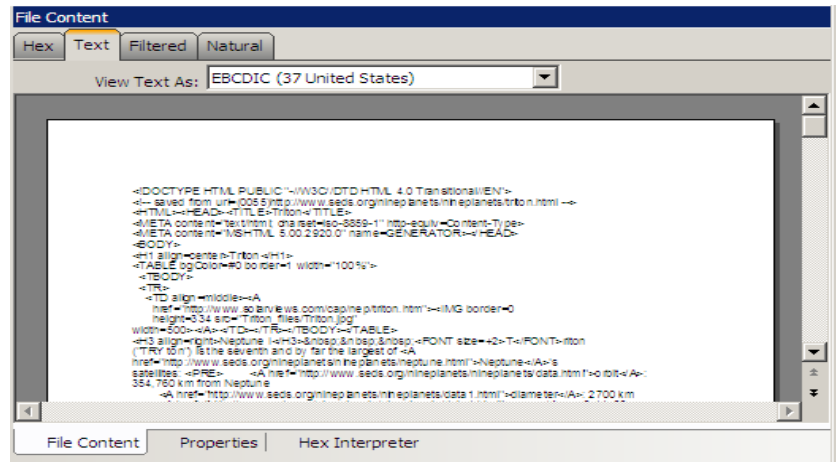
The Text tab displays the file's context as text from the code page selected from the drop-down menu. The following figure represents a portion of the drop-down selection list.

Figure 8-8 Text View Drop-Down Menu



The File Content pane currently provides many code pages from which to choose. When the desired code page is selected, the Text tab will present the view of the selected file in text using the selected code page, as shown below:

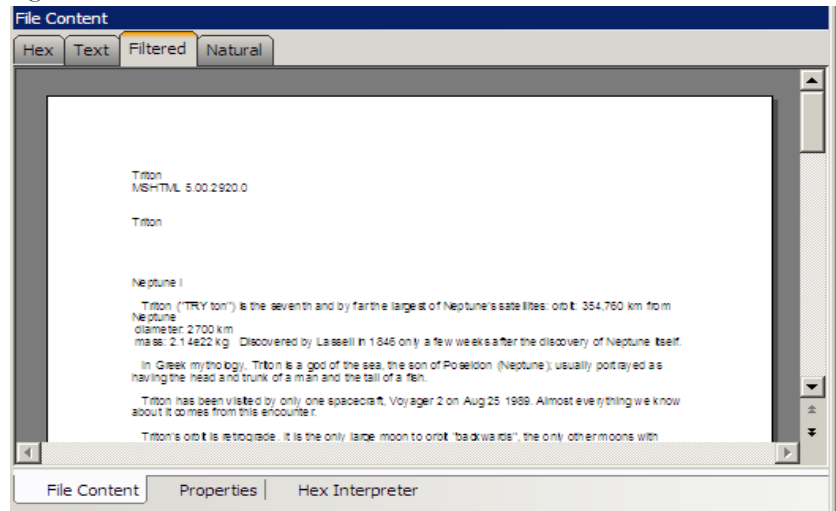
Figure 8-9 The File Content Text View Tab with the Code Page Dropdown



## FILTERED TAB

The Filtered tab shows the file text created during indexing. The following figure represents content displayed in the filtered tab.

Figure 8-10 Filtered Tab

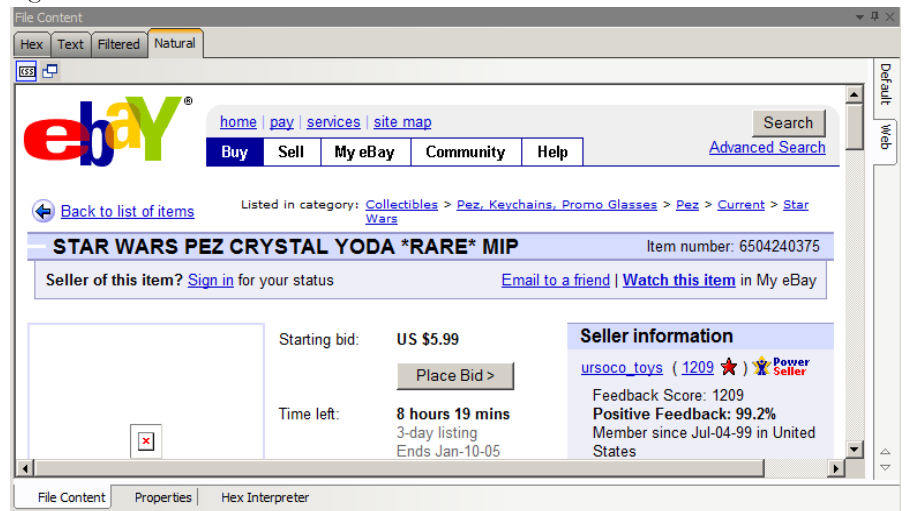


The text is taken from an index created for the current FTK session if indexing was not previously selected.

## NATURAL TAB

The Natural tab displays a file's contents as it would appear normally. This viewer uses the Oracle Stellent INSO filters for viewing hundreds of file formats without the native application being installed.

Figure 8-11



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

The Natural Tab has two tabs on the right-top border for viewing the file's contents in either the Default view, or the Web view.

In addition, the Natural tab has two additional buttons in the Web tab view. These are described below, under Web Tab.

## DEFAULT TAB

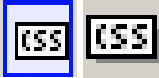

The Default Tab displays documents or files in a viewer that uses Oracle Outside In Technology, according to their file type. Case audio and video files play using an embedded Windows Media Player.

## WEB TAB

The Web view uses Internet Explorer to display the contents of the selected file in a contained field.

In the Web view, the top-left border of the pane holds two toggle buttons for enabling or disabling HTML content: Disable CSS Formatting, and Disable External Hyperlinks.

**TABLE 8-5 Natural Tab: Web Tab Toggle Buttons**

Component	Description
	Enable or Disable CSS Formatting. CSS formatting displays any fonts, colors, and layout from cascading style sheets. HTML formatting not part of a cascading style sheet might remain. Enabled feature is indicated by a blue background; disabled feature is indicated by a gray background.
	Enable or Disable External Hyperlinks. Enabled hyperlinks in the file will link to active internet pages. Enabled feature is indicated by a blue background; disabled feature is indicated by a gray background.

FTK displays the view (Web or Default) that is best for the selected file. The following figure displays an email displayed in a web tab.

*Figure 8-12 File Content, Natural Tab, Web Tab*

## OVERVIEW TAB

The Overview tab provides a general view of a case. The number of items in various categories, view lists of items, and look at individual files by category, status, and extension are displayed, as in the following figure.

*Figure 8-13 Overview Tab*

Evidence categories are represented by trees in the upper-left Case Overview pane of the application.

## FILE ITEMS CONTAINER

The File Items container itemizes files by whether they have been checked and lists in a tree view the evidence files added to the case.

## FILE EXTENSION CONTAINER

The File Extension container itemizes files by their extensions, such as .txt, .mapimail, and .doc and lists them in a tree view.

The File Extension Container content numbers do not synchronize or match up with the overall number of case items. This is because case items, such as file folders, do not have extensions and, therefore, are not listed in the File Extension Container.

## FILE CATEGORY CONTAINER

File Category Container itemizes files by function, such as a word processing document, graphic, email, executable (program file), or folder, and lists them in a tree view.

The statistics for each category are automatically listed. Expand the category tree view to see the file list associated with it.

The following table provides more detail for File Categories:

**TABLE 8-6 File Categories**

---

<b>Category</b>	<b>Description</b>
Archives	Archive files include Email archive files, Zip, Stuffit, Thumbs.db thumbnail graphics, and other archive formats.
Databases	A list of MS Access, Lotus Notes NSF, and other types of databases.
Documents	Includes most word processing, HTML, WML, HTML, or text files.
Email	Includes Email messages from Outlook, Outlook Express, AOL, Endoscope, Yahoo, Rethink, Udder, Hotmail, Lotus Notes, and MSN.
Executables	Includes Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats.
Folders	Folders or directories that are located in the evidence.
Graphics	Includes the standard graphic formats such as .tif, .gif, .jpeg, and .bmp.
Internet/Chat Files	Lists Microsoft Internet Explorer cache and history indexes.
Mobile Phone Data	Lists data acquired from supported mobile phone device(s).
Multimedia	Lists .aif, .wav, .asf, and other audio and video files.

**TABLE 8-6 File Categories**

---

<b>Category</b>	<b>Description</b>
OS/File System Files	Partitions, file systems, registry files, and so forth.
Other Encryption Files	Found encrypted files, as well as files needed for decryption such as EFS search strings, SKR files, and so forth.
Other Known Types	A miscellaneous category that includes audio files, help files, dictionaries, clipboard files, link files, and alternate data stream files such as those found in Word <b>.doc</b> files, etc.
Presentations	Lists multimedia file types such as MS PowerPoint or Corel Presentation files.
Slack/Free Space	Files, or fragments of files that are no longer seen by the file system, but have not been completely overwritten.
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, QuattroPro, and others.
Unknown Types	File types that FTK 3.0 cannot identify.
User Types	User-defined file types such as those defined in a custom File Identification File.

## FILE STATUS CONTAINER

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

The statistics for each category are automatically listed. Click the category button to see the file list associated with it. The following table displays the file status categories.

**TABLE 8-7 File Status Categories**

---

<b>Category</b>	<b>Description</b>
Bad Extensions	Files with an extension that does not match the file type identified in the file header, for example, a <b>.gif</b> image renamed as <b>graphic.txt</b> .
Data Carved Files	The results of data carving when the option was chosen for preprocessing.
Decrypted Files	The files decrypted by applying the option in the Tools menu.  <b>Note:</b> Decrypted status means FTK Decrypted the file from evidence added to the case in its original form. FTK has had control of the file and knows it was originally encrypted, that it was contained in the original evidence, and thus, is relevant to the case..

**TABLE 8-7 File Status Categories**

<b>Category</b>	<b>Description</b>
Deleted Files	Complete files or folders recovered from slack or free space that were deleted by the owner of the image, but not yet written over by new data.
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.
Email Attachments	Files attached to the email in the evidence.
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 Files and Folders" on page 226.
Flagged Ignore	Files that are flagged to be ignored are probably not important to the case.
Flagged Privileged	Files that are flagged as privileged cannot be viewed by the case reviewer.
From Email	All email related files including email messages, archives, and attachments.
From Recycle Bin	Files retrieved from the Windows Recycle Bin.
KFF Alert Files	Files identified by the HashKeeper Web site 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.
User Decrypted	Files you've previously decrypted yourself and added to the case.  <b>Note:</b> A user can add any file using Add Decrypted File, and it will be set as decrypted by user. This status indicates that FTK had nothing to do with the decryption of this file, and cannot guarantee its validity or that such a file has anything to do with the case.

## BOOKMARK CONTAINER

The Bookmark Container lists bookmarks as they are nested in the shared and the user-defined folders. Bookmarks are defined by the investigator as the case is being investigated and analyzed.

## EMAIL TAB

The Email tab displays email mailboxes and their associated messages and attachments. The display is a coded HTML format. The following figure represents the email tab.

*Figure 8-14 Email Tab*

## EMAIL STATUS TREE

The Email Status tree lists information such the sender of th email, and whether an email has attachments. They are listed according to the groups they belong to.

## EMAIL TREE

The Email tree lists message counts, AOL DBX counts, PST counts, NSF counts, MBOX counts, and other such counts.

Exchange and PST Emails can now be exported in MSG format. In addition, MSG files resulting from an export of internet email look the way they should.

**Note:** You can also export Tasks, Contacts, Appointments, Stickynotes, and Journal Entries to MSG files.

**Important:** If the Mozilla Firefox directory is added as evidence while in use, history, downloads, etc are identified as zero-legth files.

When an email-related item is selected in the File List, right-click and choose *View this item in a different list > Email* to see the file in Email context.

## GRAPHICS TAB

The Graphics tab displays the case in photo-album style. Each graphic file is shown in a thumbnail view. A graphic displays in the Graphics Tab Thumbnail view when its thumbnail is checked in the File Contents pane.



Before a graphic is fully loaded you will see the following icon:



If a graphic cannot be displayed, you will see the following icon:



The following figure displays the Graphics tab with a selected thumbnail graphic.

*Figure 8-15 Graphics Tab*

Beneath each thumbnail image is a checkbox. When creating a report, choose to include all of the graphics in the case or only those graphics that are checked. For more information on selecting graphics, see “Managing Graphics in a Report” on page 251.

The Evidence Items pane shows the Overview tree by default. Use the View menu to change the tree. Only graphic files appear in the File List when the tab filter is applied. Shut the tab filter off to view additional files.

## USING THUMBNAILS

The thumbnail settings allow large amounts of graphic data to be displayed for evidence investigation. The investigator does not need to see details to pick out evidence; scan the thumbnails for flesh tones, photographic-type graphics, and perhaps particular shapes. Once found, the graphics can be inspected more closely in the Content Viewer.

## MOVING THE THUMBNAILS PANE

The thumbnail feature is especially useful when you move the undocked graphics pane to a second monitor, freeing your first monitor to display the entire data set for the graphics files being analyzed. Do the following to move the Thumbnails pane to maximize space usage.

1. Undock the Thumbnails pane, and expand it across the screen.
2. Open the Thumbnails Settings sub-menu, and scale the thumbnails down to fit as many as possible in the pane.

## THE BOOKMARKS TAB

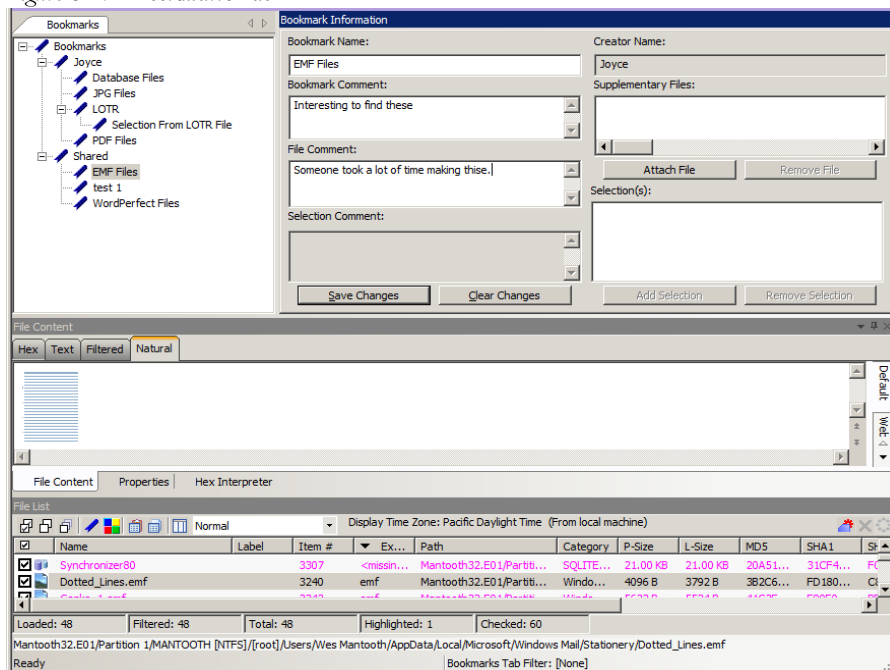
A bookmark contains a group of files that you want to reference in your case. These are user-created and the list is stored for use in the report output.

Bookmarks help organize the case evidence by grouping related or similar files. For example, you can create a bookmark of graphics that contain similar or related graphic images. The bookmark information pane is highlighted in the following figure.

*Figure 8-16 Bookmark Information Pane*

The Bookmarks tab lists all bookmarks that have been created in the current case.

Figure 8-17 Bookmark Tab



## CREATING A BOOKMARK

TABLE 8-8 Bookmarks Tab

Features	Description
Bookmark Name	Displays the name given to the bookmark when it was created.
Bookmark Comment	Displays notes included with a bookmark.
File Comment	Displays notes included with a file.
Selection Comment	Displays notes included with a selection.
Selection(s)	<p>Remembers the highlighted text in the bookmarked file and automatically highlights it when the bookmark is retrieved. The highlighted text also prints in the report.</p> <p>This can be done for multiple files with multiple selections.</p> <p>Use this option to Add and Remove Selections.</p> <ul style="list-style-type: none"> <li>• Save Changes</li> <li>• Clear Changes</li> </ul>

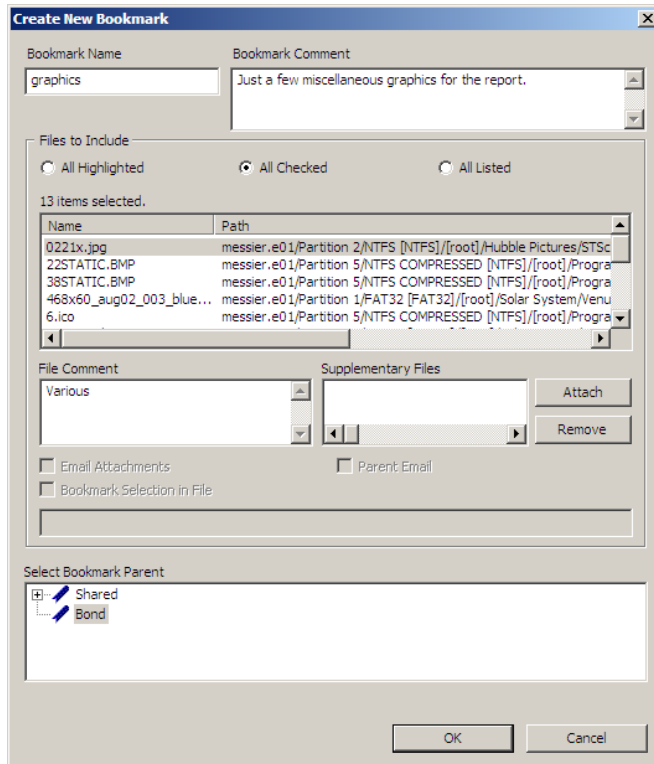
**TABLE 8-8 Bookmarks Tab**

---

<b>Features</b>	<b>Description</b>
	<ul style="list-style-type: none"><li>• Add Selection</li><li>• Remove Selection</li></ul>
Creator Name	Name of the user who created the bookmark.
Supplementary Files	Lists additional files attached to the bookmark. Options: <ul style="list-style-type: none"><li>• Attach File</li><li>• Remove File</li></ul>
File List View	New with version 3.0: Both the Sort options and Column Settings can now be unique for each bookmark.
Save Changes	Saves changes to the bookmark.
Clear Changes	Removes comments that have not been saved.

Files can be bookmarked from any tab in FTK. To create a bookmark use the information from the table above and follow these steps:

1. Right-click the files or thumbnails you want to bookmark, and click *Create Bookmark* or click the *Bookmark* button on the File List Toolbar to open the Create New Bookmark dialog.



2. Enter a name for the bookmark in the Bookmark Name field.
3. (Optional) In the Bookmark Comment field, type comments about the bookmark or its contents.
4. Click one of the following options to specify which items to add to the bookmark:
  - **All Highlighted:** Highlighted items from the current file list. Items remain highlighted only as long as the same tab is displayed.
  - **All Checked:** All items checked in the case.
  - **All Listed:** Bookmarks the contents of the File List.
5. (Optional) Type a description for each file in the File Comment field.
6. Click *Attach* to add files external to the case that should be referenced from this bookmark. The files appear in the Supplementary Files pane, and are copied to the case folder.

7. For FTK to remember the highlighted text in a file and automatically highlight it when the bookmark is re-opened, check *Bookmark Selection in File*. The highlighted text also prints in the report.
8. Select the parent bookmark under which you would like to save the bookmark.  
FTK provides a processed tree for bookmarks available to all investigators, and a bookmark tree specific to the case owner.  
If the bookmark is related to an older bookmark it can be added under the older bookmark, with the older bookmark being the parent.
9. Click *OK*.

Applying filters to a group of listed files for bookmarking can speed the process. The All Highlighted setting does not work in this instance. Enabling this feature would significantly slow the response of the program. Instead, use either the Checked Files filter, or the All Files Listed filter.

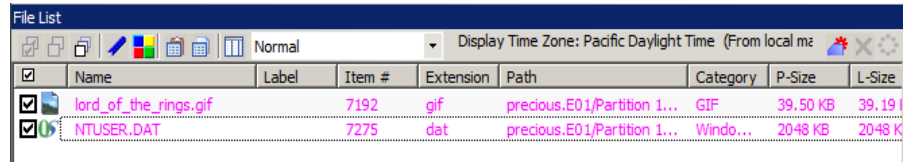
## VIEWING BOOKMARK INFORMATION

The Bookmark Information pane displays information about the selected bookmark and the selected bookmark file. The data in this pane is editable by anyone with sufficient rights.

Select a bookmark in the Bookmarks view of the Bookmarks tab, or in the Bookmarks node in the tree of the Overview tab to view information about a bookmark. The Overview tab view provides limited information about the bookmarks in the case. The Bookmark tab provides all information about all bookmarks in the case. In the Bookmark tab, the Bookmark Information pane displays the Bookmark Name, Creator Name, Bookmark Comment, and Supplementary files. When selected, a list of files contained in the bookmark displays in the File List. If you select a file from the File List the comment and selection information pertaining to that file displays in the Bookmark Information pane.

Bookmarked files appear in the File List in a different color than non-bookmarked files for easy identification

Figure 8-18 File List View Shows Bookmarks are a Different Color.



The Bookmark Information pane contains these fields:

**TABLE 8-9 Bookmark Information Pane Information**

Field	Description
Bookmark Name	The name of the bookmark. Click <i>Save Changes</i> to store any changes made to this field.
Creator Name	The user who created the bookmark.
Bookmark Comment	The investigator can assign a text comment to the bookmark. Click <i>Save Changes</i> to store any changes made to this field at any time.
Supplementary Files	Displays a list of external, supplementary files associated with the bookmark. Options are: <ul style="list-style-type: none"> <li>• <b>Attach:</b> Allows the investigator to add external supplementary files to the bookmark, these files are copied to a subdirectory within the case folder and referenced from there.</li> <li>• <b>Remove:</b> Removes a selected supplementary file from the bookmark.</li> </ul>
File Comment	The investigator can assign a different comment to each file in the bookmark. Click <i>Save Changes</i> to store any changes made to this field.

**TABLE 8-9 Bookmark Information Pane Information**

<b>Field</b>	<b>Description</b>
Selection Comment	<p>Each file within the bookmark may contain an unlimited number of selections, each of which the investigator may assign a comment. Click <i>Save Changes</i> to store any changes made to this field. These notes can be edited.</p> <ul style="list-style-type: none"><li>• <b>Save Changes:</b> Stores the changes made to the bookmark information.</li><li>• <b>Clear Changes:</b> Clears any unsaved changes made to the bookmark information.</li></ul>
Selection(s)	<p>Displays a list of stored selections within the selected file.</p> <ul style="list-style-type: none"><li>• <b>Add Selection:</b> Stores the cursor position, selection boundaries, and tab selection of the swept text in the File Content pane. This button does not store selection information for the Media or Web tabs.</li><li>• <b>Remove Selection:</b> Removes the highlighted selection from the Selections list.</li></ul>

Change any of the information displayed from this pane. Changes are automatically saved when you change the bookmark selection, but you must manually save your changes if you plan on closing FTK before selecting a different bookmark. It may be best to make a habit of saving changes everytime you make a change, to avoid forgetting and losing your changes.

**Note:** Both the Sort options and Column Settings can now be unique for each bookmark.

**Note:** In the File List, bookmarked items display in a different color for easy identification. You may need to refresh the view to force a rewrite of the screen for the different color to display. Forcing a rewrite would impact the overall performance of the program.

## **BOOKMARKING SELECTED TEXT**

Bookmarked selections are independent of the view in which they were made. Select hex data in the Hex view of a bookmarked file and save it; bookmark different text in the Filtered view of the same file and save that selection as well.

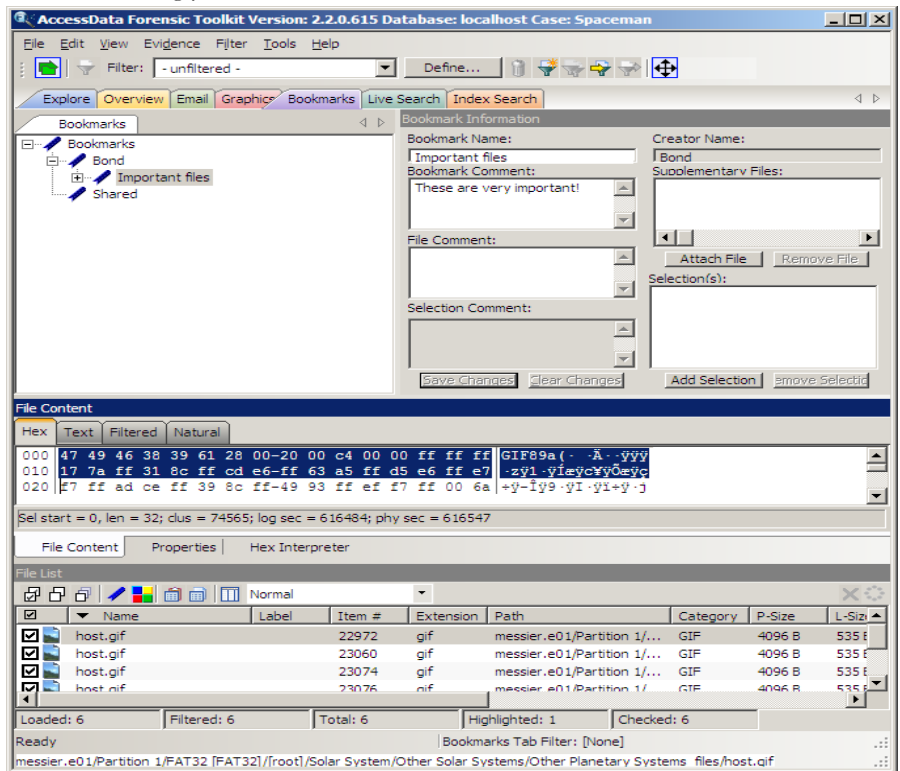
To add selected text in a bookmark perform the following steps:

1. Open the file containing the text you want to select.
2. From the Natural, Text, Filtered or Hex views, make your selection.

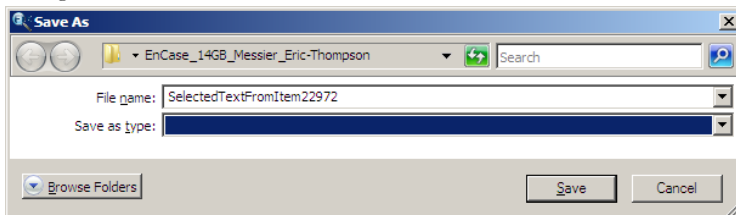


**Note:** If the file is a graphic file, you will not see, nor be able to make selections in the Text or the Natural views.

3. Click *Create Bookmark* in the File List toolbar to open the Create New Bookmark dialog.
4. When creating your bookmark, check *Bookmark Selection in File*



5. To save selected content, choose the view that shows what you want to save, then highlight the content to save.
6. Right-click on the selected content. Click *Save As*.



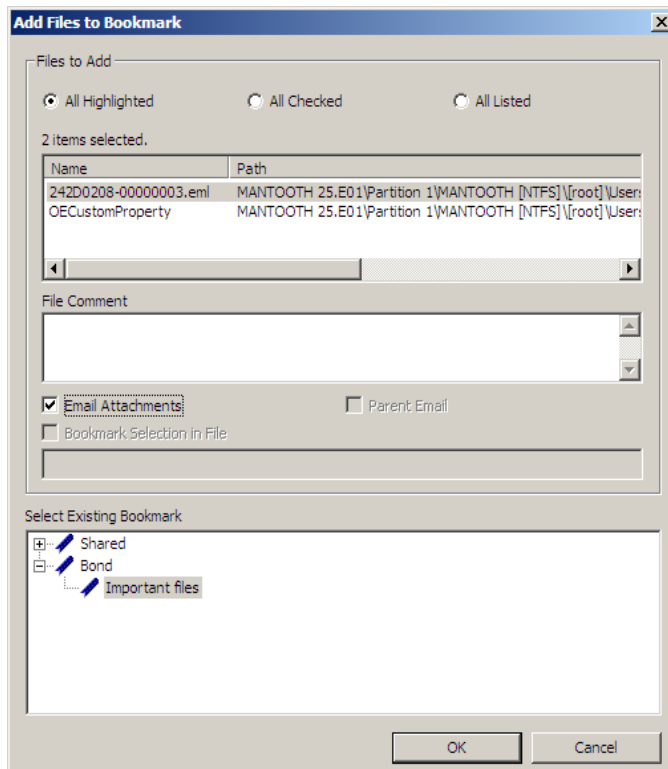
7. Name the selection and click *Save*.

The selection remains in the bookmark.

## ADDING TO AN EXISTING BOOKMARK

Sometimes additional information or files are desired in a bookmark. To add to an existing bookmark, follow these steps:

1. Right-click the new file.
2. Click *Add to Bookmark*.



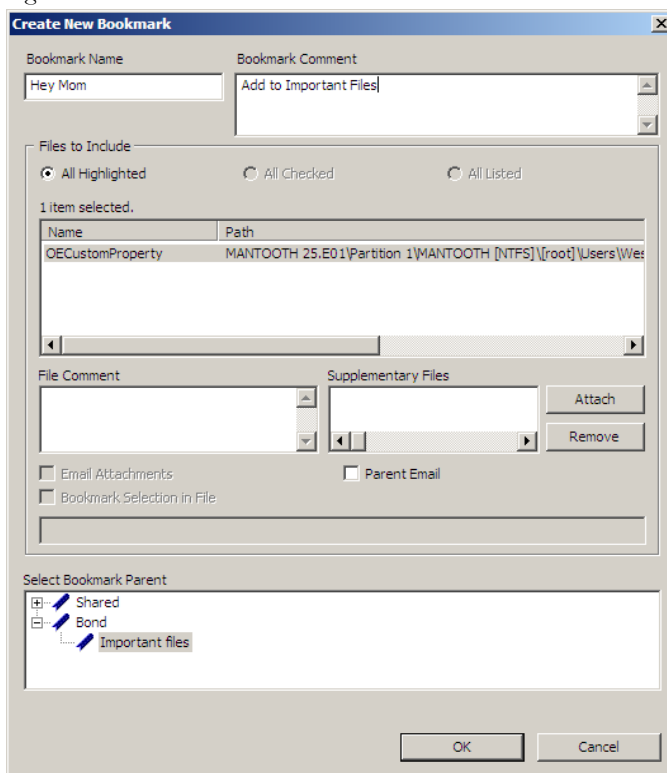
3. Select the parent bookmark.
4. Select the child bookmark to add the file or information to.
5. Click *OK*.

## CREATING EMAIL OR EMAIL ATTACHMENT BOOKMARKS

When bookmarking an email FTK allows the addition of any attachments. FTK also allows the inclusion of a parent email when bookmarking attachments to an email.

To create a bookmark for an email, follow the steps for creating a bookmark. Select the email to include in the bookmark. Right-click and choose *Create Bookmark*. Note that by default, the Email Attachments box is active, but unmarked. If only the parent email is needed the Email Attachments box should remain unselected. The following figure displays the Create New Bookmark dialog for an email with the Email Attachments checkbox selected.

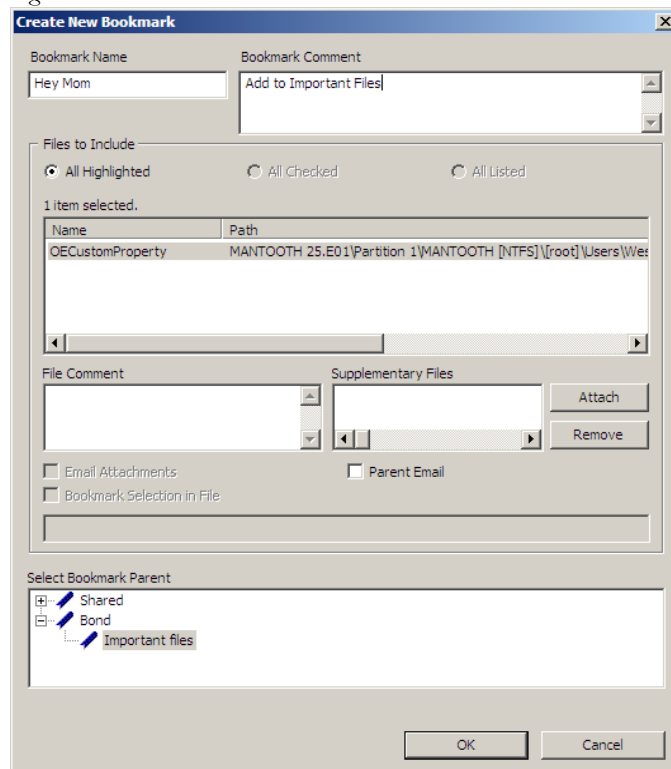
Figure 8-19 Create New Bookmark with Email Attachment



If you need to bookmark only an attachment of the email, select and right-click on the attachment. Choose *Create Bookmark*. For more information on creating bookmarks, see, “Creating a Bookmark” on page 151.

