

**ACCESSDATA**

**FTK<sup>®</sup>** **2.0**

**F O R E N S I C   T O O L K I T<sup>®</sup>**



**AccessData<sup>®</sup>**



# *AccessData Forensic Toolkit*

## **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 is a registered trademark of AccessData Corp.
- AccessData Certified Examiner is a registered trademark of AccessData Corp.
- ACE is a registered trademark of AccessData Corp.
- Distributed Network Attack is a registered trademark of AccessData Corp.
- DNA is a registered trademark of AccessData Corp.
- AccessData eDiscovery is a registered trademark of AccessData Corp.
- AccessData Enterprise is a registered trademark of AccessData Corp.
- Forensic Toolkit is a registered trademark of AccessData Corp.
- FTK is a registered trademark of AccessData Corp.
- FTK Imager is a trademark of AccessData Corp.
- Known File Filter is a trademark of AccessData Corp.
- KFF is a trademark of AccessData Corp.
- LicenseManager is a trademark of AccessData Corp.
- Password Recovery Toolkit is a registered trademark of AccessData Corp.
- PRTK is a registered trademark of AccessData Corp.
- Registry Viewer is a registered trademark of AccessData Corp.
- Ultimate Toolkit is a registered trademark of AccessData Corp.
- UTK is a registered trademark of AccessData Corp.

## DOCUMENTATION CONVENTIONS

In AccessData documentation, a greater-than symbol (>) is used to separate actions within a step.

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

We value all feedback from our customers. For technical and customer support issues, please email us at **[support@accessdata.com](mailto:support@accessdata.com)**. For documentation issues, please email us at **[documentation@accessdata.com](mailto:documentation@accessdata.com)**.

# Contents

|   |            |
|---|------------|
| <i>AccessData Forensic Toolkit</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>Contents</i> .....                       | <i>iii</i> |
| <i>Chapter 1 Welcome and Overview</i> ..... | <i>1</i>   |
| <i>Audience</i> .....                       | <i>1</i>   |
| <i>Handling Evidence</i> .....              | <i>1</i>   |
| <i>What is a Case?</i> .....                | <i>2</i>   |
| <i>Role of Forensic Toolkit</i> .....       | <i>3</i>   |
| <i>Other AccessData Products</i> .....      | <i>3</i>   |
| <i>Password Recovery Software</i> .....     | <i>3</i>   |
| <i>AccessData Enterprise</i> .....          | <i>4</i>   |
| <i>AccessData eDiscovery</i> .....          | <i>4</i>   |
| <i>Product Overview</i> .....               | <i>4</i>   |
| <i>Managing a Case</i> .....                | <i>5</i>   |
| <i>Defining the Evidence</i> .....          | <i>5</i>   |
| <i>Hashing</i> .....                        | <i>5</i>   |
| <i>Searching</i> .....                      | <i>6</i>   |

|  |    |
|--|----|
| <i>Known File Filter</i> .....                         | 6  |
| <i>Presenting Evidence</i> .....                       | 7  |
| <i>Chapter 2 Installation and Upgrade</i> .....        | 9  |
| <i>Installation Options</i> .....                      | 9  |
| <i>System Overview</i> .....                           | 10 |
| <i>Estimating hard disk space requirements</i> .....   | 11 |
| <i>Installation</i> .....                              | 11 |
| <i>CodeMeter Stick Installation</i> .....              | 13 |
| <i>Oracle Installation</i> .....                       | 13 |
| <i>Single Computer Installation</i> .....              | 18 |
| <i>Installing the FTK PROGRAM</i> .....                | 18 |
| <i>Choosing an Evidence Server</i> .....               | 20 |
| <i>Installing the KFF</i> .....                        | 23 |
| <i>Installing on Separate Computers</i> .....          | 26 |
| <i>Additional Programs</i> .....                       | 26 |
| <i>Upgrading to FTK 2.1</i> .....                      | 27 |
| <i>Upgrading a Two-Computer Configuration</i> .....    | 32 |
| <i>Chapter 3 Concepts</i> .....                        | 33 |
| <i>Starting FTK</i> .....                              | 33 |
| <i>Setting Up the Application Administrator</i> .....  | 33 |
| <i>Using the CodeMeter Stick</i> .....                 | 34 |
| <i>Using the Case Manager Window</i> .....             | 34 |
| <i>The FTK Window</i> .....                            | 37 |
| <i>Toolbar Components</i> .....                        | 42 |
| <i>File List Pane</i> .....                            | 43 |
| <i>Properties Pane</i> .....                           | 45 |
| <i>Hex Interpreter Pane</i> .....                      | 47 |
| <i>File Content</i> .....                              | 49 |
| <i>Using Tabs to Explore and Refine Evidence</i> ..... | 52 |
| <i>Explore Tab</i> .....                               | 52 |
| <i>Overview Tab</i> .....                              | 57 |

|   |     |
|---|-----|
| <i>Email Tab</i> .....  | 61  |
| <i>Graphics Tab</i> .....                                       | 62  |
| <i>Bookmarks Tab</i> .....                                      | 64  |
| <i>Search Tabs</i> .....  | 66  |
| <i>Creating Tabs</i> .....                                      | 67  |
| <i>Chapter 4 Starting a New FTK2.1 Case</i> .....               | 69  |
| <i>Launch FTK2.1</i> .....                                      | 69  |
| <i>Acquiring and Preserving the Evidence</i> .....              | 73  |
| <i>Creating a Case</i> .....                                    | 73  |
| <i>Selecting Evidence Processing Options</i> .....              | 74  |
| <i>Selecting Evidence Discovery Options</i> .....               | 77  |
| <i>Selecting Evidence Refinement (Advanced) Options</i> .....   | 79  |
| <i>Selecting Index Refinement (Advanced) Options</i> .....      | 83  |
| <i>Creating the Case</i> .....                                  | 87  |
| <i>Adding Evidence</i> .....                                    | 87  |
| <i>Processing Evidence</i> .....                                | 88  |
| <i>Viewing Processed Items</i> .....                            | 88  |
| <i>Backing Up the Case</i> .....                                | 89  |
| <i>Restoring a Case</i> .....                                   | 89  |
| <i>Deleting a Case</i> .....                                    | 90  |
| <i>Storing Case Files</i> .....                                 | 90  |
| <i>Chapter 5 Working with Cases</i> .....                       | 91  |
| <i>Opening an Existing Case</i> .....                           | 91  |
| <i>Adding Evidence</i> .....                                    | 91  |
| <i>Selecting a Language</i> .....                               | 94  |
| <i>Additional Analysis</i> .....                                | 95  |
| <i>File Content, Properties, and Hex Interpreter Tabs</i> ..... | 97  |
| <i>Properties Tab</i> .....                                     | 98  |
| <i>The Hex Interpreter Tab</i> .....                            | 101 |
| <i>Using the Bookmark Information Pane</i> .....                | 103 |
| <i>Creating a Bookmark</i> .....                                | 104 |

|   |     |
|---|-----|
| <i>Viewing Bookmark Information</i> .....                           | 106 |
| <i>Adding Evidence to an Existing Bookmark</i> .....                | 108 |
| <i>Creating Email or Email Attachment Bookmarks</i> .....           | 109 |
| <i>Moving a Bookmark</i> .....                                      | 113 |
| <i>Removing a Bookmark</i> .....                                    | 113 |
| <i>Deleting Files from a Bookmark</i> .....                         | 114 |
| <i>Verifying Drive Image Integrity</i> .....                        | 114 |
| <i>Copying Information from FTK</i> .....                           | 115 |
| <i>Export File List Info</i> .....                                  | 117 |
| <i>Exporting Files</i> .....  | 118 |
| <i>Exporting File List Info</i> .....                               | 120 |
| <i>Exporting the Word List</i> .....                                | 120 |
| <i>Fuzzy Hashing</i> .....  | 120 |
| <i>Creating a Fuzzy Hash Library</i> .....                          | 121 |
| <i>Selecting Fuzzy Hash Options During Initial Processing</i> ..... | 121 |
| <i>Additional Analysis Fuzzy Hashing</i> .....                      | 123 |
| <i>Comparing Files Using Fuzzy Hashing</i> .....                    | 124 |
| <i>Viewing Fuzzy Hash Results</i> .....                             | 124 |
| <i>Chapter 6 Searching a Case</i> .....                             | 127 |
| <i>Conducting a Live Search</i> .....                               | 127 |
| <i>Customizing the Live Search Tab</i> .....                        | 129 |
| <i>Conducting a Pattern Search</i> .....                            | 130 |
| <i>Simple Pattern Searches</i> .....                                | 130 |
| <i>Complex Pattern Searches</i> .....                               | 131 |
| <i>Predefined Regular Expressions</i> .....                         | 133 |
| <i>Conducting Hex Searches</i> .....                                | 139 |
| <i>Conducting Text Searches</i> .....                               | 139 |
| <i>Conducting an Index Search</i> .....                             | 140 |
| <i>Search Terms</i> .....   | 141 |
| <i>Search Criteria</i> .....  | 142 |
| <i>Documenting Search Results</i> .....                             | 145 |
| <i>Using Copy Special to Document Search Results</i> .....          | 145 |



|  |     |
|--|-----|
| <i>Bookmarking Search Results</i> .....                              | 146 |
| <i>Chapter 7 Data Carving</i> .....                                  | 149 |
| <i>Searching for Embedded and Deleted Files (Data Carving)</i> ..... | 149 |
| <i>Data Carving Files When Processing a New Case</i> .....           | 150 |
| <i>Data Carving Files in an Existing Case</i> .....                  | 150 |
| <i>Chapter 8 Using Filters</i> .....                                 | 151 |
| <i>The Filter Toolbar</i> .....                                      | 151 |
| <i>Applying an Existing Filter</i> .....                             | 152 |
| <i>Creating a Filter</i> .....                                       | 154 |
| <i>Refining a Filter</i> .....                                       | 155 |
| <i>Deleting a Filter</i> .....                                       | 155 |
| <i>Using the Known File Filter</i> .....                             | 156 |
| <i>Understanding KFF Hashes</i> .....                                | 156 |
| <i>Importing KFF Hashes</i> .....                                    | 156 |
| <i>Exporting KFF Hashes</i> .....                                    | 159 |
| <i>Understanding the KFF Database</i> .....                          | 159 |
| <i>Storing Hashes in the KFF Database</i> .....                      | 159 |
| <i>Creating Sets and Groups</i> .....                                | 161 |
| <i>Chapter 9 Decrypting Encrypted Files</i> .....                    | 163 |
| <i>Decrypting Files and Folders</i> .....                            | 163 |
| <i>Decrypting Windows EFS FILES</i> .....                            | 165 |
| <i>Viewing Decrypted Files</i> .....                                 | 165 |
| <i>Decrypting Domain Account EFS Files</i> .....                     | 167 |
| <i>Decrypting Credant Files</i> .....                                | 169 |
| <i>Using an Offline Key Bundle</i> .....                             | 169 |
| <i>Using an Online Key Bundle</i> .....                              | 170 |
| <i>Decrypting Safeguard Utimaco Files</i> .....                      | 172 |
| <i>Decrypting SafeBoot Files</i> .....                               | 173 |

|   |         |
|---|---------|
| <i>Chapter 10 Working with Reports</i> .....                    | 175     |
| <i>Creating a Report</i> .....                                  | 175     |
| <i>Saving Settings</i> .....                                    | 176     |
| <i>Entering Basic Case Information</i> .....                    | 177     |
| <i>Including Bookmarks</i> .....                                | 179     |
| <i>Including Graphics</i> .....                                 | 181     |
| <i>Selecting a File Path List</i> .....                         | 182     |
| <i>Selecting a File Properties List</i> .....                   | 183     |
| <i>Registry Selections</i> .....                                | 184     |
| <i>Running the report</i> .....                                 | 185     |
| <i>Selecting the Report Location</i> .....                      | 185     |
| <i>Creating the Report</i> .....                                | 186     |
| <i>Viewing a Report</i> .....                                   | 187     |
| <i>International Date and Time Stamp Issue</i> .....            | 188     |
| <i>Modifying a Report</i> .....                                 | 189     |
| <i>Printing a Report</i> .....                                  | 189     |
| <br><i>Chapter 11 Customizing the Interface</i> .....           | <br>191 |
| <i>Customizing Overview</i> .....                               | 191     |
| <i>Using the View Menu to Customize the FTK Interface</i> ..... | 191     |
| <i>Customizing the Tab Views</i> .....                          | 193     |
| <i>Using the Tab Layout Menu</i> .....                          | 194     |
| <i>Moving View Panes</i> .....                                  | 195     |
| <i>Creating Custom Tabs</i> .....                               | 197     |
| <i>Customizing File List Columns</i> .....                      | 197     |
| <i>Creating and Modifying Column Settings</i> .....             | 198     |
| <i>Available Columns</i> .....                                  | 199     |
| <br><i>Chapter 12 Other AccessData Applications</i> .....       | <br>213 |
| <i>Accessing Additional Products</i> .....                      | 213     |
| <i>Capturing Evidence with Imager</i> .....                     | 213     |
| <i>Recovering Passwords with PRTK</i> .....                     | 214     |

|   |     |
|---|-----|
| <i>How PRTK Works</i> .....                                       | 215 |
| <i>PRTK Features</i> .....  | 215 |
| <i>Obtaining Protected Information with Registry Viewer</i> ..... | 216 |
| <i>Managing Licenses with LicenseManager</i> .....                | 216 |
| <i>Starting LicenseManager</i> .....                              | 217 |
| <i>LicenseManager Interface</i> .....                             | 218 |
| <i>Opening and Saving Security Device Packet Files</i> .....      | 223 |
| <i>Viewing Product Licenses</i> .....                             | 223 |
| <i>Adding and Removing Product Licenses</i> .....                 | 224 |
| <i>Managing Product Licenses on Isolated Machines</i> .....       | 225 |
| <i>Updating Products</i> .....                                    | 227 |
| <i>Purchasing Product Licenses</i> .....                          | 228 |
| <i>Sending a Security Device Packet File to Support</i> .....     | 228 |
| <i>Selecting the Application Language</i> .....                   | 229 |
| <i>Appendix A Recognized File Types</i> .....                     | 231 |
| <i>Document File Types</i> .....                                  | 231 |
| <i>Spreadsheet File Types</i> .....                               | 235 |
| <i>Database File Types</i> .....                                  | 236 |
| <i>Graphic File Types</i> .....                                   | 237 |
| <i>Email Message Programs</i> .....                               | 238 |
| <i>Instant Messaging Programs</i> .....                           | 239 |
| <i>Executable File Types</i> .....                                | 239 |
| <i>Archive File Types</i> .....                                   | 240 |
| <i>Other Known File Types</i> .....                               | 241 |
| .....   | 243 |
| <i>Appendix B File Systems and Drive Image Formats</i> .....      | 245 |
| <i>File Systems</i> .....   | 245 |
| <i>Hard Disk Image Formats</i> .....                              | 245 |
| <i>CD and DVD Image Formats</i> .....                             | 246 |
| <i>Appendix C Recovering Deleted Material</i> .....               | 247 |

|  |         |
|--|---------|
| <i>FAT 12, 16, and 32</i> .....                                | 247     |
| <i>NTFS</i> .....  | 248     |
| <i>ext2</i> .....  | 248     |
| <i>ext3</i> .....  | 248     |
| <i>HFS</i> .....   | 249     |
| <br><i>Appendix D Program Files</i> .....                      | <br>251 |
| <i>Files and Folders for the Application</i> .....             | 251     |
| <i>Files and Folders for the Database</i> .....                | 252     |
| <i>Changing Registry Options</i> .....                         | 252     |
| <i>Changing the Logging Registry Options</i> .....             | 252     |
| <br><i>Appendix E Securing Windows Registry Evidence</i> ..... | <br>255 |
| <i>Understanding the Windows Registry</i> .....                | 255     |
| <i>Windows 9x Registry Files</i> .....                         | 256     |
| <i>Windows NT and Windows 2000 Registry Files</i> .....        | 257     |
| <i>Windows XP Registry Files</i> .....                         | 258     |
| <i>Possible Data Types</i> .....                               | 260     |
| <i>Additional Considerations</i> .....                         | 261     |
| <i>Registry Quick Find Chart</i> .....                         | 263     |
| <i>System Information</i> .....                                | 264     |
| <i>Networking</i> .....  | 266     |
| <i>User Data</i> .....   | 266     |
| <i>User Application Data</i> .....                             | 268     |
| .....  | 269     |
| <br><i>Appendix F Troubleshooting</i> .....                    | <br>271 |
| <i>Finding Answers</i> .....                                   | 271     |
| <i>Troubleshooting Tables</i> .....                            | 272     |
| <i>Diagnostics Tools</i> .....                                 | 273     |
| <i>Database Diagnostics</i> .....                              | 273     |
| <i>Uninstalling Manually</i> .....                             | 275     |

|  |     |
|--|-----|
| <i>Automated Uninstall</i> .....                       | 275 |
| <i>Manually Uninstalling the Database</i> .....        | 276 |
| <i>Find and Delete FTK Folders and Keys</i> .....      | 277 |
| <i>Handling Oracle Folders and Keys</i> .....          | 278 |
| <i>Other Issues</i> .....                              | 279 |
| <i>dtSearch Noise File List</i> .....                  | 279 |
| <i>Appendix G Corporate Information</i> .....          | 281 |
| <i>Contacting AccessData Corporation by Mail</i> ..... | 281 |
| <i>Registration</i> .....                              | 281 |
| <i>Technical Support</i> .....                         | 282 |
| <i>Documentation</i> .....                             | 282 |
| <i>FTK Glossary</i> .....                              | 283 |



# *Chapter 1 Welcome and Overview*

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

## **AUDIENCE**

The FTK2 User Guide target audience consists of law enforcement and corporate security professionals with the following competencies:

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

## **HANDLING EVIDENCE**

Computer forensics involves the acquisition, preservation, analysis, and presentation of digital evidence. This type of evidence is fragile and can easily be altered, destroyed, or rendered inadmissible if improperly obtained, preserved, and analyzed.

## WHAT IS A CASE?

To build a case involving a computer system, find evidence or supportive evidence of a civil wrong or a criminal act by the systematic inspection of the computer system and its contents. Building such a case has come to be known as Computer Forensics.

Since computer forensics must adhere to the standards of evidence that are admissible in a court of law, it requires specialized expertise and tools that go above and beyond the normal data collection and preservation techniques available to end-users or system support personnel. Often, the forensic examiner must render an opinion, based on the examination of the material that has been recovered, on whether the evidence indicates criminal activity.

Computer forensics experts investigate data storage devices such as hard drives, portable data devices (USB drives), external drives, micro drives and many more).

Computer forensics experts perform the following tasks:

1. Identify sources of documentary or other digital evidence.
2. Preserve the evidence.
3. Analyze the evidence.
4. Present the findings.

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

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

Another important legal element in computer forensics is the “chain of custody.” The chain of custody is the line of people who have controlled the evidence. Forensic investigators must be able to account for all that has happened to the evidence between its point of acquisition and its eventual appearance in court.

Only properly trained computer forensics specialists should obtain and examine digital evidence. Even the most incriminating digital evidence can be made legally inadmissible because of reckless or ill-conceived examinations.



## ROLE OF FORENSIC TOOLKIT

To acquire digital evidence, FTK Imager and other imaging software tools can be used to create a disk image of the source drives or files. A hash of the original disk image can be created to later use as a benchmark to prove the validity of the gathered case evidence. FTK Imager verifies that the disk image hash and the drive hash match when the disk image is created.

After creating the disk image and hash of the data, FTK can then perform a complete and thorough computer forensic examination, and create a report of the investigatory findings.

## OTHER ACCESSDATA PRODUCTS

In addition to FTK and FTK Imager, AccessData offers other industry-leading products. These two products are included as part of the FTK package, but are also available for separate purchase. For other products and services, please refer to our Web site, [www.accessdata.com](http://www.accessdata.com).

## PASSWORD RECOVERY SOFTWARE

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

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

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

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

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

## ACCESSDATA ENTERPRISE

AccessData Enterprise is a powerful, enterprise-scale investigative solution built on the forensic technology of FTK. With an integrated Oracle<sup>\*</sup> 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.

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 addresses 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/Enterprise.html>.

## ACCESSDATA EDISCOVERY

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 enterprise network of a company.

For more information about eDiscovery, see the AccessData Web site at <http://www.accessdata.com/ediscovery.html>.

## PRODUCT OVERVIEW

This section provides a synopsis of how FTK 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 4 Starting a New FTK2.1 Case” on page 69.

# MANAGING A CASE

Any forensic digital examination requires these basic steps:

- 1. Acquire the evidence.
- 2. Preserve the evidence.
- 3. Analyze the evidence.
- 4. Present digital evidence by creating a case report to document the evidence and investigation results.

# DEFINING THE EVIDENCE

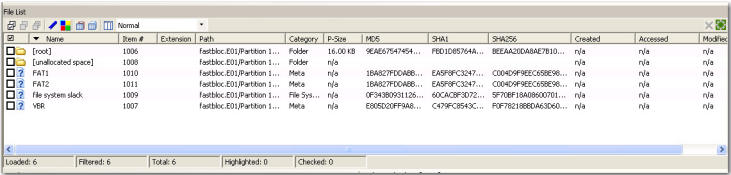
To define the evidence, FTK uses hashing, searching, and the Known File Filter (KFF®) database.

# HASHING

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

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.



| Name                | Item # | Extension | Path                       | Category    | P-Size   | MD5             | SHA1           | SHA256              | Created | Accessed | Modified |
|---------------------|--------|-----------|----------------------------|-------------|----------|-----------------|----------------|---------------------|---------|----------|----------|
| [root]              | 1006   |           | fatbloc:E01:Partition 1... | Folder      | 16.00 KB | 9EA607547454... | FED1D85764A... | BEEAA2DABA87B10...  | n/a     | n/a      | n/a      |
| [unallocated space] | 1008   |           | fatbloc:E01:Partition 1... | Folder      | n/a      |                 |                |                     | n/a     | n/a      | n/a      |
| FAT1                | 1010   |           | fatbloc:E01:Partition 1... | Meta        | n/a      | 16A827F0CA0B... | E45F9FC3247... | C04049FEECC59E36... | n/a     | n/a      | n/a      |
| FAT2                | 1011   |           | fatbloc:E01:Partition 1... | Meta        | n/a      | 16A827F0CA0B... | E45F9FC3247... | C04049FEECC59E36... | n/a     | n/a      | n/a      |
| File system slack   | 1009   |           | fatbloc:E01:Partition 1... | File Sys... | n/a      | 0F9480991126... | 0C4A29F3072... | 5F708F1DA0600701... | n/a     | n/a      | n/a      |
| VR                  | 1007   |           | fatbloc:E01:Partition 1... | Meta        | n/a      | E85D00FFA6...   | C7F9C394C...   | F4F7621980A63D65... | 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 both FTK Imager and FTK. For information on creating hashes with FTK, see “Creating a Case” on page 73.

## SEARCHING

FTK can conduct live or indexed searches of the acquired images.

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

An index 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, or later, using the tools in the program.

FTK uses dtSearch<sup>\*</sup>, one of the leading search tools available, in its index search engine. dtSearch can quickly search gigabytes of text.

For more information on searching, see “Chapter 6 Searching a Case” on page 127.

## KNOWN FILE FILTER

The Known File Filter (KFF) is an FTK 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 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; FTK does not extract its component files.

AccessData’s KFF includes hashes from the National Institute of Standards and Technology (NIST) National Software Reference Library (NSRL) hash database, and from the National Drug Intelligence Center (NDIC) HashKeeper hash database. The AD KFF is updated periodically and is available for download from [www.accessdata.com](http://www.accessdata.com) webpage. Click the Downloads link, then find and select the link for downloading the KFF library.

For more information on the KFF, see “Using the Known File Filter” on page 156.

## **PRESENTING EVIDENCE**

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

Use the FTK 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 is generated in HTML or PDF or can be generated in both formats simultaneously.

For information about creating a report, see “Creating a Report” on page 175.



## *Chapter 2 Installation and Upgrade*

This chapter details the steps for the installation of the required components for the operation of AccessData Forensic Toolkit (FTK) 2.1. The following components are required to run FTK:

- CodeMeter 3.30a Runtime software for the CodeMeter Stick:
- Oracle 10g Database
- FTK Program

These additional programs are available to aid in processing cases:

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

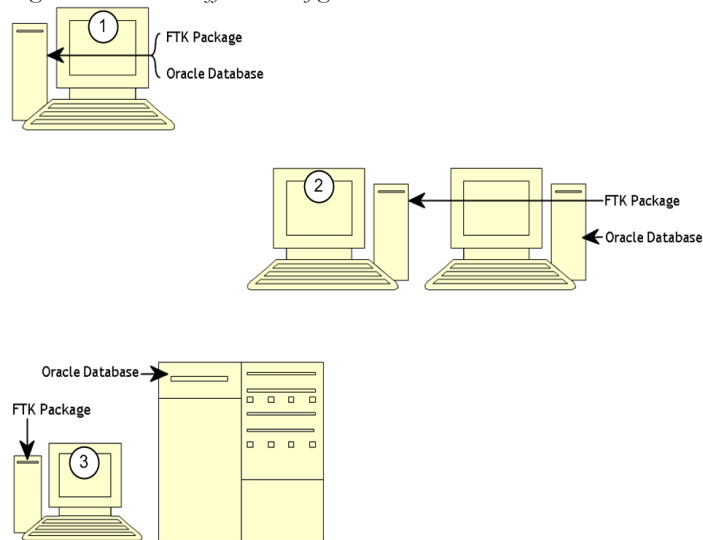
### **INSTALLATION OPTIONS**

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:

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

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

*Figure 2-1. Three Different Configurations*



## SYSTEM OVERVIEW

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 of which Oracle can make exclusive use.
- Do not run other applications that will compete with FTK or the Oracle database for hardware resources.

The FTK Program can also be installed on one workstation, and connected to an existing instance of Oracle 10g already running on a separate workstation. This is displayed in the above figure.

## 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.

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

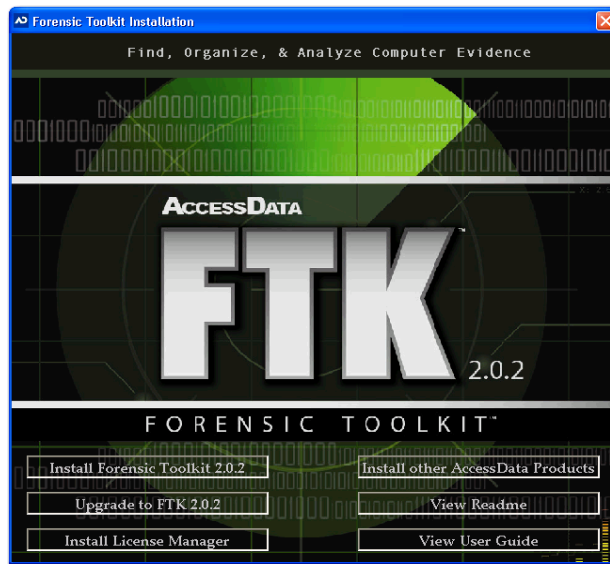
To estimate the amount of hard drive space needed, apply these suggested factors:

- 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.

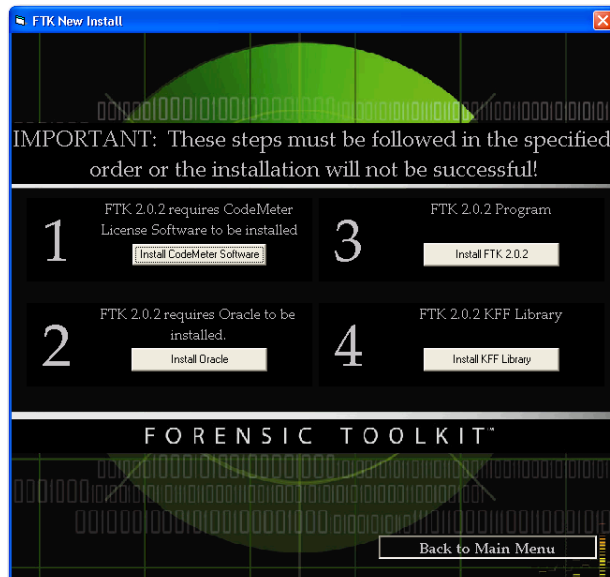
## INSTALLATION

To install FTK 2.1, follow these steps:

1. Insert the FTK 2.1 DVD into the drive.



2. Click *Install Forensic Toolkit 2.1*.



## CODEMETER STICK INSTALLATION

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

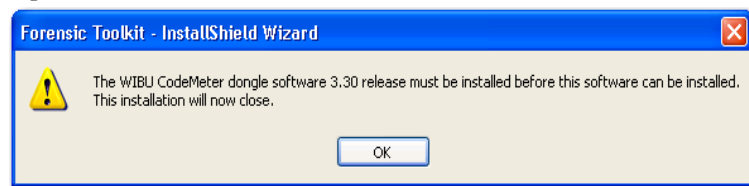
Figure 2-2. CodeMeter Installation Wizard



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

If the user attempts to install FTK 2 before installing the CodeMeter 3.0a software and the Wibu\* CmStick\*, the following error message will be displayed.

Figure 2-3. CodeMeter Error



## ORACLE INSTALLATION

FTK must link to an Oracle database. If 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.

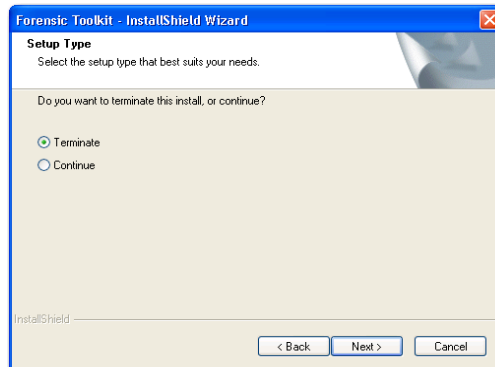
If the FTK installation is attempted before installation of Oracle, or if an install of Oracle 10g patched to version 10.2.0.3 resides elsewhere on the network or in the domain, the FTK installer warns of its dependency on Oracle and prompts the user to continue with or terminate the install, as displayed in the following figure.

*Figure 2-4. Oracle Dependency Warning*



At this point the user is prompted to continue or terminate as in the following figure.

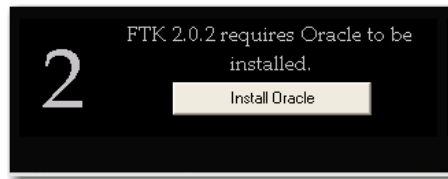
*Figure 2-5. Continue or Terminate*



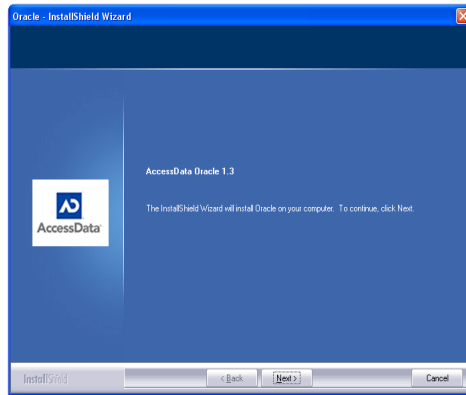
If the user continues, they will install the FTK Program, as detailed in “Installing the FTK Program” on page 14 of the User Guide.

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

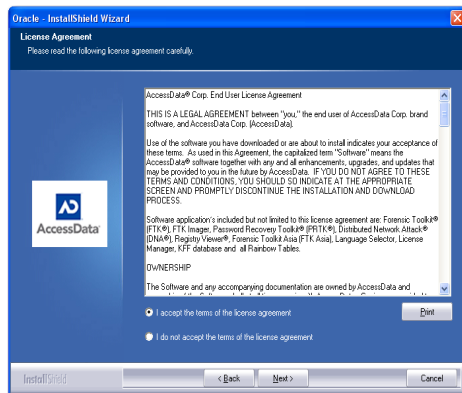
Figure 2-6. Install Oracle Button



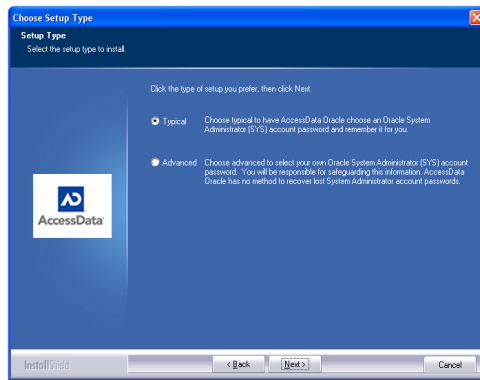
1. Launch the installer.



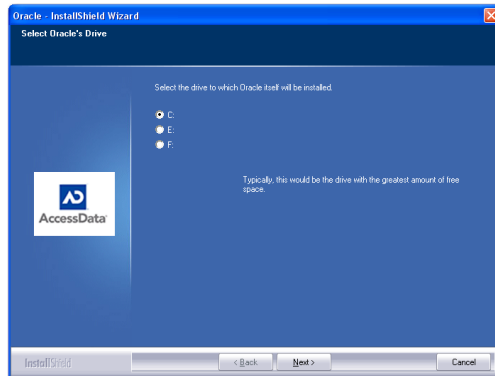
2. Click Next.



3. Read the license agreement, agree to it, and click *Next*.

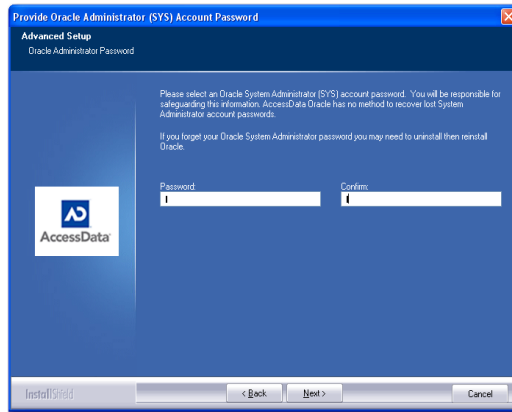


4. Wait for the installer to configure the installation.

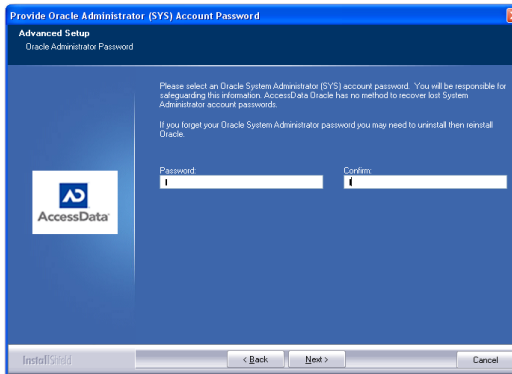


5. Select the installation drive letter.

6. Click *Next*.

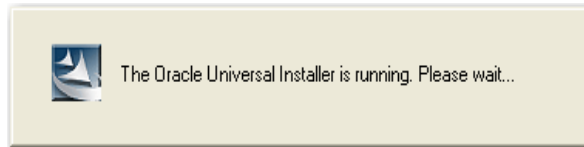


7. Agree to the Oracle Admin Password Agreement and click *Next*.



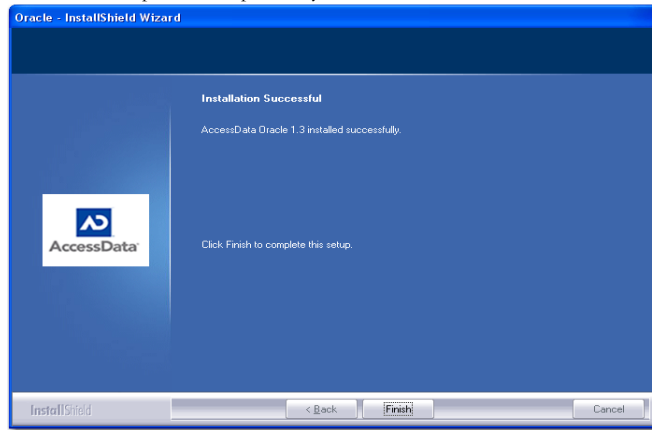
8. Provide an Oracle System Administrator password.

9. Click *Submit*.



10. Wait for the installation and configuration to finish.

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

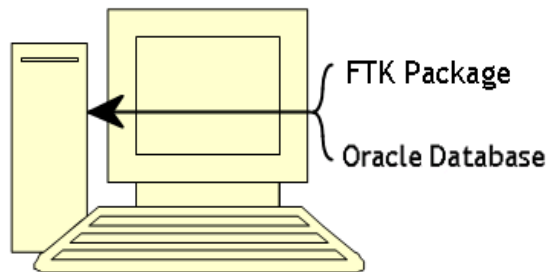


11. Click *Finish* to end the installation process.

## SINGLE COMPUTER INSTALLATION

The FTK Program can be installed on the same computer as the installed Oracle database, as displayed in the following figure.

*Figure 2-7. Single Computer Installation*



## INSTALLING THE FTK PROGRAM

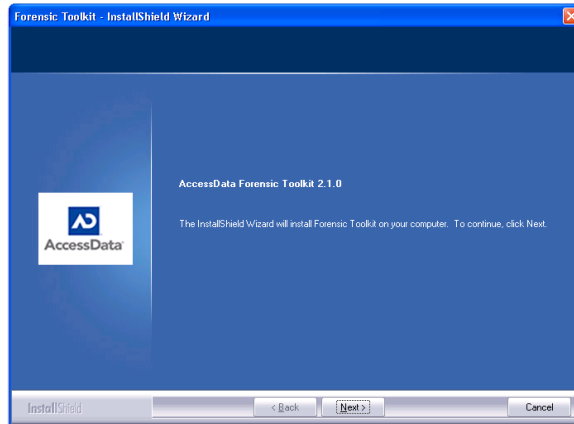
From the FTK New Install screen, perform the steps displayed in the following figure.



Figure 2-8. Install FTK 2.1 Button

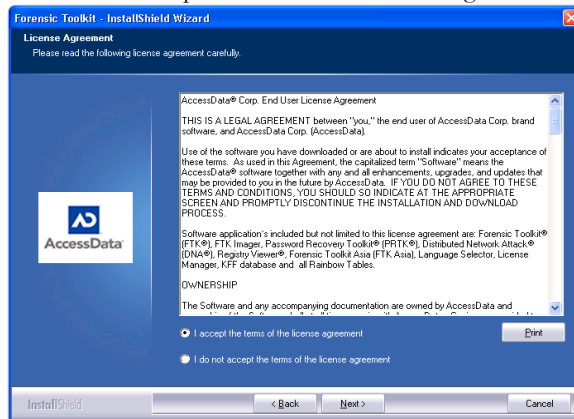


1. Click *Install FTK 2.1*.



2. Click *Next*.

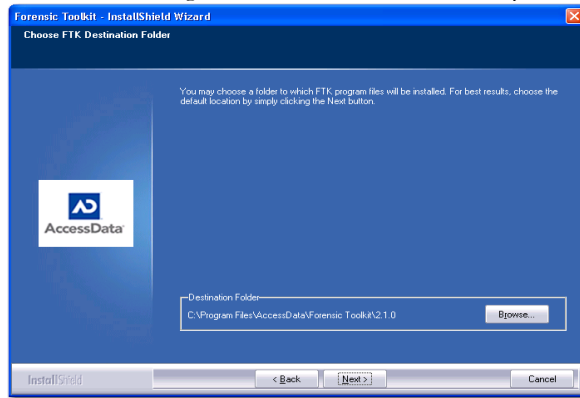
3. Read and accept the AccessData license agreement.



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 file using the Windows Browse functionality.



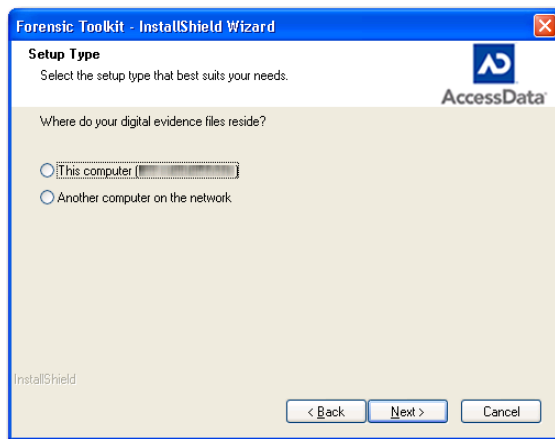
6. Click *Next*.

## CHOOSING AN EVIDENCE SERVER

After installing the FTK Program, choose the server on which contains the evidence data. These files can be stored locally or remotely in the same domain as the computer running FTK or external to the domain. To select an evidence source location, perform the following steps:

1. Select *This computer* if evidence files are stored on a volume on the computer running FTK, or on another computer that is not part of a domain. Some of these extra-

domain examples include machines in a Workgroup or a mixed-platform environment.

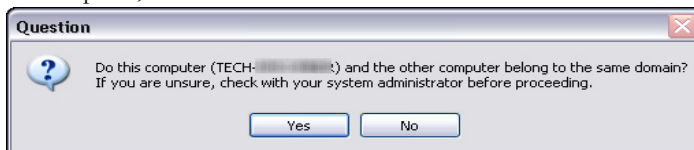


2. If the evidence is stored elsewhere on a domain network, set up access to the evidence storage computer by choosing *Another computer on the network*.
3. Click *Next*.

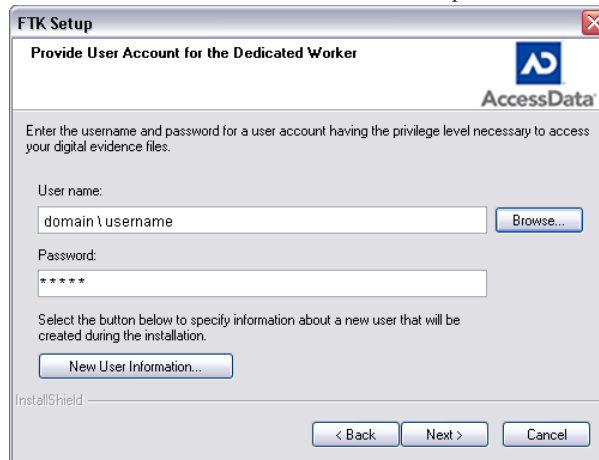
## EVIDENCE ON THE SAME DOMAIN

If the computer with the FTK Program resides in the same domain as the computer with the evidence, perform the following steps to connect the FTK computer to the evidence storage location.

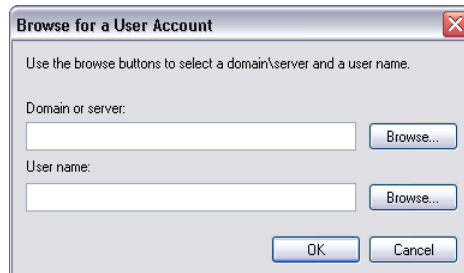
1. When asked if the evidence computer belongs to the same domain as the FTK computer, click *Yes*.



2. Enter the domain name, username, and password into the Worker Account dialog.



If the domain and username is unknown, click *Browse* to find them. The account must have administrative access to the computer and evidence repository computer. The password must be the password of the account selected.



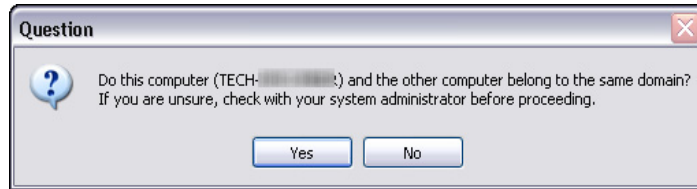
3. Click *OK*.
4. Enter the correct password.
5. Click *Next*.
6. Finish the installation and restart the machine.

## EVIDENCE EXTERIOR TO A DOMAIN

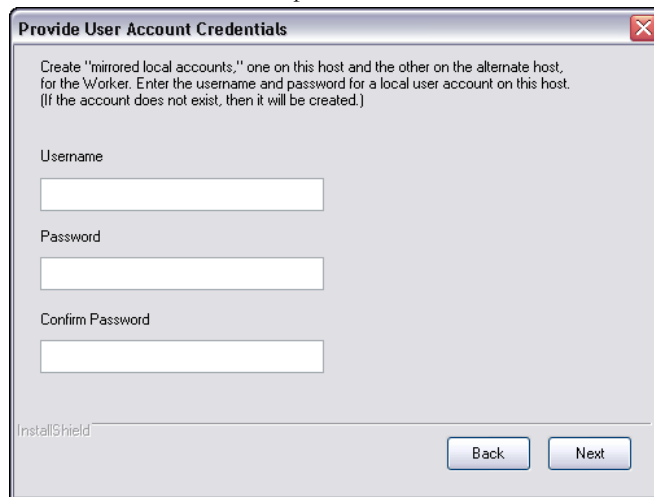
If the evidence is stored on a computer exterior to a domain or in a mixed-platform environment, follow these steps to connect FTK to that server.

