AccessData®

FTK® 2.2.1

FORENSIC TOOLKIT®

AccessData Forensic Toolkit 2.2

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.

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

www.accessdata.com

ACCESSDATA TRADEMARKS

AccessData® 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.

Forensic Toolkit® is a registered trademark of AccessData Corp.

FTK® is a registered 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.

DOCUMENTATION CONVENTIONS

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

A trademark symbol (®, ™, etc.) denotes an AccessData trademark. All third-party trademarks and copyrights are the 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**. For documentation issues, please email us at **documentation@accessdata.com**.

REGISTRATION

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

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

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

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

AccessData Contact Information

Mailing Address and General Phone Numbers

You can contact AccessData in the following ways:

TABLE FrontMatter-1 Mailing Address, Hours, and Department Phone Numbers

Corporate Headquarters	AccessData Corp. 384 South 400 West Suite 200 Lindon, UT 84042 USA **Voice**: 801.377.5410 **Fax**: 801-377-5426
General Corporate Hours:	Monday through Friday, 8:00 AM – 5:00 PM (MST) AccessData is closed on US Federal Holidays
State and Local Law Enforcement Sales	**Voice**: 800.574.5199, option 1 **Fax**: 801.765.4370 **Email**: Sales@AccessData.com
Federal Sales	**Voice**: 800.574.5199, option 2 **Fax**: 801.765.4370) **Email**: Sales@AccessData.com
Corporate Sales	**Voice**: 801.377.5410, option 3 **Fax**: 801.765.4370 **Email**: Sales@AccessData.com

TABLE FrontMatter-1 Mailing Address, Hours, and Department Phone Numbers

Training	**Voice**: 801.377.5410, option 6 **Fax**: 801-765-4370 **Email**: Training@AccessData.com
Accounting	**Voice**: 801.377.5410, option 4

TECHNICAL SUPPORT

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

TABLE FrontMatter-2 AccessData Customer & Technical Support Contact Information

Customer Service Hours:	Monday through Friday, 7:00 AM – 6:00 PM (MST)
Customer/Technical Support Free technical support is available on all AccessData products.	**Voice**: 801.377.5410, option 5 **Voice**: 800-658-5199 (Toll-free North America) **Email**: Support@AccessData.com **Website**: http://www.AccessData.com/Support

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

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

DOCUMENTATION

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

Table of Contents

Chapter 1 Introduction

This chapter provides an introduction to AccessData® (AD) Forensic Toolkit (FTK®) and information that you need to implement this powerful software in your enterprise.

Introduction to AccessData Forensic Toolkit

AccessData Forensic Toolkit is recognized around the world as the standard in computer forensic investigation technology. This court-validated platform delivers cutting edge analysis, decryption and password cracking all within an intuitive, customizable and user-friendly interface. In addition, with FTK you have the option of utilizing a back-end database to handle large data sets. You get the benefit of best-of-breed technologies that can be expanded to meet your ever-changing needs. Known for its intuitive functionality, email analysis, customizable data views and stability, FTK is the smart choice for stand-alone forensic investigations.

For more information about FTK, or any other AccessData product, see the AccessData website at www.accessdata.com.

Audience

AccessData Forensic Toolkit (FTK) is intended for law enforcement officials and corporate security and IT professionals who need to access and evaluate the evidentiary value of files, folders, and computers.

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

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

HANDLING EVIDENCE

Law enforcement officials using FTK and related tools to gather evidence need to understand the basics of computer forensics. Computer forensics involves the acquisition, preservation, analysis, and presentation of computer evidence. This type of evidence is fragile and can easily, even inadvertently, be altered, destroyed, or rendered inadmissible as evidence. Computer evidence must be properly obtained, preserved, and analyzed to be accepted as reliable and valid in a court of law.

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

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

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

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

OTHER ACCESSDATA PRODUCTS

AccessData has developed other industry-leading products to assist in forensic analysis and password recovery. The following sections offer a brief introduction to these products. For more information on any of these products, please visit our website, www.accessdata.com.

LICENSE MANAGEMENT

The following products aid in the management of your AccessData product licenses and license security devices. For more detailed information regarding licenses, LicenseManager, and license security devices, see "Appendix F Managing Security Devices and Licenses" on page 255.

LICENSEMANAGER

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

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

CODEMETER RUNTIME

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

AccessData Forensic Products

This section provides basic information about AccessData's forensic investigation products.

FTK Imager

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

Imager performs the following tasks:

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

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

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 hashs and the drive hash match when the drive image is created. Two hash functionsare available in FTK Imager: Message Digest 5 (MD5), and Secure Hash Algorighm (SHA-1 & SHA -256).

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

AccessData Language Selector

AccessData Language Selector is a utility that allows you to choose a language codepage to view your cases in. Install it from the *FTK 2.2 Install Main Menu > Install Other Products* menu. For more information, see "Install Language Selector" on page 32.

AccessData Forensic Toolkit

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

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

AccessData Enterprise

AccessData Enterprise takes network-enabled digital investigations to the next level. Built on our industry-standard, court-validated FT technology, AccessData Enterprise delivers state-of-the-art incident response capabilities, deep dive analysis of both volatile and static data, as well as superior threat detection capabilities — all within an easy-to-use interface. A role-based permission system, an intuitive incident response console, secure batch remediation capabilities, unsurpassed searching and filtering, and comprehensive logging and reporting are just a few of the reasons Enterprise is quickly being adopted by Fortune 500 companies.

AccessData eDiscovery

AccessData eDiscovery is truly a landmark technology that virtually walks you through each and every step of the eDiscovery lifecycle. Fortune 500 companies are quickly turning to eDiscovery, because it is the only true custodian-based, end-to-end eDiscovery solution on the market today. Furthermore, it is by far the easiest to use with an intuitive dashboard that conveys the real-time status of all collection activities. True custodian data mapping, the ability to schedule and manage ongoing and periodic collections to better address ongoing litigation matters, as well as powerful processing and reporting are just a few of the reasons eDiscovery is the new revelation in the industry. Not only does it give you the power to address each phase of the process in-house, but it allows you to search and collect data from network shares, email servers, Documentum, SharePoint, Open Text, databases and other structured data repositories. This gives you a level of reach unmatched by any other e-discovery solution. Simply compare other solutions' capabilities to eDiscovery and you will see why so many people are switching.

LAB

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

SILENTRUNNER

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

REGISTRY VIEWER

AccessData Registry Viewer® allows you to view the contents of Windows operating system registry files. Unlike Windows Registry Editor, which only displays the registry of the current system, Registry Viewer lets you examine registry files from any Windows system. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible in Windows Registry Editor.

MOBILE PHONE EXAMINER

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

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

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

STEGANOGRAPHY PLUG-IN

AccessData now provides a plugin application that integrates support for several steganography applications.

WHAT IS STEGANOGRAPHY?

Steganography is the process of breaking up and embedding one document or file type inside another, effectively hiding the embedded file. The file that contains the embedded file is known as a "carrier" file. The file that is embedded within the carrier file is called the "payload".

Because steganography provides an effective way of hiding files or data that could prove to be valuable evidence, the AccessData Steganography plugin is an important tool for detecting and extracting the payload from carrier files.

Some carrier files are password encrypted, and some are not. This difference is key to determining the best path for accessing the payload. AccessData provides the tools necessary to address both scenarios.

To create a carrier file and embed payload data into it, a special application is required that is designed to do so. While many such apps are available, the AccessData Steganography plugin currently supports a specific list of steganography programs.

SUPPORTED STEGANOGRAPHY PROGRAMS

Ther AccessData Steganography plugin provides support for the following steganography applications:

TABLE 1-1 FTK Steganography Plugin Supported Programs

Covert.tcp	CryptaPix
dc-Stego	FFEncode
Gzsteg	Gifshuffle
Hide 4 PGP	Hide and Seek
Jsteg	PGE-Pretty Good Envelope
S-Tools versions 1-3	S-Tools version 4
Scytale	Snow
Steganos Security Suite	Stegodos
Texto	wbStego
WNSTORM	

FILE DECRYPTION AND PASSWORD DISCOVERY

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

PRTK AND DNA

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

PRTK and DNA perform recoveries on protected files using various methods, including decryption and dictionary attacks. For difficult password key values, PRTK performs dictionary attacks using various types of dictionaries, including the Golden Dictionary (containing previously recovered passwords), as well as Biographical, Custom User, and Default dictionaries.

FEATURES OVERVIEW

PRTK and DNA perform the following basic functions:

- Hash files

  Hashing a file uses an algorithm that creates a unique hash value for a file, allowing verification that the contents of a file remain unchanged. When a file is added to PRTK or DNA for key or password recovery, it is hashed. When the key or password is recovered, the file is automatically hashed again to verify that the file itself has remained unchanged. This is particularly helpful to law enforcement personnel who need to verify that a file has not been changed while recovering a password.

- Recover passwords

  PRTK can recover the password to files created in many popular industry applications by using a variety of methods, including several types of dictionaries used within profiles, in combination with rules to achieve the desired results. PRTK can also recover multi-lingual passwords.

- Generate reports

  You can now print job information reports for password recovery jobs in .PDF format.

- Open encrypted files

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

PRTK / DNA ADD-ONS

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

PORTABLE OFFICE RAINBOW TABLES

Rainbow Tables are also pre-computed, brute-force attacks. AccessData Portable Office Rainbow Tables (PORT) are different from the full Hash tables set. A statistical analysis is done on the file itself to determine the available keys. This takes far less space than the Hash Tables, but also takes somewhat more time and costs a small percentage in accuracy.

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

Product Features

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

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

RAINBOW (HASH) TABLES

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

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

Product Features

Three Rainbow Tables Hash Sets are available:

- MS Office Word and Excel
- Acrobat PDF
- Windows LAN Hash

Each hash set takes nearly 3TB of disk space.

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

TACC Unit

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

License Management

The following products aid in the management of your AccessData product licenses and license security devices. For more detailed information regarding licenses, LicenseManager, and license security devices, see “Appendix F Managing Security Devices and Licenses” on page 255.

LicenseManager

AccessData LicenseManager lets you manage product and license subscriptions stored on your Wibu CodeMeter CmStick or Keylok dongle USB license security device.

LicenseManager communicates directly with AccessData's license server, so when license renewals take place, the information is readily and immediately accessible for download to your license device.

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

CodeMeter Runtime

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

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) 2.2. The following components are required to run FTK:

- CodeMeter 3.30a Runtime software for the CodeMeter Stick
- A CodeMeter Stick
- Oracle 10g Database
- FTK 2.2 Program

These additional programs are available to aid in processing cases:

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

Installation Options

Most notably, beginning with this version, FTK 2.2 can be installed with any one earlier version of 2.x remaining on the same computer at the same time. Installation paths will differ slightly from previous versions and registry entries will also be different. This means you may not have to uninstall your earlier version of FTK 2.x and thus will not have to convert (or lose) cases to the newer version to maintain compatibility with the database.

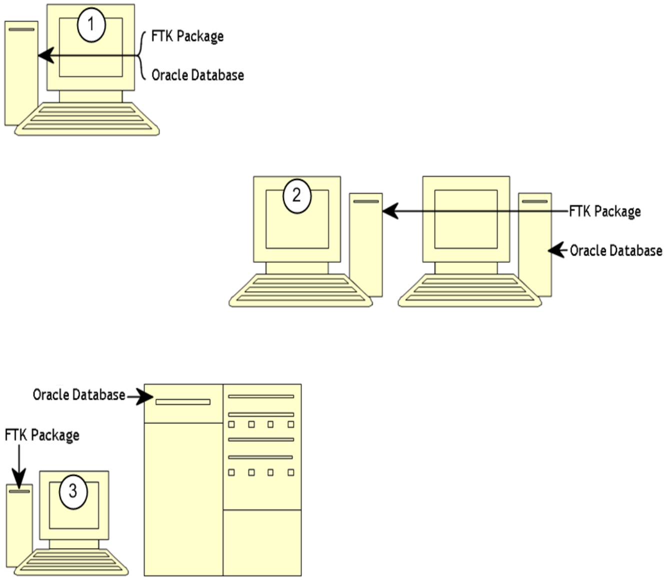
INSTALLATION CONFIGURATION OPTIONS

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

- 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 that Oracle can use exclusively.
- Do not run other applications on these machines that will compete with FTK or the Oracle database for hardware resources.

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.

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

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

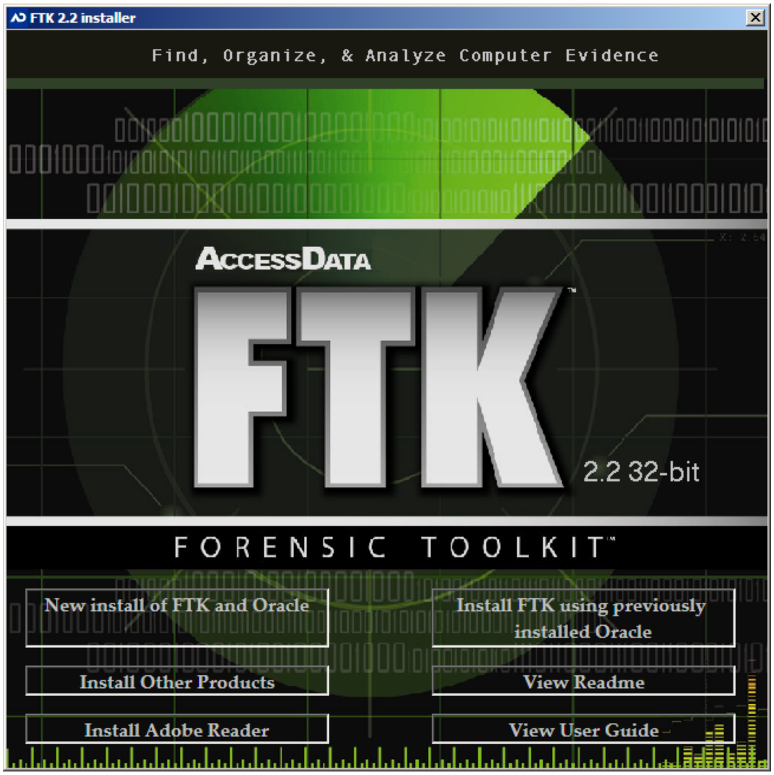
- Data: every 500,000 items require one gigabyte of space in the Oracle storage location.

- Index: every 100 megabytes of text in the evidence requires 20 megabytes of space for processing in the case storage folder.

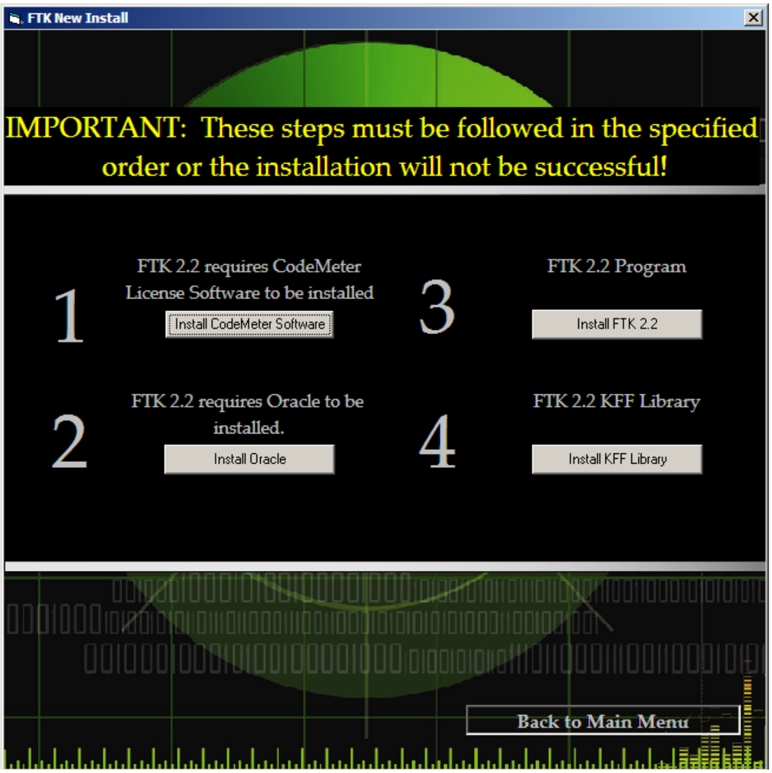
INSTALLATION

To install FTK 2.2, follow these steps:

1. Insert the FTK 2.2 DVD into the drive.



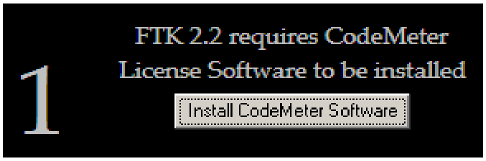
2. Click *Install Forensic Toolkit 2.2*.



FTK New Install
IMPORTANT: These steps must be followed in the specified order or the installation will not be successful!
1
FTK 2.2 requires CodeMeter License Software to be installed
Install CodeMeter Software
2
FTK 2.2 requires Oracle to be installed.
Install Oracle
3
FTK 2.2 Program
Install FTK 2.2
4
FTK 2.2 KFF Library
Install KFF Library
Back to Main Menu

Install CodeMeter

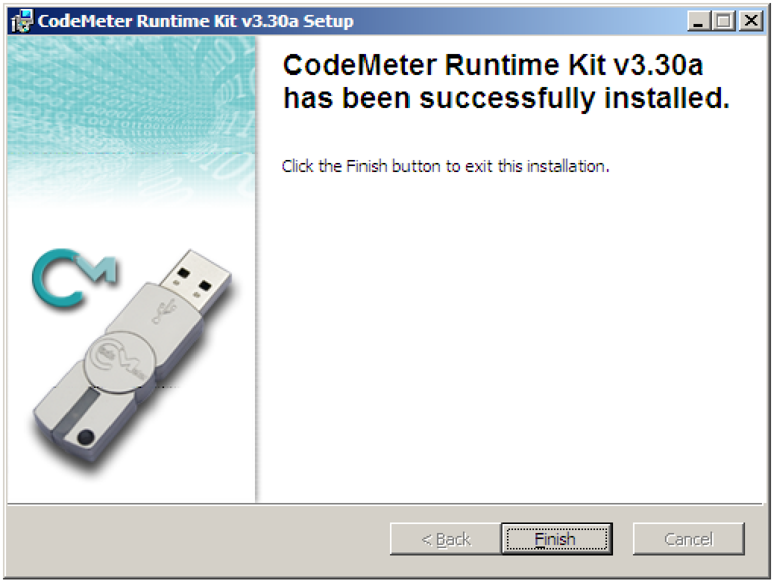
Install the WIBU CodeMeter Runtime v3.30a software for the CodeMeter Stick. Click *Install CodeMeter Software* to launch the CodeMeter installation wizard, as displayed in the following figure.



1
FTK 2.2 requires CodeMeter License Software to be installed
Install CodeMeter Software

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

Figure 2-2 CodeMeter Installation Wizard.



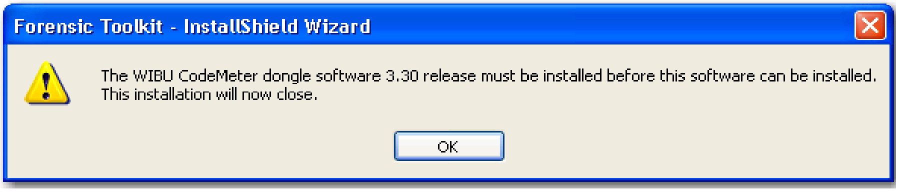
CodeMeter Runtime Kit v3.30a Setup

CodeMeter Runtime Kit v3.30a has been successfully installed.

Click the Finish button to exit this installation.

If the user attemps to install FTK 2.2 before installing the CodeMeter v3.30a software and the Wibu CmStick, a message similar to the following error message will be displayed.

Figure 2-3 CodeMeter Error



Forensic Toolkit - InstallShield Wizard

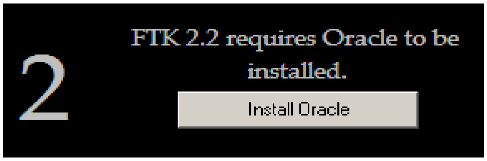
The WIBU CodeMeter dongle software 3.30 release must be installed before this software can be installed. This installation will now close.

Note: To Remedy, quit the FTK 2.2 install. Install CodeMeter Runtime 3.30a software, and connect the CmStick. Then restart FTK 2.2 installation.

INSTALL ORACLE

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

Figure 2-4 Install Oracle Button



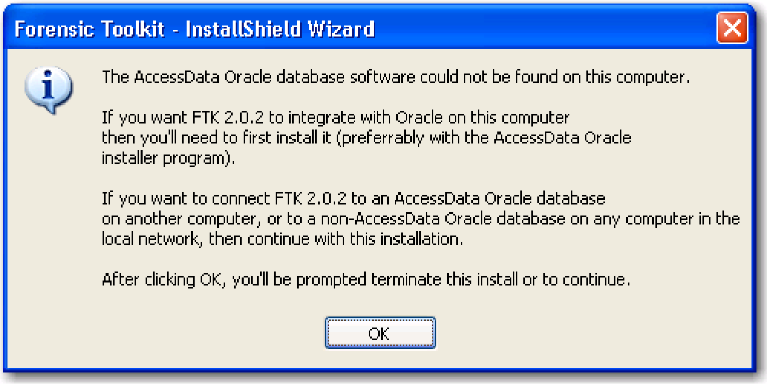
2

FTK 2.2 requires Oracle to be installed.

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, the FTK installer warns of its dependency on Oracle and prompts the user to continue with or terminate the install, in a message similar to the one displayed in the following figure.

Figure 2-5 Oracle Dependency Warning



Forensic Toolkit - InstallShield Wizard

The AccessData Oracle database software could not be found on this computer.

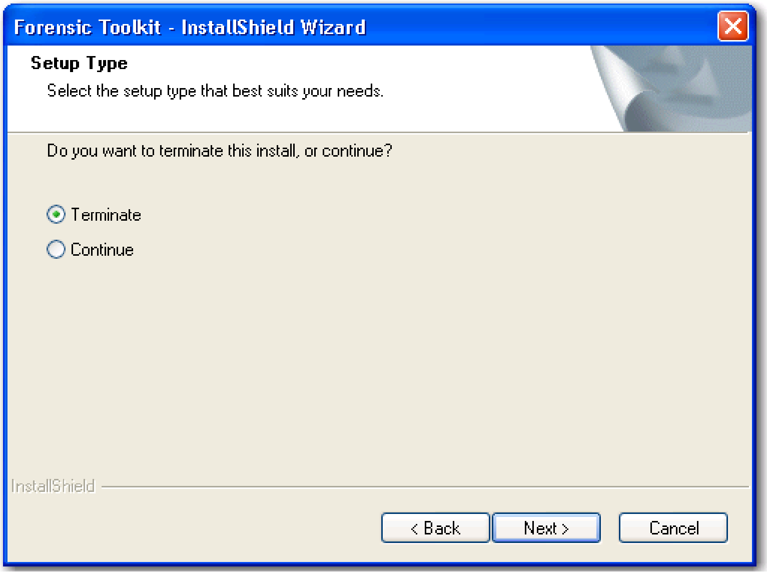
If you want FTK 2.0.2 to integrate with Oracle on this computer then you'll need to first install it (preferrably with the AccessData Oracle installer program).

If you want to connect FTK 2.0.2 to an AccessData Oracle database on another computer, or to a non-AccessData Oracle database on any computer in the local network, then continue with this installation.

After clicking OK, you'll be prompted terminate this install or to continue.

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

Figure 2-6 Terminate or Continue Install



Forensic Toolkit - InstallShield Wizard

Setup Type

Select the setup type that best suits your needs.

Do you want to terminate this install, or continue?

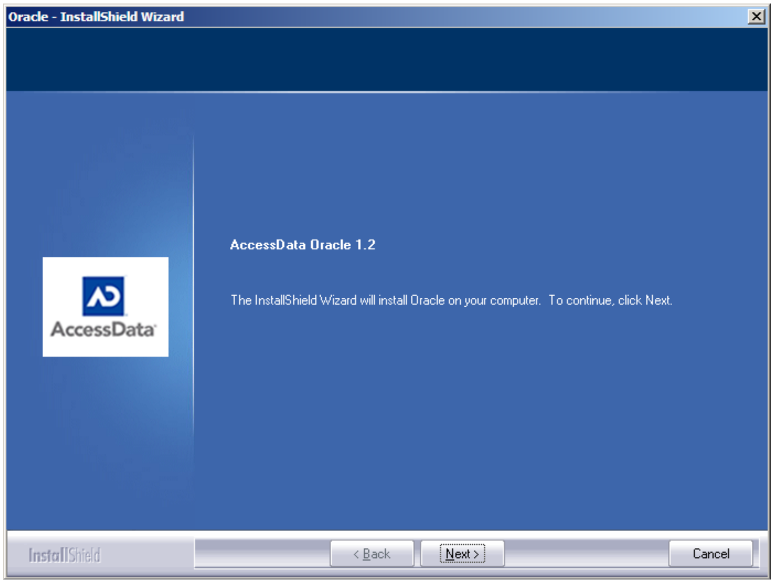
● Terminate

○ Continue

If the user continues, the FTK installation may fail, and otherwise, the program will not run properly.

Note: The solution is to properly install Oracle before attempting to install FTK 2.2.

1. Launch the installer.

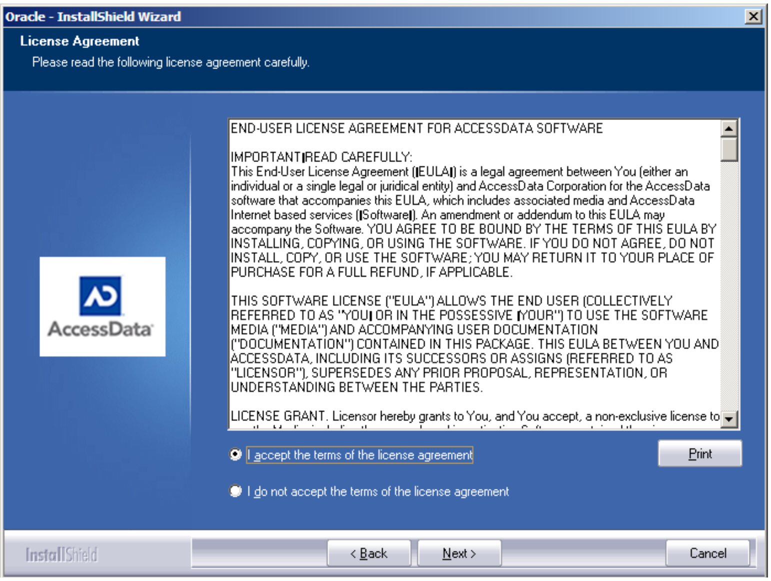


Oracle - InstallShield Wizard

AccessData Oracle 1.2

The InstallShield Wizard will install Oracle on your computer. To continue, click Next.

2. Click *Next.*



Oracle - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

END-USER LICENSE AGREEMENT FOR ACCESSDATA SOFTWARE

IMPORTANT|READ CAREFULLY:
This End-User License Agreement (|EULA|) is a legal agreement between You (either an individual or a single legal or juridical entity) and AccessData Corporation for the AccessData software that accompanies this EULA, which includes associated media and AccessData Internet based services (|Software|). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE.