Note that the Parent Email box is automatically active, allowing you to include the parent email. If the Parent Email box is checked, and there is more than one attachment, the Email Attachments box becomes active, allowing you to also include **all** attachments to the parent email. To add only the originally selected attachment to the bookmark, do not check the Parent Email box. The following figure displays the Create New Bookmark dialog with the Parent Email checkbox selected.

Figure 8-20 Create New Bookmark with Parent Email Selected

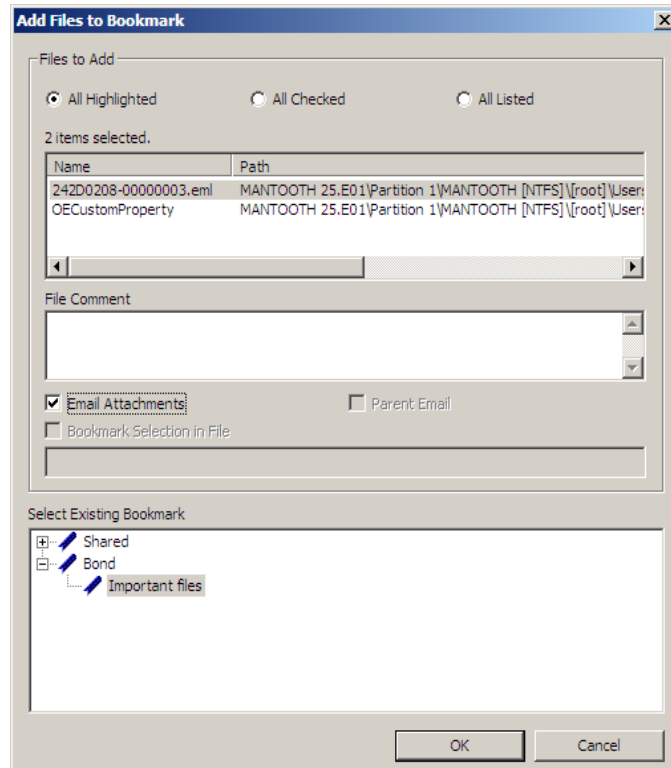


## ADDING EMAIL AND EMAIL ATTACHMENTS TO BOOKMARKS

To add an email to a bookmark, select the email to add, then right-click on the email and choose Add To Bookmark. (For more information see, “Adding to an Existing Bookmark” on page 158). Note that the Email Attachments box is active, but not marked. If only the parent email is needed the Email Attachments box can remain unselected. To include the attachment’s parent email, mark the box. The following

figure displays the Add Files to Bookmark dialog with the Email Attachments checkbox selected.

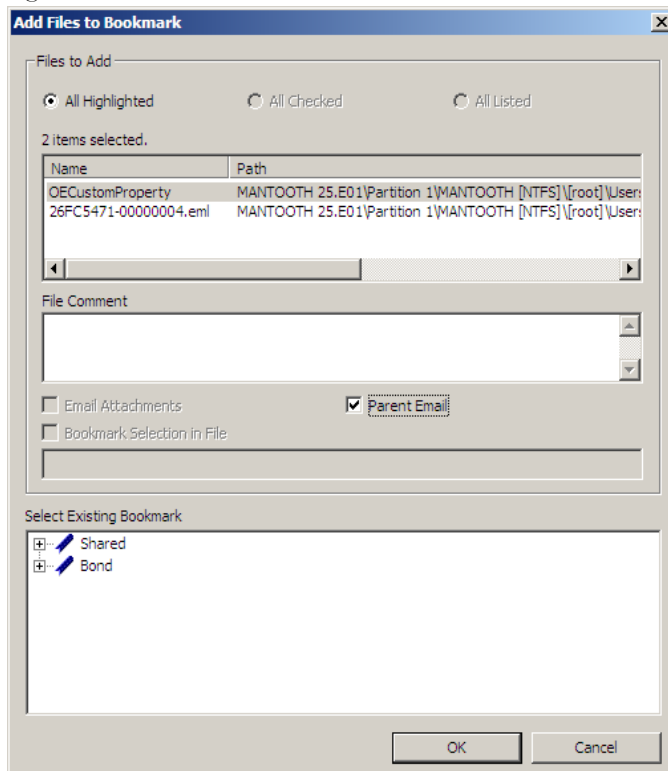
Figure 8-21 Add Files to Bookmark with Email Attachments Selected



If only an attachment of an email is needed to be added to the bookmark, select the attachment and follow the instructions for adding to a bookmark. For more information on adding to bookmarks, see, “Adding to an Existing Bookmark” on page 158.

Note that the Parent Email box is automatically active, but not selected, giving the opportunity to select the parent email if you wish to include it with the attachment to the bookmark. The following figure displays the Add Files to Bookmark dialog with the Parent Email checkbox selected.

Figure 8-22 Add Files to Bookmark with Parent Email Selected



## MOVING A BOOKMARK

The following steps detail how to move a bookmark:

1. From either the Bookmark or the Overview tab, select the bookmark you want to move.
2. Using the left or right mouse button, drag the bookmark to the desired location and release the mouse button.

## DELETING A BOOKMARK

Use the following steps to delete a bookmark:

1. In the Bookmark tab, expand the bookmark list and highlight the bookmark to be removed.

2. Press the *Delete* key.

**OR**

3. Right-click on the bookmark to delete, and choose *Delete*.

## DELETING FILES FROM A BOOKMARK

Use the following steps to delete files from bookmarks:

1. From either the Overview tab or the Bookmarks tab, open the bookmark containing the file you wish to delete.
1. Right-click the file in the Bookmark File List.
2. Select *Remove from Bookmark*.

**Note:** Deleting a file from a bookmark does not delete the file from the case.

The following table describes the features of the Bookmark tab.

## SEARCH TABS

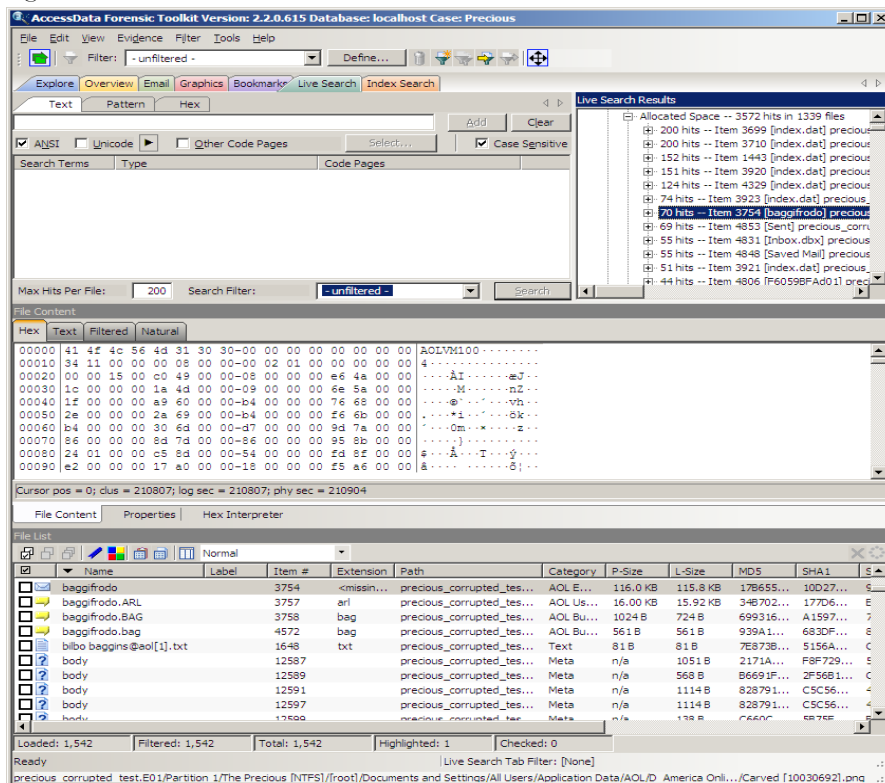
The Search Tabs allow the user to conduct an indexed search or a live search on the evidence. An indexed search is faster, while a live search is more flexible and powerful.

The results of each search appear as line items in the search results list. Click the plus icon (+) next to a search line to expand the search results branch. 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 “Chapter 9 Searching a Case” on page 175.

## LIVE SEARCH TAB

The live search is a process involving an item-by-item comparison with the search term. The following figure represents a selected Live Search tab.

Figure 8-23 Live Search Tab



A live search is flexible because it can find non-alphanumeric character patterns. Comparatively, an Index search is confined to the index of the alphanumeric patterns created with the index when the case is initially processed.

## INDEX SEARCH TAB

The indexed search uses the index file generally created in pre-processing or through additional analysis to find the search term. The following figure represents the Index Search being performed.

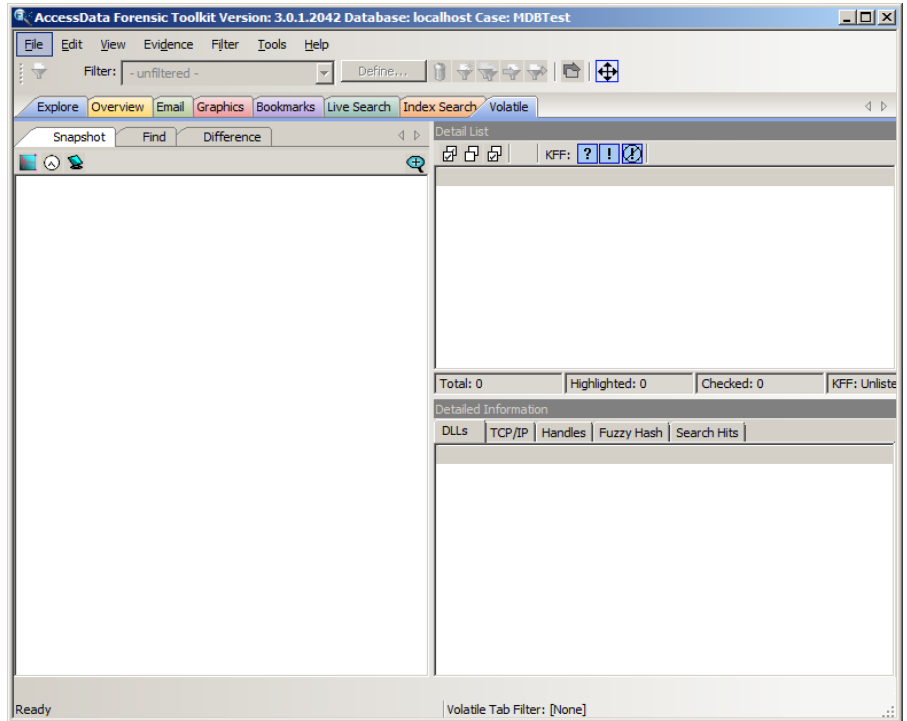
Figure 8-24 Index Search Tab

Evidence items can be indexed when they are first added to the case or at a later time.



## VOLATILE TAB

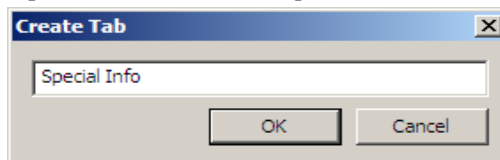
The Volatile tab provides tools for viewing, finding, and comparing data gathered from live agent systems in your network. Volatile Tab



## CREATING TABS

Create custom tabs by selecting *View > Tab Layout > Add* to bring up the Create Tab dialog, as in the following figure.

Figure 8-25 Create Tab Dialog



For more information on tab creation, see “Creating Custom Tabs” on page 267.



## *Chapter 9 Searching a Case*

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. AccessData FTK provides an index search that gives rapid results, as well as three different live search modes: hexadecimal, pattern (“regular expression”, known commonly as regex), and text. Search results, or “hits,” are easily viewed from the Search Tab File List and File Contents views.

### **CONDUCTING A LIVE SEARCH**

The live search takes more time than an index search because it involves a bit-by-bit comparison of the search term to the evidence. A live search is flexible because it can find patterns of non-alphanumeric characters that are not generally indexed. It is powerful because you can define those patterns to meet your needs in an investigation.

Live search supports Regular Expression (Regex) searches. In Live Search you can use Regex to create pattern searches—precise character strings formatted as mathematical-style statements that describe a data pattern such as a credit card or social security number. Pattern searches allow the discovery of data items that conform to the pattern described by the expression, rather than knowing and entering what you are looking for by content.

For more information about regular expressions and syntax, see “Conducting a Pattern Search” on page 179

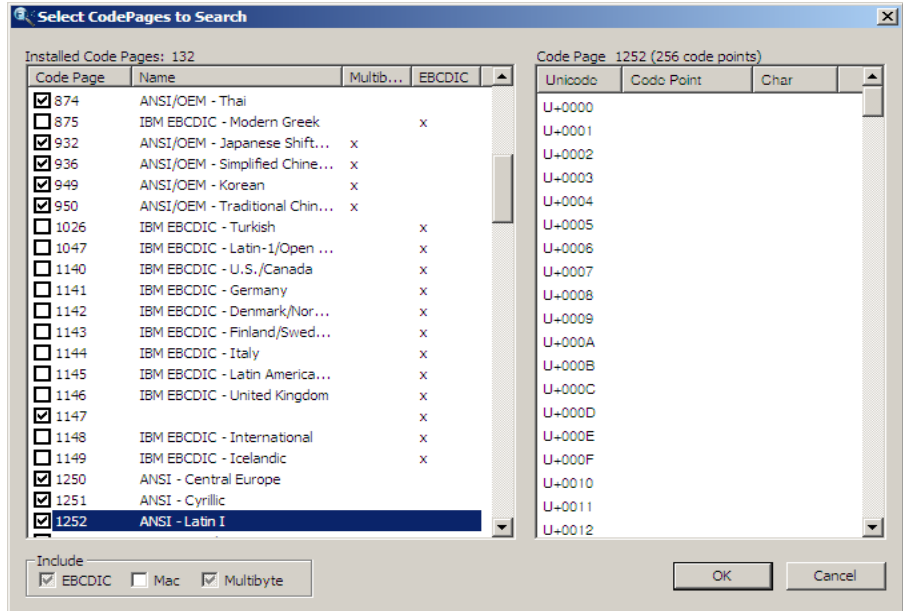
AccessData recommends live searching for items an index search cannot find.

To perform a live search:

1. In the Live Search tab, click the Text, Pattern, or Hex tab.

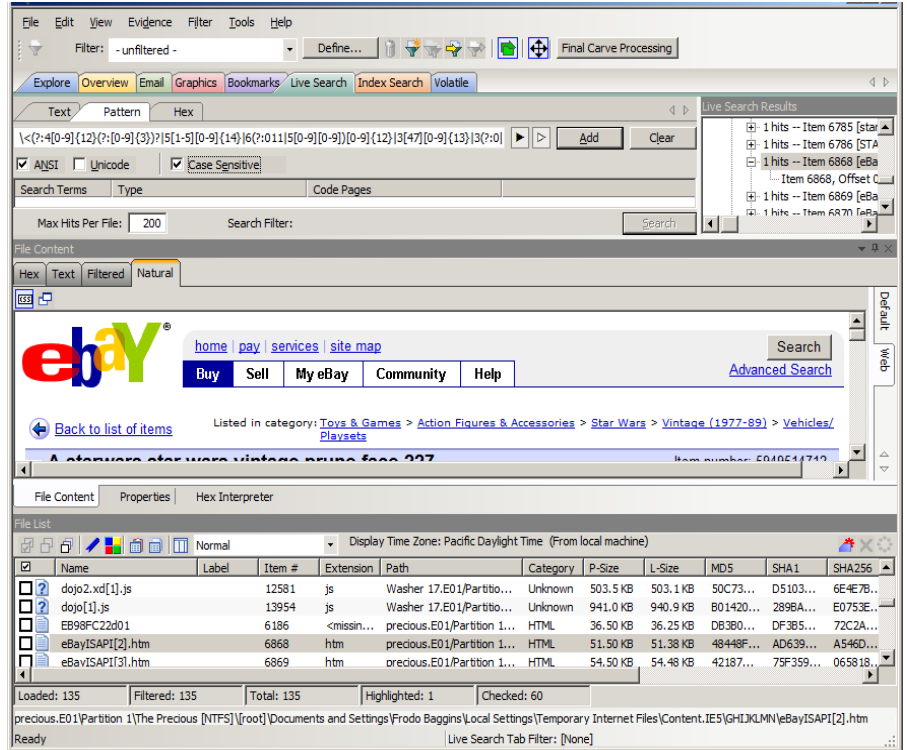
In the Text or Pattern tabs, check the character sets to include in the search. If you want to include sets other than ANSI and Unicode, check *Other Code Pages* and click *Select*.

2. *Select CodePages to Search*Select the needed sets.



3. Click to include *EBCDIC*, *Mac*, and *Multibyte* as needed.

4. Click *OK* to close the dialog.



5. Check *Case Sensitive* if you want to search specifically uppercase or lowercase letters. ignores case if this box is not checked.
6. Enter the term in the Search Term field.
7. Click *Add* to add the term to the Search Terms window.
8. Click *Clear* to remove all terms from the Search Terms window.
9. 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. The range is 1 to 65,535. If you want to apply a filter, do so from the Filter drop-down list in the bar below the Search Terms list. Applying a filter speeds up searching by eliminating items that do not match the filter. The tab filter menu has no effect on filtering for searches.
10. Click *Search*.
11. Click *Cancel* in the progress dialog to stop the search before it is complete.
12. Select the results to view from the Live Search Results pane. Click the plus icon (+) next to a search line to expand the branch. Individual search results are listed in the Live Search Results pane, and the corresponding files are listed in the File List. To

view a specific item, select the file in the search results. All search results are highlighted in the Hex View tab.

**Note:** Searching before the case has finished processing will return incomplete results. Wait until the case has finished processing and the entire body of data is available.

**Important:** Right-click on a search result in the Live Search Results pane to display more options. The available right-click options are as follows: Searching before

**TABLE 9-1 Right-Click Options in Live Search Results Pane**

Option	Description
Create Bookmark	Opens the Create New Bookmark dialog.
Copy to Clipboard	Opens a new context-sensitive menu. Options are: <ul style="list-style-type: none"><li>• All Hits In Case</li><li>• All Hist In Search</li><li>• All File Stats In Case</li><li>• All File Stats In Search</li></ul>
Export to File	Opens a new context-sensitive menu. Options are: <ul style="list-style-type: none"><li>• All Hits In Case</li><li>• All Hist In Search</li><li>• All File Stats In Case</li><li>• All File Stats In Search</li><li>•</li></ul>
Set Context Data Width	Opens the Data Export Options window. Allows you to set a context width from 32 to 2000 characters within which to find and display the search hit.
Delete All Search Results	Deletes all search results from the Live Search Results pane.
Delete this Line	Deletes only the highlighted search results line from the Live Search Results pane.

the case has finished processing will return incomplete results. Wait to search until the case has finished processing and the entire body of data is available.

**Note:** Search terms for pre-processing options only support ASCII characters.

## CUSTOMIZING THE LIVE SEARCH TAB

Change the order of the Live Search tabs by dragging and dropping them with your mouse.

*Figure 9-1 Customizing the Live Search Tab*

For more information on customizing the FTK user interface, see “Chapter 13 Customizing the FTK Interface” on page 263 .

## CONDUCTING A PATTERN SEARCH

Regex can be used to create pattern searches, allowing forensics analysts to search through large quantities of text information for repeating strings of data such as:

- Telephone Numbers
- Social Security Numbers
- Computer IP Addresses
- Credit Card Numbers

These pattern searches 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,  $5/((1+2)*3)$ :

**TABLE 9-2** Regex Pattern Search Components

---

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, pattern searches have operands, operators, sub-expressions, and a value.

**Note:** Unlike arithmetic expressions, which can only have numeric operands, operands in pattern searches can be any characters that can be typed on a keyboard, such as alphabetic, numeric, and symbol characters.

## SIMPLE PATTERN SEARCHES

A simple pattern search can be made up entirely of operands. For example, the pattern search *dress* causes the search engine to return a list of all files that contain the sequence of characters *d r e s s*. The pattern search *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 pattern search *dress*.

The search engine searches left to right. So in searching the pattern search *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 PATTERN SEARCHES

Operators allow regular expressions to search patterns of data rather than specific values. For example, the operators in the following expression enables the FTK 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.

The following table identifies the components in the Visa and MasterCard regular expression:

**TABLE 9-3 Visa and MasterCard Regular Expressions**

Example	Operands
Operands	\-, spacebar space
Operators	\<, ( ), [ ], {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 pattern 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.

**Note:** 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 or escape character (`\`), used for the modification of operands and 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 parentheses operator (`()`) groups together a sub-expression, that is, a sequence of characters that must be treated as a group and not as individual operands.

The `\d` 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 either a hyphen or a spacebar space.

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 backslash greater-than combination (`\>`), also known as the end-a-word operator, means that the preceding expression must be followed by a non-word character.

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 pattern search is not the only way to search for Visa or MasterCard credit card numbers. Because some pattern search operators have related meanings, there is more than one way to compose

a pattern search to find a specific pattern of text. For instance, the following pattern search 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 pattern search 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 many predefined regular expressions for pattern searching, including the following:

**TABLE 9-4 A Small Sampling of FTK Predefined Regular Expressions**

- 
- |                                |                               |
|--------------------------------|-------------------------------|
| • U.S. Social Security Numbers | • IP Addresses                |
| • U.S. Phone Numbers           | • Visa and MasterCard Numbers |
| • U.K. Phone Numbers           |                               |

Select regular expressions from drop-down lists under the arrows:

- Click the black arrow  to see a list of the basic components for regular expressions. You can create your own pattern by combining these components into a longer expression.

Figure 9-2 Regular Expressions Basic Components

<code>.</code> - any character
<code>\t</code> - tab
<code>\s</code> - whitespace character
<code>\d</code> - decimal digit - same as <code>[0-9]</code>
<code>\u</code> - upper case character - same as <code>[A-Z]</code>
<code>\l</code> - lower case character - same as <code>[a-z]</code>
<code>\w</code> - word character - same as <code>[a-zA-Z0-9_]</code>
<code>\n</code> - newline character
<code>\r</code> - return character
<code>\b</code> - at word boundary
<code>\B</code> - not at word boundary
<code>\&lt;</code> - at start of word
<code>\&gt;</code> - at end of word
<code>^</code> - at start of line
<code>\$</code> - at end of line
<code>\`</code> - at start of file
<code>\'</code> - at end of file
<code>?</code> - match previous 0 or 1 times
<code>*</code> - match previous 0 or more times
<code>+</code> - match previous 1 or more times
<code>{n}</code> - match previous n times
<code>{n,}</code> - match previous n or more times
<code>{m,n}</code> - match previous m to n times
<code>[:alpha:]</code> - alpha character
<code>[:alnum:]</code> - alpha-numeric character
<code>[:blank:]</code> - whitespace except line separator


- Click the white arrow  to see a list of predefined expressions.

Figure 9-3 Live Search Tab Predefined Regular Expressions

MAC Address
URL {http, https, ftp, ftps}
mailto: ...
... .com
... .edu
... .info
... .net
... .org
... .gov
... .museum
... .tv
... .<any>
... @ ... .com
... @ ... .edu
... @ ... .gov
... @ ... .net
... @ ... .org
... @ ... .<any> email address
AMEX
Visa
Mastercard 1
Discover
Credit Card Standard
Web Credit Card Transaction Receipt with X or #
Kazaa DAT file
Kazaa DBB
Limewire DAT
Link File Parser (fast) - (Run on unallocated)
Lnk File Parser with MAC/NETBIOS Info (Run on Unallocated)
Info2 Files FAST All Years
INFO2-Expanded (Run on Unallocated)
MSN Hotmail Beginning
MSN Hotmail End
HTML Search Engine Return - Google Search
INDEX.dat entries and Search Engine Return - Google Search
HTML Search Engine Return - Ebay.com, search.aol.com, mamma.com
HTML Search Engine - Ask Jeeves
Orphaned Index.dat Files (with date)
Orphaned Index.dat Files (without date)
Orphaned History Index.dat Files
Orphaned Index.dat Cookie Files
IP Address
US Phone Number
UK Phone Number
Social Security Number
Edit expressions...

The Social Security Number, U.S. Phone Number, and IP Address expressions are discussed in the following sections.

## SOCIAL SECURITY NUMBER

The pattern search for Social Security numbers follows a relatively simple model:

```
\<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 pattern search for U.S. phone numbers is more complex:

```
((\<1[\-\. ])?(\(|\<)\d\d\d[\)\.\/ ] ?)\<d\d\d[\.\- ]\d\d\d\d\>
```

The first part of the above expression,