**Note:** An identical user with identical privileges must be set up on the evidence server as well as the FTK Program server. This is called Mirrored Local Accounts.

1. When asked whether the machines belong to the same domain, click *No*.



2. Set up identical mirrored user accounts on the FTK computer and on the evidence machine to access the data on a remote (network) computer outside of the domain.
3. Enter the username and password into the User Account Credentials dialog.



4. Click *Next* to finish the install.
5. Restart the machine.

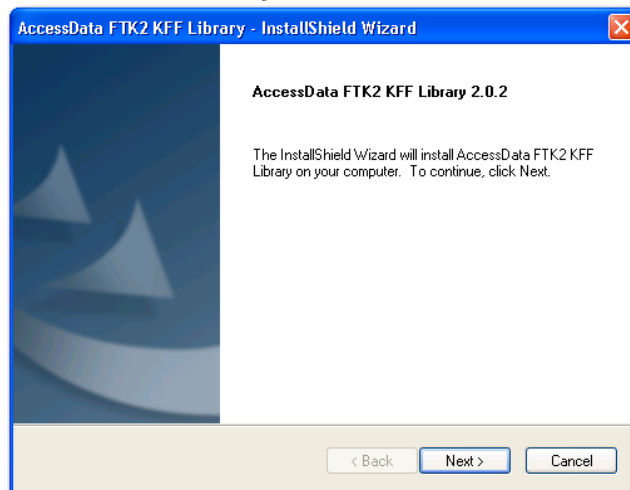
## INSTALLING THE KFF

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.

Figure 2-9. *Install KFF Button*

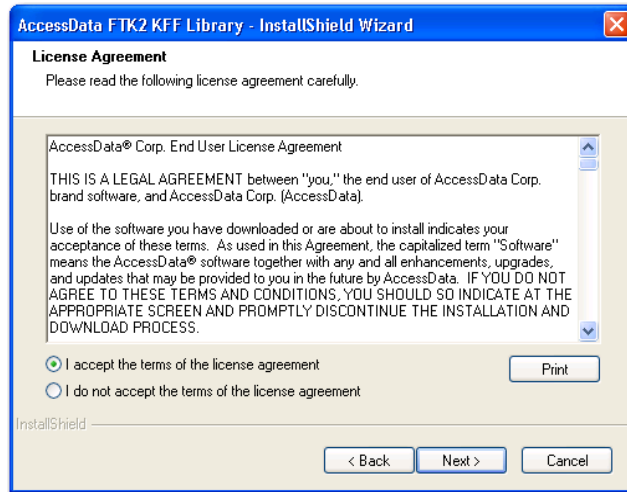


1. Click *Install KFF Library*



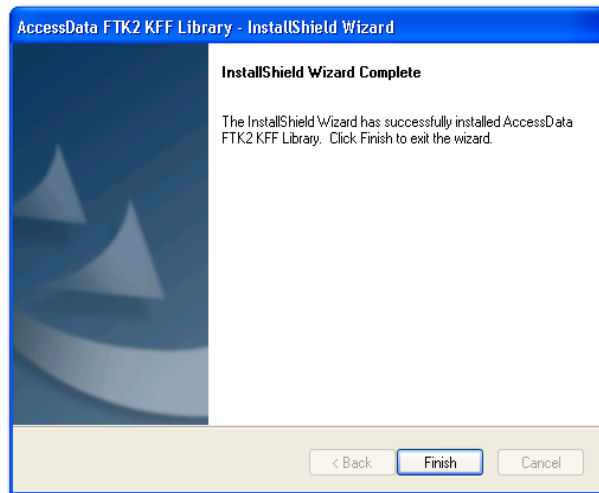
2. Click *Next*.

3. Accept the KFF license agreement.



4. Click *Next*.

5. Allow installation to progress.

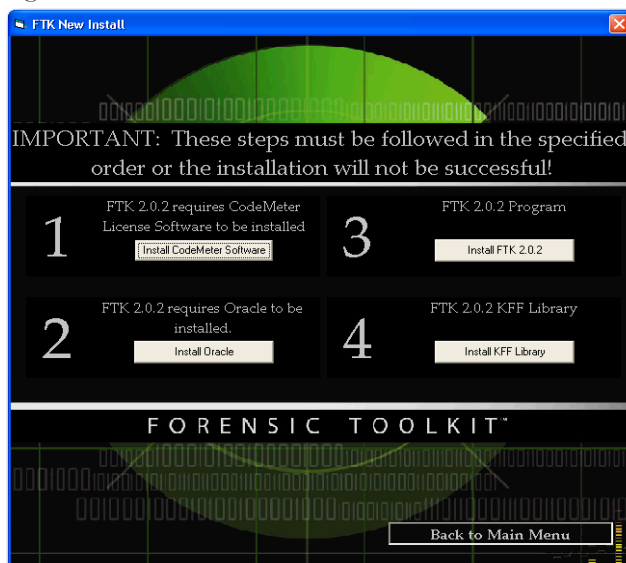


6. Click *Finish* to end the installation.

## INSTALLING ON SEPARATE COMPUTERS

FTK 2.1 can be installed on two separate computers. To do this, change the steps, as shown again in the following figure, to 2, 4, 1, 3. Perform steps 2 and 4 on the computer to run Oracle. (The KFF Library installs into the Oracle installation.) Then perform steps 1 and 3 on the computer designated to run the FTK Program.

*Figure 2-10. Install New FTK Screen*



## INSTALLATION RESULTS

If the default install location was selected, the FTK Program installation puts the program files in the following folder: C:\Program Files\AccessData\Forensic Toolkit\2.1.0\.

## ADDITIONAL PROGRAMS

To change to another supported language other than the default English (United States) that ships with FTK, LanguageSelector must be installed. For more information on LanguageSelector, see “Selecting the Application Language” on page 201 of the User Guide.



If licenses need to be managed, LicenseManager must be installed. For more information on LicenseManager, see “Managing Licenses with LicenseManager” on page 190 of the User Guide.

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

## UPGRADING TO FTK 2.1

The following instructions describe how to upgrade from AccessData® Forensic Toolkit® (FTK®) version 2.0 to FTK 2.1. For the upgrade, the original FTK 2.0, must already be installed.

**Note:** As a best practice, back up all case data (if possible) before upgrading your software.

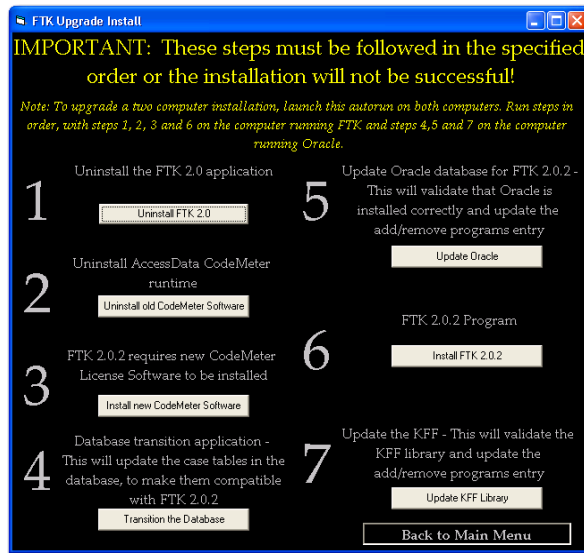
1. Insert the FTK 2.1 DVD in your computer.

Alternatively, if you downloaded the .zip file from the AccessData Web site, extract the contents to a folder and double-click the **autorun.exe** file.

If the installation utility does not launch automatically, browse to the DVD and double-click the **autorun.exe** file.



2. Click *Upgrade to FTK 2.1* to display the seven steps required to upgrade from FTK 2.0 to FTK 2.1.



3. On Step 1, click *Uninstall FTK 2.0*.

**Important:** To avoid losing case files, it is very important that you follow the instructions in this dialog carefully.

This automatically uninstalls the FTK Package from the computer. Allow the computer to restart after the uninstallation process has completed.

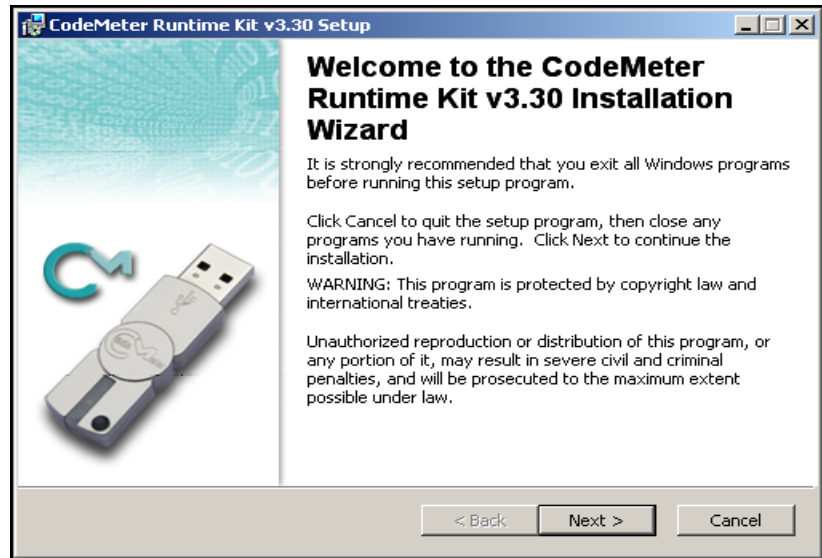
**Note:** You may need to manually end the FTK Installation program before Windows<sup>®</sup> can restart.

4. Run the autorun.exe file again.
5. On Step 2, click *Uninstall old CodeMeter Software*.

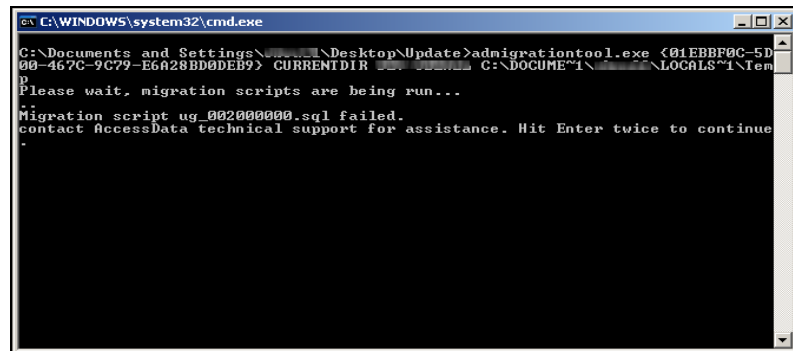
The only entry for CodeMeter<sup>\*</sup> in Add or Remove Programs should be CodeMeter Runtime Kit v3.30a. If any previous version (containing titles such as “CodeMeter” or “AccessData CodeMeter”) are installed, they need to be removed.

This process is automatically completed by this step.

6. On Step 3, click *Install new CodeMeter Software*.

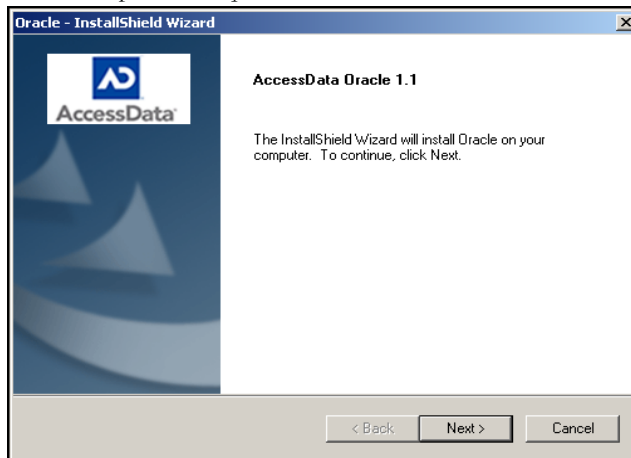


7. Click *Next* and follow the wizard installation instructions to install the CodeMeter Runtime software.
8. When CodeMeter installs successfully, click *Finish* to return to the FTK Upgrade Install window.
9. On Step 4, click *Transition the Database*.



This patch file converts the database schema to the format required by FTK 2.1. After the batch file runs, it indicates success or failure. If the batch file installed correctly, close the window and return to the FTK Upgrade Install window. If running the batch was unsuccessful, contact AccessData Customer Support.

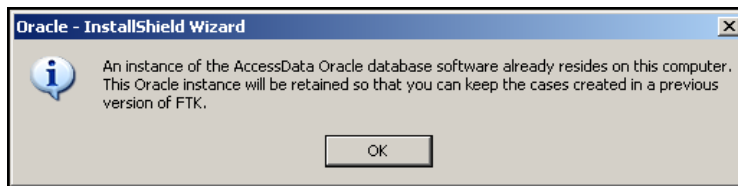
10. On Step 5, click *Update Oracle*.



This step only updates the current installation of Oracle, it does not reinstall Oracle.

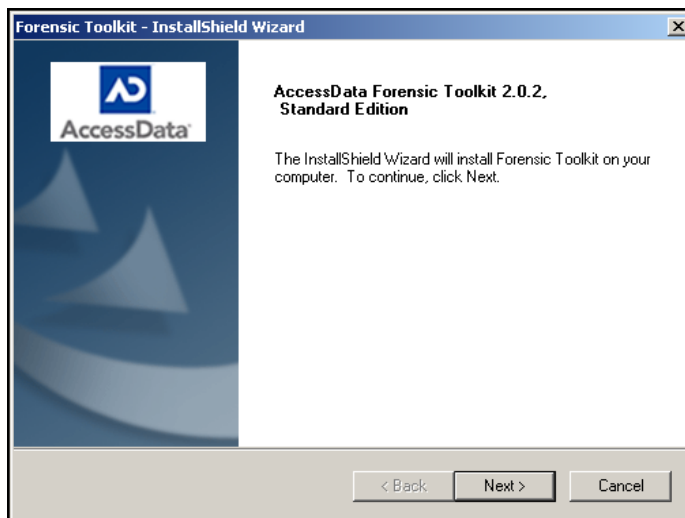
11. Click *Next* and follow the on-screen instructions.

The Oracle install wizard runs and the following dialog should appear indicating that Oracle already resides on the computer and that cases created in previous versions of FTK will be retained.

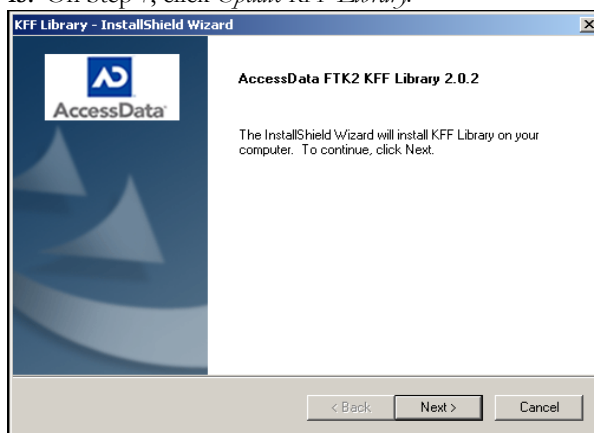


12. Click *Finish* at the Install Complete dialog to return to the FTK Upgrade Install window.

13. On Step 6, click *Install FTK 2.1* and follow the online installation instructions.



14. When FTK 2.1 installs successfully, click *Finish* to return to the FTK Upgrade Install window.
15. On Step 7, click *Update KFF Library*.

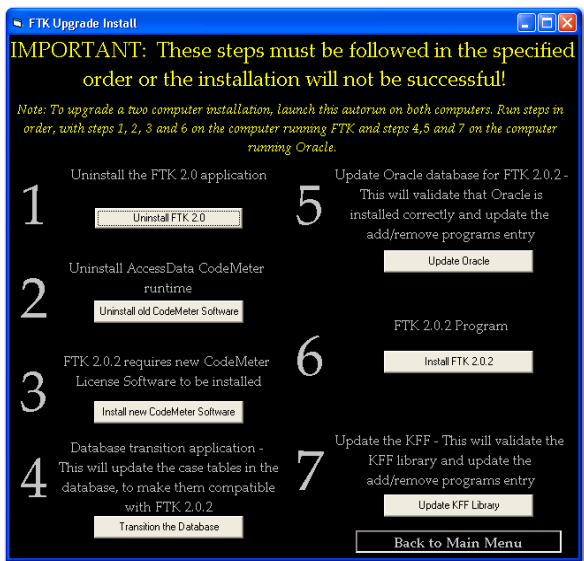


16. Click *Next* and follow the on-screen installation instructions.
17. After the KFF Update installs successfully, click *Finish* to return to the FTK Upgrade Install window.
18. Click *Back to Main Menu*.
- FTK 2.0.4 is now upgraded to FTK 2.1.

# UPGRADING A TWO-COMPUTER CONFIGURATION

To upgrade a two-computer configuration (FTK Package and associated programs on one box and Oracle and the KFF on the other machine) follow the directions specified in the following figure.

Figure 2-11. Seven Uninstall Steps



Case data is preserved through the upgrade, but it is good practice to back up all cases and perform the upgrade in this order, 1, 2, 3 on the FTK Package box (You uninstall the FTK Package and install the FTK Program indicating a major difference between FTK 2.0 and 2.1.) Then 4, 5 on the Oracle box. Then 6 on the FTK Program box. And, finally, 7 on the Oracle box to update the KFF. This process is illustrated in the table below:

TABLE 2-1 What to do Where

| Steps to Perform on FTK Machine   | Steps to Perform on Oracle Machine   |
|-----------------------------------|--------------------------------------|
| 1. Uninstall FTK 2.0x application | 4. Database Transition               |
| 2. Uninstall CodeMeter Software   | 5. Update Oracle database for 2.1.0. |
| 3. Install New CodeMeter Software | 7. Update the KFF Library            |
| 6. Install FTK 2.1 Program        |                                      |

## Chapter 3 Concepts

Before using AccessData Forensic Toolkit (FTK), a basic knowledge of the FTK interface is helpful. The FTK interface contains six main tabs, organized like tabbed pages, each with a specific focus. Most tabs also contain a common toolbar and file list with customizable columns.

### STARTING FTK

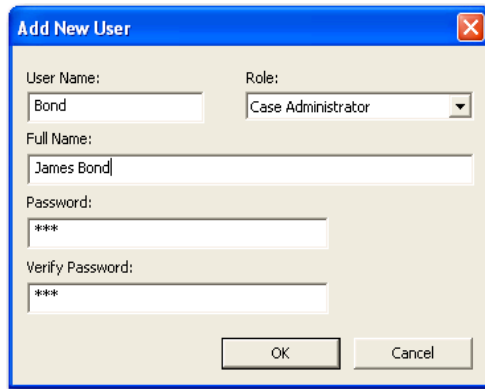
After you complete the installation, start FTK by selecting *Start > All Programs > AccessData > Forensic Toolkit > AccessData Forensic Toolkit 2.1*, or by selecting the *AccessData Forensic Toolkit 2.1* shortcut on the desktop.

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

### SETTING UP THE APPLICATION ADMINISTRATOR

On first launch a application administrator must be created to manage the database. The Add New User dialog box opens automatically. The first added user is the case and database administrator or superuser. The superuser can add new users to the database to administer (Case Administrator) or review (Case Reviewer) the case as needed by clicking *Database > Add User* to open the Add New User dialog. The following figure displays the Add New User dialog.

Figure 3-1 Add New User Dialog

The image shows a Windows-style dialog box titled "Add New User" with a blue title bar and a red close button. The dialog contains several input fields: "User Name:" with the text "Bond", "Role:" with a dropdown menu showing "Case Administrator", "Full Name:" with the text "James Bond", "Password:" with masked characters "\*\*\*\*", and "Verify Password:" with masked characters "\*\*\*\*". At the bottom right are "OK" and "Cancel" buttons.

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.

## USING THE CODEMETER STICK

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

You can use the LicenseManager application to monitor your FTK subscription. For more information, see “Managing Licenses with LicenseManager” on page 216.

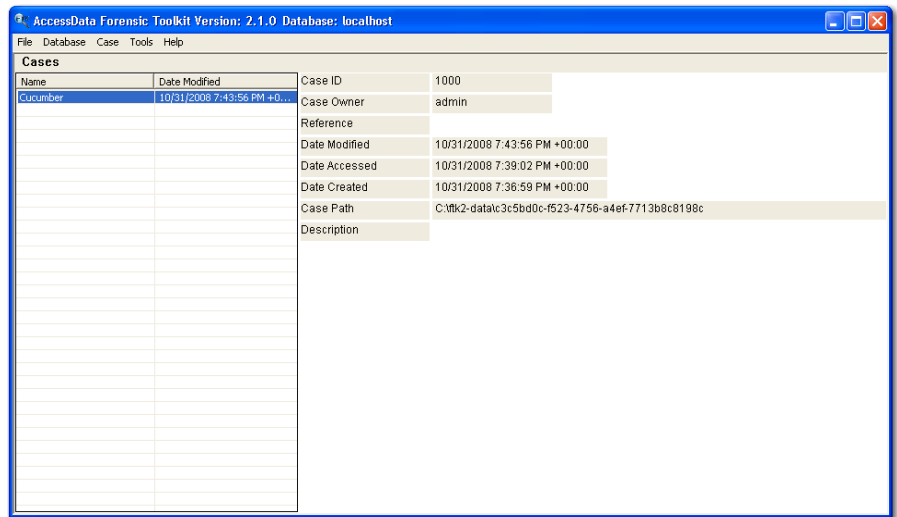
**Note:** FTK.2.0 does not work with the KEYLOK (green) dongle used with previous versions of FTK.

## USING THE CASE MANAGER WINDOW

FTK manages cases from a central database. The Case Administrator administers the case from the Case Manager window. The following figure displays the Case Manager window.



Figure 3-2 Case Manager Window.



After logging into FTK, the Case Manager window appears with the following menus:

- File
- Database
- Case
- Tools
- Help

The following tables shows the available Case Manager menu options.

**TABLE 3-1 Case Manager File Menu**

| Option | Description |
|--------|-------------|
| Exit   | Exits FTK.  |

**TABLE 3-2 Case Manager Database Menu**

| Option | Description   |
|--------|---|
| Log In | Opens the authentication dialog for users to log into the database. |

**TABLE 3-2 Case Manager Database Menu**

| Option   | Description   |
|----------|---|
| Log Out  | Logs the user out of the current case.  |
| Add User | Create a user with either Reviewer or Administrator rights to the database. This can only be done by the application administrator. |

**TABLE 3-3 Case Manager Case Menu**

| Option           | Description  |
|------------------|--|
| New              | Start a new case with the logged-in user as the Administrator. Case Reviewers cannot start a case. |
| Open             | Opens the highlighted case with its included evidence.   |
| Administer Users | Allows the Administrator to adjust or control the rights of added users.                           |
| Backup           | Backs up selected cases.   |
| Restore          | Brings back a selected, saved case.  |
| Delete           | Deletes selected cases.  |

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

| Option | Description   |
|--------|---|
| Tools  | Preferences settings: <ul style="list-style-type: none"><li>• Choose temporary file path</li><li>• Choose network security device location. Options are:<ul style="list-style-type: none"><li>• Ip Address</li><li>• Port</li></ul></li></ul> |

**TABLE 3-5 Case Manager Help Menu**

| Option      | Description   |
|-------------|---|
| Diagnostics | View the activity of the databases on which cases are stored, and of the Worker machines assigned to each case. |
| User Guide  | Opens the FTK User Guide in PDF. The manual is formatted for two-sided printing.                                |
| About       | Provides copyright and trademark information about FTK and other intellectual property of AccessData.           |

## THE FTK WINDOW

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

- File
- Edit
- View
- Evidence
- Filter
- Tools
- Help

The following tables show the available options from the FTK2.1 window menus.

**TABLE 3-6 FTK2.1 File Menu**

| Option                | Description   |
|-----------------------|---|
| 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 desination.   |
| 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.   |

**TABLE 3-6 FTK2.1 File Menu**

| Option | Description   |
|--------|---|
| Report | Opens the Report Options window for creating a case report.   |
| Close  | Closes the FTK Window and returns to the Case Manager window. |
| Exit   | Closes both the FTK and Case Manager windows.                 |

**TABLE 3-7 FTK2.1 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. |

**TABLE 3-8 FTK2.1 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>• Medium</li><li>• Small</li><li>• Tiny</li></ul> |

**TABLE 3-8 FKTK2.1 View Menu**

| Option                | Description  |
|-----------------------|--|
| Tab Layout            | <p>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:</p> <ul style="list-style-type: none"><li>• Lock</li><li>• Add</li><li>• Remove</li><li>• Save</li><li>• Save All Layouts</li><li>• Restore</li><li>• Reset to Default</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 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.   |
| File Content          | Inserts the File Content pane into the current tab.  |
| Email Attachments     | Displays the attachments to email object found in the case.<br>Available only in the email 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.  |

The tree and search views are exclusive settings, meaning that you can use only one tree view per pane, and only one search view per pane. For more information on using the View menu see, .

**TABLE 3-9 FTK2.1 Evidence Menu**

| Option              | Description   |
|---------------------|---|
| Add/Remove          | Opens the Manage Evidence dialog, used to add and remove evidence.  |
| 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. |

**TABLE 3-10 FTK2.1 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. 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.   |
| Tab Filter | Allows the selection of a filter to apply to a current tab.   |

**TABLE 3-11 FTK2.1 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</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.   |
| Verify Image Integrity | Generates hash values of the disk image file for comparison.  |
| Credant Decryption     | Opens the tools for Credant <sup>®</sup> decryption. Credant is a third party encryption tool that encrypts files, folders, partitions, or entire disks. This will be discussed in detail later in this manual.                 |
| 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> |

**TABLE 3-12 FTK2.1 Help Menu**

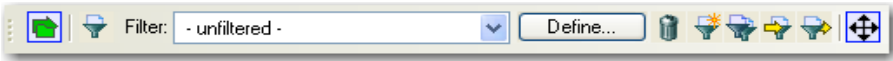
| Option      | Description   |
|-------------|---|
| User Guide  | Provides a link to the FTK 2.1 User Guide.          |
| Diagnostics | Allows the troubleshooting of database connections. |
| About       | Provides information about the current FTK release. |

# 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 “Customizing the Interface” on page 191.






# 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 3-13** Toolbar Components

| Component   | Description  |
|---|--|
|    | 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  |
|  | Creates a new filter   |



**TABLE 3-13** 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 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. |
|  | 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 197.



## FILE LIST TOOLBAR

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

**TABLE 3-14 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.  |
|  | Opens the Export File List, allowing the user to save selected files to another folder.. |
|  | Opens Copy Special dialog box.   |

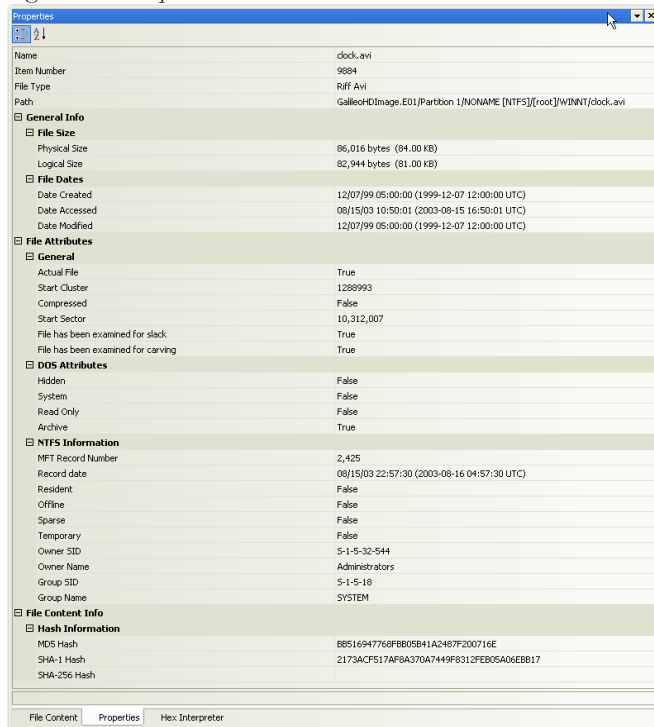
**TABLE 3-14** File List Toolbar

| Component   | Description  |
|---|--|
|  | Opens the Column Settings dialog box.  |
|  | Sets the columns to a specific set from the following list: <ul style="list-style-type: none"><li>• Default</li><li>• Email</li><li>• File Listing</li><li>• Normal (default)</li><li>• Reports: File Path Section</li><li>• Reports: Standard</li></ul> |

**PROPERTIES PANE**

The Properties pane displays information about a selected file. The following graphic displays a portion of the information contained in the Properties pane. This information corresponds to information displayed in the File List.

Figure 3-3 Properties Pane



The following table highlights the components of the Properties pane:

**TABLE 3-15 Properties Pane Components**

| Option       | Description  |
|--------------|--|
| Name         | The filename of the selected file.   |
| Item Number  | The arbitrary number assigned to the item during case processing.  |
| File Type    | The type of selected file.   |
| Path         | The path to the selected file.   |
| General Info | General information about the selected file: <ul style="list-style-type: none"> <li>• <b>File Size:</b> lists the physical and logical sizes of the file.</li> <li>• <b>File Dates:</b> lists the dates and times when the file was created, last accessed, and last modified on the imaged system.</li> </ul> |

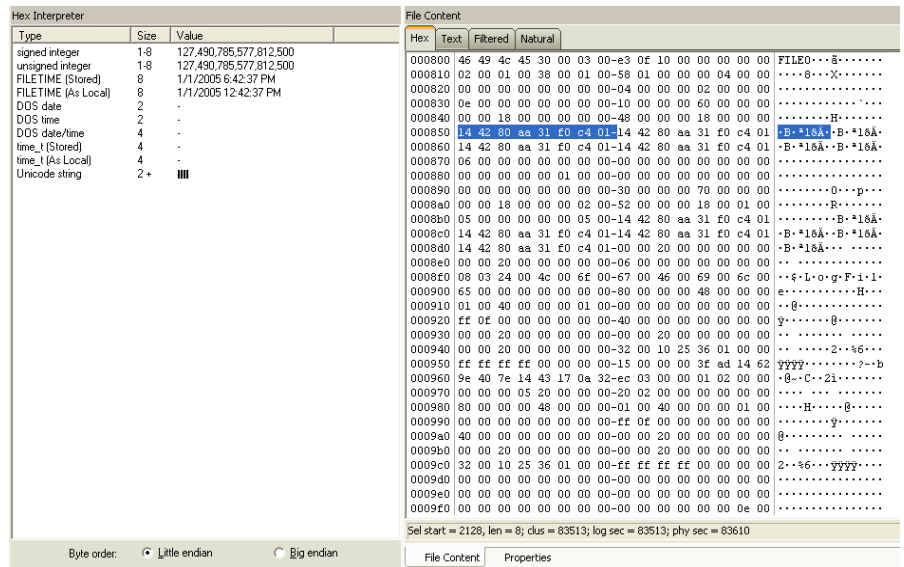
**TABLE 3-15** Properties Pane Components

| Option            | Description  |
|-------------------|--|
| File Attributes   | <p>The attributes of the file:</p> <ul style="list-style-type: none"><li>• <b>General:</b> indicates Actual File status, Start Cluster, Compression status, Start Sector, and whether the document has been examined for slack and/or carving.</li><li>• <b>DOS Attributes:</b> indicates attribute status for Hidden, System, Read Only, Archive, and 8.3 Name.</li><li>• <b>NTFS Information:</b> Indicates MFT Record Number, Record Date, indicates True or False status on whether the file is Resident, Offline, Sparse, or Temporary, and displays the Owner SID and Group SID.</li></ul> |
| File Content Info | <p>The content information and verification information of the file:</p> <ul style="list-style-type: none"><li>• <b>Hash Information:</b> lists the file's MD5 hash, SHA-1 hash, and SHA-256 hashes.</li></ul>   |

## HEX INTERPRETER PANE

The Hex Interpreter pane interprets hexadecimal values selected in the viewer into decimal integers and possible time and date values as well as unicode strings. The following graphic displays the Hex Interpreter Pane:

Figure 3-4 Hex Interpreter Pane and Corresponding File Content Pane Hex View Tab



To convert hexadecimal values, highlight one to eight adjacent bytes of hexadecimal code in the File Content Viewer, Hex tab. Select two or more bytes for the Unicode string, depending on the type of data you wish to interpret and view. Switch to the Hex Interpreter tab at the bottom of the File Content Viewer, Hex tab, or open it next to the File Content Hex Tab view, and 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 significant 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 or the other, and are now “ported” to the other system. You can’t always just apply one rule and automatically know which it is.

FTK2.1 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 “The Hex Interpreter Tab” on page 100.

## FILE CONTENT

The File Content pane shows you a file’s contents in several different views to help you see potential evidence.

### NATURAL TAB

The Natural tab displays a file’s contents as it would appear normally. The tab includes Default, Media, and Web viewers, indicated by tabs on the right.

### DEFAULT TAB

This viewer uses the Oracle Stellent\* INSO\* filters for viewing hundreds of file formats without the native application installed.

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

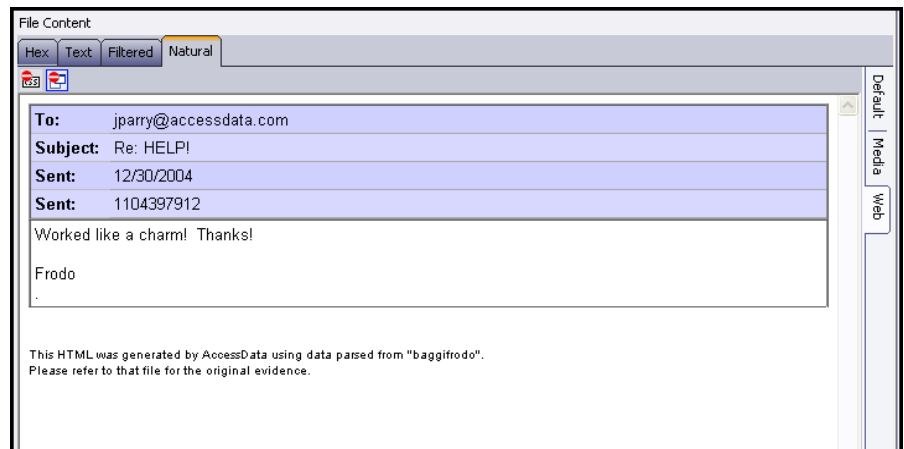
### MEDIA TAB

The Media Tab plays embedded audio and video files through 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. The following figure displays an email displayed in a web tab.

Figure 3-5 Web Tab



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 3-16 Natural Tab: Web Tab Toggle Buttons**

| Component   | Description   |
|---|---|
|    | Disable CSS Formatting. This button disables any fonts, colors, and layout from cascading style sheets. HTML formatting not part of a cascading style sheet may remain. |
|  | Disable External Hyperlinks. This button disables any hyperlinks in the file.   |

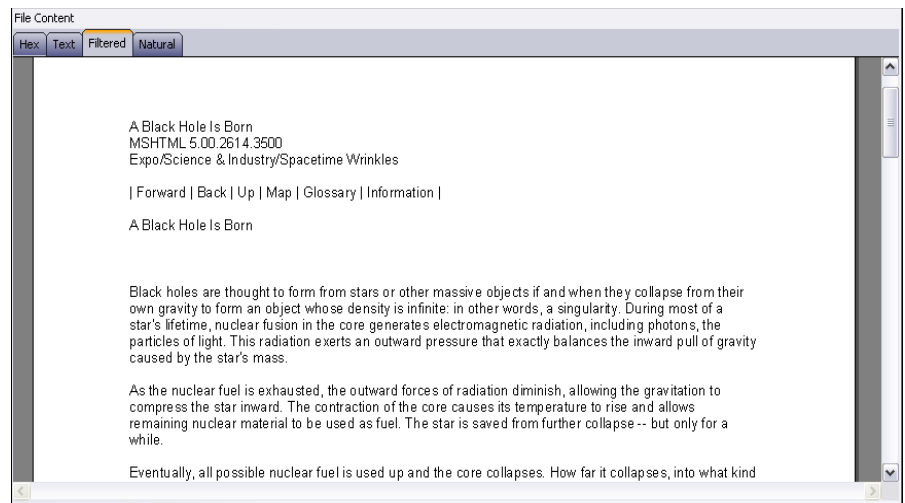
FTK displays the view (Web, Media, or Default) that is best for the selected file.

## FILTERED TAB

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



Figure 3-6 Filtered Tab

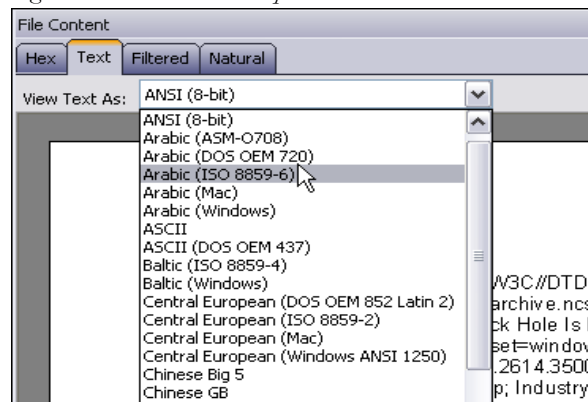


The text is taken from an index created for the current FTK session if indexing was not previously selected.

## 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 3-7 Text View Drop-Down Menu

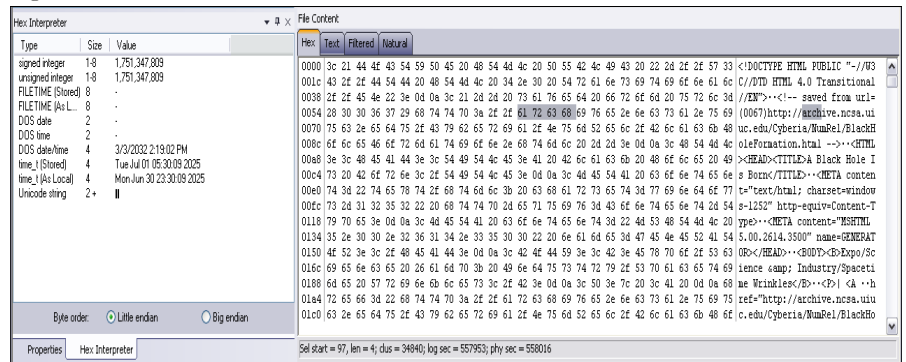


The FTK File Content pane currently provides many code pages from which to choose.

## HEX TAB

The Hex tab displays file contents in hexadecimal format. Use this view with the Hex Interpreter pane. The following figure shows the Hex tab selected, with a portion of the code selected and interpreted in the Hex Interpreter pane. For more information on the Hex Interpreter Pane, see “Hex Interpreter Pane” on page 47.

Figure 3-8 Hex Tab



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.

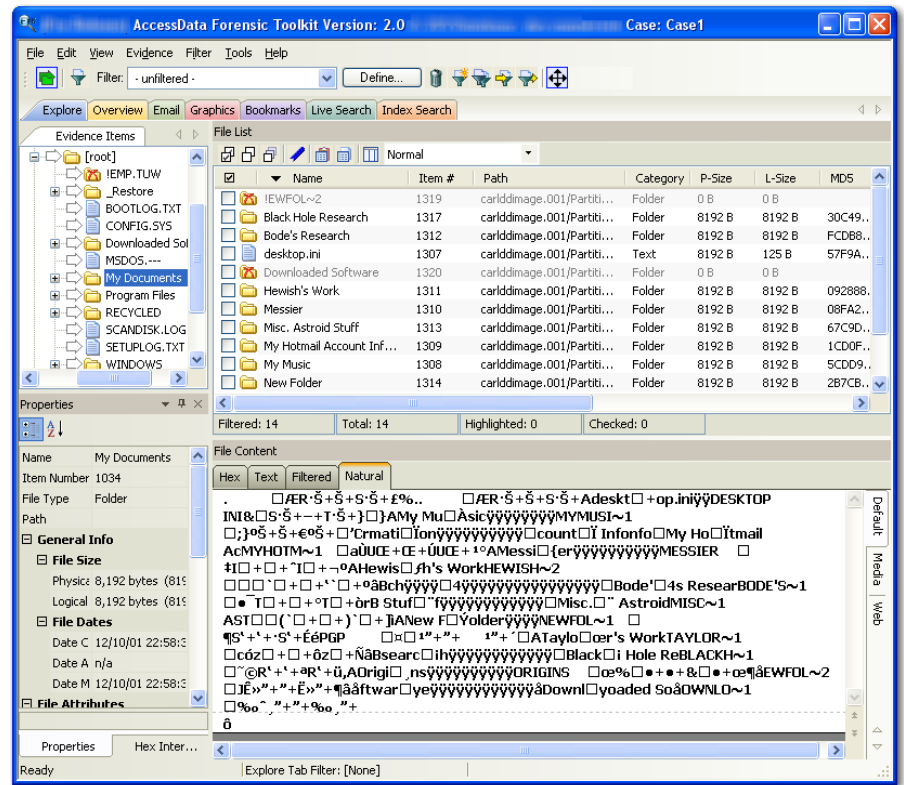
## USING TABS TO EXPLORE AND REFINE EVIDENCE

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

### 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 My Documents folder selected in the Explore Evidence Items tree.

Figure 3-9 Explore Tab



The Explore tab contains the following panes:

TABLE 3-17 Explore Tab Panes

| Pane          | Description   |
|---------------|---|
| Explorer Tree | 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 information about a file, such as filename, file path, and file type.  |

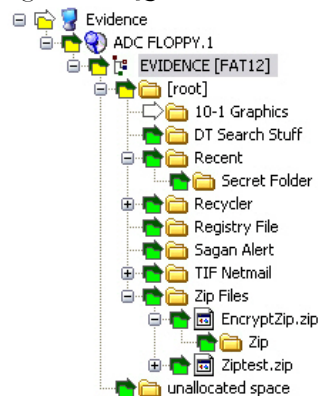
### TABLE 3-17 Explore Tab Panes

| <b>Pane</b>          | <b>Description</b>   |
|----------------------|--|
| File Content Viewer  | Displays the contents of the currently selected file from the File List. The Viewer toolbar allows the choice of different view formats. |
| Properties           | Displays characteristics and attributes, depending on the column settings being used, of the file selected in the File List.             |
| Hex Interpreter Pane | Provides possible meanings of a selection of a hexadecimal selection in the file content Viewer.   |

## 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 3-10 QuickPicks Filter Folder Selection



The QuickPicks filter simultaneously displays open and shut 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.

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.