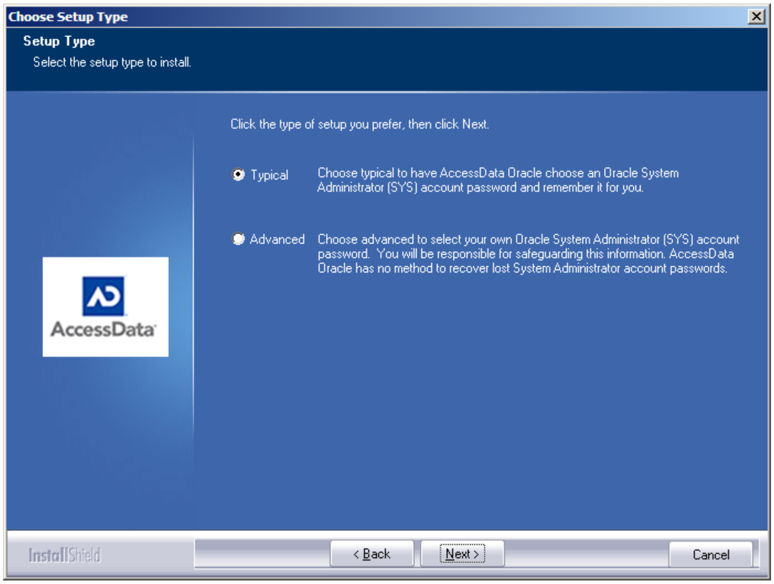
THIS SOFTWARE LICENSE ("EULA") ALLOWS THE END USER (COLLECTIVELY REFERRED TO AS "YOU| OR IN THE POSSESSIVE |YOUR") TO USE THE SOFTWARE MEDIA ("MEDIA") AND ACCOMPANYING USER DOCUMENTATION ("DOCUMENTATION") CONTAINED IN THIS PACKAGE. THIS EULA BETWEEN YOU AND ACCESSDATA, INCLUDING ITS SUCCESSORS OR ASSIGNS (REFERRED TO AS "LICENSOR"), SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

LICENSE GRANT. Licensor hereby grants to You, and You accept, a non-exclusive license to

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

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



Choose Setup Type

Setup Type

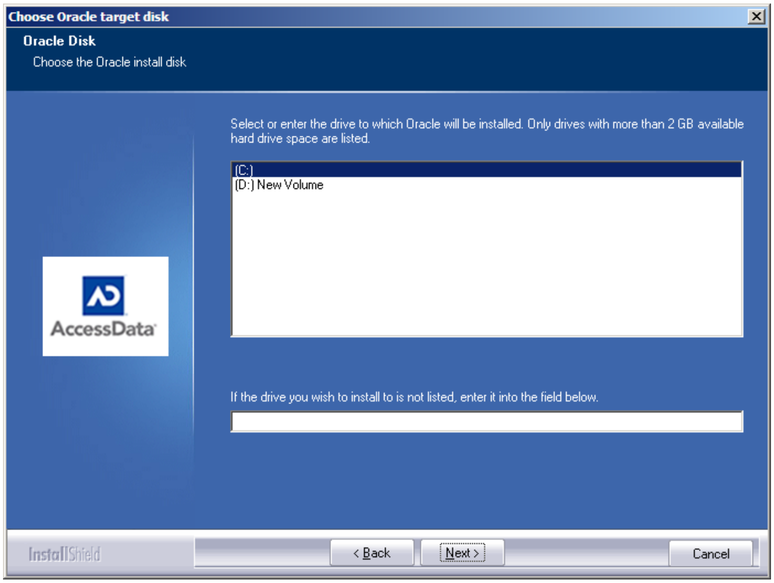
Select the setup type to install.

Click the type of setup you prefer, then click Next.

● Typical Choose typical to have AccessData Oracle choose an Oracle System Administrator (SYS) account password and remember it for you.

○ Advanced Choose advanced to select your own Oracle System Administrator (SYS) account password. You will be responsible for safeguarding this information. AccessData Oracle has no method to recover lost System Administrator account passwords.

4. Wait for the installer to configure the installation.



Choose Oracle target disk

Oracle Disk

Choose the Oracle install disk

Select or enter the drive to which Oracle will be installed. Only drives with more than 2 GB available hard drive space are listed.

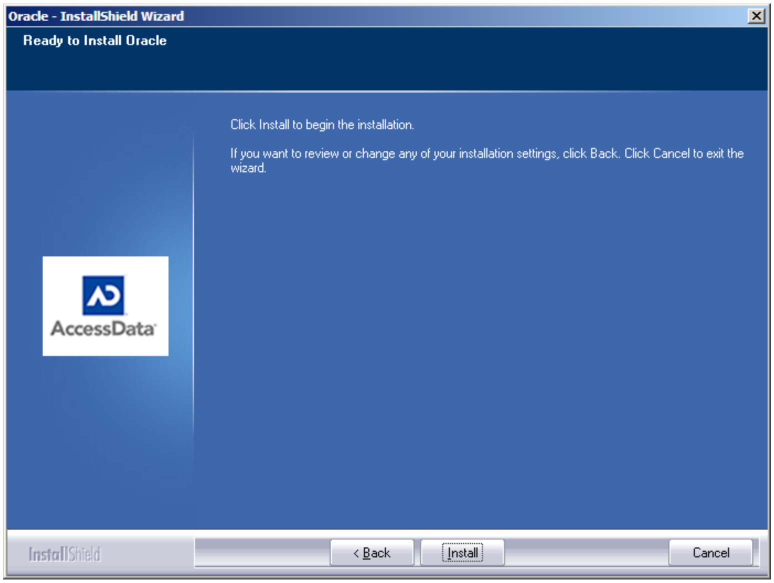
(C:)
(D:) New Volume

If the drive you wish to install to is not listed, enter it into the field below.

5. Select the installation drive letter.

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

6. Click *Next*.

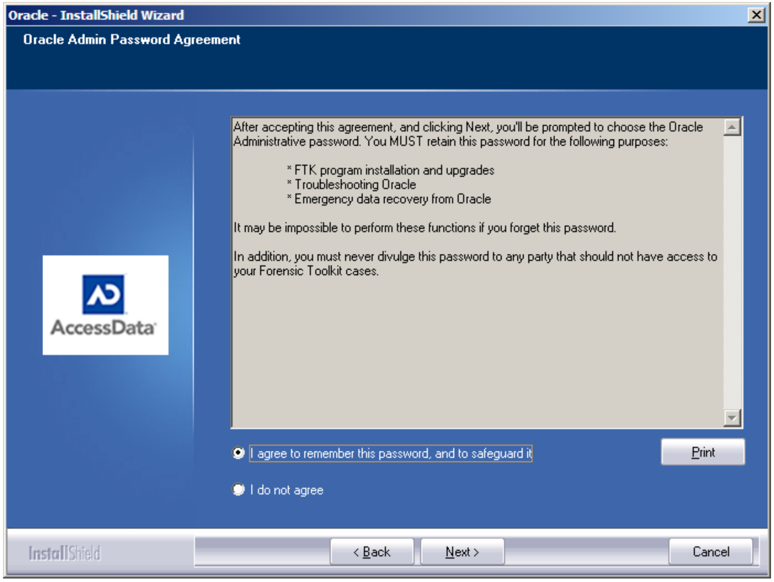


Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Note: These options are only available when Advance Installation has been selected.

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



Oracle - InstallShield Wizard
Oracle Admin Password Agreement
AccessData
Print
InstallShield
< Back
Next >
Cancel

After accepting this agreement, and clicking Next, you'll be prompted to choose the Oracle Administrative password. You MUST retain this password for the following purposes:

* FTK program installation and upgrades
* Troubleshooting Oracle
* Emergency data recovery from Oracle

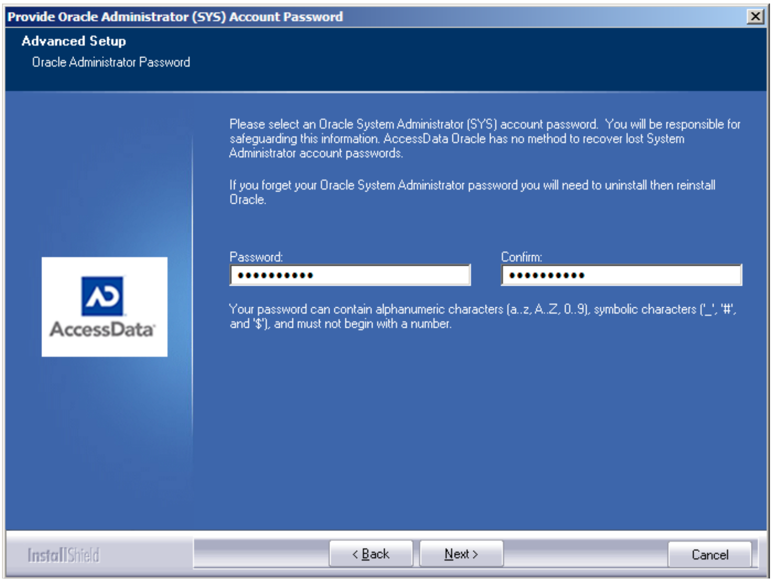
It may be impossible to perform these functions if you forget this password.

In addition, you must never divulge this password to any party that should not have access to your Forensic Toolkit cases.

● I agree to remember this password, and to safeguard it

○ I do not agree

8. Provide an Oracle System Administrator password.



Provide Oracle Administrator (SYS) Account Password

Advanced Setup

Oracle Administrator Password

Please select an Oracle System Administrator (SYS) account password. You will be responsible for safeguarding this information. AccessData Oracle has no method to recover lost System Administrator account passwords.

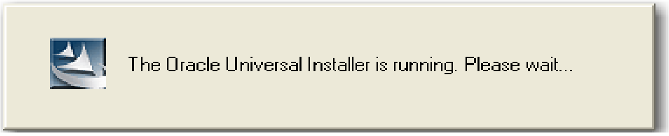
If you forget your Oracle System Administrator password you will need to uninstall then reinstall Oracle.

Password: ••••••••••

Confirm: ••••••••••

Your password can contain alphanumeric characters (a..z, A..Z, 0..9), symbolic characters ('_', '#', and '$'), and must not begin with a number.

9. Click *Submit*.

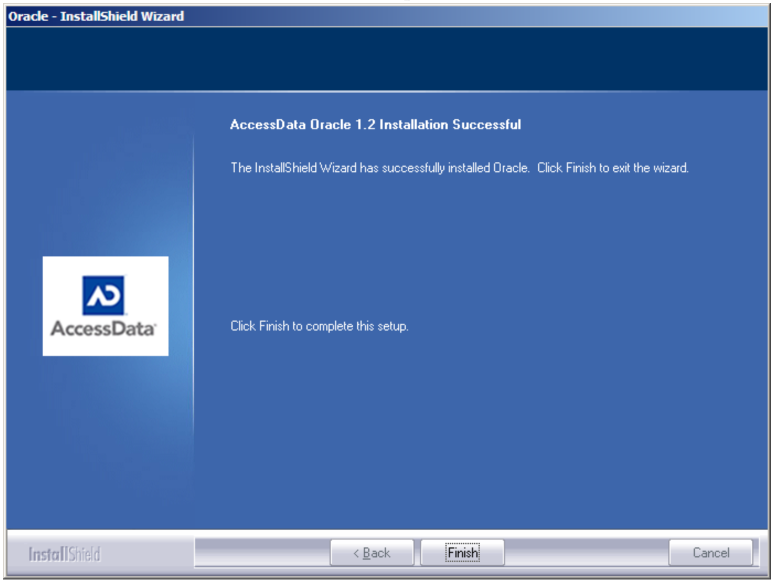


The Oracle Universal Installer is running. Please wait...

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..



AccessData Oracle 1.2 Installation Successful

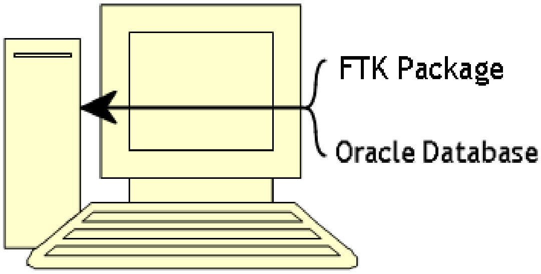
The InstallShield Wizard has successfully installed Oracle. Click Finish to exit the wizard.

Click Finish to complete this setup.

SINGLE COMPUTER INSTALLATION

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

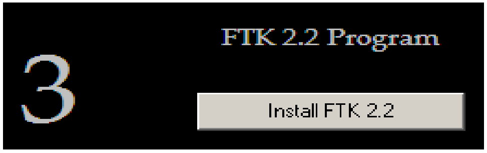
Figure 2-7 Single Computer Installation



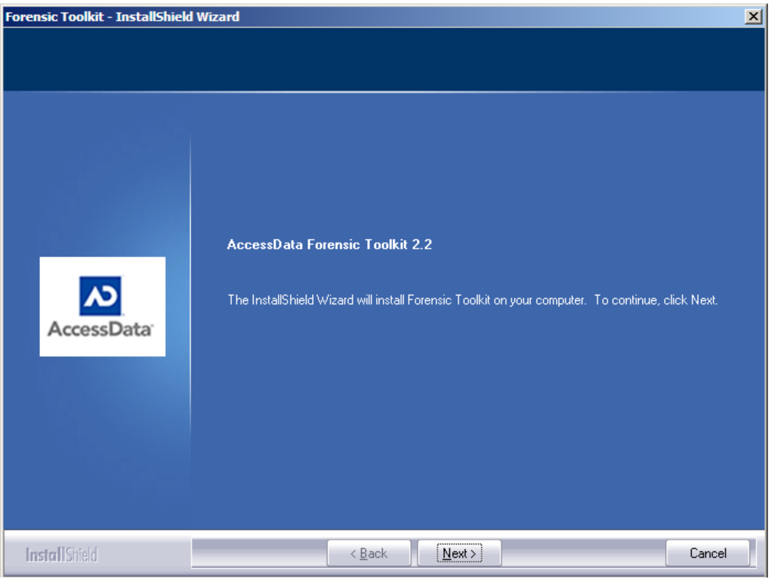
INSTALL FTK

From the FTK 2.2 New Install screen, perform the steps displayed in the following figure.

Figure 2-8 Install FTK 2.2 Button



1. Click *Install FTK 2.2.*

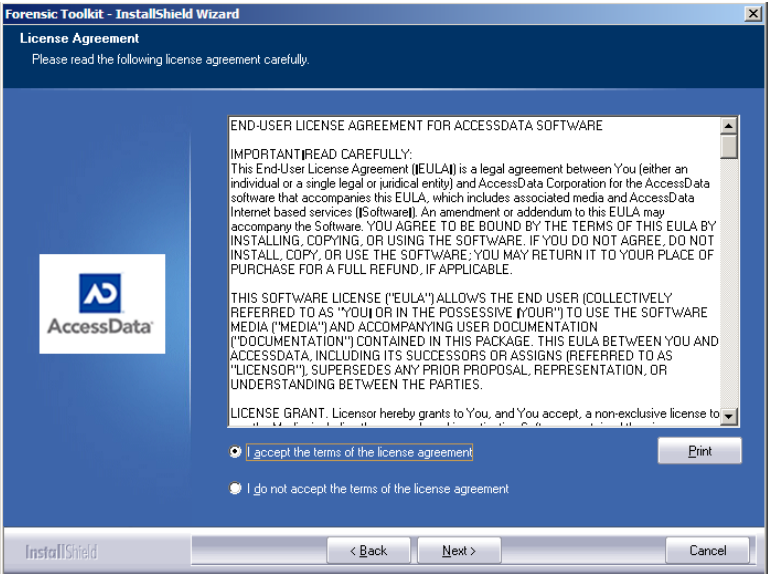


AccessData Forensic Toolkit 2.2

The InstallShield Wizard will install Forensic Toolkit on your computer. To continue, click Next.

2. Click *Next.*

3. Read and accept the AccessData license agreement.



Forensic Toolkit - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

END-USER LICENSE AGREEMENT FOR ACCESSDATA SOFTWARE

IMPORTANT|READ CAREFULLY:
This End-User License Agreement (|EULA|) is a legal agreement between You (either an individual or a single legal or juridical entity) and AccessData Corporation for the AccessData software that accompanies this EULA, which includes associated media and AccessData Internet based services (|Software|). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE.

THIS SOFTWARE LICENSE ("EULA") ALLOWS THE END USER (COLLECTIVELY REFERRED TO AS "YOU| OR IN THE POSSESSIVE |YOUR") TO USE THE SOFTWARE MEDIA ("MEDIA") AND ACCOMPANYING USER DOCUMENTATION ("DOCUMENTATION") CONTAINED IN THIS PACKAGE. THIS EULA BETWEEN YOU AND ACCESSDATA, INCLUDING ITS SUCCESSORS OR ASSIGNS (REFERRED TO AS "LICENSOR"), SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

LICENSE GRANT. Licensor hereby grants to You, and You accept, a non-exclusive license to

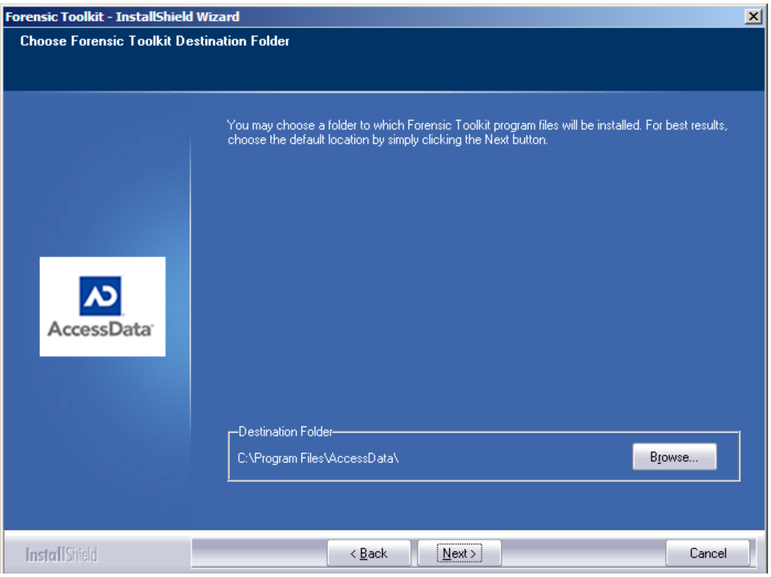
● I accept the terms of the license agreement

○ I do not accept the terms of the 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.



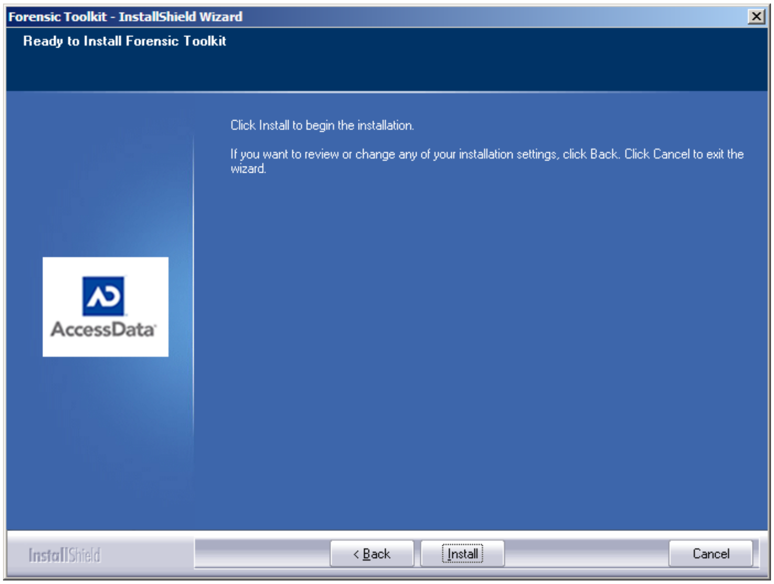
Forensic Toolkit - InstallShield Wizard

Choose Forensic Toolkit Destination Folder

You may choose a folder to which Forensic Toolkit program files will be installed. For best results, choose the default location by simply clicking the Next button.

Destination Folder
C:\Program Files\AccessData\

6. Click *Next*.



Forensic Toolkit - InstallShield Wizard

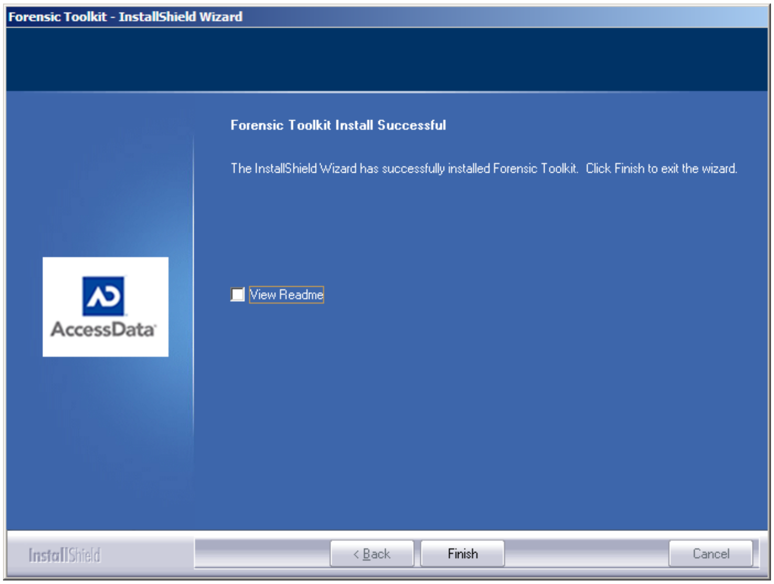
Ready to Install Forensic Toolkit

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

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

8. Follow the prompts on the screens that follow.



Forensic Toolkit - InstallShield Wizard

Forensic Toolkit Install Successful

The InstallShield Wizard has successfully installed Forensic Toolkit. Click Finish to exit the wizard.

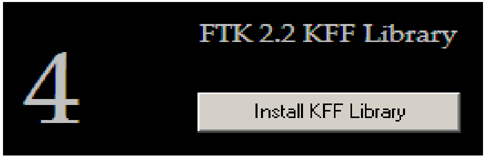
□ View Readme

9. When the installation is completed successfully, click *Finish*.

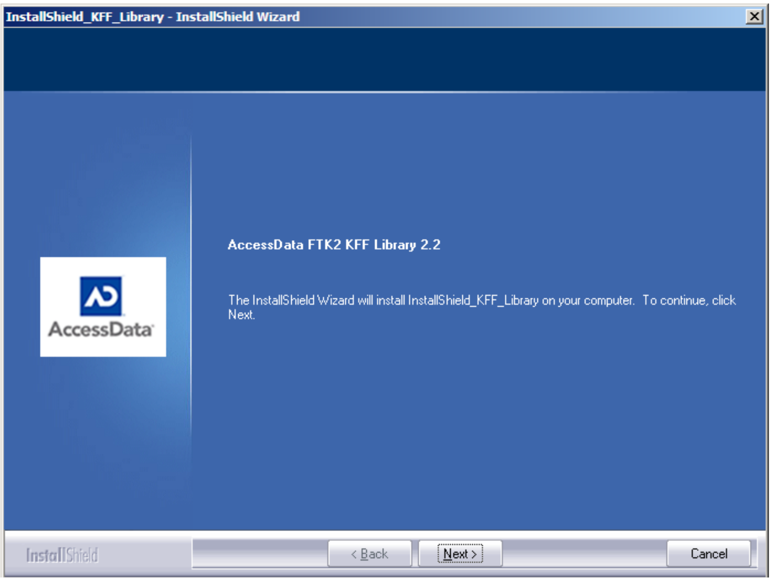
INSTALL THE KFF LIBRARY

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

Figure 2-9 Install KFF Button



1. Click *Install KFF Library*

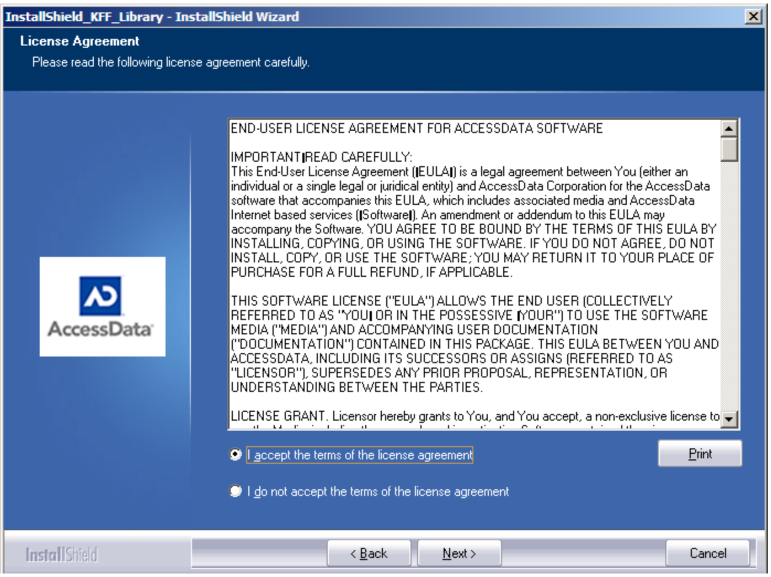


AccessData FTK2 KFF Library 2.2

The InstallShield Wizard will install InstallShield_KFF_Library on your computer. To continue, click Next.

2. Click *Next*.

3. Accept the KFF license agreement.


InstallShield_KFF_Library - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
AccessData
● I accept the terms of the license agreement
○ I do not accept the terms of the license agreement
Print
InstallShield
< Back
Next >
Cancel

END-USER LICENSE AGREEMENT FOR ACCESSDATA SOFTWARE

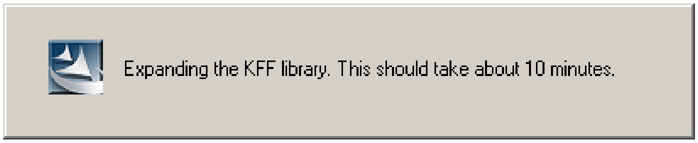
IMPORTANT|READ CAREFULLY:
This End-User License Agreement (|EULA|) is a legal agreement between You (either an individual or a single legal or juridical entity) and AccessData Corporation for the AccessData software that accompanies this EULA, which includes associated media and AccessData Internet based services (|Software|). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE.

THIS SOFTWARE LICENSE ("EULA") ALLOWS THE END USER (COLLECTIVELY REFERRED TO AS "YOU| OR IN THE POSSESSIVE |YOUR") TO USE THE SOFTWARE MEDIA ("MEDIA") AND ACCOMPANYING USER DOCUMENTATION ("DOCUMENTATION") CONTAINED IN THIS PACKAGE. THIS EULA BETWEEN YOU AND ACCESSDATA, INCLUDING ITS SUCCESSORS OR ASSIGNS (REFERRED TO AS "LICENSOR"), SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.

LICENSE GRANT. Licensor hereby grants to You, and You accept, a non-exclusive license to

4. Click *Next*.

5. Allow installation to progress.



Expanding the KFF library. This should take about 10 minutes.

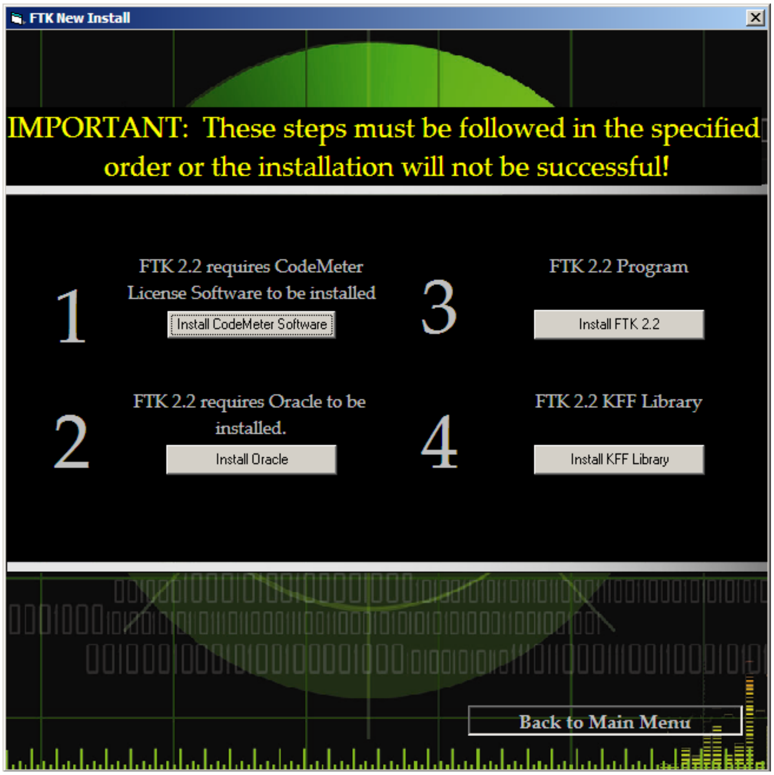
6. When the screen indicates a successful installation, click *Finish* to end the installation.

7. Click *Back to Main Menu* to return to the Main Menu and make other selections.

INSTALLING ON SEPARATE COMPUTERS

FTK 2.2 can be installed on two separate computers. To do this, change the steps, as shown again in the following figure, to 2, 1, 3, 4. 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. (The CodeMeter software and CmStick must be installed on the FTK 2.2 machine.)

Figure 2-10 Install New FTK Screen



FTK New Install

IMPORTANT: These steps must be followed in the specified order or the installation will not be successful!

1 FTK 2.2 requires CodeMeter License Software to be installed

2 FTK 2.2 requires Oracle to be installed.

3 FTK 2.2 Program

4 FTK 2.2 KFF Library

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\2.2.