```
((\<1[\-\. ])?(\(|\<)\d\d\d[\)\.\/ ] ?)?,
```

means 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. This 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. The left parenthesis is, of necessity, escaped. The initial delimiter is followed by three decimal digits, then another delimiter, 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 pattern search 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.

You can begin building your own regular expressions by experimenting with the default expressions. You can modify the default expressions to fine-tune your data searches or to create your own expressions. Visit the AccessData Website, [www.accessdata.com](http://www.accessdata.com), to find a technical document on Regular Expressions. Click *Support > Downloads > Regular Expressions*.

## CREATING CUSTOM REGULAR EXPRESSIONS

Create your own customized regular expressions using the following list of common operators

**TABLE 9-5 Common Regular Expression 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 within 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].
`	(Back quote) Starts the search at the beginning of a file.
'	(Single quote) Starts the search at the end of a file.
\<	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 requires that the next character in a search hit be “A” or “u.”
\b	Positions the cursor between characters and spaces.
\B	Matches anything not at a word boundary. For example, will find Bob in the name Bobby.
\d	Matches any single decimal digit.
\l	Matches any lowercase letter.
\n	Matches a new line.
\r	Matches a return.
\s	Matches any whitespace character such as a space or a tab.
\t	Matches a tab.
\u	Matches any uppercase letter.
\w	Matches any whole character [a-z A-Z 0-9].

**TABLE 9-5 Common Regular Expression Operators**

---

Operator	Description
<code>^</code>	Matches the start of a line.
<code>[:alpha:]</code>	Matches any alpha character (short for the <code>[a-z A-Z]</code> operator).
<code>[:alnum:]</code>	Matches any alpha numerical character (short for the <code>[a-z A-Z 0-9]</code> operator).
<code>[:blank:]</code>	Matches any whitespace, except for line separators.
<code>{n,m}</code>	Matches the preceding sub-expression at least <i>n</i> times, but no more than <i>m</i> times.

## CONDUCTING HEX SEARCHES

Click the Hex (Hexadecimal) Search tab to enter a term by typing it directly into the search field, by clicking the Hexadecimal character buttons provided, or by copying hex content from the hex viewer of another file and pasting it into the search box. Click *Add* to add the hex string to the search terms list.

*Figure 9-4 The Hex Tab in Live Search*

The instructions for conducting a live search on the hex tab are similar to conducting searches on the Pattern tab. Remember, when searching for hexadecimal values, a single alphabetic or numeric text character is represented by hex characters in pairs.

## CONDUCTING TEXT SEARCHES

The difference between a Pattern search and a Text search is that a text search searches for the exact typed text, there are no operands so the results return exactly as typed. For example, a Pattern search allows you to find all strings that match a certain pattern, such as for any 10-digit phone number (*nnn-nnn-nnnnn*), or a nine-digit social security number (*nnn-nn-nnnnn*). A Text search finds all strings that match an exact entry, such as a specific phone number (801-377-5410). When conducting a Live Text Search, there are no arrows to click for operand selection, as displayed in the following graphic.

*Figure 9-5 The Text Tab in Live Search*

Otherwise apply the instructions for the pattern search to this search.



For more information on conducting a pattern search see “Conducting a Pattern Search” on page 179.

## CONDUCTING AN INDEX SEARCH

The index search uses the index to find the search term. Evidence items may be indexed when they are first added to the case or at a later time. Whenever possible, AccessData recommends indexing a case before beginning analysis.

Index searches are instantaneous. In addition, the Index Search Results File List loads more quickly in version 3.0 than in past versions. In addition, in the Index Search Results List, the offset of the data in the hit is no longer listed in the hit. You will see it when you look at the hit file in Hex view.

Running an Index search on large files or Index Searches resulting in a large number of hits may make the scroll bar appear not to work.

For more information about indexing an evidence item, see “Indexing a Case” on page 68. The following figure displays the FTK window with the Index Search tab selected.

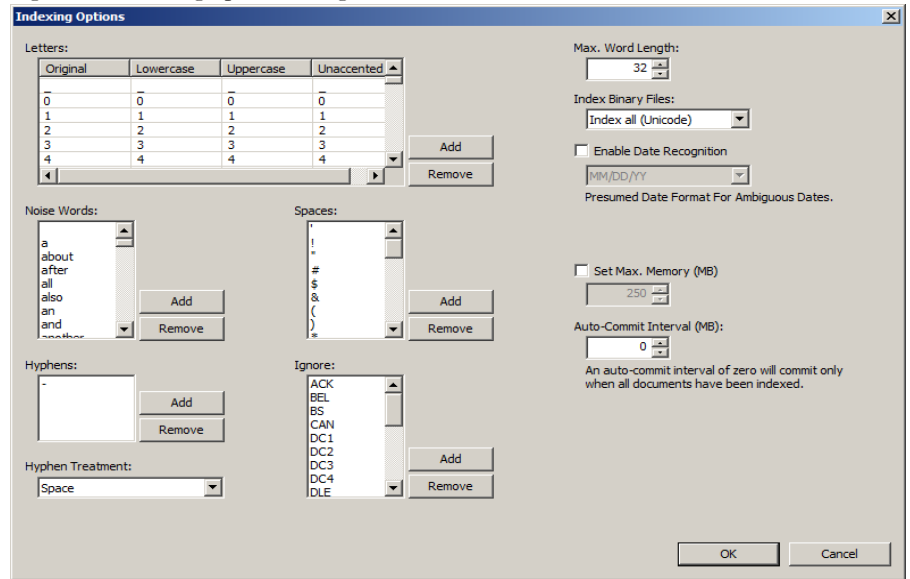
*Figure 9-6 The Index Search Tab*

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:

. , ; ' ~ ! # \$ ^ & + .

now indexes special characters. One benefit is that you can easily search on a nearly exact email address using *username@isp* (the extension, such as .com or .net, is not included automatically because a period (.) is not indexed). The following figure shows the Indexing Options dialog available prior to creating a case:

Figure 9-7 Indexing Options Dialog



These options must be set prior to case creation. In the Evidence Processing screen, mark the *dtSearch Text Index* box, then click *Indexing Options* to bring up the Indexing Options screen shown in the figure above. Set the options using the information in the following table:

**TABLE 9-6 dtSearch Indexing Options**

Option	Description
Letters	Specifies the letters and numbers to index. Specifies Original, Lowercase, Uppercase, and Unaccented. Choose <i>Add</i> or <i>Remove</i> to customize the list.
Noise Words	A list of words to be considered “noise” and ignored during indexing. Choose <i>Add</i> or <i>Remove</i> to customize the list.
Hyphens	Specifies which characters are to be treated as hyphens. You can add standard keyboard characters, or control characters. You can remove items as well.
Hyphen Treatment	Specifies how hyphens are to be treated in the index. Options are: <ul style="list-style-type: none"> <li>• Ignore</li> <li>• Space</li> <li>• Hyphen</li> <li>• All</li> </ul>

**TABLE 9-6 dtSearch Indexing Options**

Option	Description
Spaces	Specifies which special characters should be treated as spaces. Remove characters from this list to have them indexed as any other text. Choose <i>Add</i> or <i>Remove</i> to customize the list.
Ignore	Specifies which control characters or other characters to ignore. Choose <i>Add</i> or <i>Remove</i> to customize the list.
Max. Word Length	Allows you to set a maximum word length to be indexed
Index Binary Files	Specify how binary files will be indexed. Options are <ul style="list-style-type: none"><li>• Index all</li><li>• Index all (Unicode)</li><li>• Skip</li></ul>
Enable Date Recognition	Choose to enable or disable this option
Presumed Date Format For Ambiguous Dates	If date recognition is enabled, specify how ambiguous dates should be formatted when encountered during indexing. Options are: <ul style="list-style-type: none"><li>• MM/DD/YY</li><li>• YY/MM/DD</li><li>• DD/MM/YY</li></ul>
Set Max. Memory	Allows you to set a maximum size for the index.
Auto-Commit Interval (MB)	Allows you to specify an Auto-Commit Interval while indexing the case. When the index reaches the specified size, the indexed data is saved to the index. The size resets, and indexing continues until it reaches the maximum size, and saves again, and so forth.

When finished setting Detailed Options, click *OK* to close the dialog, complete the New Case Options dialog, then click *OK* to create the case.

In addition to performing searches within the case, you can also use the index to export a word list to use as a source file for custom dictionaries to improve the likelihood of and speed of password recovery related to case files when using the Password Recovery Toolkit (PRTK). You can export the index by selecting *File > Export Word List*.

## SEARCH TERMS

Type the word or term in the Search Term field. The term and terms like it appear in the Indexed Words column displaying the number of times that particular term was found in the data. Click *Add* to place the term in the Search Terms list, or double-click the term in the indexed words column to add it to the Search Terms list.

## SEARCH CRITERIA

Refine a search even more by using the Boolean operators AND and OR. You can specify the terms to use in an index search by selecting specific entries, or by searching against all entries.

You can import a list of search terms to save having to type them multiple times. This is especially helpful if the list is long, or the terms are complex. When you create a search terms document, each term begins on a new line, and is followed immediately by a hard return. Save the file in `.txt` format in any text editor, or create the list in FTK and save it for future use.

**Important:** When creating your search criteria, try to focus your search to bring up the smallest number of meaningful hits per search.

You can export a list of search terms you have added to the list of search terms to save having to find them, or type them again.

To export a set of search terms for later use, or for documentation purposes:

1. Highlight the search terms to export to a file.
2. Click *Export*.
3. Provide a filename and location for the file (the `.txt` extension is added automatically).
4. Click *Save*.

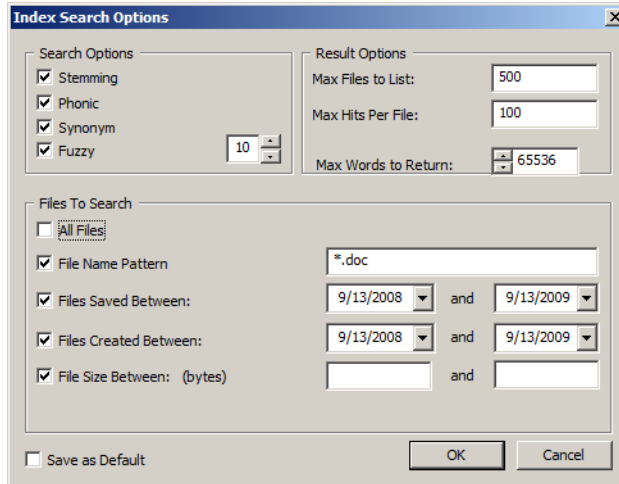
To import a saved search terms file:

1. Click *Import* to import a set of search terms.
2. Select the search terms file you previously saved.
3. Click *Open*.

## INDEX SEARCH OPTIONS

To refine an index search, from the Index Search tab, in the Search Criteria area, click *Options*.

Figure 9-8 Indexed Search Options



The following tables review the individual index search and index result options:

**TABLE 9-7 Index Search Options**

Option	Result
Stemming	Words that contain the same root, such as <i>raise</i> and <i>raising</i> .
Phonic	Words that sound the same, such as <i>raise</i> and <i>raze</i> .
Synonym	Words that have similar meanings, such as <i>raise</i> and <i>lift</i> .
Fuzzy	Words that have similar spellings, such as <i>raise</i> and <i>raize</i> .

Click the arrows to increase or decrease the number of letters in a word that can be different from the original search term. Use this feature carefully; too many letter differences may make the search less useful.

**TABLE 9-8 Index Result Options**

---

<b>Option</b>	<b>Result</b>
Max Files to List	Maximum number of files with hits that are to be listed in the results field. You can change this maximum number in the field. Searches limited in this way will be indicated by an asterisk (*) and the text “(files may be limited by “Max files to list” option)” which may be cut off if the file name exceeds the allowed line length. The maximum number of possible files with hits per search is 65,535. If you exceed this limit, the remaining hits will be truncated, and your search results will be unreliable. Narrow your search to limit the number of files with hits.
Max Hits per File	Maximum number of hits per file. You can change the maximum number in this field. Searches limited in this way will be indicated by an asterisk (*) and the text “(files may be limited by “Max hits per file” option)” which may be cut off if the file name and this text together exceed the allowed line length. The maximum number of possible hits per file is 10,000.
Max Words to Return	The maximum number of words to be returned by the search.

**TABLE 9-9 Files to Search**

---

<b>Option</b>	<b>Description</b>
All Files	Searches all the files in the case.
File Name Pattern	Limits the search to files that match the filename pattern.  Operand characters can be used to fill-in for unknown characters. The asterisk (*) and question-mark (?) operands are the only special characters allowed in an index search. The pattern can include “?” to match any single character or “*” to match an unknown number of contiguous characters.  For example, if you set the filename pattern to “d?ugl*”, the search could return results from files named “douglas”, “douglass”, or “druglord.”  To enter a filename pattern: <ol style="list-style-type: none"><li>1. Check the box.</li><li>2. In the field, type the filename pattern.</li></ol>

**TABLE 9-9 Files to Search**

---

<b>Option</b>	<b>Description</b>
Files Saved Between	Beginning and ending dates for the timeframe of the last time a file was saved. <ol style="list-style-type: none"><li>1. Check the box.</li><li>2. In the date fields, type the beginning and ending dates that you want to search between.</li></ol>
Files Created Between	Beginning and ending dates for the timeframe of the creation of a file on the suspect system. <ol style="list-style-type: none"><li>1. Check the box.</li><li>2. In the date fields, enter the beginning and ending dates that you want to search between.</li></ol>
File Size Between	Minimum and maximum file sizes, specified in bytes. <ol style="list-style-type: none"><li>1. Check the box.</li><li>2. In the size fields, enter the minimum and maximum file size in bytes that you want to search between.</li></ol>
Save as Default	Check this box to make your settings apply to all index searches.

Click *Search Now* when search criteria are prepared and you are ready to perform the search.

## DOCUMENTING SEARCH RESULTS

Once a search is refined and complete, it is often useful to document the results.

Right-click an item in the Search Results list to open the quick menu with the following options:

**Copy to Clipboard:** Copies the selected data to the clipboard (buffer) where it can be copied to another Windows application, such as an Excel (2003 or earlier) spreadsheet.

**Note:** The maximum number of lines of data that can be copied to the clipboard is 10,000.

**Export to File:** Copies information to a file. Select the name and destination folder for the information file.

Copy or export the hits and the statistics of a search result using the options on the following table:

**TABLE 9-10 Copy or Export Search Results**

<b>Option</b>	<b>Description</b>
All Hits in Case	Saves all the current search terms' hits found from the entire case.
All Hits in Search	Saves all the search hits found in each search branch.
All Hits in Term	(Live search only) saves the instances of individual terms found from the list of search terms.  For example, if a live search consisted of the list "black," "hole," "advent," and "horizon," this option would copy information on each of the terms individually.
All Hits in File	Records the instances of the search term in the selected file only.
All File Stats in Case	Creates a <b>.CSV</b> file of all information requested in the case.
All File Stats in Search	Creates a <b>.CSV</b> file of the information requested in the search.
All File Stats in Term	(Live search only) Creates a <b>.CSV</b> file of the instances of individual terms found from the list of search terms.

After the information is copied to the clipboard, it can be pasted into a text editor or spreadsheet and saved. Choose *Export to File* to save the information directly to a file. Specify a filename and destination folder for the file, then click *OK*

Search results can then be added to the case report as supplementary files.

**Important:** With FTK 3.0, when exporting Index Search result hits to a spreadsheet file, the hits are exported as a .csv file in UTF-16LE data format. When opening in Excel, use the Text to Columns function to separate the Index Search hit values into columns.

## USING COPY SPECIAL TO DOCUMENT SEARCH RESULTS

The Copy Special feature copies specific information about files to the clipboard.

To copy information about the files in your search results:

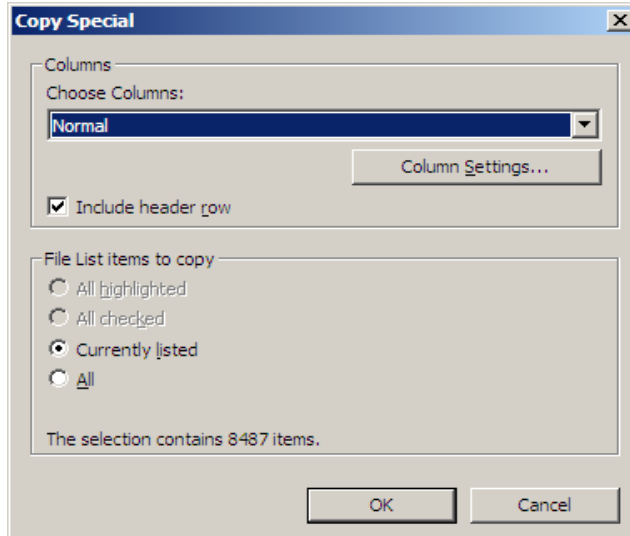
1. Click in the search results list.
2. From the Menu Bar, Select *Edit > Copy Special*.

OR

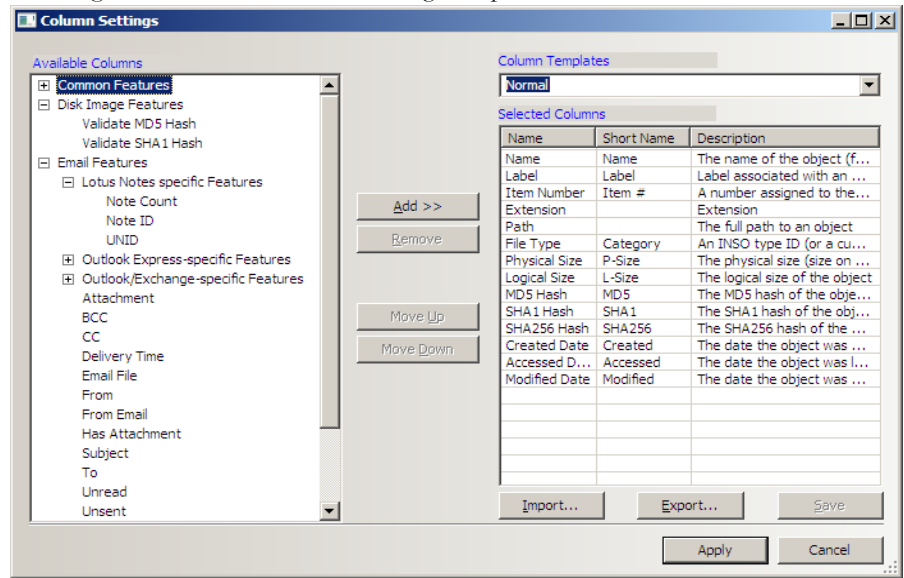


- 2a. Find that file highlighted in the File List view.
- 2b. Right-click on the desired file.
- 2c. Select *Copy Special*.

Figure 9-9 *Copy Special Options*



3. Choose the column settings template to use from the drop-down list. Click *Column Settings* to define a new column settings template.



- 3a. Modify the column template in the Column Settings Manager. For more information on customizing column templates, see “Customizing File List Columns” on page 268.
- 3b. Click Apply to return to the Copy Special dialog.
4. Select the customized column template if you created one.
5. Choose whether you want to include the header row in the file.
6. Under File List Items to Copy, select the option that best fits your needs:
  - *All Highlighted* to copy only the items currently highlighted in the list.
  - *All Checked* to copy all the checked files in the case.
  - *Currently Listed* to copy only currently listed items.
  - *All* to copy all items in the case.
7. The dialog states the number of files that your selection contains. If this meets your approval,
8. Click OK.

## BOOKMARKING SEARCH RESULTS

To keep track of particular search results, add them to new or existing bookmarks. Bookmarks of the search results in the file list can be created or added to an existing bookmark as with any other data.

To create a bookmark from the file list:

1. Select the files you want to include in the bookmark.
2. Right-click any of the selected files then choose *Create Bookmark*.
3. Complete the Create New Bookmark dialog.  
For more information, see “Creating a Bookmark” on page 151.
4. Click *OK*.

The bookmark now appears in the Bookmark tab.



## Chapter 10 Using Filters

AccessData FTK can filter files by their metadata to find specific evidence. For example, FTK can filter a large number of graphics by creation date to see only those created on the suspect machine during a certain time frame.

**Note:** Filters do not work on the Volatile tab.

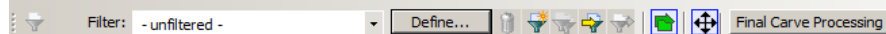
The interface for the Filter function is intended to work as a handy side-utility. It can be dragged to any part of the screen and used at any time.

### THE FILTER TOOLBAR

The Filter toolbar contains the tools you need to create and manage filters for viewing your case data.

Below is a graphic of the Filter toolbar:

*Figure 10-1 Filter Toolbar*



For an explanation of the filter toolbar and its components, see “Toolbar Components” on page 45.

## USING FILTERS

Use predefined filters, create your own, or edit filters to make them more general or more precise to fit your needs.

## PREDEFINED FILTERS

FTK contains the following predefined filters:

**TABLE 10-1** Predefined Filters

---

<b>Filter</b>	<b>Description</b>
Actual Files	Shows the actual files, as opposed to All Files. All Files is the default and includes metadata, OLE files, and alternate data stream files.
Alternate Data Streams	Shows files with alternate data streams (additional data associated with a file object).
Archive Files	Shows only archive-type file items, such as <b>.Zip</b> and <b>thumbs.db</b> .
Bad Extension Files	Shows only the files with extensions that don't match the file header.
Bookmarked	Shows only the items that are contained in a bookmark.
Carved Files	Shows only the items that have been carved.
Checked Files	Shows only the items that you have selected with a checkmark.
Decrypted Files	Shows only the items that have been decrypted by AccessData tools within the case. This indicates that FTK has had control of this file and its decryption since it was added to the case in its original encrypted form.
Deleted Files	Shows only those items that have the deleted status.
Duplicate Files	Shows only one instance of all duplicate items.
Email Attachments	Shows all email items that are not email messages.
Email Files	Shows only those items that have the email status.
Email Files and Attachments	Shows all email items, both messages and attachments.
Encrypted Files	Shows only those items flagged as EFS files or other encrypted files.
Evidence Items	Shows all evidence items added to the case.

**TABLE 10-1 Predefined Filters**

---

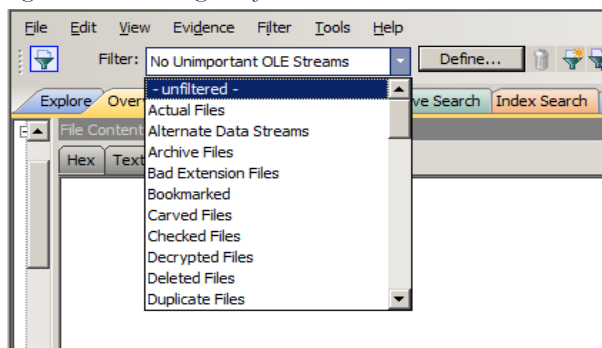
<b>Filter</b>	<b>Description</b>
Files with Alternate Data Streams	Shows files that contain Alternate Data Streams (additional data associated with a file system object).
Flagged Ignorable	Shows only those items you have identified as Ignorable.
Flagged Privileged	Shows only those items you have identified as Privileged.
Folders	Shows only folder items.
From Free Space	Shows only those items found in (carved from) free space.
From Recycle Bin	Shows only those items taken from the recycle bin.
Graphic Files	Shows only those items that have been identified as graphics.
Indexed	Shows items that have been indexed.
KFF Alert Files	Shows all files with KFF Alert status that are in a case.
KFF Ignore Files	Shows all files with KFF Ignore status that are in a case.
Labeled Files	Shows files that have a Label assigned to them.
Microsoft Office Files	Shows Word, Access, PowerPoint, and Excel files.
Mobile Phone: Call	Shows call information acquired from a mobile phone.
Mobile Phone: Contact	Shows contact information acquired from a mobile phone.
Mobile Phone: Event	Shows event information acquired from a mobile phone.
Mobile Phone: SMS	Shows SMS information acquired from a mobile phone.
Mobile Phone Files	Shows files and data from mobile devices added to the case using AccessData Mobile Phone Examiner.
No Deleted	Shows all except deleted items.
No Duplicate	Shows all except duplicate items.
No File Slack	Shows all except files found in (carved from) file slack.
No Files with Duplicates	Shows only files that have no duplicates in the case.
No KFF Ignore Files	Shows all items except KFF ignore files.
No KFF Ignore or OLE Subitems	Shows all items except KFF ignore files or OLE subitems.
No KFF Ignore or OLE Subitems or Duplicates	Shows all items except KFF ignore files, OLE subitems, or duplicate items.
No OLE Subitems	Shows all items except OLE subitems.
No Unimportant OLE Data Streams	Shows all items including OLE subitems, except that unimportant OLE data streams are not shown.
Not Flagged Ignorable	Shows all items except those you indicated Ignorable.

**TABLE 10-1 Predefined Filters**

Filter	Description
Not Flagged Privileged	Shows all items except those you flagged Privileged.
OLE Subitems	Shows only OLE archive items and archive contents.
Reclassified Files	Shows only those items whose classification you have changed.
Registry Files	Shows Windows 9x, NT, and NTFS registry files.
Thumbs.db Files	Shows <b>Thumbs.db</b> files.
Unchecked Files	Shows only those items that you have not checked.
Unimportant OLE Stream Categories	Shows only Unimportant OLE Stream Categories
Unimportant OLE Streams	Shows only Unimportant OLE Streams
User-decrypted Files	Shows only those items that you have decrypted and added to the case. Decrypted by User status is always applied to filed added using the Add Decrypted Files feature. FTK cannot confirm validity, content, or origin of such files.
Web Artifacts	Shows HTML, <b>Index.dat</b> , and empty <b>Index.dat</b> files.

To apply an existing filter, use the Filter drop-down list on the Filter toolbar, shown below. Click to select the desired filter. Click the *Filter* button to the left of the Filter drop-down to toggle the filtered view on or off.

*Figure 10-2 Selecting a Defined Filter*





# CUSTOMIZING FILTERS

## CREATING A FILTER

You can create or modify your own filters. These custom filters are saved with the case in which they were created. You can create a filter from scratch, copy an existing filter to use as a basis for a new filter, export a filter to an `.xml` file, and import a filter that has been exported/saved to `.xml` format.