## DATA PROCESSING STATUS DIALOG

The Progress dialog displays an estimation of how tasks are progressing. In the examples below, the dialog shows the progress of evidence being added to the case, both while it is in progress, and after successful completion:

*Figure 3-11 Data Processing Status: In Progress*

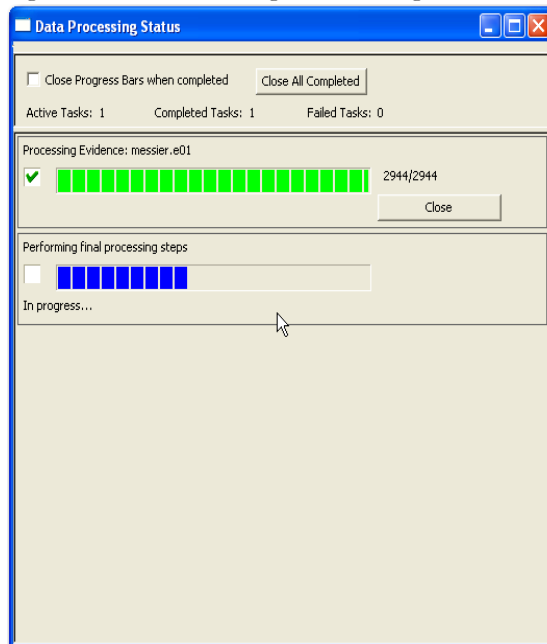
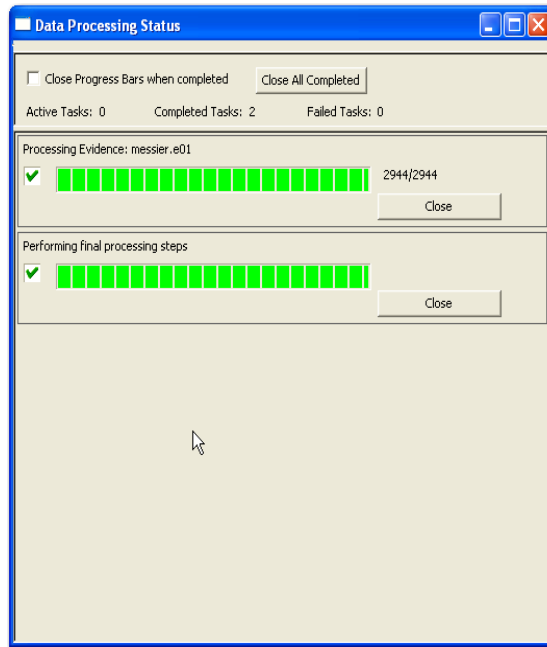



Figure 3-12 Data Processing Status: Successfully Completed



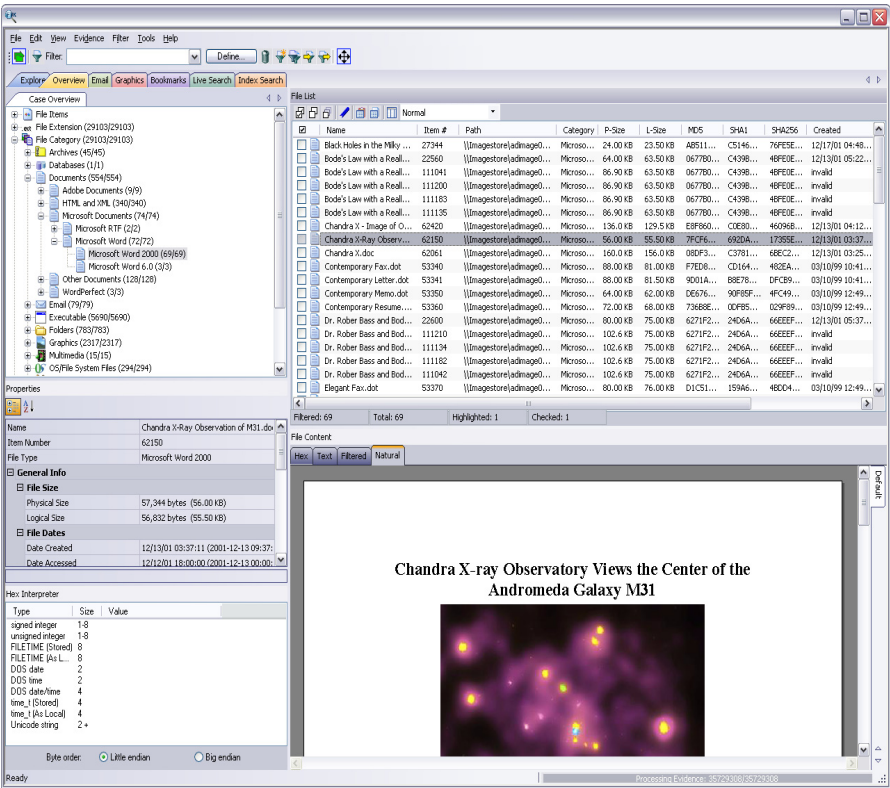
A blue progress bar for each task measures percentage complete by a ratio, or simply by a moving bar as each task progresses. An hourglass icon at the front of the bar indicates that the task is in progress, while a checkmark indicates that the task completed. When the task is complete, the blue progress bar turns green.

- Click and drag the *Scroll Bar* to view processing jobs that do not display within the default viewing area.
- Click *Close All Completed* to leave the Data Processing Status window open while any incomplete tasks remain open.
- Click the *Close* button adjacent to any individual task to remove that task and its progress bar from the dialog.
- Check *Close Progress Bars when completed* to automatically close each task bar as its task completes.
- Click the *Close*  button to close the Data Processing Status Window. This closes only the display and does not cancel any current tasks.

# 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 3-13 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 3-18 File Categories**

| Category            | Description  |
|---------------------|--|
| Archives            | Archive files include Email archive files, Zip, Stuffit, Thumbs.db thumbnail graphics, and other archive formats.        |
| Databases           | A list of MS Access 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*, 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 3-18 File Categories**

| Category               | Description  |
|------------------------|--|
| 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 <sup>*</sup> , Microsoft Excel <sup>*</sup> , QuattroPro <sup>*</sup> , and others.   |
| Unknown Types          | File types that AD FTK2.1 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 3-19 File Status Categories**

| Category          | Description   |
|-------------------|---|
| Bad Extension     | 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.   |
| 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.           |

**TABLE 3-19 File Status Categories**

| Category           | Description   |
|--------------------|---|
| Duplicate Items    | <p>Any items that have an identical hash.</p> <p>Because the filename is not part of the hash, identical files may actually have different filenames.</p> <p>The primary item is the first one found by FTK.</p>  |
| Email Attachments  | Files attached to the email in the evidence.  |
| Encrypted Files    | <p>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.</p> <p>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 Files and Folders" on page 163.</p> |
| 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.   |

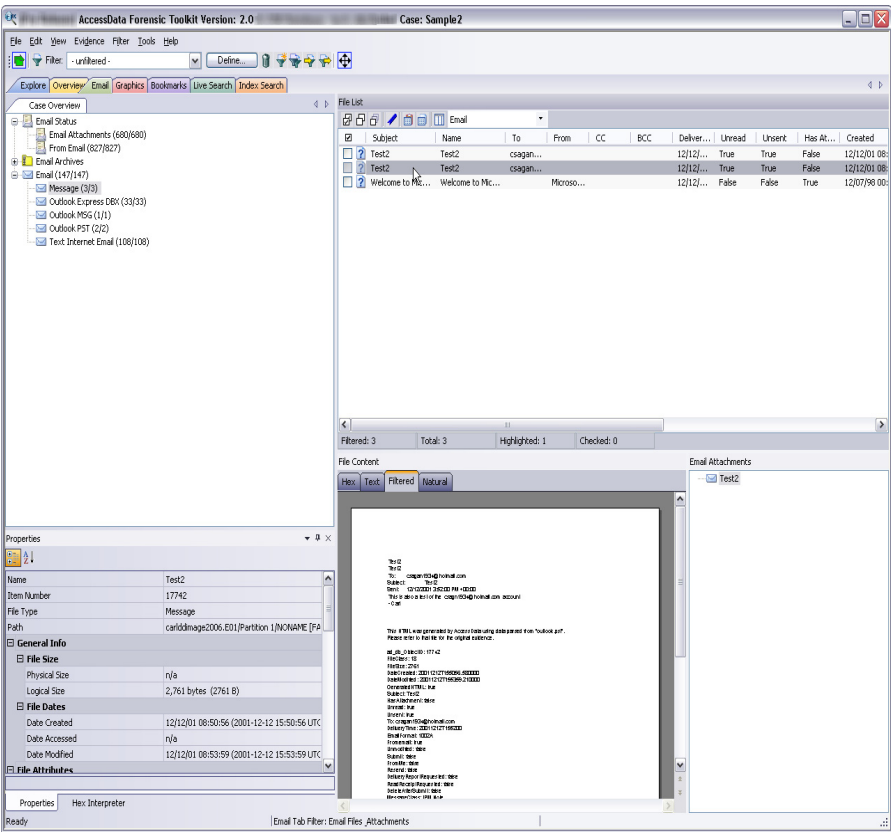
## BOOKMARK CONTAINER

The Bookmark Container lists bookmarks as they are nested in the Processed 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. For the list of the supported email applications, see “Email Message Programs” on page 238. The following figure represents the email tab.

Figure 3-14 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 their inclusions in their groups.

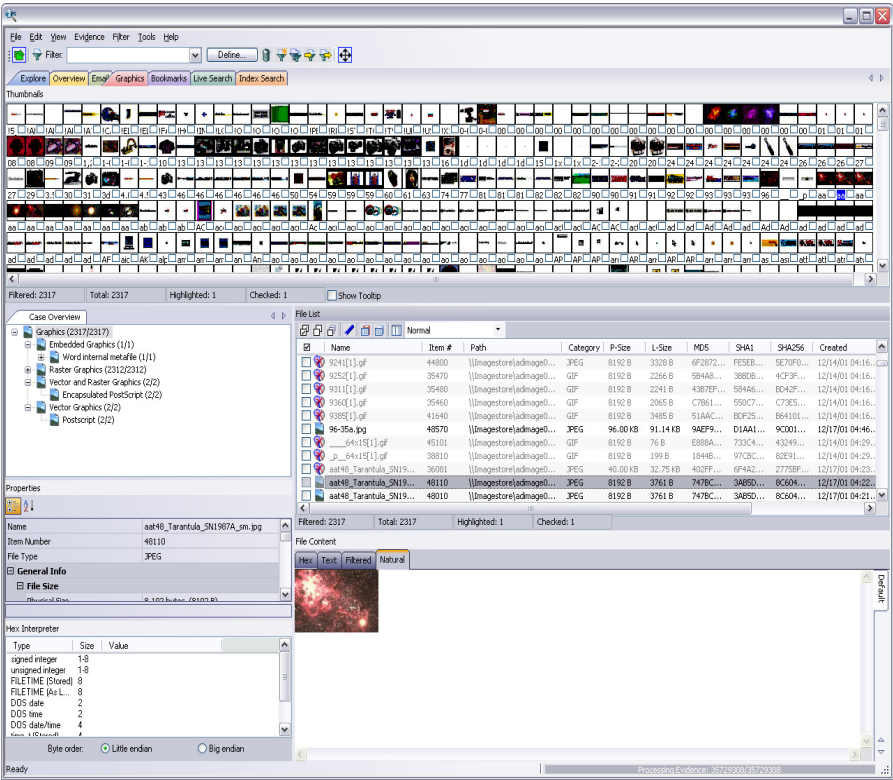
EMAIL TREE

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

GRAPHICS TAB

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

Figure 3-15 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 “Including Graphics” on page 181.

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**

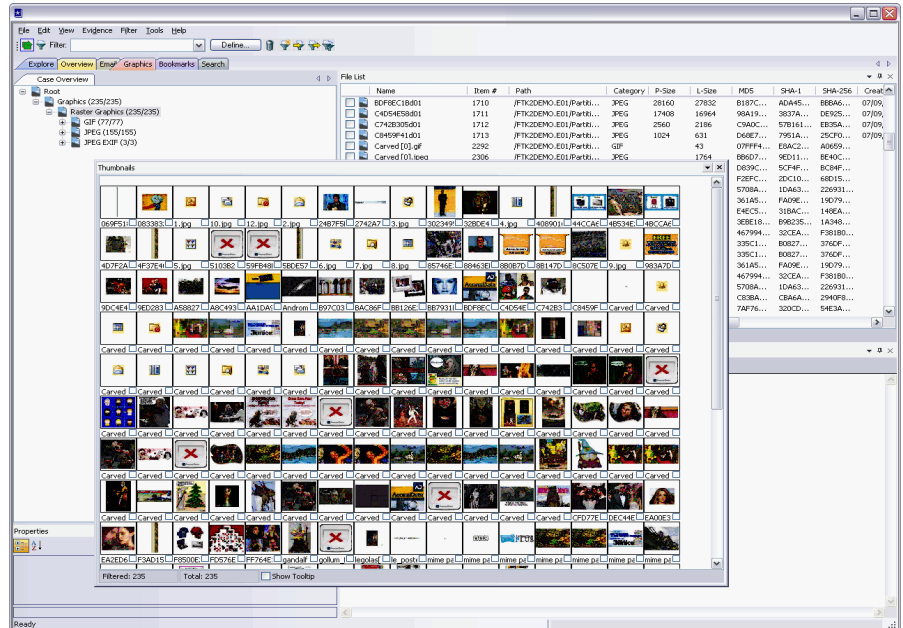
The thumbnail settings allow large amounts of graphic data to be displayed for evidence investigation. The investigator does not need to see details to pick out evidence; scan the thumbnails for flesh tones, photographic-type graphics, and perhaps particular shapes. Once found, the graphics can be inspected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

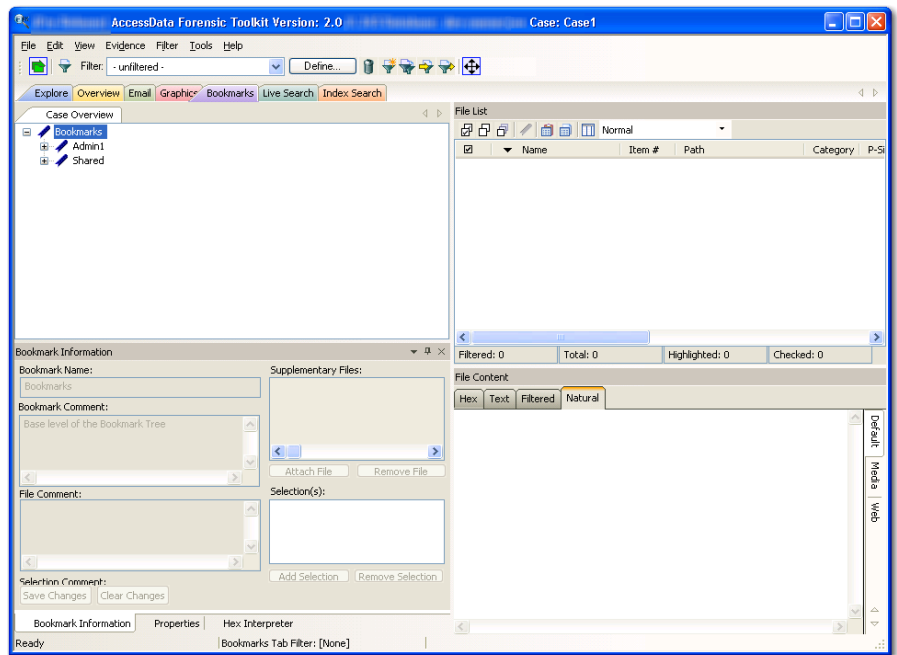
- Open the Thumbnails Settings sub-menu, and scale the thumbnails down to fit as many as possible in the pane.



## BOOKMARKS TAB

The Bookmarks tab displays all the items bookmarked as important items in the case. Add comments on the bookmarks where needed. For more information about bookmarking, see “Using the Bookmark Information Pane” on page 103.

Figure 3-16 Bookmarks Tab



The following table describes the features of the Bookmark tab.

**TABLE 3-20 Bookmark Tab**

| Features            | Description  |
|---------------------|--|
| Bookmark Comment    | Displays notes included with a bookmark.   |
| Bookmark Name       | Displays the name given to the bookmark when it was created.   |
| Clear Changes       | Removes comments that have not been saved.   |
| Selections          | 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.<br><br>This can be done for multiple files with multiple selections. |
| Save Changes        | Saves changes to the bookmark.   |
| File Comment        | Displays notes included with a file.   |
| Selection Comment   | Displays notes included with a selection.  |
| Supplementary Files | Lists additional files attached to the bookmark.   |

# SEARCH TABS

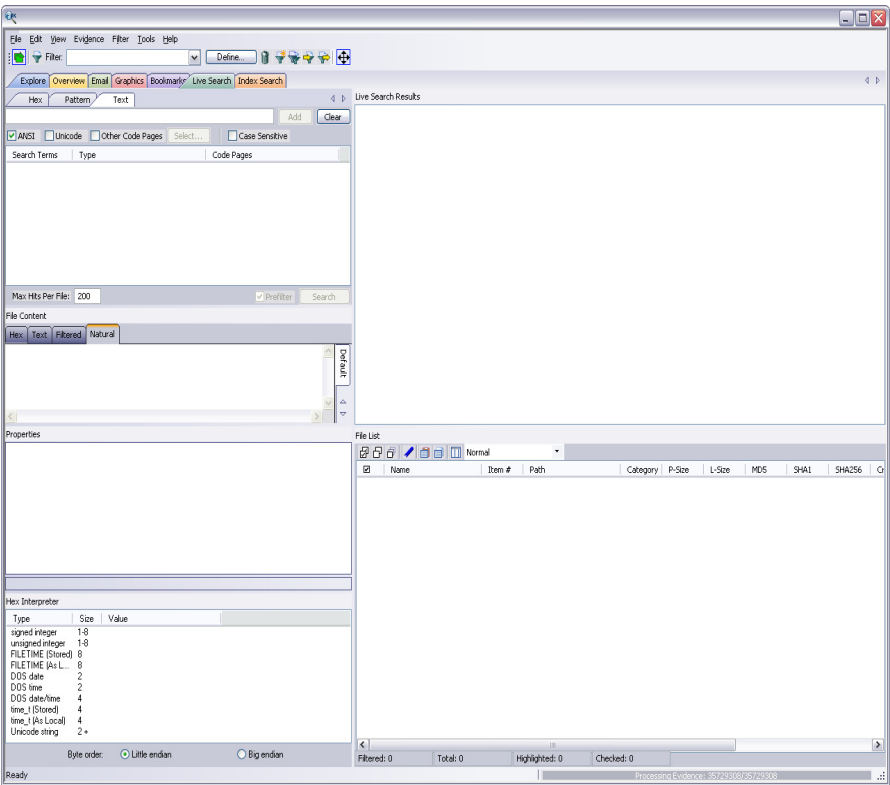
The Search Tabs allow the user to conduct an indexed search or a live search on the evidence. An indexed search is faster, while a live search is more flexible and powerful.

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 6 Searching a Case” on page 127.

## 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 3-17 Live Search Tab



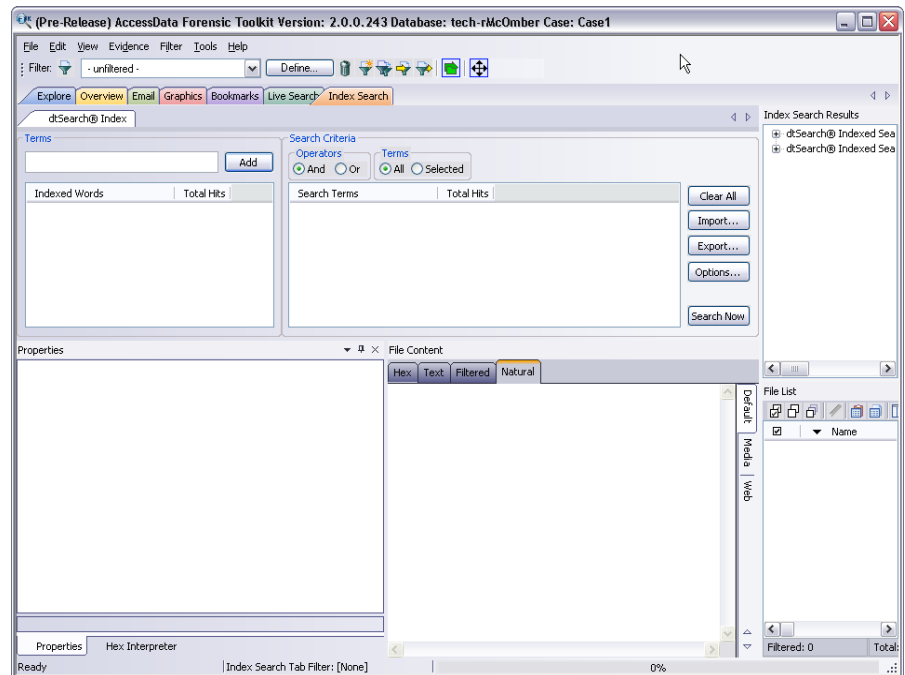


A live search is flexible because it can find non-alphanumeric character patterns. Comparatively, an Index search has to stick with the alphanumeric patterns created with an initial search index when the case is initially processed.

## 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 3-18 Index Search Tab

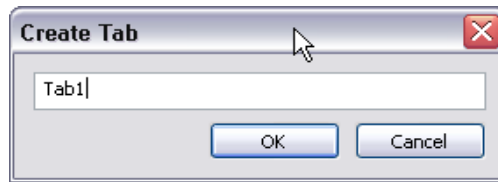


Evidence items can be indexed when they are first added to the case or at a later time.

## CREATING TABS

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

*Figure 3-19 Create Tab Dialog*



For more information on tab creation, see “Creating Custom Tabs” on page 197.

## *Chapter 4 Starting a New FTK2.1 Case*

After collecting the files or drive images to examine, start a case using AccessData Forensic Toolkit (FTK2.1).

### **LAUNCH FTK2.1**

FTK harnesses the power of multiple investigators and computer processors to analyze cases. The application administrator is created when FTK2.1 is launched the first time, and the Case Manager window opens. Run FTK2.1 by doing the following:

1. Click *Start > All Programs > AccessData > Forensic Toolkit > AccessData Forensic Toolkit 2.1*.

**Note:** Please note that it may take a few moments for FTK2.1 to run. This is because it is also launching the Oracle<sup>\*</sup> database.

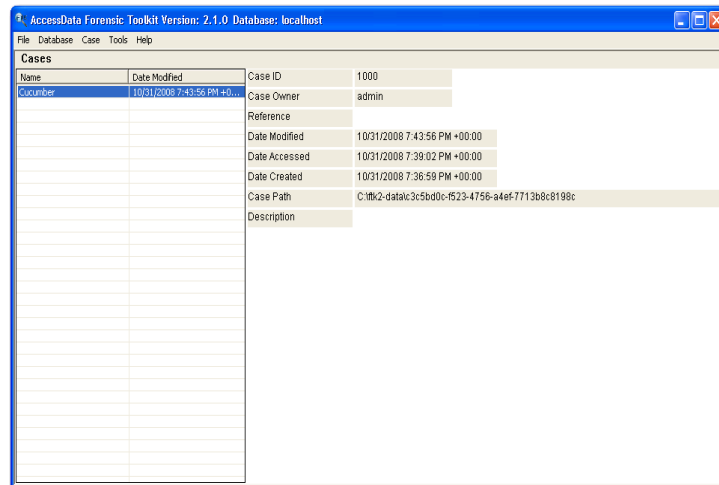
2. Log in using the case-sensitive username and password provided by the application administrator, as shown in the following figure:

Figure 4-1



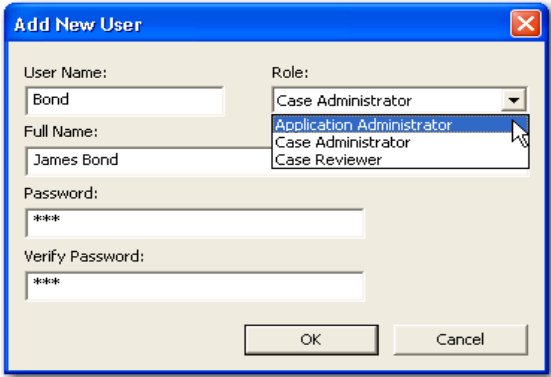
A successful login brings up the Case Manager window, as in the following figure:

Figure 4-2 Case Manager Window



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

3. Click *Database > 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.
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 4-1 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>• Application Administrator: can perform all types of tasks, including adding and managing users.</li><li>• Case Administrator: can process data and change settings to FTK, although only the application administrator can add new users.</li><li>• Case Reviewer: cannot create cases; can only process cases.</li></ul> |
| Full Name | Enter the full name of the user as it will appear on case reports.  |
| Password  | Enter and verify a password for this user.  |

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 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. A user having the Case Administrator role can perform the following tasks which are made unavailable to a user having the Case Reviewer role:

- Create cases
- Configure log options
- Data Carve
- Manually data carve
- Use the KFF Alert Editor
- Add Hashes to the KFF
- Add evidence
- Decrypt Files from the Tools menu
- Add Passwords from the Tools menu
- View items flagged as “ignorable” or “privileged.”
- Use FTK Imager
- Use Registry Viewer
- Use PRTK
- Use Find on Disk
- Use the Disk Viewer
- View file sectors
- Access the analysis tools menu
- Export files or folders
- Define, edit, delete, copy, export, or import filters

## CASE ADMINISTRATOR

A user assigned the Case Administrator role can do any of the above, however cannot create new users.

## ACQUIRING AND PRESERVING THE EVIDENCE

For digital evidence to be valid, it must be preserved in its original form. The disk image must be forensically sound, or 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 at the bit level, and allow read-only mode access to the hard drive.
- Software acquisition tools create a disk image that usually requires a hardware write-blocker, and makes no changes to the data or information on the hard drive.

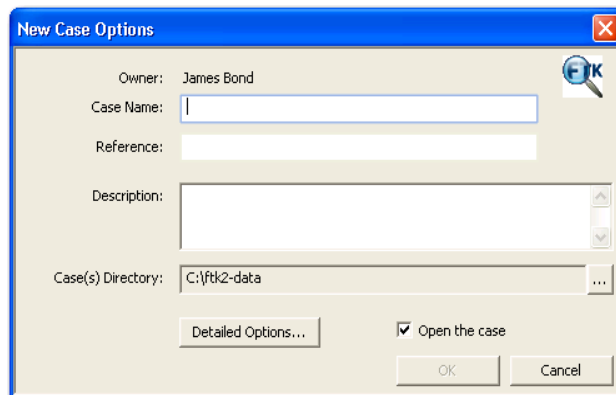
Use write-blocking devices when using these tools, because some operating systems, such as Windows, may make changes to the drive as it is reads the data to be imaged.


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 disk. 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.

## CREATING A CASE

FTK stores each case in an Oracle database, and allows case administration as they are created. When a Case Administrator creates a case, that user becomes that case's administrator. Start a new case from the Case Manager window with the following steps:

1. Launch FTK 2.1 and login. This opens the Case Manager window
2. Click *Case > New*.



3. Enter a name for the case in the Case Name field.
4. Enter the specific reference information in the Reference field. This field is not required to create a case.
5. Enter a 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 .
7. Click *Detailed Options* to choose settings for the case.
  - 7a. 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 74.
  - 7b. Click the *Evidence Discovery* icon to specify the location of the File Identification File, is one is to be used. For more information, see Figure , “Selecting Evidence Discovery Options,” on page 77.
  - 7c. 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 77.
  - 7d. 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 79.
  - 7e. Click OK.
8. Mark the *Open the Case* check box to see the case after clicking OK to close the New Case Options dialog.
9. Click OK.

**Note:** If the c:\ftk2-data folder is not set as shared, an error occurs during case creation.

## 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. 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.

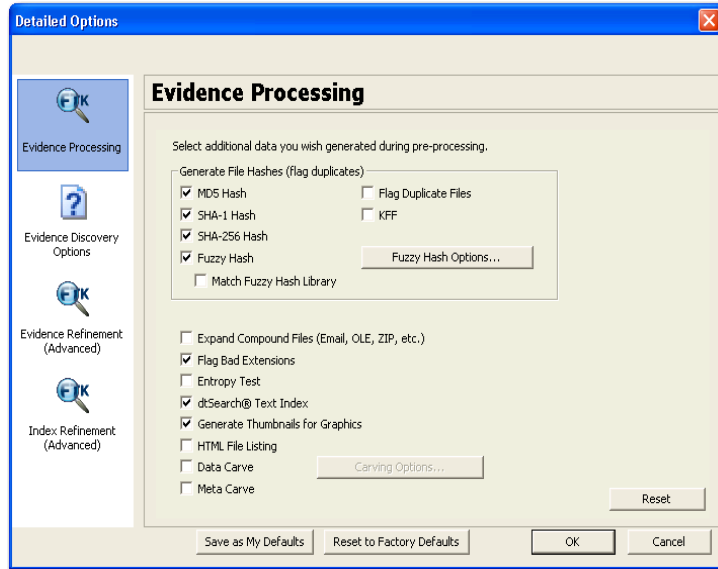
At the bottom of every Detailed Options selection screen you will find five buttons:

- 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.

Figure 4-3 Detailed Options Dialog



Another factor that can determine which processes to select is schedule. Time restraints may not allow for all tasks to be performed initially. 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.

The following table outlines the Evidence Processing options:

TABLE 4-2

| Process    | Description   |
|------------|---|
| MD5 Hash   | Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. For more information about MD5 hashes, see “Message Digest 5” on page 293.      |
| SHA-1 Hash | Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. For more information about SHA hashes, see “Secure Hash Algorithm” on page 295. |

**TABLE 4-2**

| Process                          | Description  |
|----------------------------------|--|
| SHA-256 Hash                     | Creates a digital fingerprint based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. SHA-256 is a hash function computed with 32-bit words, giving it a longer digest than SHA-1. For more information about SHA hashes, see “Secure Hash Algorithm” on page 295. |
| Fuzzy Hash                       | Mark this box to enable <i>Fuzzy hash options</i> to make options and <i>Match fuzzy hash library</i> . Fuzzy hash options allow you to specify the size of files to hash.   |
| Flag Duplicate Files             | Identifies files that are found more than once in the evidence.  |
| KFF                              | Using a database of hashes from known files, this option eliminates ignorable files and alerts to known illicit or dangerous files.<br><br>For more information about Known File Filter (KFF), see “Using the Known File Filter” on page 156.  |
| Flag Bad Extensions              | Identifies files whose types do not match their extensions.  |
| Expand Compound Files            | Automatically opens and processes the contents of compound files such as .zip files.   |
| Entropy Test                     | Determines if the data in unknown file types is compressed or encrypted.<br><br>The compressed and encrypted files identified in the entropy test are not indexed.   |
| dtSearch Index                   | 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.  |
| Generate Thumbnails for Graphics | Creates thumbnails for large graphics.   |
| HTML File Listing                | Creates an HTML version of the File Listing in the case folder.  |
| 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.<br><br>For more information on Data Carving, see “Data CarVing” on page 149.   |
| Meta Carve                       | Carves deleted directory entries.  |

## SELECTING DATA CARVING OPTIONS

When you choose to carve data select which types of data to carve:

1. Select *Data Carve*.
2. Click *Carving Options*.
3. Mark the *Exclude KFF Ignorables* box to specify not to carve those files.
4. 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.
  - Select individual file types by marking the checkboxes.
5. Define the 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
6. Click *OK*.

## INDEXING A CASE

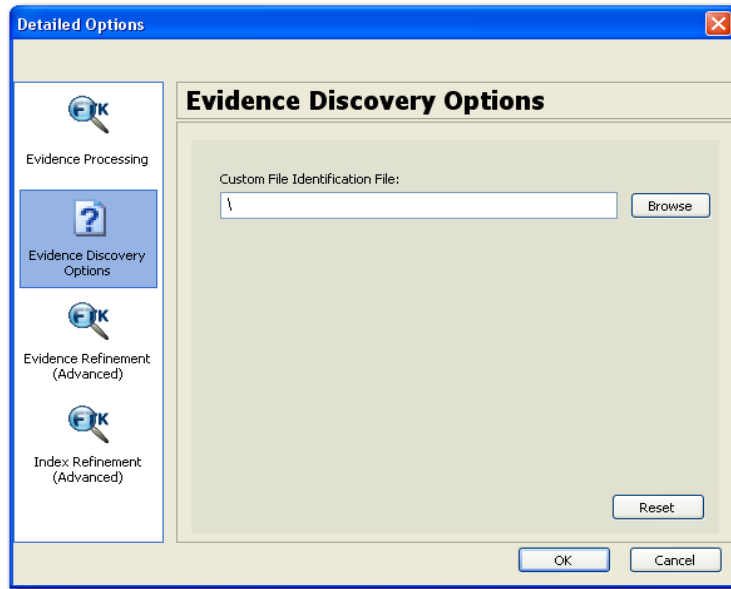
All evidence should be indexed to aid in searches. Index evidence when it is added to the case by checking the *dtSearch Text Index* box on the *Evidence Processing Options* dialog.

## 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 4-4 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 4-3 Custom Identification File Parameters**

| Parameter   | Description  |
|-------------|--|
| name        | The type displayed in the Overview tree branch. It also appears in the Category column.                      |
| description | Accompanies the Overview tree branch's name.   |
| category    | The Overview 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).                      |
| value       | An even number of hex bytes or characters with arbitrary white space.  |

**Note:** The investigator 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.

## SELECTING EVIDENCE REFINEMENT (ADVANCED) OPTIONS

The Evidence Refinement (Advanced) Options dialog allows you to specify how the evidence is sorted and displayed. The Evidence Refinement (Advanced) option allows you to exclude specific data from an individual evidence item.

Many factors can affect which processint tasks to select. For example, if you have specific information 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.

After data is excluded from an evidence item, it cannot be added back into the case. FTK does not allow the user to add the same evidence item more than once. If data that was previously excluded is found necessary, the user must create a new case. Consequently, AccessData strongly recommends the use of Include All Items unless you are absolutely certain that the excluded items are not necessary.

The following steps are for refining case evidence:

1. Click the Evidence Refinement (Advanced) icon in the left pane.

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

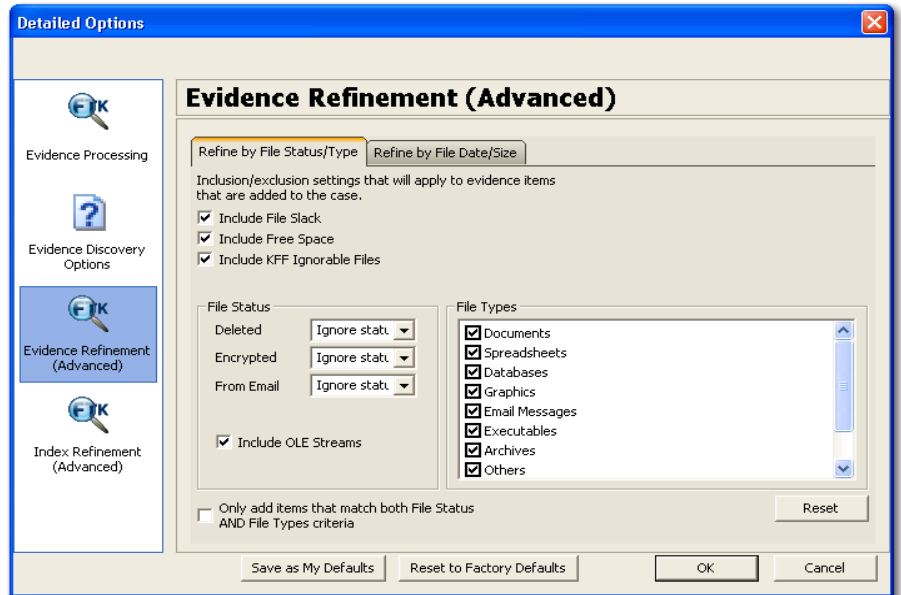
- Refine Evidence by File Status/Type

- Refine Evidence by File Date/Size
2. Click the corresponding tab to access the desired refinement type.
  3. Set the needed refinements for the current evidence item.
  4. To reset the menu to the default settings, click *Reset*.

## REFINING EVIDENCE BY FILE STATUS/TYPE

Refining evidence by file status and type allows the user to focus on specific files needed for a case. The following figure displays the detailed options dialog with Evidence Refinement selected.

Figure 4-5 Evidence Refinement by File Status/Type



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

**TABLE 4-4 Refine Evidence by File Status/Type Options**

| Options                     | Description  |
|-----------------------------|--|
| 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 | Mark to include files flagged as ignorable in the KFF for analysis.  |
| Deleted                     | Specifies the way to treat deleted files for cases where the scope of the warrant permits.<br>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 for cases where the scope of the warrant permits.<br>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 for cases where the scope of the warrant permits.<br>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 Duplicate Files     | Includes duplicate files for analysis.   |
| Include OLE Streams         | Includes encrypted files for cases where the scope of the warrant permits.   |

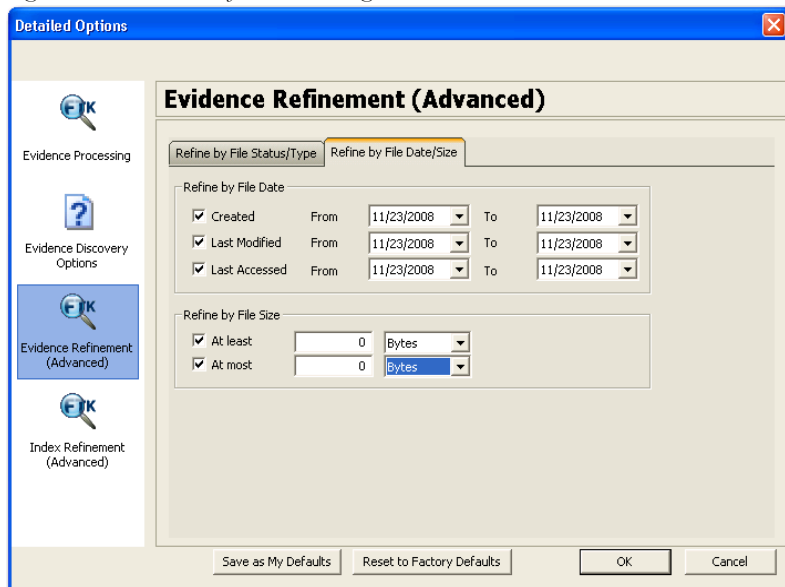
**TABLE 4-4 Refine Evidence by File Status/Type Options**

| Options   | Description                                      |
|---|--|
| File Types  | Specifies types of files to include and exclude. |
| Match using both File Type and File Status criteria | Applies both criteria to the refinement.         |

## REFINING EVIDENCE BY FILE DATE/SIZE

Make the addition of evidence items dependent on a date range or file size specified by the investigator. The following figure represents this type of selection dialog.

*Figure 4-6 Evidence Refinement Dialog*





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

**TABLE 4-5 Define Evidence by File Date/Size Options**

| Exclusion                    | Description   |
|------------------------------|---|
| Refine Evidence by File Date | To refine evidence 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 two date fields, enter beginning and ending dates.</li> </ol>               |
| Refine Evidence by File Size | To refine evidence by file size: <ol style="list-style-type: none"> <li>1. In the two size fields, enter the At Least and At Most file size values.</li> <li>2. In the drop-down list, 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 do not need to be indexed. Data can be excluded to save time and resources and to increase searching efficiency.

**Note:** AccessData strongly recommends using the default index settings.

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

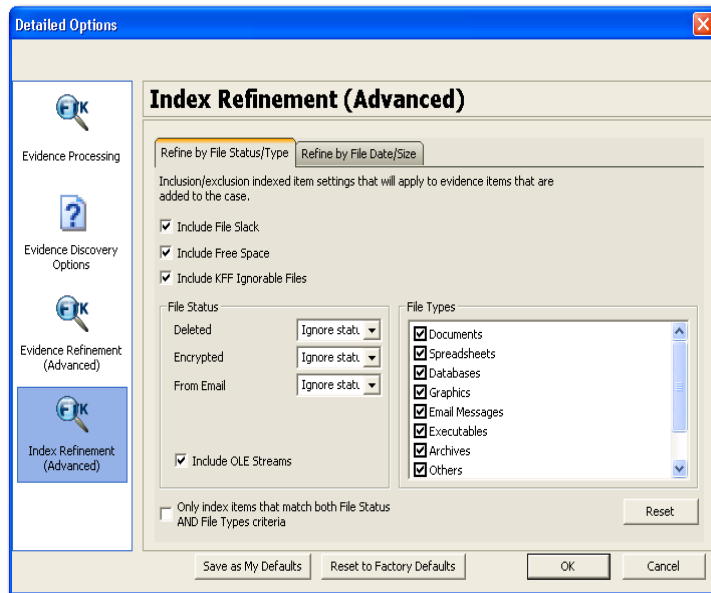
1. Click *Index Refinement (Advanced)* in the left pane.
2. The Index Refinement (Advanced) dialog is organized into two tabs:
  - Refine Index by File Status/Type
  - Refine Index by File Date/Size
3. Click the corresponding tab to access the desired refinement type.
4. Set the refinements for the current evidence item.

To reset the menu to the default settings, click *Reset*.

## 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.

Figure 4-7 Index Refinement Dialog



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

**TABLE 4-6 Refine Index by File Status/Type Options**

| Options                     | Description  |
|-----------------------------|--|
| Include File Slack          | Mark to include unallocated 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 | Mark to include files flagged as ignorable in the KFF for analysis.  |
| Deleted                     | Specifies the way to treat deleted files for cases where the scope of the warrant permits. Options are: <ul style="list-style-type: none"> <li>• Ignore status</li> <li>• Include only</li> <li>• Exclude</li> </ul> |

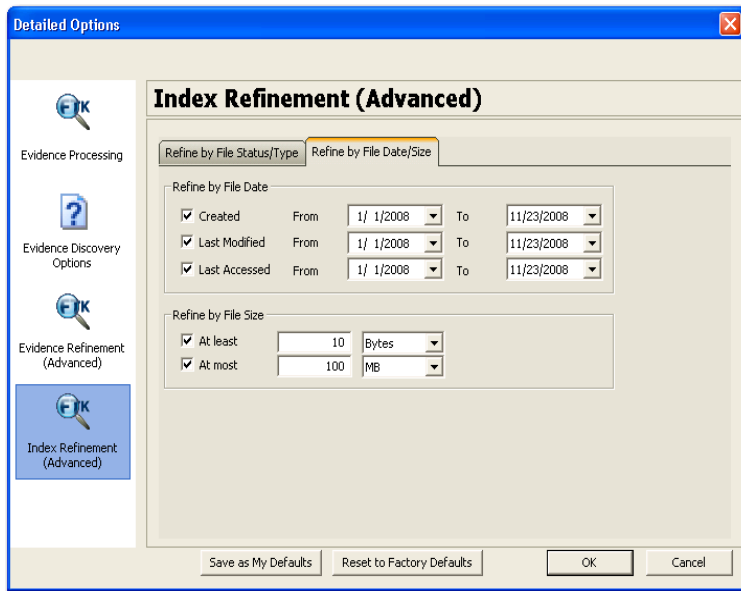
**TABLE 4-6 Refine Index by File Status/Type Options**

| Options   | Description  |
|---|--|
| Encrypted   | Specifies the way to treat encrypted files for cases where the scope of the warrant permits. 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 for cases where the scope of the warrant permits. Options are: <ul style="list-style-type: none"><li>• Ignore status</li><li>• Include only</li><li>• Exclude</li></ul>     |
| Include Duplicate Files                             | Mark to include duplicate files for analysis.  |
| Include OLE Streams                                 | Mark to include encrypted files for cases where the scope of the warrant permits.  |
| File Types  | Specifies types of files to include and exclude.   |
| Match using both File Type and File Status criteria | Applies both criteria to the refinement.   |

## REFINING AN INDEX BY FILE DATE/SIZE

Refine index items dependent on a date range or file size specified by the user as displayed in the following figure.

Figure 4-8 Index Refinement by File Date/Size



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

**TABLE 4-7 Refine Index by File Date/Size Options**

| Exclusion                 | Description   |
|---------------------------|---|
| Refine Index by File Date | To refine evidence 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> </ol> In the date fields, enter beginning and ending dates.   |
| Refine Index by File Size | To refine evidence by file size: <ol style="list-style-type: none"> <li>1. In the two size fields, enter minimum and maximum file sizes.</li> <li>2. 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 processing options needed for the current case, click *OK* > *OK* to begin case creation. FTK indicates that it is creating the case and asks you to please wait.

## ADDING EVIDENCE

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.

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. Complete the Manage Evidence dialog as indicated in the following table:

**TABLE 4-8**

| Option           | Description  |
|------------------|--|
| Display Name     | The filename of the evidence being added.  |
| Path             | The full pathname of the evidence file.  |
| ID/Name          | The optional ID/Name of the evidence being added.  |
| Description      | The optional 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> . |

**TABLE 4-8**

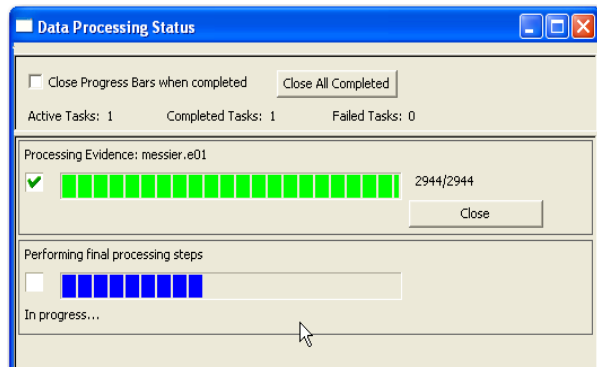
| Option             | Description  |
|--------------------|--|
| Case KFF Options   | Displays the KFF Admin dialog. Here you can view, create, edit, or delete Defined Groups and view, edit or delete Defined Sets. You can also choose to import or export groups or sets. Click done when you are finished using the KFF Admin dialog.   |
| Refinement Options | Displays the Refinement Options for Evidence Processing. This dialog has limited options compared to the Refinement Options selectable prior to case creation. For example, here you cannot choose Flag Duplicate Files, and you cannot create an HTML file listing. You cannot select Save as My Defaults, and you cannot Reset to Factory Defaults. Select the options to apply to the evidence being added, then click <i>OK</i> to close the dialog. |

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

## PROCESSING EVIDENCE

FTK shows a progress bar like the following figure.

*Figure 4-9 Data Processing Status Progress Bar*



**Note:** The count displayed in the progress bar is not equal to the number of items in the case.

## VIEWING PROCESSED ITEMS

It is not necessary to wait for the program to finish processing the case to start analyzing data. The metadata—the information about the evidence—can be viewed in

several modes before the evidence processing is complete. When processing completes you can view all the evidence from the various tabs.