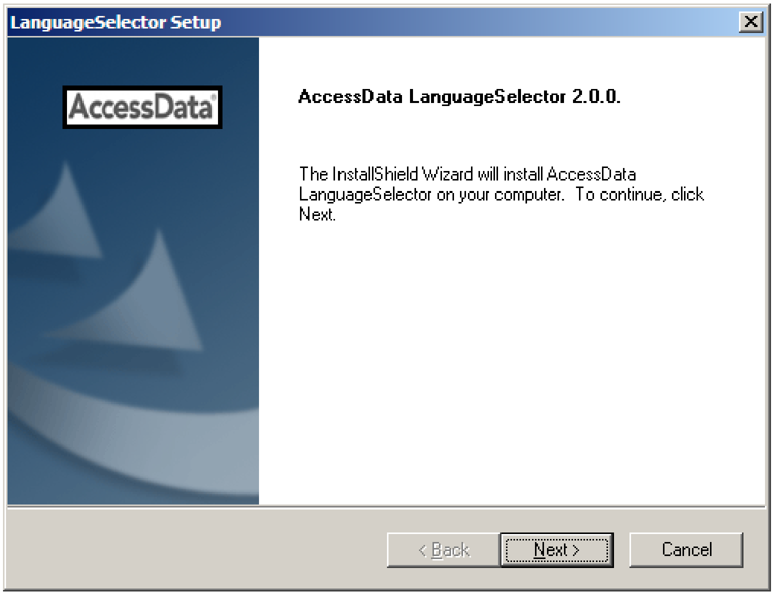
Additional Programs

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

INSTALL LANGUAGE SELECTOR

To install Language Selector follow these steps:

1. From the FTK 2.2 Autorun Main Menu, click *Install Other Products*, then click *Install Language Selector.*

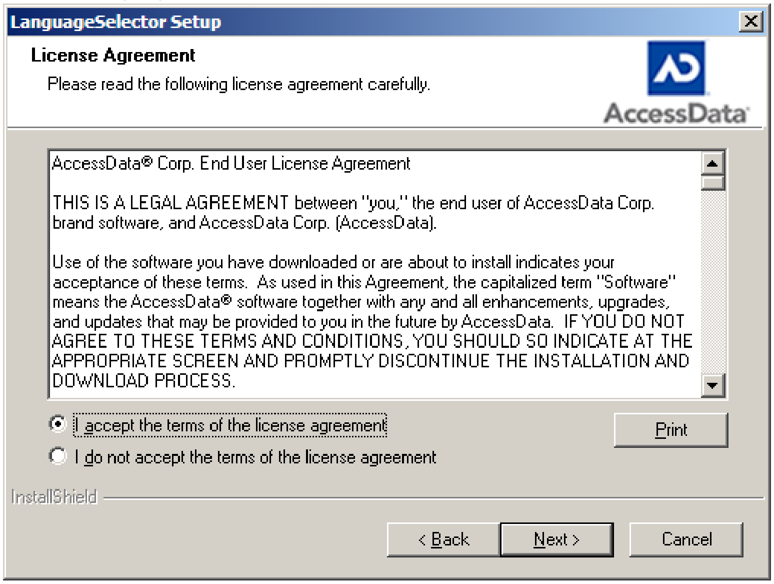


LanguageSelector Setup

AccessData LanguageSelector 2.0.0.

The InstallShield Wizard will install AccessData LanguageSelector on your computer. To continue, click Next.

2. The Language Selector Installer runs. Click *Next* to continue.



LanguageSelector Setup

License Agreement

Please read the following license agreement carefully.

AccessData® Corp. End User License Agreement

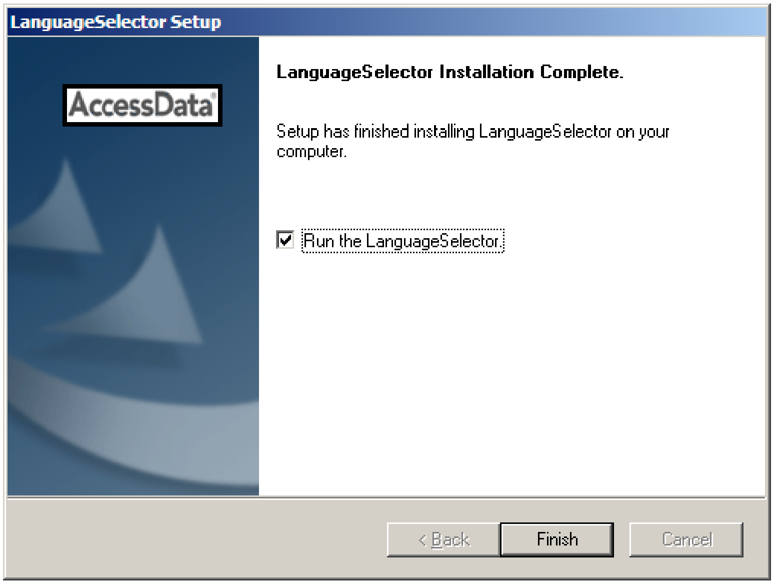
THIS IS A LEGAL AGREEMENT between "you," the end user of AccessData Corp. brand software, and AccessData Corp. (AccessData).

Use of the software you have downloaded or are about to install indicates your acceptance of these terms. As used in this Agreement, the capitalized term "Software" means the AccessData® software together with any and all enhancements, upgrades, and updates that may be provided to you in the future by AccessData. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU SHOULD SO INDICATE AT THE APPROPRIATE SCREEN AND PROMPTLY DISCONTINUE THE INSTALLATION AND DOWNLOAD PROCESS.

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

3. Read and accept the License Agreement. Click *Next* to continue.



LanguageSelector Setup

LanguageSelector Installation Complete.

Setup has finished installing LanguageSelector on your computer.

☑ Run the LanguageSelector.

4. Click Finish.

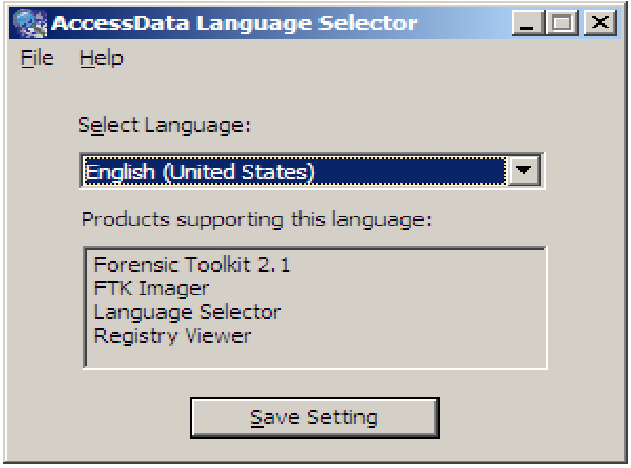
Using Language Selector

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

OR

Click the Language Selector Icon on your desktop:

Language Selector has a very simple interface, as shown in the following figure:



Select Language: English (United States)

Products supporting this language:

Forensic Toolkit 2.1
FTK Imager
Language Selector
Registry Viewer

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

TABLE 2-1 Language Selector Supported Languages

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

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

The File menu contains two choices:

- Select Language
- Exit

The Help menu contains one choice:

- About

LICENSING

If licenses need to be managed, LicenseManager must be installed. For more information on LicenseManager, see “Appendix F Managing Security Devices and Licenses” on page 255.

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

UPGRADING TO FTK 2.2

You no longer need to upgrade your previous FTK 2.x version to 2.2, or convert earlier 2.x cases to continue to use them. You can keep one earlier 2.x version installed on your machine, and still install FTK 2.2 using the same database. Your previous cases will still be available and you can work with them in their native version.

Chapter 3 Concepts

Before using AccessData Forensic Toolkit (FTK), a basic knowledge of the FTK interface is helpful. This chapter focuses on the basic features and flow of a case. The chapters that follow give more detail.

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

Regarding the CodeMeter Stick

AccessData provides a USB CodeMeter Stick security license device with FTK. The WIBU-SYSTEM 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 267.

Important: FTK.2.x does not work with the green KEYLOK security device dongle used with previous versions of FTK.

Basic Workflow

The most efficient way to work in FTK 2.2 is to begin with the end in mind. For example, your goal may be to use computer evidence to convict a criminal of wrongful acts. To do so, you will need to produce a report that presents meaningful evidence of the offenses to interested parties, such as in a court of law.

As you begin, of course, you will need to install and set up the program and users to best and most efficiently accomplish the task at hand.

Once the installation is complete, and the Application and Case Administrators are set up, a case can be created.

The basic flow of a case then, is as follows:

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 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.

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

FTK Imager is an AccessData 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 image identical in every way to the original, including file slack, and unallocated and drive free space.

Create a Case

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

ADD EVIDENCE

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

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

WORK THE CASE

IDENTIFYING MEANINGFUL EVIDENCE WITHIN A CASE

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

The beginning of the evidence defining process involves the hashing of the data added to a case. Another key to easily finding meaningful evidence is the indexing of case data. Through these two functions, Enterprise provides the foundation for successful investigation and analysis.

Using Index searching, live searching and filtering files using the Known File Filter Library (KFF) as well as built-in and custom filters applied to the data give results that can then be bookmarked and added to the report that summarizes the findings in the case.

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

As you find items of interest, you can:

- check mark them or bookmark them, so you can easily find those items again.
- Files can be exported,
- External files that are not otherwise part of the casec an be added to bookmarks as supplemental files

Generate Reports

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

Reports can be generated in several formats to make it easier to provide it in a useful way to your audience.

Moving Forward

The remainder of this chapter provides basics of the Case Management window and its options. For more detailed information about features and how they are used, see "Chapter 5 Adding and Processing Evidence" on page 77.

Starting FTK

After you complete the installation, start FTK by selecting *Start > All Programs > AccessData > Forensic Toolkit > FTK 2.2* (which executes FTK.exe), or by selecting the *AccessData Forensic Toolkit 2.2* shortcut on the desktop:

.

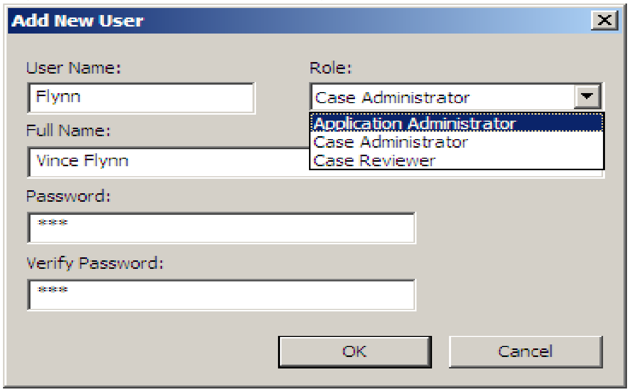
Important: Close any virus scanner program while running FTK and processing evidence. Virus scanners can slow performance significantly.

Setting Up the Application Administrator

On first launch an Application Administrator must be created to manage the database. The Add New User dialog box opens automatically. The first added user is the

Application Administrator, and has full rights for management of this FTK 2.2 installation, users, cases and database administration. The Application Administrator can add new users to the database, including Application Administrators, Case Administrators, and Case Reviewers.

Figure 3-1 Add New User Dialog



User Name: Flynn

Role: Case Administrator

Full Name: Vince Flynn

Password: ***

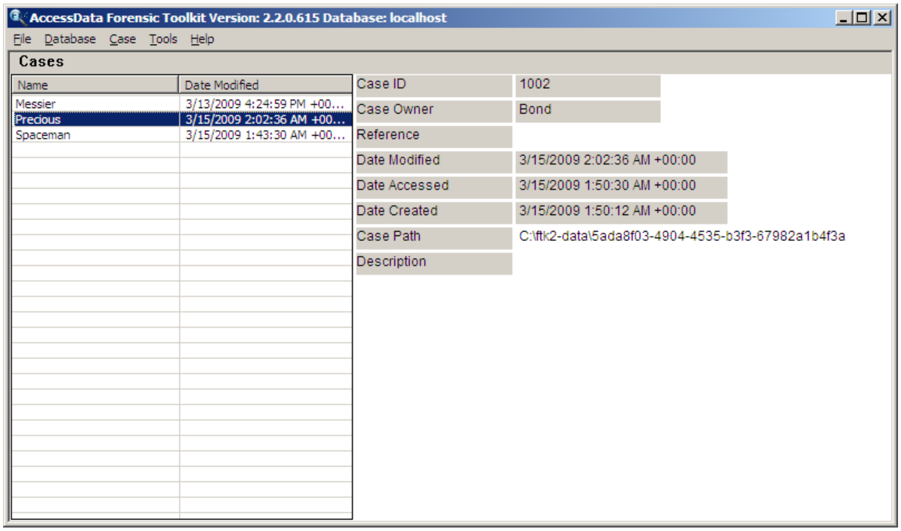
Verify Password: ****

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

Using the Case Management Window

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

Figure 3-2 Case Management Window.


AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost
File
Database
Case
Tools
Help
Cases

Name	Date Modified
Messier	3/13/2009 4:24:59 PM +00...
Precious	3/15/2009 2:02:36 AM +00...
Spaceman	3/15/2009 1:43:30 AM +00...

Case ID	1002
Case Owner	Bond
Reference	
Date Modified	3/15/2009 2:02:36 AM +00:00
Date Accessed	3/15/2009 1:50:30 AM +00:00
Date Created	3/15/2009 1:50:12 AM +00:00
Case Path	C:\ftk2-data\5ada8f03-4904-4535-b3f3-67982a1b4f3a
Description	

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

TABLE 3-1 Case Management Menus

- File
- Database
- Case
- Tools
- Help

The following tables shows the available Case Management menu options.

TABLE 3-2 Case Management File Menu

Option	Description
Exit	Exits FTK.

TABLE 3-3 **Case Management Database Menu**

Option	Description
Log In	Opens the authentication dialog for users to log into the database and to access a particular case. If someone is currently logged in to the database this option may not be available.
Log Out	Logs the user out of the current case. If no one is currently logged-in to the database, this option will not be available.
Administer Users	Available to the Application Administrator, view the list of current users, add users, and change users' passwords.
Manager KFF	Import or export KFF groups or databases, edit, or delete non-default groups, lists, or databases.
Add Database	Specify the network location of another instance of Oracle where cases can be stored and processed.
Session Management	Provides a list of database sessions and whether they are active or inactive; cases can be aborted from this menu.
Change my password	Allows the currently logged-in user to change his or her own password.
Add User	Create a user with either Reviewer or Administrator rights to the database. This can only be done by the application administrator.

TABLE 3-4 **Case Management Case Menu**

Option	Description
New	Start a new case with the logged-in user as the Case Administrator. Case Reviewers cannot create a new case.
Open	Opens the highlighted case with its included evidence.
Assign Users	Allows the Application Administrator or the Case Administrator to adjust or control the rights of other users to access a particular case..
Backup	Opens a dialog for specifying names and locations for backup of selected cases.
Restore	Opens a Windows Explorer instance for locating and restoring a selected, saved case.
Delete	Deletes the selected case.

TABLE 3-5 Case Management Tools Menu

Option	Description
Tools	
• Create Options File	Allows the creation of a Global Options File to apply to all cases as the default.
• Preferences settings:	Options are: • Choose temporary file path • Choose network security device location. Options are: •IP Address • Port

TABLE 3-6 Case Management Help Menu

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

Creating a New Case

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

For more information about creating a new case, see "Creating a Case" on page 48.

Chapter 4 Starting a New FTK 2.2 Case

After collecting the files or drive images to examine, start a case using AccessData Forensic Toolkit (FTK 2.2).

LAUNCH FTK 2.2

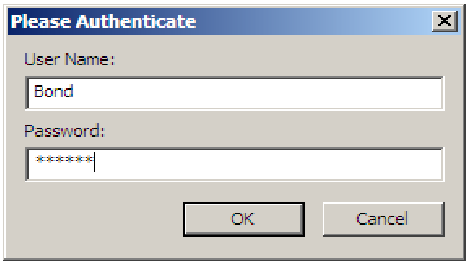
FTK harnesses the power of multiple investigators and computer processors to analyze cases. The application administrator is created when FTK 2.2 is launched the first time, and the Case Management window opens. Run FTK 2.2 by doing the following:

1. Click *Start> All Programs > AccessData > Forensic Toolkit > AccessData Forensic Toolkit 2.2.*

   Note: Please note that it may take a few moments for FTK 2.2 to run. This is because it is also launching the Oracle 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

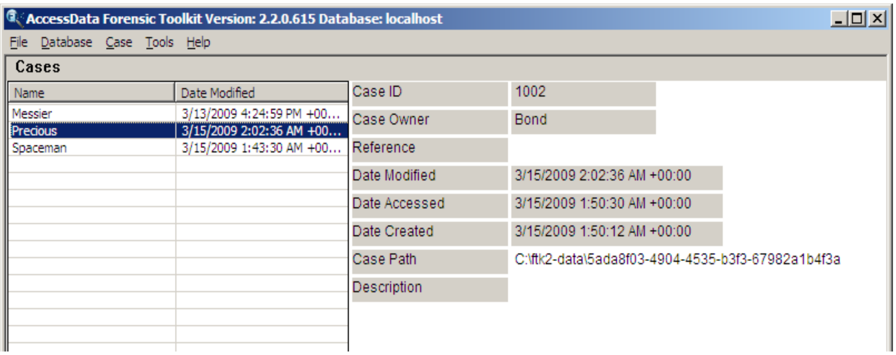


User Name: Bond

Password: *******

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

Figure 4-2   Case Management Window

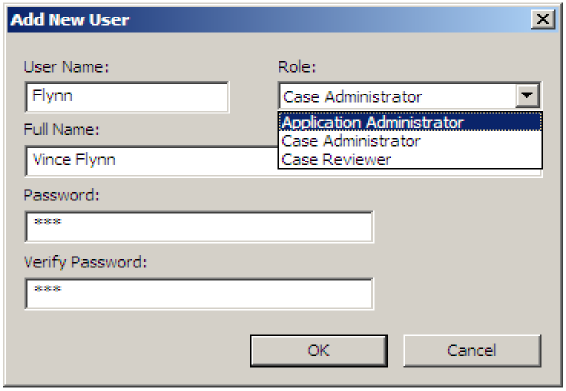

AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost
File
Database
Case
Tools
Help
Cases

Name	Date Modified
Messier	3/13/2009 4:24:59 PM +00...
Precious	3/15/2009 2:02:36 AM +00...
Spaceman	3/15/2009 1:43:30 AM +00...

Case ID	1002
Case Owner	Bond
Reference	
Date Modified	3/15/2009 2:02:36 AM +00:00
Date Accessed	3/15/2009 1:50:30 AM +00:00
Date Created	3/15/2009 1:50:12 AM +00:00
Case Path	C:\ftk2-data\5ada8f03-4904-4535-b3f3-67982a1b4f3a
Description	

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

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



User Name: Flynn

Role: Case Administrator

Full Name: Vince Flynn

Password: ****

Verify Password: ****

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: • **Application Administrator**: can perform all types of tasks, including adding and managing users. • **Case Administrator**: can process data and change settings to FTK, although only the application administrator can add new users. • **Case Reviewer**: cannot create cases; can only process cases.
Full Name	Enter the full name of the user as it is to appear on case reports.
Password	Enter and verify a password for this user.

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.

Application Administrator

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

CASE ADMINISTRATOR

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

CASE REVIEWER

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

TABLE 4-2 Permissions Denied Case Reviewer Users

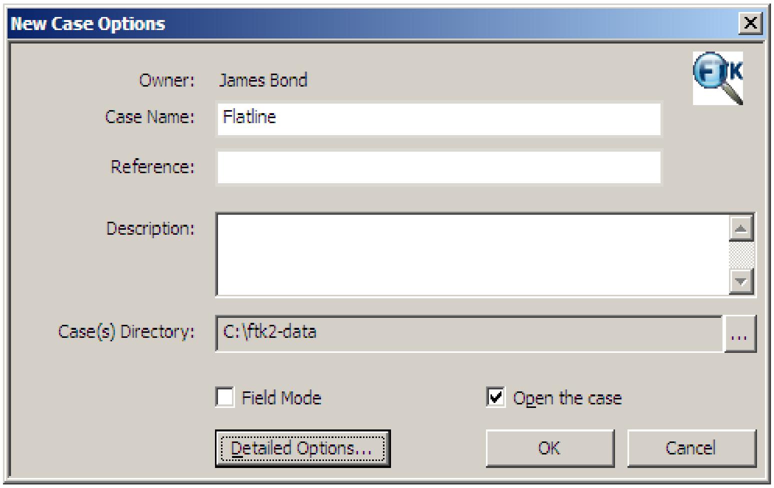
- Create, Add, or Delete cases
- Administer Users
- Data Carve
- Manually data carve
- Assign Users to cases
- Add Evidence
- Access Credant Decryption from the Tools Menu
- Decrypt Files from the Tools Menu
- Mark or View Items Flagged as "Ignorable" or "Privileged."
- Manage the KFF
- Manage Fuzzy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

CREATING A CASE

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

1. Launch FTK 2.2 and login. This opens the Case Management window

2. Click *Case* > *New*.



New Case Options

Owner: James Bond

Case Name: Flatline

Reference:

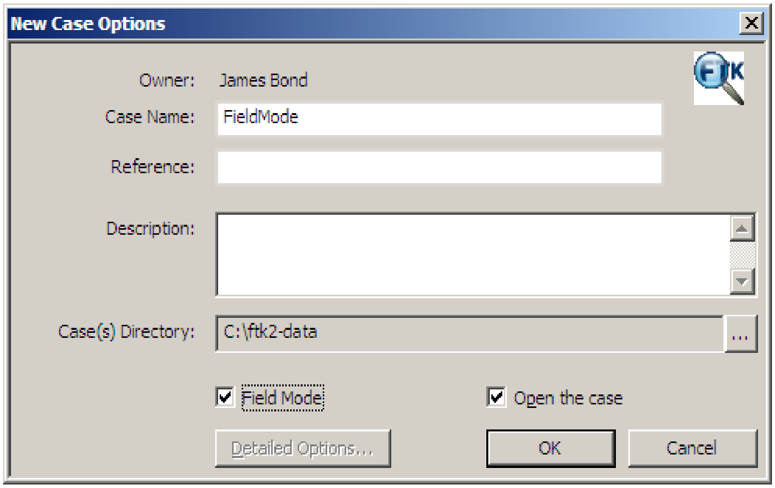
Description:

Case(s) Directory: C:\ftk2-data

□ Field Mode ☑ Open the case

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 ...

   Note: If the c:\ftk2-data folder is not set as shared, an error occurs during case creation.
7. If you wish to create the case in Field Mode, mark the *Field Mode* box. Field Mode disables the *Detailed Options* button when creating a case.



New Case Options

Owner: James Bond

Case Name: FieldMode

Reference:

Description:

Case(s) Directory: C:\ftk2-data

☑ Field Mode ☑ Open the case

In addition to disabling *Detailed Options*, Field Mode bypasses file signature analysis and the Oracle database communication queue. These things vastly speed the processing.

Note: The Job Processing screen will always show 0 for Queued when Field Mode is enabled, because items move directly from Active Tasks to Completed.

8. If you wish to open the case as soon as it is created, mark the *Open the case* box.
9. If you do not select Field Mode, click *Detailed Options* to specify how you wish the evidence to be treated as it is processed and added to the case. The case creation steps are continued in the following section.

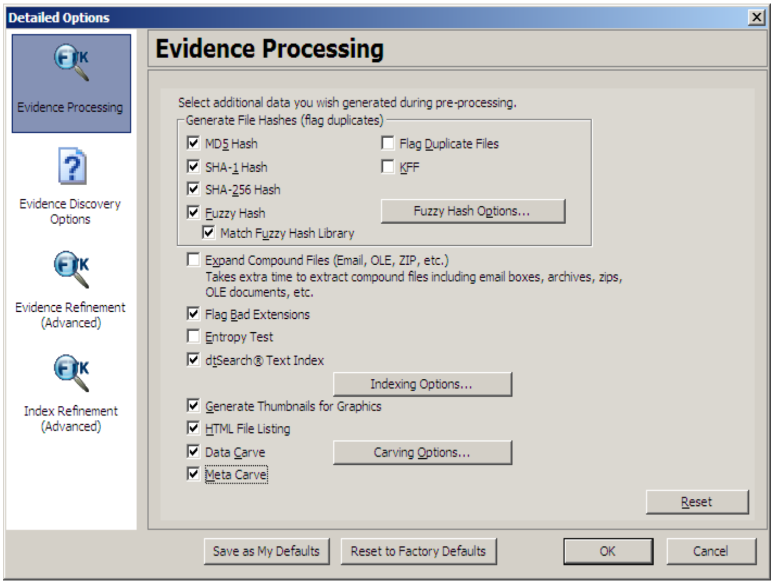
SELECTING EVIDENCE PROCESSING OPTIONS

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 Refinement Options selection screen you will find five buttons:

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

Figure 4-3 Detailed Options Dialog


Detailed Options
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)

Evidence Processing

Select additional data you wish generated during pre-processing.

Generate File Hashes (flag duplicates)

☑ MD5 Hash
☐ Flag Duplicate Files
☑ SHA-1 Hash
☐ KFF
☑ SHA-256 Hash
☑ Fuzzy Hash
Fuzzy Hash Options...
☑ Match Fuzzy Hash Library

☐ Expand Compound Files (Email, OLE, ZIP, etc.)
Takes extra time to extract compound files including email boxes, archives, zips, OLE documents, etc.

☑ Flag Bad Extensions
☐ Entropy Test
☑ dtSearch® Text Index
Indexing Options...
☑ Generate Thumbnails for Graphics
☑ HTML File Listing
☑ Data Carve
Carving Options...
☑ Meta Carve

Reset

Save as My Defaults | Reset to Factory Defaults | OK | Cancel

10. Click *Detailed Options* to choose settings for the case.

    10a. 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 50.

    10b. Click the *Evidence Discovery* icon to specify the location of the File Identification File, if one is to be used. For more information, see Figure , “Selecting Evidence Discovery Options,” on page 61.

    10c. 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 61.

    10d. 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 62.

    10e. Click *OK*.

When you are satisfied with your evidence refinement options, Click *OK* to continue to the Evidence Processing screen.

The following table outlines the Evidence Processing options:

TABLE 4-3

Process	Description
MD5 Hash	Creates a digital fingerprint using the Message Digest 5 algorithm, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. For more information about MD5 hashes, see "Message Digest 5" on page 294.
SHA-1 Hash	Creates a digital fingerprint using the Secure Hash Algorithm-1, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. For more information about SHA hashes, see "Secure Hash Algorithm" on page 296.
SHA-256 Hash	Creates a digital fingerprint using the Secure Hash Algorithm-256, based on the contents of the file. This fingerprint can be used to verify file integrity and to identify duplicate files. SHA-256 is a hash function computed with 32-bit words, giving it a longer digest than SHA-1. For more information about SHA hashes, see "Secure Hash Algorithm" on page 296.
Fuzzy Hash	Mark this box to enable *Fuzzy hash options* and *Match fuzzy hash library*. Fuzzy hash options allow you to compare files which may be similar but not identical, and also to specify the size of files to hash.
Flag Duplicate Files	Identifies files that are found more than once in the evidence. This is done by comparing file hashes.
KFF	Using a database of hashes from known files, this option flags ignorable files and alerts the user to known illicit or dangerous files. Both AD KFF Alert and AD KFF Ignore groups are selected by default. If you have custom groups and you want them to be enabled, specify them under the Case KFF Options. For more information about Known File Filter (KFF), see "Using the Known File Filter" on page 172.
Expand Compound Files	Automatically opens and processes the contents of compound files such as .ZIP, email, and OLE files.
Flag Bad Extensions	Identifies files whose types do not match their extensions, based on the file header information.

TABLE 4-3

Process	Description
Entropy Test	Determines if the data in unknown file types is compressed or encrypted. The compressed and encrypted files identified in the entropy test are not indexed.
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. Click *Indexing Options* for extensive options for indexing the contents of the case.
Generate Thumbnails for Graphics	Creates thumbnails for large graphics. **Note:** All thumbnails are generated in .JPG format, regardless of the original graphic file type.
HTML File Listing	Creates an HTML version of the File Listing in the case folder.
Data Carve	Carves data immediately after pre-processing. Click *Carving Options*, then select the file types to carve. Uses file signatures to identify deleted files contained in the evidence. All available file types are selected by default. For more information on Data Carving, see “Selecting Data Carving Options” on page 60.
Meta Carve	Carves deleted directory entries. This process can uncover dvidence clues that might otherwise not be found.

FUZZY HASHING

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

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

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

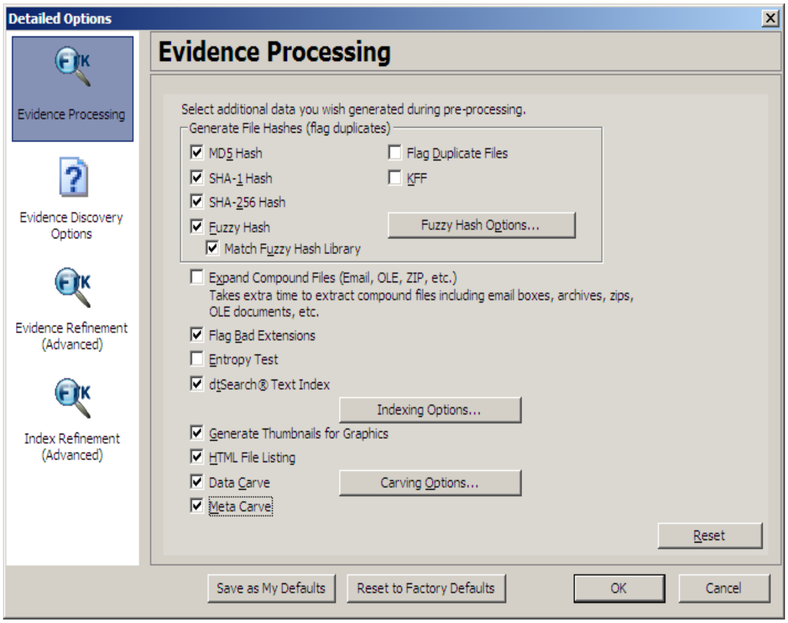
Creating a Fuzzy Hash Library

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

Selecting Fuzzy Hash Options During Initial Processing

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

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



Detailed Options
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)

Evidence Processing

Select additional data you wish generated during pre-processing.