Filters consist of a name, a description, and as many rules as you need. A filter rule consists of a property, an operator, and one or two criteria. (You may have two criteria in something like a date range.)

To create a new filter, do the following:

1. Click *Filter > New*, or click the *New Filter* button on the Filter toolbar.



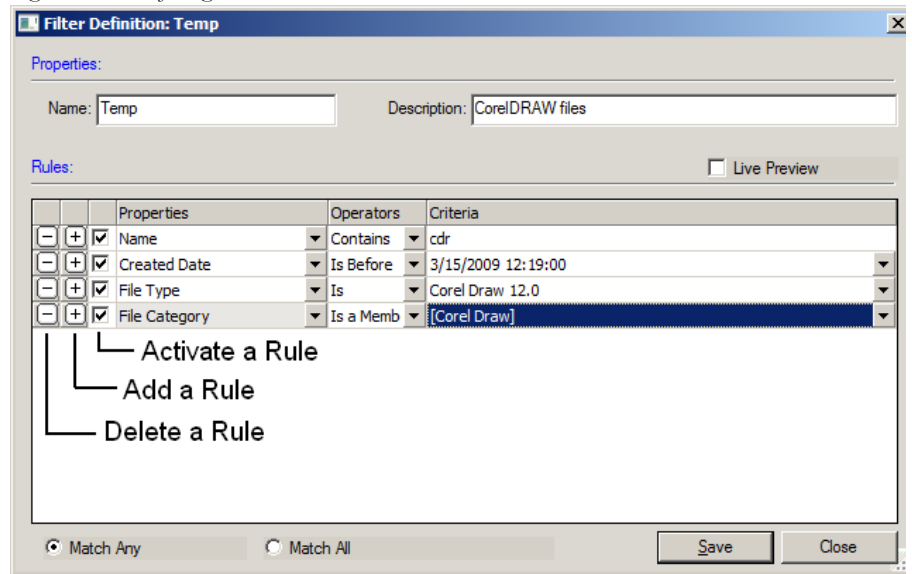
2. Type a name and a short description of the filter.
3. Select a property from the drop-down menu.
4. Select an operator from the Properties drop-down menu.
5. Select the applicable criteria from the Properties drop-down menu.  
Each property has its own set of operators, and each operator has its own set of criteria. The possible combinations are vast.
6. Select the *Match Any* operator to filter out data that satisfies any one of the filter rules or the *Match All* operator to filter out data that satisfies all rules of the filter.
7. Click *Save*.

You can test the filter without having to save it first. Check the Live Preview box to test the filter as you create it.

## REFINING A FILTER

As your investigation progresses, you will become more familiar with patterns and file types in the case and can adjust your filters to find this specific data

Figure 10-3 Refining a Filter.



To modify an existing filter:

1. Select the filter to modify from the Filter drop-down list.
2. Click *Define*.
3. To make your filters more precise, click the Plus (+) button to add a rule, or the Minus (–) button to remove one.
4. When you are satisfied with the filter you have created or modified, click *Save*, then *Close*.
5. Select the newly created filter from the Filter drop-down in the toolbar to apply it.

## EXPORTING A FILTER

Filters can be exported for use in other cases. The name of the filter cannot have any special or invalid characters or the export will not work.

## DELETING A FILTER

You can delete a custom filter if you no longer need it. Predefined system filters cannot be deleted.

To delete a filter:

1. Select the filter you want to delete from the Filter drop-down menu list.
2. Click *Filter > Delete*

**OR**

Click the *Delete Filter* button on the Filter toolbar .

3. Confirm the deletion.

## USING THE KNOWN FILE FILTER

The Known File Filter (KFF) uses a collection of hash values of known files used to filter the files found in the evidence. When you add evidence to the case, you can compare all the files in the case to the hash values contained in the KFF Library database.

FTK records the hashes of the files it discovers in the evidence in order to demonstrate that the files have not been modified and to quickly determine if two files have the same contents.

FTK computes the hash based on the contents of the file only. Attributes such as filename and time stamp do not affect the hash computed, nor are they affected by the hashing of the file.

## A CLOSER LOOK AT THE ACCESSDATA KFF LIBRARY

### KFF LIBRARY SOURCES

This section includes a description of the hash collections that make up the AccessData KFF Library.

All of the hash sets currently within the KFF come from one of three federal government agencies:

- NDIC HashKeeper
- NIST NSRL
- DHS

Use the following rules of thumb to identify the origin of any hash set within the KFF:

1. All HashKeeper Alert sets begin with “ZZ”, and all HashKeeper Ignore sets begin with “Z”. (There are a few exceptions. See below.) These prefixes are often followed by numeric characters (“ZZN\*” or “ZN\*” where N is any single digit, or group of digits, 0-9), and then the rest of the hash set name. Here are two examples of HashKeeper Alert sets: “ZZ00001 Suspected child porn” and “ZZ14W”. Here’s a HashKeeper Ignore set: “Z00048 Corel Draw 6”.
2. The NSRL hash sets do not begin with “ZZN\*” or “ZN\*”. In addition, in the FTK 3.0 KFF, all the NSRL hash set names are appended (post-fixed) with multi-digit numeric identifier. This is discussed later in this chapter.
3. The DHS collection is broken down as follows:
  - In FTK 1.81.4 there are two sets named “DHS-ICE Child Exploitation JAN-1-08 CSV” and “DHS-ICE Child Exploitation JAN-1-08 HASH”.
  - In FTK 3.0 there is just one such set, and it is named “DHS-ICE Child Exploitation JAN-1-08”.

Once an investigator has identified the vendor from which a hash set has come, he/she may then need to consider the vendor’s philosophy on categorizing hash sets, and the methods used by the vendor to gather hash values into sets, in order to determine the relevance of Alert (and Ignore) hits to his/her case. The following commentary on each of the three vendors should assist the investigator in making these considerations.

## NDIC/HASHKEEPER

NDIC’s HashKeeper collection uses the Alert/Ignore designation. The Alert sets are hash values contributed by law enforcement agents working in various jurisdictions within the US - and a few that apparently come from Luxemburg. All of the Alert sets were contributed because they were believed by the contributor to be one form of child pornography or another. The Ignore sets within HashKeeper are computed from files belonging to application software.

During the creation of the KFF, AccessData staff retains the Alert and Ignore designations given by the NDIC, with the following exceptions. AccessData labels the following sets Alert even though HashKeeper had assigned them as Ignore: “Z00045 PGP files”, “Z00046 Steganos”, “Z00065 Cyber Lock”, “Z00136 PGP Shareware”, “Z00186 Misc Steganography Programs”, “Z00188 Wiping Programs”. The names of these sets may suggest the intent to conceal on the part of the suspect, and AccessData marks them Alert with the assumption that investigators using AccessData products would want to be “alerted” to the fact that data obfuscation or elimination software had been installed/loaded by the suspect. NIST NSRL

The NIST NSRL collection is being actively expanded. See its website: <http://www.nsrl.nist.gov/index.html>. This collection is much larger than HashKeeper in terms of the number of sets and the total number of hashes. It is composed entirely of hash sets being generated from application software. So, all of its hash sets are given Ignore status by AD staff except for those whose names make them sound as though they could be used for illicit purposes.

The NSRL collection divides itself into many sub-collections of hash sets with similar names. In addition, many of these hash sets are “empty”, i.e. they are not accompanied by any hash values. The size of the NSRL collection, combined with the similarity in set naming and the problem of empty sets, gives AccessData motive to take a certain liberty in modifying (or selectively altering) NSRL’s own set names to remove ambiguity and redundancy.

In previous FTK 2.x releases, the NSRL sets can be identified as those that don’t start with “Z” or “ZZ” in the manner of HashKeeper. Lastly, please note that, according to <http://www.nsrl.nist.gov/nsrl-faqs.html#faq17>, the NSRL team does not install the software packages that they hash. They run the installer programs for those packages through their own tools that decompress and extract the individual files, and then compute hash values on the extracted files. This is not a foolproof method for isolating files.

Find contact info at <http://www.nsrl.nist.gov/Contacts.htm>.

## DHS

The DHS collection is new to AccessData. It is being released for the first time with FTK 1.81.4 and FTK 3.0. The DHS sets are marked Alert in both 1.81.4 and 3.0.

## IMPORTING KFF HASHES

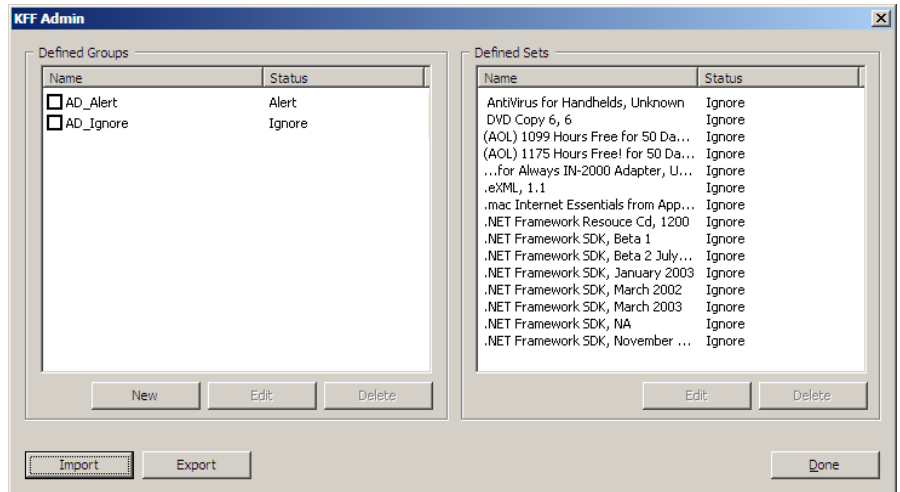
When using the Import KFF Hashes feature, you can import hashes from several supported formats.

To import hashes to the KFF database:

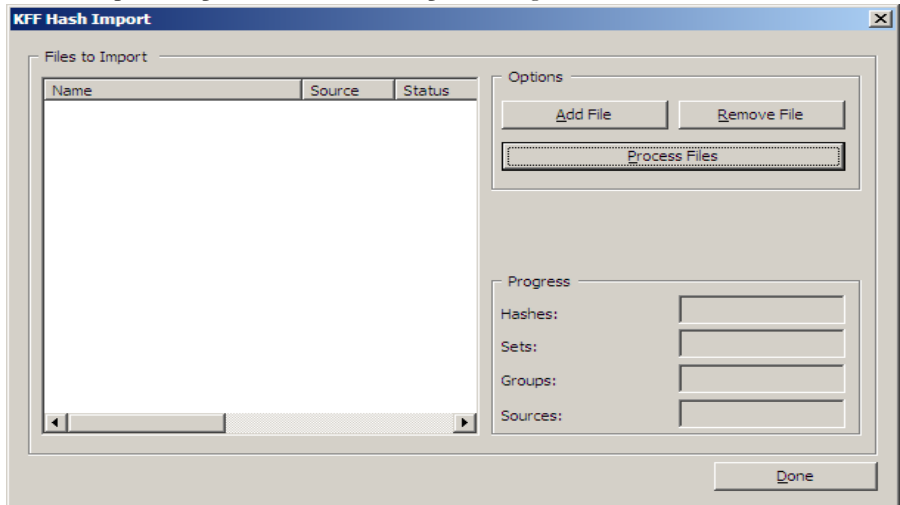
1. Click *Tools > KFF > Manage* to open the KFF Administration dialog.

**Note:** Both the AD Alert group and the AD Ignore group are marked by default.

Figure 10-4 KFF Administration



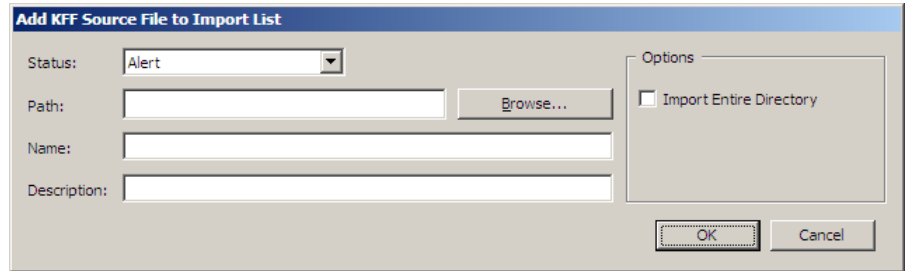
2. Click *Import* to open the KFF Hash Import dialog.



3. Click *Add File* and select one of the following file types:

- AccessData Hash Database (.hdb)
- FTK Imager Hash List (.csv)
- Hashkeeper Hash Set (.hke, hke.txt)
- Tab Separated Value (.tsv)

- National Software Reference Library (.nsrl)
- Hash (.hash)
- FTK(.KFF)



- 3a. Click the Status drop-down list to select either Alert or Ignore status for the list you are importing.
- 3b. Browse to the path where the new source file is found.
- 3c. Type a name for the new source.
- 3d. Include a description of the new source file.
- 3e. Mark the *Import Entire Directory* box if all the files in the source path are to be included in this import.
- 3f. Click *OK* to close this dialog and return to the KFF Hash Import dialog keeping the new source files, or click *Cancel* to close this dialog without adding the new source files.
4. Close the dialogs back to the KFF Administration dialog. Verify the information, and click *Import*. The imported hash set is merged into the existing hash set and saved.
 

**Note:** Duplicate hashes are not added.

## EXPORTING KFF HASHES

To export a KFF hash file, follow these steps:

1. Click *Tools > KFF > Manage*.
2. Click *Export*.
3. Select the location to which you want to save the exported KFF file. FTK saves the file as *.kff* by default.
4. Click *Save*.

## UNDERSTANDING HOW THE KFF DATABASE IS USED

FTK divides hashes into three tables: AccessData, Case Specific, and Shared.

**TABLE 10-2 Hash Tables**

---

Table	Description
AccessData	These tables contain the hashes, sets, and groups which are distributed with FTK. You can create groups from these sets, but the sets are read-only.
Case Specific	Create your own sets and groups. You should create non-case specific hash sets and groups here.
Shared	Sets or groups in these tables are accessible to anyone using the same KFF database instance (cases are stored in the same Oracle <sup>*</sup> database). Groups in these tables may include sets from the AccessData or shared tables but not from the case specific tables.

When setting the status of sets or groups it is important to be mindful of other examiners or cases which may be using the KFF database. Remember that all cases will have access to the AccessData and user tables so if you want to adjust statuses for your case without interfering with other investigations, you should create case specific sets or groups.

## STORING HASHES IN THE KFF DATABASE

The KFF database organizes hashes into sets and groups.

A **set** represents a related collection of hashes. For example, a group of hashes from a particular case, from a particular provider such as NIST, or from a particular known program.

A **group** represents a collection of related sets. For example, legitimate software, known child pornography, or known hacker tools.

Sets and groups allow examiners to rapidly specify to which type of files they want to be alerted, to more easily comply with search warrant limitations by rapidly disregarding files outside the warrant, to eliminate useless information from the case, reducing the data set that needs analysis, and to make the KFF more manageable and easier to use.



Each set or group is assigned a status so that FTK can respond when it encounters hashes that belong to the set or group.

Assign any of the following statuses to a set or group:

**TABLE 10-3 Set or Group Statuses**

---

<b>Status</b>	<b>Description</b>
Alert	Selecting this status indicates that you want to be alerted to the existence of any matching file in the set or group.
Disregard	This case specific status allows you to avoid violating search warrant limitations. You can mark a group with the disregard status to treat any matching files as if they were unknown. The files will still be indexed, carved, and can be searched, but they will not automatically alert you to their presence in the suspect's drive image.
Ignore	This status is used to identify files that are without forensic significance (known software packages or shared DLLs, for example). When you have chosen to add KFF Ignorable files to the case, utilizing this status allows the FTK to sift these uninteresting files away from view.

The group's status supersedes the statuses of any of its sets, but does not actually change the sets' statuses. You can manually change the status of thousands of sets that don't apply to your case, or you can simply organize all of those sets into related groups and change each group's status. Any time you dissolve a group, each set in that group retains the status it had prior to forming the group.

Only groups are analyzed. The two default groups: Alert and Ignore update dynamically as a user modifies sets.

If you include the same set in two different groups, FTK prioritizes the status and returns the highest priority status as follows:

1. Alert
2. Ignore
3. Disregard

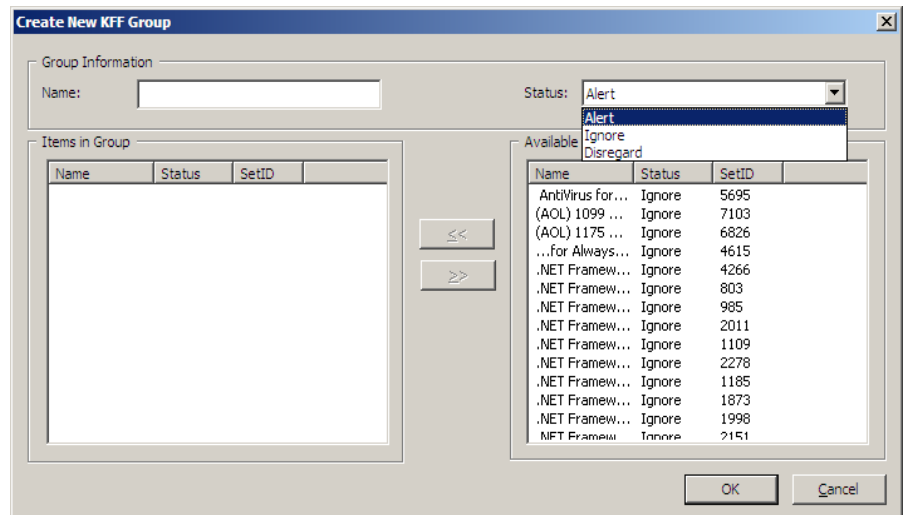
## CREATING SETS AND GROUPS

The toolkit also provides a mechanism for you to add your own hashes to the KFF database. When you select a hash set inFTK, generally, the source reporting agency is displayed in a text box.

**Note:** It is good practice when creating sets to put your own agency in the source field so that other examiners know where the hashes came from.

To create sets and organize them into groups, follow these steps:

1. Select *Tools > KFF > Manage*.
2. Click *New*.



3. Name the group.
4. Assign the group a status.
5. Select the sets you want in the group from the Available Sets list and move them to the Items in Group list by clicking the double-arrow button.
6. Click *Apply* to create the group without closing the Create New KFF dialog.
7. Click *OK* to save the group and close.

# *Chapter 11 Decrypting EFS and Other Encrypted Files*

Windows 2000, XP Professional, 2003, and Vista include the ability to encrypt files and folders. AccessData FTK can break file encryption so that additional evidence can be uncovered.

This section contains the information that allows you to understand the Encrypting File System (EFS) and how FTK breaks the encryption.

## **UNDERSTANDING EFS**

EFS is built in to Windows 2000, XP Professional, 2003, and Vista. It is not supported in Windows XP Home Edition.

In Windows, 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 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.

**Important:** When a user marks an encrypted file as privileged and that file is later decrypted, all associated data with the newly decrypted file are able to be found in an index search as hits. When a user attempts to view the hits in a different list, an error is displayed that the path is invalid.

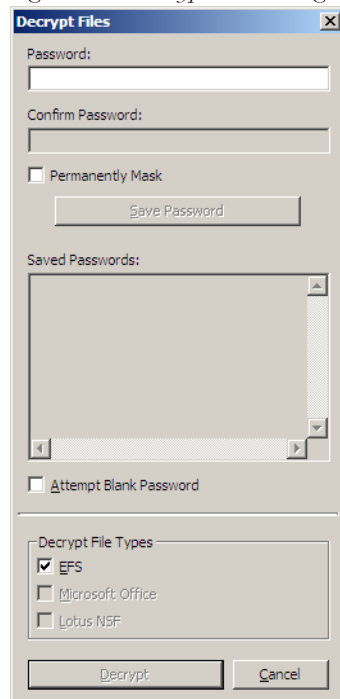
## DECRYPTING EFS FILES AND FOLDERS

AccessData FTK 3.0 is designed to decrypt EFS, Microsoft® Office, and Lotus® Notes (NSF) files and folders. To do so, the password must already be known.

To find the passwords, export encrypted files and add them as jobs in PRTK or DNA. When passwords are found, you are ready to decrypt the encrypted files in .

Click *Tools > Decrypt Files* to begin decryption. The following sections review the requirements to decrypt EFS files on Windows systems.

Figure 11-1 Decrypt Files Dialog



To use the decryption menu, do the following:

1. Type a password in the Password box.
  - 1a. Confirm the password by typing it again in the Confirm Password box
2. Mark *Permanently Mask* to display the password in the Saved Passwords list as asterisks, hiding the actual password.
3. Click *Save Password* to save the password into the Saved Password List.

4. Mark *Attempt Blank Password* to decrypt files with no password, or whose password is blank.

**Note:** FTK 3.0 will automatically detect encrypted files in the case. Decrypt File Types will automatically be marked according to the file types found. Unselect any file types you wish not to decrypt.

5. Click *Decrypt* to begin the decryption process.

**Note:** The *Decrypt* button is disabled until at least one password is entered, or until *Attempt Blank Password* is marked.

Click *Cancel* to return to the case.

## DECRYPTING WINDOWS EFS FILES

Windows 2000, XP Professional, 2003, and Vista include the ability to encrypt files and folders through the Encrypting File System (EFS). AccessData FTK can break file encryption so that additional evidence can be uncovered.

### UNDERSTANDING EFS

EFS is built in to Windows 2000, XP Professional, 2003, and Vista. It is not supported in Windows XP Home Edition.

EFS can be used to encrypt files or folders. Within Windows, 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.

There are certain files that cannot be encrypted, including system files, NTFS compressed files, and files in the [drive]:\[Windows\_System\_Root] and its subdirectories.

**Note:** All EFS decryption requires either the user's or the Recovery Agent's password.

### WINDOWS 2000 AND XP SYSTEMS PRIOR TO SP1

FTK automatically decrypts EFS files on Windows 2000 prior to Service Pack 4 and Windows XP systems prior to Service Pack 1. Simply select the *Decrypt EFS Files* option when adding evidence to a case and FTK uses PRTK technology to decrypt the EFS files.

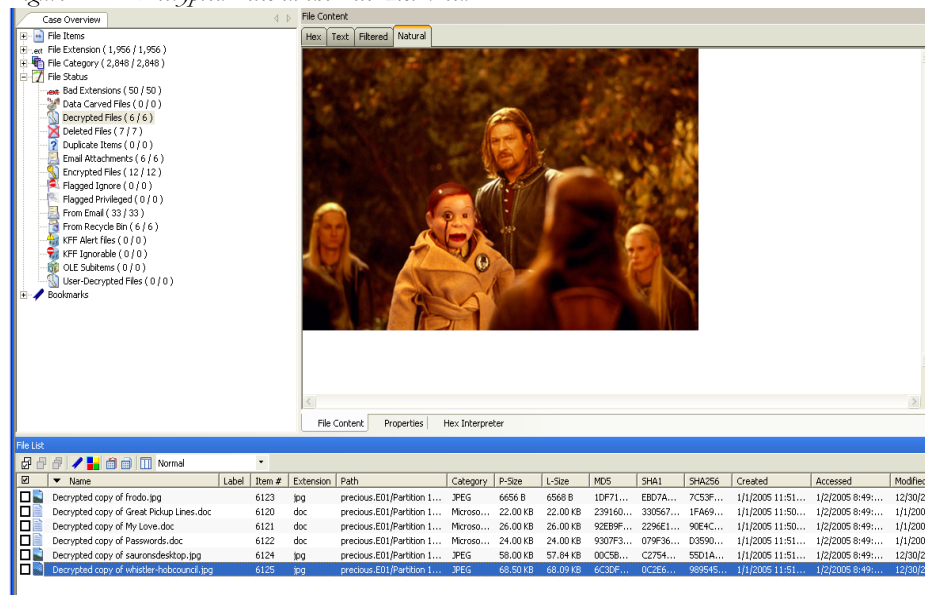
## WINDOWS XP SP1 OR LATER

For systems running Windows XP Service Pack 1 or later, or Windows 2000 Service Pack 4 or later, FTK needs the user's or the Recovery Agent's password before it can decrypt EFS files.

## VIEWING THE DECRYPTED FILES

The decrypted files are displayed in the Overview tree, in the *File Status > Decrypted* container. Click on an individual file in the File List to view the file in the File Content pane.

Figure 11-2 Decrypted Files in the File List View



**Note:** Regardless of the encryption type, once decrypted, the files will appear in the File List Name column as “Decrypted copy of [filename],” as seen in the following figure:

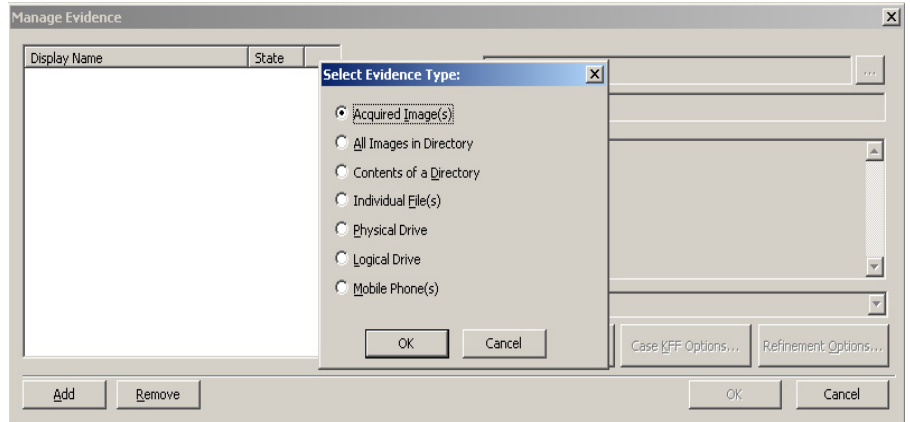
## DECRYPTING DOMAIN ACCOUNT EFS FILES FROM LIVE EVIDENCE

The following steps describe how to decrypt and view EFS files taken from live evidence:

1. Create a new case with no evidence added.

2. In the main menu, click *Evidence > Add/Remove*.
3. Click *Add*.

Figure 11-3 Add / Remove Evidence

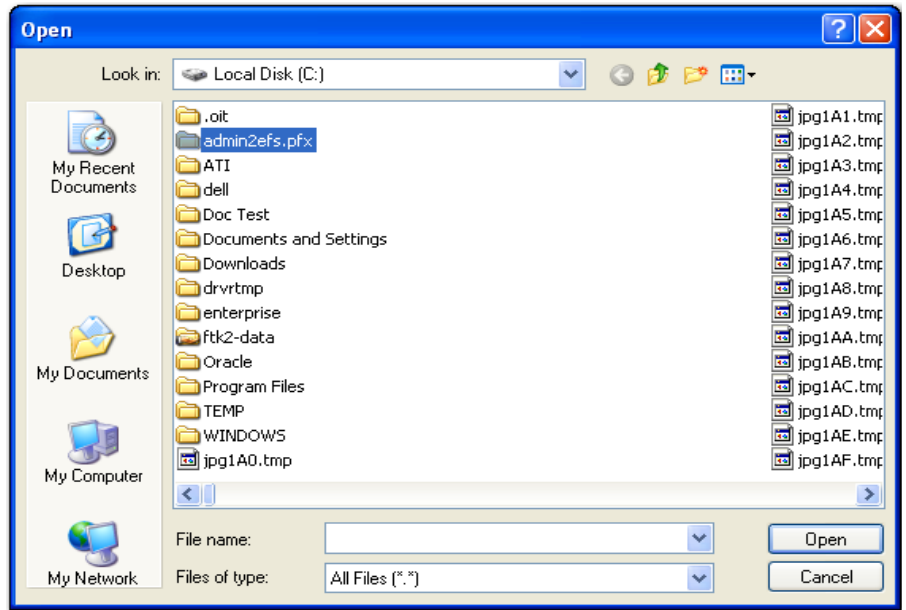


4. Select *Individual File(s)* and click *OK*.
5. Navigate to the PFX file (domain recovery key).

**OR**

Type the file's full path including the filename into the File Name field of the Open dialog.

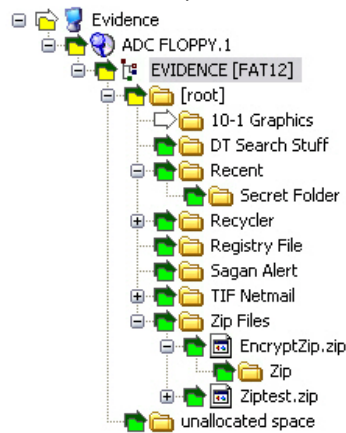
Figure 11-4 The Open Dialog



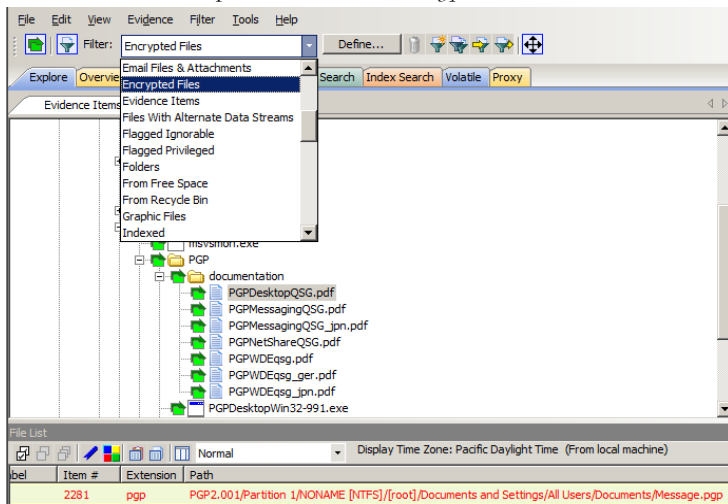
6. Click *Open*.
7. Click *No* when asked if you want to create an image of the evidence you are adding.
8. Select the proper time zone for the PFX file from the Time Zone drop-down list in the Manage Evidence Dialog.
9. Click *OK*.
10. FTK begins processing the PFX file and the progress dialog appears.
11. Remote Preview (Add Remote Data) the computer that contains the EFS files you want to decrypt or view (you can also preview multiple machines simultaneously).
12. In the Explore Tab navigate to the desired drive or drives.



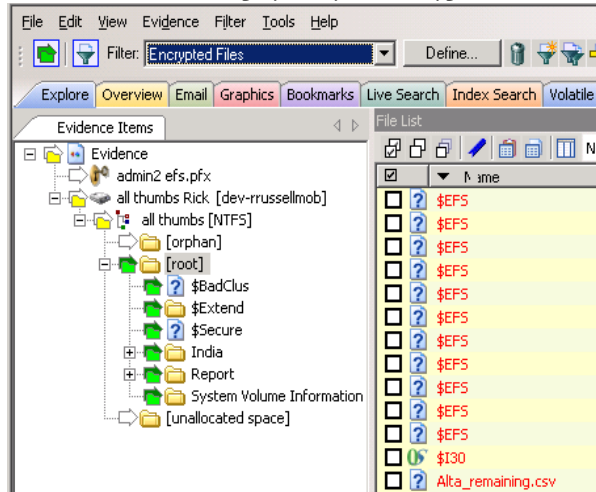
13. Use *Quick Picks* on the [ROOT] folder of the target system. This shows the evidence items on that system.



14. In the Filter drop-down list, click *Encrypted Files*.

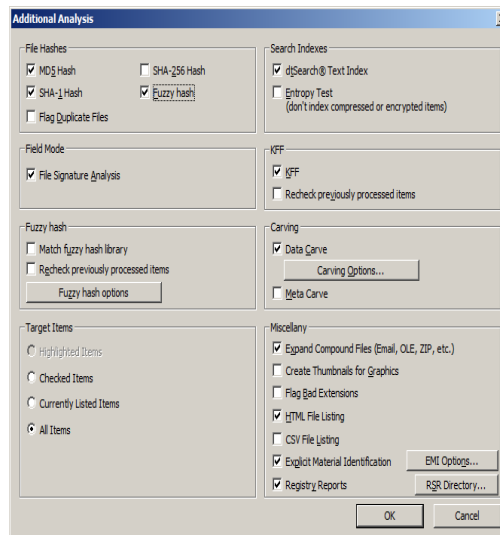


The file list now displays only the encrypted files found on the target system.



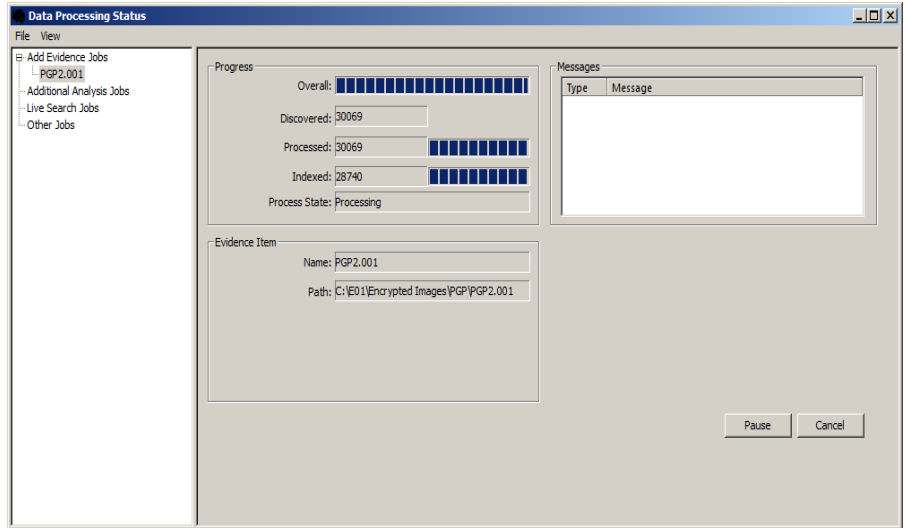
15. From the main menu, select *Evidence > Additional Analysis*.
16. In the Additional Analysis window, select *Listed Items* and *File Signature Analysis*.
17. Click *OK*.

Figure 11-5 Choosing File Signature Analysis for EFS Decryption



The Data Processing Status dialog appears. A blue bar indicates status and activity.

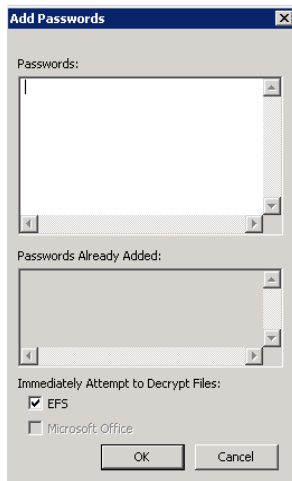
Figure 11-6 Data Processing Status



When all items are added to the queue, a checkmark to the left of the process bar indicates that the process was completed successfully

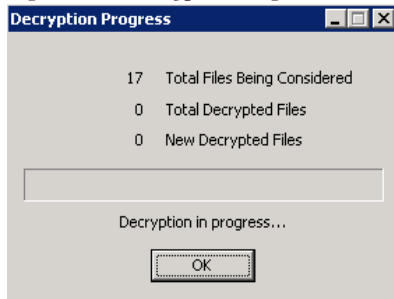
18. When all processing has completed, go to the main menu and click *Tools > Decrypt Files*.
19. In the Add Passwords window, enter <EFS recovery password(s)> in the Passwords text box. Select the *EFS* checkbox (if not selected by default), and click *OK*.

Figure 11-7 Add Passwords Dialog



FTK begins to decrypt the files and a decryption process dialog appears.

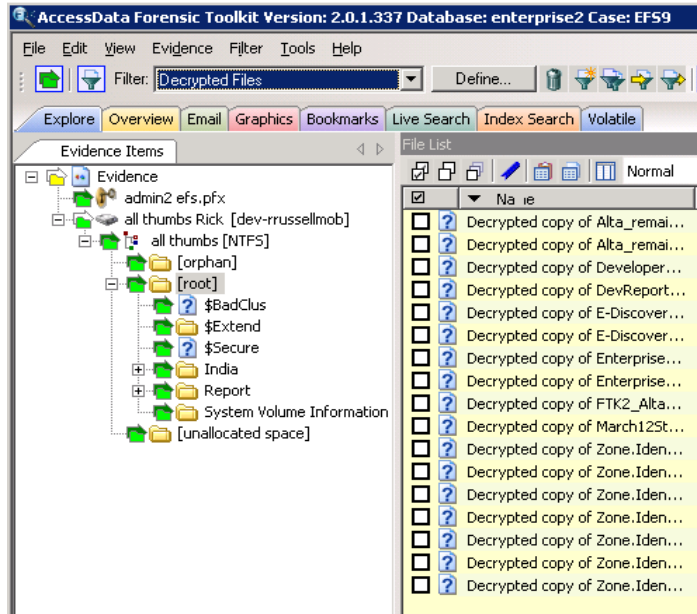
Figure 11-8 Decryption Progress Screen



20. When decryption completes, click *OK*.
  21. Apply *Quick Picks* on the [ROOT] folder of the target system.
  22. Select the files you want to view.
    - To view only the decrypted files, choose *Decrypted* files in the Filter drop-down list.
    - If you want to see all files (not just decrypted files), choose *-unfiltered-* from the Filter drop-down list.
  23. Click *OK* to close the dialog. Decryption will continue.
- Note:** When completed, decrypted files will appear in the File List Name column as “Decrypted copy of <file name>.”

The following graphic illustrates the File List view of decrypted files:

Figure 11-9 Viewing Decrypted Files using the Filter Drop-down List



## DECRYPTING CREDANT FILES

Credant encryption is file-based and works much like EFS. Process drives with Credant encryption normally. The Credant Decryption option in the tools menu is unavailable unless the image contains Credant encryption.

The integration with FTK allows two options for decryption: offline, and online. For a key bundle located on the user's local machine or network, use the offline option. For a key bundle located on a remote server use the online option.

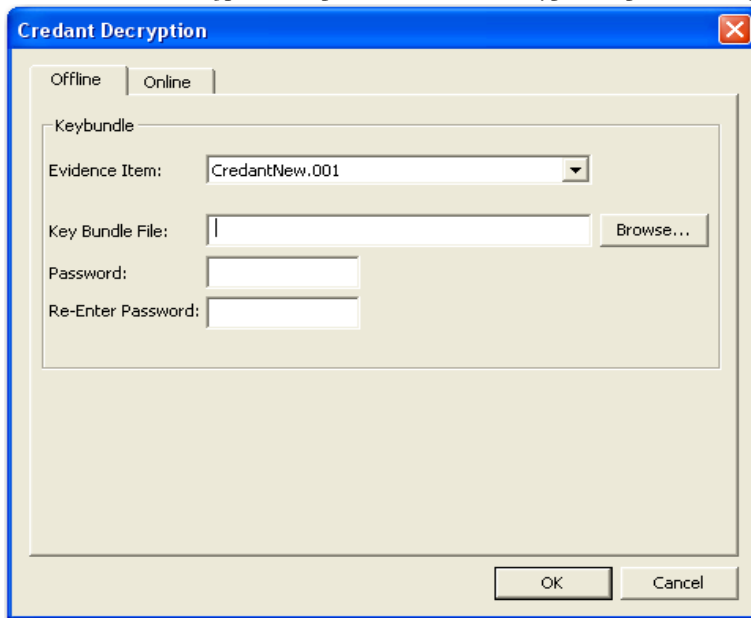
**Important:** If you click *Cancel* to process the evidence without decrypting, you will not be able to decrypt at a later time. You will have to create a new case to decrypt and process this evidence

Click *Tools > Credant Decryption* to open the Credent decryption options, as displayed in the figures that follow below.

## USING AN OFFLINE KEY BUNDLE

Offline decryption is a quicker and more convenient option if the key bundle can be placed on the investigator's local computer. Perform the following steps to decrypt an encrypted image offline: select the key bundle file and enter the password used to decrypt it. This is detailed in the following steps:

1. Click *Tools > Decryption* to open the Credant decryption options dialog.

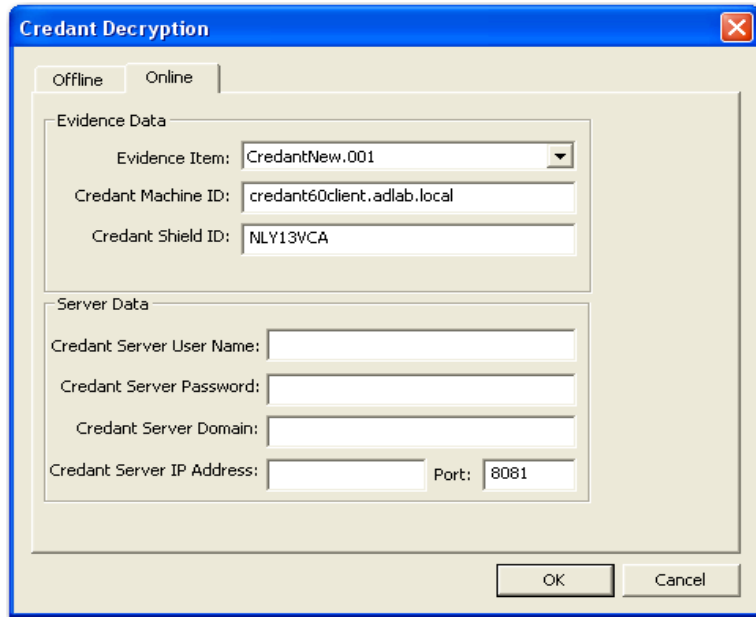


2. Select the key bundle file by entering its location or browsing to it.
3. Enter the password.
4. Re-enter the password.
5. Click *OK*.

## USING AN ONLINE KEY BUNDLE

Online decryption can occur only when the machine processing the image can directly access the server over the network. The following figure displays the online tab:

Figure 11-10 Decryption Online Tab Options



Usually FTK auto-populates the *Machine ID* and *Shield ID* fields. The *Machine ID* can be found on the server as the *Unique ID* on the *Properties* tab. The *Shield ID* can be found as the “Recovery ID” on the “Shield” tab. It looks similar to this: “ZE3HM8WW”.

The Server Data group box contains information on how to contact the server. It includes the Credant Server user name, password, and IP address. The port should be 8081, and is auto-populated.

Offline decryption requires you to get a key bundle file from the server. Then select the key bundle file and enter the password used to decrypt it. Get the key bundle file by executing the `CFGetBundle.exe` file with a command like that looks like this:

```
CFGetBundle -Xhttps://10.1.1.131:8081/xapi -asuperadmin -Achangeit  
-dpx1.accessdata.lab -sZE3HM8WW -oKeyBundle.bin -ipassword
```

-X for the server address

-a for administrator name

-A for the administrator password

-d for the Machine ID

-s for the Shield ID

-o for the output file

-i for the password used to encrypt the keybundle

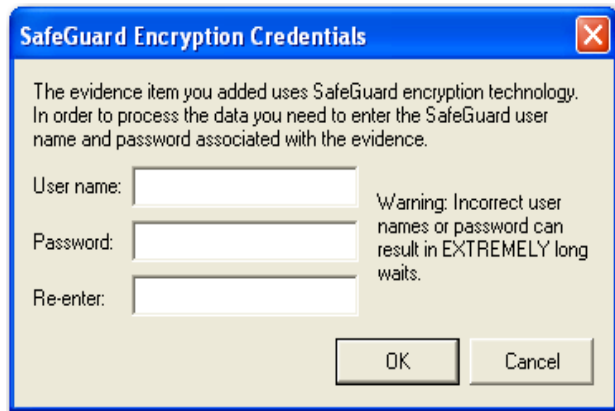
**Note:** All command line switches are case sensitive. Also, as in the example above, there is no space between the switch and the datatype.

Once you have used either the online or the offline method, the files will be decrypted immediately and the decrypted file will become a child of the encrypted file. After decryption, the files will be processed with the same settings last used to process a file.

## DECRYPTING SAFEGUARD UTIMACO FILES

Safeguard Utimaco is a full-disk encryption program.

*Figure 11-11 Provide the Safeguard Encryption Credentials*



The Safeguard dialog box appears only when FTK 3.0 reads a valid Utimaco-encrypted image.

The username and password used to create the encrypted image are required for decryption. Once the credentials have been added, click *OK* to return to the Manage Evidence dialog. Select a time zone from the Time Zone drop-down, then click *OK* to begin processing.

**Important:** Type the User Name and Password carefully and verify both before clicking *OK*. If this information is entered incorrectly, FTK 3.0 checks the entire image for matching information before returning with an error message. Each wrong entry results in a longer wait.



**Important:** If you click *Cancel* to process the evidence without decrypting, you will not be able to decrypt at a later time. You will have to create a new case to decrypt and process this evidence

## DECRYPTING SAFEBOOT FILES

SafeBoot is a program that encrypts drives and/or partitions. When FTK 3.0 detects a SafeBoot-encrypted drive or partition, the following dialog is displayed.

Figure 11-12 *SafeBoot Encryption Key Entry*



The encryption key must be available to enter into the *Key* field. All recognized partitions are selected by default, up to a maximum of eight. You can unselect any partition you wish not to add to the case.

**Important:** If you click *Cancel* to process the evidence without decrypting, you will not be able to decrypt at a later time. You will have to create a new case to decrypt and process this evidence.

Once the key has been added and the appropriate partitions selected, click *OK* to return to the Manage Evidence dialog. Select a time zone from the Time Zone drop-down, then click *OK* to begin processing.

## DECRYPTING GUARDIAN EDGE FILES

When a GuardianEdge-encrypted image is added to FTK 3.0, FTK 3.0 automatically detects that it is a GuardianEdge image and a dialog will appear asking for credentials. The dialog has a drop-down list box with the user names that have been found to be associated with the image. Select the user name for which you have a password and then enter the password. Enter the password in one of two ways:

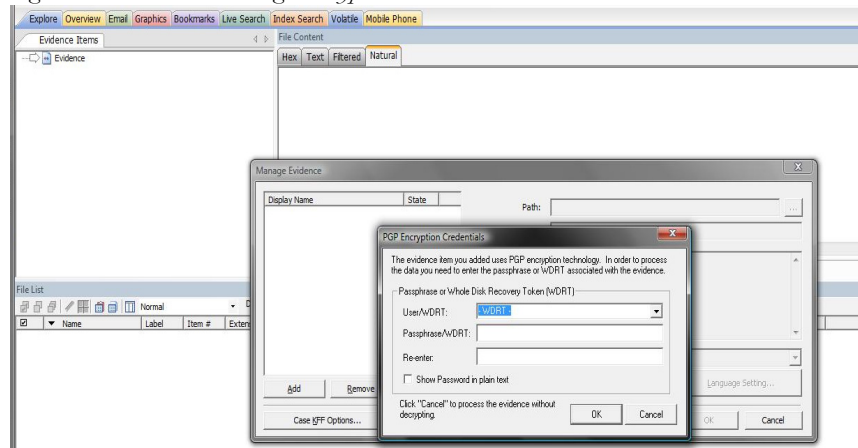
- Enter it twice with dots appearing for each character (if you don't want someone to see what it is)

**OR**

- Check the *Show in plain text* box and enter it once.

**Important:** If you click *Cancel* to process the evidence without decrypting, you will not be able to decrypt at a later time. You will have to create a new case to decrypt and process this evidence

Figure 11-13 Guardian Edge Decryption Credentials Box



## DECRYPTING AN IMAGE ENCRYPTED WITH PGP® WHOLE DISK ENCRYPTION (WDE)

FTK 3.0 now supports the processing of acquired images from disks that have been protected with PGP® Whole Disk Encryption. This section describes this support and the process of specifying the credentials necessary to decrypt the image. Note that decryption is only possible if an existing credential, such as a user passphrase or a previously-configured Whole Disk Recovery Token, is available

## ABOUT PGP® CORPORATION AND PGP® WHOLE DISK ENCRYPTION

PGP® Corporation's origins date back to the early 1990's, when Phil Zimmermann released his seminal encryption program, "Pretty Good Privacy." PGP® Corporation is now a world leader in encryption solutions, with products for securing email, network files, removable media, and hard disks, all centrally managed by the PGP® Universal™ Server console.

Individuals and organizations typically use PGP® Whole Disk Encryption (PGP® WDE) to protect the information on their laptop computers in case of loss or theft. Encrypted disks prompt for a user's passphrase before Windows loads, allowing data to be decrypted on the fly as it is read into memory or encrypted just before being written to disk. Disks remain encrypted at all times.

Administrators can instruct PGP® WDE devices that are managed by a PGP® Universal™ Server to automatically secure an encrypted disk to additional credentials based on a company's central policy. These could include a WDE Administrator key (for IT support purposes), an Additional Decryption Key (also called a corporate recovery key) and/or a Whole Disk Recovery Token ("WDRT"). WDRTs are commonly used to reset a forgotten passphrase and, in FTK 3.0, can also be used by authorized administrators or examiners to decrypt an acquired image of a PGP® WDE encrypted drive.

## PGP® WDE DECRYPTION IN FTK 3.0

FTK/FTK 3.0 support for PGP® WDE functions similarly to Access Data's support for other full-disk encryption products.

1. After creating a case, click *Evidence > Add Evidence > Acquired Image > Add*.
2. Browse to the location of the image files and select the first of the set to add to this case.
3. You may enter any user's boot password or passphrase, or use the Whole Disk Recovery Token (WDRT) to decrypt a drive or image.

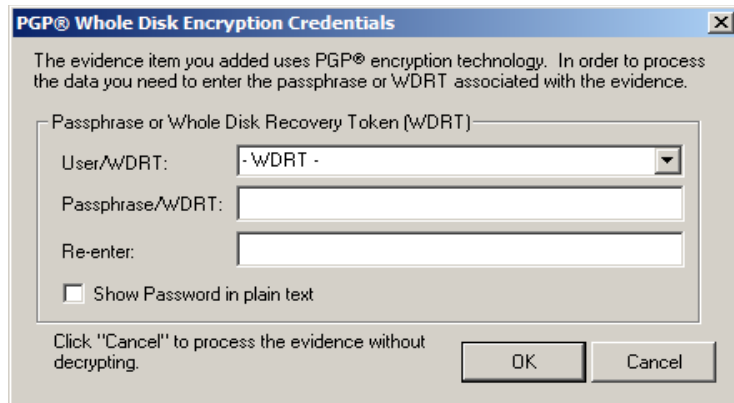
**Boot passwords:** The users for the drive are displayed in the drop-down list in the PGP® Encryption Credentials box. Select the user and enter that user's boot password.

**OR**

**Whole Disk Recovery Token (WDRT):** Obtain the WDRT by doing the following:

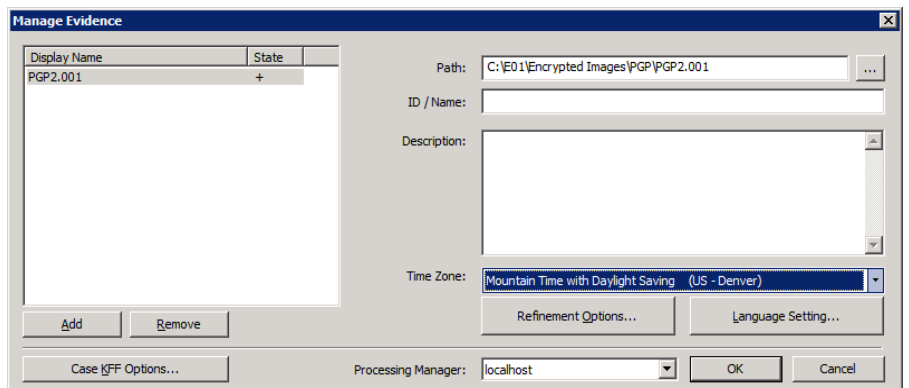
- 3a. Log into the PGP® Universal™ Server
- 3b. Select the Users tab

- 3c. Click on the User Name with a recovery icon for the system being examined.
- 3d. In the popup that appears, you will find a list of computers. The far right column contains a link for the WDRT. Click the link to display a popup that shows the WDRT. The WDRT will look similar to this:  
 ULB53-UD7A7-1C4QC-GPDZJ-CRNPA-X5A
- 3e. You can enter the key, with or without the dashes, in the Passphrase/WDRT field as the credential to decrypt a drive or image. The WDRT can be copied and pasted into the text field to avoid errors.
- 3f. Click *OK*.



**Important:** If you click *Cancel* to process the evidence without decrypting, you will not be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence

4. Verify that the PGP® WDE encrypted image is added to the case Manage Evidence list.



5. Select the options to use for this evidence, including Case KFF Options, Refinement Options, and Language Setting, if different from the global/default options that were selected prior to case creation.
6. Choose the Processing Manager to use, if different from localhost.
7. Enter an ID or Name for the Evidence, and a Description if you desire.
8. Specify the time zone for the evidence being added.

When all options have been selected, click *OK* to begin processing the evidence into the case, or click *Cancel* to abandon the addition of this evidence.

**Note:** PGP® WDE decryption was developed using version 9.9 of the product.



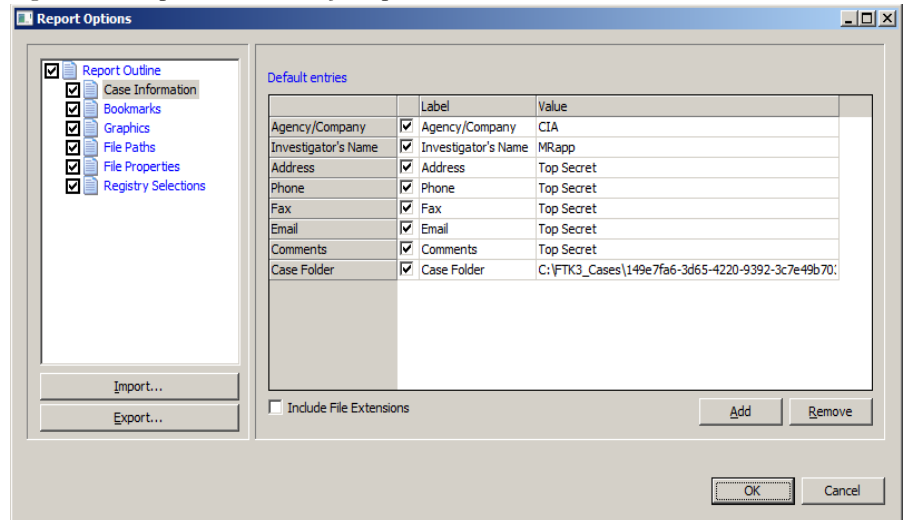
## *Chapter 12 Working with Reports*

At any time during or after the investigation and analysis of a case, you can have AccessData FTK create a report that summarizes the relevant evidence of the case. The final report is made available in several formats, including HTML and PDF format including one that is viewable in a standard Web browser.

### **CREATING A REPORT**

Use the Report Wizard to create a report. Access the Report Wizard by selecting *File > Report*. The Report Wizard is displayed in the following figure:

Figure 12-1 Report Creation Wizard Options



To create a report run the Report Wizard and do the following:

1. Enter basic case information.
2. Select the properties of bookmarks.
3. Decide how to handle graphics.
4. Decide whether you want a file path list.
5. Decide whether you want a file properties list.
  - 5a. Select the properties for the file properties list.
6. Add the Registry Viewer sections.

Each step is discussed in detail in the following sections.

## SAVING YOUR SETTINGS

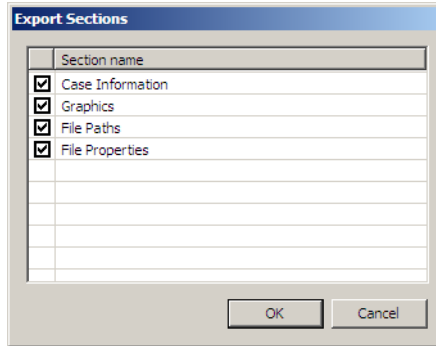
When you finish specifying the report settings, the selected settings are automatically saved when you click *OK* to generate the report.

Export report settings at any time, while creating a report, and after you finish specifying the report settings. Import and reapply those settings to a new report in the same case, or to a report in a new case, as desired.

To export report settings do the following:



1. Click *Export*. The Export Sections dialog opens.



2. Check the sections for which you want to save the settings.
3. Click *OK*.
4. Type a name for the setting file, with no extension.
5. Click *OK* to save the settings as an *.XML* file.

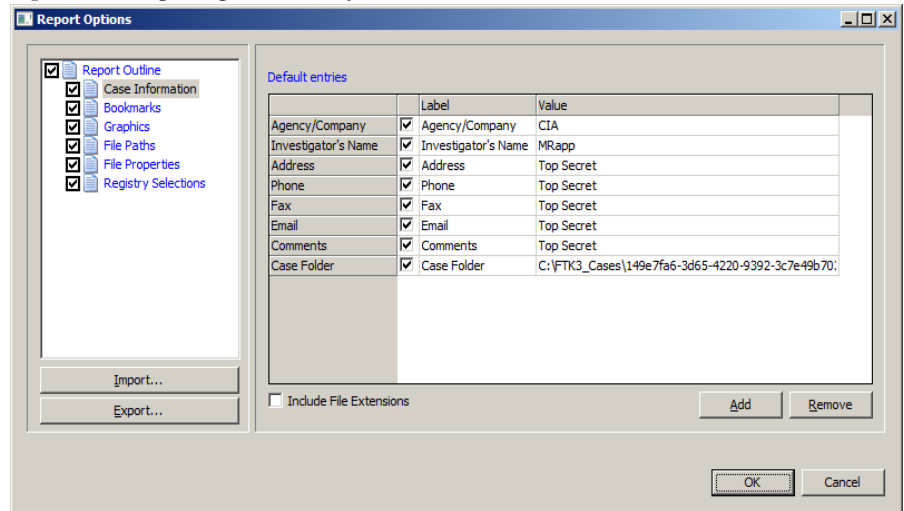
To apply saved settings to a new report:

1. Click *Import*.
2. Browse to the settings file you want to apply, then select it.
3. Click *Open* to import the settings file to your current report.

## ENTERING CASE INFORMATION

The Case Information dialog provides fields for basic case information, such as the investigator and the organization that analyzed the case. The following figure displays the Report Options dialog with the case information displayed.

Figure 12-2 Report Options Case Information



To include basic case information in the report, do the following:

1. Check the *Case Information* box in the Report Outline on the left side of the screen.
2. In the Default Entries pane, check the entries to include in the report (all are checked by default).
3. Double-click the Value field to enter the required information.

Add and remove entries with the *Add* and *Remove* buttons below Default Entries. Mark the Include File Extensions box to include a File Extensions List and count in the File Overview portion of the report.

**Important:** Below the Case Information Pane there is a new button, *Include File Extensions*. This box is unmarked by default. If you wish to include in the report a list of file extensions such as is found in *Overview > File Extensions*, mark the Include File Extensions box. The list of file extensions will appear in the report under Case Information, after File Items and File Category, and before File Status.

The File Extensions List is long and may span many pages. If you intend to print the Report, this may not be desirable.

To add a Case Information entry do the following:

1. Click *Add*. A new entry line appears at the bottom of the list.
2. Provide a label and a value for the new entry.

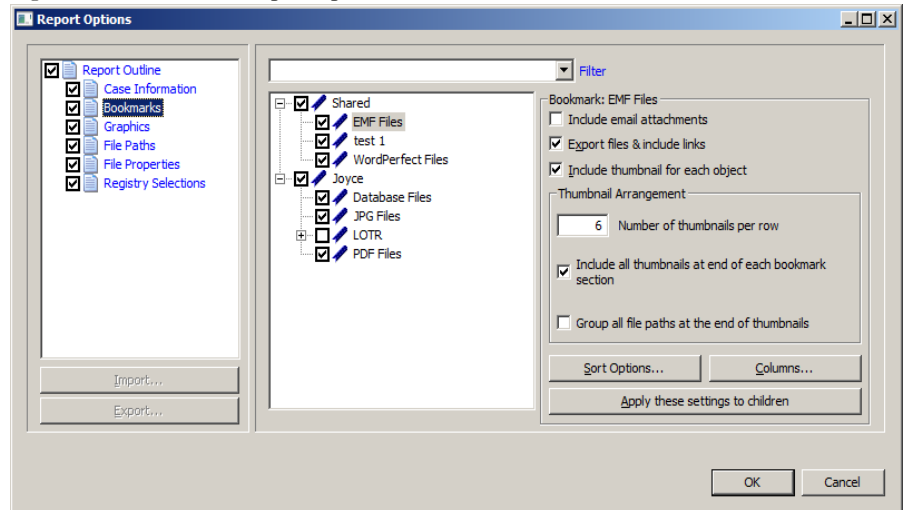
To remove a Case Information entry, do the following:

1. Highlight the entry line to be removed.
2. Click *Remove*.

## MANAGING BOOKMARKS IN A REPORT

The Bookmarks dialog allows you to create a section in the report that lists the bookmarks that were created during the case investigation. You can also choose not to create a bookmark section by unselecting the Bookmarks checkbox. To customize the Bookmarks settings, do the following:

Figure 12-3 Bookmarks Report Options



1. If you wish to apply a filter to the bookmarked data, do the following:
  - 1a. Click *Filter* for the dropdown Filters list.
  - 1b. Select any filter from the list

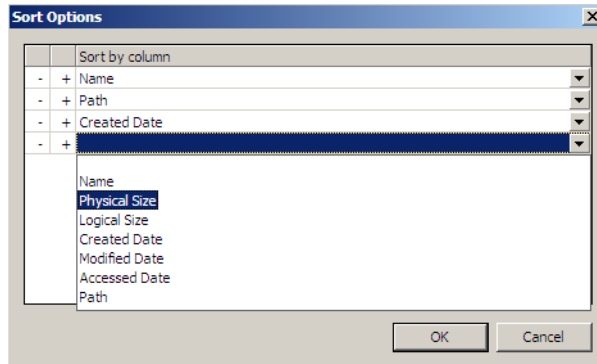
### OR

Select the blank line at the top of the list if you decide not to apply a filter.

2. Mark the boxes to indicate which bookmarks to include. Choose Shared and/or User bookmarks by group, or individually.
3. For each bookmark you choose to include, you can choose options from the Bookmark box on the right. Options are:
  - Include email attachments

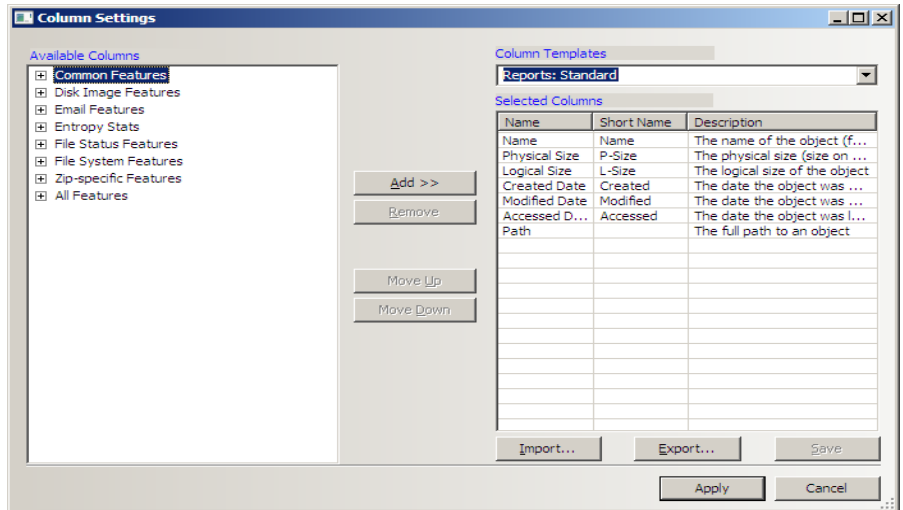
- Export files & include links
  - Include thumbnail for each object
4. Choose options for Thumbnail Arrangement for each bookmark or bookmark group. Options are:
    - Number of thumbnails per row
    - Include all thumbnails at end of each bookmark section
    - Group all file paths at the end of thumbnails
  5. Choose whether to export the files and include links to them in the report when it is generated.
  6. Choose whether to include graphic thumbnails that may be part of any bookmarks.
 

**Note:** If you want to create links to original files in the report, choose both to export the original files and to include graphic thumbnails when the report is generated.
  7. To sort bookmark information by columns, do the following:
    - 7a. Click *Sort Options*. The Sort Options dialog appears.



- 7b. Click the plus (+) to add a criterion, or click minus (-) to delete a criterion.
  - 7c. Click the down arrow button on the right side of each line to open the dropdown of available sort columns.
  - 7d. Click *OK* to save the selected Sort Options and close the dialog.
8. To customize the properties columns to display in the report, do the following:

8a. Click *Columns*.

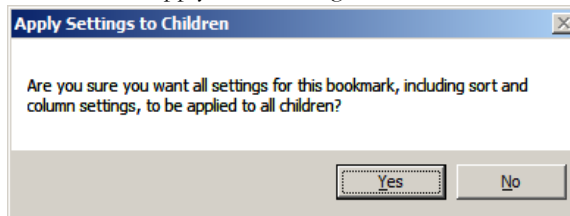


8b. Select or customize the properties columns to include in the report. You can import an existing column template and use it here if the template you want is not readily available or would take too long to create again.

8c. When you are done defining the columns settings to use, click *Apply*.

9. To apply all settings for this bookmark to child files, do the following:

9a. Click *Apply* these settings to children.



9b. You will be prompted to confirm this action. Click *Yes* to confirm and apply.

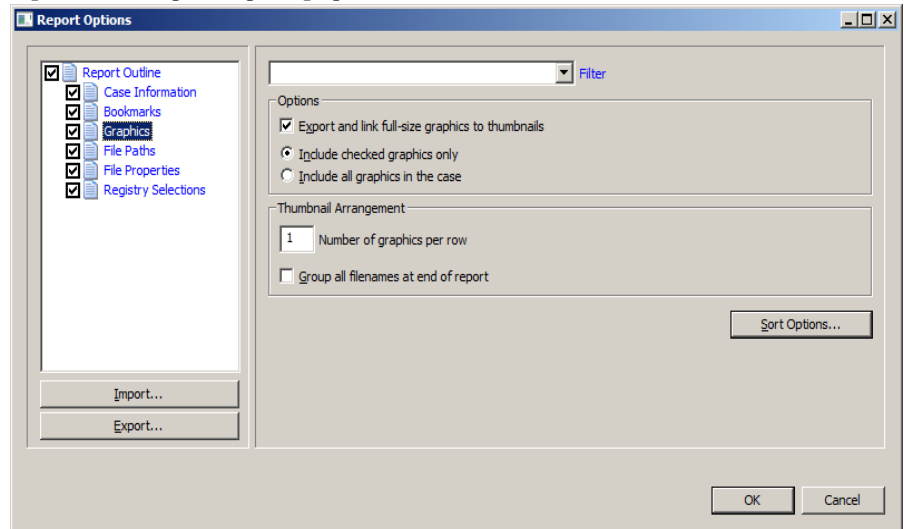
**OR**

Click *No* to abandon the selection. For more information on customizing columns, see “Customizing File List Columns” on page 268.

## MANAGING GRAPHICS IN A REPORT

The Graphics dialog allows you to create a section in the report that displays thumbnail images of the case graphics and can link them to original graphics if desired.

Figure 12-4 Graphics Reporting Options.



To apply a filter to your graphics files, do the following:

1. Click Filter to open the Filter dropdown list.
2. Select a filter.

To view full-sized graphics in the report, do the following:

1. Mark the box for “Export and link full-size graphics to thumbnails.”
2. Select a radio button:

*Include Checked graphics only*

**OR**

*Include all graphics in the case*

To specify the Thumbnail Arrangement, do the following:

1. Specify the number of graphics to display per row
2. Mark the *Group all filenames at end of report* box to group all the graphics filenames at the end of the report.

**OR**

Leave the *Group all filenames at end of report* box unmarked to show the graphics filenames with the graphics in the report.

To sort the graphics by Name or by Path, do the following:

1. Click Sort Options.
2. Click Plus (+) to add a sort option.

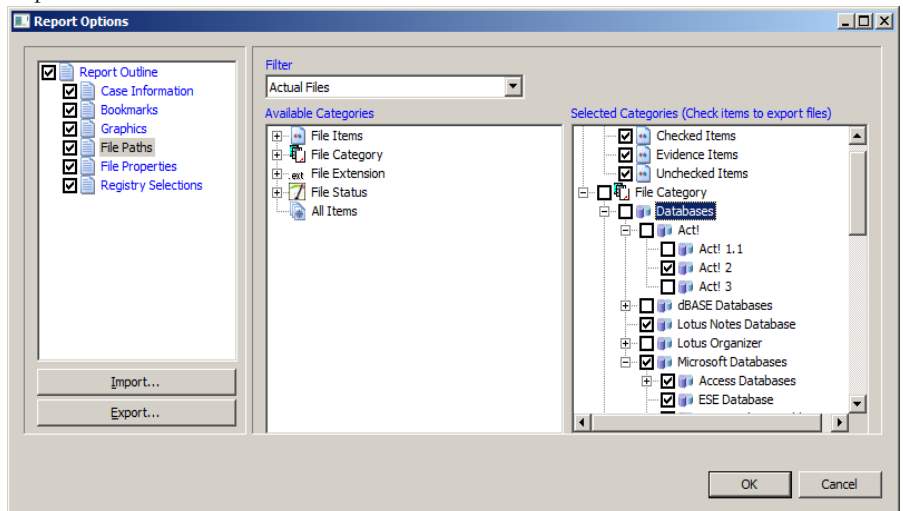
**OR**

Click Minus (-) to remove a sort option

3. Click the dropdown arrow on the right side of the line to select either Name or Path.
4. Click *OK* to save the sort options and close the dialog.

## SELECTING A FILE PATH LIST

The File Paths dialog allows you to create a section in the report that lists the file paths of files in selected categories. The File Paths section simply displays the files and their file paths; it does not contain any additional information. Defining File Paths for the Report



To customize the File Path List, do the following:

1. Select a filter from the Filter dropdown, or leave the Filter box blank.  
The Available Categories list contains the same categories as in the Overview Tab in FTK.
2. Select from the Available Categories list to include the category or categories in the report by dragging the category to the Selected Categories list.  
Any category item or sub-item can be dragged back to the Available Categories list if you change your mind about what to include.

3. Export and link to selected files in the File Path list by checking the box next to the items in the Selected Categories box.

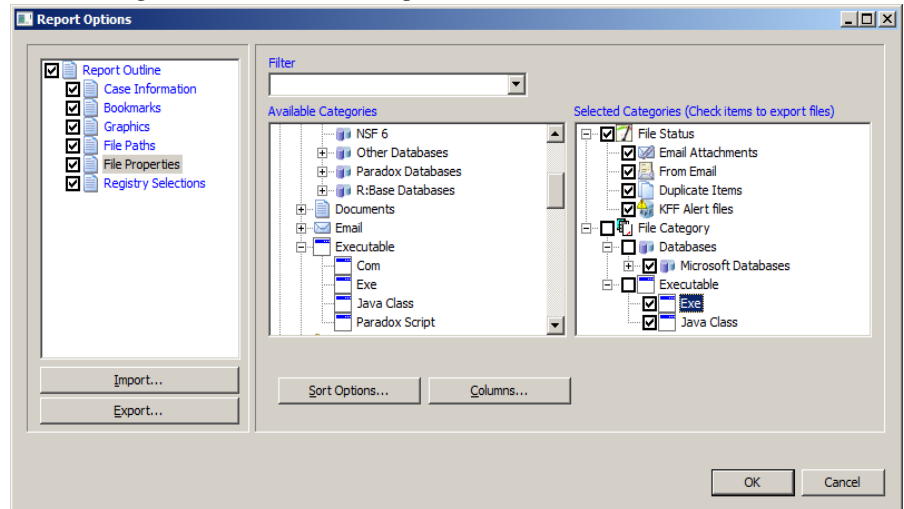
If the box is left empty in the Selected Categories list, the File Path will be included, but the files themselves will not be exported and linked to the File Path in the report.

## ADDING A FILE PROPERTIES LIST

The File Properties dialog allows you to create a section in the report that lists the file properties of files in selected categories.

To customize a File Properties list in your report, do the following:

1. Under Report Outline, click *File Properties*.



2. Choose a filter for the File Properties list by clicking the Filter dropdown arrow and selecting the desired filter.

**OR**

Choose no filter by selecting the blank entry at the top of the Filter dropdown list.

3. Drag and drop the categories you want to include from the Available Categories window to the Selected Categories window.
4. Check a category in the Selected Categories window to export related files and link them to the File Properties list in the report. Checking an item automatically selects the files and folders under it.

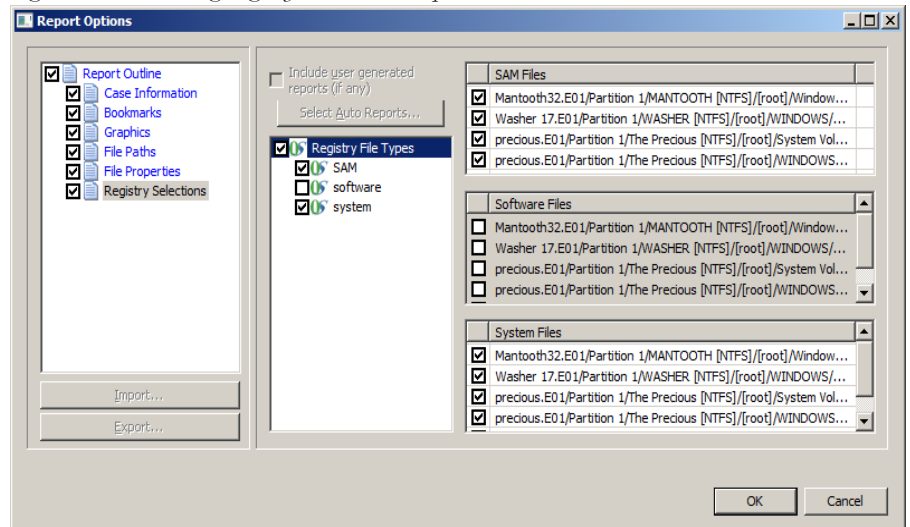


5. To modify your Sort Options, click *Sort Options*. For more information on modifying the Sort Options, see “Selecting the Report Output Options” on page 256.
6. To modify your column settings, click *Columns*. The Column Settings dialog opens. For more information on setting columns, see “Customizing File List Columns” on page 268.

## REGISTRY SELECTIONS

If your drive image contains registry files, you can include them in your report.

Figure 12-5 Including Registry Files in the Report



To customize the list of Registry information in the report, do the following:

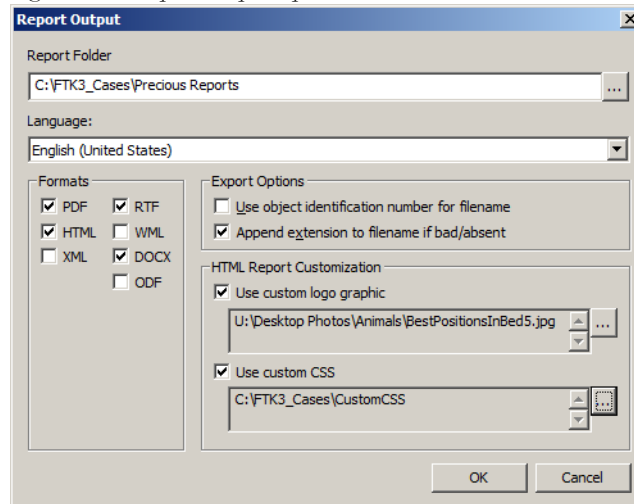
1. In the Registry File Types window, check the file types for which you want headings in your report.
2. In the right window, check the registry file paths you want included in your report.
3. Mark the box *Include user generated reports (if any)* if you have generated Registry Reports using Registry Viewer, and you want to include them in this report.
4. Mark the box *Select Auto Reports*, to view and select which Registry Reports to include in the report from those that were generated automatically based on the Registry Reports selection in *Case Manager > Case > New > Detailed Options > Evidence Refinement*.

- When you have completed defining the report, click *OK* to open the Report Output options dialog.

## SELECTING THE REPORT OUTPUT OPTIONS

The Report Output dialog allows you to select the location of the report. You can also recreate the directory structure of exported items.

Figure 12-6 Report Output Options



To select the report output options:

- Type the folder in which to save the report, or use the *Browse* button to locate and select a location.
- Use the drop-down arrow to select the language for the written report. Options are:

**TABLE 12-1 Available Report Languages**

• Chinese (Simplified, PRC)	• English (United States)
• German (Germany)	• Japanese (Japan)
• Korean (Korea)	• Portuguese (Brazil)
• Russian (Russia)	• Spanish (Spain, Traditional Sort)
• Swedish (Sweden)	

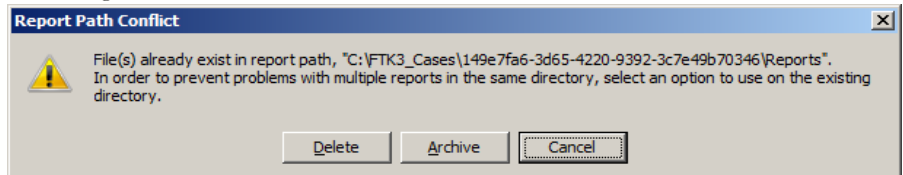
3. Indicate the formats for publishing the report. You can choose any or all of the output formats. Options are:

**TABLE 12-2 Available Report Output Formats**

• PDF	• HTML
• XML	• RTF
• WML	• DOCX
• ODF	•

4. Under Export Options,
  - 4a. Check the *Use object identification number for filename* to shorten the paths to data in the report. Links are still created for proper viewing of the files.  
**Note:** The unique File ID numbers, when used in a report, keep the pathnames shorter. This makes burning the report to a CD or DVD more reliable.
  - 4b. Check the *Append extension to filename if bad/absent* box to add the correct extension where it is not correct, or is missing.
5. Under HTML Report Customization, choose from the following options:
  - 5a. If you wish to use your own custom graphic or logo, mark the *Use custom logo graphic* box, then browse to the file and select it. Use .GIF, .JPG, .JPEG, .PNG, or .BMP file types.
  - 5b. If you wish to use a custom CSS file, mark the *Use custom CSS* box. Select the folder where the custom CSS files have been saved. Click OK. The folder you selected displays in the Use Custom CSS text box. See “Customizing the Formatting of Reports” on page 257.
6. Click OK to run the report.

If the report folder you selected is not empty, you will see the following error message:



Choose to Delete or Archive the contents of the folder, or cancel the report.

## CUSTOMIZING THE FORMATTING OF REPORTS

The formatting of FTK Reports can be customized by someone who is very familiar with Cascading Style Sheets. FTK Reports stores a file path you select (default or

custom) to the folder containing the custom CSS files. When CSS is not selected, FTK Reports uses its default settings.

The CSS file code has been reorganized and rewritten for clarification and is easy to modify for someone with an intimate knowledge of CSS.

For reports to utilize the cascading style sheets, three CSS files are necessary, and must all be located in the specified CSS folder:

- Common.css
- Bookmarks.css
- Navigation.css

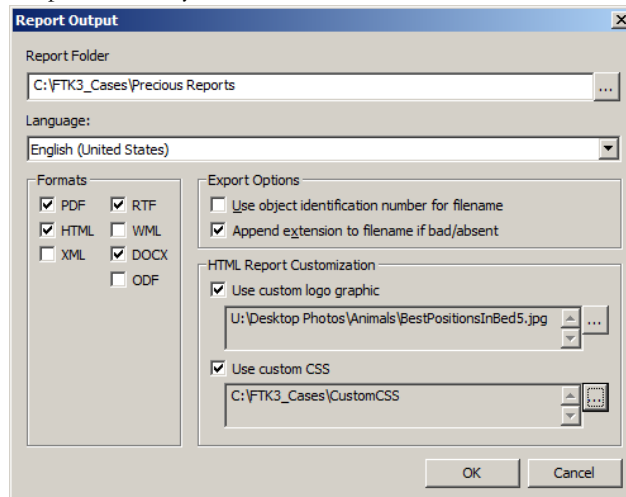
The original CSS files are found in the following path if no changes were made to the default:

`c:\Program Files\AccessData\Forensic Toolkit\3.0\bin\ReportResources`

Copy the \*.CSS files to a different directory. Do not make changes to the original files.

When CSS is selected, FTK Reports checks for those files in the specified directory. If any of the three files is missing you are notified and the report does not proceed.

The UI option consists of a checkbox and a text path string. The path string points to the path directory that contains the 3 needed css files.



**Note:** The UI options settings are persistent per Windows login user. Thus, it will be persistent across case list the custom graphic feature.

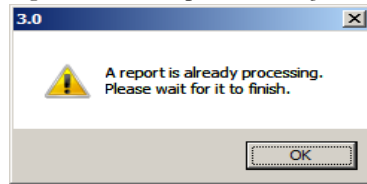
## CREATING THE REPORT

The progress bar dialog indicates the progress of the report.

The report displays after it has finished processing. You can process only one report at a time.

If you start another report too soon, you will be prompted to wait.

*Figure 12-7 A Report is Already Processing.*



## VIEWING AND DISTRIBUTING A REPORT

The report contains the information that you selected in the Report Wizard. When included in the report, files appear in both raw data and in the report format.

An example of the main page of the report (index.htm) is shown below:

Figure 12-8 Viewing the Report in HTML Format

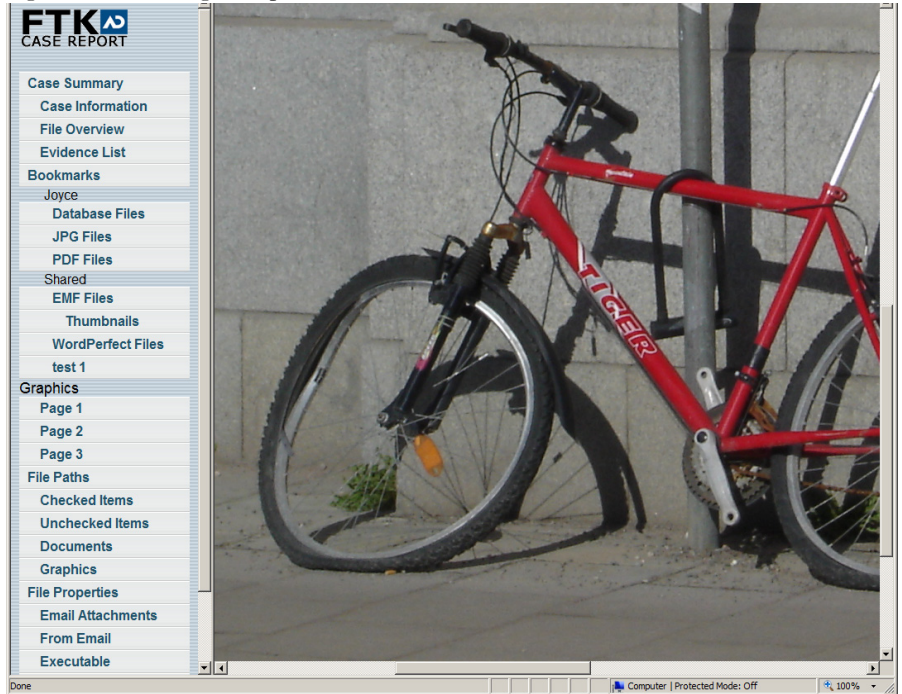


Figure 12-9 The Report in PDF Format



To view the report, click *Yes*.

To view the report outside of FTK, browse to the report file and click on the report file:

- Click on `index.htm` to open an HTML document in your Web browser.
- Click on the file `[report].pdf` to open the report in a PDF viewer.

After creating the report, burn only the contents from the root of the report folder, and not the report folder itself, to a CD or DVD. The autorun automatically launches the report's main page (`index.htm`) using the default browser when the CD is read on a Windows computer.

**Note:** The Windows computer must be configured to automatically execute autorun files

**Note:** If you burn the folder that contains the report to the CD or DVD, the autorun will not be at the root of the disk, and will not work properly.

## MODIFYING A REPORT

Modify the report by recreating it. Add the new evidence or change report settings to modify the report to meet your needs. Change the report settings for each report as needed. All previously distributed reports should be retracted to keep all recipients current.

## PRINTING A REPORT

Print the report from the program used to view it. The PDF report is designed specifically for printing hard copies with preserved formatting and correct organization. The HTML report is better for electronic distribution.





# Chapter 13 Customizing the FTK Interface

The AccessData FTK interface provides a highly visual user interface to make evidence more recognizable and easier to process. Customize the interface to further accommodate the current case and your personal style.

## CUSTOMIZING OVERVIEW

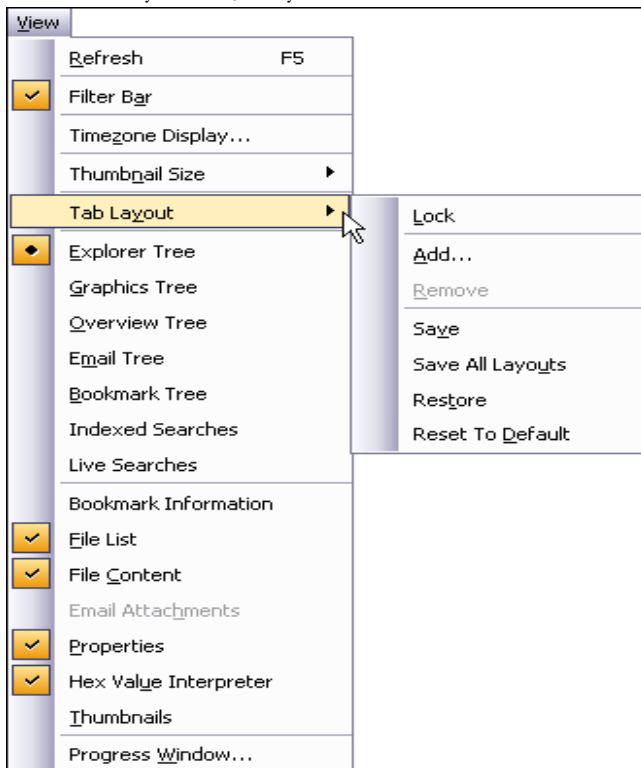
You can adjust the size of the panes in the tabs by clicking on a border and dragging it to a new size. You can also rearrange the order of the tabs by dragging and dropping.

You can add or remove panes from the current tab using the View menu. Click *View* and click the pane you would like to add to the current view.

To save the new arrangement, Click *View > Tab Layout > Save*.

## THE VIEW MENU

Use the View menu to control the pane views displayed in each tab. FTK provides several tabs by default, but you can create an interface view that best suits your needs.



The View menu allows you to do the following:

- Refresh the current view's data
- View the Filter Bar
- Display the Timezone for the evidence
- Choose the display size for graphic thumbnails
- Manage Tabs
- Select Trees and viewing panes to include in various tabs
- Open the Progress Window

## THE TAB LAYOUT MENU

Use the options in the Tab Layout menu to save changes to tabs, restore original settings, and lock settings to prevent changes.

The following table describes the options in the Tab Layout menu.

**TABLE 13-1 Tab Layout Menu Options**

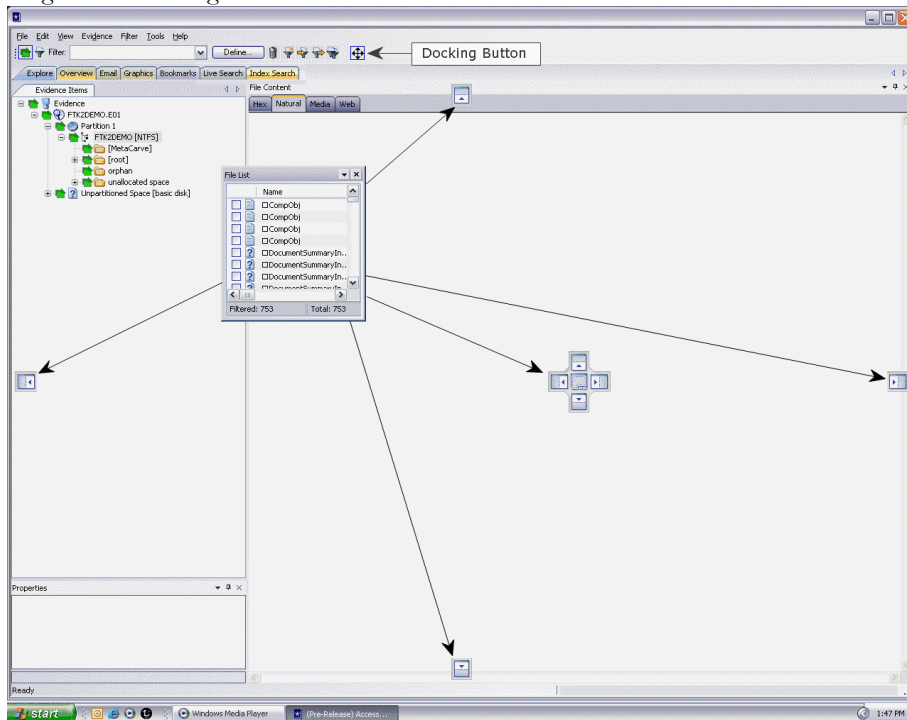
---

<b>Option</b>	<b>Description</b>
Lock	Locks the panes in place so that they cannot be moved.
Add	Adds a blank tab to the Enterprise window. The new tab will be like the one selected when this option is used.
Remove	Removes the selected tab from the Enterprise window.
Save	Saves the changes made to the current tab.
Save All Layouts	Saves the changes made to all tabs.
Restore	Restores the Enterprise window to the settings from the last saved layout. Custom settings can be restored.
Reset to Default	Sets the Enterprise window to the setting that came with the program. Custom settings will be lost.

## MOVING VIEW PANES

Move view panes on the interface by placing the cursor on the title of the pane, clicking, dragging, and dropping the pane on the location desired. Holding down the mouse button undocks the pane. Use the guide icons to dock the pane in a pre-set location. The pane can be moved outside of the interface frame.

Figure 13-1 Moving View Panes






To place the view pane at a specific location on the application:


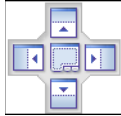
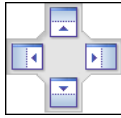

1. Place the mouse (while dragging a view pane) onto a docking icon. The icon changes color.
2. Release the mouse button and the pane seats in its new position.

The following table indicates the docking options available:

**TABLE 13-2 Docking Icons**

Docking Icon	Description
	Docks the view pane to the top half of the tab.
	Docks the view pane to the right half of the tab.
	Docks the view pane to the left half of the tab.

**TABLE 13-2 Docking Icons**

Docking Icon	Description
	Docks the view pane to the bottom half of the tab.
	Docks the view pane to the top, right, left, bottom, or center of the pane. When docked to the center, the new pane overlaps the original pane, and both are indicated by tabs on the perimeter of the pane.
	Docks the view pane to the top, right, left, or bottom of the tree pane. The tree panes cannot be overlapped.
	Locks the panes in the application in place, making them immovable. When the lock is applied, the blue box turns grey. This button is found on the toolbar.

## CREATING CUSTOM TABS

Create a custom tab to specialize an aspect of an investigation, add desired features, and apply filters as needed to accommodate conditions specific to a case.

To create a custom tab, do the following:

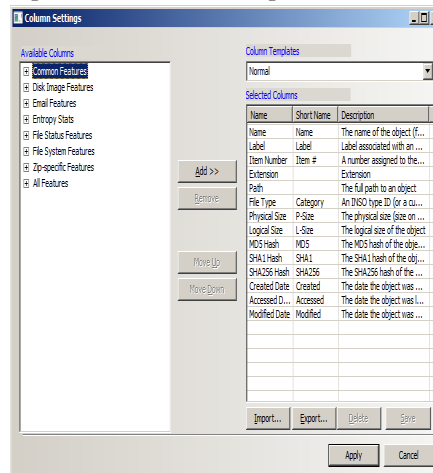
1. Select the tab that is most like the tab you want to create.
2. Click *View > Tab Layout > Add*.
3. Enter a name for the new tab and click *OK*. The resulting tab is a copy of the tab you were on when you created the new one.
4. From the View menu, select the features you need in your new tab.  
**Note:** Features marked with diamonds are mutually exclusive, only one can exist on a tab at a time. Features with check marks can co-exist in more than one instance on a tab.
5. When you are satisfied with your new tab's design, click *Save* to save this new tab's settings, or *View > Tab Layout > Save*.
6. (Optional) Click *View > Tab Layout > Save All* to save all changes and added features on all tabs.
7. To remove tabs, highlight the tab to remove, then click *View > Tab Layout > Remove*.