## BACKING UP THE CASE

Backup your case from the Case Manager window.

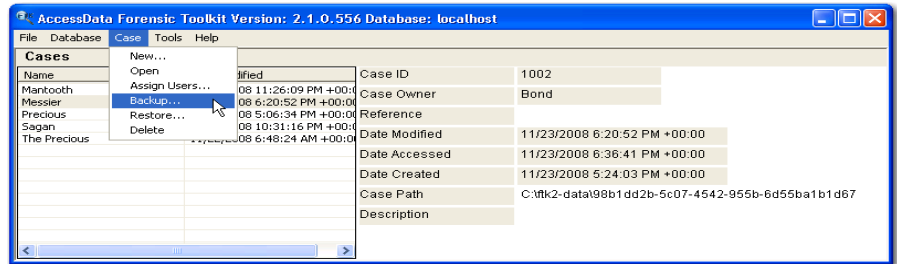
When backing up a case, FTK copies case information and database files (but not evidence) to a chosen folder. Keep copies of your drive images and other evidence independent of the backed-up case. Individual files and folders processed into the case are converted to an **.AD1** (custom content) image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

Case administrators backup cases and must maintain the library of backups against unauthorized restoration, because the user that 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 does the database plus the case folder.

To back up a case perform the following steps:

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



2. Select an archive folder location.
3. Click *Save*.

## RESTORING A CASE

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

To restore a case:

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

2. Browse to and select the archive folder to be restored.
3. Click OK.

## DELETING A CASE

To delete a case from the database:

1. In the Case Manager window, highlight the case to delete from the database.
2. Click *Case > 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 processors' speed by saving evidence files to a separate server. For more information, see Figure , "Choosing an Evidence Server," on page 20.

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.



## Chapter 5 Working with Cases

After creating a case in AccessData Forensic Toolkit (FTK) Case Manager, open the case. Investigate the case by bookmarking and exporting relevant files, verifying the drive image integrity, defining the evidence, and performing other tasks.

### OPENING AN EXISTING CASE

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

1. Log on to FTK2.1.
2. Double-click on the case you want to open, or highlight the case and click *Case > Open*.

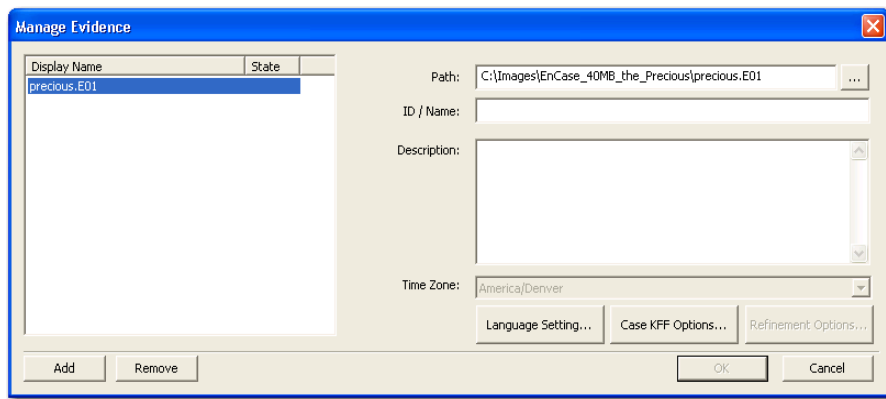
### ADDING EVIDENCE

After setting up a case, evidence must be added to it for processing. Additional evidence files and images can be added and processed later, if needed, as evidence in the case.

If a new case is being created, click *OK* on the New Case Options dialog to open the Manage Evidence dialog as represented in the following figure. If evidence is being added to an existing case, select *Evidence > Add/Remove* from the menu bar and continue as shown below.

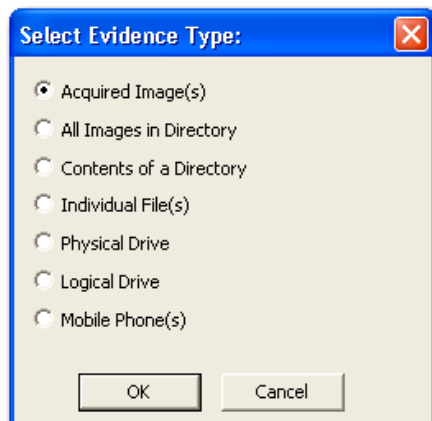
**Note:** Use universal naming convention (UNC) syntax in your evidence path for best results.

Figure 5-1 Managing Evidence



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


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

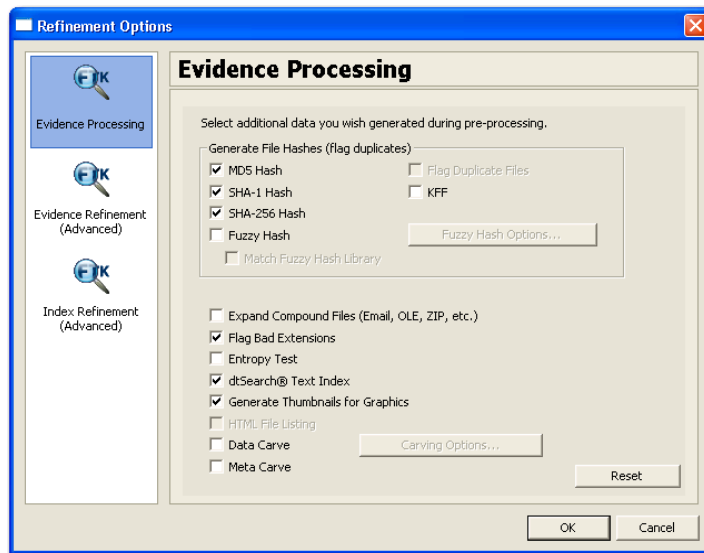


**Note:** Evidence taken from any physical source that is removable, whether it is a “live” drive or an image, will become inaccessible to the case if the drive letters change or the evidence-bearing source is moved. Instead create a disk image of this drive, save it locally, or to the drive you specified 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.

- 4a. (Optional) Click the ellipsis 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 a 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.



The sections available are:

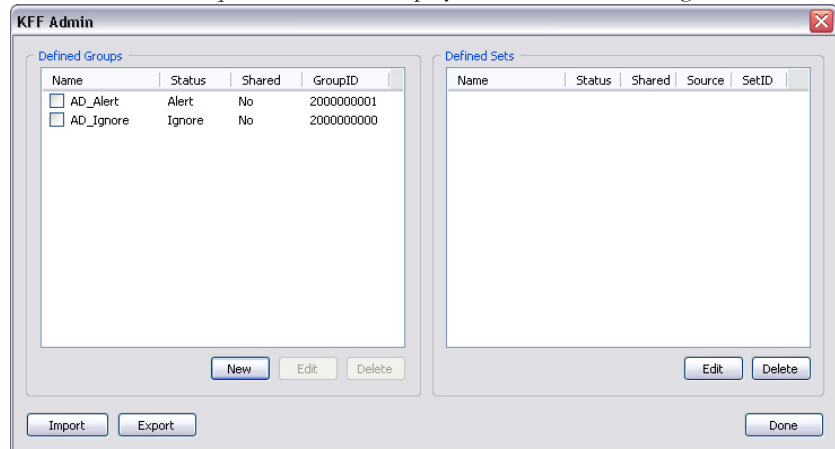
- Evidence Processing
- Evidence Refinement (Advanced)
- Index Refinement (Advanced)

For more information on Evidence Processing options, see “Selecting Evidence Processing Options” on page 74.

For more information on Evidence Refinement (Advanced) options, see “Selecting Evidence Refinement (Advanced) Options” on page 79.

For more information on Index Refinement (Advanced), see “Selecting Index Refinement (Advanced) Options” on page 83.

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.



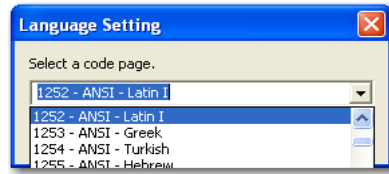
See “Using the Known File Filter” on page 156 for detailed information about the KFF.

11. Click *Done* to accept settings and return to the Manage Evidence dialog.
12. Click Language Settings to change the codepage for the language to view the evidence in.
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 5-2

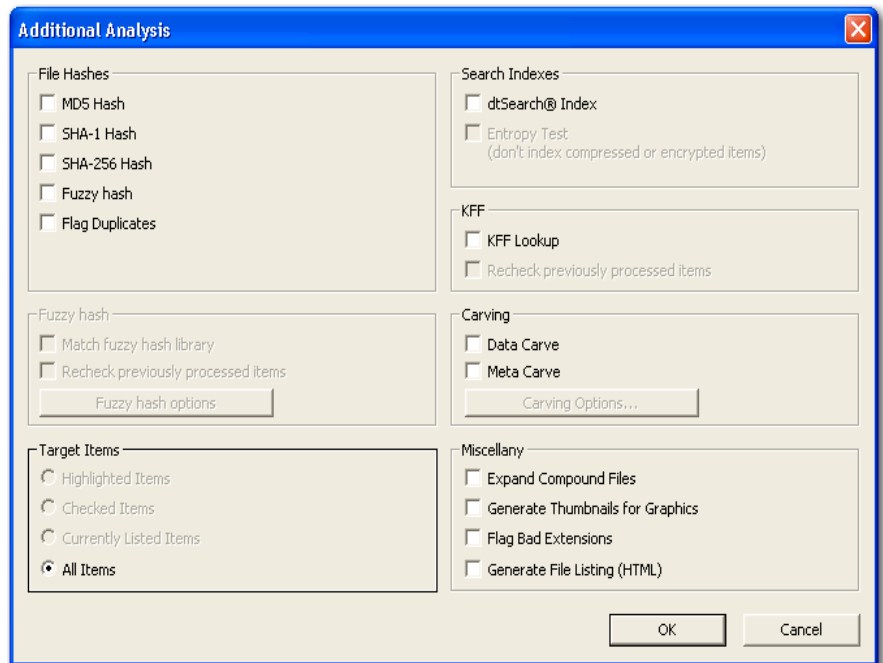


The Language Setting dialog appears, allowing you to select a code page from a drop-down list. When the setting is made, click **OK**.

## ADDITIONAL ANALYSIS

To further analyze selected evidence, click *Evidence > Additional Analysis*. The following figure represents the Additional Analysis dialog.

Figure 5-3 *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 5-1 Additional Analysis Options**

| Field        | Description  |
|--------------|--|
| File Hashes  | <p>These options create file hashes for the evidence.</p> <ul style="list-style-type: none"> <li>• MD5 Hash</li> <li>• SHA-1</li> <li>• SHA-256</li> <li>• Fuzzy Hash</li> <li>• Flag Duplicates</li> </ul> <p>Choosing one of these hash options 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. To flag the identified duplicate files select <i>Flag Duplicates</i>.</p> <p>Flag Duplicates is only available if selected during case creation.</p> <p>For more information about MD5 hashes, see “Message Digest 5” on page 293. For more information about SHA hashes, see “Secure Hash Algorithm” on page 295. For more information about Fuzzy Hashing, see, “Fuzzy Hashing” on page 120.</p> |
| Target Items | <p>Select the items on which to perform the additional analysis. Checked items will be unavailable if no items are 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 the evidence items in the File List pane when you selected Additional Analysis.</li> <li>• <b>All Items:</b> Performs the additional analysis on all evidence items in the case.</li> </ul> |

**TABLE 5-1 Additional Analysis Options**

| Field          | Description   |
|----------------|---|
| Search Indexes | <p>Choose <i>dtSearch® Index</i> to create a dtSearch index that allows index searches.</p> <p>Select <i>Entropy Test</i> to exclude compressed or encrypted items from the index.</p>  |
| KFF            | <p>Select <i>KFF Lookup</i> to filter targeted files in the KFF. When KFF is selected, the user can select to <i>Recheck previously processed items</i> when searching for new information.</p>   |
| Carving        | <p>Click <i>Carving Options</i>, to select the file types to carve.</p> <p>Select to either</p> <ul style="list-style-type: none"><li>• Data Carve</li><li>• Meta Carve</li></ul> <p>Carving uses file signatures to identify deleted files contained in the evidence.</p> <p>For further information on these selections see “Selecting Evidence Processing Options” on page 74.</p> <p>For more information on Data Carving, see “Data Carving” on page 149.</p>  |
| Miscellany     | <p>These miscellaneous options apply when performing the additional analysis:</p> <ul style="list-style-type: none"><li>• <b>Expand Compound Files:</b> Opens compound files such as ZIP and indexes the contained files.</li><li>• <b>Generate Thumbnails for Graphics:</b> Generates thumbnail graphics of the analyzed graphics.</li><li>• <b>Flag Bad Extensions:</b> Lists file extensions where the extension does not match the data type from the selected and analyzed files.</li><li>• <b>Generate File Listing (HTML):</b> Generates a list of processed files to an HTML file stored in C:\ftk2-data\caseID. This option is unavailable if this option was not selected during case generation..</li></ul> <p>For further information on using the EFS, see “Decrypting Files and Folders” on page 163.</p> |

## FILE CONTENT, PROPERTIES, AND HEX INTERPRETER TABS

The File Content, Properties, and Hex Interpreter tabbed panes default to the bottom left of the File Content pane in any tab where it is used. Click any of these tabs to switch

between them. The information displayed applies to the currently selected file in the File List pane.

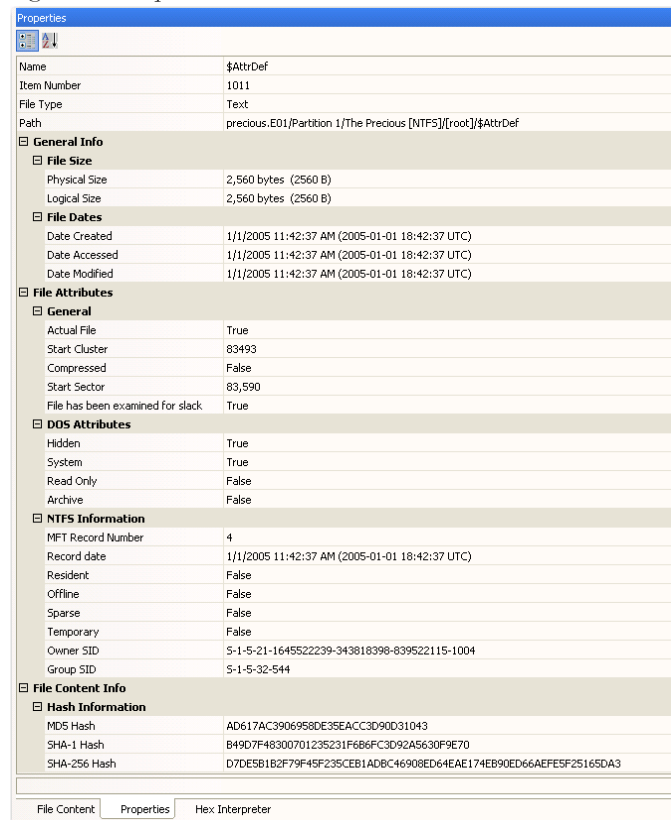
## PROPERTIES TAB

The Properties pane is organized into the following sections:

- General Info
- File Attributes
- File Content Info

The following figure shows the File Properties pane:

*Figure 5-4 Properties Tab Pane*





## PROPERTIES INFO

The Properties pane contains the following file information:

**TABLE 5-2 Properties File Information**

| Property    | Description   |
|-------------|---|
| Name        | The name of the file.   |
| Item Number | The unique number assigned to the item.   |
| File Type   | The file type, such as an HTML file or a Microsoft Word 98 document.<br>FTK uses the file header to identify each item's file type. |

## GENERAL INFO

The General Info section displays the following information:

**TABLE 5-3 Properties General Information**

| Property          | Description   |
|-------------------|---|
| <b>File Size</b>  |   |
| Physical Size     | The physical file size. This value includes file slack.             |
| Logical Size      | The logical file size. This value excludes file slack.              |
| <b>File Dates</b> |   |
| Date Created      | The date that the file was created, shown in UTC time format.       |
| Date Accessed     | The date that the file was last accessed, shown in UTC time format. |
| Date Modified     | The date that the file was last modified, shown in UTC time format. |

# FILE ATTRIBUTES

This section lists the characteristics of the item selected in the File List pane. The attributes correspond with the columns in the File List pane, but are not editable. The following table provides more detail:

**TABLE 5-4 General File Attributes**

| Property                          | Description  |
|-----------------------------------|--|
| Actual                            | True if an actual file. False if derived from an actual file.  |
| Start Cluster                     | The start cluster of the file on the disk.                     |
| Compressed                        | True if compressed. False otherwise.                           |
| Start Sector                      | The start sector of the file on the disk.                      |
| File has been examined for slack. | True if the file has been examined for slack. False otherwise. |

**TABLE 5-5 DOS File Attributes**

| Property  | Description  |
|-----------|--|
| Hidden    | True if Hidden attribute was set on file. False otherwise.   |
| System    | True if file is a DOS system file. False Otherwise           |
| Read Only | True if Read Only attribute was set on file. False otherwise |
| Archive   | True if Archive bit was set on file. False otherwise         |

**TABLE 5-6 NTFS File Attributes**

| Property          | Description  |
|-------------------|--|
| MFT Record Number | Number of the file in the MFT record.  |
| Record Date       | UTC date and time record was created.  |
| Resident          | 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.) |

**TABLE 5-6 NTFS File Attributes**

| Property  | Description  |
|-----------|--|
| Offline   | True or False value  |
| Sparse    | True or False value  |
| Temporary | True if the item was a temporary file. False otherwise.  |
| Owner SID | The Windows-assigned security identifier of the owner of the object.                           |
| Group SID | The Windows-assigned security identifier of the group that the owner of the object belongs to. |

## FILE CONTENT INFO

The File Content Info section displays the following information:

**TABLE 5-7 File Content Information**

| Property     | Description   |
|--------------|---|
| KFF Status   | Indicates if the file is identified by the KFF as an illicit or contraband file, or ignorable file. |
| MD5 Hash     | The MD5 (16 bytes) hash of the file (default).  |
| SHA-1 Hash   | The SHA-1 (20 bytes) hash of the file (default).  |
| SHA-256 Hash | The SHA-256 (32 bytes) hash of the file (default).  |

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.

## THE HEX INTERPRETER TAB

The Hex Value Interpreter tab converts hexadecimal values selected in the File Content View from the Hex tab into decimal integers and possible time and date values, as well as Unicode strings. This feature is most useful if you are familiar with the internal code structure of different file types and know where to look for specific data patterns or time and date information.

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

1. Switch the File Content pane to Hex view.
2. Select one to eight (more with the Unicode string) couplets.

| Hex Interpreter     |      |                         | File Content |  |
|---------------------|------|-------------------------|--------------|--|
| Type                | Size | Value                   | Hex          | Text   |
| signed integer      | 1-8  | 127 490 785 577 812 500 | 000080       | 46 49 4c 45 30 00 03 00-e3 0f 10 00 00 00 00 00 FILE0...ä.....       |
| unsigned integer    | 1-8  | 127 490 785 577 812 500 | 000010       | 02 00 01 00 38 00 01 00-58 01 00 00 04 00 00 00 .....8...X.....      |
| FILETIME (Stored)   | 8    | 1/1/2005 6:42:37 PM     | 000020       | 00 00 00 00 00 00 00 00-04 00 00 02 00 00 00 .....0.....             |
| FILETIME (As Local) | 8    | 1/1/2005 12:42:37 PM    | 000030       | 0e 00 00 00 00 00 00 00-10 00 00 60 00 00 00 .....0.....             |
| DOS date            | 2    | -                       | 000040       | 00 03 18 00 00 00 00 00-48 00 00 18 00 00 00 .....0.....             |
| DOS time            | 2    | -                       | 000050       | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....0.....             |
| DOS date/time       | 4    | -                       | 000060       | 14 42 80 aa 31 f0 c4 01-14 42 80 aa 31 f0 c4 01 B*1A&...B*1A&...     |
| time_t (Stored)     | 4    | -                       | 000070       | 05 00 00 00 00 00 00 00-00 00 00 00 00 00 00 .....0.....             |
| time_t (As Local)   | 4    | -                       | 000080       | 00 00 00 00 00 00 01 00-00 00 00 00 00 00 00 .....0.....             |
| Unicode string      | 2+   | ■                       | 000090       | 00 00 00 00 00 00 00 00-00 30 00 00 00 00 00 .....0...p.....         |
|                     |      |                         | 0000a0       | 00 00 18 00 00 00 00 00-02 52 00 00 18 00 01 00 .....R.....          |
|                     |      |                         | 0000b0       | 05 00 00 00 00 00 05 00-14 42 80 aa 31 f0 c4 01 B*1A&...B*1A&...     |
|                     |      |                         | 0000c0       | 14 42 80 aa 31 f0 c4 01-14 42 80 aa 31 f0 c4 01 B*1A&...B*1A&...     |
|                     |      |                         | 0000d0       | 14 42 80 aa 31 f0 c4 01-00 20 00 00 00 00 00 00 B*1A&...B*1A&...     |
|                     |      |                         | 0000e0       | 00 00 20 00 00 00 00 00-06 00 00 00 00 00 00 .....0.....             |
|                     |      |                         | 0000f0       | 08 23 24 00 4c 00 6f 00-67 00 46 00 69 00 6c 00 ...&L&g&F&1&...      |
|                     |      |                         | 000090       | 65 00 00 00 00 00 00 00-80 00 00 00 48 00 00 00 .....e.....H.....    |
|                     |      |                         | 000010       | 01 00 40 00 00 00 01 00-00 00 00 00 00 00 00 .....0.....             |
|                     |      |                         | 000020       | ff 0f 00 00 00 00 00 00-40 00 00 00 00 00 00 .....y.....0.....       |
|                     |      |                         | 000030       | 00 00 20 00 00 00 00 00-20 00 00 00 00 00 00 .....0.....             |
|                     |      |                         | 000040       | 00 00 00 00 00 00 00 00-32 00 10 25 36 01 00 00 .....0.....2&6.....  |
|                     |      |                         | 000050       | ff ff ff ff 00 00 00 00-15 00 00 00 3f ad 14 62 yyyyyy.....?~b...    |
|                     |      |                         | 000060       | 9e 40 7e 14 43 17 0a 32-ec 03 00 00 01 02 00 00 ...&C&-21.....?~b... |
|                     |      |                         | 000070       | 00 00 00 05 20 00 00 00-20 02 00 00 00 00 00 00 .....0.....          |
|                     |      |                         | 000080       | 80 00 00 00 48 00 00 00-01 00 40 00 00 00 01 00 .....H...0.....      |
|                     |      |                         | 000090       | 00 00 00 00 00 00 00 00-ff 0f 00 00 00 00 00 00 .....y.....          |
|                     |      |                         | 0000a0       | 40 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....8.....          |
|                     |      |                         | 0000b0       | 00 00 20 00 00 00 00 00-20 00 00 00 00 00 00 00 .....0.....          |
|                     |      |                         | 0000c0       | 32 00 10 25 36 01 00 00-ff ff ff ff 00 00 00 00 ...2&6...yyyyy...    |
|                     |      |                         | 0000d0       | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....0.....          |
|                     |      |                         | 0000e0       | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....0.....          |
|                     |      |                         | 0000f0       | 00 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 .....0.....          |

The following table lists the available options and their descriptions:

|                  |                                 |
|------------------|---------------------------------|
| • 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 |

4. 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.

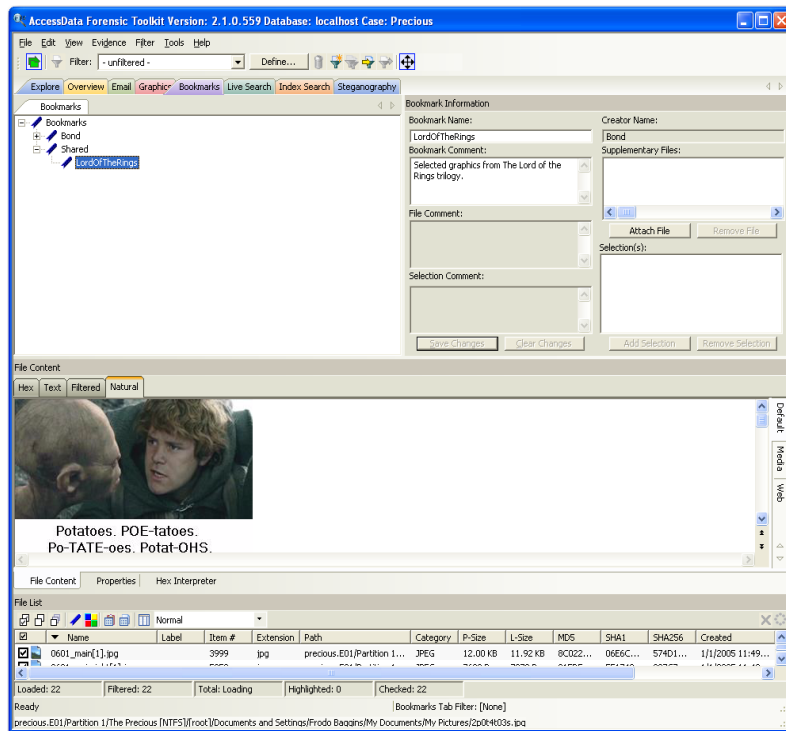


## USING THE BOOKMARK INFORMATION PANE

A bookmark contains a group of files that you want to reference in your case. These are selected 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 drive images. The bookmark information pane is highlighted in the following figure.

Figure 5-5 Bookmark Information Pane

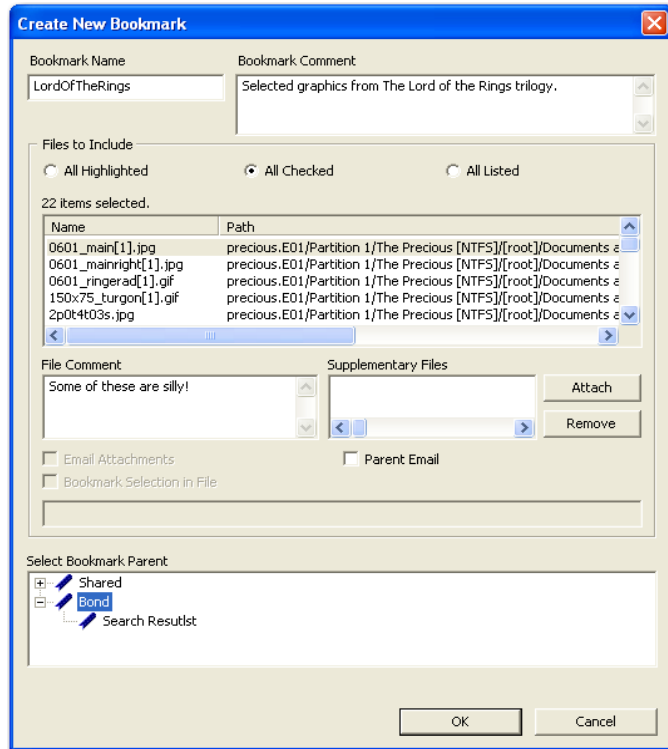


The Bookmarks tab lists all bookmarks that have been created in the current case

## CREATING A BOOKMARK

Files can be bookmarked from any tab in FTK. To create a bookmark 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 with the older bookmark as the parent.
9. Click *OK*.

## 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 display in the Bookmark Information pane.

The Bookmark Information pane contains these fields:

**TABLE 5-9 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.   |
| 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. |
| Creator Name        | The FTK2 user who created the bookmark.  |
| Supplementary Files | Displays a list of external, supplementary files associated with the bookmark.   |



**TABLE 5-9 Bookmark Information Pane Information**

| Field             | Description   |
|-------------------|---|
| 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.  |
| Attach File       | 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.   |
| Remove File       | Removes a selected supplementary file from the bookmark.  |
| Selection(s)      | Displays a list of stored selections within the selected file.  |
| Add Selection     | 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.                                     |
| Remove Selection  | Remove the highlighted selection from the Selections list.  |
| Selection Comment | 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. |
| Save Changes      | Stores the changes made to the bookmark information.  |
| Clear Changes     | Clears any unsaved changes made to the bookmark information.  |

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.

## BOOKMARKING SELECTED TEXT

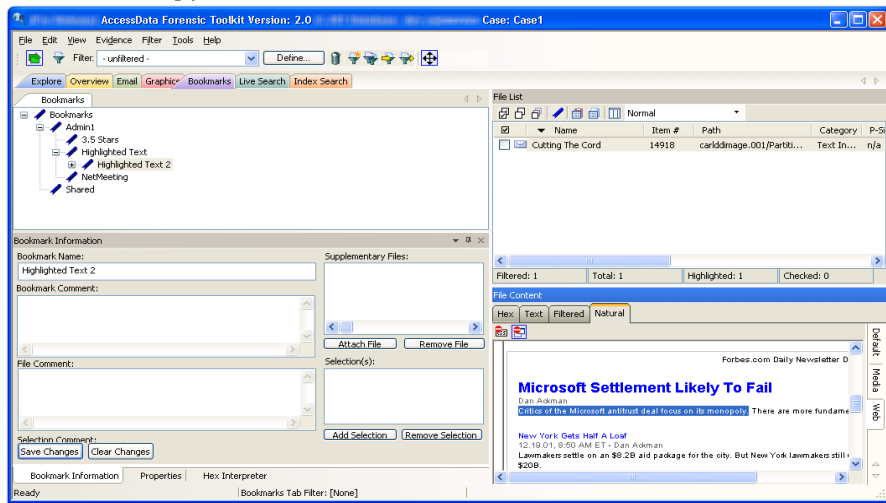
Bookmarked selections are independent of the view in which they were made. Select hex data in the Hex view of a bookmarked file and save it; bookmark different text in the Filtered view of the same file and save that selection as well.

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*.



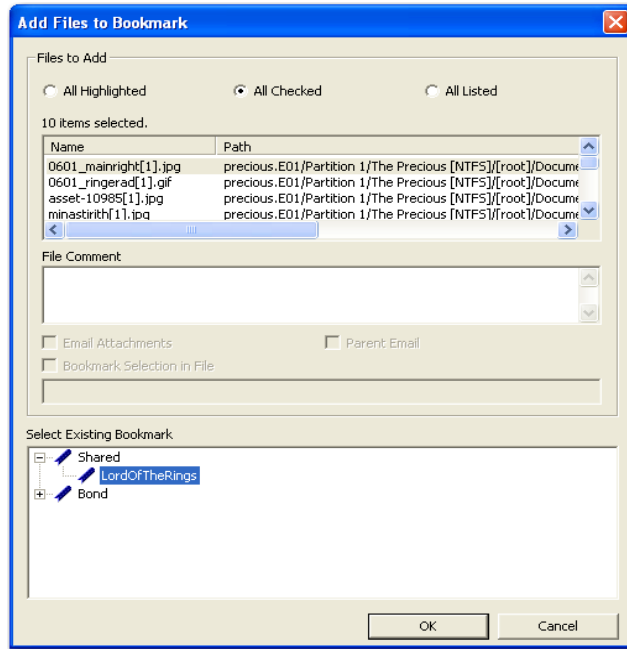
The selection remains in the bookmark.

## ADDING EVIDENCE TO AN EXISTING BOOKMARK

Sometimes additional evidence is desired in a bookmark. To add the evidence, follow these steps:

1. Right-click the new file.

2. Click *Add to Bookmark*.



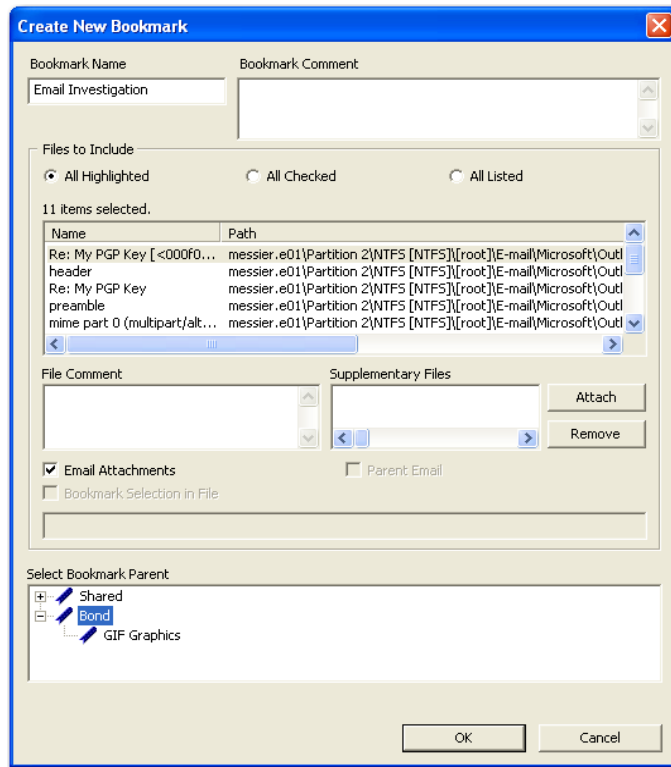
3. Select the parent bookmark.
4. Select the child bookmark to add the file to.
5. Click *OK*.

## 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.

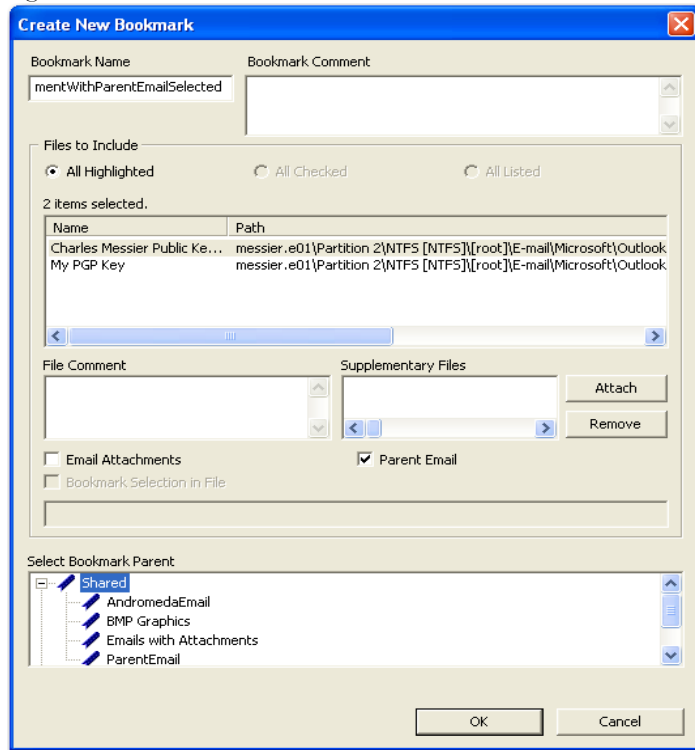
To create a bookmark for an email, follow the steps for creating a bookmark. Select the email to include in the bookmark. Right-click and choose *Create Bookmark*. Note that the Email Attachments box is active, but unmarked. If only the parent email is needed the Email Attachments box can remain unselected.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

Figure 5-6 Create New Bookmark with Email Attachments



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 104.) Note that the Parent Email box is automatically active, allowing you to include the parent email. If the Parent Email box is checked, 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.

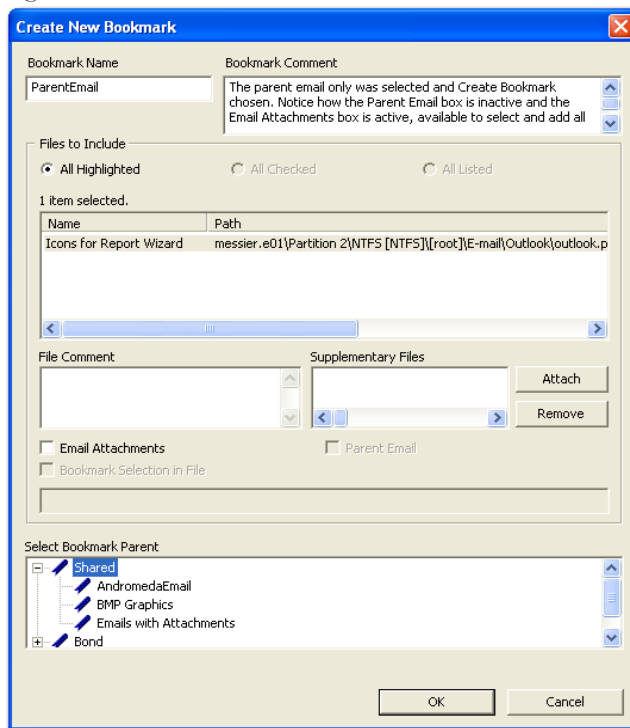
Figure 5-7 Create New Bookmark with Parent Email Selected



## ADDING EMAIL AND EMAIL ATTACHMENTS TO BOOKMARKS

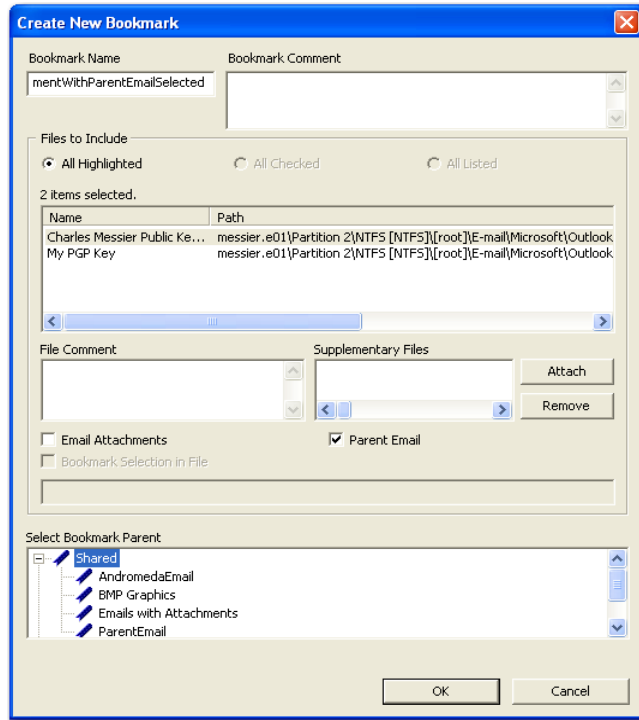
To add an email to a bookmark, select the email to add, then right-click on the email and choose Add To Bookmark. (For more information see, “Adding Evidence to an Existing Bookmark” on page 108). Note that the Email Attachments box is active, but not marked. If only the parent email is needed the Email 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 5-8 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 Evidence to an Existing Bookmark” on page 108.) 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 5-9 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 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.

## REMOVING A BOOKMARK

Use the following steps to remove a bookmark:

1. In the Bookmark tab, expand the bookmark list and highlight the bookmark to be removed.
2. Press the *Delete* key.

# DELETING FILES FROM A BOOKMARK

Use the following steps to delete files from bookmarks:

- 1. Right-click the file in the Bookmark File List.
- 2. Select *Remove from Bookmark*.

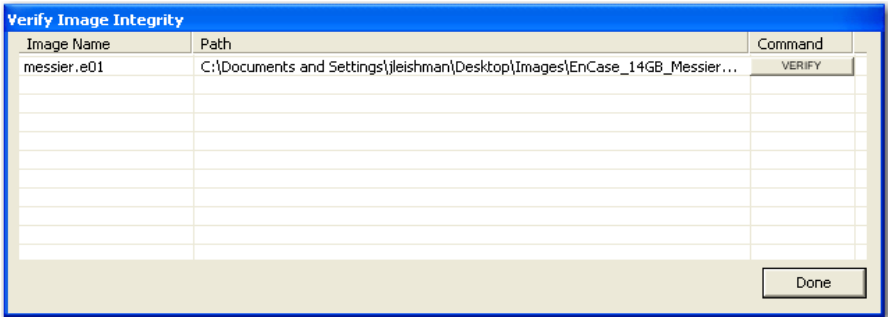
# VERIFYING DRIVE IMAGE INTEGRITY

A drive image can be altered or corrupted due to bad media, bad connectivity during image creation, or by deliberate tampering. To validate the integrity of your case evidence, FTK allows you to determine if a drive image has changed from the original evidence drive, or the original image. This feature works with file types that store the hash within the drive image itself, such as EnCase\* and SMART\* images.

To verify a drive image’s integrity, FTK generates a hash of the current file and compares 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.



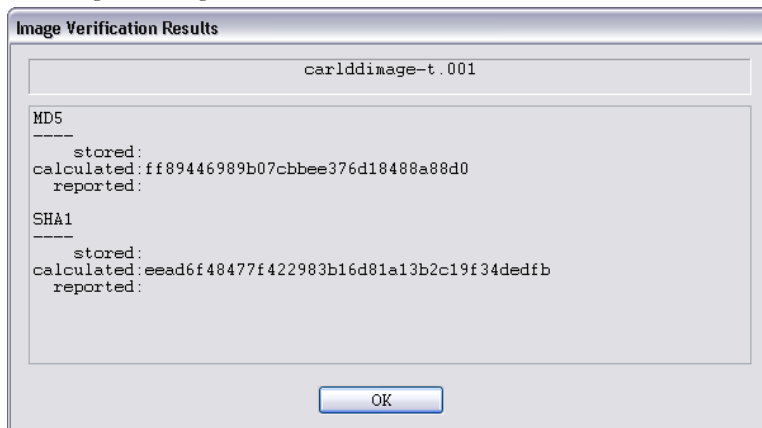
In case the image file does not contain a stored hash, FTK can calculate one. The Verify Image Integrity dialog provides the following information:

**TABLE 5-10** Verify Image Integrity

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

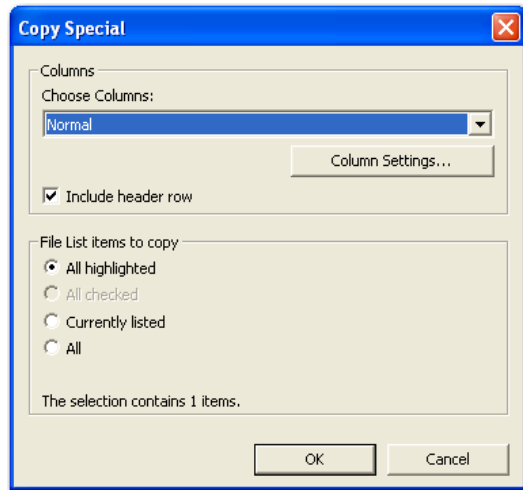
## COPYING INFORMATION FROM FTK

The Copy Special dialog allows you to copy information about the files in your case to the clipboard. The file information can include any column item, 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 following:

**TABLE 5-11 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. Items remain highlighted only as long as the same tab is displayed.                     |
| All Checked        | All items checked in all file lists. The user can check files in multiple lists. Checked items remain checked until user unchecks them. |
| Currently Listed   | All items in the current file list.   |
| All                | All items in the case.  |

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.

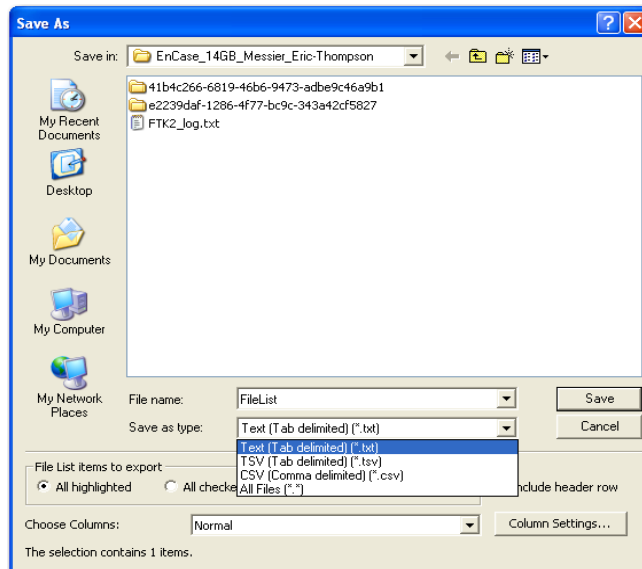
For more information about Column Settings, see “Creating and Modifying Column Settings” on page 198.

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

## 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 .tsv files that displayed in a text editor program like Notepad\*. Files saved in .tsv or .csv display in the default spreadsheet program.