Generate File Hashes (flag duplicates)

☑ MD5 Hash
☐ Flag Duplicate Files
☑ SHA-1 Hash
☐ KFF
☑ SHA-256 Hash
☑ Fuzzy Hash
☑ Match Fuzzy Hash Library

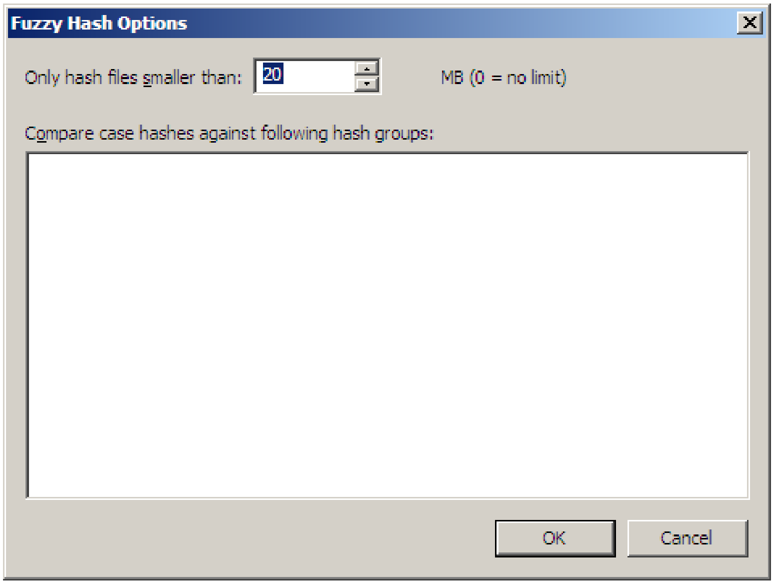
☐ Expand Compound Files (Email, OLE, ZIP, etc.)
Takes extra time to extract compound files including email boxes, archives, zips, OLE documents, etc.

☑ Flag Bad Extensions
☐ Entropy Test
☑ dtSearch® Text Index
☑ Generate Thumbnails for Graphics
☑ HTML File Listing
☑ Data Carve
☑ Meta Carve

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.


Fuzzy Hash Options
Only hash files smaller than:
20
MB (0 = no limit)
Compare case hashes against following hash groups:
OK
Cancel

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

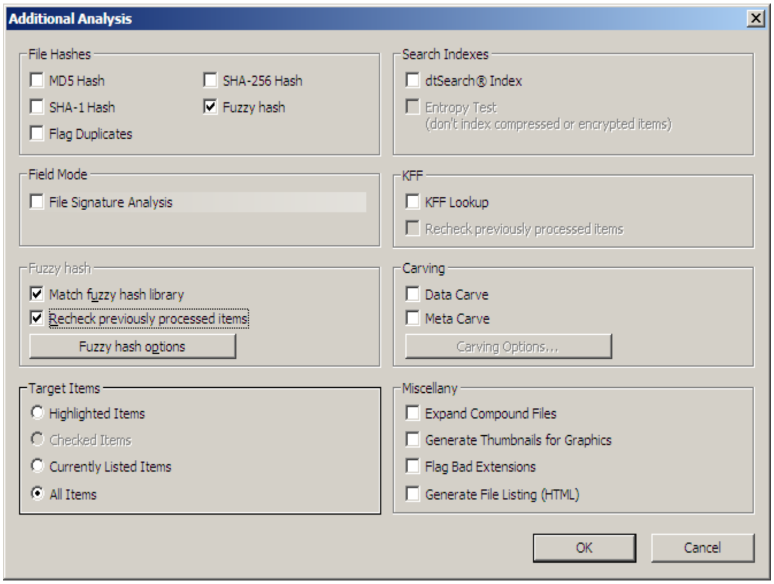
2d. Click *OK* to set the value.

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

Additional Analysis Fuzzy Hashing

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

1. Click *Evidence > Additional Analysis.*



Additional Analysis

File Hashes
- ☐ MD5 Hash
- ☐ SHA-256 Hash
- ☐ SHA-1 Hash
- ☑ Fuzzy hash
- ☐ Flag Duplicates

Search Indexes
- ☐ dtSearch® Index
- ☐ Entropy Test (don't index compressed or encrypted items)

Field Mode
- ☐ File Signature Analysis

KFF
- ☐ KFF Lookup
- ☐ Recheck previously processed items

Fuzzy hash
- ☑ Match fuzzy hash library
- ☑ Recheck previously processed items

Carving
- ☐ Data Carve
- ☐ Meta Carve

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

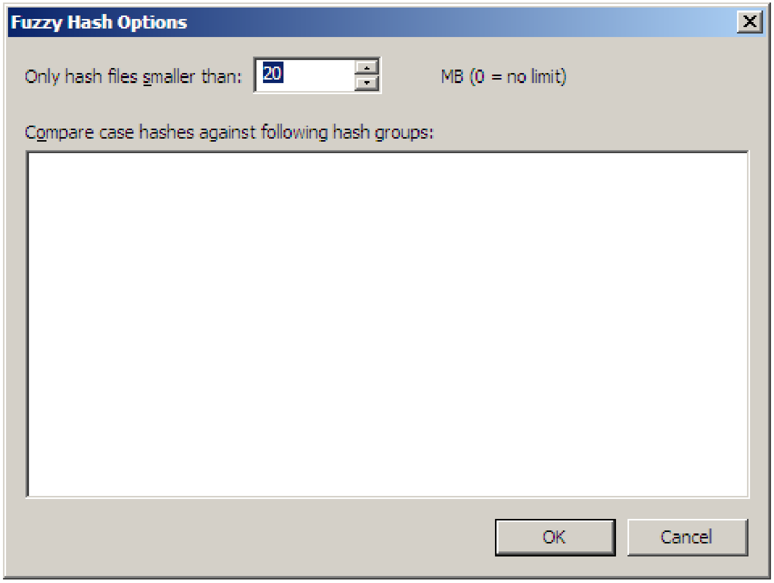
Miscellany
- ☐ Expand Compound Files
- ☐ Generate Thumbnails for Graphics
- ☐ Flag Bad Extensions
- ☐ Generate File Listing (HTML)

2. Select *Fuzzy Hash.*

3. (Optional) Select if the evidence needs to matched against the Fuzzy Hash library.

   3a. (Optional) If performing this additional analysis after adding new information, the fuzzy hashing can be done again against previously processed items.

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



Fuzzy Hash Options

Only hash files smaller than: 20 MB (0 = no limit)

Compare case hashes against following hash groups:

3c. Set the file size limit on the files to be hashed.

3d. Click *OK*.

4. Click *OK* to close the Additional Analysis dialog and begin the fuzzy hashing.

Comparing Files Using Fuzzy Hashing

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

Viewing Fuzzy Hash Results

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

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

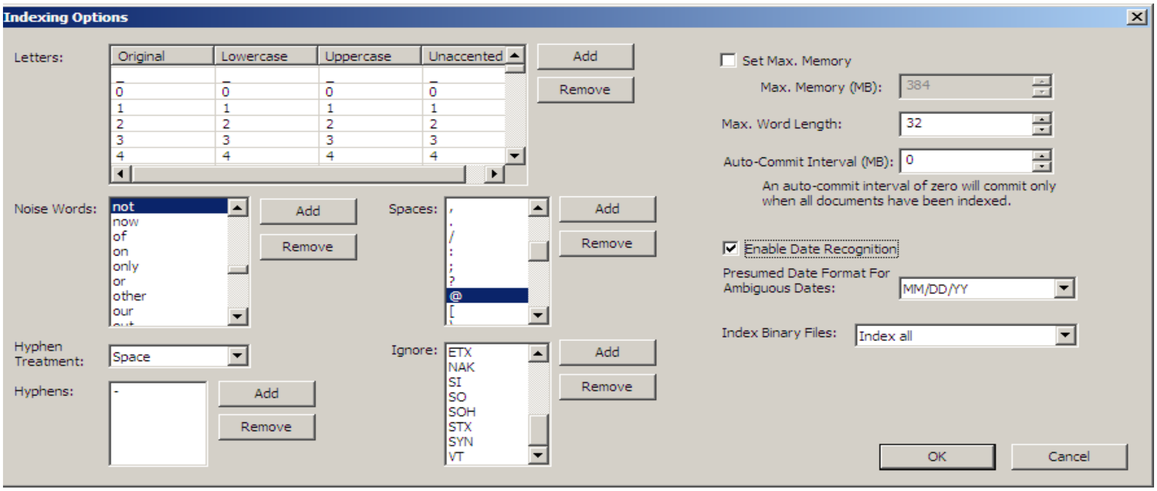
TABLE 4-4 Fuzzy Hash Column Settings

Column Setting	Description
Fuzzy Hash blocksize	Dictates which fuzzy hash values can be used to compare against a file. Fuzzy hashes can only be compared to another fuzzy hash value which is half the fuzzy hash value, equa.l to the actual fuzzy hash value, or two times the fuzzy hash value.
Fuzzy Hash Library Group	The highest matching group value for a file. To find all of the library groups which have been used to compare a file against, double click on the value in column settings.
Fuzzy Hash	The actual fuzzy hash value given to a file.
Fuzzy Hash Library Score	The value of the highest group score a file has been compared against. To find all of the library scores, double click on the value in the column settings.
Fuzzy Hash Library Status	Set to either alert or ignore, which is similar to the KFF alert or ignore settings.

SELECTING DTSEARCH TEXT INDEXING OPTIONS

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

Figure 4-4 dtSearch Text Index: Indexing Options



Letters:

Original	Lowercase	Uppercase	Unaccented
_	_	_	_
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

Noise Words: not, now, of, on, only, or, other, our, out

Spaces: , . / : ; ? @ [\

Hyphen Treatment: Space

Hyphens: -

Ignore: ETX, NAK, SI, SO, SOH, STX, SYN, VT

☐ Set Max. Memory

Max. Memory (MB): 384

Max. Word Length: 32

Auto-Commit Interval (MB): 0

An auto-commit interval of zero will commit only when all documents have been indexed.

☑ Enable Date Recognition

Presumed Date Format For Ambiguous Dates: MM/DD/YY

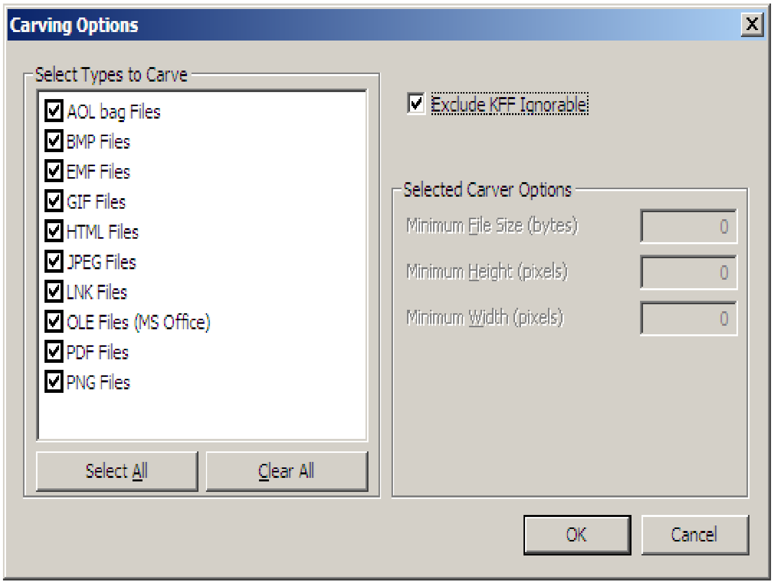
Index Binary Files: Index all

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

For more detailed information regarding the Indexing Options dialog, see “Chapter 7 Searching a Case” on page 143.

Selecting Data Carving Options

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



Carving Options

Select Types to Carve

☑ AOL bag Files
☑ BMP Files
☑ EMF Files
☑ GIF Files
☑ HTML Files
☑ JPEG Files
☑ LNK Files
☑ OLE Files (MS Office)
☑ PDF Files
☑ PNG Files

☑ Exclude KFF Ignorable

Selected Carver Options

Minimum File Size (bytes) 0
Minimum Height (pixels) 0
Minimum Width (pixels) 0

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

1. Select *Data Carve*.
2. Click *Carving Options*.
3. Mark the *Exclude KFF Ignorable* 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 optional limiting factors to be applied to each file type.
    - 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, or index after the fact by clicking and specifying indexing options.

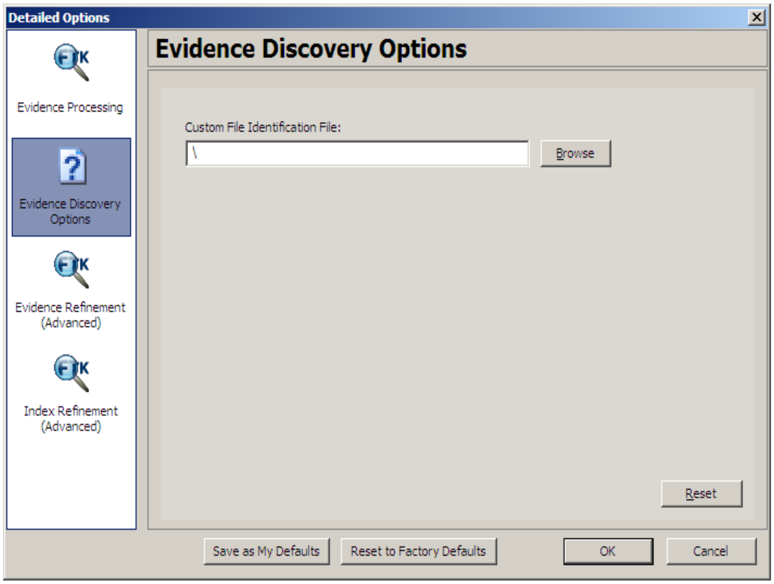
Another factor that can determine which processes to select is schedule. Time restraints may not allow for all tasks to be performed initially. For example, if you disable indexing, it shortens the time needed to process a case. You can return at a later time and index the case if needed.

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 4-5 Evidence Discovery Options



Evidence Discovery Options

Custom File Identification File: \

Detailed Options
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Browse
Reset
Save as My Defaults
Reset to Factory Defaults
OK
Cancel

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 4-5 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 processing 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 is not used, an entropy test may not be needed.

After data is excluded from an evidence item in a case, the same evidence cannot be added back into the case to include the previously excluded evidence. If data that was previously excluded is found necessary, the user must remove the related evidence item from the case, then add the evidence again, using options that will include the desired data.

Use the following steps for refining case evidence:

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

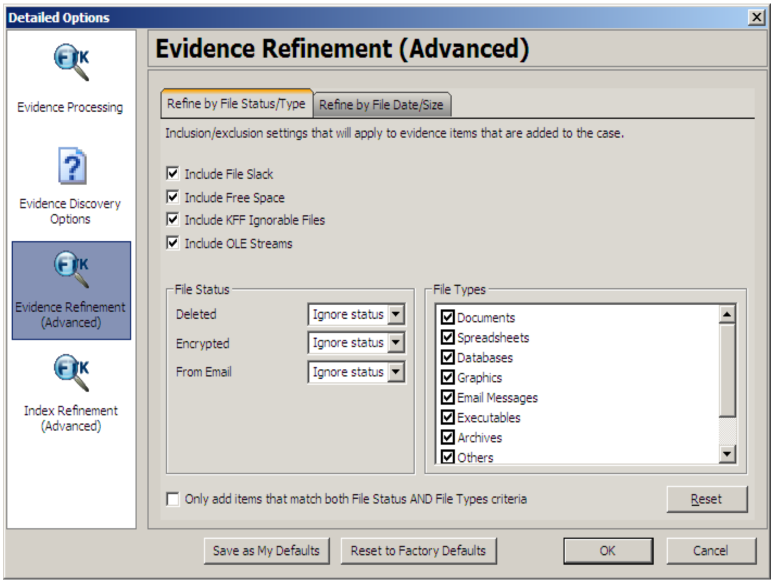
   The Evidence Refinement (Advanced) dialog is organized into two tabs:

   - 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 4-6 Evidence Refinement by File Status/Type


Detailed Options
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Refine by File Status/Type
Refine by File Date/Size
Reset
Save as My Defaults
Reset to Factory Defaults
OK
Cancel

Evidence Refinement (Advanced)

Inclusion/exclusion settings that will apply to evidence items that are added to the case.

☑ Include File Slack
☑ Include Free Space
☑ Include KFF Ignorable Files
☑ Include OLE Streams

File Status

Deleted	Ignore status
Encrypted	Ignore status
From Email	Ignore status

File Types

☑ Documents
☑ Spreadsheets
☑ Databases
☑ Graphics
☑ Email Messages
☑ Executables
☑ Archives
☑ Others

□ Only add items that match both File Status AND File Types criteria

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

TABLE 4-6 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. Options are: • Ignore Status • Include Only • Exclude Defaults to "Ignore Status."

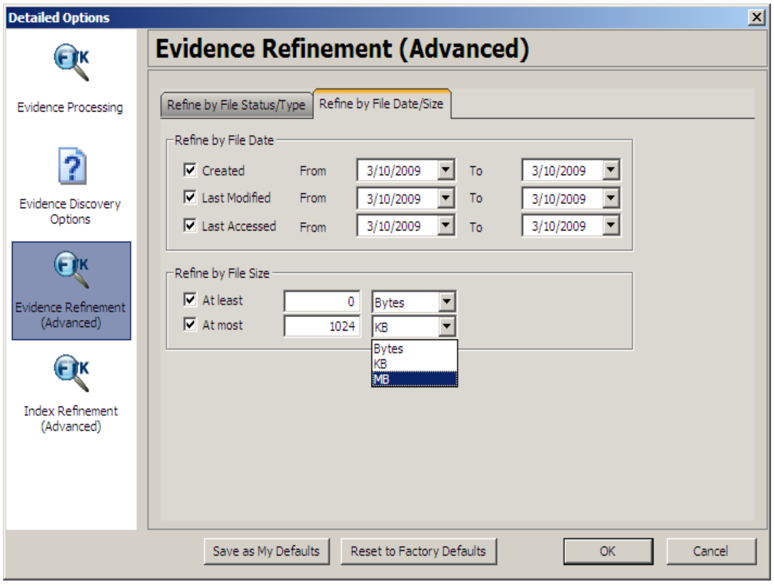
TABLE 4-6 Refine Evidence by File Status/Type Options

Options	Description
Encrypted	Specifies the way to treat encrypted files. Options are: • Ignore Status • Include Only • Exclude Defaults to “Ignore Status.”
From Email	Specifies the way to treat email files. Options are: • Ignore Status • Include Only • Exclude Defaults to “Ignore Status.”
Include OLE Streams	Includes Object Linked or Embedded (OLE) files found within the evidence.
File Types	Specifies types of files to include and exclude.
Match using both File Type and File Status criteria	Applies selected criteria from both tabs to the evidence as it is processed.

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 4-7 Evidence Refinement Dialog


Detailed Options
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Evidence Refinement (Advanced)
Refine by File Status/Type
Refine by File Date/Size
Bytes
KB
MB
Save as My Defaults
Reset to Factory Defaults
OK
Cancel

Refine by File Date

☑ Created From 3/10/2009 To 3/10/2009

☑ Last Modified From 3/10/2009 To 3/10/2009

☑ Last Accessed From 3/10/2009 To 3/10/2009

Refine by File Size

☑ At least 0 Bytes

☑ At most 1024 KB

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

TABLE 4-7 Define Evidence by File Date/Size Options

Exclusion	Description
Refine Evidence by File Date	To refine evidence by file date: 1. Select *Created*, *Last Modified*, or *Last Accessed*. 2. In the two date fields, enter beginning and ending dates.
Refine Evidence by File Size	To refine evidence by file size: 1. In the two size fields, enter the At Least and At Most file size values. 2. In the drop-down list, select *Bytes*, *KB*, or *MB*.

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.

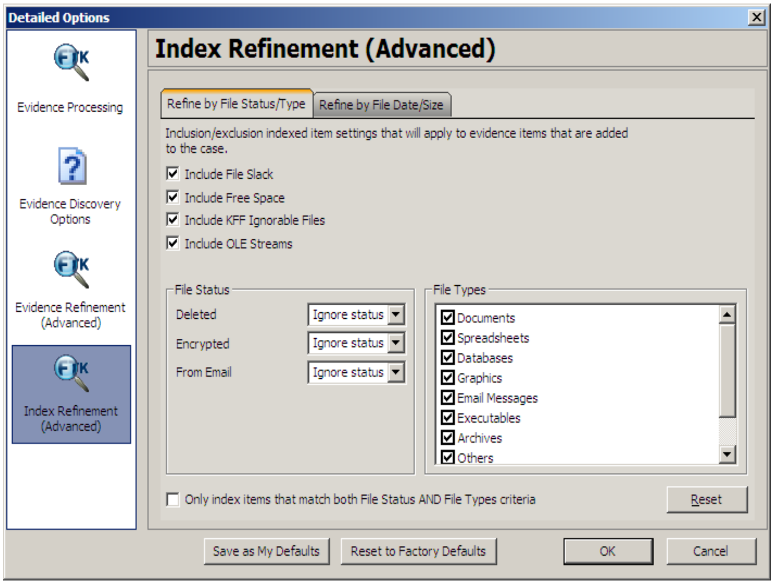
   To reset the menu to the default settings, click *Reset*.

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.

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

Figure 4-8 Index Refinement Dialog


Detailed Options
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Refine by File Status/Type
Refine by File Date/Size
Reset
Save as My Defaults
Reset to Factory Defaults
OK
Cancel

Index Refinement (Advanced)

Inclusion/exclusion indexed item settings that will apply to evidence items that are added to the case.

☑ Include File Slack

☑ Include Free Space

☑ Include KFF Ignorable Files

☑ Include OLE Streams

File Status

Deleted	Ignore status
Encrypted	Ignore status
From Email	Ignore status

File Types

☑ Documents
☑ Spreadsheets
☑ Databases
☑ Graphics
☑ Email Messages
☑ Executables
☑ Archives
☑ Others

☐ Only index items that match both File Status AND File Types criteria

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

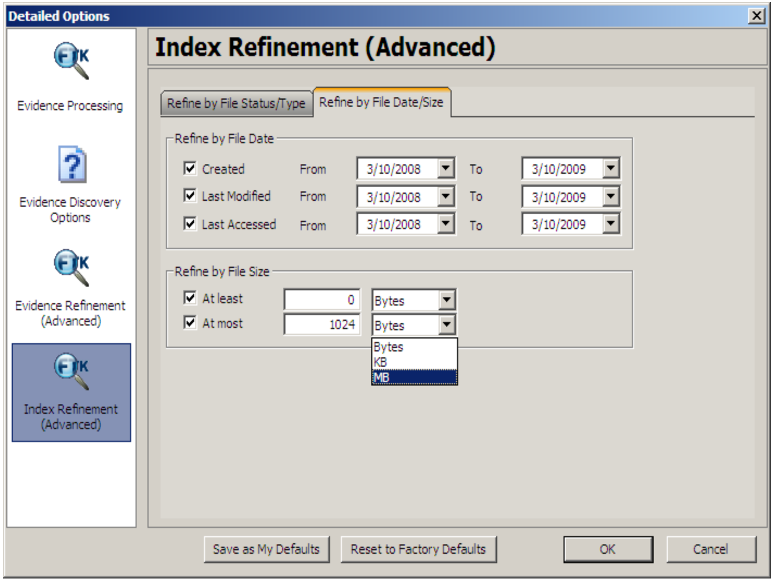
TABLE 4-8 Refine Index by File Status/Type Options

Options	Description
Include File Slack	Mark to include slack space at the end of a file footer, in which evidence may be found.
Include Free Space	Mark to include both allocated (partitioned) and unallocated (unpartitioned) space in which evidence may be found.
Include KFF Ignorable Files	Mark to include files flagged as ignorable in the KFF for analysis.
Deleted	Specifies the way to treat deleted files. Options are: • Ignore status • Include only • Exclude
Encrypted	Specifies the way to treat encrypted files. Options are: • Ignore status • Include only • Exclude
From Email	Specifies the way to treat email files. Options are: • Ignore status • Include only • Exclude
Include OLE Streams	Mark to include encrypted files.
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 4-9 Index Refinement by File Date/Size


Detailed Options
Evidence Processing
Evidence Discovery Options
Evidence Refinement (Advanced)
Index Refinement (Advanced)
Index Refinement (Advanced)
Refine by File Status/Type
Refine by File Date/Size
Save as My Defaults
Reset to Factory Defaults
OK
Cancel

Refine by File Date

☑ Created From 3/10/2008 To 3/10/2009
☑ Last Modified From 3/10/2008 To 3/10/2009
☑ Last Accessed From 3/10/2008 To 3/10/2009

Refine by File Size

☑ At least 0 Bytes
☑ At most 1024 Bytes

Bytes
KB
MB

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

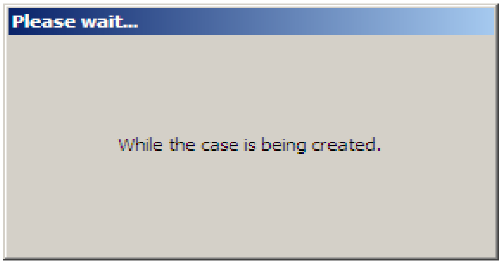
TABLE 4-9 Refine Index by File Date/Size Options

Exclusion	Description
Refine Index by File Date	To refine index content by file date: 1. Select *Created*, *Last Modified*, or *Last Accessed*. In the date fields, enter beginning and ending dates within which to include files.
Refine Index by File Size	To refine index content by file size: 1. In the two size fields, enter minimum and maximum file sizes to include. 2. In the drop-down lists, select whether the specified minimum and maximum file sizes refer to *Bytes*, *KB*, or *MB*.

Creating the Case

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

Figure 4-10 Please Wait While the Case is Being Created



Please wait...

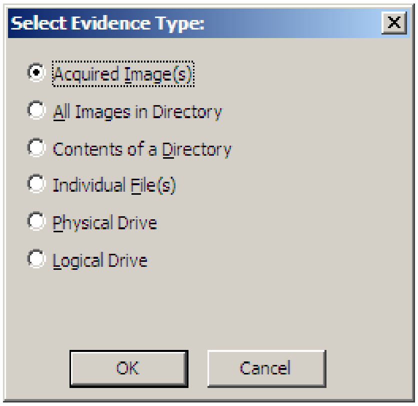
While the case is being created.

ADDING EVIDENCE TO A NEW CASE

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

To add evidence to a case, do the following:

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



Select Evidence Type:

● Acquired Image(s)

○ All Images in Directory

○ Contents of a Directory

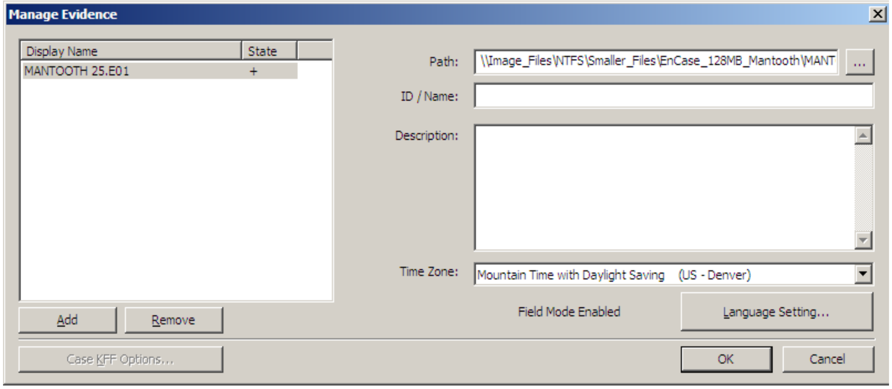
○ Individual File(s)

○ Physical Drive

○ Logical Drive

2. Select the type of evidence item(s) to add to the case at this time.
3. Click *OK*.
4. Browse to the evidence item(s) to add. Select the item(s). Click *Open*.
5. If you are in Field Mode, the Manage Evidence dialog will indicate Field Mode below the Time Zone Selection, will not be able to specify any detailed evidence

options; you will still be able to change the Language Setting however, as shown in the figure below::



Manage Evidence

Display Name	State
MANTOOTH 25.E01	+

Path: \\Image_Files\NTFS\Smaller_Files\EnCase_128MB_Mantooth\MANT

ID / Name:

Description:

Time Zone: Mountain Time with Daylight Saving (US - Denver)

Field Mode Enabled

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

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

TABLE 4-10 Manage Evidence Options

Option	Description
Add	Opens the Select Evidence Type dialog. Click to select the evidence type, and a Windows Explorer instance will open, allowing you to navigate to and select the evidence you choose
Remove	Displays a caution box and asks if you are sure you want to remove the selected evidence item from the case. Removing evidence items that are referenced in bookmarks and reports will remove references to that evidence and they will no longer be available. Click *Yes* to remove the evidence, or click *No* to cancel the operation.
Display Name	The filename of the evidence being added.
Path	The fill pathname of the evidence file. **Note:** Use universal naming convention (UNC) syntax in your evidence path for best results.
ID/Name	The optional ID/Name of the evidence being added.
Description	The options description of the evidence being added. This can be the source of the data, or other description that may prove helpful later.
Time Zone	The time zone of the original evidence. Select a time zone from the drop-down list.