## CUSTOMIZING FILE LIST COLUMNS

The Column Settings dialog allows the modification or creation of new definitions for the information that displays in the File List, and in what order. Column settings are also used to define which file information appears in the Bookmark and File List Properties sections of case reports.

Using custom column settings allows you to narrow the information provided in the File List and case reports. Columns display specific information about, or properties of, the displayed files.


Figure 13-2 Column Settings



**Note:** Custom column settings can be exported as an .XML file, and imported for use in other cases.

## CREATING AND MODIFYING COLUMN SETTINGS

To modify or create column settings:

1. Right-click a heading in the File List, or click the Manage Columns button  on the File List toolbar. The Manage Columns context menu opens.
2. Click *Column Settings*. The Column Settings dialog opens.

3. From the Available Columns pane, select a category from which you want to take a column heading. You can add the entire contents of a category or expand the category to select individual headings.

**Note:** Column widths in most view panes can be adjusted by hovering the cursor over the column heading borders, and dragging the column borders wider or narrower.

Click on a column heading in the file list view to sort on that column. Hold down the Shift key while clicking a different column header to make the newly selected column the primary sorted column, while the previous primary-sorted column becomes the secondary sorted column. There are only two levels of column sorting, primary and secondary.

To undo a secondary sort, click on a different column header to make it the primary sorted column.

## AVAILABLE COLUMNS

The following tables describe all available columns in the File List. The columns you actually see depend on which tab and which columns category you are in.

**Note:** When viewing data in the File List, use the type-down control feature to locate the information you are looking for. Sort the column, then select the first item in the list. Type the first letter of the filename you are searching for. Enterprise will move down the list to the first filename beginning with that letter.

## COMMON FEATURES

These column headings tend to be most shared among objects.

**TABLE 13-3 Common Column Headings**

Column	Description
Accessed Date	The timestamp showing when the object was last accessed.
Accessed Date (FAT)	The date the object was last accessed.
Actual File	The actual file in the file system, not from an archive such as .zip, .pst, etc.
Bad Extension	Indicates if the file type does not match its header.
Carved	Indicates whether the object has been carved.
Compressed File Size	Displays the size of the compressed files. Only displays on compressed files.

**TABLE 13-3 Common Column Headings**

---

<b>Column</b>	<b>Description</b>
Compressed	Indicates whether the object is compressed. Only displays on compressed files.
Container	Indicates whether the object has child objects.
Created Date	Indicates the date the object was created on the source system.
Decrypted	Indicates that the object has been decrypted.
Decrypted by User	Indicates that the object was decrypted by the user before being added to the case.
Deleted	A string representing the object and its parents by their IDs.
Duplicate File	The file is a duplicate of another file in the case.
Encrypted	Indicates whether the object is encrypted. Only displays on files.
Extension	Displays the object's extension.
File Class	Matches a container on the Overview tree.
File Type	An ID reflecting the identified or reclassified type of a file.
Flagged Ignorable	Indicates that the object was marked as ignorable. Not accessible to a reviewer.
Flagged Privileged	Indicates that the object was marked as privileged. Not accessible to a reviewer.
From Recycle Bin	Displays a Recycle Bin index file, or a recycled file still in the Recycle Bin folder.
Item Number	Displays the unique File ID number assigned to the object by Enterprise during processing.
Logical Size	Displays the logical size of an object.
MD5 Hash	Displays the MD5 hash of the object's contents.
Modified Date	Displays the date the object was last modified.
Name	Displays the name of the object.
Object Type	Indicates the type of the object.
Original File Type	Indicates the original type of an object whose type has been changed.
Path	Displays the full path of an object.
Physical Size	Indicates the amount of space the object takes up on a disk.
Recycle Bin Original Name	Displays the name of a file in the Recycle Bin folder before the file was recycled.



**TABLE 13-3 Common Column Headings**

---

<b>Column</b>	<b>Description</b>
SHA*-1 Hash	Indicates the SHA-1 hash of the object's contents.
SHA-256 Hash	Indicates the SHA-256 hash of the object's contents.

## DISK IMAGE FEATURES

The following table displays the stored hashes for the logical image.

**TABLE 13-4 Disk Image Headings**

---

<b>Column</b>	<b>Description</b>
Validate MD5	Displays the validated MD5 hash of the object. This is the internal stored hash of an image such as E01 or Smart (S01).
Validate SHA-1 Hash	Indicates the validated SHA-1 hash of the object. This is the internal stored hash of an image such as E01 or Smart (S01).

## EMAIL FEATURES

These column headings list features specific to email in general, and specifically to Microsoft Outlook/Exchange, and to Outlook Express.

**TABLE 13-5 Email Headings**

---

<b>Column</b>	<b>Description</b>
BCC	Displays addresses in the Blind Carbon Copy field.
CC	Displays addresses in the Carbon Copy field.
Delivery Time	For outgoing email, it indicates the time the object was sent; for incoming email, it indicates the time the object was received.
From	Lists the sender's addresses in the object's From field.
From Email	Indicates whether the object came from an email or an email archive.
Has Attachment	Indicates whether the object has an attachment.
Subject	Displays the text in the object's Subject field.
To	Lists the addresses in the object's To field.
Unread	Indicates whether the object is marked as Unread.
Unsent	Indicates whether the object is marked as Sent.

## MICROSOFT OUTLOOK EXPRESS HEADINGS

These email headings are specific to Microsoft Outlook Express only:

**TABLE 13-6 Outlook Express Headings**

---

<b>Column</b>	<b>Description</b>
Account Name	Displays the name of the account associated with the object.
Account Registry Key	Displays the registry key associated with the object's account.
Answered	Indicates whether the object was answered.
Answered Message ID	Displays the ID of the object's answered message.
Digitally Signed	Indicates whether the object was digitally signed.
Email Size	Displays the size of the object.
Has Attachment (Outlook Express)	Indicates whether the object has an attachment.
Hotmail Message ID	Displays the ID of a Hotmail object.
Marked	Indicates whether the object has been marked.
Message ID	Displays the message ID.
Message Offset	Displays the block of memory occupied by the object.
News	Indicates whether the object was a news item.
Priority	Displays the priority assigned to the object.
Recipient Address	Lists the addresses in the object's recipient field.
Recipient Name	Lists the names in the object's recipient field.
Sender Address	Displays the address in the object's sender field.
Sender Address and Name	Displays the address and name in the object's sender field.
Sender Name	Displays the name in the object's sender field.
Server	Displays the server used to send the object.
Server Info	Displays the server information of the object.
Subject (Outlook Express)	Displays the text on the object's subject field.
Subject Without Prefix	Displays the text without the prefix on the object's subject field.
Thread Ignored	Indicates whether a thread was marked as Ignore.
Thread Watched	Indicates whether a thread was marked as Watch.
Time Message Saved (Outlook Express)	Displays the time an object was Saved.

**TABLE 13-6 Outlook Express Headings**

---

<b>Column</b>	<b>Description</b>
Time Received (Outlook Express)	Displays the time an incoming object was received.
Time Sent (Outlook Express)	Displays the time an outgoing object was sent.

**MICROSOFT OUTLOOK/EXCHANGE HEADINGS**

These email headings are set for Microsoft Outlook/Exchange only:

**TABLE 13-7 Outlook / Exchange Headings**

---

<b>Column</b>	<b>Description</b>
Attachment MIME Tag	Lists the attachment MIME tag of the object.
Client Submit Time	Indicates the time the client submitted the email.
Comment	Displays any comment associated with the email.
Content Count	Indicates the content count of the object.
Content Unread	Indicates whether the object is marked Unread.
Conversation Topic	Displays the object's conversation topic.
Delete After Submit	Indicates whether the object was marked for deletion after it was submitted.
Display Name	Displays the object's display name.
From Me	Indicates whether the object was marked From Me.
Importance	Indicates the object's assigned importance.
Message Class	Indicates the class assigned to the message in the object.
Message Size	Displays the size of the object.
Originator Delivery Report Requested	Indicates whether an Originator Delivery Report was requested.
Provider Submit Time	Displays the time at which the provider submitted the object.
Read Receipt Requested	Indicates whether the email sent requested confirmation of the email.
Received By Email Address	Displays the time at which the addressee received the object.
Received By Name	Lists the names of the addresses that received the object.

**TABLE 13-7 Outlook / Exchange Headings**

---

<b>Column</b>	<b>Description</b>
Received Representing Email Address	Displays the address of a Representing Email recipient.
Reply Recipient Names	Displays the addresses in the Reply To: field.
Resend	Indicates whether the object was marked Resend.
Sender Email Address	Displays the address in the object's Sender field.
Sensitivity	Indicates the sensitivity assigned the object.
Sent Representing Email Addresses	Displays the address of a Representing Email sender.
Sent Representing Name	Displays the name of the Representing Email sender.
Submitted	Indicates whether the object was marked as Submit.
Transport Message Headers	Lists the Simple Mail Transfer Protocol (SMTP) headers.
Unmodified	Indicates whether the object has been marked as Modified.

## ENTROPY STATISTICS

These column headings list information that may indicate possible encryption or compression.

**TABLE 13-8 Entropy Statistics Headings**

---

<b>Column</b>	<b>Description</b>
Arithmetic Mean	The result of summing all the bytes and dividing by the file length. If random, the value should be about 1.75; if the mean departs from this value, the values are consistently high or low.
Chi Squared Error Percent	This distribution is calculated for the stream of bytes in the file and expressed as an absolute number. This percentage indicates how frequently a truly random number would exceed the value calculated.
Entropy	Shows the information density of a file in bits per character. Amounts close to 8 indicate randomness.

**TABLE 13-8 Entropy Statistics Headings**

---

<b>Column</b>	<b>Description</b>
MCPI Error Percent	Monte Carlo algorithm, named after Monte Carlo, Monaco, is a method involving statistical techniques for finding solutions to problems.  This heading shows the result of using a Monte Carlo algorithm to approximate Pi.
Serial Correlation Coefficient	Indicates the amount to which each byte in an object relies on the previous byte. Amounts close to 0 indicate randomness.

## FILE STATUS FEATURES

The file status columns show hash set names that match the file and its status.

**TABLE 13-9 File Status Features**

---

<b>Column</b>	<b>Description</b>
Hash Group	Indicates the set from which the hash came. Lists the sequence entered into the database, or the program that generated the hash.
KFF Status	Lists the status of the hash set that Enterprise matches (Alert or Ignore).
Not KFF Ignore or OLE Subitem	Indicates that the hash is neither in the KFF Ignore List nor a OLE subitem.
Not KFF Ignore or Duplicate	Indicates that the hash is neither in the KFF Ignore List nor a duplicate file.

If a file has matches from more than one set, the status with the height value is used. For more information, see “Chapter 10 Using Filters” on page 205.

## FILE SYSTEM FEATURES

These column headings list information specific to a particular file system.

**TABLE 13-10 File System Headings**

---

<b>Column</b>	<b>Description</b>
DOS Features	See below
ext2 Features	See below

**TABLE 13-10 File System Headings**

---

<b>Column</b>	<b>Description</b>
HFS Features	See below
NTFS Features	See below
Unix Security Features	See below
Start Cluster	Indicates the starting cluster where a file begins from the beginning of a disk or volume.
Start Sector	Indicates the starting sector where a file begins from the beginning of a disk or volume.

## DOS FILE SYSTEMS

These column headings list information specific to DOS.

**TABLE 13-11 DOS Headings**

---

<b>Column</b>	<b>Description</b>
8.3 Name	Displays the 8.3 format name of the object.
Archive	Indicates whether the Archive attribute was set on the object.
Hidden	Indicates whether the Hidden attribute was set on the object.
Read Only	Indicates whether the Read Only attribute was set on the object.
System	Indicates whether the System attribute was set on the object.

## EXT2 FILE SYSTEMS

These column headings list information specific to Unix ext2.

**TABLE 13-12 ext2 Headings**

---

<b>Column</b>	<b>Description</b>
Deleted Date	Lists the date on which the object was deleted. Set on Unix objects only.
inode Number	<p>Lists the inode Number of an object. Displays on Unix objects only. Data structures contain information about files in Unix file systems that are created when a file system is created. Each file has an inode and is identified by an inode number (i-number) in the file system where it resides. User and group ownership, access mode (read, write, execute permissions) and type inodes provide important information about files.</p> <p>There is a set number of inodes, which indicates the maximum number of files the system can hold.</p> <p>A file's inode number can be found using the [ls -i] command, while the [ls -l] command will retrieve inode information.</p>

## HFS FILE SYSTEMS

These column headings list information specific to Apple Macintosh HFS and HFS+.

**TABLE 13-13 HFS Headings**

---

<b>Column</b>	<b>Description</b>
Backup Date	Displays the date on which the object was backed up.
Catalog Node ID	Displays the catalog node ID of the object.
Color (HFS)	Indicates the color of the object.
File Creator (HFS)	Displays the object's creator.
File Locked (HFS)	Indicates whether the object was locked.
File Type (HFS)	Indicates the object's file type.
Folder Valence (HFS)	Displays the number of files and folders directly contained in any given object.
Invisible (HFS)	Indicates whether the object is invisible.
Name Locked (HFS)	Indicates whether the object's file name is locked.
Put Away Folder ID (HFS)	Displays the ID of the object's Put Away folder.

## NTFS FILE SYSTEMS

These column headings list information specific to Microsoft NTFS.

**TABLE 13-14 NTFS Headings**

---

<b>Column</b>	<b>Description</b>
Alternate Data Stream Count	Displays the number of alternate data streams.
Group Name	Displays the Group Name of the object's owner.
Group SID	Displays the group SID of the object's owner.
MFT Record Number	Displays the object's Master File Table (MFT) record number and indicates what metadata is needed to retrieve an object.
Offline	Indicates whether the object's Offline attribute is set.
Owner Name	Displays the name of the object's owner.
Owner SID	Displays the SID of the object's owner.
Record Date	Displays the record date of the object.
Resident	Indicates whether the Resident attribute is set for the object.
Sparse	Indicates whether the Sparse attribute is set for the object.
Temporary	Indicates whether the Temporary attribute is set for the object.

## UNIX SECURITY FILE SYSTEMS

These column headings list information specific to the Unix security file system.

**TABLE 13-15 Unix Security Headings**

---

<b>Column</b>	<b>Description</b>
GID	Displays the Group ID of the object.
Group Name (Unix)	Displays the Group Name of the object.
Permissions	Lists the Permission settings for the object.
UID	Displays the User ID of the object.
Username	Displays the Username of the object.

## MOBILE DEVICES

For documentation of the Mobile Phone Examiner, please see the Mobile Phone Examiner User guide.



## ZIP-SPECIFIC FEATURES

These column headings list information specific to files zipped or compressed into a single file.

**TABLE 13-16 Zip Headings**

---

<b>Column</b>	<b>Description</b>
Checksum	Displays the checksum value of the object.
Compression Method	Displays the compression method of the object.
Extract Version	Displays the extract version of the object.

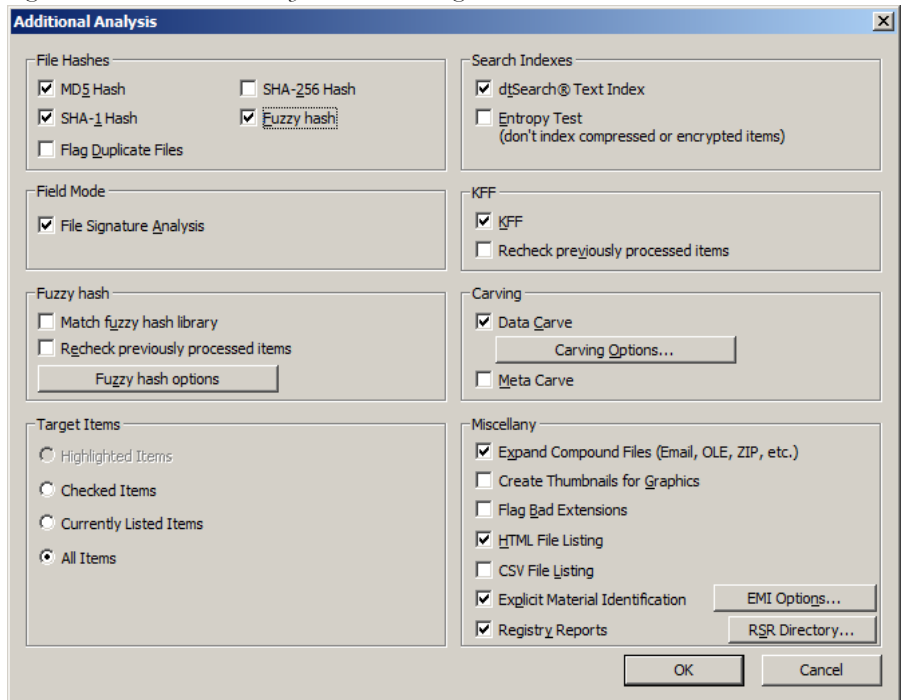
## TEMPORARY FILE FOLDER

The temporary file folder stores temporary files, including files extracted from Zip and email archives. The folder is also used as scratch space during text filtering and indexing. Enterprise frequently uses the temporary file folder.

## DATA CARVING

If you decide not to include Data Carving or Meta Carving in the case pre-processing options, you can run Data Carving and Meta Carving from the Additional Analysis Options screen.

Figure 13-3 Additional Analysis: Data Carving



- Data carving extracts a collection of data from the unallocated file system space using file-type-specific header and footer values.
- Meta carving searches unallocated clusters for metadata that is no longer referenced by the file system. Unlike traditional undelete methods, meta carving can recover deleted folders, and also the names and contents of files and folders that existed prior to reformatting the volume.

For more information on Data Carving, see “Data Carving” on page 97.

# *Appendix A File Systems and Drive Image Formats*

This appendix lists the file systems and image formats that FTK 3.0 analyzes.

## FILE SYSTEMS

**TABLE A-1** Recognized File System

- 
- |                          |             |
|--------------------------|-------------|
| • FAT 12, FAT 16, FAT 32 | • NTFS      |
| • Ext2, Ext3             | • HFS, HFS+ |
| • ReiserFS 3             | •           |

## HARD DISK IMAGE FORMATS

**TABLE A-2** Supported Hard Disk Image Formats

- 
- |                                  |                  |
|----------------------------------|------------------|
| • Encase                         | • SnapBack       |
| • Safeback 2.0 and under         | • Expert Witness |
| • Linux DD                       | • ICS            |
| • Ghost (forensic images only)   | • SMART          |
| • AccessData Logical Image (AD1) | •                |

## CD AND DVD IMAGE FORMATS

**TABLE A-3** Supported CD and DVD Image Formats

- 
- |                      |                    |
|----------------------|--------------------|
| • Alcohol (*.mds)    | • CloneCD (*.ccd)  |
| • ISO                | • IsoBuster CUE    |
| • Nero (*.nrg)       | • Pinnacle (*.pdi) |
| • PlexTools (*.pxi)  | • Roxio (*.cif)    |
| • Virtual CD (*.vc4) | •                  |

# *Appendix B Recovering Deleted Material*

FTK 2.3 finds deleted files on supported file systems by their file header.

## **FAT 12, 16, AND 32**

When parsing FAT directories, FTK 2.3 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 file's starting cluster (C) and size. From the size of the file and the starting cluster, FTK 2.3 computes the total number of clusters (N) occupied by the file.

FTK 2.3 then examines the File Allocation Table (FAT) and counts the number of unallocated clusters starting at C (U). It 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 2.3 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, it uses an exclamation mark ("!") as the first letter of the filename.

FTK 2.3 meta carves, or searches 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 2.3 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. It 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 2.3 searches to find inodes that are marked deleted: the link count is zero and the deletion timestamp is nonzero.

For each deleted inode, FTK 2.3 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 the application is attempting to recover.

FTK 2.3 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 2.3 does not recover deleted files from ext3 volumes because ext3 zeroes out a file's indirect block pointers when it is deleted.

## HFS

FTK 2.3 does not recover deleted files from HFS.

## Appendix C Program Files

The following tables list key FTK 2.3 files and folders, their functions, and their locations.

### FILES AND FOLDERS FOR THE APPLICATION

These files and folders exist on the computer running FTK 2.3.

**TABLE C-1 FTK 2.3 Folders and File Locations**

File or Folder	Location	Function
FTK2-Data (shared)	Root of system drive or partition [drive]:\ftk2-data\	Contains all case data not stored in the database.
summary_install_log_2.3.txt	[drive]:\Program Files\ AccessData\Forensic Toolkit\ 2.3\logs\	Points to a set of log files including a summary installation log to help Technical Support with troubleshooting.
KFF Logs	[drive]:\Program Files\ AccessData\KFF Library FTK 2.3	Records whether the Known File Filter was added to the schema.
FTK.exe	[drive]:\Program Files\ AccessData\Forensic Toolkit\ 2.3\bin\	Program executable

**TABLE C-1 FTK 2.3 Folders and File Locations**

File or Folder	Location	Function
FTK2_log.txt	[drive]:\Program Files\ AccessData\Forensic Toolkit\ 2.3\	Log file recording information specific to the application.
FTK2crash[timestamp].dmp	[drive]:\Program Files\AccessData\AccessData Forensic Toolkit\2. 2\ 	Dump file with the timestamp from an FTK crash.

## FILES AND FOLDERS FOR THE DATABASE

These files and folders exist on the computer running the Oracle database.

**TABLE C-2 Oracle Database File Locations**

File or Folder	Location	Function
ftk2	[drive]:\Oracle	Contains files FTK 2.3 uses to work with the Oracle database, such as JRE, libraries, configuration scripts, etc.
logs	[drive]:\Program Files\Oracle\Inventory	Contains installation logs intended to help Technical Support with installation troubleshooting.
FTK2_KFF.DBF	[drive]:\Oracle\ftk2\database	Contains the hashes that make up the AccessData Known File Filter.

## CHANGING REGISTRY OPTIONS

The following sections cover small changes that can be made to items in the registry to aid in the functionality and desired efficiency of FTK.



# *Appendix D Gathering Windows Registry Evidence*

This appendix contains information about the Windows Registry and what information can be gathered for evidence.

## **UNDERSTANDING THE WINDOWS REGISTRY**

For forensic work, registry files are particularly useful because they can contain important information such as the following:

- Usernames and passwords for programs, email, and Internet sites
- A history of Internet sites accessed, including dates and times
- 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

AccessData 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 or user. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible from within 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.

## WINDOWS 9X REGISTRY FILES

The following table describes each item on the Windows 9x registry files:

**TABLE D-1 Windows 9x Registry files**

Filename	Location	Contents
system.dat	\Windows	<ul style="list-style-type: none"> <li>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 Web sites, email 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.</li> <li>Lists installed programs, their settings, and any usernames and passwords associated with them.</li> <li>Contains the System settings.</li> </ul>
user.dat	\Windows If there are multiple user accounts on the system, each user has a user.dat file located in \Windows\profiles\user account	<ul style="list-style-type: none"> <li>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 see 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.</li> <li>User preference settings (desktop configuration, etc.).</li> </ul>

# WINDOWS NT AND WINDOWS 2000 REGISTRY FILES

The following table describes each item in the Windows NT and Windows 2000 registry files:

**TABLE D-2 Windows NT and Windows 2000 Registry Files**

Filename	Location	Contents
NTUSER.DAT	\Documents and Settings\[ <i>user account</i> ] If there are multiple user accounts on the system, each user has an ntuser.dat file.	<ul style="list-style-type: none"><li>• 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 Web sites, email 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.</li><li>• All installed programs, their settings, and any usernames and passwords associated with them.</li><li>• User preference settings (desktop configuration, etc.)</li></ul>
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

# WINDOWS XP REGISTRY FILES

The following table describes each item in the Windows XP registry files:

**TABLE D-3 Windows XP Registry Files**

Filename	Location	Contents
NTUSER.DAT	\Documents and Settings\ <i>[user account]</i> If there are multiple user accounts on the system, each user has an ntuser.dat file.	<ul style="list-style-type: none"><li>• 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 Web sites, email 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.</li><li>• All installed programs, their settings, and any usernames and passwords associated with them.</li><li>• User preference settings (desktop configuration, etc.)</li></ul>
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

The logical registry is organized into the following tree structure:

The top level of the tree is divided into hives. A hive is a discrete body of keys, subkeys, and values that is rooted at the top of the registry hierarchy. On Windows XP systems, the registry hives are as follows:

- HKEY\_CLASSES\_ROOT (HKCR)

- HKEY\_CURRENT\_USER (HKCU)
- HKEY\_LOCAL\_MACHINE (HKLM)
- HKEY\_USERS (HKU)
- HKEY\_CURRENT\_CONFIG (HKCC)
- HKEY\_DYN\_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 computer is docked, and another if the computer is not docked. Based on the computer 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.

## POSSIBLE DATA TYPES

The following table lists the Registry's possible data types:

**TABLE D-4 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 REG_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.
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_SZ	String Value	A text string of any length.
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 that 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_FULL_RESOURCE_DESCRIPTOR	Binary Value	A series of nested arrays designed to store a resource list used by a physical hardware device. This data is displayed in hexadecimal format as a Binary Value.

**TABLE D-4 Possible Data Types**

<b>Data Type</b>	<b>Name</b>	<b>Description</b>
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_LINK	Link	A Unicode string naming a symbolic link.
REG_QWORD	QWORD Value	Data represented by a number that is a 64-bit integer.

## 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 suspect(s).
- 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 9x 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:

- Load the suspect's drive image and export his or her registry files to view them 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 see hex or binary values in the registry.
- Use Registry Viewer. Registry Viewer integrates seamlessly with FTK 2.3 to display registry files within the image and create reports.

**Important:** Registry Viewer shows everything you normally see 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 it displays values in the Protected Storage System Provider key (PSSP). Registry Viewer also shows information that is normally hidden in null-terminated keys.

## SEIZING WINDOWS SYSTEMS

Information stored in the registry—Internet Messenger sessions, Microsoft Office MRU lists, usernames and passwords for Internet Web sites 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.

**Note:** Passwords and MRU lists are not saved unless these options are enabled.

**Important:** Because normal seizure procedures require that there be no alteration of the suspect's computer in any way, you must be able to articulate why you closed any active applications before pulling the plug on the suspect's computer. Sometimes it is better to simply pull the plug on the computer; other times, it makes more sense to image the computer in place while it is on. It may depend on what is the most important type of data expected to be found on the computer.

For example, Windows updates some program information in the registry when the changes are made. Other information is not updated until a program is closed. Also, if the computer's drive is encrypted and you cannot decrypt it or don't have the Key or password, you may have no choice except to image the live drive.

The Registry Quick Find Chart gives more information.