Figure 5-10 Export File List Info Dialog



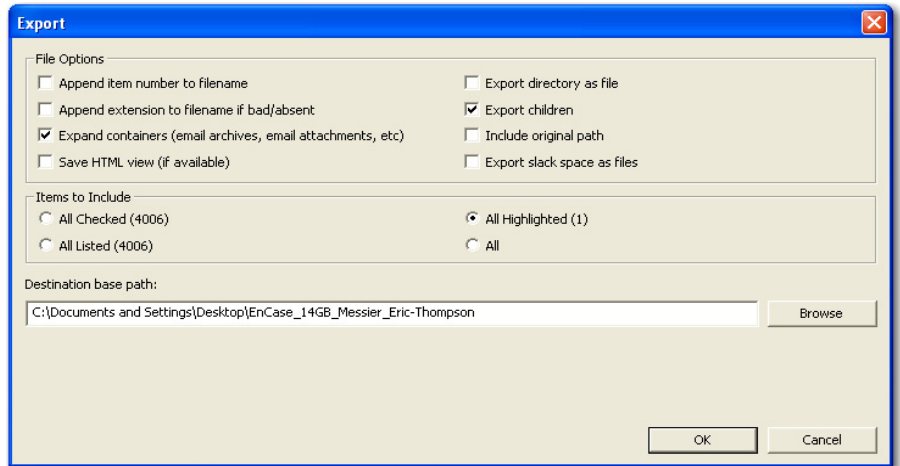
Select the Save As options, *All Highlighted*, *All Checked*, *All Listed*, or *All*, and choose whether to include a Header Row for the exported file. Select the file type for the exported data. The default filename is *FileList*; change it if you choose. The location for the file is the case folder. Choose the data set to use from the *Choose Columns* drop-

down, or click *Column Settings* to define your own columns template. For information on Copy Special, see “Copying Information from FTK” on page 115.

## EXPORTING FILES

FTK allows the export of files used in the investigation. Files can be exported for additional processing or 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 or Registry Viewer can read files within a drive image.) The following figure represents the Export Files dialog.

Figure 5-11 *Export Files Dialog*



**Note:** Bookmarked files and graphics can be automatically exported with reports. For more information about exporting files with a report, see “Creating a Bookmark” on page 104.

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 5-12**

| 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.  |
| Save HTML view (if available)                               | If a file can be exported and saved in HTML format, it will be done.                              |
| 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..

**TABLE 5-13 Export Files Selection Options**

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

Each item displays its filename and path.

4. In the Destination Path field, browse to and select the export the file location.  
The default path is **C:\case\_folder\Report\Export\**.
5. Click **OK** to begin the export.

## EXPORTING FILE LIST INFO

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
3. Choose whether to include a header row in the exported file
4. Select column information
5. Specify the filename for the exported information.
6. Browse to and select the destination folder for the exported file.
7. Click *Save*.

## EXPORTING THE WORD LIST

The contents of the case index can be exported to use as the basis for a custom dictionary in the password recovery process. 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 file and location to which you want to write the word list.

The default filename is **Ftk2WordList.txt**. If you intend to use the wordlist as the basis for a custom dictionary in DNA or PRTK, it is a good idea to name the wordlist by the casename. For example, FTK2PreciousWordList.txt

3. Click *Save*.

## 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 sequence of data between the two files.

Traditional forensic hashes (MD5, SHA1, SHA256, 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.

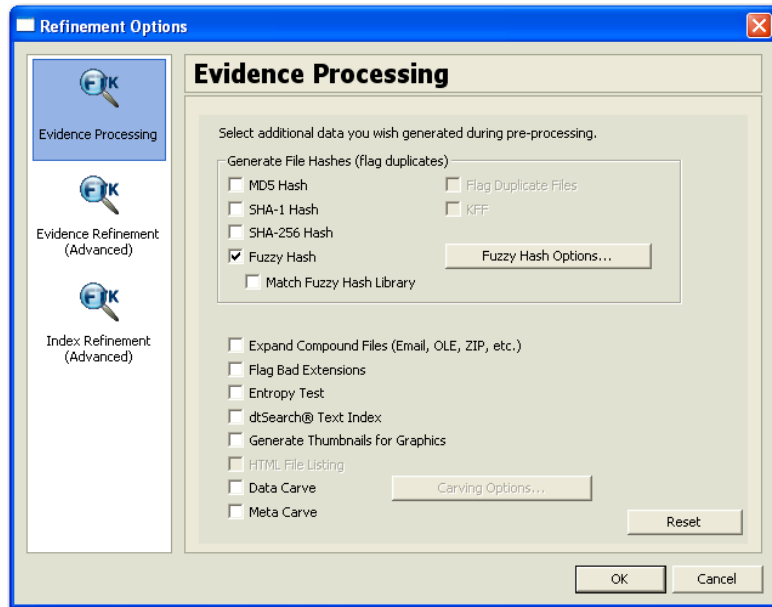
## CREATING A FUZZY HASH LIBRARY

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 get to the Fuzzy Hash Library screen go to *Tools>Fuzzy Hash>Manage Library*.

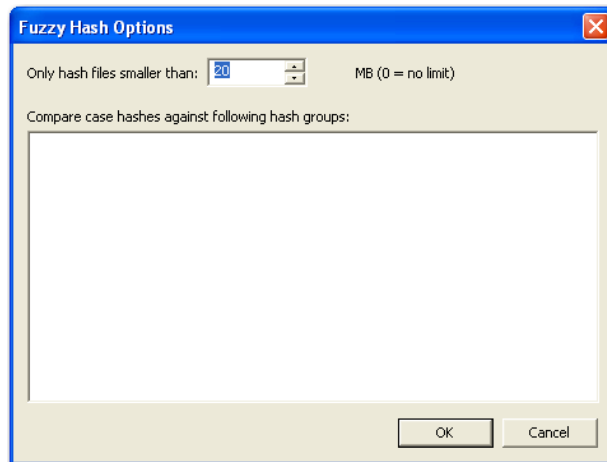
## SELECTING FUZZY HASH OPTIONS DURING INITIAL PROCESSING

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.



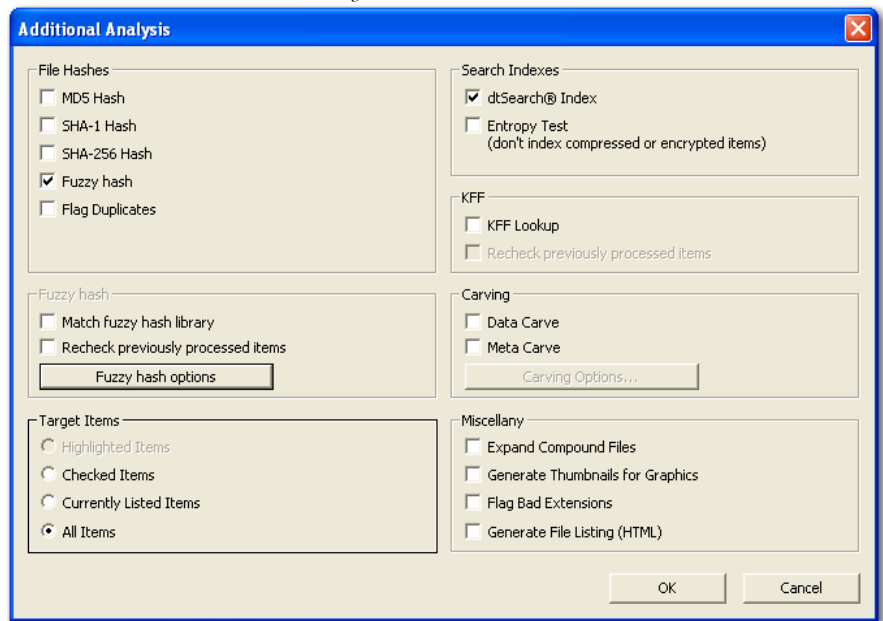


- 2c. Set the size of files to hash. The size defaults to 20 MB, 0 indicates no limit.
- 2d. Click *OK* to set the value.
3. Select *OK* to close the detailed options dialog.

## ADDITIONAL ANALYSIS FUZZY HASHING

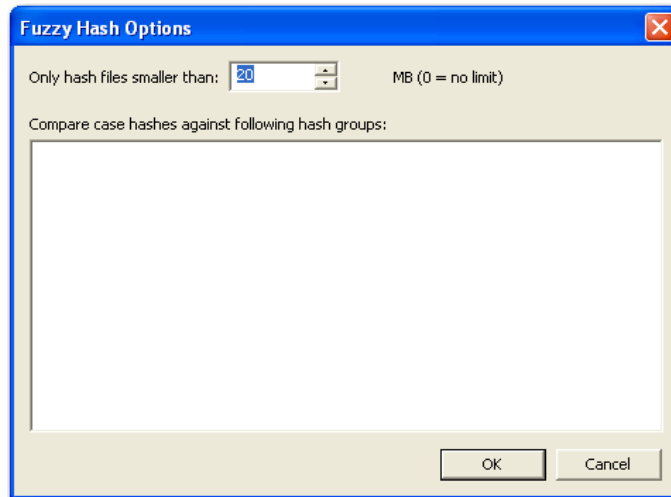
Fuzzy hashing can also be initialized on the current data by the following steps:

1. Click *Evidence > Additional Analysis*.



2. Select *Fuzzy Hash*.
  - 2a. (Optional) Select if the evidence needs to matched against the fuzzy hash library.
  - 2b. (Optional) If performing this additional analysis after adding new information, the fuzzy hashing can be done again against previously processed items.

2c. (Optional) Click *Fuzzy Hash Options* to open the Fuzzy Hash Options dialog.



2d. Set the file size limit on the files to be hashed.

2e. Click *OK*.

3. 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 5-14 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, 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                | is the actual fuzzy hash value given to a file.   |
| 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.  |



## Chapter 6 Searching a Case

Searching evidence for information pertaining to a case can be one of the most crucial steps in the examination. AccessData Forensic Toolkit (FTK) provides three different live search modes: hexadecimal, pattern (or “regular expression”), and text. Search results, or “hits,” appear highlighted in the File Content view.

### CONDUCTING A LIVE SEARCH

The live search is a time-consuming process involving an item-by-item comparison with the search term. A live search is flexible because it can find patterns of non-alphanumeric characters.

Live search also supports pattern searches. Pattern searches, also called regular expression searches, are searches for mathematical 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. For more information about regular expressions and syntax, see “Conducting a Pattern Search” on page 130.

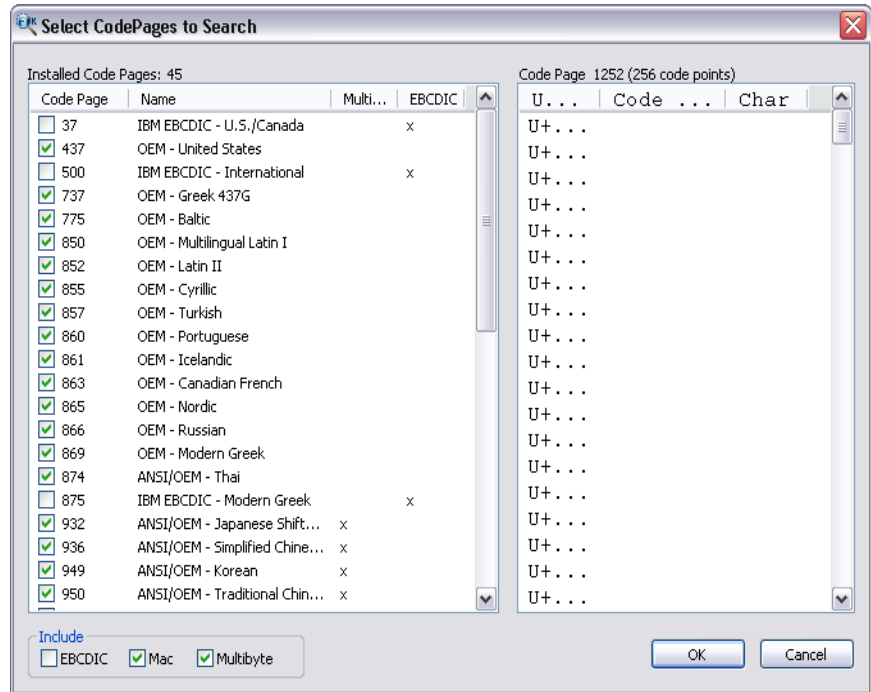
AccessData recommends live searching for items an index search cannot find.

To perform a live search do the following steps:

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 Unicode is selected, you To include sets other than ANSI and Unicode, check *Other Code Pages*, then click *Select*.

**Note:** You must select at least one of the CodePage choices. If you try to unselect all of the choices on the CodePage selection bar, the next available option is automatically marked.



2. Click to select the needed sets.
3. Click to include EBCDIC, Mac, and Multibyte as needed.
4. Click *OK* to close the dialog.
5. Click to mark Case Sensitive if you want to search specifically uppercase or lowercase letters. FTK 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 search terms.
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.
10. (Optional) Apply a filter from the drop-down list. Applying a filter speeds searching by eliminating items that do not match the filter.
11. Click *Search*.

**Note:** Click *Cancel* in the Data Processing Status dialog to halt the search.

12. Select the results to see 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.

Right-click on a search result in the Live Search Results pane to display more options. The available right-click options are as follows:

**TABLE 6-1 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></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 fine 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.  |

**Important:** Searching before 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.

## CUSTOMIZING THE LIVE SEARCH TAB

Change the order of the Live Search tabs by dragging and dropping them into the desired order. The following figure shows the live search tabs.

Figure 6-1 Live Search Tabs



For more information on customizing the FTK user interface, see “Customizing the Interface” on page 191.

## CONDUCTING A PATTERN SEARCH

Pattern searching, also known as regular expression searching, allows forensics analysts to search through large quantities of text information for repeating formats of data such as:

- Telephone Numbers
- Social Security Numbers
- Computer IP Addresses
- Credit Card Numbers

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 6-2 Mathematical Components of Arithmetic Expressions**

| Component       | Example             |
|-----------------|---------------------|
| Operands        | 5, 1, 2, 3          |
| Operators       | /, (), +, *         |
| Sub-Expressions | (1+2), ((1+2)*3)    |
| Value           | Approximately 0.556 |

**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 symbolic 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 6-3 Visa and MasterCard Regular Expressions**

| Component       | Example   |
|-----------------|---|
| 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 (`()`) group 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 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 back slash 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 the following predefined regular expressions to be used in pattern searches, such as items on the following list:

- U.S. Social Security Numbers
- U.S. Phone Numbers
- U.K. Phone Numbers
- IP Addresses
- Visa and MasterCard Numbers

Select regular expressions from drop-down lists under the arrows:


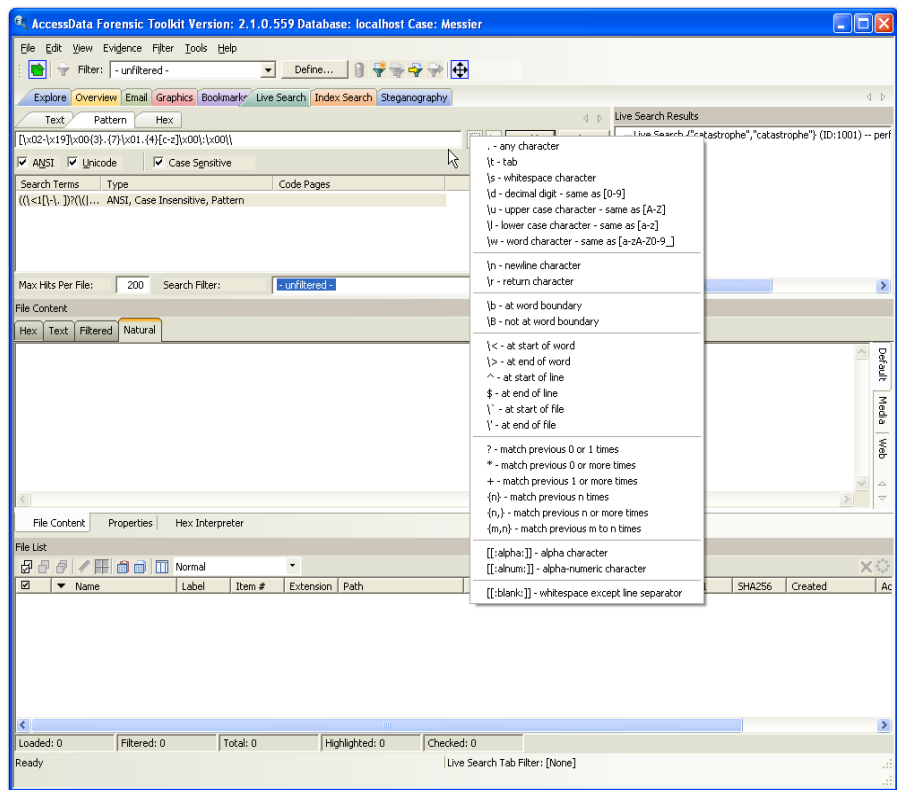
- Click the black arrow  to see a list, as displayed in the following figure, of the basic components for regular expressions. You can create your own pattern by combing these components into a longer expression.

Figure 6-2 Regular Expressions Components




- Click the white arrow  to see a list of predefined expressions, as displayed in the following table:

TABLE 6-4 Predefined Pattern Searches

|             |                              |
|-------------|------------------------------|
| MAC Address | URL {http, https, ftp, ftps} |
| Mailto:     | ... .com                     |
| ... .edu    | ... .info                    |
| ... .net    | ... .org                     |
| ... .gov    | ... .museum                  |

**TABLE 6-4 Predefined Pattern Searches**

---

|   |  |
|---|--|
| ... .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)             |
| 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 | THTML Search Engine - Ask Jeeves                           |
| Orphaned Index.dat Files (with date)                            | Orphaned Index.dat Files (Without Date)                    |
| Orphaned Histore 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. The U.S. Phone Number expression finds telephone numbers with or without area codes.

This expression also indicates that if an area code is present, a number one (1) may or may not precede the area code. This meaning is achieved through the sub-expression `(\<1[\-\. ])?`, which says that if there is a “1” before the area code, it will follow a non-word character and be separated from the area code by a delimiter (period, hyphen, or spacebar space).

The next sub-expression, `(\(|\<)\d\d\d[\)\.\/ ] ?`, specifies how the area code must appear in any search hits. The `(\(|\<)` requires that the area code begin with a left parenthesis or other delimiter. 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 in FTK. You can modify the default expressions to fine-tune your data searches or to create your own expressions.

# COMMON OPERATORS

The following is a list of common operators:

**TABLE 6-5 Common Regular Expressions Operators**

| Operators | 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.”<br><br>A hyphen (-) specifies ranges of characters with the brackets. For example, “ab[0-3]” will find “ab0,” “ab1,” “ab2,” and “ab3.” You can also specify case specific ranges such as [a-r], or [B-M]. |
| ‘         | (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 decimal digit.   |
| \l        | Matches any lowercase letter.  |
| \n        | Matches a new line.  |
| \r        | Matches a return.  |
| \s        | Matches any white space 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].   |



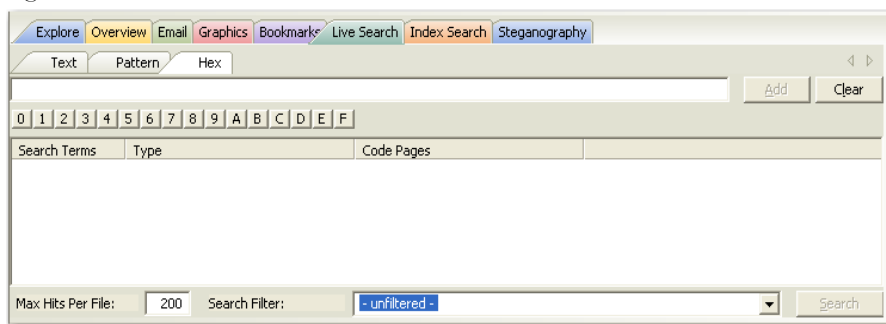
**TABLE 6-5 Common Regular Expressions Operators**

| Operators              | 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, or by clicking the Hexadecimal character buttons provided, as displayed in the following figure.

*Figure 6-3 Hex Search Tab*

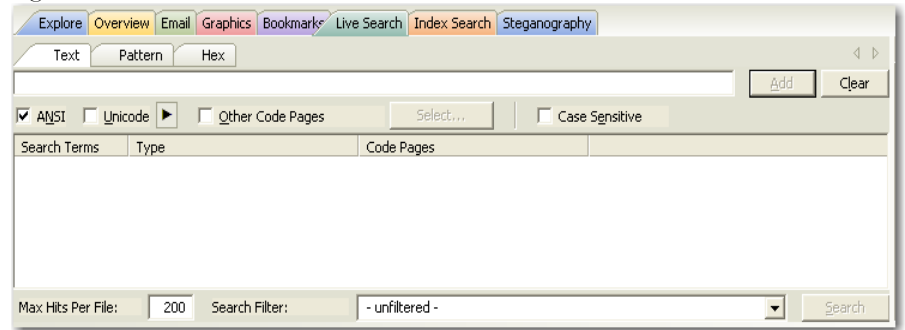


The instructions for conducting a live search on the hex tab are similar to conducting searches on the Pattern tab. For more information on conducting a Pattern search, see the beginning of this section, “Conducting a Pattern Search” on page 130.

## 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. Also, there are no arrows to click for operand selection as displayed in the following graphic.

Figure 6-4 Live Search: Text Search Tab



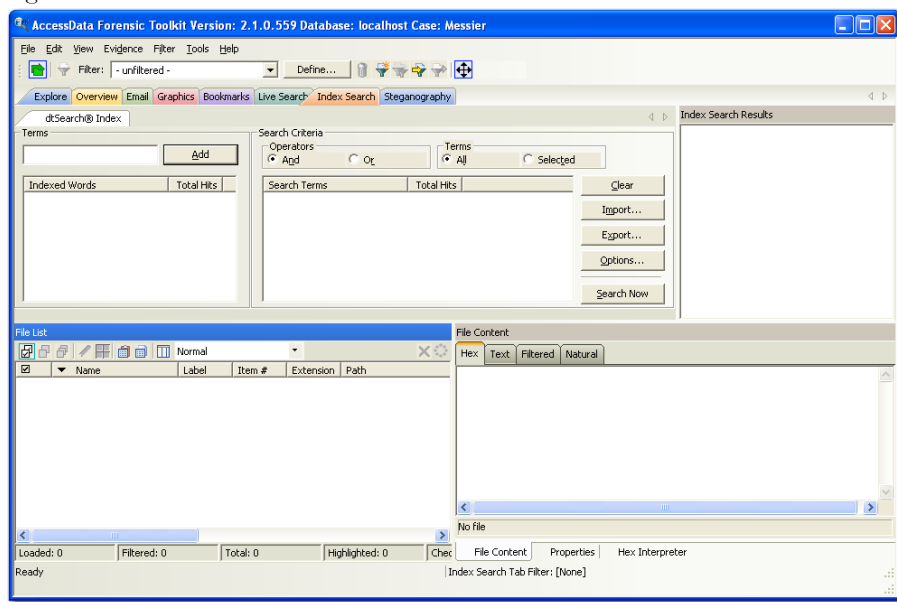
Otherwise apply the instructions for the pattern search to this search. For more information on conducting a pattern search see “Conducting a Pattern Search” on page 130.

## CONDUCTING AN INDEX SEARCH

The index search uses index files to find the search term. Evidence items may be indexed when they are first added to the case or at a later time. AccessData recommends always indexing a case before beginning analysis.

For more information about indexing an evidence item, see “Indexing a Case” on page 77. The following figure displays the FTK window with the Index Search tab selected.

Figure 6-5 Index Search Tab



The index files contain all discrete words or number strings found in both the allocated and unallocated space in the case evidence. FTK2 does not index spaces or symbols, including the following:

. , ; ; " ' ~ ! # \$ % ^ & = + .

In addition to performing searches within the case, you can also use the index as a dictionary for password recovery processes in the Password Recovery Toolkit (PRTK). You can export the index by selecting *File > Export Word List*.

## SEARCH TERMS

Type the term or its dialog 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 to the Search Terms list, or double-click a term from 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 indexed search by selecting specific entries, or by searching against all entries. Click *Clear* to clear these search criteria. If any items are selected, clicking *Clear* will clear the selected item(s) only. If no items, or all items, are selected, clicking *Clear* will clear all items from the list.

**Important:** When creating your search criteria, try to focus your search to bring up the smallest number of meaningful hits per search.

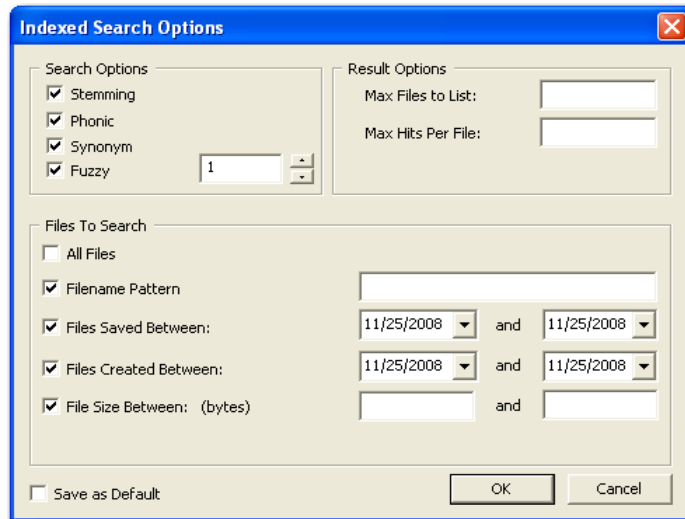
Click *Export* to save a set of search terms, then save the file.

Click *Import* to apply a set of search terms then select the file you previously saved.

## INDEX SEARCH OPTIONS

To conduct an index search, select the *Options* button to refine the search by opening the Indexed Search Options dialog, as in the following figure.

Figure 6-6 *Index Search Options Dialog*



The following tables review the individual search and result options:

**TABLE 6-6 Individual Search and Result 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> .<br><br>Click the arrows to increase or decrease the number of letters in a word that can be different from the original search term. |

**TABLE 6-7 Max Files to List and Max Hits per File**

| Option            | Result  |
|-------------------|---|
| Max Files to List | Maximum number of files with hits that are listed in the results. You can change the maximum number in the field. The default is 200, if no entry is made. 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.   |
| Max Hits per File | Maximum number of hits per file. You can change the 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 hits per file” option)” which may be cut off if the file name exceeds the allowed line length.<br><br>The maximum number applies separately to files with hits from both Allocated and Unallocated disk space. Reducing the number of hits to display per file reduces the time it takes to display all items. |

**Important:** When running the search, limit the number of files with hits (200 is default) to list at one time, and try to have only one tree node in the Index Search Results list expanded at a time for either Allocated or Unallocated space hits. Having too many tree items expanded (to display

3,000 or more files with hits) can cause long delays in viewing selected hits..

**TABLE 6-8 Search by Date and Time**

| Option                | Description   |
|-----------------------|---|
| All Files             | Search all the files in the case.   |
| File Name Pattern     | Limits the search to files that match the filename pattern.<br><br>The pattern can include "?" to match a single character or "*" to match zero or more characters. Operator characters can be used to fill in for unknown characters. The asterisk (*) and question-mark (?) operators are the only allowed characters in the search. The "*" means any or no unknown characters and the "?" means any one unknown character.<br><br>For example, if you set the filename pattern to "d?ugl*", the search could return results from files named "douglas", "douglass", or "druglord."<br><br>To enter a filename pattern:<br><br>Check the box.<br><br>In the field, enter the filename pattern. |
| Files Saved Between   | Beginning and ending dates for the last time a file was saved. Do the following to set these parameters:<br><br><ol style="list-style-type: none"><li>1. Check the box.</li><li>2. In the date fields, enter the beginning and ending dates to search.</li></ol>  |
| Files Created Between | Beginning and ending dates for the creation of a file. Do the following to set these parameters:<br><br><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.</li></ol>  |
| File Size Between     | Minimum and maximum file sizes, specified in bytes.<br><br>Check the box.<br><br>In the size fields, enter the minimum and maximum size in bytes of the files that you want to search.  |
| Save as Default       | Check this box to make you settings apply to all index searches.  |

When search criteria are prepared and you are ready to perform the search, click *Search*  
*Now*:

# DOCUMENTING SEARCH 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 where it can be copied to another Windows application, such as an Excel spreadsheet  
**Note:** 10,000 is the maximum number of evidence items that can be copied in a single copy operation.
- **Export to File:** Copies information to a file. Select the name and location for the information file.

Copy or export the hits and the statistics of a search result using the options on the following table:

**TABLE 6-9 Result Copy or Export Options**

| Option                   | Description   |
|--------------------------|---|
| All Hits in Case         | Saves all the search terms found from the entire case.              |
| All Hits in Search       | Saves all the search terms found in each search branch.             |
| All File Stats in Case   | Creates a CSV file of all file information in the case.             |
| All File Stats in Search | Creates a CSV file of the file information requested in the search. |

After the information is copied to the clipboard, it can be pasted into a text editor or spreadsheet and saved.

Search results can then be added to the case report as supplementary files.

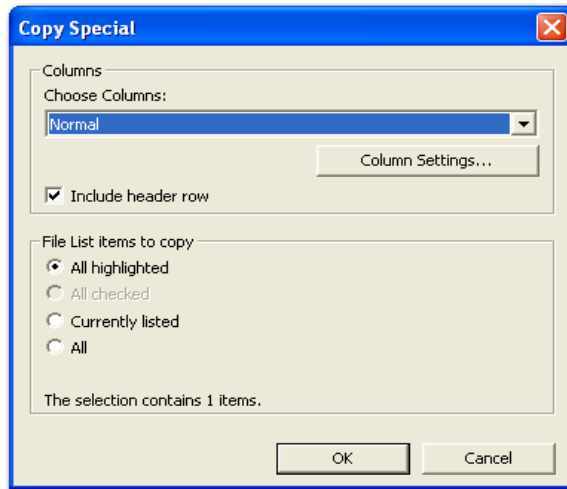
## USING COPY SPECIAL TO DOCUMENT SEARCH RESULTS

The Copy Special feature allows the copying of specific information about files to the clipboard or a file.

To copy information about the files in your search results:

1. In the Index Search Results list, highlight the search hit you want to document.
2. Find that file highlighted in the File List view.
3. Right-click on the desired file.

4. Select *Copy Special*.



5. In the Copy Special dialog, under Choose Columns, click the dropdown select the columns definition to use, or click *Column Settings* to define a new column template.
  - 5a. Modify the column template in the Column Settings Manager. For more information on customizing column templates, see “Customizing File List Columns” on page 197.
6. Mark *Include Header Row* if you want a header row included in the exported file.
7. Under *File List Items to Copy*, select from *All Highlighted*, *All Checked*, *Currently Listed*, or *All* to specify which files you want the Copy Special to apply to.
8. Click *OK*.

## BOOKMARKING SEARCH RESULTS

To keep track of the files that were returned in a particular search, bookmark the search results. Bookmarks from the search results in the file list can be created or added to a 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 the selected files then select *Create Bookmark*.
3. Complete the Create New Bookmark dialog. For more information, see “Creating a Bookmark” on page 104.



4. Click *OK*.

The bookmark now appears in the Bookmark tab.



## *Chapter 7 Data Carving*

AccessData Forensic Toolkit (FTK) has the ability to carve data. Data carving is the ability to locate files that have been deleted or that are embedded in other files.

### **SEARCHING FOR EMBEDDED AND DELETED FILES (DATA CARVING)**

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 searching for items, such as graphics, embedded in other files. It allows the recovery of previously deleted files located in unallocated space. Users can also carve directory entries to find information about data or metadata.

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. A new filename is determined and the file is saved. 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:

- AOL Bag Files

- BMP Files
- EMF Files
- GIF Files
- HTML Files
- JPEG Files
- Link Files
- PDF Files
- OLE Archive Files (Office Documents)
- PDF Files
- PNG Files

## DATA CARVING FILES WHEN PROCESSING A NEW CASE

Select to data carve when a case is created by selecting Data Carve in the Evidence Processing dialog. Select Carving Options and the file types to carve.

For more information, see “Selecting Evidence Processing Options” on page 74.

## 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. Check *Data Carve*.
3. Click *Carving Options*.
4. Set the data carving options to use.
5. Click *OK* to close the Carving Options dialog.
6. Select the target items to carve data from.
7. Click *OK*.

The carved files are added to the case, and can be searched, bookmarked, and organized along with the existing files. For more information, see “Chapter 5 Working with Cases” on page 91.

## Chapter 8 Using Filters

AccessData Forensic Toolkit (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 made during a certain time frame

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.

*Figure 8-1 The Filter Toolbar*



For an explanation of the filter toolbar and its components, see “Toolbar Components” on page 42.

## APPLYING AN EXISTING FILTER

FTK contains the following predefined filters:

**TABLE 8-1 Pre-defined Filters**

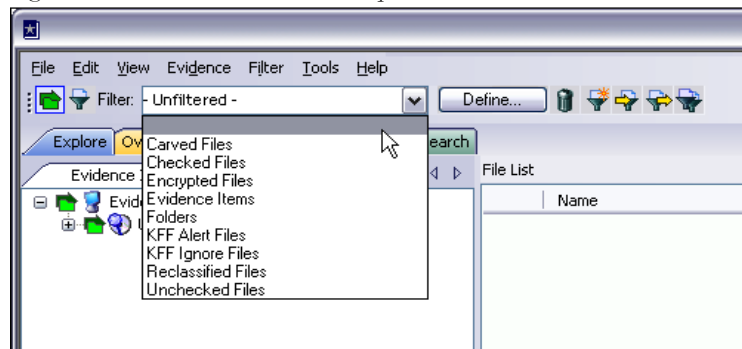
| Filter                      | Description  |
|-----------------------------|--|
| Archive Files               | Shows only archive file items.   |
| Bad Extension Files         | Shows only the files with extensions that don't match the file.  |
| Carved Files                | Shows only the items 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, or have been decrypted by the user then added to the case.        |
| Deleted Files               | Shows only those items that have the deleted status.   |
| Duplicate Files             | Shows only items that have duplicates. Displays the primary copy and all secondary copies of each file that has multiple instances.. |
| Email Attachments           | Shows all items sent as attachments to a message, but does not include the most recent email "container" message.                    |
| Email Files                 | Shows only those items that have the email status.   |
| Email Files and Attachments | Shows all email items including email messages, related attachments, and others, such as notes, appointments, and so forth.          |
| Encrypted Files             | Shows only those items flagged as EFS files or other encrypted or compressed files.  |
| Evidence Items              | Shows all items from the root-level tree.  |
| Flagged Ignorable           | Shows only those items you have identified as Ignorable.   |
| Flagged Privileged          | Shows only those items you have identified as Privileged.  |
| Folders                     | Show only folder items.  |
| From Recycle Bin            | Shows only those items taken from the recycle bin.   |
| Graphic Files               | Show only those items that have been identified as graphics.   |
| KFF Alert Files             | Shows all KFF alert files that are in a case.  |
| Microsoft Office Files      | Show Word, Access, PowerPoint, and Excel files.  |
| KFF Ignore Files            | Shows KFF ignore files that are in a case.   |
| No Deleted                  | Shows all but deleted items.   |

**TABLE 8-1 Pre-defined Filters**

| Filter                                     | Description   |
|--|---|
| No Duplicate                               | Shows all files, but where duplicates are found, includes only the primary (generally the first instance encountered by the program during processing) copy, and does not display any secondary (all subsequent instances of a file whose hash exactly matches another instance of a file already added to the case) duplicate files. |
| No KFF Ignore Files                        | Shows all items but KFF ignore files.   |
| Not Flagged Ignorable                      | Shows all items but those you indicated Ignorable.  |
| No KFF Ignore or OLE Subitems              | Shows all items but KFF ignore files or OLE subitems.   |
| No KFF Ignore or OLE Subitems or Duplicate | Shows all items but KFF ignore files, OLE subitems, or duplicate items.   |
| Not Flagged Privileged                     | Shows all items but those you flagged Privileged.   |
| OLE Subitems                               | Shows only OLE archive items and archive contents.  |
| Reclassified Files                         | Shows only those item you have changed the classification.  |
| Registry Files                             | Shows Window 9x and NT registry files.  |
| Thumbs.db Files                            | Shows Thumbs.db files.  |
| Unchecked Files                            | Shows only those items that you have not checked.   |
| User-decrypted Files                       | Shows only those items that you have decrypted and added to the case.   |
| Web Artifacts                              | Shows HTML, Index.dat, and empty Index.dat files.   |

To apply an existing filter, use the Filter drop-down list on the File List toolbar, displayed in the following figure.

Figure 8-2 File List Toolbar Filter Dropdown List



## CREATING A FILTER

You can create or modify your own filters. These custom filters are saved with the case in which they are created.

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 might have two criteria in something like a date range.)

**Note:** Using filters adds work and time to processing a case. The more filters applied, the more time needed to process. Shut down the FTK user interface to speed up case processing.

1. Select *Unfiltered* from the Select a Filter drop-down menu.
2. Click *Filter > New*, or click *Define* on the Filter toolbar.
3. Type a name and a short description of the filter.
4. Select a property from the drop-down menu.
5. Select an operator from the Operators drop-down menu.
6. Select the applicable criteria from the Criteria drop-down menu.

Each property has its own set of operators, and each operator has its own set of criteria. The combinations are vast to allow you to customize filters that fit your needs.

7. 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.
8. Click *Save*.

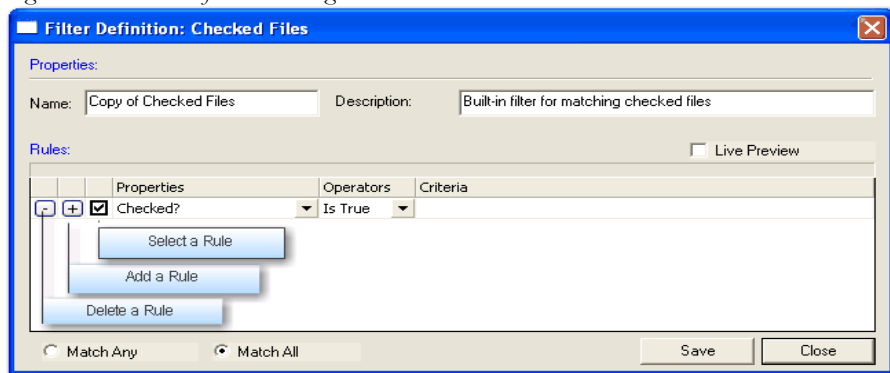
Test the filter without having to save it first by selecting the *Live Preview* checkbox to test the filter while creating it.



## REFINING A FILTER

As the investigation progresses, investigators become more familiar with patterns and file types needed in the case, and can adjust the filters to find this specific data. The following figure displays the Filter Definition dialog used for changing and refining filters.

Figure 8-3 Filter Definition Dialog



To modify an existing filter:

1. Select the filter you want 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*.

## DELETING A FILTER

You can delete a custom filter if you no longer need it. Predefined, or system filters cannot be deleted.

To delete a custom filter:

1. Select the filter 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 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 database.

FTK creates and records hashes of the files it discovers in the evidence to demonstrate that the files have not been modified since acquisition, and to allow for quick determination if two files have the same contents.

## UNDERSTANDING KFF HASHES

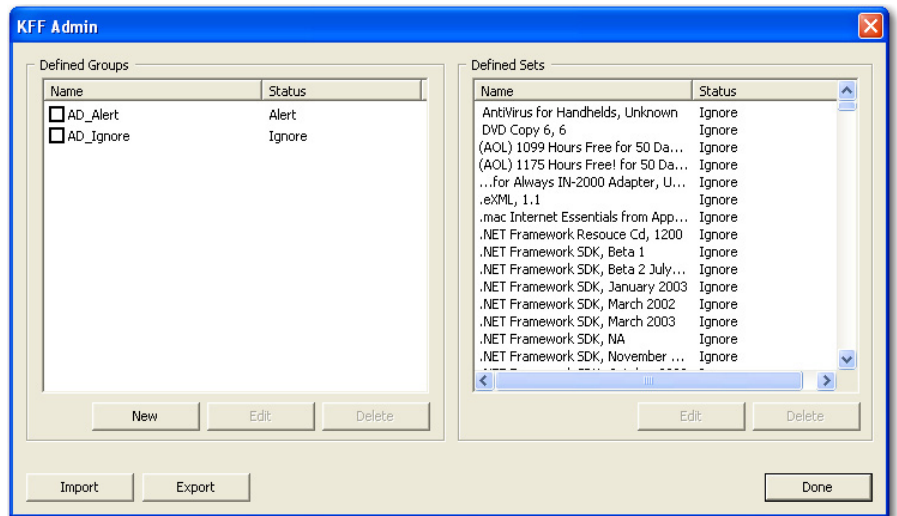
FTK includes hashes from two major reporting agencies, The National Institute of Standards and Technology (NIST), and Hashkeeper. The toolkit also provides a mechanism for the addition of hashes from other sources to the KFF database. When you select a set in FTK the source reporting agency is displayed in a text box. It is good practice when creating sets to put your own agency in the source field so that other investigators know where the hashes came from.

## IMPORTING KFF HASHES

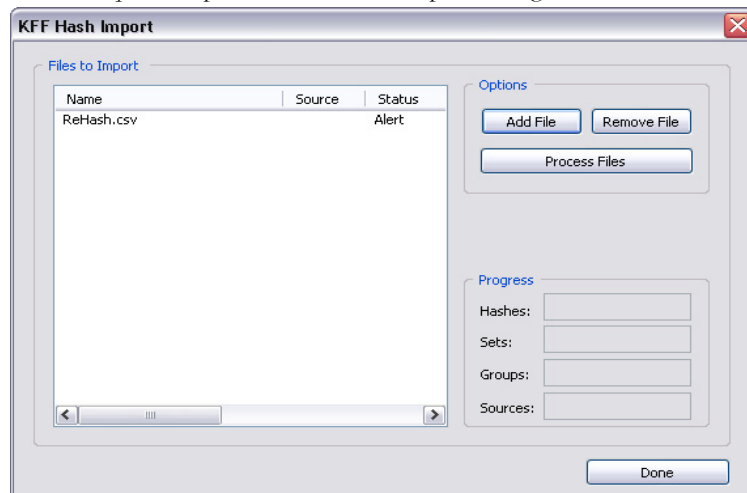
When using the Import KFF Hashes feature, you can import hashes from several supported formats.

To import hashes to the KFF database do the following steps:

1. Click *Tools > KFF > Manage* to open the KFF Administration dialog.



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.0 (.KFF)

The dialog box titled "Add KFF Source File to Import List" has a blue header. It contains a "Status:" dropdown menu set to "Alert". Below it are three text input fields labeled "Path:", "Name:", and "Description:". To the right of the "Path:" field is a "Browse..." button. To the right of the "Name:" and "Description:" fields is an "Options" section with a checkbox labeled "Import Entire Directory". At the bottom right are "OK" and "Cancel" buttons.

3a. If you need to create a source, click *Create New* to open the KFF Source Management dialog.

The dialog box titled "KFF Source Management" has a standard Windows title bar with a close button. It features a section labeled "KFF Sources" with a large empty list box. To the right of the list box are three buttons: "New", "Edit", and "Delete". At the bottom center is a "Done" button.

3b. Click *New* to open the Add New KFF Source dialog.

This is a duplicate of the "Add KFF Source File to Import List" dialog box described in the first image. It contains a "Status:" dropdown menu set to "Alert", three text input fields for "Path:", "Name:", and "Description:", a "Browse..." button next to the "Path:" field, an "Options" section with a checkbox for "Import Entire Directory", and "OK" and "Cancel" buttons at the bottom right.

3c. Type name for the new source.

3d. Click *OK*.

4. Close the dialogs back to the KFF Administration dialog, and click *Import*.

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

## 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 THE KFF DATABASE

FTK divides hashes into three table: AccessData, Case-specific, and Shared.

**TABLE 8-2 KFF Library Groups**

| 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.   |
| Shared     | Create your own sets and groups. You should create non-case specific hash sets and groups here. Sets or groups in these tables are accessible to anyone using the same KFF database instance (cases are stored in the same 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 investigators 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 evidence files. For example, WordPerfect 5.1, Quicken 7, or a collection of photographs taken at a suspects home.

A **group** represents a collection of related sets. For example, legitimate software, known child pornography, or known hacker tools.

Sets and groups allow investigators to rapidly specify what kind of files to which they want to be alerted, to more easily comply with search warrant limitations by rapidly disregarding files outside the warrant, and 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 8-3 KFF Group Status Options**

| Status    | Description  |
|-----------|--|
| Alert     | Selecting this status indicates to the Forensic Toolkit that you want to be alerted to the existence of any file in the set or group.  |
| Disregard | This case specific status allows the investigator 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 the Forensic Toolkit will not automatically alert the investigator 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). Utilizing this status allows the Forensic Toolkit to sift these uninteresting files away from the investigators view.  |

The group's status supersedes the statuses of any of its sets without actually changing 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. They contain all sets in the KFF and cannot be modified manually by the user.