TABLE 4-10 Manage Evidence Options

Option	Description
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 *OK*.
Case KFF Options	Opens the KFF Admin box for managing KFF libraries, groups, and sets.
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 Dafaults, but you can click *Reset* to reset these options to the Factory Defaults. Select the options to apply to the evidence being added, then click *OK* to close the dialog.

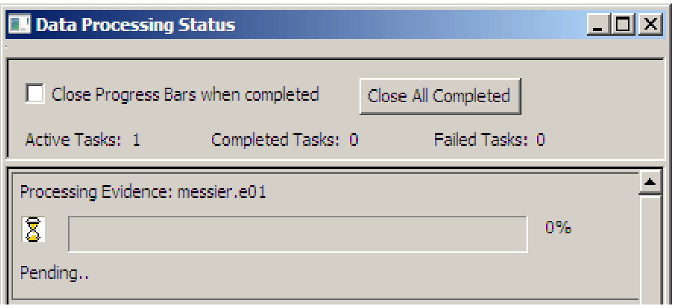
7. When you are satisfied with the evidence options selected, click *OK*.

PROCESSING EVIDENCE

FTK shows the Data Processing Status screen with at least one progress bar similar to those in the following figures:

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

Figure 4-11 Data Processing Status: Pending



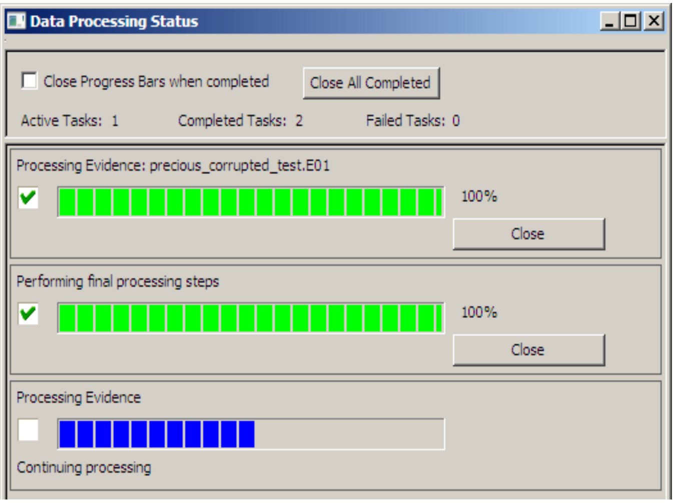
Active Tasks: 1 Completed Tasks: 0 Failed Tasks: 0

Processing Evidence: messier.e01

0%

Pending..

Figure 4-12 Data Processing Status: Once Complete, One In Progress



□ Close Progress Bars when completed

Active Tasks: 1 Completed Tasks: 2 Failed Tasks: 0

Processing Evidence: precious_corrupted_test.E01

✓ 100%

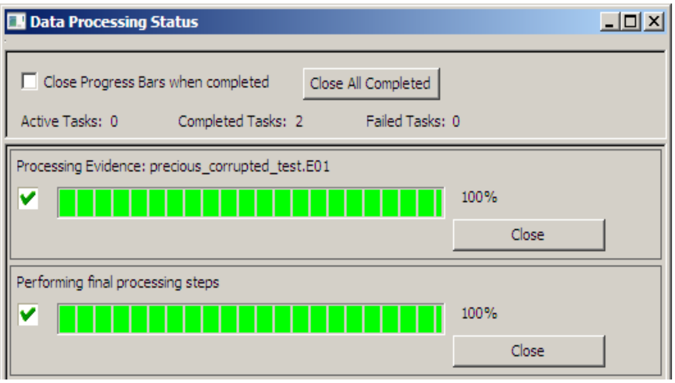
Performing final processing steps

✓ 100%

Processing Evidence

Continuing processing

Figure 4-13 Data Processing Status: Successfully Completed



□ Close Progress Bars when completed

Active Tasks: 0 Completed Tasks: 2 Failed Tasks: 0

Processing Evidence: precious_corrupted_test.E01

✓ 100%

Performing final processing steps

✓ 100%

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 withing 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.

The FTK User Interface

When a case has been created, before evidence has been added you will see the FTK User Interface. The FTK User Interface is described in detail in Chapter 5. For more information, see "Chapter 5 Adding and Processing Evidence" on page 77.

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.

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

Backing Up the Case

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

Backup your case from the Case Management window.

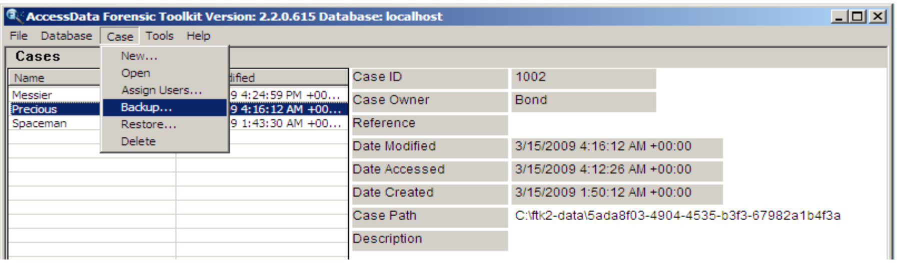
When backing up a case, FTK copies case information and database files (but not the evidence) to a chosen folder. Keep copies of your drive images and other evidence independent of the backed-up case. Individual files and folders processed into the case are converted to an .AD1 (custom content) image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

Important: 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 Management window, click *Case* > *Backup*.



Name	...dified
Messier	9 4:24:59 PM +00...
Precious	9 4:16:12 AM +00...
Spaceman	9 1:43:30 AM +00...

Case ID	1002
Case Owner	Bond
Reference	
Date Modified	3/15/2009 4:16:12 AM +00:00
Date Accessed	3/15/2009 4:12:26 AM +00:00
Date Created	3/15/2009 1:50:12 AM +00:00
Case Path	C:\ftk2-data\5ada8f03-4904-4535-b3f3-67982a1b4f3a
Description	

2. In the Save As dialog, select an archive folder location.
3. Click *Save*.

Restoring a Case

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

To restore a case:

1. In the Case Management 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 Management window, highlight the case to delete from the database.
2. Click *Case* > *Delete*.
3. Click *Yes* to confirm deletion. Allow ample time for the case to be deleted.

Storing Case Files

Storing case files and evidence on the same drive substantially taxes the processors' throughput. The system slows as it saves and reads huge files. For desktop systems in laboratories, increase the processing speed by saving evidence files to a separate server. For more information, see the "Installation Configuration Options" on page 14.

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, such as on a laptop.

Chapter 5 Adding and Processing Evidence

After creating a case in AccessData Forensic Toolkit (FTK) Case Management, open the case. Investigate the case by running searches, bookmarking, and exporting relevant files, verifying the drive image integrity, identifying the evidence, and performing other tasks. For more information regarding creating a new case, see “Chapter 4 Starting a New FTK 2.2 Case” on page 45.

OPENING AN EXISTING CASE

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

1. Log on to FTK 2.2.
2. Double-click on the case you want to open, or highlight the case and click *Case > Open*.

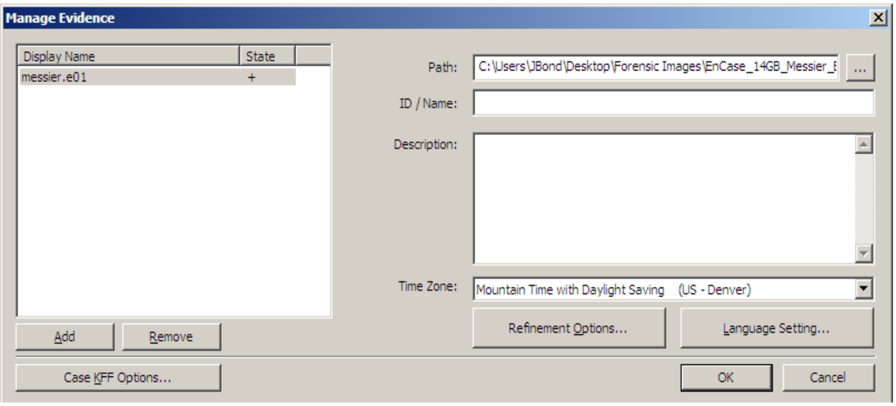
ADDING EVIDENCE

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.

To add evidence 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



Display Name	State
messier.e01	+

Path: C:\Users\JBond\Desktop\Forensic Images\EnCase_14GB_Messier_E

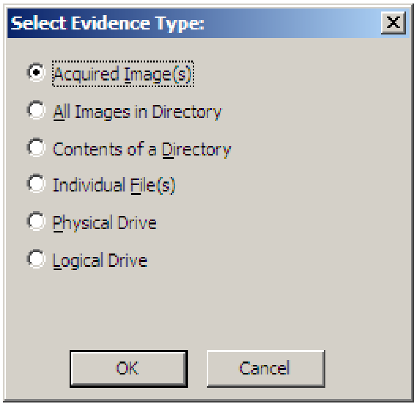
ID / Name:

Description:

Time Zone: Mountain Time with Daylight Saving (US - Denver)

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

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



● Acquired Image(s)
○ All Images in Directory
○ Contents of a Directory
○ Individual File(s)
○ Physical Drive
○ Logical Drive

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

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

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

4a. (Optional) Click the ellipsis button ... at the end of the Path field to browse to another path.

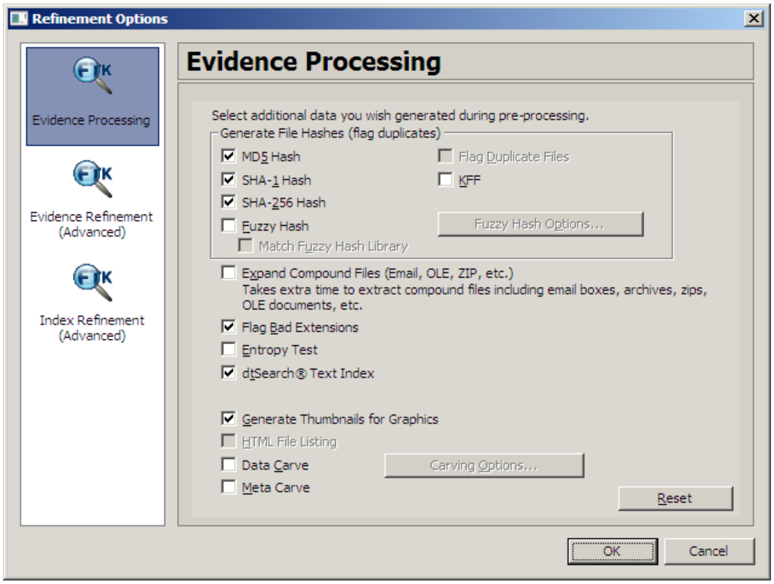
5. Fill in the ID/Name field with any specific ID or Name data applied to this evidence for this case.

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.



Evidence Processing

Select additional data you wish generated during pre-processing.

Generate File Hashes (flag duplicates)

☑ MD5 Hash □ Flag Duplicate Files

☑ SHA-1 Hash □ KFF

☑ SHA-256 Hash

□ Fuzzy Hash

□ Match Fuzzy Hash Library

□ Expand Compound Files (Email, OLE, ZIP, etc.)
Takes extra time to extract compound files including email boxes, archives, zips, OLE documents, etc.

☑ Flag Bad Extensions

□ Entropy Test

☑ dtSearch® Text Index

☑ Generate Thumbnails for Graphics

□ HTML File Listing

□ Data Carve

□ Meta Carve

The sections available are:

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

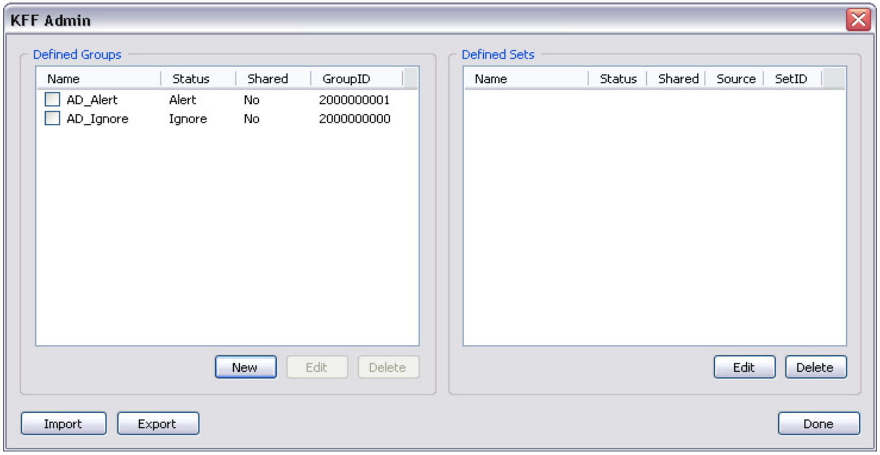
For more information on Evidence Processing options, see “Selecting Evidence Processing Options” on page 50.

For more information on Evidence Refinement (Advanced) options, see “Selecting Evidence Refinement (Advanced) Options” on page 63.

For more information on Index Refinement (Advanced), see “Selecting Index Refinement (Advanced) Options” on page 66.

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

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



Name	Status	Shared	GroupID
☐ AD_Alert	Alert	No	2000000001
☐ AD_Ignore	Ignore	No	2000000000

Name	Status	Shared	Source	SetID

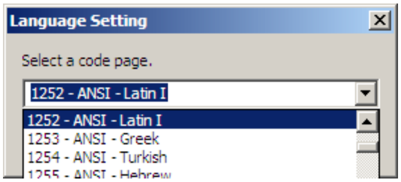
See “Using the Known File Filter” on page 172 for detailed information about the KFF.

11. Click *Done* to accept settings and return to the Manage Evidence dialog.
12. Click *Language Settings* to select the codepage for the language for viewing the evidence.
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



Language Setting

Select a code page.

1252 - ANSI - Latin I

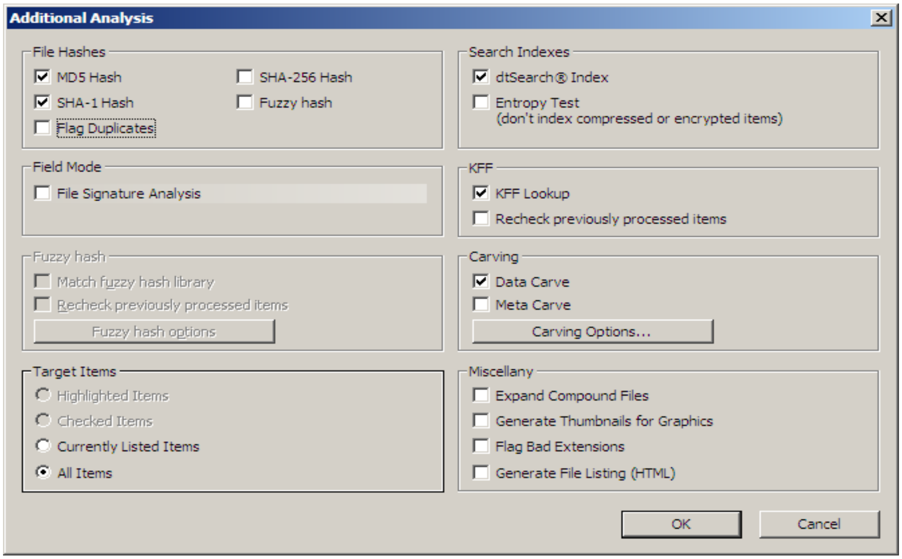
- 1252 - ANSI - Latin I
- 1253 - ANSI - Greek
- 1254 - ANSI - Turkish
- 1255 - ANSI - Hebrew

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



Additional Analysis

File Hashes

- ☑ MD5 Hash
- ☐ SHA-256 Hash
- ☑ SHA-1 Hash
- ☐ Fuzzy hash
- ☐ Flag Duplicates

Field Mode

- ☐ File Signature Analysis

Fuzzy hash

- ☐ Match fuzzy hash library
- ☐ Recheck previously processed items

Target Items

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

Search Indexes

- ☑ dtSearch® Index
- ☐ Entropy Test (don't index compressed or encrypted items)

KFF

- ☑ KFF Lookup
- ☐ Recheck previously processed items

Carving

- ☑ Data Carve
- ☐ Meta Carve

Miscellany

- ☐ Expand Compound Files
- ☐ Generate Thumbnails for Graphics
- ☐ Flag Bad Extensions
- ☐ Generate File Listing (HTML)

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.

Field	**Description**
File Hashes	These options create file hashes for the evidence. The Options are: • MD5 Hash • SHA-1 • SHA-256 • Fuzzy Hash • Flag Duplicates 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 *Flag Duplicates*. Marking Flag Duplicates produces an information message stating that "Changing this setting will apply to all items, regardless of whether "All Items" is selected. Proceed anyway?" Click *Yes* to flag all duplicates found in the case, or click *No* to unmark *Flag Duplicates*. For more information about MD5 hashes, see "Message Digest 5" on page 294. For more information about SHA hashes, see "Secure Hash Algorithm" on page 296.For more information about Fuzzy Hashing, see, "Fuzzy Hashing" on page 53.
Field Mode	If you are processing this case in Field Mode, you can select File Signature Analysis, which is not otherwise done in Field Mode.
Target Items	Select the items on which to perform the additional analysis. Highlighted, and Checked items will be unavailable if no items in the case are highlighted or checked. The following list shows the available options: • **Highlighted Items**: Performs the additional analysis on the items highlighted in the File List pane when you select Additional Analysis. • **Checked Items**: Performs the additional analysis on the checked evidence items in the File List pane when you select Additional Analysis. • **Currently Listed Items**: Performs the additional analysis on all the evidence items currently listed in the File List pane when you selecte Additional Analysis. • **All Items**: Performs the additional analysis on all evidence items in the case.

Field	Description
Search Indexes	Choose *dtSearch® Index* to create a dtSearch index that enables index searches. Marking *dtSearch® Index* activates the Entropy Test check box. Select *Entropy Test* to exclude compressed or encrypted items from the index.
KFF	Select *KFF Lookup* to filter targeted files in the KFF. When *KFF Lookup* is selected, the user can select to *Recheck previously processed items* when searching for new information, or when a KFF group is added or changed.
Carving	Click *Carving Options*, to select the file types to carve. Options are: • **Data Carve**: When selected, the Carving Options button is active. • **Meta Carve**: Marking or unmarking has no effect on the Carving Options button. Carving uses file signatures to identify deleted files contained in the evidence. More detailed information on Data Carving is presented following this table.
Miscellany	These miscellaneous options apply when performing the additional analysis: • **Expand Compound Files**: Opens compound files such as ZIP and indexes the contained files. • **Generate Thumbnails for Graphics**: Generates thumbnail graphics of the analyzed graphics. • **Flag Bad Extensions**: Lists file extensions where the extension does not match the data header type from the selected and analyzed files. • **Generate File Listing (HTML)**: 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. For further information on using the EFS, see "Decrypting Files and Folders" on page 179.

DATA CARVING

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

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

The data carving feature allows 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 child object is created with a name reflecting the type of object carved and its offset into the parent object's data stream. FTK can find any embedded or deleted item as long as the file header still exists.

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

TABLE 5-1 Recognized File Types for Data Carving

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

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

Data Carving Files When Processing a New Case

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

For more information, see "Selecting Evidence Processing Options" on page 50.

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 objects and files are added to the case, and can be searched, bookmarked, and organized along with the existing files. For more information, see “Chapter 6 Using Tabs to Explore & Refine Evidence” on page 105.

THE FTK USER INTERFACE

The FTK user interface is comprised of several components. There is a Menu Bar, a ToolBar, UI Tabs, and various panes. The user interface has many customizable features. For more information on customizing the FTK 2.2 user interface, see“Chapter 11 Customizing the Interface” on page 207.

MENU BAR

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

TABLE 5-2 FTK 2.2 Menu Bar Items

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

The following tables show the available options from the FTK 2.2 window menus.

File Menu Options

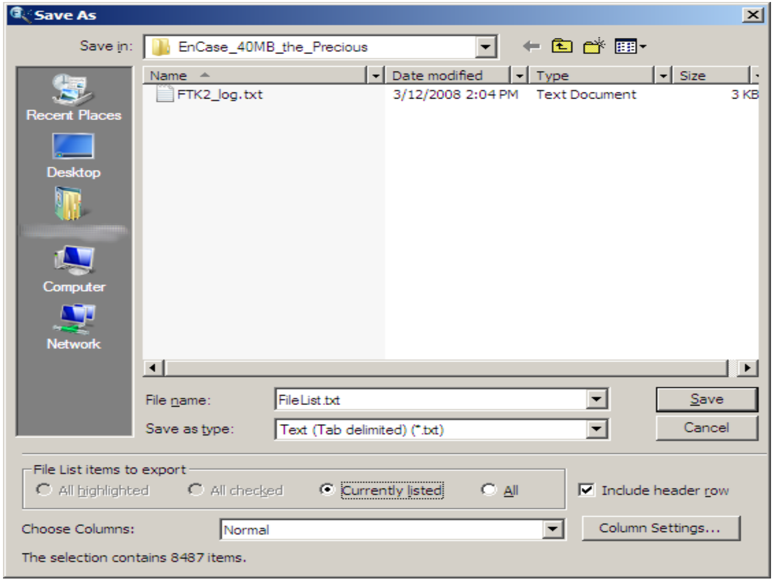
TABLE 5-3 FTK 2.2 File Menu

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 .csv, .tsv, and .txt formats.
Export Word List	Exports the index as a text file from which a dictionary for PRTK can be created.
Report	Opens the Report Options window for creating a case report.
Close	Closes the FTK Window and returns to the Case Management window.
Exit	Closes both the FTK and Case Management windows.

Export File List Info

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

Figure 5-4 Export File List Info Dialog



Save in: EnCase_40MB_the_Precious

Name	Date modified	Type	Size
FTK2_log.txt	3/12/2008 2:04 PM	Text Document	3 KB

File name: FileList.txt

Save as type: Text (Tab delimited) (*.txt)

File List items to export

○ All highlighted ○ All checked ● Currently listed ○ All

☑ Include header row

Choose Columns: Normal

The selection contains 8487 items.

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 “Export File List Info” on page 86.

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

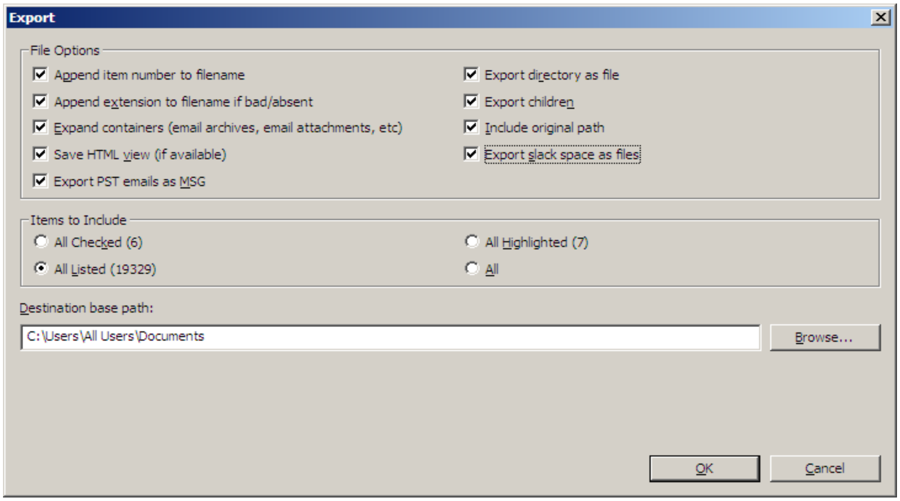
1. Select *File > Export File List Info*, or click *Export File List* on the File List pane, or right-click on a file in the File List pane and select *Export File List Info.*
2. Select the File List Items to Export.
3. Choose whether to include a header row in the exported file.
4. Select column information.
5. Specify the filename for the exported information.
6. Browse to and select the destination folder for the exported file.

Click *Save.*

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 nor Registry Viewer can read files within a drive image.) The following figure represents the Export Files dialog.

Figure 5-5 Export Files Dialog



Export

File Options

☑ Append item number to filename

☑ Append extension to filename if bad/absent

☑ Expand containers (email archives, email attachments, etc)

☑ Save HTML view (if available)

☑ Export PST emails as MSG

☑ Export directory as file

☑ Export children

☑ Include original path

☑ Export slack space as files

Items to Include

○ All Checked (6)

● All Listed (19329)

○ All Highlighted (7)

○ All

Destination base path: C:\Users\All Users\Documents

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 5-4 Export Files Dialog Options

Option	Description
Append Item number to Filename	Appends the FTK unique File ID to a filename.
Append extension to filename if bad/absent	Adds the extension to a filename if it is bad or missing, based on the file's header information.
Expand containers (email archives, email attachments, etc.)	Expands container-type files and exports their contents.
Save HTML view (if available)	If a file can be exported and saved in HTML format, it will be done.

TABLE 5-4 Export Files Dialog Options

Option	Description
Export PST emails as MSG	Exports PST email format to MSG format for broader compatibility.
Export directory as file	Creates a file containing the binary data of the directory being exported.
Export children	Exports all child files of a parent folder.
Include original path	Includes the full path from the root to the file; maintains folder structure for exported files.
Export slack space as files	Exports slack space from files and saves it as files for easier viewing.

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

TABLE 5-5 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 file location.

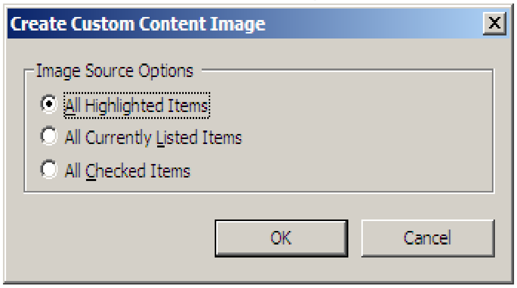
   The default path is C:\case_folder\Report\Export\.

5. Click *OK* to begin the export.

EXPORTING TO IMAGE

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

1. Click File > Export to Image.



Create Custom Content Image

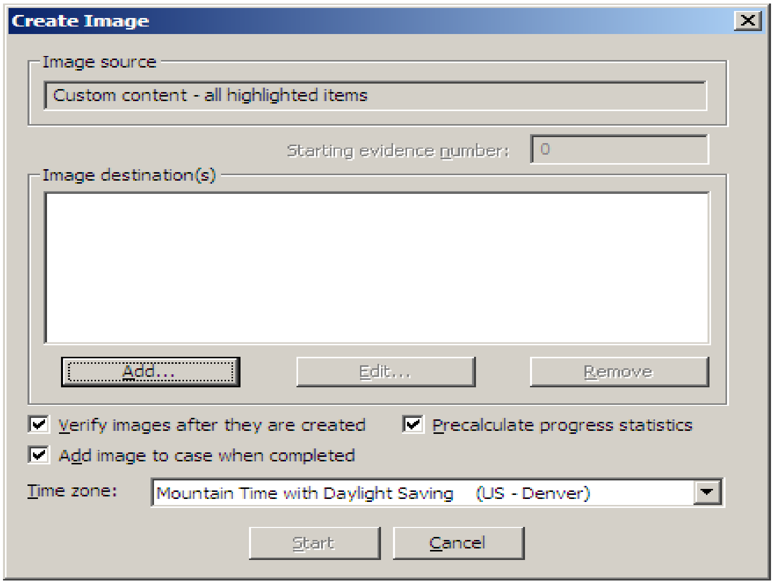
Image Source Options

● All Highlighted Items

○ All Currently Listed Items

○ All Checked Items

2. Select the Image Source for your AD1 file.
3. Click *OK*.



Create Image

Image source: Custom content - all highlighted items

Starting evidence number: 0

Image destination(s)

☑ Verify images after they are created

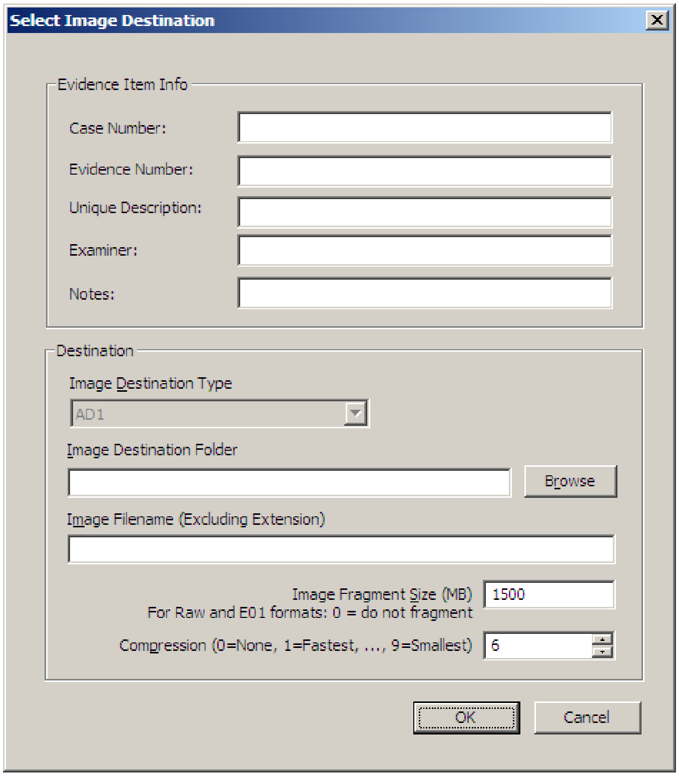
☑ Precalculate progress statistics

☑ Add image to case when completed

Time zone: Mountain Time with Daylight Saving (US - Denver)

4. In the Create Image Dialog, .click *Add*. This brings up the Select Image Destination dialog.
5. Specify the options under Evidence Item Info and Destination. When you are satisfied that the information you have provided is accurate, click *OK*.