## REGISTRY QUICK FIND CHART

The following charts discuss common locations where you can find data of forensic interest in the Windows Registry.



## SYSTEM INFORMATION

**TABLE D-5 System Information From HKLM**

Information	File or Key	Location	Description
Registered Owner	Software	Microsoft\Windows NT\CurrentVersion	This information is entered during installation, but can be modified later.
Registered Organization	Software	Microsoft\Windows NT\CurrentVersion	This information is entered during installation, but can be modified later.
Run	Software	Microsoft\Windows\CurrentVersion\Run	Programs that appear in this key run automatically when the system boots.
Logon Banner Message	Software	Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	This is a banner that users must click through to log on to a system.
Mounted Devices	System	MountedDevices	Database of current and prior mounted devices that received a drive letter.
Current Control Set	System	Select	Identifies which control set is current.
Shutdown Time	System	ControlSetXXX\Control\Windows	System shutdown time.
Event Logs	System	ControlSetXXX\Services\Eventlog	Location of Event logs.
Dynamic Disk	System	ControlSetXXX\Services\DMIO\Boot Info\Primary Disk Group	Identifies the most recent dynamic disk mounted in the system.
Pagefile	System	ControlSetXXX\Control\Session Manager\Memory Management	Location, size, set to wipe, etc.
Last User Logged In	Software	Microsoft\Windows NT\CurrentVersion\Winlogon	Last user logged in - can be a local or domain account.
Product ID	Software	Microsoft\Windows NT\CurrentVersion	
O\S Version	Software	Microsoft\Windows NT\CurrentVersion	
Logon Banner Title	Software	Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	User-defined data.
Logon Banner Message	Software	Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	User-defined data.
Time Zone	System	ControlSet001(or002)\Control\TimeZoneInformation\StandardName	This information is entered during installation, but can be modified later.

## NETWORKING

**TABLE D-6 Registry Networking Information**

Information	File or Key	Location	Description
Map Network Drive MRU	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	Most recently used list of 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	Contains user security identifiers (only users with profile on the system).
Network Map	NTUSER.DAT	Documents and Settings\username	Browser history and last-viewed lists attributed to the user.

## USER DATA

**TABLE D-7 Registry User Data Information**

Information	File or Key	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.

**TABLE D-7 Registry User Data Information**

Information	File or Key	Location	Description
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

**TABLE D-8 Registry User Application Data Information**

Information	File or Key	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 URLs	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 password-encrypted values.
IE Auto-Complete Web Addresses	NTUSER.DAT	\Software\Microsoft\Protected Storage System Provider	Lists Web pages where auto complete was used.
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.

**TABLE D-8 Registry User Application Data Information**

<b>Information</b>	<b>File or Key</b>	<b>Location</b>	<b>Description</b>
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 E Managing Security Devices and Licenses*

This chapter acquaints you with the managing AccessData product licenses. Here you will find details regarding the LicenseManager interface and how to manage licenses and update products using LicenseManager.

## **NLS SUPPORT**

Beginning with the PRTK 6.4 and DNA 3.4 release, AccessData's Network License Service (NLS) is supported. If you have NLS, you should also have documentation on how to install and implement it.

## **INSTALLING AND MANAGING SECURITY DEVICES**

Before you can manage licenses with LicenseManager, you must install the proper security device software and/or drivers. This section explains installing and using the Wibu CodeMeter Runtime software and USB CmStick, as well as the Keylok USB dongle drivers and dongle device.

## **INSTALLING THE SECURITY DEVICE**

As discussed previously, AccessData products require a licensing security device that communicates with the program to verify the existence of a current license. The device can be the older Keylok dongle, or the newer Wibu CmStick. Both are USB devices, and both require specific software to be installed prior to connecting the devices and running your AccessData products. You will need:

- The Wibu CodeMeter Runtime software with a Wibu CodeMeter (CmStick)
- The Wibu CodeMeter Runtime software, and the AccessData Dongle Drivers with a Keylok dongle

**Note:** The Codemeter Runtime software and either a silver Wibu CmStick or a green Keylok dongle are required to run PRTK or DNA. Without them, you can run PRTK or DNA in Demo mode only.

The CmStick or dongle should be stored in a secure location when not in use.

You can install PRTK and the CodeMeter software from the shipping CD or from downloadable files available on the AccessData website at [www.accessdata.com](http://www.accessdata.com). Click *Support > Downloads*, and browse to the product to download. Click the download link and save the file locally prior to running the installation files.

For solutions to commonly asked installation questions, see “Chapter 11 Troubleshooting” on page 189.

## INSTALLING THE CODEMETER RUNTIME SOFTWARE

When you purchase the full PRTK package, AccessData provides a USB CmStick with the product package. The green Keylok dongles are no longer provided, but can be purchased separately through your AccessData Sales Representative.

To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping CD, or from the setup file downloaded from the AccessData Web site.

### LOCATING THE SETUP FILE

To install the CodeMeter Runtime software from the CD, you can browse to the setup file, or select it from the Autorun menu.

To download the CodeMeter Runtime software, go to [www.accessdata.com](http://www.accessdata.com) and do the following:

1. Click *Support > Downloads*.
2. Find
  - 2a. CodeMeter Runtime 3.30a (32 bit)  
MD5: 9F299EC832152E593D9E8D76F199C723  
(MD5 hash applies only to this version)

### OR

- 2b. CodeMeter Runtime 3.30a (64 bit)

MD5: 1140085cbbd0f15ade393f632b56d00c

(MD5 hash applies only to this version)

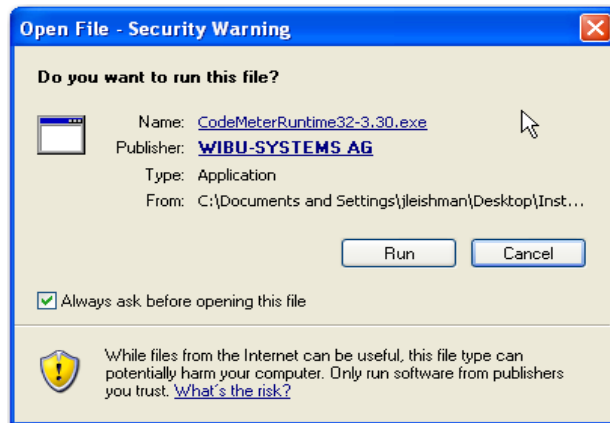
3. Click the *Download* link.
4. Save the file to your PC and run after the download is complete.

When the download is complete, double-click on the **CodeMeterRuntime32-3.30.exe** or the **CodeMeterRuntime64-3.30.exe**.

## RUNNING THE CODEMETER RUNTIME SETUP

Whichever way you choose to access the CodeMeter Runtime setup file, when you run it you will see the following:

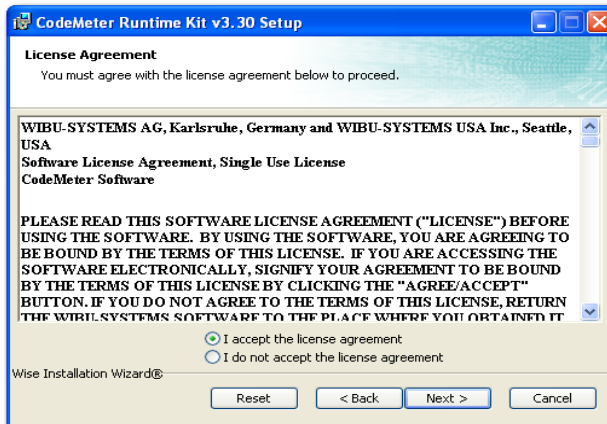
1. The CodeMeter Runtime Open File Security Warning will appear to allow you to verify that you really want to open this file.



2. Click *Run*.



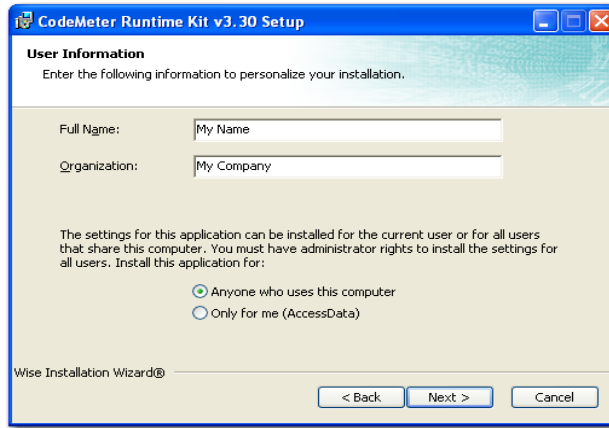
3. On the Welcome screen, click *Next*.



4. Accept the License Agreement.



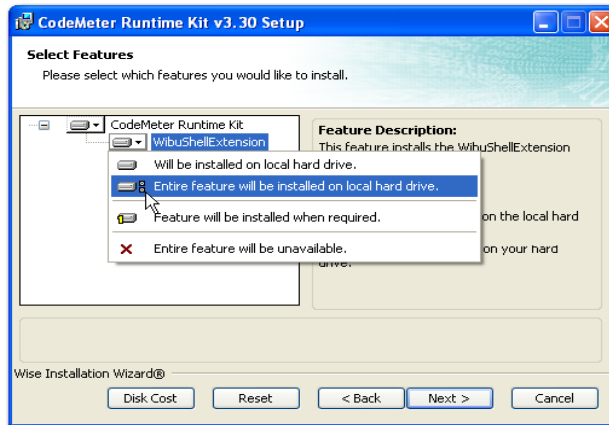
5. Click *Next*.



6. In the User Information screen, enter your name and your company name.

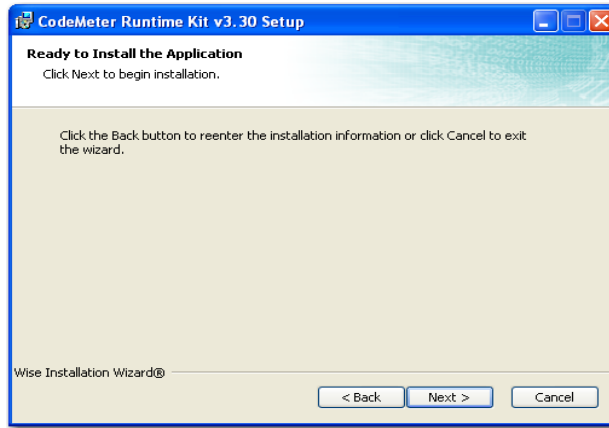
7. Specify whether this application should be available only when you log in, or for anyone who uses this computer.

8. Click *Next*.



9. Select the features you want to install.

10. Click *Next*.



11. When you are satisfied with the options you have selected, click *Next*.



12. Installation will run its course. When complete, you will see the “CodeMeter Runtime Kit v3.30 has been successfully installed” screen. Click *Finish* to exit the installation.

## THE CODEMETER CONTROL CENTER

When the CodeMeter Runtime installation is complete, the CodeMeter Control Center pops up. This is a great time to connect the CmStick and verify that the device is recognized and is Enabled. Once verified, you can close the control center and run your AccessData product(s).

For the most part there is nothing you need to do with this control center, and you need make no changes using this tool with very few exceptions. If you have problems

with your CmStick, contact AccessData Support and an agent will walk you through any troubleshooting steps that may need to be performed.

## INSTALLING KEYLOK DONGLE DRIVERS

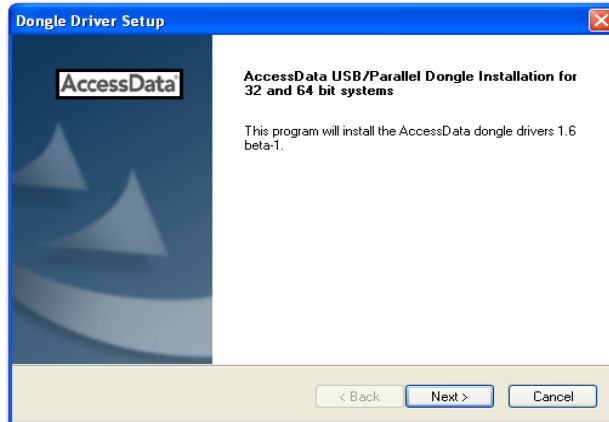
To install the Keylok USB dongle drivers do the following:

1. If installing from CD, insert the CD into the CD-ROM drive and click *Install the Dongle Drivers*.

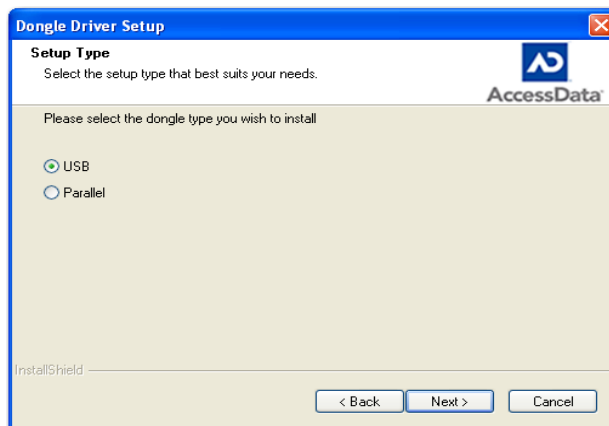
If auto-run is not enabled, select *Start > Run*. Browse to the CD-ROM drive and select *Autorun.exe*.

### OR

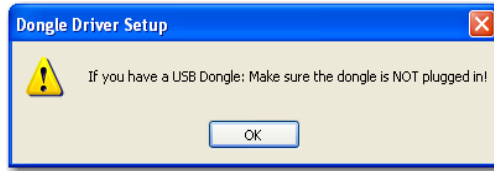
1. If installing from a file downloaded from the AccessData Web site, locate the *Dongle\_driver\_1.6.exe* setup file, and double-click it.



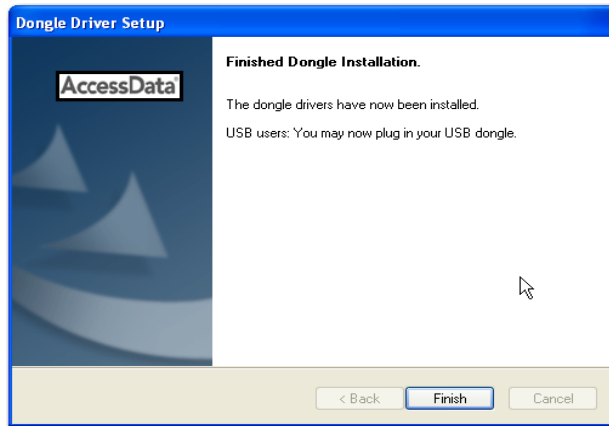
2. Click *Next*.



3. Select the type of dongle to install the drivers for.
4. Click *Next*.



5. If you have a USB dongle, verify that it is not connected.
6. Click *Next*.



7. Click *Finish*.
8. Connect the USB dongle. Wait for the Windows Found New Hardware wizard, and follow the prompts.

**Important:** If the Windows Found New Hardware wizard appears, complete the wizard. Do not close without completing, or the dongle driver will not be installed.

## WINDOWS FOUND NEW HARDWARE WIZARD

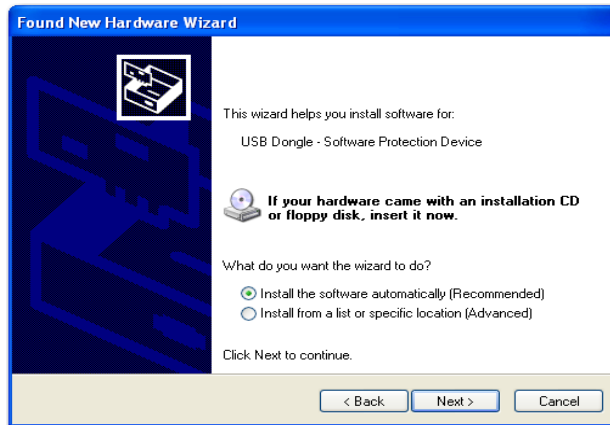
When you connect the dongle after installing the dongle drivers, you should wait for the Windows Found New Hardware Wizard to come up. It is not uncommon for users to disregard this wizard, and then find that the dongle is not recognized and their AccessData software will not run.

When the Found New Hardware Wizard pops up, do the following:

1. When prompted whether to connect to Windows Update to search for software, choose, “No, not this time”.



2. Click *Next*.
3. When prompted whether to install the software automatically or to install from a list of specific locations, choose, “Install the software automatically (Recommended)”.



4. Click *Next*.

5. Click *Finish* to close the wizard.



Once you have installed the dongle drivers and connected the dongle and verified that Windows recognizes it, you can use LicenseManager to manage product licenses.

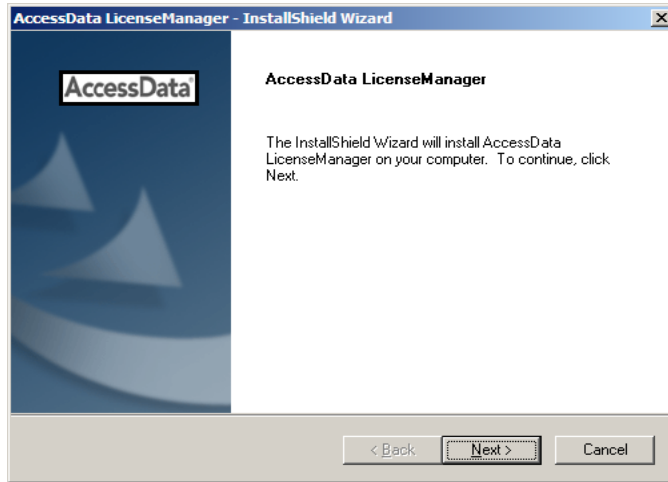
## INSTALLING LICENSEMANAGER

LicenseManager lets you manage product and license subscriptions using a security device or device packet file.

To install LicenseManager from the downloadable file:

1. Go to the AccessData download page at <http://www.accessdata.com/downloads.htm>.
2. On the download page, click the LicenseManager *Download* link.
3. Save the installation file (currently `lm-license_manager-2.2.4.exe`) to a temporary directory on your drive.
4. To launch the installation program, go to the temporary directory and double-click the installation file you downloaded in step 3.

5. Click *Next* on the Welcome screen.

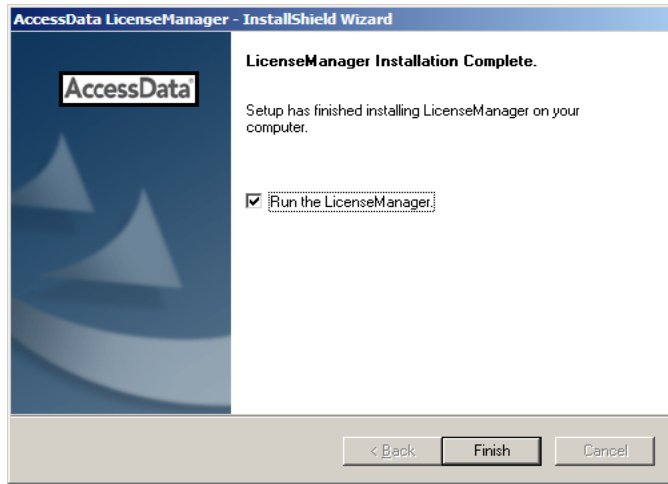



6. Click *Yes* to accept the license agreement.



7. Wait while the installation completes.

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



Run LicenseManager later by selecting  
*Start > Programs > AccessData > LicenseManager > LicenseManager*  
or by double-clicking the LicenseManager icon on your desktop  .

## MANAGING LICENSES WITH LICENSEMANAGER

LicenseManager manages AccessData product licenses on a Keylok dongle or Wibu CodeMeter Stick security device, or in a security device packet file. LicenseManager and the CodeMeter Stick installation are no longer integrated with FTK2 installation.

LicenseManager displays license information, allows you to add or remove existing licenses to a dongle or CmStick. LicenseManager can also be used to export a security device packet file. Packet files can be saved and reloaded onto the dongle or CmStick, or sent via email to AccessData support.

In addition, you can use LicenseManager to check for product updates and download the latest product versions.

LicenseManager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all AccessData products. The Purchase Licenses button connects directly to the AccessData website and allows you to browse the site for information about products you may wish to purchase. Contact AccessData by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.



LicenseManager provides information as displayed in the following figures:

Figure 5-1 LicenseManager Installed Components Tab

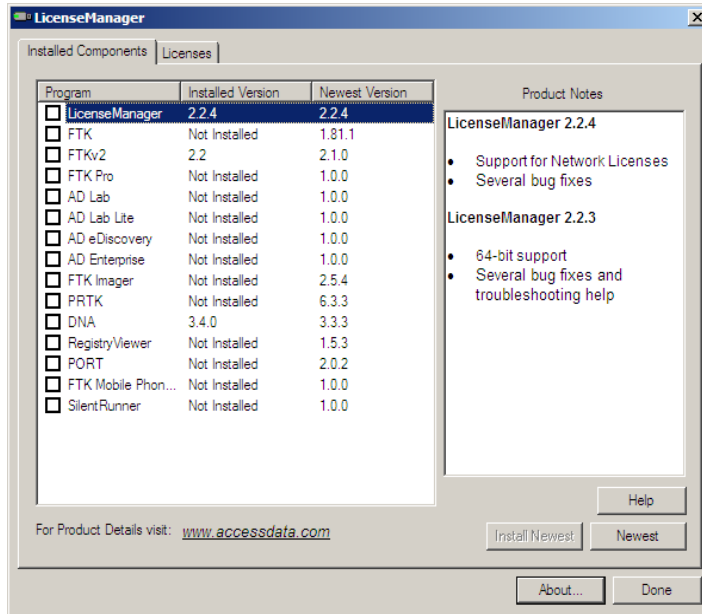
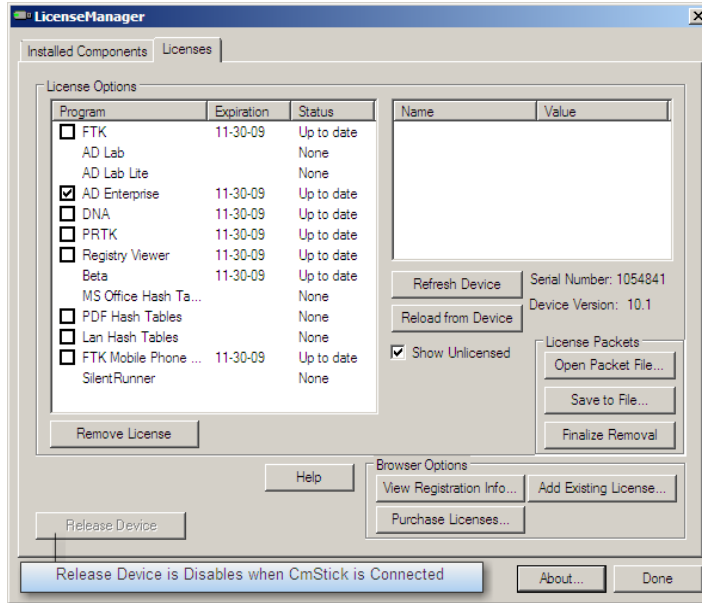


Figure 5-2 LicenseManager Licenses Tab




## STARTING LICENSEMANAGER

LicenseManager.exe is located in C:\Program Files\AccessData\Common Files\AccessData LicenseManager\. You can execute the program from this location if you wish.

Click *Start > All Programs > AccessData > LicenseManager > LicenseManager*,

OR

Click or double-click (depending on your Windows settings) the *LicenseManager* icon on your desktop .

OR

From some AccessData programs, you can run LicenseManager from the *Tools > Other Applications* menu. This option is not available in PRTK or DNA.



The LicenseManager program opens.

When starting LicenseManager, License Manager reads licensing and subscription information from the installed and connected Wibu CodeMeter Stick, or Keylok dongle.

If using a Keylok dongle, and LicenseManager either does not open or displays the message, “Device Not Found”, do the following:

1. Make sure the correct dongle driver is installed on your computer.
2. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
3. Remove the dongle after the device has been uninstalled.
4. Reboot your computer.
5. After the reboot is complete, and all startup processes have finished running, connect the dongle.
6. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, “No, not this time.”
7. Click *Next* to continue.
8. On the next options screen, choose, “Install the software automatically (Recommended)”
9. Click *Next* to continue.
10. When the installation of the dongle device is complete, click *Finish* to close the wizard.
11. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run LicenseManager.

If using a CodeMeter Stick, and LicenseManager either does not open or displays the message, “Device Not Found”, do the following:

1. Make sure the CodeMeter Runtime 3.30a software is installed. It is available at [www.accessdata.com/support](http://www.accessdata.com/support). Click Downloads and browse to the product. Click on the download link. You can Run the product from the Website, or Save the file locally and run it from your PC. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray: .
2. Make sure the CodeMeter Stick is connected to the USB port. When the CmStick is then connected, you will see the icon change to look like this: .

If the CodeMeter Stick is not connected, LicenseManager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

To open LicenseManager without a CodeMeter Stick installed:

1. Click *Tools > LicenseManager*.

LicenseManager displays the message, “Device not Found”.

2. Click *OK*, then browse for a security device packet file to open.

**Note:** Although you can run LicenseManager using a packet file, FTK 2.3 will not run with a packet file alone. You must have the CmStick connected to the computer to run FTK 2.3.

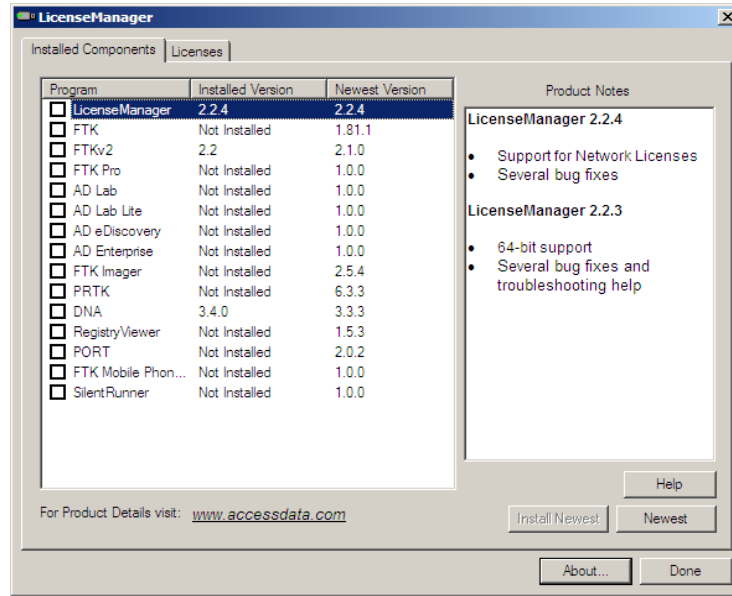
## THE LICENSEMANAGER INTERFACE

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 the machine. The Installed Components tab is displayed in the following figure.

Figure 5-3 LicenseManager Installed Components



The following information is displayed on the Installed Components tab:

**TABLE 5-1 LicenseManager Installed Components Tab Features**

Item	Description
Program	Lists all AccessData products installed on the host.
Installed Version	Displays the version of each AccessData product installed on the host.
Newest Version	Displays the latest version available of each AccessData product installed on the host. Click Newest to refresh this list.
Product Notes	Displays notes and information about the product selected in the program list.
AccessData Link	Links to the AccessData product page where you can learn more about AccessData products.

The following buttons provide additional functionality from the Installed Components tab:

**TABLE 5-2 LicenseManager Installed Components Buttons**

---

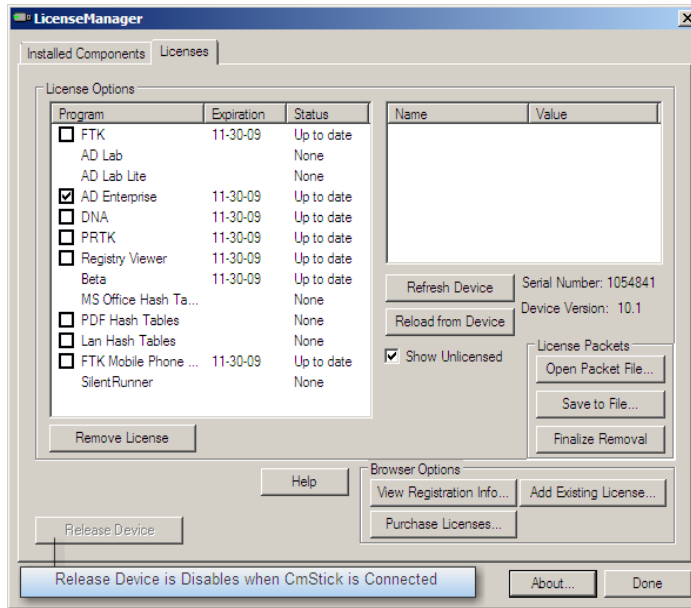
<b>Button</b>	<b>Function</b>
Help	Opens the LicenseManager Help web page.
Install Newest	Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser.
Newest	Updates the latest version information for your installed products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

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 CodeMeter Stick information for the current security device packet file and licensing information for AccessData products available to the owner of the CodeMeter Stick, as displayed in the following figure.

Figure 5-4 LicenseManager Licenses Tab



The Licenses tab provides the following information:

**TABLE 5-3 LicenseManager Licenses Tab Features**

Column	Description
Program	Shows the owned licenses for AccessData products.
Expiration Date	Shows the date on which your current license expires.
Status	Shows these status of that product's license: <ul style="list-style-type: none"> <li>• <b>None:</b> the product license is not currently owned</li> <li>• <b>Days Left:</b> displays when less than 31 days remain on the license.</li> <li>• <b>Never:</b> the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables.</li> </ul>
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 contained in or required for its license.
Show Unlicensed	When checked, the License window displays all products, whether licensed or not.

The following license management actions can be performed using buttons found on the License tab:

**TABLE 5-4 License Management Options**

<b>Button</b>	<b>Function</b>
Remove License	Removes a selected license from the Licenses window and from the CodeMeter Stick or dongle. Opens the AccessData License Server web page to confirm success.
Refresh Device	Connects to the AccessData License Server. Downloads and overwrites the info on the CodeMeter Stick or dongle with the latest information on the server.
Reload from Device	Begins or restarts the service to read the licenses stored on the CodeMeter Stick or dongle.
Release Device	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.  This option is disabled for the CodeMeter Stick.
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. The default location is My Documents.
Finalize Removal	Finishes the removal of licenses in the unbound state. Licenses must be unbound from the CmStick or dongle before this button takes effect.
View Registration Info	Displays an HTML page with your CodeMeter Stick number and other license information.
Add Existing License	Allows you to bind an existing unbound license to your CodeMeter Stick, through an internet connection to the AccessData License Server.
Purchase License	Brings up the AccessData product page from which you can learn more about AccessData products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.



## OPENING AND SAVING DONGLE PACKET FILES

You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

To save a security device packet file:

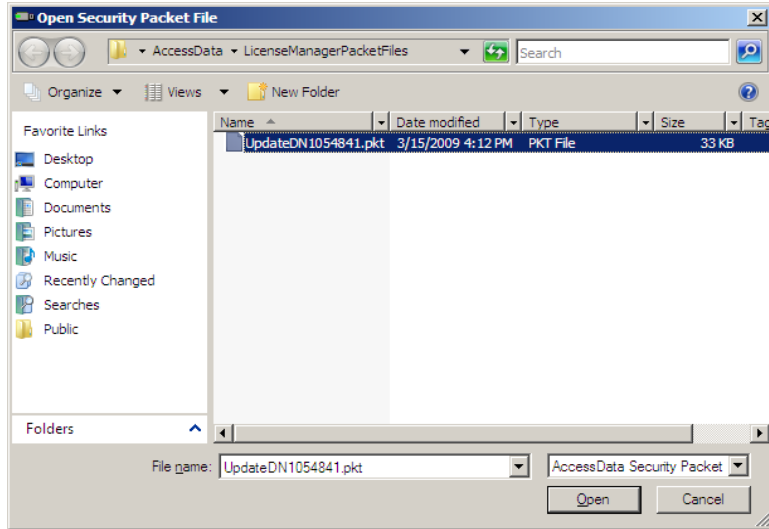
1. Click the *Licenses* tab, then under License Packets, click *Save to File*.
2. Browse to the desired folder and accept the default name of the **.pkt** file; then click *Save*.

**Note:** In general, the best place to save the .pkt files is in the AccessData LicenseManager folder. The default path is C:\Program Files\AccessData\Common Files\AccessData LicenseManager\.

To open a security device packet file:

1. Select the *Licenses* tab, then under License Packets, click *Open Packet File*.
2. Browse for a dongle packet file to open. Select the file, then click *Open*.

Figure 5-5 LicenseManager Open Packet File



## ADDING AND REMOVING PRODUCT LICENSES

On a computer with an Internet connection, LicenseManager lets you add available product licenses to, or remove them from, a dongle.

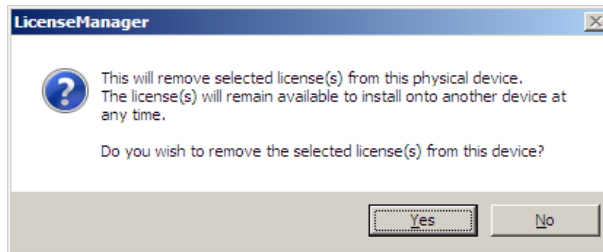
To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and LicenseManager, click on the Licenses tab to add the product license to the second dongle.

### REMOVE A LICENSE

To remove (unassociate) a product license:

1. From the Licenses tab, mark the program license to remove. This action activates the Remove License button below the Program list box.
2. Click *Remove License*. This connects your machine to the AccessData License Server through the Internet.

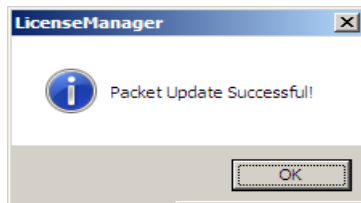
3. You will be prompted to confirm the removal of the selected license(s) from the device.



Click *Yes* to continue, or *No* to cancel.

4. You will see some screens indicating the connection and activity on the License Server, and when the license removal is complete, you will see the following screen:

Figure 5-6 Packet Update Successful



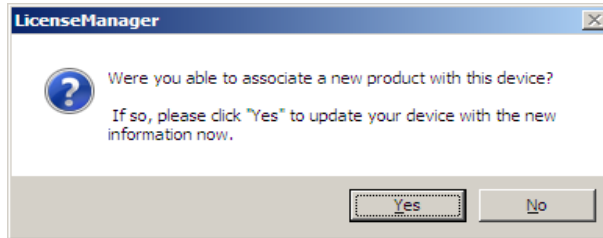
5. Click OK to close the message box. You will then see an Internet browser screen from LicenseManager with a message that says, “The removal of your license(s) from Security Device was successful?” You may close this box at any time.

## ADD A LICENSE

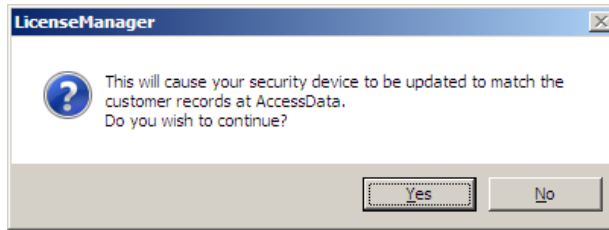
To add a new or released license:

1. From the Licenses tab, under Browser Options, click *Add Existing License*.  
The AccessData LicenseManager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click *Submit*.
2. An AccessData LicenseManager Web page will open, displaying the following message, “The AccessData product(s) that you selected has been bound to the record for Security Device *nnnnnnn* within the Security Device Database.

“Please run LicenseManager’s “Refresh Device” feature in order to complete the process of binding these product license(s) to this Security Device.” You may close this window at any time.



3. Click *Yes* if LicenseManager prompts, “Were you able to associate a new product with this device?”
4. Click *Refresh Device* in the Licenses tab of LicenseManager. Click *Yes* when prompted.



You will see the newly added license in the License Options list.

## ADDING AND REMOVING PRODUCT LICENSES REMOTELY

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, such as a forensic lab computer, that does not have an Internet connection.

If 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, and 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.

### ADD A LICENSE REMOTELY

To remotely add (associate) a product license:

1. On the computer where the security device resides:
  - 1a. Run LicenseManager.
  - 1b. From the *Licenses* tab, click *Reload from Device* to read the dongle license information.
  - 1c. Click *Save to File* to 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. Remove any attached security device.
  - 3b. Launch LicenseManager. You will see a notification, “No security device found”.
  - 3c. Click *OK*.
  - 3d. An “Open” dialog box will display. Highlight the *.pkt* file, and click *Open*.
  - 3e. Click on the *Licenses* tab.
  - 3f. Click *Add Existing License*.
  - 3g. Complete the process to add a product license on the *Website* page.
  - 3h. Click *Yes* when the LicenseManager prompts, “Were you able to associate a new product with this dongle?”
  - 3i. 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, *[serial#].wibuCmRaU*.
  - 3j. 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 by double-clicking it. (It is an executable file.)
  - 5b. After an update file downloads and installs, click *OK*.
  - 5c. Run LicenseManager.
  - 5d. From the *Licenses* tab, click *Reload from Device* to verify the product license has been added to the dongle.

## REMOVE A LICENSE REMOTELY

To remotely remove (unassociate) a product license:

1. On the computer where the dongle resides:
  - 1a. Run LicenseManager.

- 1b. From the Licenses tab, click *Reload from Device* to read the dongle license information.
- 1c. Click *Save to File* to 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. Launch LicenseManager. You will see a notification, “No security device found”.
  - 3b. Click *OK*.
  - 3c. An “Open” dialog box will display. Highlight the *.pkt* file, and click *Open*.
  - 3d. Click on the Licenses tab.
  - 3e. Mark the box for the product license you want to unassociate; then click *Remove License*.
  - 3f. When prompted to confirm the removal of 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.
  - 3g. Click *Yes* to save the update file to the local computer.

The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.
  - 3h. 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 by double-clicking it. This runs the executable update file and copies the new information to the security device.
  - 5b. Run LicenseManager
  - 5c. On the Licenses tab, click *Reload from Device* in LicenseManager to read the security device and allow you to verify the product license is removed from the dongle.
  - 5d. Click *Save to File* to save the updated dongle packet file to the local machine.
6. Copy the file to a computer with an Internet connection.

## 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, see the AccessData Website at [http://www.accessdata.com/subscription\\_renewal.htm](http://www.accessdata.com/subscription_renewal.htm).

## CHECK FOR PRODUCT UPDATES

To check for product updates, on the Installed Components tab, click *Newest*. This refreshes the list to display what version you have installed, and the newest version available.

## DOWNLOAD PRODUCT UPDATES

To install the newest version, mark the box next to the product to install, then click Install Newest.

**Note:** Some products, such as FTK 2.x, Enterprise, and others, are too large to download, and are not available. A notification displays if this is the case.

To download a product update:

1. Ensure that LicenseManager displays the latest product information by clicking the Installed Components tab. Click *Newest* to refresh the list showing the latest releases, then compare your installed version to the latest release.  
If the latest release is newer than your installed version, you may be able to install the latest release from our Website.
2. Ensure that the program you want to install is not running.
3. Mark the box next to the program you want to download; then click *Install Newest*.
4. When prompted, click *Yes* to download and install the latest install version of the product.
5. If installing the update on a remote computer, copy the product update file to another computer.
6. Install the product update.

For information about installing the product update, refer to the installation information for the product. You may need to restart your computer after the update is installed.

## PURCHASE PRODUCT LICENSES

Use LicenseManager to link to the AccessData Web site to find information about all our products.

Purchase product licenses through your AccessData Sales Representative. Call 801-377-5410 and follow the prompt for Sales, or send an email to [sales@accessdata.com](mailto:sales@accessdata.com).

**Note:** Once a product has been purchased and appears in the AccessData License Server, add the product license to a CodeMeter Stick, dongle, or security device packet file by clicking *Refresh Device*.

## SEND A DONGLE PACKET FILE TO SUPPORT

Send a security device packet file *only* when specifically directed to do so by AccessData support.

To create a dongle packet file, do the following:

1. Run LicenseManager
2. Click on the Licenses tab.
3. Click *Load from Device*.
4. Click *Refresh Device* if you need to get the latest info from AD's license server.
5. Click *Save to File*, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to:  
[support@accessdata.com](mailto:support@accessdata.com).

**Note:** For a more complete list of AccessData Corporation's contact information, see "AccessData Contact Information" on page iii.



# *AccessData Glossary*

## **A**

### **AccessData Recovery Session**

In PRTK, selecting one or more files and starting the password recovery process is called an AccessData Recovery (ADR) session. Typically, each case has one session unless you have a large number of encrypted files.

### **Address**

A location of data, usually in main memory or on a disk. You can think of computer memory as an array of storage boxes, each of which is one byte in length. Each storage box has an address (a unique number) assigned to it. By specifying a memory address, programmers can access a particular byte of data. Disks are divided into tracks and sectors, each of which has a unique address.

### **Advanced Encryption Standard**

A common symmetric encryption system that has replaced Data Encryption Standard as the encryption standard. It uses a 128, 192, or 256-bit key.

### **Application Administrator**

The first user created in an AccessData FTK2 system. The Application Administrator has all rights within the application, including adding users and assigning roles. Application Administrators can assign the role of Application Administrator to new users as they are created.