If you have included the same set in two different groups, FTK prioritizes the status and returns the highest priority status:







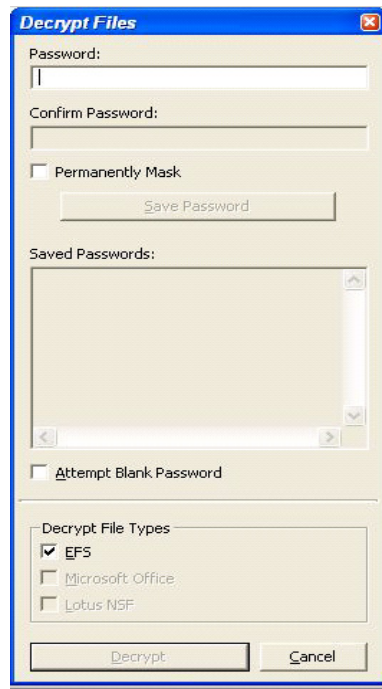
# *Chapter 9 Decrypting Encrypted Files*

## **DECRYPTING FILES AND FOLDERS**

FTK2.1 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 FTK2.

Click *Tools > Decrypt Files...* to begin decryption. The following figure displays the decryption menu:

Figure 9-1 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 2.1 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.
6. 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 Forensic Toolkit (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.

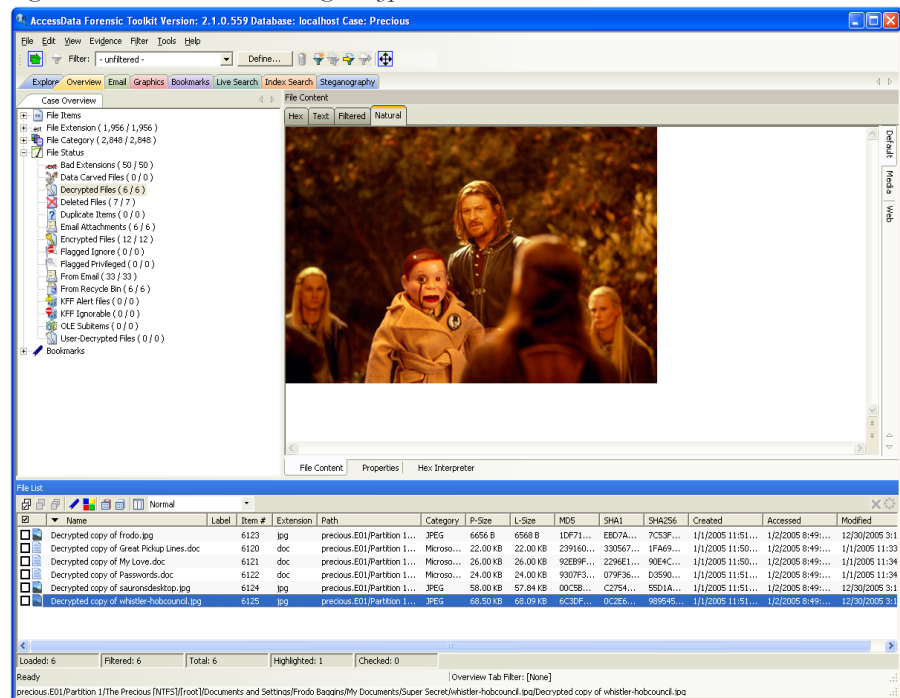
There are certain files that cannot be encrypted, including system files, NTFS compressed files, and files in the C:\Windows\_System\_Root and its subdirectories.

**Note:** All EFS decryption requires the user's or Recovery Agent's password.

## VIEWING DECRYPTED FILES

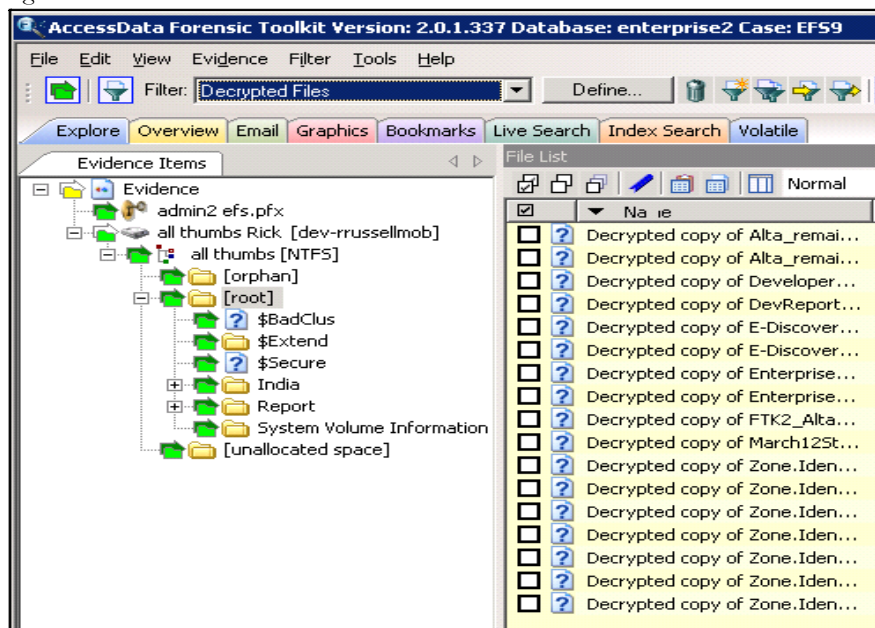
Find the decrypted files in the Overview tree, under the *File Status > Decrypted Files* branch. Click on an individual file in the File List to view the file in the File Content pane.

Figure 9-2 Overview Tab Viewing Decrypted Files



**Note:** Regardless of the encryption type, once decrypted, the files will appear in the File List Name column as “Decrypted copy of <file name>,” as seen in the following figure:

Figure 9-3



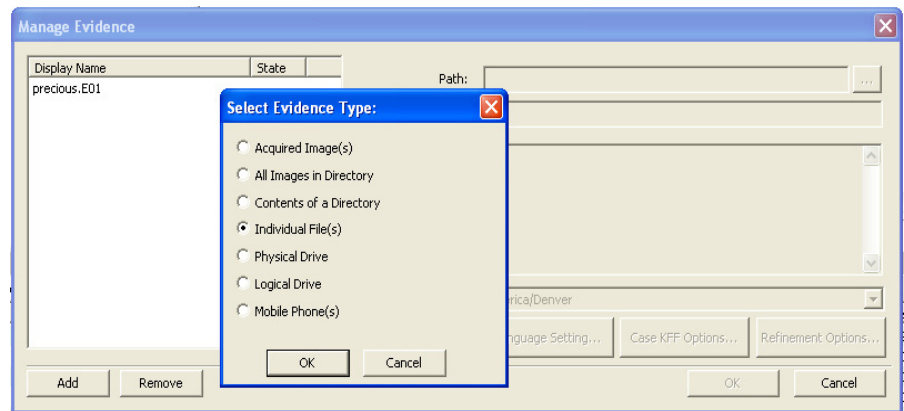
## DECRYPTING DOMAIN ACCOUNT EFS FILES

This section deals with decrypting domain account EFS files using FTK. These can be decrypted from image files, individually, or the whole image may contain the encrypted files.

To decrypt EFS files from a file image, perform the following steps:

1. Create a new case with no evidence added.

2. From the main menu, click *Evidence > Add/Remove*.



3. Click *Add*.

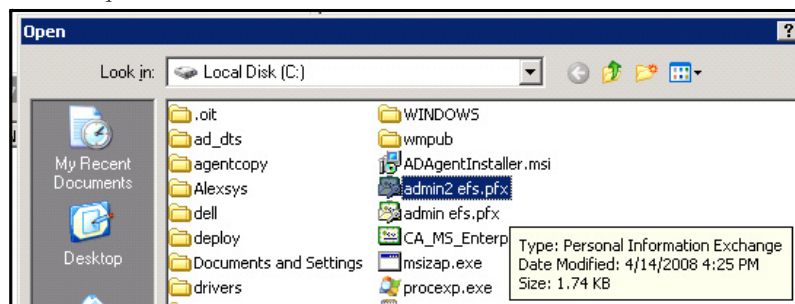
4. Select *Individual File(s)*.

5. Click *OK*.

6. Navigate to the PFX file (domain recovery key).

Or type the full path and filename into the File Name field of the Open dialog.

7. Click *Open*.



8. Click *No* when the application asks if you want to create an image of the evidence you are adding.

9. Select the proper time zone for the PFX file from the Time Zone drop-down list in the Manage Evidence window, and click *OK*.

FTK2.1 begins processing the PFX file and the progress dialog appears.

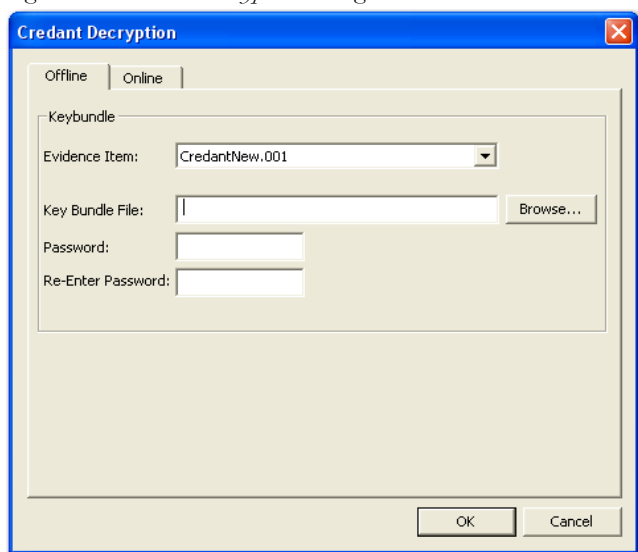
**Note:**

## 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.

Click *Tools > Credant Decryption* to open the Credent decryption options, as displayed in the following figure:

Figure 9-4 Credant Decryption Dialog

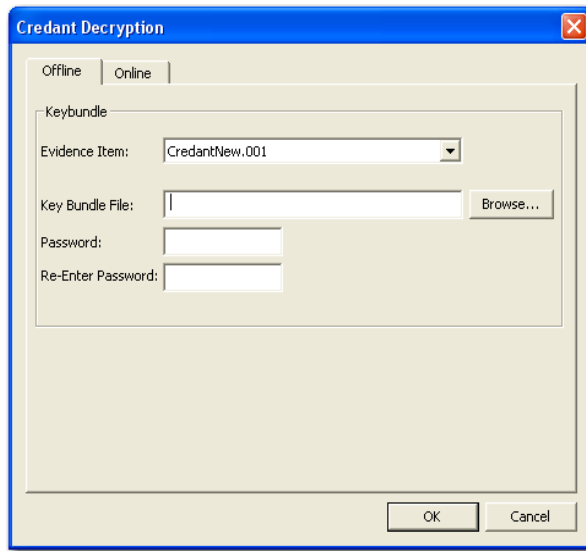


The Credant integration for FTK allows two options for decryption; offline, and online. For a key bundle located on the user's local machine or network, use the offline option with. For a key bundle located on a remote server use the online option.

## 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 computer. Perform the following steps to decrypt a Credant encrypted image offline: select the key bundle file and enter the password used to decrypt it.

1. 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 only occur when the machine processing the image can directly access the Credant server over the network. The following figure displays the online tab:



Figure 9-5 Credant Decryption Online Options

The screenshot shows a Windows-style dialog box titled "Credant Decryption". It has two tabs: "Offline" and "Online", with "Online" currently selected. The dialog is divided into two main sections: "Evidence Data" and "Server Data".

**Evidence Data Section:**

- Evidence Item:** A dropdown menu showing "CredantNew.001".
- Credant Machine ID:** A text field containing "credant60client.adlab.local".
- Credant Shield ID:** A text field containing "NLY13VCA".

**Server Data Section:**

- Credant Server User Name:** An empty text field.
- Credant Server Password:** An empty text field.
- Credant Server Domain:** An empty text field.
- Credant Server IP Address:** An empty text field.
- Port:** A text field containing "8081".

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

Usually FTK auto-populates the *Credant Machine ID* and *Credant Shield ID* fields. The *Credant Machine ID* can be found on the Credant server as the *Unique ID* on the *Properties* tab. The *Credant Shield ID* can be found as the "Recovery ID" on the "Shield" tab. It looks like this: "ZE3HM8WW".

The Server Data group box contains information on how to contact the Credant server. It includes the Credant Server user name, password, and IP. The port should be 8081 (and is auto-populated).

The offline decryption requires you to get a key bundle file from the server. You need to select the key bundle file and enter the password used to decrypt it. You can 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 -dcredantxp1.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

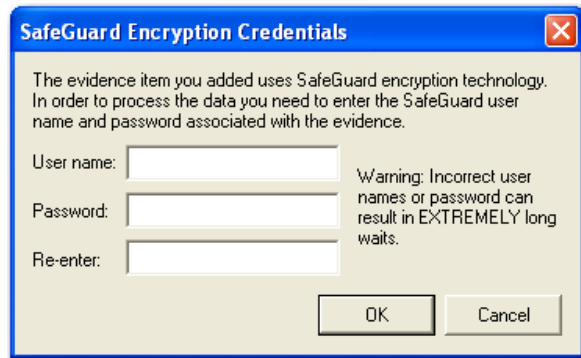
-s for the Shield ID  
-o for the output file  
-i for the password used to encrypt the keybundle

Once you have either used the online or 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 9-6 *Decryption\_SafeguardEncryptionCredentials*



The Safeguard dialog box appears only when FTK2.1 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 timezone from the Time Zone drop-down, then click **OK** to begin processing.

**Important:** Type the User Name and Password carefully and verify before clicking **OK**. If this information is entered incorrectly, FTK2.1 checks the entire image for matching information before returning with an error message. Each wrong entry results in a longer wait.

## DECRYPTING SAFEBOOT FILES

SafeBoot is a program that encrypts drives and/or partitions. When FTK2.1 detects a SafeBoot-encrypted drive or partition, the following dialog is displayed.

*Figure 9-7 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.

Once the key has been added and the appropriate partitions selected, click *OK* to return to the Manage Evidence dialog. Select a timezone from the Time Zone drop-down, then click *OK* to begin processing.



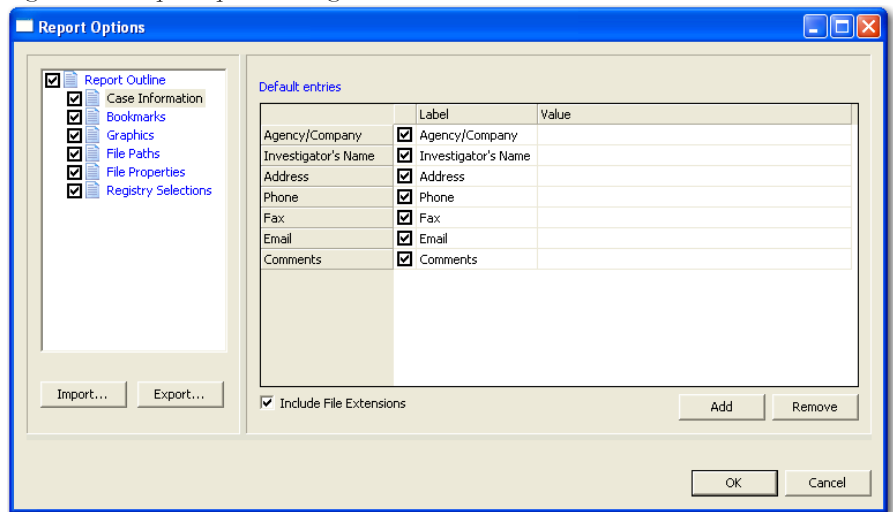
## *Chapter 10 Working with Reports*

Upon completion of the case investigation, AccessData Forensic Toolkit (FTK) can create a report that summarizes the relevant evidence of the case. The final report is made available in several formats and is viewable in a standard Web browser.

### **CREATING A REPORT**

You create a report with the Report Wizard, as displayed in the following figure. You access the Report Wizard by selecting *File > Report*.

Figure 10-1 Report Options Dialog



To create a report:

1. Enter basic case information.
2. Select the properties of bookmarks.
3. Decide how to handle graphics.
4. Decide whether to add a file path list.
5. Decide whether to add a file properties list.
6. Select the properties of the file properties list.
7. Add the Registry Viewer sections.

Each step is discussed in detail in the following sections.

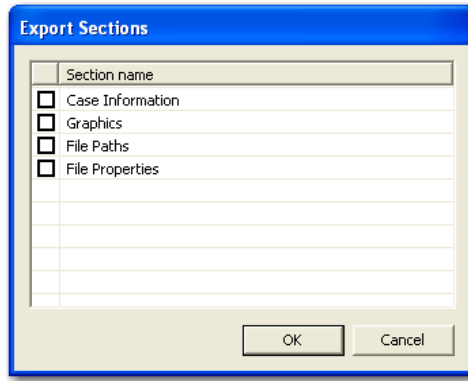
## SAVING SETTINGS

Report settings are automatically saved when you finish specifying the report settings, and click **OK** to generate the report.

Export report settings at anytime while creating a report, and after you finish specifying the report settings. Import and reapply those settings to a new report, or a report in a new case, as desired.

To export report settings do the following:

1. Click *Export*. The Export Selections dialog opens.



2. Check the sections to export the settings for.
3. Click *OK*.
4. Type a name for the setting file. Click *OK* to save the settings as an **.XML** file.

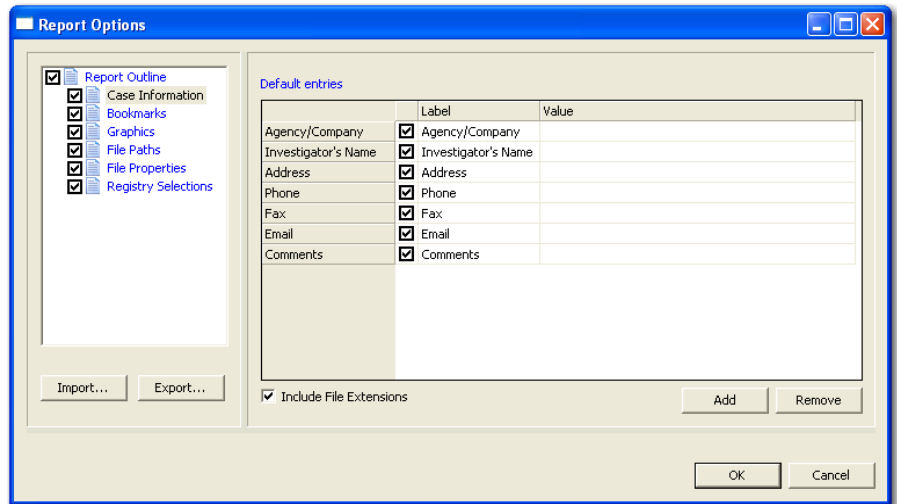
To import settings to a new report in another case, perform the following steps:

1. Open a different case.
  1. Click *File > Report > Import*.
  2. Browse to and select the settings file you want to import.
  3. Click *Open* to import the settings file to your current case and report.

## ENTERING BASIC 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 basic case information displayed.

Figure 10-2 Basic Case Information



To include basic case information in the report, check the Case Information box in the Report Outline on the left side of the screen. In the Default Entries pane, check the entries to include in the report (all are checked by default). 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 ensure that file extensions are included in case information exported to the report.

To add an entry for case information 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*.

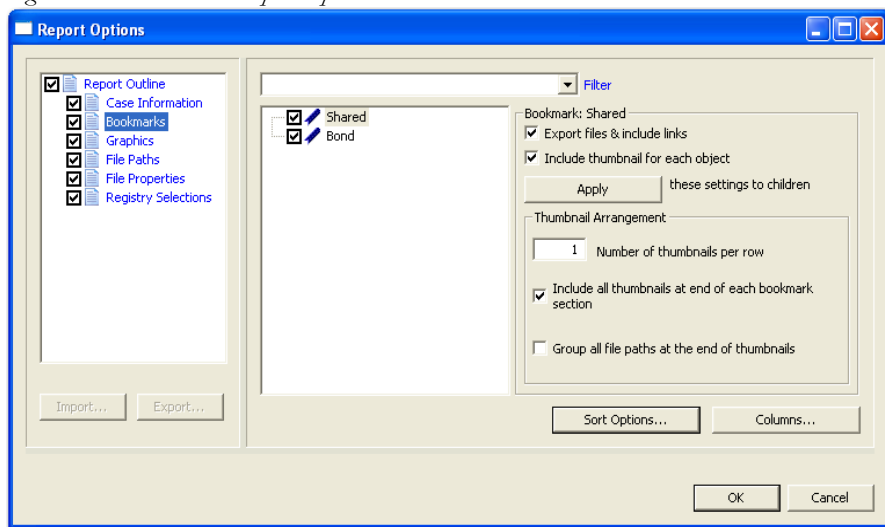


## INCLUDING BOOKMARKS

Marking the Bookmarks dialog creates a section in the report that lists the bookmarks that were created during the case investigation, as displayed in the following figure.

The investigator can also choose to not create a bookmark section by unselecting the Bookmarks checkbox.

Figure 10-3 *Bookmark Report Options*

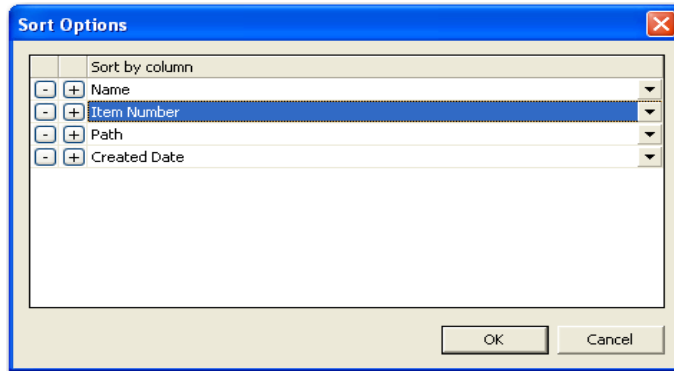


Mark the boxes to include Shared and/or User bookmarks. Choose whether to export the files and include links to them in the report when it is generated and whether to include graphic thumbnails that may be part of any bookmarks.

## SELECTING SORT OPTIONS

Select the primary sort criterion for the bookmarks by clicking *Sort Options*. To set the sort order for the bookmarks in the report, do the following:

1. Click *Sort Options* to open the Sort Options dialog.

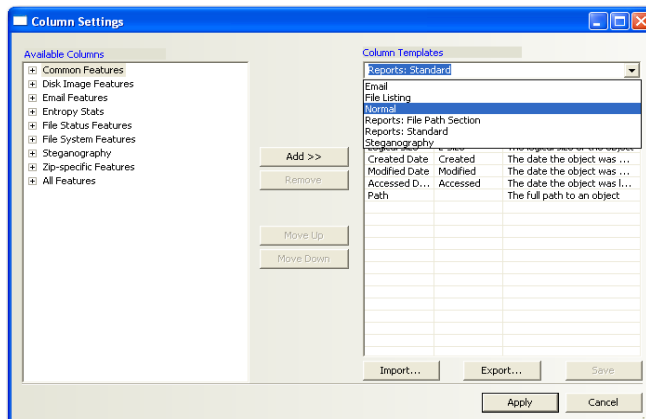


2. Add a sort line by clicking Plus (+). Remove a sort line by clicking Minus (-).
3. Add sorting criteria by clicking the drop-down list button at the right end of the sort line.
4. Click *OK* to close the dialog when you are satisfied with the sort options you have selected.

## SETTING BOOKMARK COLUMNS

The columns can be modified to display specific information about bookmarks included in the report.

*Figure 10-4*

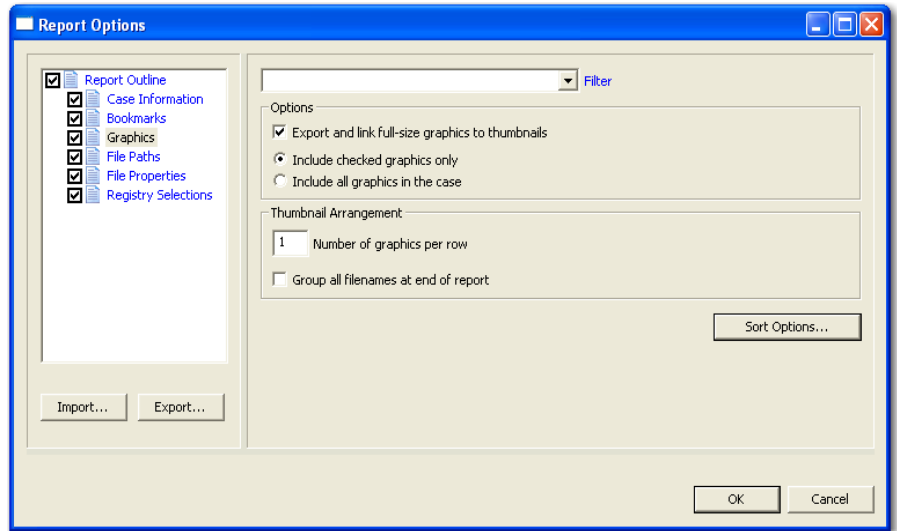


To modify the column setting, click *Columns*. The Column Settings dialog opens. Select a pre-defined columns template, or create your own. For more information on setting columns, see “Customizing File List Columns” on page 197.

## INCLUDING GRAPHICS

Mark the Graphics box under Report Outline to include graphics in the report. The Graphics section in the report displays thumbnail images of the graphics in the case and can link them to original graphics if desired, as displayed in the following figure.

*Figure 10-5 Report Options: Graphics*

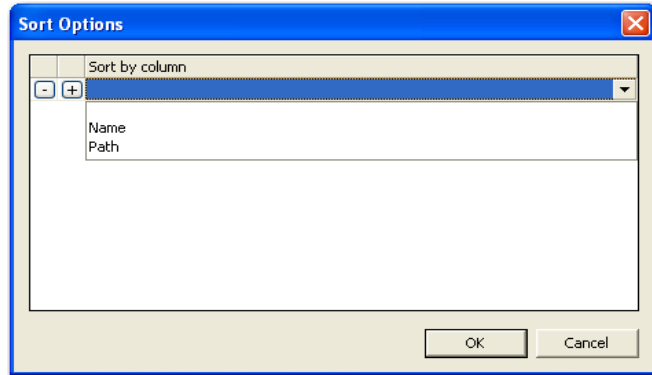


Select the options as follows:

1. Apply no filter, or one of several filters to your graphics files.
2. If desired, mark the box to Export and link full-size graphics to thumbnails. This allows the person viewing the report to click on a thumbnail and see the original graphic that was found in the case.
3. Choose either of the following:
  - Include all graphics in the case
  - Include checked graphics only
4. Set the number of graphics to display per row.

5. If you want filenames displayed all together at the end of the report, mark the box for Group all filenames at end of report. If this box is not marked, each filename displays with its respective thumbnail.
6. Click *Sort Options* to access the Sort Options Page.

*Figure 10-6 Report Graphics Sort Options*

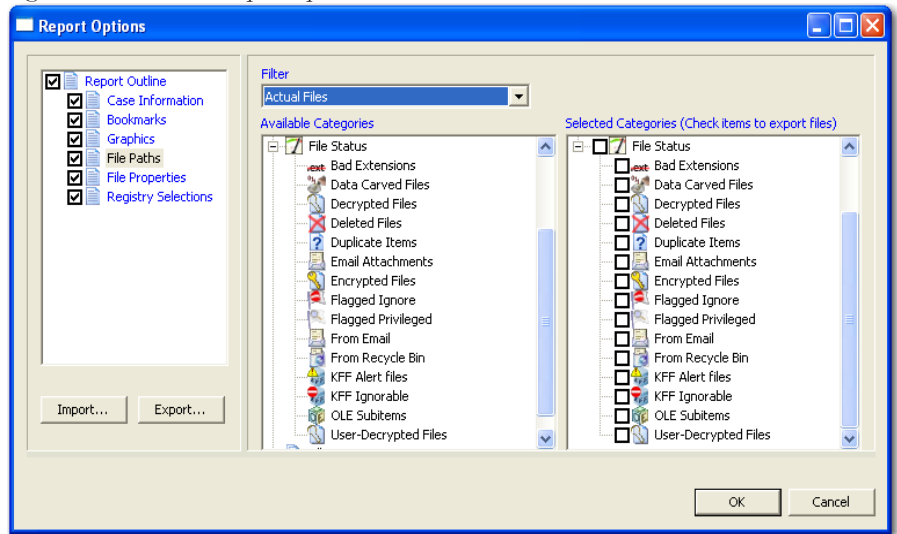


7. Set the desired sort options (note that only two options are available here).
8. Click OK to return to the Bookmark Options page for the report.

## SELECTING A FILE PATH LIST

The List by File Path dialog creates a section in the report that lists the file paths of files in selected categories. The List by File Path section simply displays the files and their file paths; it does not contain any additional information. The files can be exported and link to the files in the File Path list by selecting category item checkboxes to be exported.

Figure 10-7 File Path Report Options

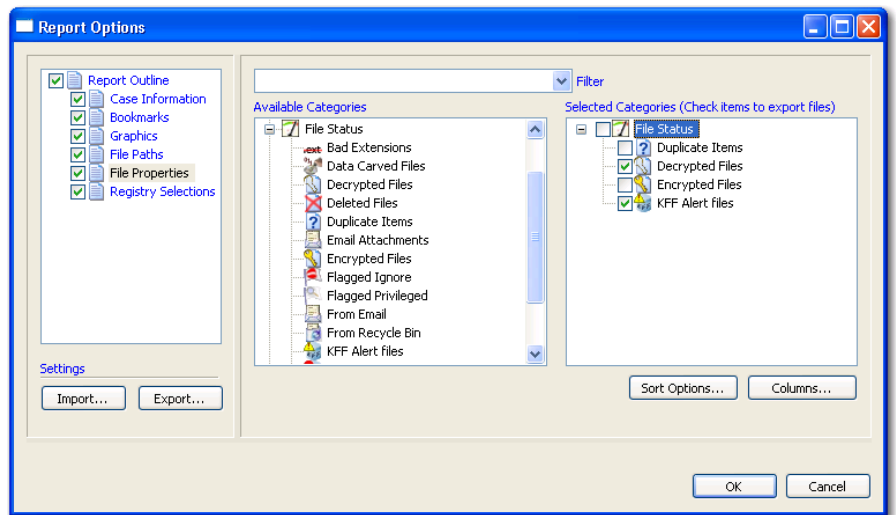


Drag and drop an item to the Selected Categories window to copy an item and its parent category. You can then check a category item to export its contents to the report. Checking an item automatically selects the files and folders under it.

## SELECTING A FILE PROPERTIES LIST

The File Properties options allow the creation a section in the report that lists file properties for files in selected categories. The options are displayed in the following figure.

Figure 10-8 File Properties Report Options



Drag and drop items from the Available Categories box to the Selected Categories box. Check items in the Selected Categories box items to export them to the report. Checking an item automatically selects the files and folders under it.

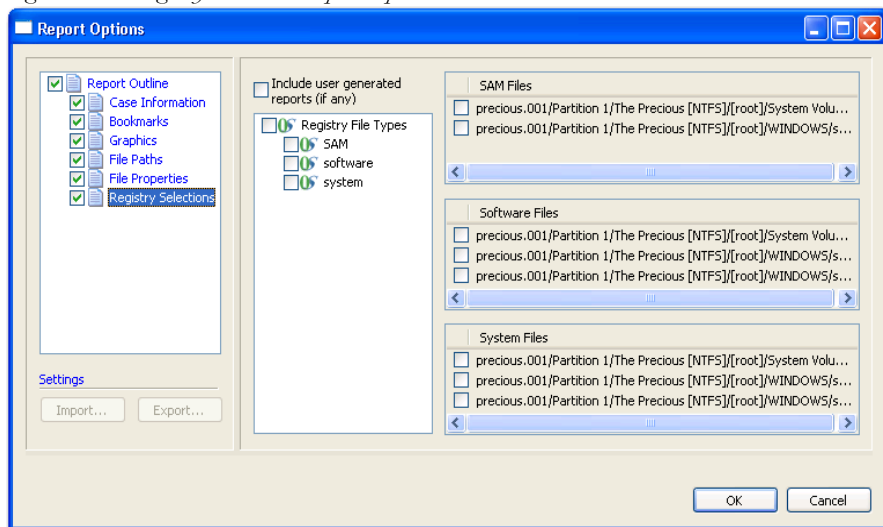
To modify the Sort Options, click *Sort Options*. For more information on modifying the Sort Options, see “Selecting Sort Options” on page 179.

To modify column settings, click *Columns*. The Column Settings dialog opens. For more information on setting columns, see “Customizing File List Columns” on page 197.

## REGISTRY SELECTIONS

If the evidence drive image contains registry files, they can be included in the report through the Registry Selections report options.

Figure 10-9 Registry Selections Report Options



In the Registry File Types window, check the file types for headings to include in the report. In the right window, check the registry file paths to included in the report.

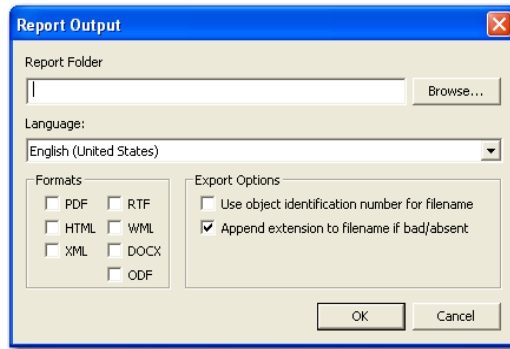
## RUNNING THE REPORT

When all report options have been selected, click OK to display the Report Output dialog.

## SELECTING THE REPORT LOCATION

The Report Output dialog allows the selection of the report location. The investigator can also recreate the directory structure of exported items.

Figure 10-10 Report Output Dialog



To select the report location do the following:

1. Type the folder to save the report to, or use the *Browse* button to find a location.
2. Use the drop-down arrow to select the output language of the report.
3. Indicate the output format to publish the report.
4. Select the optional Export Options for the report:
  - 4a. Use object identification number for filename.
  - 4b. Append extension to filename if bad/absent.
5. When output selections have been made, click *OK* to begin report generation.

## CREATING THE REPORT

When the options are selected and you click OK, the Data Processing Status window appears. The progress bar dialog indicates the progress of the report.

The report displays when processing is complete. You can process only one report at a time.

If another report generation is attempted while a report is generating, the investigator is prompted to wait, as in the following dialog.



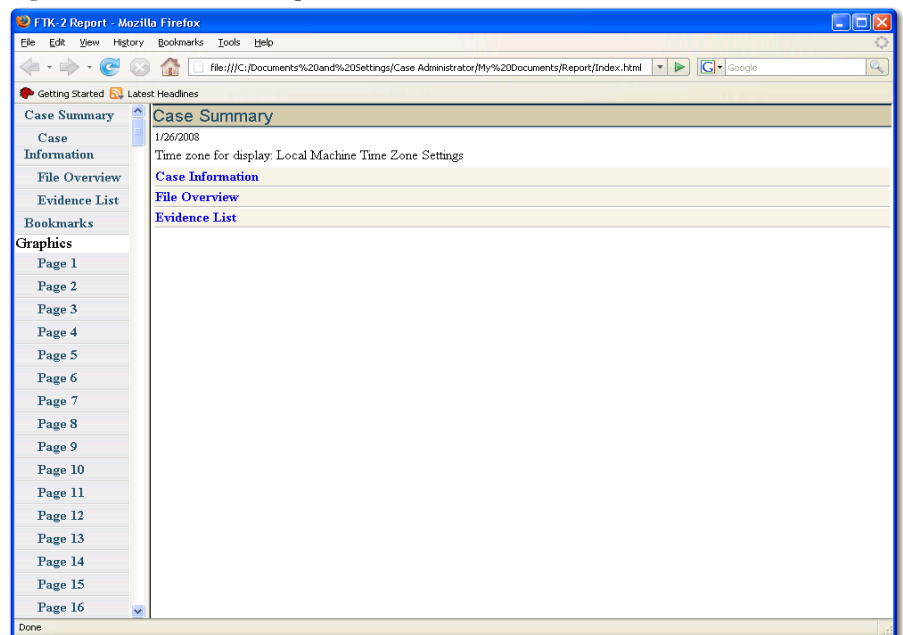
Figure 10-11 Wait Dialog



## VIEWING A REPORT

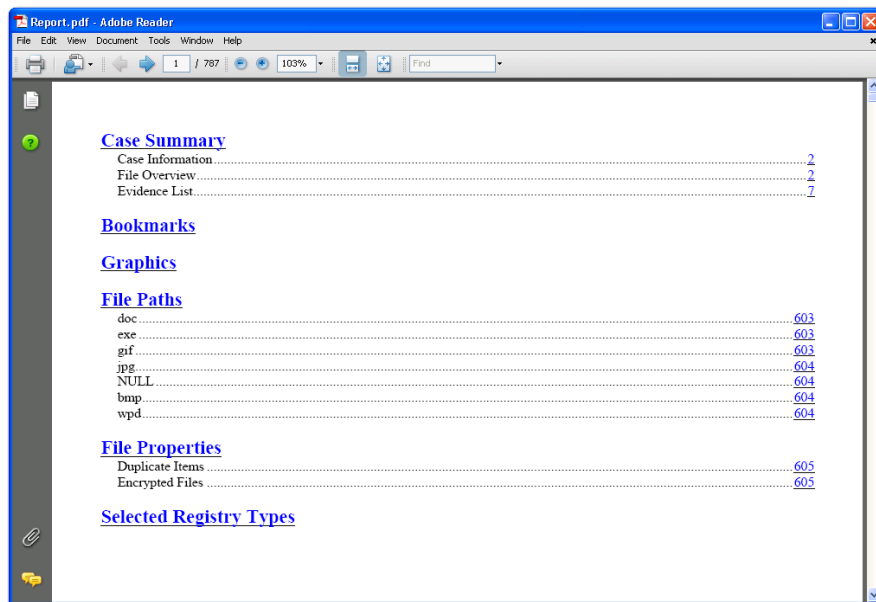
The report contains the information that you selected in the Report Wizard. When included in the report, files appear in both raw data and in the report format. An example of the main page of the HTML (index.htm) report is displayed in the following figure.

Figure 10-12 HTML Case Report



The following figure represents the PDF version of the report as displayed in a viewer.

Figure 10-13 PDF Report



To view the report without opening it from FTK, browse to the report file and click on the report file. The report will open in the appropriate program for the report file type selected. For example:

- Click on index.htm to open an HTML document in a Web browser.
- Click on the file report.pdf to open the report in a PDF viewer.
- Click on the file report.docx to open the report in Microsoft Word 2007.

## INTERNATIONAL DATE AND TIME STAMP ISSUE

Be sure, when distributing a report that the date and time stamp are in the format of the intended recipient of the report. Once dates, as interpreted HTML views of binary files in FTK, are put into a report, the output is always in the preferred format for the computer that generated the report. So if the date and time are placed in the report in a European format of dd/mm/yyyy versus the United States format of mm/dd/yyyy, some problems can be presented. For example, a situation of 02/01/2003 could be interpreted as 2 January 2003 (in the European format) or 1 February 2003 (in the United States format). This interpretation could cause problems with internationally circulated cases and reports.

## **MODIFYING A REPORT**

Recreate the report with the added evidence or changed report settings to modify the report. Change the report settings for each report as needed. All previously distributed reports should be retracted from the recipients 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, and will hold its formatting better than the HTML report.



# *Chapter 11 Customizing the Interface*

The AccessData Forensic Toolkit (FTK) interface provides a highly visual user interface to make evidence more recognizable and easy to process. To help further, adjust the interface to accommodate the current case and the user's personal style.

## **CUSTOMIZING OVERVIEW**

Adjust the size of the panes in the tabs by clicking on a border and dragging it to a new size. The order of the tabs are rearranged by dragging and dropping them in the desired order.

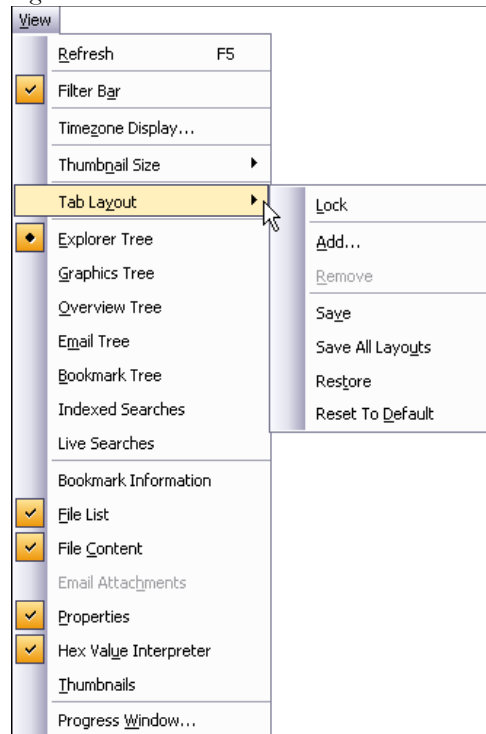
Users can add or remove panes from the current tab using the View menu. Click *View* and click the pane you would like to add to the current view.

To save the new arrangement, Click *View > Tab Layout > Save*.

## **USING THE VIEW MENU TO CUSTOMIZE THE FTK INTERFACE**

Use the View menu to control the pane views displayed in each tab. Several tabs are available by default, but tabs can be customized, or new ones created to fit your needs.

Figure 11-1 FTK View Menu



The View menu contains the following options:

- Refresh the current view's data
- View the Filter Bar
- Select the desired time zone for viewing
- Choose the display size for graphic thumbnails. Select from the following:
  - Large - default
  - Medium
  - Small
  - Tiny
- Customize the Tab Layout. Options are:
  - Lock the tabs to prevent changes.
  - Add a new tab.

- Remove a tab.
- Save an individual tab
- Save all tab Layouts
- Restore to before previous change.
- Reset to factory defaults.
- Explorer Tree
- Graphics Tree
- Overview Tree
- Email Tree
- Bookmark Tree
- Index Searches
- Live searches.
- Bookmark Information
- File List
- File Content
- Email Attachments
- Properties
- Hex Value Interpreter
- Thumbnails
- Progress Window

## CUSTOMIZING THE TAB VIEWS

From the View menu you can add panes to the current tab. Note that the Tree panes, such as Explorer Tree, or Overview Tree, are “exclusive”, and only one can exist on a single tab at any time.

To add other panes to a tab, Click *View*, then click to checkmark the pane to add. Options are described in the table below:

**TABLE 11-1 View Panes Available from the View Menu**

| View Pane             | Description   |
|-----------------------|---|
| Bookmark Information  |   |
| File List             | Adds the File List Pane to the current tab.         |
| File Content          | Adds the File Content Pane to the current tab.      |
| Email Attachments     | Adds the Email Attachment Pane to the current tab.  |
| Properties            | Adds the Properties Pane to the current tab.        |
| Hex Value Interpreter | Adds the Hex Value Interpreter to the current tab.  |
| Thumbnails.           | Adds the Thumbnails Viewer Pane to the current tab. |

## USING 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 11-2 Tab Layout Menu Options**

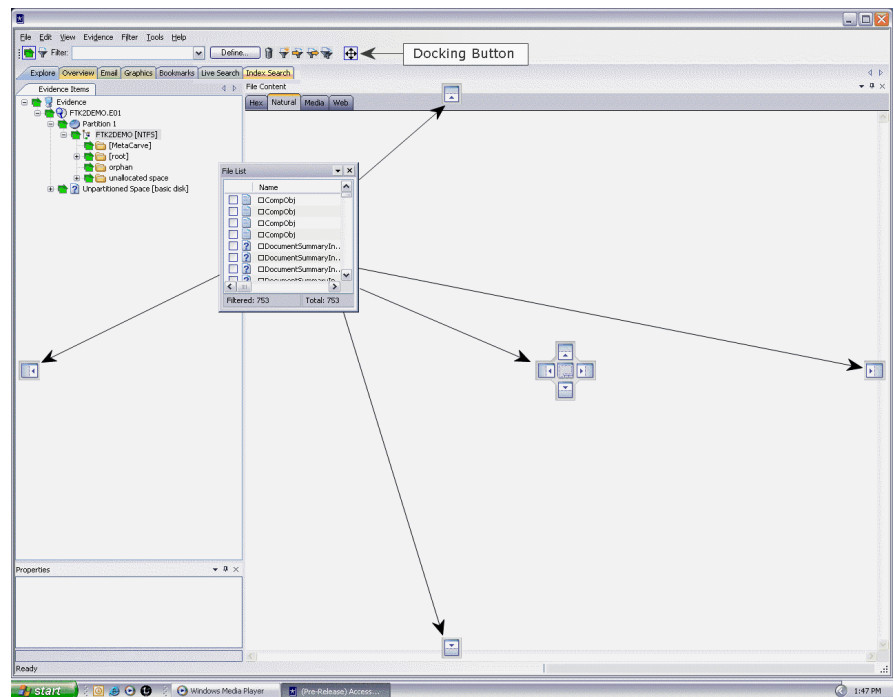
| Option           | Description   |
|------------------|---|
| Lock             | Locks the panes in place so that they cannot be moved.  |
| Add              | Adds a blank tab to the FTK window. The new tab will be like the one selected when this option is used. |
| Remove           | Removes the selected tab from the FTK window.   |
| Save             | Saves the changes made to the tab.  |
| Save All Layouts | Saves the changes made to all tabs.   |
| Restore          | Restores the FTK window to the settings from the last saved layout. Custom settings can be restored.    |
| Reset to Default | Resets the FTK 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. Hover the mouse over the title bar of the pane until a Move icon (a four-direction arrow) appears. Hold down the mouse button to undock 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 11-2 Pane in Movement*





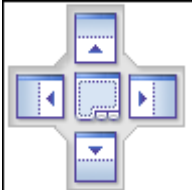
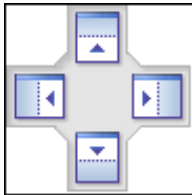



To place the view pane at a specific location on the application:

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 11-3 Docking Options**

| 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  |
|    | 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 the 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 down, making them immovable. When the lock is applied, the blue box turns grey.   |

## CREATING CUSTOM TABS

Create a custom tab to specialize an aspect of an investigation, add in desired features, apply filters as needed, and to accommodate conditions specific to a case.