6. Select the processing options you want.



Select Image Destination

Evidence Item Info

Case Number:

Evidence Number:

Unique Description:

Examiner:

Notes:

Destination

Image Destination Type: AD1

Image Destination Folder:

Image Filename (Excluding Extension):

Image Fragment Size (MB): 1500
For Raw and E01 formats: 0 = do not fragment

Compression (0=None, 1=Fastest, ..., 9=Smallest): 6

7. Specify the Time Zone of the evidene.
8. Click Start to begin the AD1 image creation, or click Cancel to return to the main FTK 2.2 user interface window.

Exporting the Word List

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

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

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

1. Select *File > Export Word List.*

2. Select the Registry Keys to export to the word list.
3. Click *Export*.
4. Select the filename and location for the exported word list. Click Browse Folders to select the folder location for the wordlist file.

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

EDIT MENU OPTIONS

TABLE 5-6 FTK 2.2 Edit Menu

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

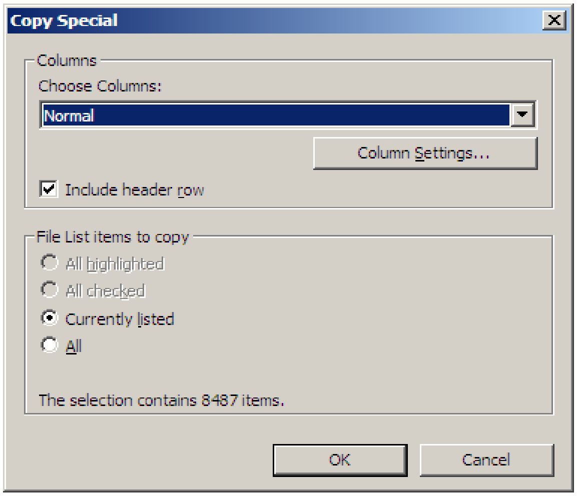
COPYING INFORMATION FROM FTK

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

To copy file information perform the following steps:

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

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



Copy Special

Columns

Choose Columns: Normal

Column Settings...

☑ Include header row

File List items to copy

○ All highlighted

○ All checked

● Currently listed

○ All

The selection contains 8487 items.

3. In the Copy Special dialog, select from the following:

TABLE 5-7 Copy Special Dialog Options

Item	Description
Choose Columns	From the drop-down, select the column template to use, or click *Column Settings* 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. **Note:** Items remain highlighted only as long as the same tab is displayed.
All Checked	All items checked in all file lists. You can check files in multiple lists. Checked items remain checked until you uncheck them.
Currently Listed	All items in the current file list.
All	All items in the case. **Note:** Selecting All Items can create a very large TSV or .CSV file, and can exceed the 10,000 item capacity of the clipboard.

4. In the Choose Columns drop-down list, select the column template that contains the file information that you want to copy.

5. To define a new column settings template click *Column Settings* to open the Column Settings manager.

   5a. Create the column settings template you need.

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

5c. Close the Column Settings manager.

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

For more information about Column Settings, see “Creating and Modifying Column Settings” on page 214.

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

VIEW MENU OPTIONS

TABLE 5-8 FTK 2.2 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: • Large-default • Medium • Small • Tiny
Tab Layout	Manages tab settings: the user can lock an existing setting, add and remove settings, save settings one tab at a time or all at once. The user can also restore previous settings. or reset them to the default settings. These options are in the following list: • Lock • Add • Remove • Save • Save All Layouts • Restore • Reset to Default
Explore Tree	Displays the Explore Tree in the upper-left pane.
Graphics Tree	Displays the Graphics Tree in the upper-left pane.
Overview Tree	Displays the Overview Tree in the upper-left pane.
Email Tree	Displays the Email Tree in the upper-left pane.
Bookmark Tree	Displays the Bookmark pane in the upper-left pane.
Indexed Searches	Displays the Index Search Results pane in the upper-left pane.
Live Searches	Displays the Live Search Results pane in the upper-left pane.
Bookmark Information	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. 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.

TABLE 5-8 FTK 2.2 View Menu

Option	Description
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.

EVIDENCE MENU OPTIONS

TABLE 5-9 FTK 2.2 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.

FILTER MENU OPTIONS

TABLE 5-10 FTK 2.2 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.

TOOLS MENU OTIONS

TABLE 5-11 FTK 2.2 Tools Menu

Option	Description
KFF	Known File Filter (KFF) sets and groups can be managed, archived, and cleared. The following menu option is available: • Manage

TABLE 5-11 FTK 2.2 Tools Menu

Option	Description
Fuzzy Hash	Allows you to • Find Similar Files • Manage Fuzzy Hash Library
Decrypt Files	Decrypts EFS and Microsoft Office files passwords that matched those entered.
Credant Decryption	Opens the tools for Credant 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.
Verify Image Integrity	Generates hash values of the disk image file for comparison.
Disk Viewer	Opens a viewer that allows you to see and search evidence items.
Other Applications	Opens other AccessData tools to complement the investigational analysis: • Imager • PRTK • Registry Viewer • LicenseManager • Language Selector

VERIFYING DRIVE IMAGE INTEGRITY

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

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

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

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

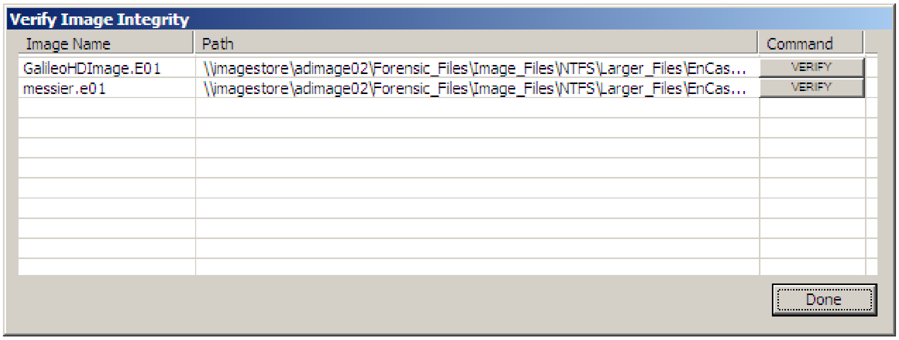


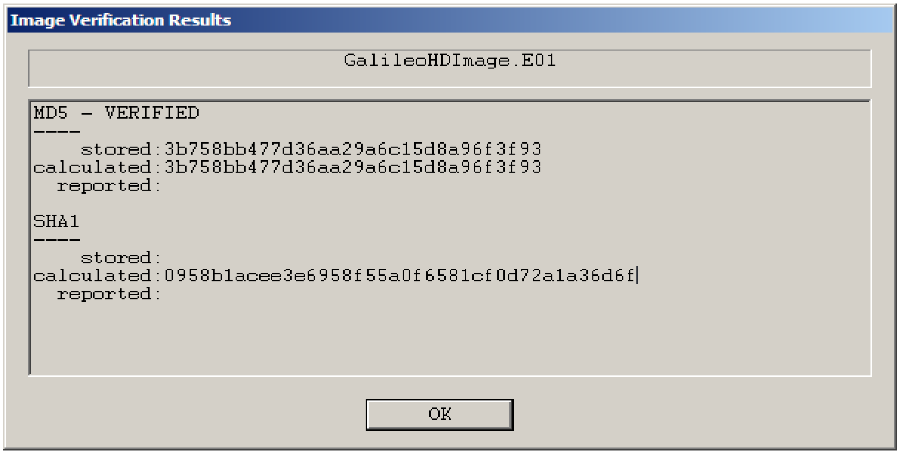
Image Name	Path	Command
GalileoHDImage.E01	\\imagestore\adimage02\Forensic_Files\Image_Files\NTFS\Larger_Files\EnCas...	VERIFY
messier.e01	\\imagestore\adimage02\Forensic_Files\Image_Files\NTFS\Larger_Files\EnCas...	VERIFY

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 5-12 Verify Image Integrity

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

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



```
MD5 - VERIFIED
----
    stored:3b758bb477d36aa29a6c15d8a96f3f93
calculated:3b758bb477d36aa29a6c15d8a96f3f93
  reported:

SHA1
----
    stored:
calculated:0958b1acee3e6958f55a0f6581cf0d72a1a36d6f
  reported:
```

The Progress Dialog appears and displays the status of the verification. If the image file has a stored hash, when the verification is complete, the dialog shows and compares both hashes. Completing the processes may take some time, depending on the size of the evidence, the processor type, and the amount of available RAM.

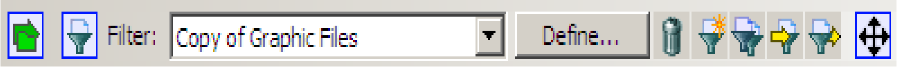
Help Menu Options

TABLE 5-13 FTK 2.2 Help Menu

Option	Description
User Guide	Provides a link to the FTK 2.2 User Guide.
Diagnostics	Allows the troubleshooting of database connections.
About	Provides information about the current FTK release.

Toolbar Components

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



The following table shows the available components of the toolbar.

TABLE 5-14 Toolbar Components

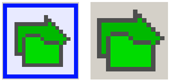
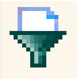
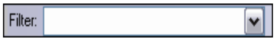
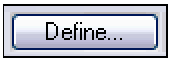
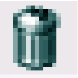
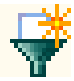
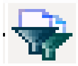
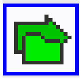
Component	Description
	Turns Quick Picks On or Off. The blue border indicates QuickPicks is On. The gray background and lack of a border indicates QuickPicks is Off.
	Turns the filter on or off. Filtered data is shown in a colored pane to indicate that it is filtered.
 Filter:	Applies the selected filter. A drop-down menu lists defined filters.
 Define...	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

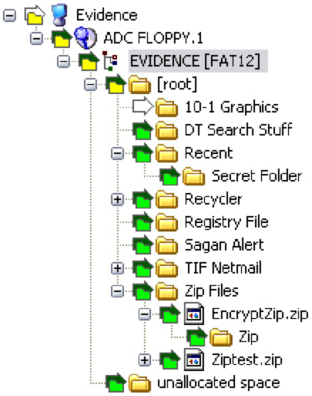
TABLE 5-14 Toolbar Components

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.

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 5-6 QuickPicks Filter Folder Selection



```
⊟ Evidence
  ⊟ ADC FLOPPY.1
    ⊟ EVIDENCE [FAT12]
      ⊟ [root]
          10-1 Graphics
          DT Search Stuff
        ⊟ Recent
            Secret Folder
        ⊞ Recycler
          Registry File
          Sagan Alert
        ⊞ TIF Netmail
        ⊟ Zip Files
          ⊟ EncryptZip.zip
              Zip
          ⊞ Ziptest.zip
        unallocated space
```

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 decendent folder 10-1 Graphics is unselected. Its arrow icon is white.

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

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

File List Pane

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

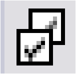
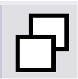
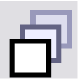
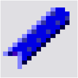
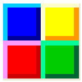
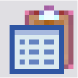
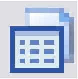
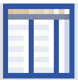
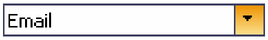
When viewing data in the File List, use the type-down control feature to locate specific files. When the list is sorted by name, select an item in the list, then type the first letter of the desired file. FTK will move down the list to the first file beginning with that letter. The more letters you type,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

For more information, see "Customizing File List Columns" on page 213.

File List Toolbar

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

TABLE 5-15 File List Toolbar

Component	Description
	Checks all of the files in the current list.
	Unchecks all of the files in the current list.
	Unchecks all of the files in the current case.
	Opens Create New Bookmark dialog box.
	Opens Manage Labels dialog box.
	Opens Copy Special dialog box.
	Opens the Export File List, allowing the user to save selected files to another folder..
	Opens the Column Settings dialog box.
 Email	Sets the columns to a specific set from the following list • Normal (Default) • Email • File Listing • Normal (default) • Reports: File Path Section • Reports: Standard

USING TABS

The FTK 2.x user interface is organized into tabbed pages to make organization and navigation easier. For a detailed description of the FTK 2.x tabbed pages, see “Chapter 6 Using Tabs to Explore & Refine Evidence” on page 105.

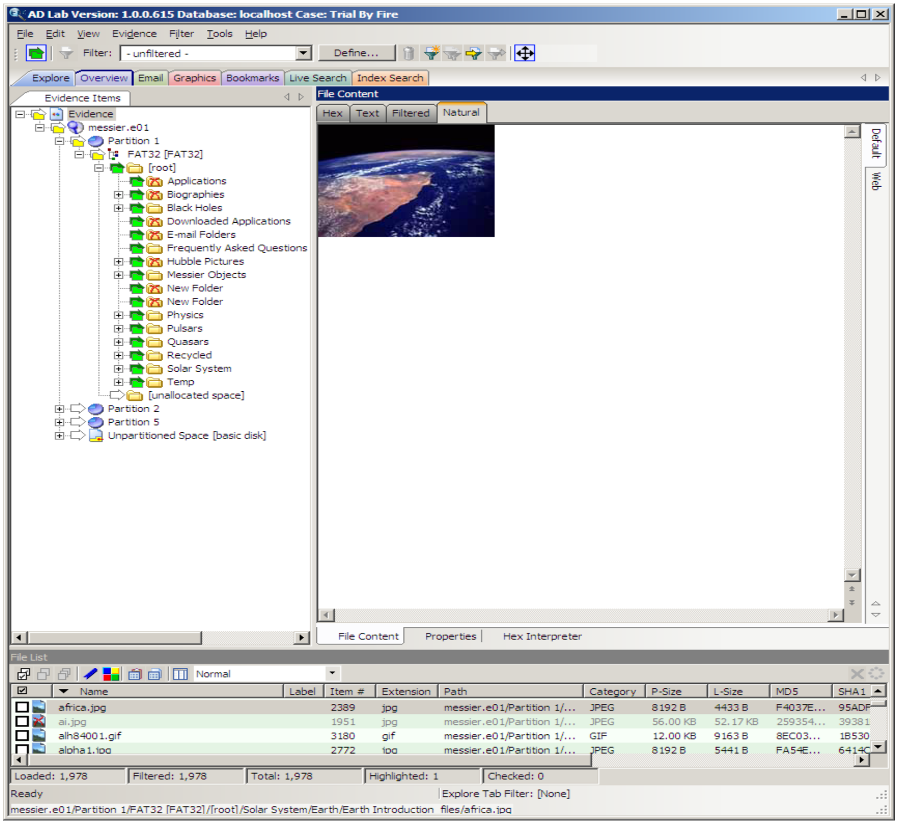
Chapter 6 Using Tabs to Explore & Refine Evidence

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

EXPLORE TAB

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

Figure 6-1 Explore Tab



☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1
□	africa.jpg		2389	jpg	messier.e01/Partition 1/...	JPEG	8192 B	4433 B	F4037E...	95ADF
□	ai.jpg		1951	jpg	messier.e01/Partition 1/...	JPEG	56.00 KB	52.17 KB	259354...	39381
□	alh84001.gif		3180	gif	messier.e01/Partition 1/...	GIF	12.00 KB	9163 B	8EC03...	1B530
□	alpha1.jpg		2772	jpg	messier.e01/Partition 1/...	JPEG	8192 B	5441 B	FA54E...	6414C

Loaded: 1,978 Filtered: 1,978 Total: 1,978 Highlighted: 1 Checked: 0

Ready Explore Tab Filter: [None]

messier.e01/Partition 1/FAT32 [FAT32]/[root]/Solar System/Earth/Earth Introduction files/africa.jpg

The Explore tab contains the following panes:

TABLE 6-1 Explore Tab Panes

Pane	Description
Explorer Tree Pane	Lists directory structure of each evidence item, similar to the way one would view directory structure in Windows Explorer. An evidence item is a physical drive, a logical drive or partition, or drive space not included in any partitioned drive, as well as any file, folder, or image of a drive.
File List	Displays case files and pertinent information about files, such as filename, file path, file type and many more properties as defined in the current filter.

TABLE 6-1 Explore Tab Panes

Pane	Description
File Content Pane	Displays the contents of the currently selected file from the File List. The Viewer toolbar allows the choice of different view formats. Choices are: • File Content Tab The File content tab has a Default tab and a Web tab for each of the following tabbed views: •HexTab •Text Tab •Filterd Tab •Natural Tab • Properties Tab • Hex Interpreter Tab

Viewer Pane

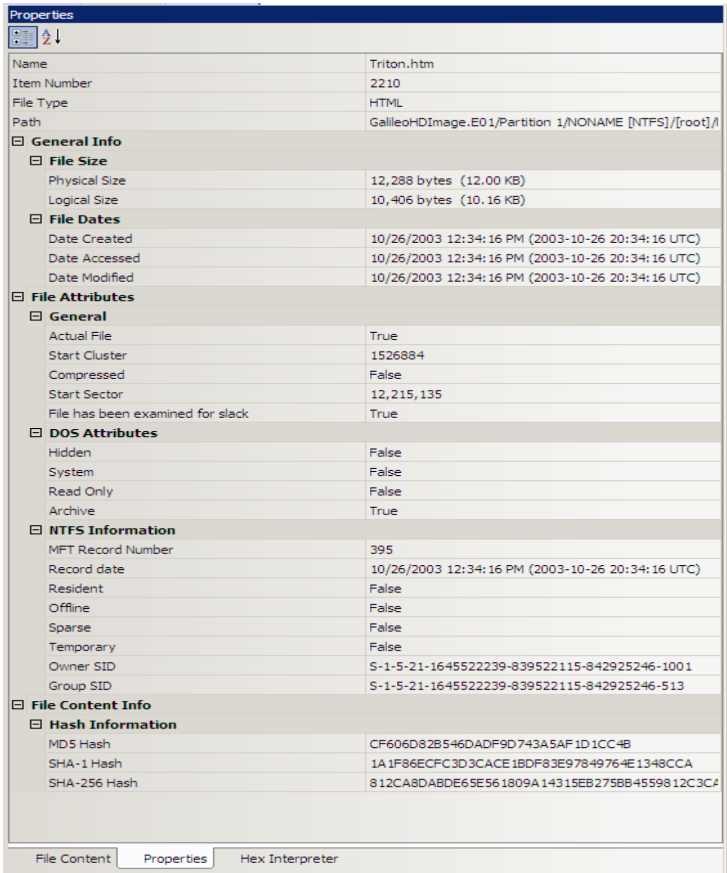
The Viewer pane now contains the File Content, Properties, and Hex Interpreter tabs, at the bottom of the pane. The File Content, Properties, and Hex Interpreter tabs default to the bottom left of the File Content pane in any program tab where it is used.

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

Properties Tab

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

Figure 6-2 Properties Pane



Properties

Name	Triton.htm
Item Number	2210
File Type	HTML
Path	GalileoHDImage.E01/Partition 1/NONAME [NTFS]/[root]/
⊟ **General Info**	
⊟ **File Size**	
Physical Size	12,288 bytes (12.00 KB)
Logical Size	10,406 bytes (10.16 KB)
⊟ **File Dates**	
Date Created	10/26/2003 12:34:16 PM (2003-10-26 20:34:16 UTC)
Date Accessed	10/26/2003 12:34:16 PM (2003-10-26 20:34:16 UTC)
Date Modified	10/26/2003 12:34:16 PM (2003-10-26 20:34:16 UTC)
⊟ **File Attributes**	
⊟ **General**	
Actual File	True
Start Cluster	1526884
Compressed	False
Start Sector	12,215,135
File has been examined for slack	True
⊟ **DOS Attributes**	
Hidden	False
System	False
Read Only	False
Archive	True
⊟ **NTFS Information**	
MFT Record Number	395
Record date	10/26/2003 12:34:16 PM (2003-10-26 20:34:16 UTC)
Resident	False
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-1645522239-839522115-842925246-1001
Group SID	S-1-5-21-1645522239-839522115-842925246-513
⊟ **File Content Info**	
⊟ **Hash Information**	
MD5 Hash	CF606D82B546DADF9D743A5AF1D1CC4B
SHA-1 Hash	1A1F86ECFC3D3CACE1BDF83E97849764E1348CCA
SHA-256 Hash	812CA8DABDE65E561809A14315EB275BB4559812C3C

The following table highlights the components of the Properties pane:

TABLE 6-2 Properties Pane Components

Option	Description
Name	The filename of the selected file.
Item Number	The arbitrary number assigned to the item by FTK 2.2 during case processing.
File Type	The type of selected file, such as an HTML file or a Microsoft Word 98 document. FTK uses the file header to identify each item's file type.

TABLE 6-2 **Properties Pane Components**

Option	Description
Path	The path from the evidence to the selected file from the evidence source down..
General Info	General information about the selected file: **File Size:** lists the physical size of the file, including file slack, and logical size of the file, excluding file slack. **File Dates:** lists the dates and times when the file was created, last accessed, and last modified on the imaged system. All dates are listed in UTC fime.
File Attributes	The attributes of the file: **General**: • **Actual File**: True if an actual file; False if derived from an actual file. • **Start Cluster**: Start cluster of the file on the disk • **Compessed**: True if compressed. False otherwise. • **Start Sector**: 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. **DOS Attributes**: • **Hidden**: True if Hidden attribulte was set on the file. False otherwise. • **System**: True if this is a DOS system file. False otherwise. • **Read Only**: True or False value • **Archive**: True if Read Only attribute was set on the file. False otherwise. • **8.3 Name**: Name of the file in the DOS 8.3 naming convention, such as [*filename.ext*]

TABLE 6-2 Properties Pane Components

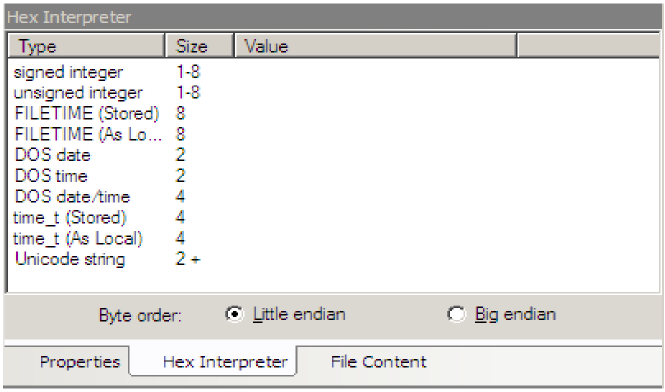
Option	Description
	NTFS Information • **NTFS Record Number**: The number of the file in the NTFS MFT record. • **Record Date**: UTC time and date record was created. • **Resident**: True if the item was Resident, meaning it was stored in the MFT and the entire file fit in the available space. False 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.) • **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 content information and verification information of the file: **KFF Status**: Indicates if the file is identified by the KFF as an illicit or contraband file, or as an 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 (32bytes) 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.

HEX INTERPRETER TAB

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

Figure 6-3 The Hex Interpreter Tab



Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (Stored)	8	
FILETIME (As Lo...	8	
DOS date	2	
DOS time	2	
DOS date/time	4	
time_t (Stored)	4	
time_t (As Local)	4	
Unicode string	2 +	

Byte order: ● Little endian ○ Big endian

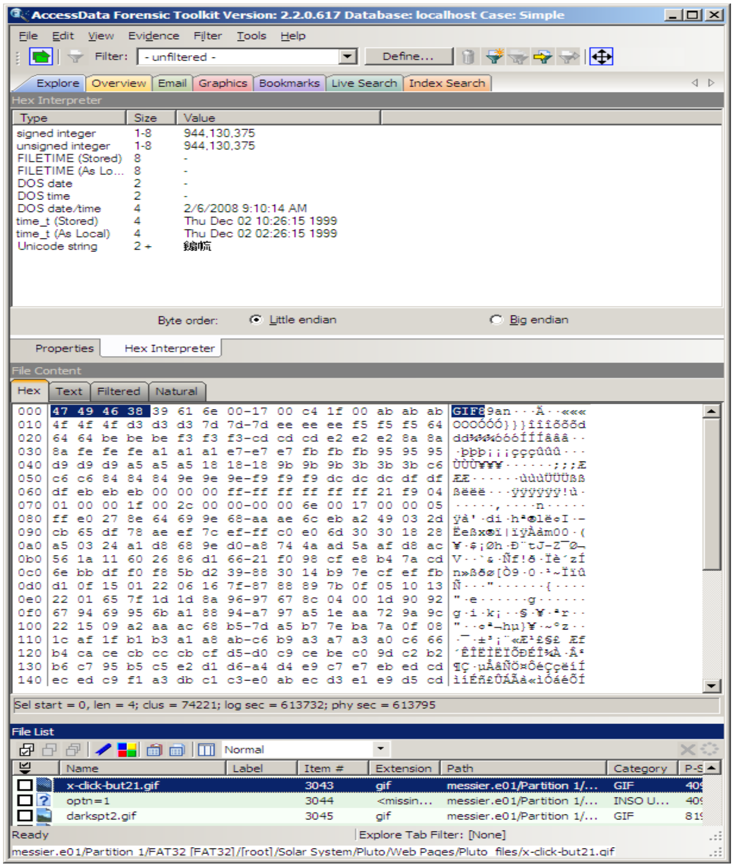
The Hex tab displays file contents in hexadecimal format. Use this view together with the Hex Interpreter pane.

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

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

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

Figure 6-4 Hex Interpreter Tab and Corresponding File Content Pane Hex View Tab


AccessData Forensic Toolkit Version: 2.2.0.617 Database: localhost Case: Simple
File Edit View Evidence Filter Tools Help
Filter: - unfiltered -
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search
Hex Interpreter
Properties Hex Interpreter
File Content
Hex Text Filtered Natural
File List
Normal

Type	Size	Value
signed integer	1-8	944,130,375
unsigned integer	1-8	944,130,375
FILETIME (Stored)	8	-
FILETIME (As Lo...	8	-
DOS date	2	-
DOS time	2	-
DOS date/time	4	2/6/2008 9:10:14 AM
time_t (Stored)	4	Thu Dec 02 10:26:15 1999
time_t (As Local)	4	Thu Dec 02 02:26:15 1999
Unicode string	2 +	鍚瑺

Byte order: ● Little endian ○ Big endian

```
000 47 49 46 38 39 61 6e 00-17 00 c4 1f 00 ab ab ab GIF89an···Ä··«««
010 4f 4f 4f d3 d3 d3 7d 7d-7d ee ee ee f5 f5 f5 64 OOOÓÓÓ}}}îîîõõõd
020 64 64 be be be f3 f3 f3-cd cd cd e2 e2 e2 8a 8a dd¾¾¾óóóÍÍÍâââ··
030 8a fe fe fe a1 a1 a1 e7-e7 e7 fb fb fb 95 95 95 ·þþþ¡¡¡çççûûû···
040 d9 d9 d9 a5 a5 a5 18 18-18 9b 9b 9b 3b 3b 3b c6 ÙÙÙ¥¥¥······;;;Æ
050 c6 c6 84 84 84 9e 9e 9e-f9 f9 f9 dc dc dc df df ÆÆ······ùùùÜÜÜßß
060 df eb eb eb 00 00 00 ff-ff ff ff ff ff 21 f9 04 ßëëë···ÿÿÿÿÿÿ!ù·
070 01 00 00 1f 00 2c 00 00-00 00 6e 00 17 00 00 05 ·····,····n·····
080 ff e0 27 8e 64 69 9e 68-aa ae 6c eb a2 49 03 2d ÿà'·di·hª®lë¢I·-
090 cb 65 df 78 ae ef 7c ef-ff c0 e0 6d 30 30 18 28 Ëeßx®ï|ïÿÀàm00·(
0a0 a5 03 24 a1 d8 68 9e d0-a8 74 4a ad 5a af d8 ac ¥·$¡Øh·Ð¨tJ-Z¯Ø¬
0b0 56 1a 11 60 26 86 d1 66-21 f0 98 cf e8 b4 7a cd V··`&·Ñf!ð·Ïè´zÍ
0c0 6e bb df f0 f8 5b d2 39-88 30 14 b9 7e cf ef fb n»ßðø[Ò9·0·¹~Ïïû
0d0 d1 0f 15 01 22 06 16 7f-87 88 89 7b 0f 05 10 13 Ñ···"······{····
0e0 22 01 65 7f 1d 1d 8a 96-97 67 8c 04 00 1d 90 92 "·e······g······
0f0 67 94 69 95 6b a1 88 94-a7 97 a5 1e aa 72 9a 9c g·i·k¡··§·¥·ªr··
100 22 15 09 a2 aa ac 68 b5-7d a5 b7 7e ba 7a 0f 08 "···¢ª¬hµ}¥·~ºz··
110 1c af 1f b1 b3 a1 a8 ab-c6 b9 a3 a7 a3 a0 c6 66 ·¯·±³¡¨«Æ¹£§£ Æf
120 b4 ca ce cb cc cb cf d5-d0 c9 ce be c0 9d c2 b2 ´ÊÎËÌËÏÕÐÉÎ¾À·Â²
130 b6 c7 95 b5 c5 e2 d1 d6-a4 d4 e9 c7 e7 eb ed cd ¶Ç·µÅâÑÖ¤ÔéÇçëíÍ
140 ec ed c9 f1 a3 db c1 c3-e0 ab ec d3 e1 e9 d5 cd ìíÉñ£ÛÁÃà«ìÓáéÕÍ
```

Sel start = 0, len = 4; clus = 74221; log sec = 613732; phy sec = 613795

	Name	Label	Item #	Extension	Path	Category	P-S
□	x-click-but21.gif		3043	gif	messier.e01/Partition 1/...	GIF	40
□	optn=1		3044	<missin...	messier.e01/Partition 1/...	INSO U...	40
□	darkspt2.gif		3045	gif	messier.e01/Partition 1/...	GIF	81

Ready | Explore Tab Filter: [None]

messier.e01/Partition 1/FAT32 [FAT32]/[root]/Solar System/Pluto/Web Pages/Pluto_files/x-click-but21.gif

To convert hexadecimal values do the following:

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

Little-endian and big-endian refer to which bytes are most significance in multi-byte data types, and describe the order in which a sequence of bytes is stored in a computer's memory. Microsoft Windows generally runs as Little Endian, because it was developed on and mostly runs on Intel-based, or Intel-compatible machines.