## Asymmetric Encryption

A type of encryption in which the encryption and decryption keys are different. Asymmetric encryption uses a public key (which can be posted on an Internet site or made “public” through other means) and a private key, which remains secret. In this system, something that has been encrypted with the private key can be decrypted only by the public key, and vice versa. Asymmetric algorithms are slower than symmetric algorithms, but can nonetheless be very useful. They are often used in combination with symmetric algorithms, as with EFS Encryption.

The number of possible key values refers to the actual number of different key words or passwords that can exist, based on the particular algorithm used to create the key value in question. A  $n$ -bit key has  $2^n$  possible values. For example, a 40-bit key has 240 possible values, or 1,099,511,627,776 possibilities.

The security of an algorithm should rely on the secrecy of the key only, not the secrecy of the algorithm.

Do not compare key sizes between symmetric and asymmetric algorithms. For example, a 128-bit symmetric key is approximately as strong as a 512-bit asymmetric key.

## B

### BestCrypt

A common symmetric encryption system that can be used with any of the following hash functions and encryption algorithms:

**TABLE Glossary-1 BestCrypt Hash Functions and Encryption Algorithms**

---

• GOST	• CAST
• SHA-1 Hash	• AES
• Blowfish	• RC6
• IDEA	• 3DES encryption
• Twofish	•

### Binary

Pertaining to a number system that has just two unique digits. Computers are based on the binary numbering system, which consists of just two unique numbers, 0 and 1. All

operations that are possible in the decimal system (addition, subtraction, multiplication, and division) are equally possible in the binary system.

## **BIOS**

Acronym for Basic Input/Output System. The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

## **Bit-stream Image**

See “Forensic Image” on page 334.

## **Bookmark**

A menu entry or icon on a computer that is most often created by the user and that serves as a shortcut to a previously viewed location (as an Internet address). The term “bookmark” as used in a Computer Crimes Unit report refers to locating a file, folder or specific item of interest to the examiner or to the investigator. The location of the data (file name, file location, relative path, and hardware address) is identified. Other data can be addressed as well.

## **Boot**

To load the first piece of software that starts a computer. Because the operating system is essential for running all other programs, it is usually the first piece of software loaded during the boot process.

## **Boot Record**

All the three types of FAT have a boot record, which is located within an area of reserved sectors. The DOS format program reserves 1 sector for FAT12 and FAT16 and usually 32 sectors for FAT32.

# **C**

## **Chunk Size**

The number of passwords the supervisor machine can process in the amount of time specified.

## Cluster

Fixed-length blocks that store files on the FAT media. Each cluster is assigned a unique number by the computer operating system. Only the part of the partition called the “data area” is divided into clusters. The remainder of the partition are defined as sectors. Files and directories store their data in these clusters. The size of one cluster is specified in a structure called the Boot Record, and can range from a single sector to 128 sectors. The operating system assigns a unique number to each cluster and the keeps track of files according to which cluster they use.

## CMOS

Short for Complementary Metal Oxide Semiconductor. Pronounced SEE-moss, CMOS is a widely used type of semiconductor. CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor. This makes them particularly attractive for use in battery-powered devices, such as portable computers. Personal computers also contain a small amount of battery-powered CMOS memory to hold the date, time, and system setup parameters.

## CRC

Short for Cyclical Redundancy Check. It performs a complex calculation on every byte in the file, generating a unique number for the file in question. If so much as a single byte in the file being checked were to change, the cyclical redundancy check value for that file would also change. If the CRC value is known for a file before it is downloaded, you can compare it with the CRC value generated by this software after the file has been downloaded to ascertain whether the file was damaged in transit. The odds of two files having the same CRC value are even longer than the odds of winning a state-run lottery—along the lines of one in 4,294,967,296.

## Cylinder

A single-track location on all the platters making up a hard disk. For example, if a hard disk has four platters, each with 600 tracks, then there will be 600 cylinders, and each cylinder will consist of 8 tracks (assuming that each platter has tracks on both sides).

## D

### **dd**

(Linux) Makes a copy of a input file (STDIN) using the specified conditions, and sends the results to the output file (STDOUT).

### **Data Carving**

Data carving is the process of extracting a collection of data from a larger data set. Data carving techniques frequently occur during a digital investigation when the unallocated file system space is analyzed to extract files. The files are “carved” from the unallocated space using file type-specific header and footer values. File system structures are not used during the process.

### **Data Encryption Standard**

A 56-bit symmetric encryption system that is considered weak by current standards. It has been broken in a distributed environment.

### **Device**

Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, mice, and modems. These particular devices fall into the category of peripheral devices because they are separate from the main computer.

Most devices, whether peripheral or not, require a program called a device driver that acts as a translator, converting general commands from an application into specific commands that the device understands.

### **Disk**

A round plate on which data can be encoded. There are two basic types of disks: magnetic disks and optical disks.

## E

## Encrypting File System (EFS)

EFS is a file system driver that provides filesystem-level encryption in Microsoft Windows (2000 and later ) operating systems, except Windows XP Home Edition, Windows Vista Basic, and Windows Vista Home Premium. The technology enables files to be transparently encrypted on NTFS file systems to protect confidential data from attackers with physical access to the computer.

## EnScript (also “e script”)

EnScript is a language and API that has been designed to operate within the EnCase environment. EnScript is compatible with the ANSI C++ standard for expression evaluation and operator meanings but contains only a small subset of C++ features. In other words, EnScript uses the same operators and general syntax as C++ but classes and functions are organized differently.

## Evidence Item

A physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive.

# F

## File Allocation Table (FAT)

A table that the operating system uses to locate files on a disk. A file may be divided into many sections that are scattered around the disk. The FAT keeps track of all these pieces.

There is a field in the Boot Record that specifies the number of FAT copies. With FAT12 and FAT16, MS-DOS uses only the first copy, but the other copies are synchronized. FAT32 was enhanced to specify which FAT copy is the active one in a 4-bit value part of a Flags field.

Think of the FAT as a singly linked list. Each of the chains in the FAT specify which parts of the disk belong to a given file or directory.

A file allocation table is a simple array of 12-bit, 16-bit, or 32-bit data elements. Usually there will be two identical copies of the FAT.

**FAT12:** The oldest type of FAT uses a 12-bit binary number to hold the cluster number. A volume formatted using FAT12 can hold a maximum of 4,086 clusters, which is  $2^{12}$  minus a few values (to allow for reserved values to be used in the FAT). FAT12 is most suitable for very small volumes, and is used on floppy disks and hard disk partitions smaller than about 16 MB (the latter being rare today.)

**FAT16:** The FAT used for older systems, and for small partitions on modern systems, uses a 16-bit binary number to hold cluster numbers. When you see someone refer to a FAT volume generically, they are usually referring to FAT16, because it is the de facto standard for hard disks, even with FAT32 now more popular than FAT16. A volume using FAT16 can hold a maximum of 65,526 clusters, which is  $2^{16}$  less a few values (again for reserved values in the FAT). FAT16 is used for hard disk volumes ranging in size from 16 MB to 2,048 MB. VFAT is a variant of FAT16.

**FAT32:** The newest FAT type, FAT32 is supported by newer versions of Windows, including Windows 95's OEM SR2 release, as well as Windows 98, Windows ME, and Windows 2000. FAT32 uses a 28-bit binary cluster number—not 32 because 4 of the 32 bits are reserved. 28 bits is still enough to permit very large volumes—FAT32 can theoretically handle volumes with over 268 million clusters, and will theoretically support drives up to 2 TB in size. To do this, however, the size of the FAT grows very large.

VFAT features the following key improvements compared to FAT12 and FAT16:

- **Long File Name Support:** Prior to Windows 95, FAT was limited to the eleven-character (8.3) file name restriction. VFAT's most important accomplishment enabled the use of long file names by the Windows 95 operating system and applications written for it, while maintaining compatibility with older software that had been written before VFAT was implemented.
- **Improved Performance:** The disk access and file system management routines for VFAT were rewritten using 32-bit protected-mode code to improve performance. At the same time, 16-bit code was maintained, for use when required for compatibility.
- **Better Management Capabilities:** Special support was added for techniques like disk locking to allow utilities to access a disk in exclusive mode without fear of other programs using it in the meantime.

## File Header

The data at the beginning of a file that identifies the file type: .gif, .doc, .txt, etc.

## File Footer

The data at the end of the file signifying the file is complete and allows the file to be understood by the operating system.

## File Item

Any item FTK can parse from the evidence. This includes complete files as well as sub-elements such as graphics, files, or OLE objects embedded in other files; deleted items recovered from unallocated space; and so forth.

## 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.

## Forensic Image

A process where all areas of a physical disk are copied, sector by sector, to storage media. This image may be a raw file, as in the case of the Linux utility DD, or it may be a forensically correct copy, such as SPADA provides. These images replicate exactly all sectors on a given storage device. All files, unallocated data areas, and areas not normally accessible to a user are copied.

## Forensically Prepared Media

Digital media (such as a diskette, tape, CD, hard drive) that is sanitized (wiped clean) of all data. This means computer media that may be sanitized up to the Department of Defense standards 5220.22-M (National Industrial Security Program Operating Manual Supplement) using software wipe utilities such as Dan Mares (Maresware) Declassify, New Technologies Inc (NTI) Disk Scrub or M-Sweep Pro or Symantec (Norton) WipeInfo to remove all data by overwriting the existing data with random or pre-defined characters. The Linux OS may also be used to write out a value of zero (0) to a device.

The media is then examined using tools to determine that no data exists (MD5, SHA-1 or Diskedit). The partition information is removed and the media is sanitized from the physical address of (cylinder/head/sector) 0/0/1 to the physical (versus logical) end of the media.



This process involves using a program such as I-wipe, Encase, Linux, Drivespy, SPADA or any program capable of writing multiple passes of a single character over the entire drive.

Checksum is a form of redundancy check, a very simple measure for protecting the integrity of data by detecting errors in data. It works by adding up the basic components of a message, typically the bytes, and storing the resulting value. Later, anyone can perform the same operation on the data, compare the result to the authentic checksum and (assuming that the sums match) conclude that the message was probably not corrupted.

Redundancy check is extra data added to a message for the purposes of error detection and error correction.

The value of the checksum of forensically prepared media will be zero (0) provided the write process is done using zeros.

## G

### Graphic Image Files

Computer graphic image files such as photos, drawings, etc. Come in various standard formats. Some of the most common file types include but are not limited to Joint Photographic Experts Group (JPEG, JPG), Bitmap (BMP), Graphics Interchange Format (GIF, JFIF) and AOL image file (ART).

### Golden Dictionary

The Golden Dictionary file, ADPasswords.dat, contains all recovered passwords for all PRTK sessions on the current computer. It is stored in the AccessData program directory (C:\Program Files\AccessData\Recovery\). Recovered passwords are used as the first level of attack in all password recovery sessions. Most people use the same password for different files, so recovering the password for a simple file often opens the door to more difficult files.

### Graphic Interchange Format (GIF)

A common graphics format that can be displayed on almost all Web browsers. GIFs typically display in 256 colors and have built-in compression. Static or animated GIF images are the most common form of banner creation.

## H

### Hard Disk (Drive)

A magnetic disk on which you can store computer data. The term hard is used to distinguish it from a soft or floppy disk. Hard disks hold more data and are faster than floppy disks. A hard disk, for example, can store anywhere from 10 gigabytes to several terabytes, whereas most floppies have a maximum storage capacity of 1.4 megabytes.

### 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.

### Head

The mechanism that reads data from or writes data to a magnetic disk or tape. Hard disk drives have many heads, usually two for each platter.

### Hexadecimal

The base-16 number system, which consists of 16 unique symbols: the numbers zero through nine and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (eight bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

## K

### Known File Filter (KFF)

The KFF is a database utility that compares the hash values of case files to a database of hash values from known files. The KFF can significantly reduce the amount of time you spend analyzing files by eliminating unimportant files such as system and application files, or identifying alert files such as known child pornography images. After you compare case files to the KFF database, FTK and Enterprise place unimportant files (known system and application files) in the KFF Ignorable container and alert files (known criminal files) in the KFF Alert Files container within the Overview tab.

## M

### Markov Permutation

The Markov permutation records the times certain words, letters, punctuation, and spaces occur together in a given amount of text, then generates random output that has the same distribution of groups.

For example: if you were to scan through the text and create a huge frequency table of what words come after the words “up the,” you might find “tree,” “ladder,” and “creek” most often. You would then generate output from the words “up the,” and get the results “up the tree,” “up the creek,” and “up the ladder” randomly.

If the words “up the” were followed most frequently by the word “creek” in your sample text, the phrase “up the creek” would occur most frequently in your random output.

Andrey Andreyevich Markov (June 14, 1856–July 20, 1922) was a Russian mathematician.

### Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips; the word storage is used for memory that exists on tapes or disks. Moreover, the term memory is usually used as shorthand for physical memory, which refers to the actual chips capable of holding data.

### Message Digest 5

A 128-bit digital fingerprint based on a file's content. An algorithm created in 1991 by Professor Ronald Rivest of RSA that is used to create digital signatures, or a 128-bit

digital fingerprint based on a file's content. Message Digest 5 (MD5) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a hash or digest. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest. When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been changed. This comparison is called a hash check. 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.

## Metadata

Literally data about data. Metadata describes how, when, and by whom a particular set of data was collected and how the data is formatted. Metadata is essential for understanding information stored in data warehouses and has become increasingly important in XML-based Web applications.

## Mount

To make a mass storage device available to the OS, or to a user or user group. It may also mean to make a device physically accessible. In a Unix environment, the mount command attaches discs or directories logically rather than physically. The Unix mount command makes a directory accessible by attaching a root directory of one file system to another directory, which makes all the file systems usable as if they were subdirectories of the file system they are attached to. Unix recognizes devices by their location, while Windows recognizes them by their names (C: drive, for example). Unix organizes directories in a tree-like structure in which directories are attached by mounting them on the branches of the tree. The file system location where the device is attached is called a mount point. Mounts may be local or remote. A local mount connects disk drives on one machine so that they behave as one logical system. A remote mount uses Network File System (NFS) to connect to directories on other machines so that they can be used as if they were all part of the user's file system.

# N

## NT File System (**NTFS**)

One of the file systems for the Windows NT operating system (Windows NT also supports the FAT file system). NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories or individual files. NTFS files are not accessible from other operating systems, such as DOS. For large applications, NTFS supports spanning volumes, which means files and directories can be spread out across several physical disks.

## P

### Pagefile (.sys)

The paging file is the area on the hard disk that Windows uses as if it were random access memory (RAM). This is sometimes known as virtual memory. By default, Windows stores this file on the same partition as the Windows system files.

### Parallel Framework Extensions (**PFX**)

PFX is a managed concurrency library being developed by a collaboration between Microsoft Research and the CLR team at Microsoft. It is composed of two parts: **Parallel LINQ (PLINQ)** and **Task Parallel Library (TPL)**.

### Pretty Good Privacy

A common symmetric encryption system used for exchanging files and email. It provides both privacy and authentication.

## R

### RC4

RC4, or ARC4, is a variable key-length stream cipher designed by RSA. Stream ciphers are key-dependent, pseudo-random number generators whose output is XORed with the data  $\langle \text{plaintext} \rangle \text{ XOR } \langle \text{random-looking stream} \rangle = \langle \text{random-looking ciphertext} \rangle$ . Because XOR is symmetric (in other words,  $[A \text{ XOR } B] \text{ XOR } B = A$ ),

XORing the ciphertext with the stream again returns the plaintext. Microsoft Word and Excel use RC4 and a 40-bit key to encrypt their files. An exhaustive key space attack has a much better chance at succeeding with a 40-bit key space.

## S

### Sector

A sector is a group of bytes within a track and is the smallest group of bytes that can be addressed on a drive. There are normally tens or hundreds of sectors within each track. The number of bytes in a sector can vary, but is almost always 512. The maximum number of sectors in a cluster is 64. CDROMS normally have 2048 bytes per sector. Sectors are numbered sequentially within a track, starting at 1. The numbering restarts on every track, so that “track 0, sector 1” and “track 5, sector 1” refer to different sectors. Modern drives use a system known as Logical Block Addressing (LBA) instead of CHS to track sectors.

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 ten sectors.

Physical sectors are relative to the entire drive. Logical sectors are relative to the partition.

### Secure Hash Algorithm

A 160-bit digital fingerprint based on a file’s content. 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 impossible to derive any information about the input from the hash. It is also computationally impossible to find another file that will produce the same output. SHA-1 hashes are used by the KFF to identify known files.

FTK uses SHA-1 and SHA-256. The KFF library contains some A hashes.

### SHA

The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard.

The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512—sometimes collectively referred to as SHA-2.

Attacks have been found for both SHA-0 and SHA-1. No attacks have yet been reported on the SHA-2 variants, but since they are similar to SHA-1, researchers are worried, and are developing candidates for a new, better hashing standard.

## **Spool (spooling, print spool)**

Acronym for Simultaneous Peripheral Operations On-Line, spooling refers to putting jobs in a buffer, a special area in memory or on a disk where a device can access them when it is ready. Spooling is useful because devices access data at different rates. The buffer provides a waiting station where data can rest while the slower device catches up.

The most common spooling application is print spooling. In print spooling, documents are loaded into a buffer (usually an area on a disk), and then the printer pulls them off the buffer at its own rate. Because the documents are in a buffer where they can be accessed by the printer, you can perform other operations on the computer while printing takes place in the background. Spooling also lets you place a number of print jobs on a queue instead of waiting for each one to finish before specifying the next one.

## **Slack (File and RAM)**

Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called file slack. Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. Larger cluster sizes mean more file slack and also the waste of storage space when Windows 95 systems are involved.

File slack potentially contains randomly selected bytes of data from computer memory. This happens because DOS/Windows normally writes in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector in a file, DOS/Windows makes up the difference by padding the remaining space with data from the memory buffers of the operating system. This randomly selected data from memory is called RAM Slack because it comes from the memory of the computer.

RAM Slack can contain any information that may have been created, viewed, modified, downloaded or copied during work sessions that have occurred since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past.

RAM slack pertains only to the last sector of a file. If additional sectors are needed to round out the block size for the last cluster assigned to the file, then a different type of slack is created. It is called drive slack and it is stored in the remaining sectors which might be needed by the operating system to derive the size needed to create the last cluster assigned to the file. Unlike RAM slack, which comes from memory, drive slack is padded with what was stored on the storage device before. Such data could contain remnants of previously deleted files or data from the format pattern associated with disk storage space that has yet to be used by the computer.

For example, take a file that is created by writing the word "Hello." Assuming that this is the only data written in the file and assuming a two sector cluster size for the file, the data stored to disk and written in file slack could be represented as follows:

---

Hello+++++++|—————(EOC)

RAM Slack is indicated by "+"

Drive Slack is indicated by "-"

---

File Slack is created at the time a file is saved to disk. When a file is deleted under DOS, Windows, Windows 95, Windows 98 and Windows NT/2000/XP, the data associated with RAM slack and drive slack remains in the cluster that was previously assigned to the end of the deleted file. The clusters which made up the deleted file are released by the operating system and they remain on the disk in the form of unallocated storage space until the space is overwritten with data from a new file.

File slack potentially contains data dumped randomly from the computer's memory. It is possible to identify network login names, passwords, and other sensitive information



associated with computer usage. File slack can also be analyzed to identify prior uses of the subject computer and such legacy data can help the computer forensics investigator. File slack is not a trivial item. On large hard disk drives, file slack can involve several hundred megabytes of data. Fragments of prior email messages and word processing documents can be found in file slack. From a computer forensic standpoint, file slack is very important as both a source of digital evidence and security risks

## **String Searches**

A string search is a data string containing standard text or non-text data. The term may be a word, phrase or an expression. Keyword searches are designed to aid in the identification of potentially relevant data on the examined media.

## **Superuser Administrator**

A person with unlimited access privileges who can perform any and all operations on the computer and within the operating system and file system. These privileges do not necessarily transfer to the applications installed on the computer.

## **Symmetric Encryption**

A type of encryption in which the encryption and decryption keys are the same. Some common symmetric encryption systems are Data Encryption Standard, Triple-DES, Pretty Good Privacy, BestCrypt, and Advanced Encryption Standard.

# **T**

## **Thumbnail**

A smaller-sized version of a graphics image.

# **U**

## **Unallocated Space**

Also called free space, it consists of all the clusters on a drive that are not currently assigned to a file. Some of these clusters may still contain data from files that have been deleted but not yet overwritten by other files.

Until the first file is written to the data storage area of a computer storage device, the clusters are unallocated by the operating system in the File Allocation Table (FAT). These unallocated clusters are padded with format pattern characters and the unallocated clusters are not of interest to the computer forensics specialist until data is written to the clusters. As the computer user creates files, clusters are allocated in the File Allocation Table (FAT) to store the data. When the file is deleted by the computer user, the clusters allocated to the file are released by the operating system so new files and data can be stored in the clusters when needed. However, the data associated with the deleted file remains behind. This data storage area is referred to as unallocated storage space and it is fragile from an evidence preservation standpoint. However, until the unallocated storage space is reassigned by the operating system, the data remains behind for easy discovery and extraction by the computer forensics specialist. Unallocated file space potentially contains intact files, remnants of files and subdirectories and temporary files, which were transparently created and deleted by computer applications and also the operating system. All of such files and data fragments can be sources of digital evidence and also security leakage of sensitive data and information.

## URL

Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use and the second part specifies the IP address or the domain name where the resource is located.

## V

## Volume

A volume refers to a mounted partition. There may be only one volume on a disk, such as a floppy disk or a zip disk. There may be several volumes on a disk as on a partitioned hard drive. A volume is a logical structure, not a physical device. There can be up to 24 of these logical volumes on a disk and they show up as drive “c,” “d,” or “e” in DOS.

## Volume Boot Sector

Since every partition may contain a different file system, each partition contains a volume boot sector which is used to describe the type of file system on the partition and usually contains boot code necessary to mount the file system.