To create a custom tab, do the following:

1. Click *View > Tab Layout > Add*.
2. 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.
3. 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.

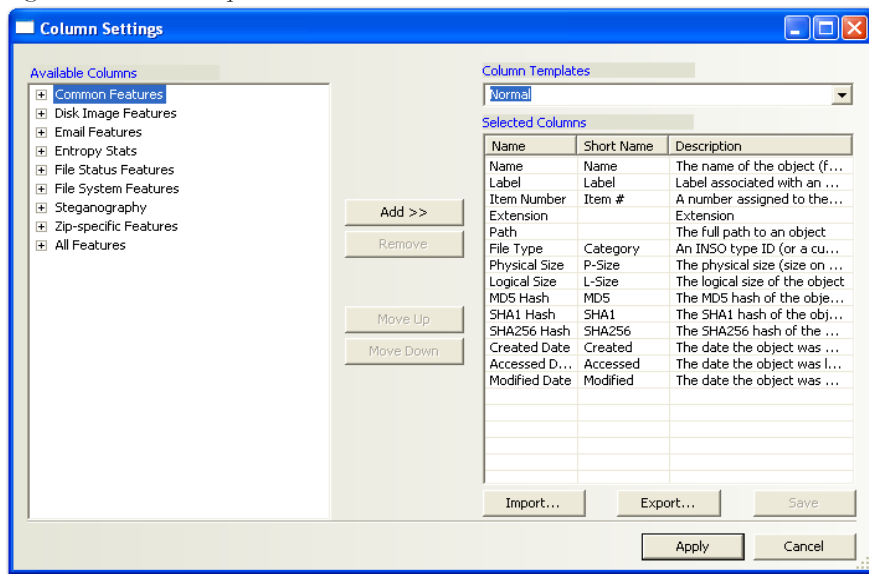
4. When satisfied with your new tab's content, click *Save* to save the current tab's settings, or *View > Tab Layout > Save*.
5. (Optional) Click *View > Tab Layout > Save All* to save all changed and added features.
6. To remove tabs, click *View > Tab Layout > Remove*.

## 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 what file information appears in the Bookmark and List File Properties sections of case reports.

Using custom column settings, as displayed in the following figure, narrows the information provided in the File List and case reports. Columns display specific information about the listed files.

Figure 11-3 Column Options



Custom column settings can be exported as an .XML file, and imported for use in other cases.

To export column settings to an .xml file, do the following:


1. Click Export.
2. Select a folder and provide a filename for the exported column settings file.
3. Click Save.

To import a column settings file, do the following:

1. From the Column Settings dialog, click Import.
2. Find and select the column settings .xml file.
3. Click Open.

## CREATING AND MODIFYING COLUMN SETTINGS

To modify or create column settings:

1. Right-click a heading in the File List, or click the *Column Settings*  button to open the Manage Columns context menu.
2. Click *Column Settings*. The Column Settings dialog opens.
3. From the Available Columns pane, select a category from which to use a column heading. 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 dragging the column borders wider or narrower.

Click on a column heading in the file list view to sort by that column. Hold down the Shift key while clicking a column heading to make that column the primary sorted column while the previously sorted column becomes the secondary sorted column.

To undo a secondary sort, click on a column heading 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 what tab and 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 first, then type the first letter of what you are searching for. FTK will move down the list to the first file containing that letter. As you continue to type, the search gets more specific until you have typed the entire name of the item. You may find exactly what you are looking for with only a few characters. You can use the scroll button to move up and down the list at any point. When you find the item in the list, select it.

## COMMON FEATURES

The following column headings tend to be most shared among objects.

**TABLE 11-4 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.                   |

**TABLE 11-4 Common Column Headings**

| Column                   | Description  |
|--------------------------|--|
| Actual File              | Yes (Y) or No (N) value to indicate whether this is an Actual File which is the file as the user or file system normally sees it, as opposed to a member of All Files which includes metadata, document summary info, etc. |
| Bad Extension            | Indicates if the file type does not match its header.  |
| Carved                   | Indicates whether the object has been carved.  |
| Compressed               | Indicates whether the object is compressed. Only set on files.   |
| Compressed File Size     | Displays the size of the compressed files. Only set on compressed files.   |
| Container                | Indicates whether the object has child objects.  |
| Created Date             | Indicates the date the object was created.   |
| Decrypted                | Indicates that the object has been decrypted.  |
| Decrypted by User        | Indicates that the object has been decrypted by the user before having been added to the case.   |
| Deleted                  | Yes (Y) or No (N) value to indicate whether an item was deleted.   |
| Duplicate File           | The file is a duplicate of another file in the case.   |
| Encrypted                | Indicates whether the object is encrypted. Only set on files.  |
| Extension                | Displays the object's extension.   |
| File Class               | Matches a branch 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         | Yes (Y) or No (N) value to indicate a Recycle Bin index file, or a recycled file still in the Recycle Bin folder.  |
| Fuzzy Hash               | Opens the Fuzzy Hash dialog where you can specify the number of words files must have in common to determine how closely files relate to each other.   |
| Fuzzy hash blocksize     | Fuzzy hash blocksize   |
| Fuzzy hash library group | Fuzzy hash library group   |
| Fuzzy hash library score | Fuzzy hash match score   |

**TABLE 11-4 Common Column Headings**

| Column                    | Description   |
|---------------------------|---|
| Fuzzy hash library status | Fuzzy hash library status   |
| Item Number               | Displays a unique ID number assigned the object by FTK.                             |
| Logical Size              | Indicates the logical size of an object.  |
| MD5 Hash                  | Indicates the MD5 hash of the object's contents.                                    |
| Modified Date             | Indicates the date the object was last modified.                                    |
| Name                      | Indicates the name of the object.   |
| Object Type               | The type of the object.   |
| Original File Type        | Indicates the original type of an object whose type has been changed.               |
| Path                      | Shows 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. |
| 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 11-5 Column Headings for Viewing Hashes**

| Column              | Description  |
|---------------------|--|
| Validate MD5        | Indicates the validated MD5 hash of the object. This is the internal stored hash of an image such as E01 or SMART.   |
| 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. |

## EMAIL FEATURES

These column headings listed in this table are features specific to email in general, to Microsoft Outlook\*/Exchange\*, and to Outlook Express.

**TABLE 11-6 Common Email Column Headings**

| Column                             | Description  |
|------------------------------------|--|
| Lotus Notes-specific features      | Options include: <ul style="list-style-type: none"><li>• <b>Note ID:</b> The Lotus Notes NOTE_ID (unique to the NSF file).</li><li>• <b>UNID:</b> The Lotus Notes Universal Note ID (globally unique).</li></ul> |
| Outlook Express-specific Features  | See below, table titled <b>Microsoft Outlook Express Column Headings</b>   |
| Outlook/Exchange-specific Features | See below, table titled <b>Microsoft Outlook/Exchange Column Headings</b>  |
| Attachment                         | Whether the email contained an attachment  |
| BCC                                | Indicates addresses in the Blind Carbon Copy field.  |
| CC                                 | Indicates 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.  |
| Email File                         | True if file is part of email.   |
| From                               | Lists the 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                            | Lists 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 was marked as Sent.   |



## MICROSOFT OUTLOOK EXPRESS HEADINGS

These email headings are set for Microsoft Outlook Express only:

**TABLE 11-7 Microsoft Outlook Express Column Headings**

| Column                              | Description   |
|-------------------------------------|---|
| Account Name                        | Indicates the name of the account associated with the object.   |
| Account Registry Key                | Indicates the registry key associated with the object's account.  |
| Answered                            | Indicates whether the object was answered. True if the Email has been answered, false otherwise.  |
| Answered Message ID                 | Displays the ID of the email's answered message.  |
| Digitally Signed                    | Indicates whether the email was digitally signed.   |
| Email Size                          | Indicates the size of the email. Only set on emails from Outlook Express.   |
| Has Attachment<br>(Outlook Express) | Indicates whether the email has an attachment. True if the email has at least one attachment, false otherwise. Only set on emails from Outlook Express. |
| Hotmail Message ID                  | Displays the ID of a Hotmail email message.   |
| Marked                              | Indicates whether the email has been marked. True if the email has been marked, false otherwise. Only set on emails from Outlook Express.               |
| Message ID                          | Displays the message ID. Only set for Outlook Express.  |
| Message Offset                      | Shows the message offset of the email.  |
| News                                | Indicates whether the email was a news item. True if the email is a news item, false otherwise. Only set on emails from Outlook Express.                |
| Priority                            | Shows the priority assigned the email. Only set for Outlook Express.  |
| Recipient Address                   | Lists the addresses in the email's recipient field. Only set for Outlook Express.   |
| Recipient Name                      | Lists the names in the email's recipient field. Only set for Outlook Express.   |
| Sender Address                      | Lists the addresses in the email's sender field. Only set for Outlook Express.  |
| Sender Address and Name             | Lists the addresses and names in the email's sender field. Only set for Outlook Express.  |

**TABLE 11-7 Microsoft Outlook Express Column Headings**

| Column                                  | Description   |
|---|---|
| Sender Name                             | Lists the name in the email's sender field. Only set for Outlook Express.                     |
| Server                                  | Lists the server used to send the email. Only set for Outlook Express.                        |
| Server Info                             | Lists the server information the email. Only set for Outlook Express.                         |
| Subject<br>(Outlook Express)            | Lists the text on the email's subject field. Only set for Outlook Express.                    |
| Subject Without Prefix                  | Lists the text without the prefix on the email's subject field. Only set for Outlook Express. |
| Thread Ignored                          | Indicates whether a thread was marked as Ignore. Only set for Outlook Express.                |
| Thread Watched                          | Indicates whether a thread was marked as Watch. Only set for Outlook Express.                 |
| Time Message Saved<br>(Outlook Express) | Indicates the time an email was Saved. Only set for Outlook Express.                          |
| Time Received<br>(Outlook Express)      | Indicates the time an incoming email was received. Only set for Outlook Express.              |
| Time Sent<br>(Outlook Express)          | Indicates the time an outgoing email was sent. Only set for Outlook Express.                  |

**MICROSOFT OUTLOOK/EXCHANGE HEADINGS**

These email headings are set for Microsoft Outlook/Exchange only:

**TABLE 11-8 Microsoft Outlook/Exchange Column Headings**

| Column              | Description  |
|---------------------|--|
| Attachment MIME Tag | Lists the attachment MIME tag of the email.        |
| Client Submit Time  | Indicates the time the client submitted the email. |
| Comment             | Lists any comment associated with the email.       |
| Content Count       | Indicates the content count of the email.          |
| Content Unread      | Indicates whether the email is marked Unread.      |
| Conversation Topic  | Indicates the email's conversation topic.          |

**TABLE 11-8 Microsoft Outlook/Exchange Column Headings**

---

| <b>Column</b>                        | <b>Description</b>  |
|--------------------------------------|---|
| Delete After Submit                  | Indicates whether the email was marked for deletion after it was submitted. |
| Display Name                         | Lists the email's display name.   |
| From Me                              | Indicates whether the email was marked From Me.                             |
| Importance                           | Indicates the email's assigned importance.                                  |
| Message Class                        | Indicates the class assigned to the message in the email.                   |
| Message Size                         | Indicates the size of the email.  |
| Originator Delivery Report Requested | Indicates whether an Originator Delivery Report was requested.              |
| Provider Submit Time                 | Indicates the time at which the provider submitted the email.               |
| Read Receipt Requested               | Indicates whether the email sent requested confirmation of the email.       |
| Received By Email Address            | Indicates the time at which the addressee received the email.               |
| Received By Name                     | Lists the name on the addresses that received the email.                    |
| Received Representing Email Address  | Displays the address of a Representing email recipient.                     |
| Reply Recipient Names                | Lists the addresses in the Reply To: field.                                 |
| Resend                               | Indicates whether the email was marked Resend.                              |
| Sender Email Address                 | Lists the address in the email's Sender field.                              |
| Sensitivity                          | Indicates the sensitivity assigned the email.                               |
| 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 email was marked as Submit.                           |
| Transport Message Headers            | Lists the Simple Mail Transfer Protocol (SMTP) headers.                     |
| Unmodified                           | Indicates whether the email has been marked as Modified.                    |

## ENTROPY STATISTICS

These column headings list information that indicate entropy statistic possibilities such as encryption and compression.

**TABLE 11-9 Entropy Statistics Column Headings**

| Column                         | Description  |
|--------------------------------|--|
| 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.   |
| MCPI Error Percent             | Monte Carlo algorithm, named after Monte Carlo, Monaco, is a method involving statistical techniques for finding solutions to problems.<br><br>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 email 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 their status.

**TABLE 11-10 File Status Column Headings**

| Column     | Description   |
|------------|---|
| Hash Set   | 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 KFF status of the file.   |
| Label      | Label associated with an object.  |

**TABLE 11-10 File Status Column Headings**

| Column                                    | Description  |
|---|--|
| Not KFF Ignore or OLE Subitem             | True if the file is not marked KFF Ignore, or the file is not an OLE subitem.  |
| Not KFF Ignore, OLE Subitem, or Duplicate | True if the file is not marked KFF Ignore or the file is not an OLE subitem, or the file is not a duplicate of another file. |

If a file has matches from more than one set, the status with the height value is used. For more information, see “Using Filters” on page 151.

## FILE SYSTEM FEATURES

These column headings list information specific to a particular file system.

**TABLE 11-11 File Status Column Headings**

| Column                  | Description   |
|-------------------------|---|
| DOS Features            | See below, in the table titled <b>DOS File System Column Headings</b> .           |
| ext2 Features           | See below, in the table titled <b>ext2 File System Column Headings</b> .          |
| HFS Features            | See below, in the table titled <b>HFS File System Column Headings</b> .           |
| NTFS Features           | See below, in the table titled <b>NTFS File System Column Headings</b> .          |
| Unix* Security Features | See below, in the table titled <b>Unix Security File System Column Headings</b> . |
| Start Cluster           | Indicates the starting cluster of a file on a disk or volume.                     |
| Start Sector            | Indicates the starting sector of a file on a disk or volume.                      |

## DOS FILE SYSTEMS

These column headings list information specific to DOS.

**TABLE 11-12 DOS File System Column Headings**

| Column    | Description  |
|-----------|--|
| 8.3 Name  | Lists 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 an object.     |

## EXT2 FILE SYSTEMS

These column headings list information specific to ext2.

**TABLE 11-13 ext2 File System Column Headings**

| Column       | Description  |
|--------------|--|
| 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. Set on Unix objects only. Data structures that 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 on files.</p> <p>There are 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 <code>ls -li</code> command, while the <code>ls -li</code> command will retrieve other inode information.</p> |

## HFS FILE SYSTEMS

These column headings list information specific to HFS.

**TABLE 11-14 HFS File System Column Headings**

| Column                   | Description   |
|--------------------------|---|
| 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)       | Lists 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)     | Lists 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) | Lists the ID of the object's Put Away folder.                                 |

## NTFS FILE SYSTEMS

These column headings list information specific to NTFS.

**TABLE 11-15 NTFS File System Column Headings**

| Column                      | Description  |
|-----------------------------|--|
| Alternate Data Stream Count | The number of alternate data streams contained in the object.  |
| Group Name                  | Displays the Group Name of the object's owner.   |
| Group SID                   | Displays the group SID of the object owner.  |
| MFT Record Number           | Displays the object's Master File Table (MFT) record number, indicating 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 owner.   |
| Owner SID                   | Displays the SID of the object owner.  |
| Record Date                 | Indicates the record date of the object.   |
| Resident?                   | Indicates whether the Resident attribute is set for the object.  |

**TABLE 11-15 NTFS File System Column Headings**

| Column    | Description  |
|-----------|--|
| 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 11-16 Unix Security File System Column Headings**

| Column            | Description                                   |
|-------------------|---|
| 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.          |

**STEGANOGRAPHY**

These column headings list information specific to files where steganography is found:

**TABLE 11-17 Steganography Column Headings**

| Column             | Description  |
|--------------------|--|
| Confidence         | Level of confidence that this file contains a steganographic payload   |
| Highest Confidence | Level of highest confidence that this file contains a steganographic payload among all the candidate steganography applications. |
| Stego App          | Application used to extract this steganographic payload.   |
| Stego Password     | Password used by steganography application to extract this steganographic payload.   |



# ZIP-SPECIFIC FEATURES

These column headings list information specific to files zipped (combined) or compressed into a single file.

**TABLE 11-18 Zip-Specific Column Headings**

| Column             | Description                                    |
|--------------------|--|
| 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.    |



## *Chapter 12 Other AccessData Applications*

In addition to AccessData Forensic Toolkit (FTK), other AccessData products can be used to capture and further analyze data.

### **ACCESSING ADDITIONAL PRODUCTS**

Click *Tools > Other Applications* to access the following choices.

- Imager
- PRTK & DNA
- Registry Viewer
- LicenseManager
- Language Selector

For more information on these products, see the users' manuals on the AccessData Downloads Web page at [www.accessdata.com/support](http://www.accessdata.com/support).

### **CAPTURING EVIDENCE WITH IMAGER**

FTK Imager is a data preview and imaging tool used to quickly assess electronic evidence to determine if further analysis with FTK is warranted. Imager creates forensic images (exact copies) of computer data without making changes to the original

evidence. The forensic image is identical in every way to the original, including file slack and unallocated space or 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, and USB storage devices.
- Create forensic images of local hard drives, floppy diskettes, Zip disks, CDs, DVDs, and USB storage devices.
- 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.

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 hash 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).

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

## RECOVERING PASSWORDS WITH PRTK

Password Recovery Toolkit (PRTK) is a software solution that provides tools to recover passwords and gain access to computer files:

- Passworded and/or encrypted files law enforcement needs access to as part of an investigation
- Vital personal files protected by a forgotten password
- Password-protected network files

PRTK provides password-breaking modules for many popular software applications you encounter.

## HOW PRTK WORKS

PRTK analyzes passworded and encrypted files to determine passwords and decryption keys using recovery modules for supported applications. Before recovering passwords for protected files, PRTK creates hash values that can be used to establish that the content of a file was not changed during the password recovery.

PRTK ships with many default dictionary files and rule sets that it uses in cracking passwords. PRTK also uses custom dictionaries created from word lists you import, (often exported from an FTK case), and rules you define, to attempt every conceivable password possibility against a file. Whenever a password is successfully found, that password is added to the Golden dictionary.

After recovering passwords, PRTK lets you verify hashes, print reports, and decrypt/open recovered files.

## PRTK FEATURES

PRTK performs the following functions:

- **Hash files:** Hashing a file uses a unique algorithm that verifies the identity of a file. Before recovering the password of a file, PRTK automatically hashes that file. 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 passwords for files created in most popular software applications by using a variety of methods, including the dictionary attack, which recovers a password using different dictionaries and word combinations. PRTK also recovers multi-lingual passwords.
- **Decrypt files:** many PRTK modules include a keyspace attack in addition to a dictionary attack. A keyspace attack attempts to determine the decryption key of a file where no password has been used.
- **Generate reports:** Print file information for password recovery jobs.
- **Open recovered files:** Open recovered files in their native if the applications using the password or key provided by PRTK.

## OBTAINING PROTECTED INFORMATION WITH REGISTRY VIEWER

The Windows Registry stores all the information necessary for the Windows operating system to control hardware, software, user information, and the overall functionality of the Windows interface. Unlike Windows Registry Editor, which only displays the registry settings for the currently authenticated user, AccessData Registry Viewer lets you examine registry files from any user on the computer, or network. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor.

Detailed information on Registry Viewer functionality is available in the Registry Viewer manual.

Integrating Registry Viewer with FTK allows you to view registry files and create registry reports from within FTK. Any created reports are saved by default in the current FTK case folder.

Integration also allows you to extract and open registry files on the fly from hard drive images. FTK automatically creates a temporary registry file from the drive image and opens it in Registry Viewer. FTK deletes the temporary file when the user finishes with the temporary file.

For more information, see Appendix E: "Appendix E Securing Windows Registry Evidence" on page 255.

## 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 AccessData such products as FTK, eDiscovery, Enterprise, PRTK, DNA, and Registry Viewer. 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.

The licensing information provides the following:

- Names of programs
- Versions of programs
- Subscription expiration date
- Number of licensed clients

## STARTING LICENSEMANAGER


LicenseManager.exe is located in **C:\Program Files\AccessData\Common Files\AccessData LicenseManager\**. When starting LicenseManager, License Manager reads licensing and subscription information from the installed CodeMeter Stick.

From within FTK2, click *Tools > Other Applications > LicenseManager*,

OR


Click *Start > All Programs > AccessData > LicenseManager > LicenseManager*,


OR

Click or double-click (depending on your Windows settings) the *LicenseManager* icon on your desktop .

The LicenseManager program opens.

If using a CodeMeter Stick, and LicenseManager either does not open or displays the message, “Device Not Found”, do the following:

- 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. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray .

- 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, FTK2.1 will not run with a packet file alone. You must have the CmStick connected to the computer to run FTK2.1.

## LICENSEMANAGER INTERFACE

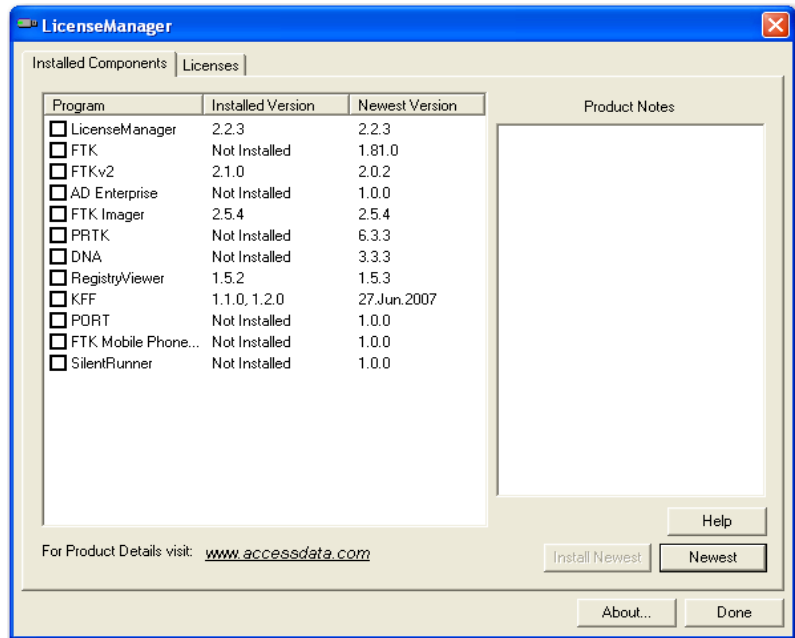
The LicenseManager interface consists of two tabs that organize the options in the LicenseManager window: the Installed Components tab and the Licenses tab.

### 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 12-1 Licence Manager Installed Components



The following information is displayed on the Installed Components tab:

**TABLE 12-1 LicenseManager Installed Components Tab Features**

| Item              | Description  |
|-------------------|--|
| Program           | Shows a list of AccessData products installed on the host.                               |
| Installed Version | Shows the version of each AccessData product installed on the host.                      |
| Newest Version    | Shows the latest version available of each AccessData product installed on the host.     |
| Product Notes     | Displays notes and information about the product selected in the program list.           |
| AccessData Link   | Links to the AccessData product page where you can learn more about AccessData products. |
| Help              | Opens the LicenseManager Help web page.  |

**TABLE 12-1 LicenseManager Installed Components Tab Features**

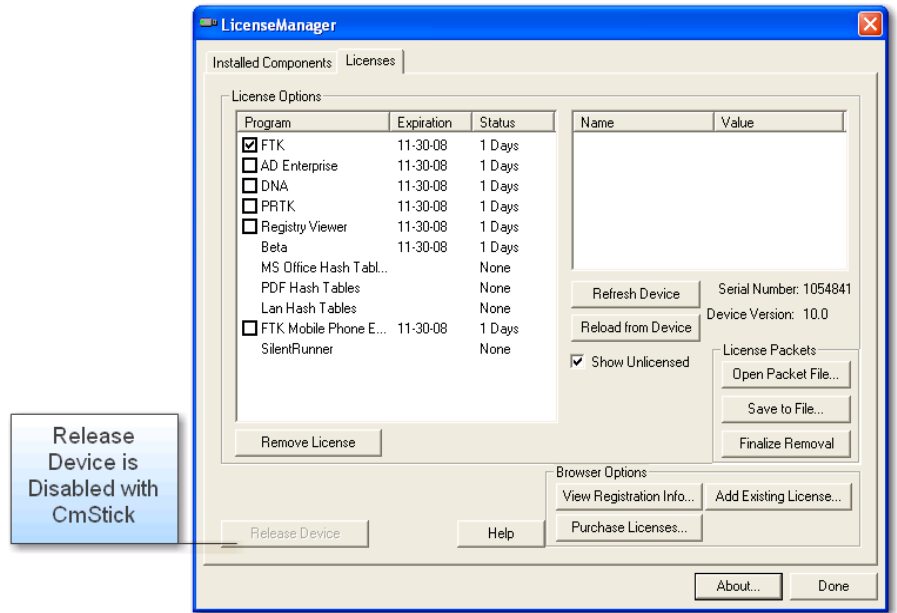
| Item                  | Description   |
|-----------------------|---|
| Install Newest Button | Installs the newest version of the programs checked in the product window. You can also get the latest versions from our website using your Internet browser. |
| Newest Button         | Downloads a list of AccessData's available products and their latest versions.  |
| 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 12-2 License Manager Licenses Tab



The Licenses tab provides the following information:

**TABLE 12-2 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.   |

**TABLE 12-2 LicenseManager Licenses Tab Features**

| Column          | Description  |
|-----------------|--|
| Value           | Shows the values of additional parameters or information a product requires 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 in the License tab:

**TABLE 12-3 License Management Options**

| Button                 | Function  |
|------------------------|---|
| 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.<br><br>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.  |

**TABLE 12-3 License Management Options**

| Button           | Function   |
|------------------|--|
| 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 SECURITY DEVICE PACKET FILES

Open or save security device packet files using LicenseManager. You must save a packet file to create it before you can open it.

To save a security device packet file, on the Licenses tab do the following:

1. Click *Save to File*.
2. The packet file is already named. The default folder is My Documents. Accept, or specify a different folder location for the .pkt file, then click *Save*.

**Note:** When started, LicenseManager attempts to read licensing and subscription information from the installed CodeMeter Stick. If the CodeMeter Stick is not installed, LicenseManager opens a browse window to locate a security device packet file.

To open a security device packet file, open the Licenses tab and do the following:

1. Click *Open Packet File*.
2. Browse for a security device packet file to open, then click *Open*.

## VIEWING PRODUCT LICENSES

LicenseManager lets you view product license information for products registered (or associated) with your CodeMeter Stick or security device packet file.

To view product licenses that are currently associated with the connected CodeMeter Stick, click *Reload from Device*.

To view all available product licenses that are or can be associated with a CodeMeter Stick (according to Web site database), click *View Registration Info*.

To synchronize a CodeMeter Stick with the product license information in the AccessData Web site database, click *Refresh Device*.

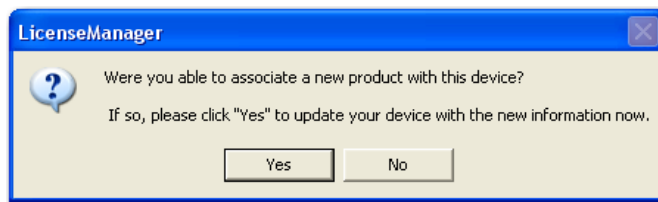
## ADDING AND REMOVING PRODUCT LICENSES

On a computer with an Internet connection, LicenseManager adds or removes available product licenses on a CodeMeter Stick.

### ADDING A PRODUCT LICENSE

To add, or “bind” an existing product license follow these steps:

1. Click the Licenses tab
2. Click *Add Existing License*.
3. On the Web site that comes up, click the box labeled *Bind* to select the product license you want to add.
4. Click *Submit*.
5. The Web site displays a window confirming the license has been associated with the attached security device.
6. Close the internet browser.



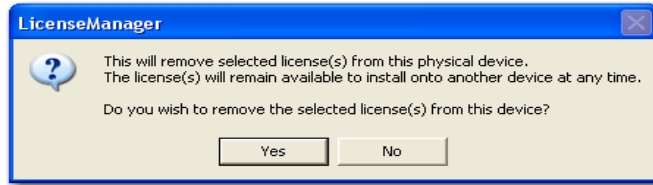
7. Click *Yes* when the LicenseManager prompts, “Were you able to associate a new product with this Device?”
8. Click *OK* on the Packet Update Successful dialog.

### REMOVE A PRODUCT LICENSE

The following steps help to remove, or “unbind,” a product license from the current CodeMeter Stick or dongle in the computer:

1. Open LicenseManager
2. Click the Licenses tab.
3. Select the program licenses to remove.

4. Click *Remove License*.



5. Click *Yes*.
6. Click *OK* on the Packet Update Successful dialog.
7. Close the Web browser.

**Note:** The licenses remain under your name and your control. They are simply “unbound” from the device they were bound to, and remain available to be re-bound to the same device later, or bound to a different device.

## MANAGING PRODUCT LICENSES ON ISOLATED MACHINES

When unable to connect to the Internet, the easiest way to move licenses from one CodeMeter Stick to another is to physically move the CodeMeter Stick to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, then physically move the CodeMeter Stick back to the original computer. However, if the CodeMeter Stick cannot be moved or removed from its current machine or area and there is no machine available with Internet access or email, contact your AccessData Sales Representative for special instructions.

### ADDING OR REMOVING A PRODUCT LICENSE ON AN ISOLATED MACHINE

To add (associate) a product license do the following:

1. On the computer where the CodeMeter Stick resides do the following:
  - 1a. Click *Reload from Device* in the Licenses tab to read the CodeMeter Stick license information.
  - 1b. Save the security device packet file to the local machine.
2. Copy the security device packet file to a computer with an Internet connection.
3. On the computer with an Internet connection:
  - 3a. Open the copied security device packet file in LicenseManager.
  - 3b. Click *Add Existing License*.

Ignore the prompt for now; you will answer it in the next step. Complete the process to add a product license on the Web site instead. When complete, move to the next step.

- 3c. Click *Yes* when the LicenseManager prompts, “Were you able to associate a new product with this security device?”

When LicenseManager does not detect a dongle or the serial number of the security device does not match the serial number in the dongle packet file, it prompts to save the updated file (an executable).

4. After the update file is downloaded, copy the update file to the computer where the dongle resides.
5. On the computer where the dongle resides do the following:
  - 5a. Run the update file.
  - 5b. Click *Reload From Device* in the Licenses tab to verify the product license has been added to the dongle.

**Note:** On the computer with an Internet connection, click *View > Registration Info* in LicenseManager to see license information for associated and unassociated product licenses.

## REMOVING A PRODUCT LICENSE FROM AN ISOLATED MACHINE

To remove (unbind) a product license:

1. On the computer where the dongle resides do the following:
  - 1a. Click *Reload from Device* in the Licenses tab to read the dongle license information.
  - 1b. Save the security device packet file to the local machine.
2. Copy the file to a computer with an Internet connection.
3. On the computer with an Internet connection:
  - 3a. Open the copied security device packet file in LicenseManager.
  - 3b. Select the product license to unbind then click *Remove License*.
  - 3c. When prompted to remove the selected license from the security device, 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, LicenseManager prompts to save the update file.
  - 3d. Save the updated 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. Double-click to execute the update file.
    - 5b. Click *Reload From Device* in the Licenses tab to verify the product license is removed from the dongle.
    - 5c. Save the security device packet file to the local machine.
  6. Copy the file to a computer with an Internet connection.
  7. On the computer with an Internet connection:
    - 7a. Open the copied security device packet file in LicenseManager.
    - 7b. Click *Finalize Removal*.
- Note:** On the computer with an Internet connection, click *View > Registration Info* in LicenseManager to see license information for associated and unassociated product licenses.

## UPDATING PRODUCTS

Use LicenseManager to check for product updates and download the latest product versions.

For more information on the general features of the subscription service, contact your AccessData Sales Representative.

### CHECKING FOR PRODUCT UPDATES

When checking for updates, LicenseManager checks for an updated version of LicenseManager. If there is one, a prompt appears. When prompted whether to update LicenseManager, click *Yes* to download and install the latest product version of LicenseManager, or click *No* to update product version information for the products listed in the LicenseManager window.

To check for product updates, click *Newest* from the Installed Components tab.

To determine whether you have the latest version of a product, check for updates, then compare the installed version with the latest version number listed in the Products window.

### DOWNLOADING PRODUCT UPDATES

To download a product update do the following:

1. Ensure that LicenseManager displays the latest product information.
2. Check the programs to download.
3. Click *Install Newest*.
4. When prompted, click *Yes* to download the latest install program for that product.
5. Follow the installation wizard to install the product update.

**Note:** Due to the size and nature of certain of AccessData programs, downloading updates for those programs is not practical or possible. These programs include FTK2.x, Enterprise, eDiscovery, and SilentRunner. The FTK2.x installer can be downloaded from the AccessData Support website, but the others cannot at this time. You will need to contact your AccessData Sales Representative for updates to Oracle (there are none at this time), Enterprise, eDiscovery, and SilentRunner, as they become available.

## PURCHASING PRODUCT LICENSES

Use LicenseManager to link to the AccessData Web site to purchase products.

To purchase a product, click *Purchase Licenses* from the Licenses tab.

**Note:** Once a product has been purchased and appears in the AccessData License Server, add the product license to a CodeMeter Stick, dongle, or security device packet file by clicking *Refresh Device*.

## SENDING A SECURITY DEVICE PACKET FILE TO SUPPORT

Send a security device packet file *only* when specifically directed to do so by AccessData support.

To send a security device packet file, email a security device packet file to [support@accessdata.com](mailto:support@accessdata.com).

# SELECTING THE APPLICATION LANGUAGE

Use the Language Selector tool to choose the language in which the FTK interface is displayed. Language Selector is not installed with FTK and must be installed to change FTK2's language. Select one of the following languages:

**TABLE 12-4 Available Application Languages**

---

|              |            |
|--------------|------------|
| Chinese      | German     |
| Dutch        | Italian    |
| English (US) | Japanese   |
| French       | Spanish    |
| Korean       | Portuguese |
| Hindi        | Russina    |
| Swedish      | Turkish    |

Selections take effect with an application.



# *Appendix A Recognized File Types*

This appendix lists the different file types that are recognized by AccessData (AD) FTK2. The file type is a string in the document header that identifies the program used to create the document. AD FTK2 looks at the document headers to identify the file types.

## DOCUMENT FILE TYPES

The following table lists the AD FTK2 recognized document file types:

**TABLE A-1 Document File Types**

|                           |  |
|---------------------------|--|
| 7-Bit Text                | Acrobat Portable Document Format (PDF) |
| Ami Pro Document          | Ami Pro Snapshot                       |
| Ami Professional          | AreHangeul                             |
| CEO Word                  | CEO Write                              |
| CHTML (Compact HTML)      | Cyrillic (Ansi 1251)                   |
| Cyrillic (KOI8-R)         | DEC DX 3.0 and lower                   |
| DEC DX 3.1                | DisplayWrite 4                         |
| DisplayWrite 5            | Enable Word Processor 3.x              |
| Enable Word Processor 4.x | Excel 2000 Save As... HTML             |
| FTDF                      | Hana                                   |

**TABLE A-1 Document File Types**

---

|  |                                   |
|--|-----------------------------------|
| HDML (Handheld Device Markup Language) | HTML - Central European           |
| HTML - Chinese Big5                    | HTML - Chinese EUC                |
| HTML - Chinese GB                      | HTML - CSS                        |
| HTML - Cyrillic (KOI8-R)               | HTML - Japanese EUC               |
| HTML - Japanese ShiftJIS               | HTML - Korean Hangul              |
| HTMLAG                                 | HTMLWCA                           |
| Hypertext Document                     | IBM DCA/RFT                       |
| IBM FFT                                | IBM Writing Assistant             |
| IchiTaro 3                             | IchiTaro 4                        |
| IchiTaro 8                             | Interchange File Format Text File |
| Interleaf                              | Interleaf (Japanese)              |
| JustWrite 1                            | JustWrite 2                       |
| Legacy                                 | Legacy Clip                       |
| Lotus Manuscript 1                     | Lotus Manuscript 2                |
| Lotus screen snapshot                  | MacWrite II                       |
| Mass 11                                | Mass 11 (Vax)                     |
| Matsu 4                                | Matsu 5                           |
| Microsoft Windows Write                | Microsoft Word 1 Document         |
| Microsoft Word 2 Document              | Microsoft Word 2000 Document      |
| Microsoft Word 3 Document (Mac)        | Microsoft Word 4 Document (DOS)   |
| Microsoft Word 4 Document (Mac)        | Microsoft Word 5 Document (DOS)   |
| Microsoft Word 5 Document (Japanese)   | Microsoft Word 5 Document (Mac)   |
| Microsoft Word 6 Document              | Microsoft Word 6 Document (DOS)   |
| Microsoft Word 6 Document (Mac)        | Microsoft Word 7 Document         |
| Microsoft Word 8 Document (Mac)        | Microsoft Word 97 Document        |
| Microsoft Word Document                | Microsoft Works (Windows)         |
| Microsoft Works 1                      | Microsoft Works 2                 |
| Microsoft Works 2 (Mac)                | MIFF                              |
| MIFF 3                                 | MIFF 3 (Japanese)                 |
| MIFF 4                                 | MIFF 4 (Japanese)                 |
| MIFF 5                                 | MIFF 5 (Japanese)                 |
| MIFF 5.5                               | MIFF 6                            |

---

**TABLE A-1 Document File Types**

---

|                                |                                 |
|--------------------------------|---------------------------------|
| MIFF 6 Japanese                | MS Works/Win 3 (Windows)        |
| MS Works/Win 4                 | MultiMate 3.6                   |
| MultiMate 4                    | MultiMate Advantage II          |
| MultiMate Note                 | Navy DIF                        |
| OfficeWriter                   | P1                              |
| PC File 5.0 - Letter           | PerfectWorks 1                  |
| PFS: First Choice 2.0          | PFS: First Choice 3.0           |
| PFS: WRITE A                   | PFS: WRITE B                    |
| Pocket Word                    | PowerPoint 2000 Save As... HTML |
| Professional Write 1           | Professional Write 2            |
| Professional Write PLUS        | Professional Write PLUS Clip    |
| Q&A Write                      | Q&A Write 3                     |
| Rainbow                        | Rich Text Format                |
| Rich Text Format (Japanese)    | Samna                           |
| Signature                      | SmartWare II                    |
| Sprint                         | StarOffice Writer 5.2           |
| TotalWord                      | Unicode Text Document           |
| vCard Electronic Business Card | Volkswriter                     |
| Wang                           | WangIWP                         |
| WML - Chinese Big 5            | WML - Chinese EUC               |
| WML - Chinese GB               | WML - CSS                       |
| WML - Cyrillic 1251            | WML - Cyrillic KOI8             |
| WML - Japanese EUC             | WML - Japanese JIS              |
| WML - Japanese Shift JIS       | WML - Korean Hangul             |
| WML - Latin 2                  | Word 2000 Save As... HTML       |
| WORDMARC                       | WordPad                         |
| WordPerfect 4 Document         | WordPerfect 4.2                 |
| WordPerfect 5                  | WordPerfect 5 Asian             |
| WordPerfect 5 Mac              | WordPerfect 6.0                 |
| WordPerfect 6.0 Asian          | WordPerfect 6.0 Asian (Enh)     |
| WordPerfect 6.0 (Enh)          | WordPerfect 6.0 Mac             |
| WordPerfect 6.0 Mac (Enh)      | WordPerfect 6.1                 |

---

**TABLE A-1 Document File Types**

---

|                           |                             |
|---------------------------|-----------------------------|
| WordPerfect 6.1 Asian     | WordPerfect 6.1 Asian (Enh) |
| WordPerfect 6.1 (Enh)     | WordPerfect 6.1 Mac         |
| WordPerfect 6.1 Mac (Enh) | WordPerfect 7               |
| WordPerfect 7 Asian       | WordPerfect 7 Asian (Enh)   |
| WordPerfect 7 (Enh)       | WordPerfect 7 Mac           |
| WordPerfect 7 Mac (Enh)   | WordPerfect 8               |
| WordPerfect 8 Asian       | WordPerfect 8 Asian (Enh)   |
| WordPerfect 8 (Enh)       | WordPerfect 8 Mac           |
| WordPerfect 8 Mac (Enh)   | WordPerfect 9               |
| WordPerfect 9 (Enh)       | WordPerfect 9 Mac (Enh)     |
| WordPerfect 9 Mac         | WordPerfect Document        |
| Word Pro Document         | Word Pro 96 Document        |
| Word Pro 97 Document      | WordStar 4 and lower        |
| WordStar 5                | WordStar 5.5                |
| WordStar 6                | WordStar 7                  |
| WordStar 2000             | WordStar for Windows        |
| WPF Encrypt               | WPF Unknown                 |
| WPS Plus                  | WWrite ChineseBig5          |
| WWrite ChineseGB          | WWrite Hangeul              |
| WWrite Shift-JIS          | XHTMLB                      |
| XML                       | XyWrite / Nota Bene         |



# SPREADSHEET FILE TYPES

**TABLE A-2 Spreadsheet File Types**

|                                   |                                   |
|-----------------------------------|-----------------------------------|
| 1-2-3 1.A Document                | 1-2-3 2.0 Document                |
| 1-2-3 2.01 Document               | 1-2-3 3.0 Document                |
| 1-2-3 4.0 Document                | 1-2-3 97 Document                 |
| 1-2-3 Document                    | 1-2-3 Japanese Document           |
| 1-2-3 Seal Document               | CEO Spreadsheet                   |
| Enable SpreadSheet                | First Choice (Spreadsheet)        |
| Generic WKS format                | Lotus 1-2-3 2 (FRM)               |
| Lotus 1-2-3 6                     | Lotus 1-2-3 9                     |
| Lotus 1-2-3 OS/2 2                | Lotus 1-2-3 OS/2 Chart            |
| Lotus Symphony 1.0 Document       | Mac Works 2 (SS)                  |
| Microsoft Excel 2 Worksheet       | Microsoft Excel 2000 Worksheet    |
| Microsoft Excel 3 Workbook        | Microsoft Excel 3 Worksheet       |
| Microsoft Excel 4 Workbook        | Microsoft Excel 4 Workbook (Mac)  |
| Microsoft Excel 4 Worksheet       | Microsoft Excel 4 Worksheet (Mac) |
| Microsoft Excel 5 Worksheet (Mac) | Microsoft Excel 7 Worksheet       |
| Microsoft Excel 97 Worksheet      | Microsoft Excel Worksheet         |
| Microsoft Multiplan 4.x           | Mosaic Twin                       |
| MS Works Spreadsheet              | MS Works/Win 3 (SS)               |
| MS Works/Win 4 (SS)               | MS Works/Win Spreadsheet          |
| PFS Plan                          | PlanPerfect File                  |
| Quattro Pro 4                     | Quattro Pro 7.0 Graph             |
| Quattro Pro 9 for Windows         | Quattro Pro Notebook              |
| Quattro Pro Notebook 1.0          | Quattro Pro Notebook 1.0J         |
| Quattro Pro Notebook 3.0 (DOS)    | Quattro Pro Notebook 4.0 (DOS)    |
| Quattro Pro Notebook 5.0          | Quattro Pro Notebook 5.5 (DOS)    |
| Quattro Pro Notebook 6.0          | Quattro Pro Notebook 7.0          |
| Quattro Pro Notebook 8.0          | Smart SpreadSheet                 |
| SuperCalc 5                       | VP Planner                        |

# DATABASE FILE TYPES

**TABLE A-3 Database File Types**

|                       |                         |
|-----------------------|-------------------------|
| DBase IV/V File       | First Choice (Database) |
| Framework III         | Mac Works 2 (DB)        |
| Microsoft Project98   | Microsoft Works (DB)    |
| MS Jet 2 Database     | MS Jet 3 Database       |
| MS Jet 4 Database     | MS Jet Database         |
| MS Money 1 File       | MS Money 2 File         |
| MS Money 2000 File    | MS Money 3 File File    |
| Paradox 3             | MS Money 4 File         |
| MS Money 5 File       | MS Money 98 File        |
| MS Money File         | MS Works Database       |
| MS Works/Win 3 (DB)   | MS Works/Win 4 (DB)     |
| MS Works/Win Database | Organizer 1.1 File      |
| Organizer 2 File      | Organizer 3 File        |
| Organizer 4           | Paradox 3.5             |
| Paradox 4             | Paradox Database File   |
| Paradox Script File   | Quicken 5 File          |
| Quicken 6 File        | Quicken 98 File         |
| Quicken 99 File       | Q&A Database            |
| Quickbooks 2 File     | Quickbooks 2000 File    |
| Quickbooks 3.1 File   | Quickbooks 5 File       |
| Quickbooks 6 File     | Quickbooks 99 File      |
| Quickbooks File       | Quicken 2000 File       |
| Quicken 2001 File     | Quicken 3 File          |
| Quicken 4 File        | Quicken File            |
| RBase 5000            | RBase File 1            |
| RBase File 3          | RBase V                 |
| Reflex 2.0 Database   | Smart DataBasez         |

# GRAPHIC FILE TYPES

**TABLE A-4 Graphics File Types**

|   |   |
|---|---|
| Acrobat Portable Document Format (Mac)  | Adobe Illustrator                           |
| Adobe Photoshop File                    | Ami Professional Draw                       |
| Animated Cursor                         | Animatic Film File                          |
| Animation                               | AOL Art Files version 3.0                   |
| Apple Quicktime File                    | AutoCAD Drawing Exchange File               |
| AutoCAD Drawing Interchange (DXF-ASCII) | AutoCAD Drawing Interchange (DXF-Binary)    |
| AutoCAD DWG 12                          | AutoCAD DWG 13                              |
| AutoCAD Native Drawing Format (DWG)     | AutoCAD Native Drawing Format 14 (DWG)      |
| AutoCAD Drawing Exchange Format (DXB)   | Autodesk 3D Studio File                     |
| Autodesk Animator File                  | AutoShade (RND)                             |
| Bentley Microstation DGN                | Bitmap File                                 |
| CALS Raster File Format                 | Candy 4                                     |
| CAS Fax File                            | CCITT Group 3                               |
| Computer Graphic Metafile               | ComputerEyes Raw Data File                  |
| Harvard Graphics Presentation           | Corel Draw 2                                |
| HP Gallery                              | Hewlett Packard Graphics Language           |
| IBM Picture Interchange Format          | IBM Graphics Data Format (GDF)              |
| IGES Drawing                            | Icon  |
| JNG File (JPEG Network Graphics)        | Intel Digital Video File                    |
| JPEG/JFIF File                          | JPEG File Interchange Format                |
| Kodak Photo CD                          | Kodak Flash Pix (FPX)                       |
| Lotus screen snapshot                   | Lotus PIC                                   |
| Macintosh Picture 2                     | Macintosh Picture 1                         |
| Micrografx Designer (DRW)               | MAC-Paint File                              |
| MIFFG                                   | Micrografx File                             |
| Multi-page PCX (DCX)                    | MiNG File (Multiple-image Network Graphics) |
| Windows DIB                             | NEOChrome Animation File                    |
| Windows Metafile                        | Windows Icon                                |
| WordPerfect Graphic File                | WordPerfect Graphic (WPG)                   |
| Corel Draw 3                            | WordPerfect MAC SOFT Graphics               |
| Corel Draw 5                            | Corel Draw 4                                |
| Corel Draw 7                            | Corel Draw 6                                |
|   | Corel Draw 8                                |

**TABLE A-4 Graphics File Types**

---

|  |                             |
|--|-----------------------------|
| Acrobat Portable Document Format (Mac) | Adobe Illustrator           |
| Corel Draw 9                           | Corel Draw Clipart          |
| Cursor                                 | Cyber Paint Sequence File   |
| DrawPerfect File                       | Dual PowerPoint 95/97       |
| Encapsulated PostScript (EPS)          | Enhanced Windows Metafile   |
| Excel 3 Chart                          | Excel 4 Chart               |
| Excel 5 Chart                          | Excel Chart                 |
| Framemaker                             | Freelance                   |
| Freelance 96                           | GEM Bitmap (IMG)            |
| GEM IMG File                           | GEM Metafile                |
| GIF File                               | Graphic File                |
| Hanako 1                               | Hanako 2                    |
| Harvard Graphics                       | Harvard Graphics 2.x Chart  |
| Harvard Graphics 3.x Chart             | OS/2 PM Metafile            |
| OS/2 Warp Bitmap                       | Paintshop Pro (PSP)         |
| PCPAINT File                           | PCX Paintbrush File         |
| PNG File (Portable Network Graphics)   | Portable Bitmap (PBM)       |
| Portable Graymap (PGM)                 | Portable Pixmap (PPM)       |
| PostScript                             | PowerPoint 2000             |
| PowerPoint 3                           | PowerPoint 3 (Mac)          |
| PowerPoint 4                           | PowerPoint 4 (Mac)          |
| PowerPoint 7                           | PowerPoint 97/98            |
| Progressive JPEG                       | Sun Raster File             |
| Targa File                             | TIFF File                   |
| Video Clip                             | Visio 2000                  |
| Visio 4                                | Visio 5                     |
| WordPerfect Presentations              | WordPerfect Presentations 7 |
| XBM - X-Windows Bitmap                 | XPM - X-Windows Pixmap      |
| XWD - X-Windows Dump                   |                             |

## EMAIL MESSAGE PROGRAMS

AD FTK2 handles email messages differently from other categories. It recognizes the source of the email messages based on email archives and special headers.

AD FTK2 includes extended support for AOL including buddy lists, global settings, user history, URL history, thumbnail extraction, and address book extraction.

The following are supported email applications:

**TABLE A-5 Supported Email Applications**

|                 |             |
|-----------------|-------------|
| AOL             | Earthlink   |
| Eudora          | Hotmail     |
| Lotus Notes     | MSN Email   |
| Netscape        | Outlook     |
| Outlook Express | ThunderBird |
| Yahoo           |             |

## INSTANT MESSAGING PROGRAMS

AD FTK2 can recover instant messaging chat logs, if set to save conversations locally, and additional information such as buddy lists.

The following are supported instant messaging applications:

**TABLE A-6 Supported Instant Messaging Programs**

|                 |               |
|-----------------|---------------|
| AOL IM          | Google Chat   |
| Yahoo Messenger | MSN Messenger |

## EXECUTABLE FILE TYPES

AD FTK2 recognizes these executable file types:

**TABLE A-7 Recognized Executable File Types**

|                       |                             |
|-----------------------|-----------------------------|
| Executable File (EXE) | Executable File (COM)       |
| JavaScript            | NT Executable File          |
| OS/2 Executable File  | Windows VxD Executable File |

# ARCHIVE FILE TYPES

AD FTK2 Identifies but does not extract the following file types:

**TABLE A-8 Identified Archive File Types**

| File Types Identified but not Extracted | File Types Identified and Extracted |
|---|-------------------------------------|
| ARC Archive                             |                                     |
| BestCrypt GOST/BLOWFISH                 |                                     |
| BestCrypt GOST/DES                      |                                     |
| BestCrypt GOST/GOST                     |                                     |
| BestCrypt GOST/TWOFISH                  |                                     |
| BestCrypt GOST/Unknown                  |                                     |
| BestCrypt SHA/BLOWFISH                  |                                     |
| BestCrypt SHA/DES                       |                                     |
| BestCrypt SHA/GOST                      |                                     |
| BestCrypt SHA/TWOFISH                   |                                     |
| BestCrypt SHA/Unknown                   |                                     |
| BestCrypt Unknown Key Generation        |                                     |
| CAB Archive                             |                                     |
|   | Email Archive                       |
| GZIP Archive                            |                                     |
| Jetico BestCrypt Container              |                                     |
|   | MS Exchange/Outlook                 |
| Old Format PGP Secret Key Ring          |                                     |
|   | OLE Archive                         |
|   | OLE Embedded Object                 |
|   | OLE Embedded Storage Container      |
|   | Outlook Express 5 Archive           |
|   | Outlook Express Archive             |
| PGP Disk 4.0 File                       |                                     |
| PGP Disk File                           |                                     |
| PGP Secret Key Ring                     |                                     |
|   | PK Zip Archive                      |

**TABLE A-8 Identified Archive File Types**

| File Types Identified but not Extracted | File Types Identified and Extracted |
|---|-------------------------------------|
|   | Self-Extracting Zip Archive         |
| Stuffit Archive                         |                                     |
|   | Thumbs.db Thumbnail Graphics        |
| UNIX TAR Archive                        |                                     |
|   | Zip Archive                         |

**OTHER KNOWN FILE TYPES**

AD FTK2 identifies and adds the following known file types to a case:

**TABLE A-9 Other Known File Types**

|   |   |
|---|---|
| 8 Bit Sample Voice                              | Access File                               |
| Access System File                              | AccessData Recovery 5.0 Biographical Data |
| AccessData Recovery 5.0 Biographical Dictionary | AccessData Recovery 5.0 Dictionary        |
| AccessData Recovery 5.0 Hard Drive Dictionary   | AccessData Recovery 5.0 Password Data     |
| AccessData Recovery 5.0 Profile Data            | AccessData Recovery 5.0 Status Report     |
| ACT File  | Address Book Entry                        |
| Appointment                                     | Approach                                  |
| Audio Clip                                      | Audio Director                            |
| Audio Flash                                     | Contact Information                       |
| Drive Free Space                                | Email Folder                              |
| Encapsulated PostScript File                    | Envoy                                     |
| Envoy 7   | Escher                                    |
| File Slack                                      | File System Slack                         |
| Help File                                       | ICF                                       |
| Internet Cookie File                            | Internet Explorer Link Files              |
| Journal Entry                                   | LZH Compress                              |
| Microsoft Office Binder                         | MIDI Sequence                             |
| MPEG Version 1.0                                | MPEG Version 2.0                          |

**TABLE A-9 Other Known File Types**

---

|  |  |
|--|--|
| 8 Bit Sample Voice                       | Access File                              |
| MPEG Version 2.5                         | QuickFinder                              |
| Sample Music                             | Scheduler File                           |
| Self-Extracting LZH                      | Shortcut FileSticky Note                 |
| UNIX Compress                            | Wave Sound                               |
| Win95 Screensaver Settings               | Windows Clipboard File                   |
| Windows Swap File                        | WordPerfect 4.2 (Vax)                    |
| WordPerfect Application Resource Library | WordPerfect Block File                   |
| WordPerfect Calculator                   | WordPerfect Calendar                     |
| WordPerfect Character Map                | WordPerfect Column Block                 |
| WordPerfect Dictionary                   | WordPerfect Dictionary -- Rules          |
| WordPerfect Display Resource File        | WordPerfect Equation Resource            |
| WordPerfect External Spell Code Module   | WordPerfect External Spell Dictionary    |
| WordPerfect File Manager                 | WordPerfect Graphic Driver               |
| WordPerfect Help File                    | WordPerfect Hyph Lex Module              |
| WordPerfect Hyphenation Code Module      | WordPerfect Hyphenation Data Module      |
| WordPerfect InForms 1                    | WordPerfect Install Options              |
| WordPerfect Keyboard Definition          | WordPerfect Macro Editor                 |
| WordPerfect Macro File                   | WordPerfect Macro Resource               |
| WordPerfect Mouse Driver                 | WordPerfect Notebook                     |
| WordPerfect Office                       | WordPerfect Overlay File                 |
| WordPerfect Printer                      | WordPerfect Printer Q Codes              |
| WordPerfect Printer Resource File        | WordPerfect Program Editor               |
| WordPerfect Rectangular Block            | WordPerfect Rhymmer Pronunciation        |
| WordPerfect Rhymmer Word File            | WordPerfect Scheduler                    |
| WordPerfect Setup File                   | WordPerfect Shell                        |
| WordPerfect Spell Code Module--Rules     | WordPerfect Spell Code Module--Word List |
| WordPerfect Thesaurus                    | WordPerfect Unix Setup File              |
| WordPerfect Vax Keyboard Definition      | WordPerfect Vax Setup                    |







# *Appendix B File Systems and Drive Image Formats*

This appendix lists the file systems and image formats that AD FTK2 analyzes.

## **FILE SYSTEMS**

- FAT 12, FAT 16, FAT 32
- NTFS
- Ext2, Ext3
- HFS, HFS+
- ReiserFS 3

## **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**

- Alcohol (\*.mds)
- CloneCD (\*.ccd)
- ISO
- IsoBuster CUE
- Nero (\*.nrg)
- Pinnacle (\*.pdi)
- PlexTools (\*.pxi)
- Roxio (\*.cif)
- Virtual CD (\*.vc4)

# *Appendix C Recovering Deleted Material*

AD FTK2 finds deleted files on the supported file systems by their file header.

## **FAT 12, 16, AND 32**

When parsing FAT directories, AD FTK2 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, AD FTK2 computes the total number of clusters (N) occupied by the file.

AD FTK2 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.

AD FTK2 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.

AD FTK2 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

AD FTK2 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

AD FTK2 searches to find inodes that are marked deleted. The link count is zero and the deletion timestamp is nonzero.

For each deleted inode, AD FTK2 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.

AD FTK2 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

AD FTK2 does not recover deleted files from ext3 volumes because ext3 zeroes out a file's indirect block pointers when it is deleted.

## HFS

AD FTK2 does not recover deleted files from HFS.





# Appendix D Program Files

The following tables list key FTK2 files and folders, their functions, and their locations.

## FILES AND FOLDERS FOR THE APPLICATION

These files and folders exist on the computer running FTK.

| File or Folder          | Location  | Function  |
|-------------------------|---|---|
| FTK2-Data (shared)      | Root of system drive or partition (C:\ftk2-data\)                     | Contains all case data not stored in the database.  |
| summary_install_log.txt | C:\Program Files\AccessData\AccessData Forensic Toolkit 2             | Points to a set of log files including a summary installation log to help Technical Support with troubleshooting. |
| KFF Logs                | C:\Program Files\AccessData\AccessData Forensic Toolkit 2             | Records whether the Known File Filter was added to the schema.  |
| FTK2.exe                | C:\Program Files\AccessData\AccessData Forensic Toolkit 2\Application | Program executable  |
| FTK2_log.txt            | C:\Program Files\AccessData\AccessData Forensic Toolkit 2\Application | Log file recording information specific to the application.   |

---

| File or Folder           | Location  | Function                                     |
|--------------------------|---|--|
| FTK2crash[timestamp].dmp | C:\Program Files\AccessData\AccessData Forensic Toolkit 2\Application | Dump file with a timestamp from an FTK crash |

## FILES AND FOLDERS FOR THE DATABASE

These files and folders exist on the computer running the Oracle database.

---

| File or Folder | Location                          | Function  |
|----------------|-----------------------------------|---|
| ftk2           | C:\Oracle                         | Contains files FTK uses to work with the Oracle database, such as JRE, libraries, configuration scripts, etc. |
| logs           | C:\Program Files\Oracle\Inventory | Contains installation logs intended to help Technical Support with installation troubleshooting.              |
| FTK2_KFF.DBF   | C:\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.

### CHANGING THE LOGGING REGISTRY OPTIONS

To make changes in the registry for the available logging options do the following:

1. Click *Start > Run*.
2. Enter **regedit** and click **OK**.
3. Open **HKLM\SOFTWARE\AccessData\Shared\Version Manager\sds\**
4. Change any of the following values to the desired setting:
  - **errorlog** = controls if LOG\_WARN/LOG\_ERROR logs to ftkWorker.errorlog.txt (defaults to 1)

- infolog = controls if LOG\_INFO logs to ftkWorker.infolog.txt (defaults to 1)
- userlog = controls if LOG\_USER logs to ftkWorker.userlog.txt (defaults to 0)  
This is required by ediscovery.
- tracelog = controls LOG\_TRACE logs to ftkWorker.tracelog.txt (defaults to 0)  
Logs object created/complete messages.
- memlog = controls memory logging to ftkWorker.infolog.txt (defaults to 0)
- timelog = controls time logging to ftkWorker.infolog.txt (defaults to 0)

**Note:** Log files initialize when **ftkworker.exe** starts. Registry keys read only during the startup process.

## CHATTY WORKER

In the worker diagnostic page, "Chatty" now controls if the worker LEVEL\_\* logs to stdout/stderr (therefore showing up in the text pane).



# *Appendix E Securing 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 in Windows Registry Editor.

The files that make up the registry differ depending on the version of Windows. The tables below list the registry files for each version of Windows, along with their locations and the information they contain.

## WINDOWS 9X REGISTRY FILES

The following table describes each item on the Windows 9x registry files:

**TABLE E-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<sup>*</sup> 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<br><br>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 E-2 Windows NT and Windows 2000 Registry Files**

| Filename   | Location   | Contents   |
|------------|--|--|
| NTUSER.DAT | \Documents and Settings\user account<br>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 E-3 Windows XP Registry Files**

| Filename   | Location   | Contents   |
|------------|--|--|
| NTUSER.DAT | \Documents and Settings\user account<br><br>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 9x systems, the registry hives are as follows:

- HKEY\_CLASSES\_ROOT (HKCR)



- HKEY\_CURRENT\_USER (HKU)
- HKEY\_LOCAL\_MACHINE (HKLM)
- HKEY\_USERS (HKCU)
- HKEY\_CURRENT\_CONFIG (HKCC)
- HKEY\_KYN\_DATA (HKDD)

HKEY\_LOCAL\_MACHINE and HKEY\_USERS are the root hives. They contain information that is used to create the HKEY\_CLASSES\_ROOT, HKEY\_CURRENT\_USER, and HKEY\_CURRENT\_CONFIG hives.

HKEY\_LOCAL\_MACHINE is generated at startup from the system.dat file and contains all the configuration information for the local machine. For example, it might have one configuration if the 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 E-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 <code>DWORD_LITTLE_ENDIAN</code> (least significant byte is at the lowest address) and <code>REG_DWORD_BIG_ENDIAN</code> (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 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.   |

**TABLE E-4 Possible Data Types**

| Data Type                    | Name         | Description  |
|------------------------------|--------------|--|
| REG_FULL_RESOURCE_DESCRIPTOR | Binary Value | A series of nested arrays deigned to store a resource list used by a physical hardware device. This data is displayed in hexadecimal format as a Binary Value. |
| REG_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.
- 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:

- Boot the suspect's image to view his or her registry in Registry Editor.
- Mount a restored image as a drive, launch Registry Editor at the command line from your processing machine, export the registry files from the restored image, then view them in a third-party tool.

**Note:** The problem with this method is that you can only view the registry as text. Registry Editor displays everything in ASCII so you can't see hex or binary values in the registry.

- Export the registry files from the image and view them in a third-party tool.
- Use Registry Viewer. Registry Viewer integrates seamlessly with AD FTK2 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. 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 registry.

## SYSTEM INFORMATION

**TABLE E-5 System Information**

| Information             | File     | 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.  |

**TABLE E-5 System Information**

|                      |          |   |   |
|----------------------|----------|---|---|
| Logon Banner Message | Software | Microsoft\Windows\Current Version\Policies\System\Legal NoticeCaption | User-defined data.  |
| Time Zone            | System   | ControlSet001(or002)\Control\TimeZoneInformation\Standard Name        | This information is entered during installation, but can be modified later. |

## NETWORKING

**TABLE E-6** Networking

| Information                          | File       | 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 E-7** User Data

| Information | File       | Location                                      | Description   |
|-------------|------------|---|---|
| Run         | NTUSER.DAT | Software\Microsoft\Windows\CurrentVersion\Run | Programs that appear in this key run automatically when the user logs on. |



**TABLE E-7 User Data**

|  |            |   |  |
|--|------------|---|--|
| Media Player<br>Recent List                | NTUSER.DAT | Software\Microsoft\Media<br>Player\Player\ RecentFileList             | This key contains the user's<br>most recently used list for<br>Windows Media Player.                   |
| O\S Recent<br>Docs                         | NTUSER.DAT | Software\Microsoft\Windows\<br>CurrentVersion\Explorer\<br>RecentDocs | MRU list pointing to shortcuts<br>located in the recent directory.                                     |
| Run MRU                                    | NTUSER.DAT | \Software\Microsoft\Windows\<br>CurrentVersion\Explorer\RunM<br>RU    | MRU list of commands<br>entered in the “run” box.  |
| Open And Save<br>As Dialog<br>Boxes MRU    | NTUSER.DAT | \Software\Microsoft\Windows\<br>CurrentVersion\Explorer\<br>ComDlg32  | MRU lists of programs\files<br>opened with or saved with the<br>“open” or “save as” dialog<br>box(es). |
| Current Theme                              | NTUSER.DAT | Software\Microsoft\Windows\<br>CurrentVersion\Themes                  | Desktop theme\wallpaper.   |
| Last Theme                                 | NTUSER.DAT | Software\Microsoft\Windows\<br>CurrentVersion\Themes\Last<br>Theme    | Desktop theme\wallpaper.   |
| File Extensions\<br>Program<br>Association | NTUSER.DAT | Software\Microsoft\Windows\<br>CurrentVersion\Explorer\<br>FileExts   | Identifies associated programs<br>with file extensions.  |

## USER APPLICATION DATA

**TABLE E-8 User Application Data**

| Information                            | File       | Location  | Description   |
|--|------------|---|---|
| Word User Info                         | NTUSER.DAT | Software\Microsoft\office\<br>version\Common\UserInfo                           | This information is entered during installation, but can be modified later. |
| Word Recent Docs                       | NTUSER.DAT | Software\Microsoft\office\<br>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\<br>version\Outlook\Security                          | Location where attachments are stored when opened from Outlook.             |
| AIM                                    | NTUSER.DAT | Software\America Online\AOL Instant Messenger\<br>CurrentVersion\Users\username | IM contacts, file transfer information, etc.                                |
| Word User Info                         | NTUSER.DAT | Software\Microsoft\office\<br>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 MessengerService\*             | IM contacts, file transfer information, etc.                                |
| Kazaa                                  | NTUSER.DAT | Software\Kazaa\*  | Configuration, search, download, IM data, etc.                              |

**TABLE E-8 User Application Data**

|                       |            |                                       |  |
|-----------------------|------------|---------------------------------------|--|
| Yahoo                 | NTUSER.DAT | Software\Yahoo\Pager\Profiles\*       | IM contacts, file transfer information, etc. |
| Google Client History | NTUSER.DAT | Software\Google\NavClient\1.1\History |  |
| Adobe                 | NTUSER.DAT | Software\Adobe\*                      | Acrobat, Photo deluxe, etc.                  |



## *Appendix F Troubleshooting*

FTK2.1 is a complex program and troubleshooting can be challenging. While this section attempts to present some basic solutions to commonly asked questions, and directions for using AccessData Forensic Toolkit (FTK) Diagnostics Tools, it would not be practical to list every possibility here. Thus, this section is limited.

### **FINDING ANSWERS**

The most up-to-date troubleshooting and problem solving information is available on the AccessData website, in our Knowledgebase.

Here's how to get into the Knowledge Base:

1. Open your Internet browser to <http://www.accessdata.com/support.html>
2. Click on link to *KnowledgeBase*
3. Be sure to log in using "Sign In" link located at the upper right hand corner to see the majority of articles.
4. If you are unable to log in, please contact support at:  
support@accessdata.com or 800-658-5199

# TROUBLESHOOTING TABLES

The following table provides limited, basic information for troubleshooting FTK 2.1.

**TABLE F-1 FTK 2.1 Troubleshooting**

| Problem  | Suggested Resolution   |
|--|--|
| Application GUI cannot connect to the Oracle database.   | Ensure connectivity on port 1521.  |
| The File List pane may not always seem to correspond with the graphic selected.                                    | Refresh the File List pane to match up with the selected graphics. Press F5 or click <i>View &gt; Refresh</i> to manually update the view.   |
| The installer cannot connect to your Oracle database.  | Check to see if the Oracle host has been changed.<br>Test connectivity at port 1521.   |
| When you change the name or domain affiliation of the Oracle host, the Oracle instance on that host will not work. | Verify that the SYS password is entered correctly.<br>Changing the Host name or Domain affiliation causes the <b>FTK2.exe</b> connection to Oracle to fail. Windows will allow a workgroup or domain change at any time, and Oracle has no way to know about that change until you tell it. Since Oracle currently is using a fully qualified name, it fails when the domain or workgroup name changes.<br>Log in to the host running Oracle.<br>Stop the listener control program by entering “lsnrctl stop” at a command prompt.<br>From a text editor, open the file:<br><b>c:\Oracle\ftk2\NETWORK\ADMIN\listener.ora.</b><br>Edit the line containing the Oracle hostname. For example, if the Oracle hostname were changed from “privateeye” to “ciaoperative,” the line should be changed from (ADDRESS = (PROTOCOL = TCP)(HOST = privateeye)(PORT = 1521)) to: (ADDRESS = (PROTOCOL = TCP)(HOST = ciaoperative)(PORT = 1521))<br>Save the change and exit the text editor.<br>Restart the listener service by entering “lsnrctl start” at a command prompt. |

**TABLE F-1 FTK 2.1 Troubleshooting**

| Problem  | Suggested Resolution   |
|--|--|
| The file names listed in my Explorer tree have boxes in place of characters.   | The characters in the file name are non-ASCII, and the character set FTK is using does not have a character to represent the value contained in the file name.                       |
| Even after several minutes, the progress bar indicates that FTK is not processing the evidence I just added.   | The user that launched FTK2.1 may not have rights to access the computer on which the data is found. Manually change the user's access to the evidence.                              |
| User operates several non-Network License Service (NLS) applications but cannot open FTK 2.1 using an NLS license. Error message reads: "No more user licenses are available." | FTK 2.1 is looking on the local CmStick for a license. To correct the problem, remove the local CmStick. Launch FTK2.1, reattach the local CmStick for other applications to access. |

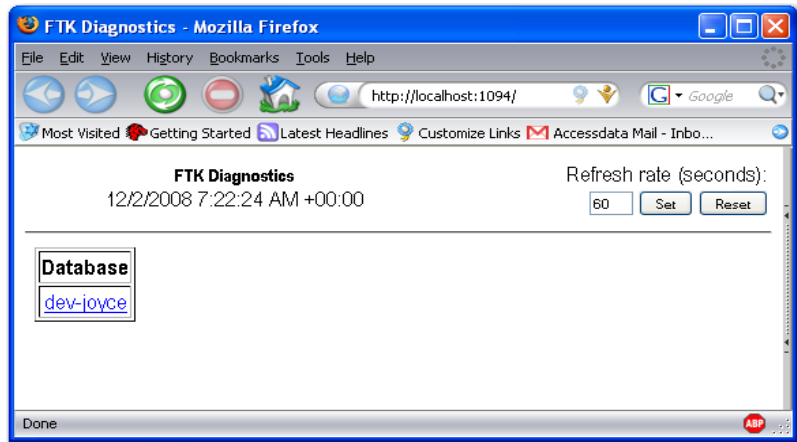
## DIAGNOSTICS TOOLS

FTK provides a Diagnostics tool to help troubleshoot problems with evidence processing. It also displays the activity of the databases where cases are stored and a list of the Worker machines assigned to each case.

## DATABASE DIAGNOSTICS

To access the FTK Database Diagnostics tool:

1. Select *Help > Diagnostics* to open the database in the browser.



2. Click on the database hostname link in the Database box. The FTK Version Management Diagnostics page opens. The page displays the following information:
  - Host IP address or hostname
  - Time and date of the host's connection
  - Refresh rate
  - GUI Information
    - Host ID
    - Version ID
    - User ID
    - Case ID number for each open case
  - Case Information ("Cases")
    - Case Number(s)
    - User logged in to work on that case
    - Worker Helper Status
    - Database Helper Status
  - Time and date at which the case was opened, in the following format:  
MM/DD/YYYY TimeHoursMinutesDecimalSeconds AM/PM.
  - Logging options



- Log of database activity

**FTK Version Management Diagnostic Page**  
 2008-12-02T07:24:54

Refresh rate (seconds):

| GUIs                |          |      |      |
|---------------------|----------|------|------|
| Host                | Version  | User | Case |
| dev-joyce.adata.com | 2.1.0[0] | 1002 |      |

| Cases |         |               |                 |
|-------|---------|---------------|-----------------|
| Case  | User(s) | Worker Helper | Database Helper |
| 1001  |         | -             | -               |

Logging Options: ☐ Also log to file ☐ Verbose

```

20081202T072216.549412 [?] Unregistering case <1002> at: dev-joyce.adata.com
20081202T035506.485878 [?] Registering case <1002> at: dev-joyce.adata.com
20081202T035502.419972 [?] Unregistering case <1001> at: dev-joyce.adata.com
20081202T012157.475765 [?] Registering case <1001> at: dev-joyce.adata.com
20081201T201016.741437 [?] Unregistering case <1040> at: dev-joyce.adata.com
20081201T154812.170941 [?] Registering case <1040> at: dev-joyce.adata.com
20081201T154734.005418 [?] Unregistering case <1001> at: dev-joyce.adata.com
20081201T052010.965173 [?] Registering case <1001> at: dev-joyce.adata.com
20081201T052005.902867 [?] Unregistering case <1002> at: dev-joyce.adata.com
20081201T035807.406661 [?] Registering case <1002> at: dev-joyce.adata.com
20081201T035758.745734 [?] Unregistering case <1001> at: dev-joyce.adata.com
20081201T025827.987882 [?] Registering case <1001> at: dev-joyce.adata.com
20081201T025819.607881 [?] Registering GUI at: dev-joyce.adata.com
20081201T025804.261620 [?] Listening on port: 6901      Diagnostics on port: 1097
  
```

## UNINSTALLING MANUALLY

If for any reason you need to uninstall FTK, and in particular in the case of a failed FTK 2.1 install, there are steps you can follow to ensure a successful uninstall. Do not try to reinstall FTK over the top of a failed installation. In this situation, it is essential to completely clean off the FTK components as described in this section, and then run the install again.

This section covers the steps necessary for a successful uninstall of FTK2.1.

## AUTOMATED UNINSTALL

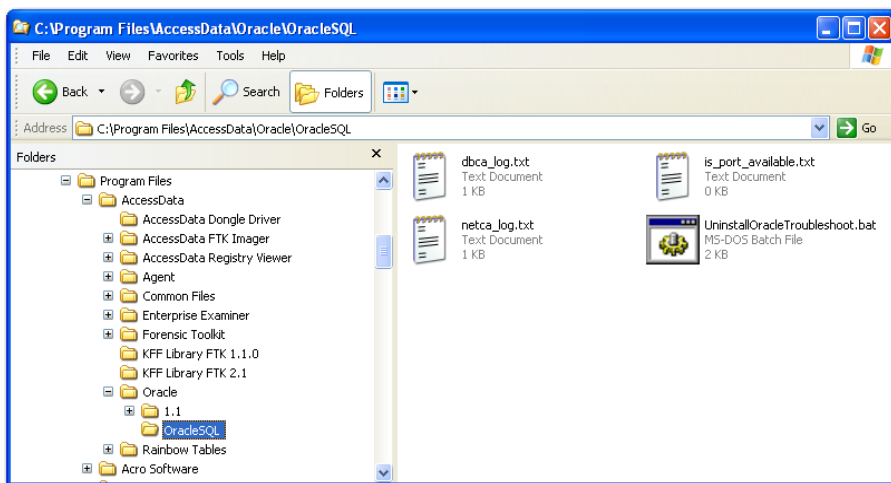
Try uninstalling in Add or Remove Programs in the Windows Control Panel. If for any reason this process fails, move to the instructions for Manually Uninstalling the Database.

## MANUALLY UNINSTALLING THE DATABASE

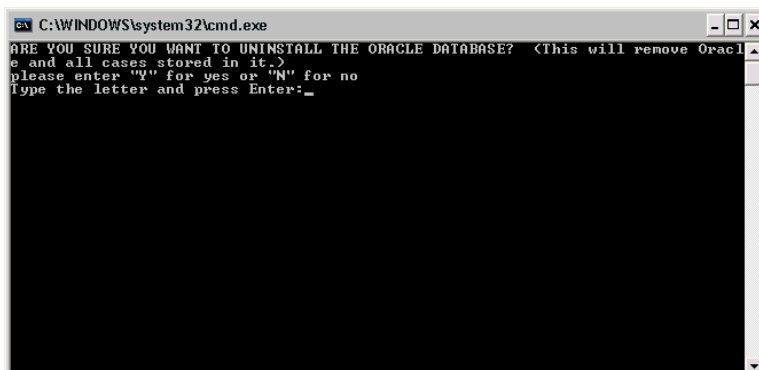
Carefully read and follow these instructions before attempting to run the installation again. All previously installed components should be cleared out before attempting to re-install.

If, for any reason, you are unable to uninstall the Oracle database using Windows Add or Remove Programs, you need to run the FTK Oracle uninstall .bat file.

1. Open Windows Explorer.
2. Browse to C:\Program Files\AccessData\Oracle\OracleSQL\.



3. Double-click *UninstallOracleTroubleshoot.bat*.



4. Answer Yes by typing "y."

5. Press enter.
6. Reboot (shutdown and restart) your system before continuing.

## FIND AND DELETE FTK FOLDERS AND KEYS

The first program folder to delete is the main program folder, `C:\Program Files\AccessData\Forensic Toolkit`.

## FIND AND DELETE FTK REGISTRY KEYS

Before continuing, AccessData recommends that you back up your registry. Run the Registry Editor. *Click File > Export*. Name the exported registry file. The default folder is My Documents. You may select a different location. When the name and location are specified, click *Save*.

These entries are numerous. Take great care deleting registry entries to avoid corrupting the OS or disabling another application's software.

These entries differ from FTK 2.0.2 to FTK 2.1.0 Both registry path sets are listed below.

1. From the Windows Run prompt, start regedit.
2. If uninstalling FTK 2.0.2, find and delete these keys:
  - `C:\Program Files\AccessData\Forensic Toolkit\2.0.2`
  - `C:\Program Files\AccessData\KFF Library FTK 2.0.2`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Forensic Toolkit`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\AccessData\Products\Forensic Toolkit`
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AccessData - Database Monitor`
  - `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AccessData - Worker Monitor`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{E6596466-BD67-490F-AC56-101DA884E90D}`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{556A689E-CA83-4FF7-976E-0F49BA6D048C}`
3. If uninstalling FTK 2.1, find and delete these keys:
  - `C:\Program Files\AccessData\Forensic Toolkit\2.1.0`

- C:\Program Files\AccessData\KFF Library FTK 2.1
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\GUID will not be known until final build.
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{6F9DBF75-D45D-4266-8854-ADCD6D74CB64}

## HANDLING ORACLE FOLDERS AND KEYS

The following steps are to be used in case of failure of the automated removal of the Oracle database through the batch file referenced in “Uninstalling Manually” on page 275.

### STOP ORACLE SERVICES

Before deleting the Oracle folders and registry keys stop the affected Oracle services that may be installed and running. The following lists the Oracle Services associated with FTK.

- OracleDBConsoleftk2
- Oracleftk2TNSListener
- OracleJobSchedulerFTK2
- OracleServiceFTK2

### DELETE ORACLE FOLDERS

Delete the following Oracle folders and their contents:

- C:\Program Files\Oracle
- C:\Oracle

### DELETE THE ORACLE KEYS

These entries are numerous, and you should take great care in deleting registry entries to avoid corrupting your OS, or disable some other applications software.

1. From the Windows Run prompt, start regedit.
2. Find and delete these registry keys:
  - C:\Oracle
  - C:\Program Files\AccessData\Oracle

- HKEY\_LOCAL\_MACHINE\SOFTWARE\AccessData\Oracle
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Oracleftk2TNS Listener
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\OracleJobSchedulerFTK2
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\OracleServiceFTK2
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\OracleDBConsoleftk2
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{25C2FB0D-7CC4-4B4E-B587-A12C549DF2AC} --Use for Version 1.2
- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\{25C2FB0D-7CC4-4B4E-B587-A12C549DF2AC} -- Use for Version 1.1

**Note:** Verify that C:\Oracle\ftk2\bin is not listed in the System Path Environment Variable.

## OTHER ISSUES

The following issues may also be encountered while using FTK.

### DTSEARCH NOISE FILE LIST

The noise file (**noise.dat**) shipped with FTK contains a list of common words like “is,” “about,” and “what” that are excluded from the case index when evidence is added. When these words are included in an index search, dtSearch allows any word to replace the noise word. If, for example, the string “what about bob” was searched, since the words “what” and “about” are included in the **noise.dat** file list, the search returns any hit with two words followed by the word “bob.”

Some cases require an empty or customized **noise.dat** file. The following steps are a way of creating an empty or customized **noise.dat** file.

1. Open the alerting the investigator toc:\Program Files\AccessData\Forensic Toolkit\2.1.0\bin folder.
2. Back up **noise.dat** by renaming it or copying and pasting it into the same folder.
3. Open **noise.dat** in a text editor.
4. Select all the words in the list.

5. Press Delete.
6. Add any words (if any) to the list that you wish to be considered “noise”. If you want the file to be empty, save it with no content.
7. Save the file as **noise.dat**.

## *Appendix G Corporate Information*

This appendix contains information about AccessData and its products.

### **CONTACTING ACCESSDATA CORPORATION BY MAIL**

Please send correspondence through the US Postal Service to:

AccessData Corp.  
384 South 400 West, Suite 200  
Lindon, Utah 84042  
USA

### **REGISTRATION**

AccessData provides a USB CodeMeter Stick with AD FTK2 as a registration compliance and security device that is configured as part of the installation process. It maintains AD FTK2 licensing and subscription information and is required to use AD FTK2.

In addition, the licensing of the product takes place when the product is purchased, and the licensing information is stored in our database. If you receive your CodeMeter Stick and it does not have a license on it, with the CodeMeter Stick connected, run

LicenseManager and refresh the device. If this does not resolve your issue, please contact Customer Support by phone or by email.

If you have sales questions or questions regarding the CodeMeter Stick and licensing issues, please contact your Sales Rep at 801-377-5410.

## TECHNICAL SUPPORT

AccessData offers free technical support on all of its software from 7:00 a.m. to 6:00 p.m. Mountain Standard Time. When contacting Customer Support by phone, please have your CodeMeter Stick or dongle serial number ready, and always include it in any email or fax correspondence. Please do not send a fax unless requested by a Support Agent.

**TABLE G-1 Contacting AccessData Support**

| Contact Us By | Using This Information   |
|---------------|--|
| Phone:        | 801.377.5410 (Toll)<br>800.658.5199 (Toll Free)  |
| Fax           | 800.765.4370; ATTN: Support  |
| Web site      | <a href="http://www.accessdata.com">http://www.accessdata.com</a><br><br>Product-specific FAQs that list common questions and their quick fixes.<br><br>Find both the AccessData Forum and the Online Support Form to submit support requests at <a href="http://www.accessdata.com/support">http://www.accessdata.com/support</a> . All support inquiries are typically answered within 24 hours. If there is an urgent need for support, contact AccessData via phone. |
| Email         | <a href="mailto:support@accessdata.com">support@accessdata.com</a>   |

## DOCUMENTATION

Please email any problems you find with the documentation to:  
**[documentation@accessdata.com](mailto:documentation@accessdata.com)**.



# *FTK Glossary*

## **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 computer 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.

## BestCrypt

A common symmetric encryption system that can be used with any of the following hash functions and encryption algorithms:

- GOST
- SHA-1 Hash
- Blowfish
- IDEA
- Twofish
- CAST
- AES
- RC6
- 3DES encryption

## 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 290.

## **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.

## **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).

## 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.

## **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.

## 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.

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.

## 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.

## 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 megabytes to several gigabytes, 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.

## 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.

## **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.

## **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.

## **Pretty Good Privacy**

A common symmetric encryption system used for exchanging files and email. It provides both privacy and authentication.

## **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  $\text{plaintext} \oplus \text{random-looking stream} = \text{random-looking ciphertext}$ . Because XOR is symmetric (in other words,  $[A \oplus B] \oplus B = A$ ), 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.

## **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.

## **(File and RAM) Slack**

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.

## Thumbnail

A smaller-sized version of a graphics image.

## 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.

## **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.



## A

- archiving
  - see backing up case 93

## B

- backing up case 93
- bookmarks 104
  - creating 105
  - export files to report 171
  - including in report 171
  - moving 114
  - tab 68
  - viewing 107

## C

- carved files
  - adding 81
- carving
  - see data carving 145
- case 35
  - adding evidence 95
  - backing up 93
  - creating 77
  - entering information in a report 169
  - indexing 82
  - processing of evidence 78
  - refining evidence 84
- Case Manager Window 36
- CmStick 36, 207, 209
- CodeMeter 36
- column headings
  - common 188
  - compressed 200
  - DOS 197
  - email 190
  - ext2 197
  - file status 195
  - file system 196
  - HFS 198
  - NTFS 199
  - Outlook/Exchange 193
  - stored hashes 190
  - Unix 200

- Creating 71
- custom identification file 83
- customizing 184
  - data carving 201
  - file list columns 186
  - tab layout 183
  - view panes 183

## D

- data carving 145
  - customizing 201
  - existing case 146
  - new case 81, 146
- Database File Types 239
- decrypted files
  - locating 80
- decrypting 161
  - viewing decrypted files 163
- diagnostics
  - workers 223
- docking
  - options 184
- Document File Types 234
- dongle 36, 209
- dtSearch 8, 82

## E

- EFS 161
  - decrypting files 80
- email
  - file types 243
  - window 68
- evidence
  - excluding from index 89
  - processing of 78
  - refining 84
- exporting
  - bookmarked files to report 171
  - files 118
  - index 138
  - registry files 121

## F

- file
  - exporting 118
- file category 60
- file content 50
  - filter tab 52
  - hex tab 53
  - natural tab 51
  - text tab 53
- file list columns
  - customizing 186
- file listing database 80
- file properties
  - in report 174
  - viewing 102
- file status 60, 61
- file types
  - email message 243
- filter 149
  - Known File Filter (KFF) 154
  - toolbar 149
- filtering
  - creating or modifying 152
- FTK 2 window 38
- FTK Imager 77

## G

- Graphic File Types 241

## H

- hardware acquisition tools 76
- hashing
  - databases of 9
  - overview of 8
  - sample of 8
- HashKeeper database 9
- hex interpreter 49
- hexadecimal 49
- HTML file listing 80

## I

- index
  - contents of 138
  - selecting 78

## L

License Manager  
    updating 216

## M

MD5  
    see Message Digest 5 8  
Message Digest 5 8  
    selecting 78

## N

NTFS 161, 249  
    decrypt EFS files 80

## O

or 35

## P

packet file 212  
partition  
    evidence item 278  
    NTFS 80, 249  
Password Recovery Toolkit 138, 204  
    features 205  
progress dialog 57  
Properties Pane 48  
PRTK  
    see Password Recovery Toolkit 204

## Q

QuickPicks 45  
QuickPicks Filter 56

## R

registry files 206  
Registry Viewer 206, 257  
regular expression 123  
reports  
    entering case information 169  
    including bookmarks in 171

- including list of file properties in 174
  - modifying 180
  - sample of 178
  - selecting location of 176
  - viewing 178
- roles 75

## S

- searching 8
  - regular expressions 129
- Secure Hash Algorithm 8
- Secure Hash algorithm
  - selecting 78
- security device 212
- SHA-1
  - see Secure Hash Algorithm 8
- software acquisition tools 76
- Spreadsheet File Types 238
- status 158

## T

- tab
  - Bookmark 68
  - Email 63
  - Explore 54
  - Graphics 65
  - Overview 58
  - Search 69
  - User-defined 71
- Tab Layout menu 183
- temporary file folder 200
- thumbnails
  - creating 78
  - marking 65
  - see Graphics Tab 66
- toolbar 45
  - file list 47

## U

- updating
  - products 216

## V

View menu 182

view panes

moving 183

## W

window

email 68

Windows Registry

file types 258

Windows 9x file types 258

Windows NT and 2000 file types 259

Windows XP file types 260