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

FTK 2.2 uses Little-endian as the default setting. If you view a data selection in the Hex Interpreter and it does not seem right, try choosing *Big endian* to see if the data displayed makes more sense.

For further information on using the Hex Interpreter pane, see "Hex Interpreter Tab" on page 110.

FILE CONTENT TAB

HEX TAB

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

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

The following table lists the available options and their descriptions:

TABLE 6-3 File Content Hex View Right-click Menu Options

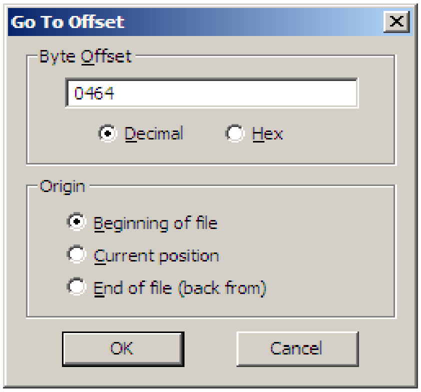
• Select all	• Show decimal offsets
• Copy text	• Show text only
• Copy hex	• Fit to windows
• Copy Unicode	• Save current settings

TABLE 6-3 **File Content Hex View Right-click Menu Options**

• Copy raw data	• Got to offset
• Save Selection	• Save selection as carved file

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

Figure 6-5 Go to Offset Dialog



Go To Offset

Byte Offset

0464

● Decimal ○ Hex

Origin

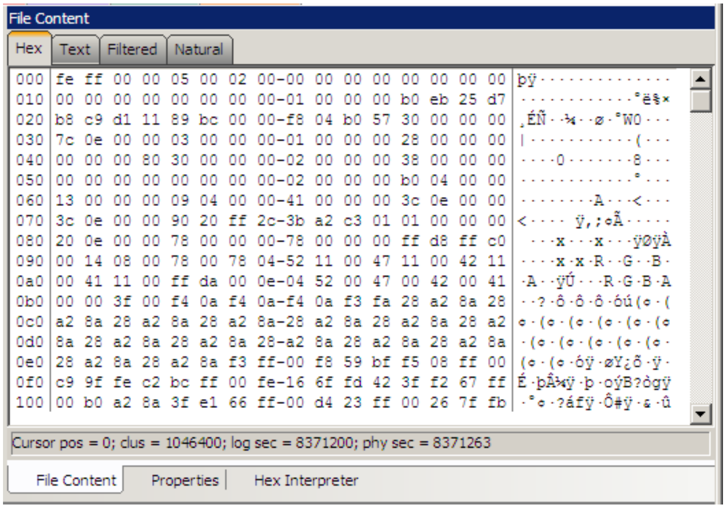
● Beginning of file

○ Current position

○ End of file (back from)

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

Figure 6-6 The File Content Hex Tab



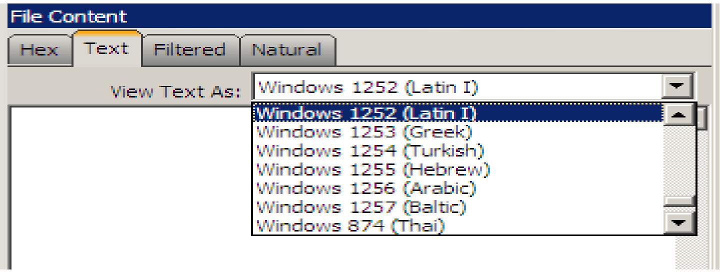
```
000 fe ff 00 00 05 00 02 00-00 00 00 00 00 00 00 00 þÿ··············
010 00 00 00 00 00 00 00 00-01 00 00 00 b0 eb 25 d7 ············°ë%×
020 b8 c9 d1 11 89 bc 00 00-f8 04 b0 57 30 00 00 00 ¸ÉÑ··¼··ø·°W0···
030 7c 0e 00 00 03 00 00 00-01 00 00 00 28 00 00 00 |···········(···
040 00 00 00 80 30 00 00 00-02 00 00 00 38 00 00 00 ····0·······8···
050 00 00 00 00 00 00 00 00-02 00 00 00 b0 04 00 00 ············°···
060 13 00 00 00 09 04 00 00-41 00 00 00 3c 0e 00 00 ········A···<···
070 3c 0e 00 00 90 20 ff 2c-3b a2 c3 01 01 00 00 00 <···· ÿ,;¢Ã·····
080 20 0e 00 00 78 00 00 00-78 00 00 00 ff d8 ff c0  ···x···x···ÿØÿÀ
090 00 14 08 00 78 00 78 04-52 11 00 47 11 00 42 11 ····x·x·R··G··B·
0a0 00 41 11 00 ff da 00 0e-04 52 00 47 00 42 00 41 ·A··ÿÚ···R·G·B·A
0b0 00 00 3f 00 f4 0a f4 0a-f4 0a f3 fa 28 a2 8a 28 ··?·ô·ô·ô·óú(¢·(
0c0 a2 8a 28 a2 8a 28 a2 8a-28 a2 8a 28 a2 8a 28 a2 ¢·(¢·(¢·(¢·(¢·(¢
0d0 8a 28 a2 8a 28 a2 8a 28-a2 8a 28 a2 8a 28 a2 8a ·(¢·(¢·(¢·(¢·(¢·
0e0 28 a2 8a 28 a2 8a f3 ff-00 f8 59 bf f5 08 ff 00 (¢·(¢·óÿ·øY¿õ·ÿ·
0f0 c9 9f fe c2 bc ff 00 fe-16 6f fd 42 3f f2 67 ff É·þÂ¼ÿ·þ·oýB?ògÿ
100 00 b0 a2 8a 3f e1 66 ff-00 d4 23 ff 00 26 7f fb ·°¢·?áfÿ·Ô#ÿ·&·û
```

Cursor pos = 0; clus = 1046400; log sec = 8371200; phy sec = 8371263

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.

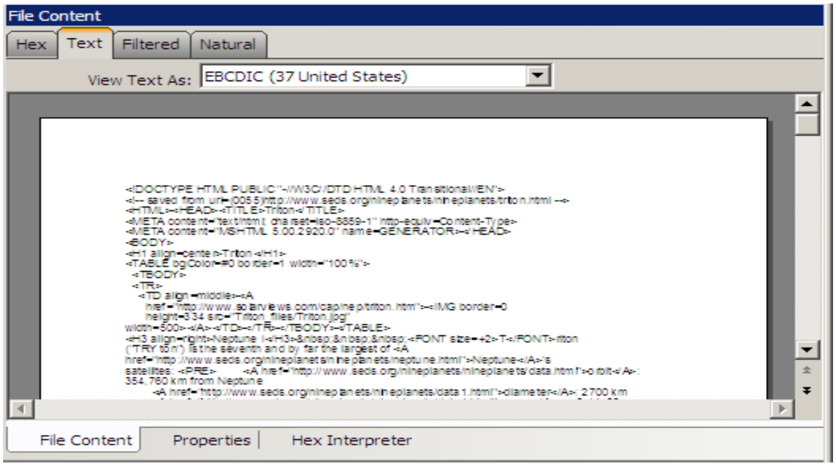
Figure 6-7 Text View Drop-Down Menu



View Text As: Windows 1252 (Latin I)

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

Figure 6-8



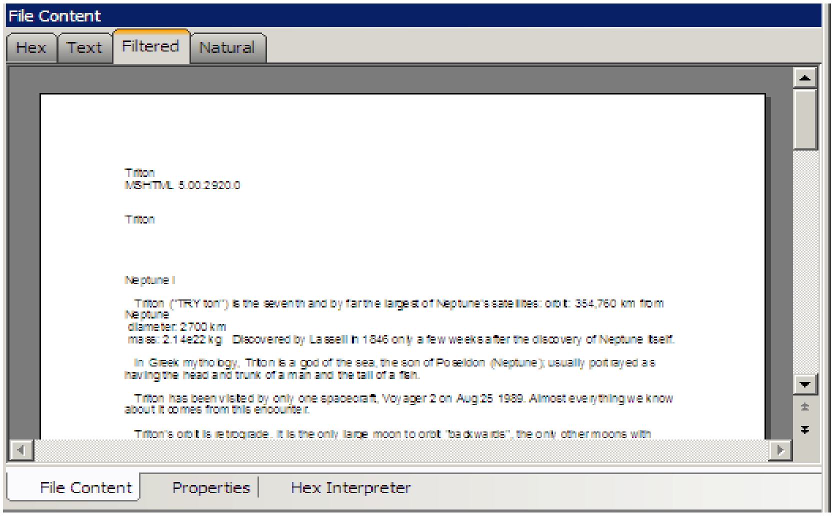
View Text As: EBCDIC (37 United States)

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<!-- saved from url=(0055)http://www.seds.org/nineplanets/nineplanets/triton.html -->
<HTML><HEAD><TITLE>Triton</TITLE>
<META content="text/html; charset=iso-8859-1" http-equiv=Content-Type>
<META content="MSHTML 5.00.2920.0" name=GENERATOR></HEAD>
<BODY>
<H1 align=center>Triton </H1>
<TABLE bgColor=#0 border=1 width="100%">
  <TBODY>
  <TR>
    <TD align=middle><A
      href="http://www.solarviews.com/cap/nep/triton.htm"><IMG border=0
      height=334 src="Triton_files/Triton.jpg"
width=500></A></TD></TR></TBODY></TABLE>
<H3 align=right>Neptune I</H3>&nbsp;&nbsp;&nbsp;<FONT size=+2>T</FONT>riton
("TRY ton") is the seventh and by far the largest of <A
href="http://www.seds.org/nineplanets/nineplanets/neptune.html">Neptune</A>'s
satellites: <PRE>       <A href="http://www.seds.org/nineplanets/nineplanets/data.html">orbit</A>:
354,760 km from Neptune
         <A href="http://www.seds.org/nineplanets/nineplanets/data1.html">diameter</A>: 2700 km
```

FILTERED TAB

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

Figure 6-9 Filtered Tab



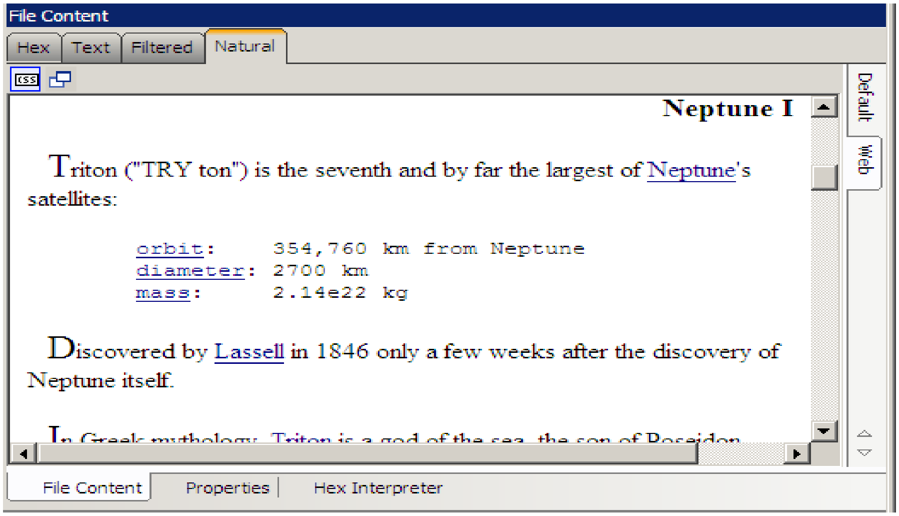
```
Triton
MSHTML 5.00.2920.0


Triton




Neptune I

   Triton ("TRY ton") is the seventh and by far the largest of Neptune's satellites: orbit: 354,760 km from
Neptune
 diameter: 2700 km
 mass: 2.14e22 kg   Discovered by Lassell in 1846 only a few weeks after the discovery of Neptune itself.

   In Greek mythology, Triton is a god of the sea, the son of Poseidon (Neptune); usually portrayed as
having the head and trunk of a man and the tail of a fish.

   Triton has been visited by only one spacecraft, Voyager 2 on Aug 25 1989. Almost everything we know
about it comes from this encounter.

   Triton's orbit is retrograde. It is the only large moon to orbit "backwards", the only other moons with
```

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

Natural Tab

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

Figure 6-10



Neptune I

Triton ("TRY ton") is the seventh and by far the largest of Neptune's satellites:

```
orbit:     354,760 km from Neptune
diameter:  2700 km
mass:      2.14e22 kg
```

Discovered by Lassell in 1846 only a few weeks after the discovery of Neptune itself.

In Greek mythology, Triton is a god of the sea, the son of Poseidon

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

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

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

Default Tab

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

Web Tab

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

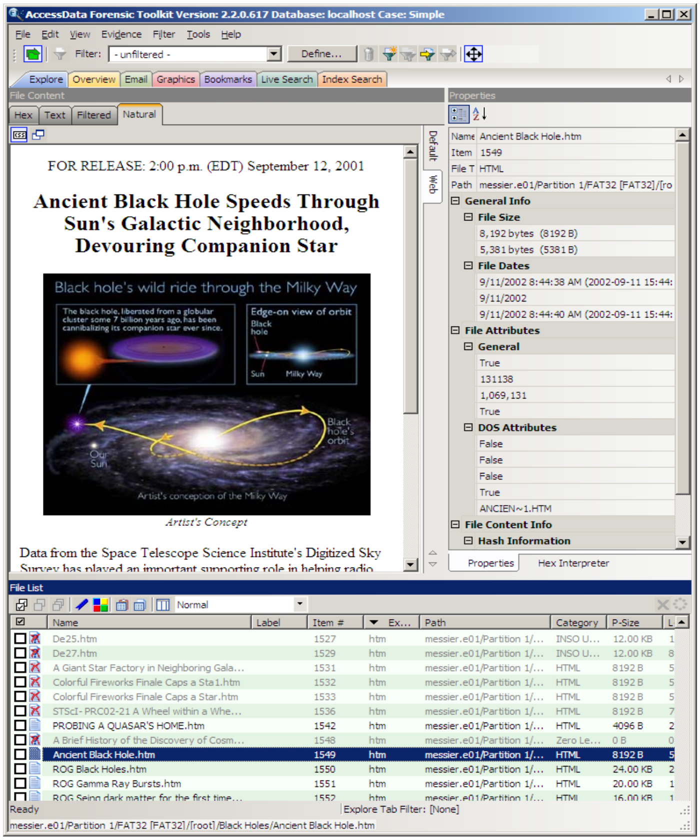
In the Web view, the top-left border of the pane holds two toggle buttons for enabling or disabling HTML content: Disable CSS Formatting, and Disable External Hyperlinks.

TABLE 6-4 Natural Tab: Web Tab Toggle Buttons

Component	Description
CSS	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 or Default) that is best for the selected file.The following figure displays an email displayed in a web tab.

Figure 6-11 File Content, Natural Tab, Web Tab


AccessData Forensic Toolkit Version: 2.2.0.617 Database: localhost Case: Simple
File
Edit
View
Evidence
Filter
Tools
Help
Filter:
Define...
Explore
Overview
Email
Graphics
Bookmarks
Live Search
Index Search
File Content
Hex
Text
Filtered
Natural
Default
Web
Properties
Black hole's wild ride through the Milky Way
The black hole, liberated from a globular cluster some 7 billion years ago, has been cannibalizing its companion star ever since.
Edge-on view of orbit
Black hole
Sun
Milky Way
Black hole's orbit
Our Sun
Artist's conception of the Milky Way
Properties
Hex Interpreter
File List

Filter: - unfiltered -

FOR RELEASE: 2:00 p.m. (EDT) September 12, 2001

Ancient Black Hole Speeds Through Sun's Galactic Neighborhood, Devouring Companion Star

Artist's Concept

Data from the Space Telescope Science Institute's Digitized Sky Survey has played an important supporting role in helping radio

Name	Ancient Black Hole.htm
Item	1549
File T	HTML
Path	messier.e01/Partition 1/FAT32 [FAT32]/[ro
⊟ **General Info**	
⊟ **File Size**	
	8,192 bytes (8192 B)
	5,381 bytes (5381 B)
⊟ **File Dates**	
	9/11/2002 8:44:38 AM (2002-09-11 15:44:
	9/11/2002
	9/11/2002 8:44:40 AM (2002-09-11 15:44:
⊟ **File Attributes**	
⊟ **General**	
	True
	131138
	1,069,131
	True
⊟ **DOS Attributes**	
	False
	False
	False
	True
	ANCIEN~1.HTM
⊟ **File Content Info**	
⊟ **Hash Information**	

Normal

☑	Name	Label	Item #	Ex...	Path	Category	P-Size	L
□	De25.htm		1527	htm	messier.e01/Partition 1/...	INSO U...	12.00 KB	1
□	De27.htm		1529	htm	messier.e01/Partition 1/...	INSO U...	12.00 KB	8
□	A Giant Star Factory in Neighboring Gala...		1531	htm	messier.e01/Partition 1/...	HTML	8192 B	5
□	Colorful Fireworks Finale Caps a Sta1.htm		1532	htm	messier.e01/Partition 1/...	HTML	8192 B	5
□	Colorful Fireworks Finale Caps a Star.htm		1533	htm	messier.e01/Partition 1/...	HTML	8192 B	5
□	STScI- PRC02-21 A Wheel within a Whe...		1536	htm	messier.e01/Partition 1/...	HTML	8192 B	7
□	PROBING A QUASAR'S HOME.htm		1542	htm	messier.e01/Partition 1/...	HTML	4096 B	2
□	A Brief History of the Discovery of Cosm...		1548	htm	messier.e01/Partition 1/...	Zero Le...	0 B	0
□	Ancient Black Hole.htm		1549	htm	messier.e01/Partition 1/...	HTML	8192 B	5
□	ROG Black Holes.htm		1550	htm	messier.e01/Partition 1/...	HTML	24.00 KB	2
□	ROG Gamma Ray Bursts.htm		1551	htm	messier.e01/Partition 1/...	HTML	20.00 KB	1
□	ROG Seing dark matter for the first time...		1552	htm	messier.e01/Partition 1/...	HTML	16.00 KB	1

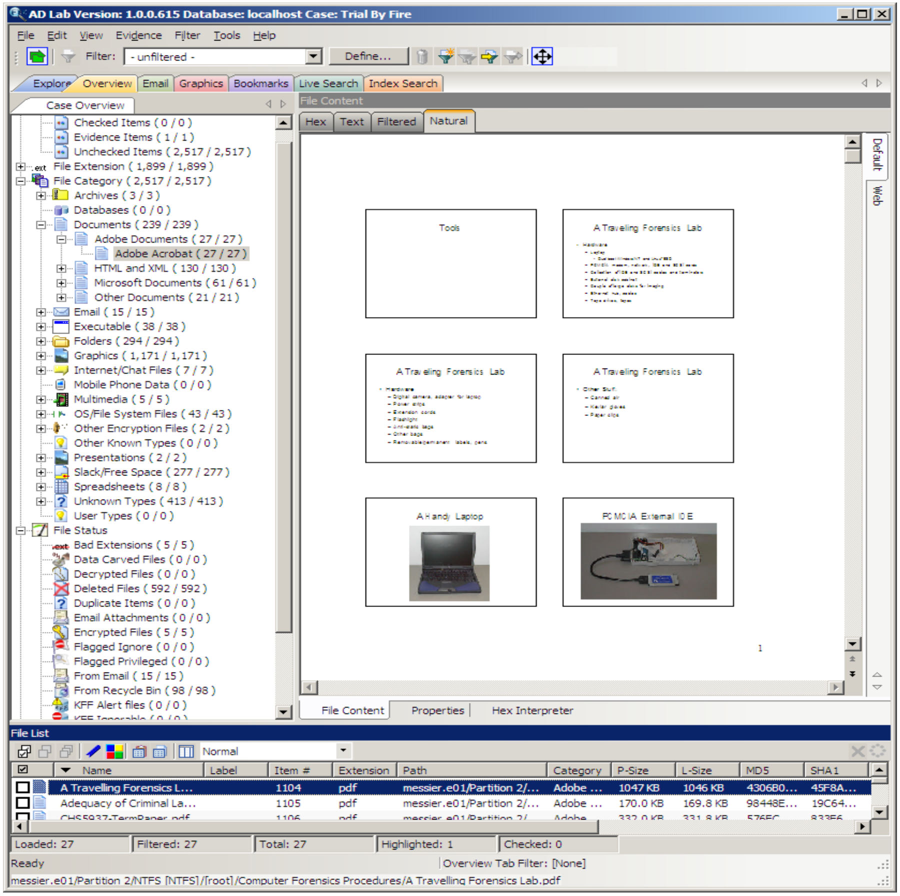
Ready | Explore Tab Filter: [None]

messier.e01/Partition 1/FAT32 [FAT32]/[root]/Black Holes/Ancient Black Hole.htm

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 6-12   Overview Tab



AD Lab Version: 1.0.0.615 Database: localhost Case: Trial By Fire
File Edit View Evidence Filter Tools Help
Filter: - unfiltered -
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search
Case Overview
File Content
Hex Text Filtered Natural
Default Web
Tools
A Traveling Forensics Lab
A Traveling Forensics Lab
A Traveling Forensics Lab
A Handy Laptop
PCMCIA External IDE
1
File Content Properties Hex Interpreter
File List
Normal

- Checked Items (0 / 0)
- Evidence Items (1 / 1)
- Unchecked Items (2,517 / 2,517)
- File Extension (1,899 / 1,899)
- File Category (2,517 / 2,517)
  - Archives (3 / 3)
  - Databases (0 / 0)
  - Documents (239 / 239)
    - Adobe Documents (27 / 27)
      - Adobe Acrobat (27 / 27)
    - HTML and XML (130 / 130)
    - Microsoft Documents (61 / 61)
    - Other Documents (21 / 21)
  - Email (15 / 15)
  - Executable (38 / 38)
  - Folders (294 / 294)
  - Graphics (1,171 / 1,171)
  - Internet/Chat Files (7 / 7)
  - Mobile Phone Data (0 / 0)
  - Multimedia (5 / 5)
  - OS/File System Files (43 / 43)
  - Other Encryption Files (2 / 2)
  - Other Known Types (0 / 0)
  - Presentations (2 / 2)
  - Slack/Free Space (277 / 277)
  - Spreadsheets (8 / 8)
  - Unknown Types (413 / 413)
  - User Types (0 / 0)
- File Status
  - Bad Extensions (5 / 5)
  - Data Carved Files (0 / 0)
  - Decrypted Files (0 / 0)
  - Deleted Files (592 / 592)
  - Duplicate Items (0 / 0)
  - Email Attachments (0 / 0)
  - Encrypted Files (5 / 5)
  - Flagged Ignore (0 / 0)
  - Flagged Privileged (0 / 0)
  - From Email (15 / 15)
  - From Recycle Bin (98 / 98)
  - KFF Alert files (0 / 0)

☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1
□	A Travelling Forensics L...		1104	pdf	messier.e01/Partition 2/...	Adobe ...	1047 KB	1046 KB	4306B0...	45F8A...
□	Adequacy of Criminal La...		1105	pdf	messier.e01/Partition 2/...	Adobe ...	170.0 KB	169.8 KB	98448E...	19C64...

Loaded: 27 | Filtered: 27 | Total: 27 | Highlighted: 1 | Checked: 0

Ready | Overview Tab Filter: [None]

messier.e01/Partition 2/NTFS [NTFS]/[root]/Computer Forensics Procedures/A Travelling Forensics Lab.pdf

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 6-5 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, Lotus Notes NSF, and other types of databases.
Documents	Includes most word processing, HTML, WML, HTML, or text files.
Email	Includes Email messages from Outlook, Outlook Express, AOL, Endoscope, Yahoo, Rethink, Udder, Hotmail, Lotus Notes, and MSN.
Executables	Includes Win32 executables and DLLs, OS/2, Windows VxD, Windows NT, JavaScript, and other executable formats.
Folders	Folders or directories that are located in the evidence.
Graphics	Includes the standard graphic formats such as .tif, .gif, .jpeg, and .bmp.
Internet Chat Files	Lists Microsoft Internet Explorer cache and history indexes.
Mobile Phone Data	Lists data acquired from supported mobile phone device(s).
Multimedia	Lists .aif, .wav, .asf, and other audio and video files.

TABLE 6-5 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 .doc files, etc.
Presentations	Lists multimedia file types such as MS PowerPoint or Corel Presentation files.
Slack/Free Space	Files, or fragments of files that are no longer seen by the file system, but have not been completely overwritten.
Spreadsheets	Includes spreadsheets from Lotus, Microsoft Excel, QuattroPro, and others.
Unknown Types	File types that AD FTK 2.2 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 6-6 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 .gif image renamed as graphic.txt.
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 6-6 File Status Categories

Category	Description
Duplicate Items	Any items that have an identical hash. Because the filename is not part of the hash, identical files may actually have different filenames. The primary item is the first one found by FTK.
Email Attachments	Files attached to the email in the evidence.
Encrypted Files	Files that are encrypted or have a password. This includes files that have a read-only password; that is, they may be opened and viewed, but not modified by the reader. If the files have been decrypted with EFS and you have access to the user's login password, you can decrypt these files. See "Decrypting Files and Folders" on page 179.
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.

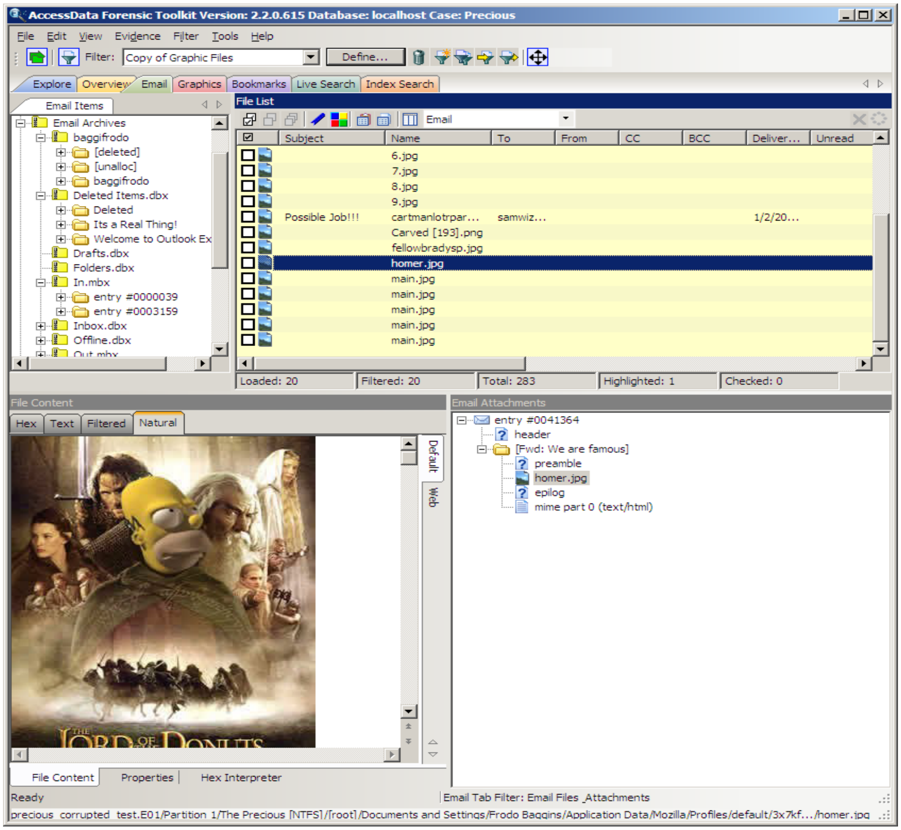
Bookmark Container

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

EMAIL TAB

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

Figure 6-13 Email Tab



AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost Case: Precious

Filter: Copy of Graphic Files

- Email Archives
  - baggifrodo
    - [deleted]
    - [unalloc]
    - baggifrodo
  - Deleted Items.dbx
    - Deleted
    - Its a Real Thing!
    - Welcome to Outlook Ex
  - Drafts.dbx
  - Folders.dbx
  - In.mbx
    - entry #0000039
    - entry #0003159
  - Inbox.dbx
  - Offline.dbx
  - Out.mbx

☑	Subject	Name	To	From	CC	BCC	Deliver...	Unread
□		6.jpg						
□		7.jpg						
□		8.jpg						
□		9.jpg						
□	Possible Job!!!	cartmanlotrpar...	samwiz...				1/2/20...	
□		Carved [193].png						
□		fellowbradysp.jpg						
□		homer.jpg						
□		main.jpg						
□		main.jpg						
□		main.jpg						
□		main.jpg						
□		main.jpg						

Loaded: 20 | Filtered: 20 | Total: 283 | Highlighted: 1 | Checked: 0

- entry #0041364
  - header
  - [Fwd: We are famous]
    - preamble
    - homer.jpg
    - epilog
    - mime part 0 (text/html)

Ready

Email Tab Filter: Email Files _Attachments

precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/Application Data/Mozilla/Profiles/default/3x7kf.../homer.jpg

EMAIL STATUS TREE

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

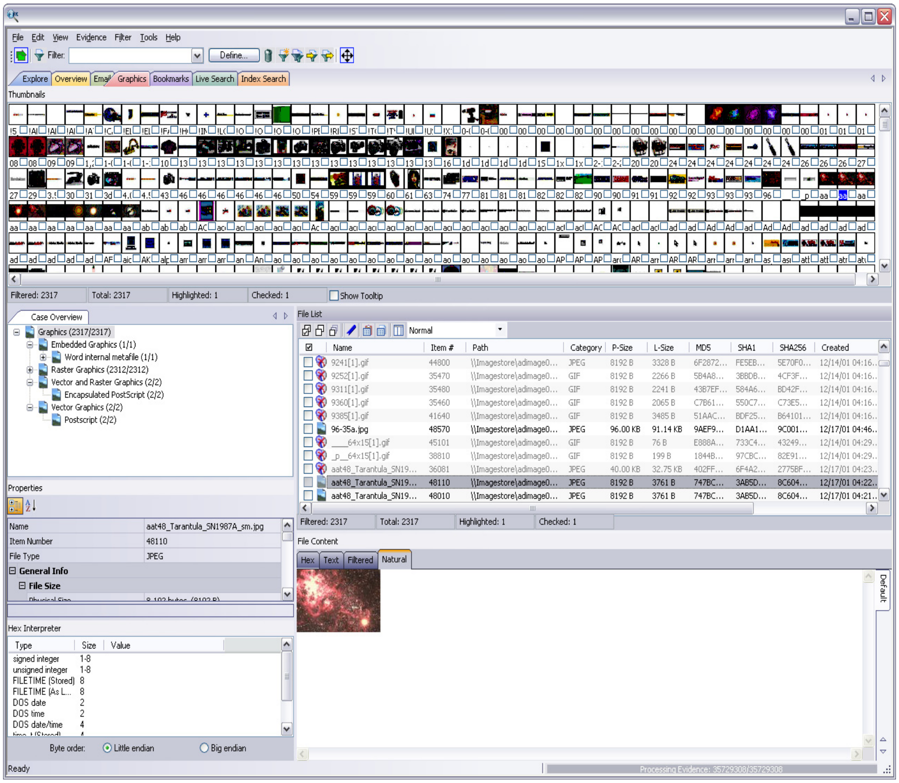
Email Tree

The Email tree lists message counts, DBX counts, PST counts, NSF 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 6-14 Graphics Tab


File Edit View Evidence Filter Tools Help
Filter:
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search
Thumbnails
Show Tooltip
Case Overview
File List
Properties
Hex Interpreter
File Content
Hex Text Filtered Natural
Default
Ready
Processing Evidence: 35729308/35729308

Filtered: 2317 | Total: 2317 | Highlighted: 1 | Checked: 1

- Graphics (2317/2317)
  - Embedded Graphics (1/1)
    - Word internal metafile (1/1)
  - Raster Graphics (2312/2312)
  - Vector and Raster Graphics (2/2)
    - Encapsulated PostScript (2/2)
  - Vector Graphics (2/2)
    - Postscript (2/2)

Normal

☑	Name	Item #	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
□	9241[1].gif	44800	\\Imagestore\adimage0...	JPEG	8192 B	3328 B	6F2872...	FE5EB...	5E70F0...	12/14/01 04:16...
□	9252[1].gif	35470	\\Imagestore\adimage0...	GIF	8192 B	2266 B	5B4A8...	3BBDB...	4CF3F...	12/14/01 04:16...
□	9311[1].gif	35480	\\Imagestore\adimage0...	GIF	8192 B	2241 B	43B7EF...	584A6...	BD42F...	12/14/01 04:16...
□	9360[1].gif	35460	\\Imagestore\adimage0...	GIF	8192 B	2065 B	C7B61...	550C7...	C73E5...	12/14/01 04:16...
□	9385[1].gif	41640	\\Imagestore\adimage0...	GIF	8192 B	3485 B	51AAC...	BDF25...	B64101...	12/14/01 04:16...
□	96-35a.jpg	48570	\\Imagestore\adimage0...	JPEG	96.00 KB	91.14 KB	9AEF9...	D1AA1...	9C001...	12/17/01 04:46...
□	____64x15[1].gif	45101	\\Imagestore\adimage0...	GIF	8192 B	76 B	E888A...	733C4...	43249...	12/14/01 04:29...
□	_p__64x15[1].gif	38810	\\Imagestore\adimage0...	GIF	8192 B	199 B	1844B...	97CBC...	82E91...	12/14/01 04:29...
□	aat48_Tarantula_SN19...	36081	\\Imagestore\adimage0...	JPEG	40.00 KB	32.75 KB	402FF...	6F4A2...	2775BF...	12/17/01 04:23...
□	aat48_Tarantula_SN19...	48110	\\Imagestore\adimage0...	JPEG	8192 B	3761 B	747BC...	3AB5D...	8C604...	12/17/01 04:22...
□	aat48_Tarantula_SN19...	48010	\\Imagestore\adimage0...	JPEG	8192 B	3761 B	747BC...	3AB5D...	8C604...	12/17/01 04:21...

Filtered: 2317 | Total: 2317 | Highlighted: 1 | Checked: 1

Name	aat48_Tarantula_SN1987A_sm.jpg
Item Number	48110
File Type	JPEG
⊟ **General Info**	
⊟ **File Size**	
Physical Size	8,192 bytes (8192 B)

Type	Size	Value
signed integer	1-8	
unsigned integer	1-8	
FILETIME (Stored)	8	
FILETIME (As L...	8	
DOS date	2	
DOS time	2	
DOS date/time	4	
time_t (Stored)	4	

Byte order: ● Little endian ○ Big endian

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 197.

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

Using Thumbnails

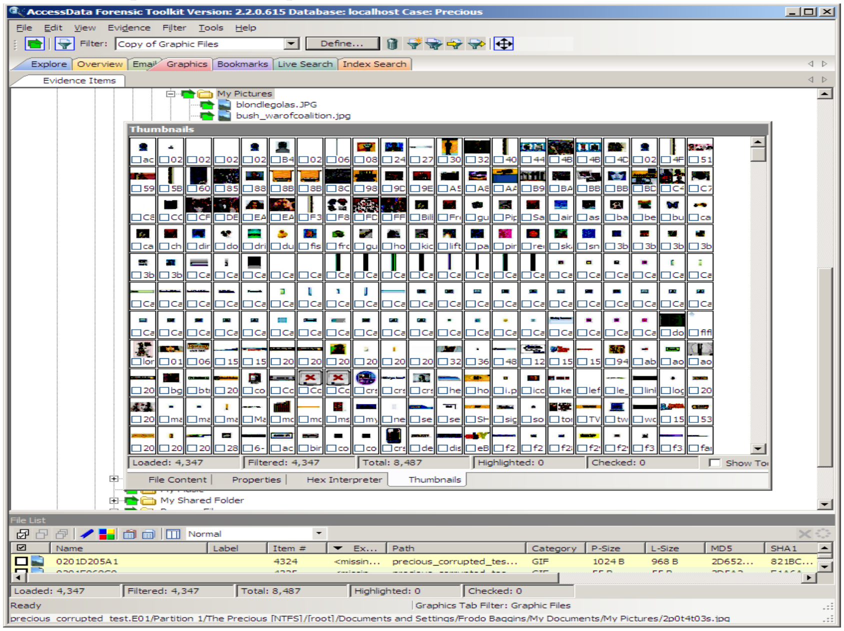
The thumbnail settings allow large amounts of graphic data to be displayed for evidence investigation. The investigator does not need to see details to pick out evidence; scan the thumbnails for flesh tones, photographic-type graphics, and perhaps particular shapes. Once found, the graphics can be inspected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

Moving the Thumbnails Pane

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

1. Undock the Thumbnails pane, and expand it across the screen.

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



AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost Case: Precious

Filter: Copy of Graphic Files

Loaded: 4,347 Filtered: 4,347 Total: 8,487 Highlighted: 0 Checked: 0

Name	Label	Item #	Ex...	Path	Category	P-Size	L-Size	MD5	SHA1
0201D205A1		4324	<missin...	precious_corrupted_tes...	GIF	1024 B	968 B	2D652...	821BC...

Loaded: 4,347 Filtered: 4,347 Total: 8,487 Highlighted: 0 Checked: 0

Ready

Graphics Tab Filter: Graphic Files

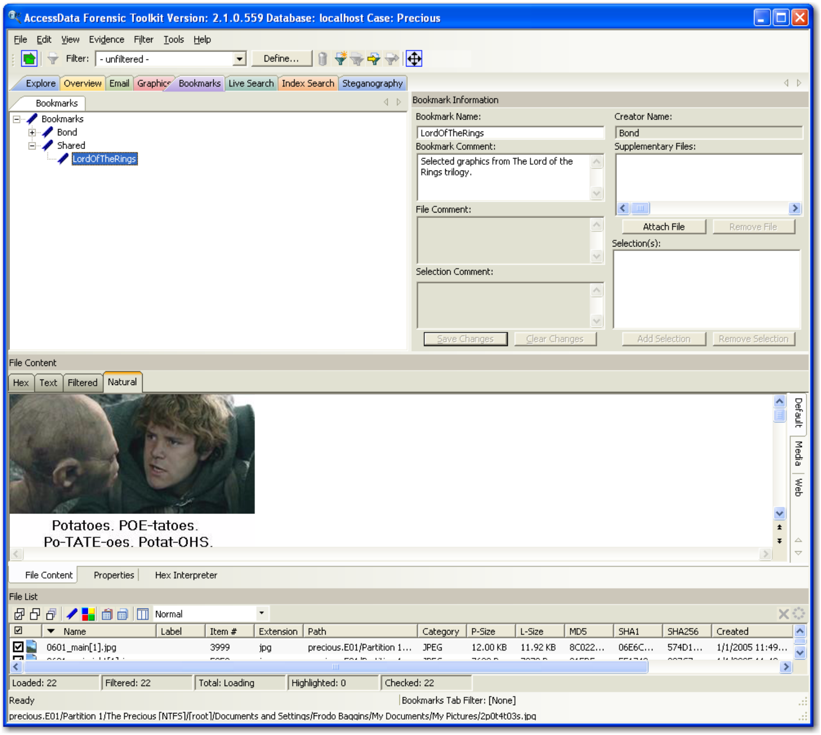
precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/My Pictures/2p0t4t03s.jpg

THE BOOKMARKS TAB

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

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

Figure 6-15 Bookmark Information Pane



Bookmark Name: LordOfTheRings

Creator Name: Bond

Bookmark Comment: Selected graphics from The Lord of the Rings trilogy.

Supplementary Files:

File Comment:

Selection(s):

Selection Comment:

☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
☑	0601_main[1].jpg		3999	jpg	precious.E01/Partition 1...	JPEG	12.00 KB	11.92 KB	8C022...	06E6C...	574D1...	1/1/2005 11:49...

Loaded: 22 | Filtered: 22 | Total: Loading | Highlighted: 0 | Checked: 22

Ready | Bookmarks Tab Filter: [None]

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/My Pictures/2p0t4t03s.jpg

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

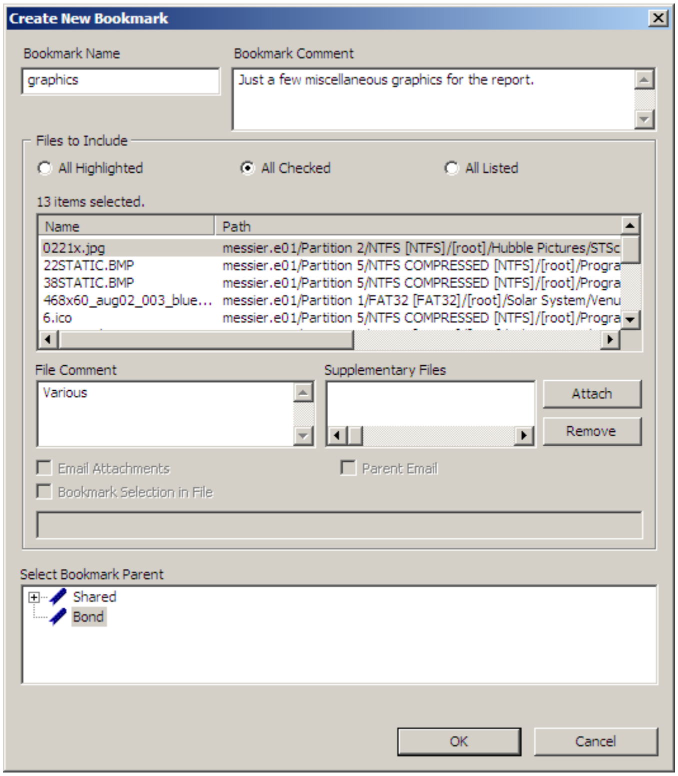
CREATING A BOOKMARK

TABLE 6-7 Bookmarks Tab

Features	Description
Bookmark Name	Displays the name given to the bookmark when it was created.
Bookmark Comment	Displays notes included with a bookmark.
File Comment	Displays notes included with a file.
Selection Comment	Displays notes included with a selection.
	• Save Changes • Clear Changes
Selection(s)	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. This can be done for multiple files with multiple selections. Use this option to Add and Remove Selections.
	• Add Selection • Remove Selection
Creator Name	Name of the user who created the bookmark.
Supplementary Files	Lists additional files attached to the bookmark. Options:
	• Attach File • Remove File
Save Changes	Saves changes to the bookmark.
Clear Changes	Removes comments that have not been saved.

Files can be bookmarked from any tab in FTK. To create a bookmark 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.



Create New Bookmark

Bookmark Name: graphics

Bookmark Comment: Just a few miscellaneous graphics for the report.

Files to Include

○ All Highlighted ● All Checked ○ All Listed

13 items selected.

Name	Path
0221x.jpg	messier.e01/Partition 2/NTFS [NTFS]/[root]/Hubble Pictures/STSc
22STATIC.BMP	messier.e01/Partition 5/NTFS COMPRESSED [NTFS]/[root]/Progra
38STATIC.BMP	messier.e01/Partition 5/NTFS COMPRESSED [NTFS]/[root]/Progra
468x60_aug02_003_blue…	messier.e01/Partition 1/FAT32 [FAT32]/[root]/Solar System/Venu
6.ico	messier.e01/Partition 5/NTFS COMPRESSED [NTFS]/[root]/Progra

File Comment: Various

Supplementary Files

□ Email Attachments □ Parent Email

□ Bookmark Selection in File

Select Bookmark Parent

Shared

Bond

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 displays in the Bookmark Information pane.

The Bookmark Information pane contains these fields:

TABLE 6-8 Bookmark Information Pane Information

Field	Description
Bookmark Name	The name of the bookmark. Click *Save Changes* to store any changes made to this field.
Bookmark Comment	The investigator can assign a text comment to the bookmark. Click *Save Changes* to store any changes made to this field at any time.
Creator Name	The FTK2 user who created the bookmark.

TABLE 6-8 Bookmark Information Pane Information

Field	Description
Supplementary Files	Displays a list of external, supplementary files associated with the bookmark. Options are: **Attach**: 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**: Removes a selected supplementary file from the bookmark.
File Comment	The investigator can assign a different comment to each file in the bookmark. Click *Save Changes* to store any changes made to this field.
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 *Save Changes* 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. It may be best to make a habit of saving changes everytime you make a change, to avoid forgetting and losing your changes.

BOOKMARKING SELECTED TEXT

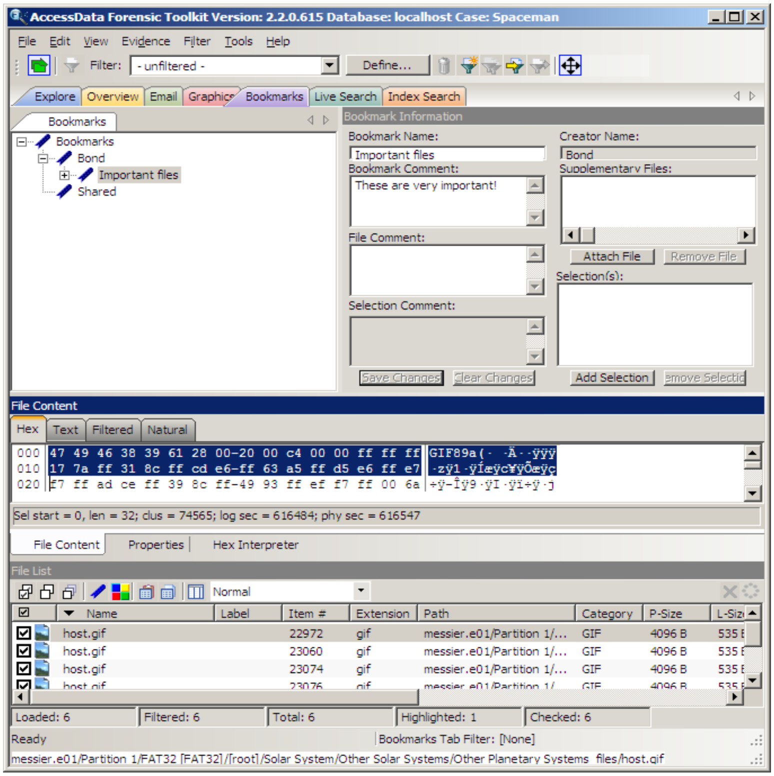
Bookmarked selections are independent of the view in which they were made. Select hex data in the Hex view of a bookmarked file and save it; bookmark different text in the Filtered view of the same file and save that selection as well.

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*



AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost Case: Spaceman

Filter: - unfiltered -

Bookmarks
- Bookmarks
  - Bond
    - Important files
  - Shared

Bookmark Name: Important files

Creator Name: Bond

Bookmark Comment: These are very important!

Supplementary Files:

File Comment:

Selection(s):

Selection Comment:

File Content

```
000 47 49 46 38 39 61 28 00-20 00 c4 00 00 ff ff ff GIF89a(· ·Ä··ÿÿÿ
010 17 7a ff 31 8c ff cd e6-ff 63 a5 ff d5 e6 ff e7 ·zÿ1·ÿÍæÿc¥ÿÕæÿç
020 f7 ff ad ce ff 39 8c ff-49 93 ff ef f7 ff 00 6a ÷ÿ-Îÿ9·ÿI·ÿï÷ÿ·j
```

Sel start = 0, len = 32; clus = 74565; log sec = 616484; phy sec = 616547

Normal

☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size
☑	host.gif		22972	gif	messier.e01/Partition 1/...	GIF	4096 B	535
☑	host.gif		23060	gif	messier.e01/Partition 1/...	GIF	4096 B	535
☑	host.gif		23074	gif	messier.e01/Partition 1/...	GIF	4096 B	535
☑	host.gif		23076	gif	messier.e01/Partition 1/	GIF	4096 B	535

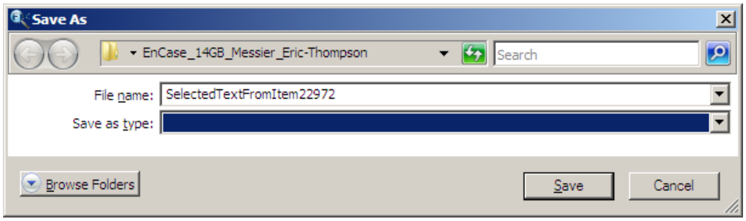
Loaded: 6 | Filtered: 6 | Total: 6 | Highlighted: 1 | Checked: 6

Ready | Bookmarks Tab Filter: [None]

messier.e01/Partition 1/FAT32 [FAT32]/[root]/Solar System/Other Solar Systems/Other Planetary Systems files/host.gif

5. To save selected content, choose the view that shows what you want to save, then highlight the content to save.

6. Right-click on the selected content. Click *Save Selection*..



EnCase_14GB_Messier_Eric-Thompson

File name: SelectedTextFromItem22972

Save as type:

7. Name the selection and click *Save.*

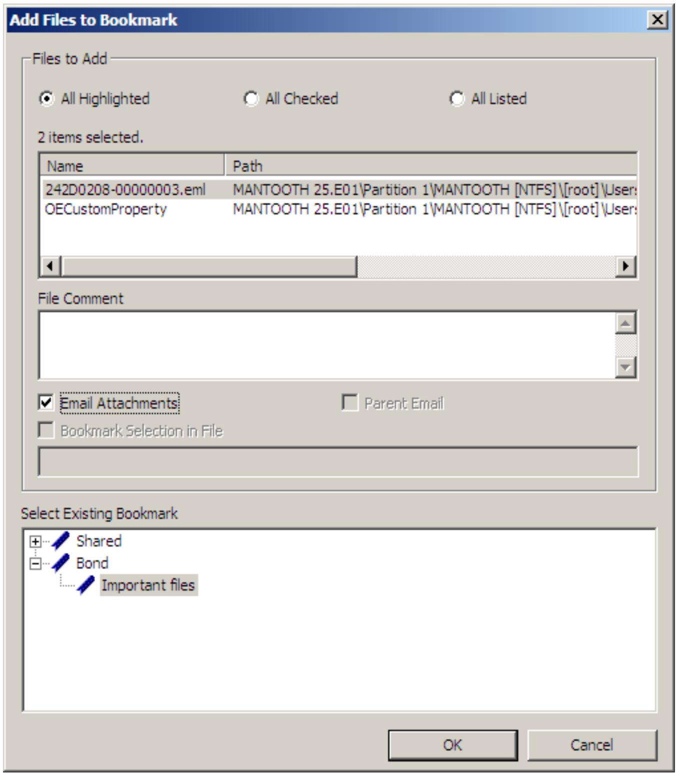
   The selection remains in the bookmark.

Adding to an Existing Bookmark

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

1. Right-click the new file.

2. Click *Add to Bookmark*.



Add Files to Bookmark

Files to Add

● All Highlighted ○ All Checked ○ All Listed

2 items selected.

Name	Path
242D0208-00000003.eml	MANTOOTH 25.E01\Partition 1\MANTOOTH [NTFS]\[root]\User:
OECustomProperty	MANTOOTH 25.E01\Partition 1\MANTOOTH [NTFS]\[root]\User:

File Comment

☑ Email Attachments □ Parent Email

□ Bookmark Selection in File

Select Existing Bookmark

- Shared
- Bond
  - Important files

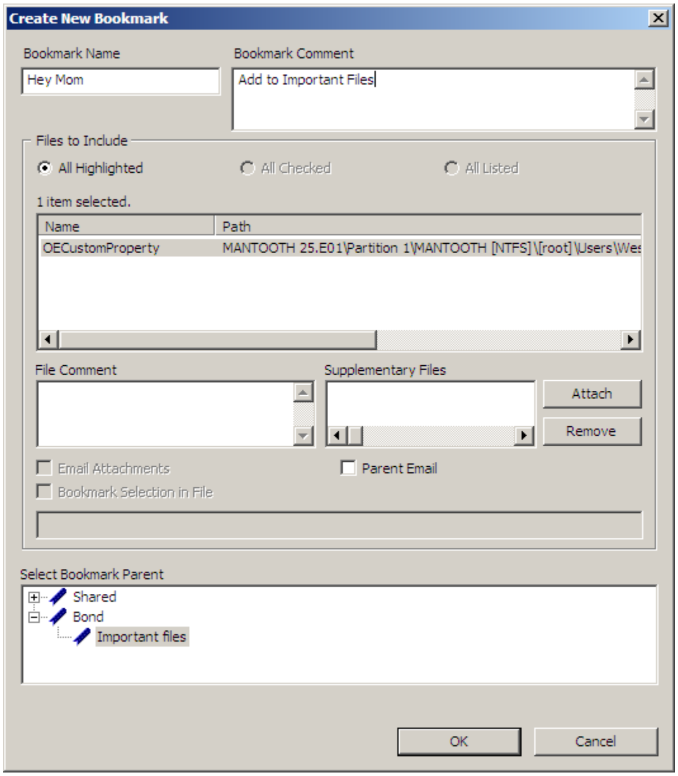
3. Select the parent bookmark.
4. Select the child bookmark to add the file or information to.
5. Click *OK*.

Creating Email or Email Attachment Bookmarks

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

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

Figure 6-16 Crete New Bookmark with Email Attachment



Create New Bookmark

Bookmark Name: Hey Mom

Bookmark Comment: Add to Important Files

Files to Include

● All Highlighted ○ All Checked ○ All Listed

1 item selected.

Name	Path
OECustomProperty	MANTOOTH 25.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes

File Comment

Supplementary Files

□ Email Attachments

□ Parent Email

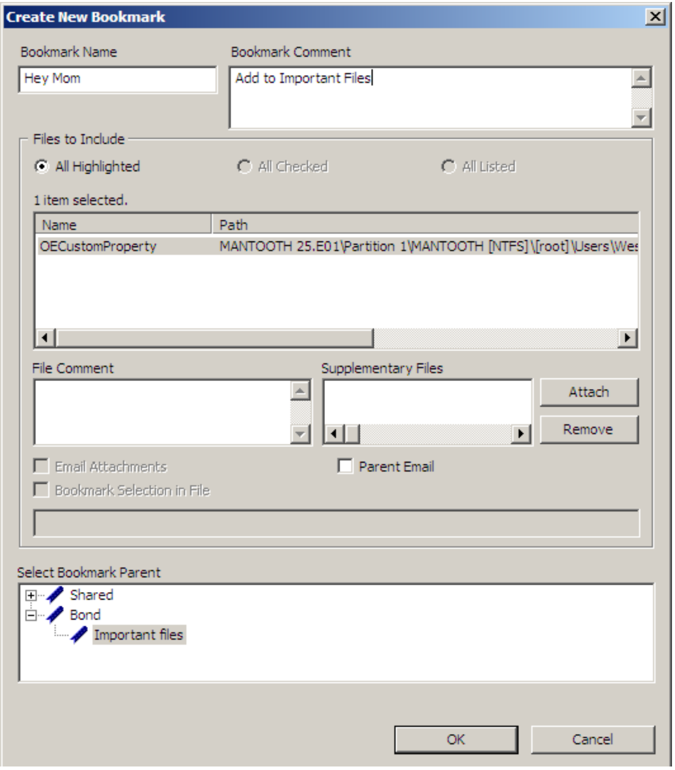
□ Bookmark Selection in File

Select Bookmark Parent

- Shared
- Bond
  - Important files

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

Figure 6-17 Create New Bookmark with Parent Email Selected



Create New Bookmark

Bookmark Name: Hey Mom

Bookmark Comment: Add to Important Files

Files to Include

● All Highlighted ○ All Checked ○ All Listed

1 item selected.

Name	Path
OECustomProperty	MANTOOTH 25.E01\Partition 1\MANTOOTH [NTFS]\[root]\Users\Wes

File Comment

Supplementary Files

□ Email Attachments

□ Bookmark Selection in File

□ Parent Email

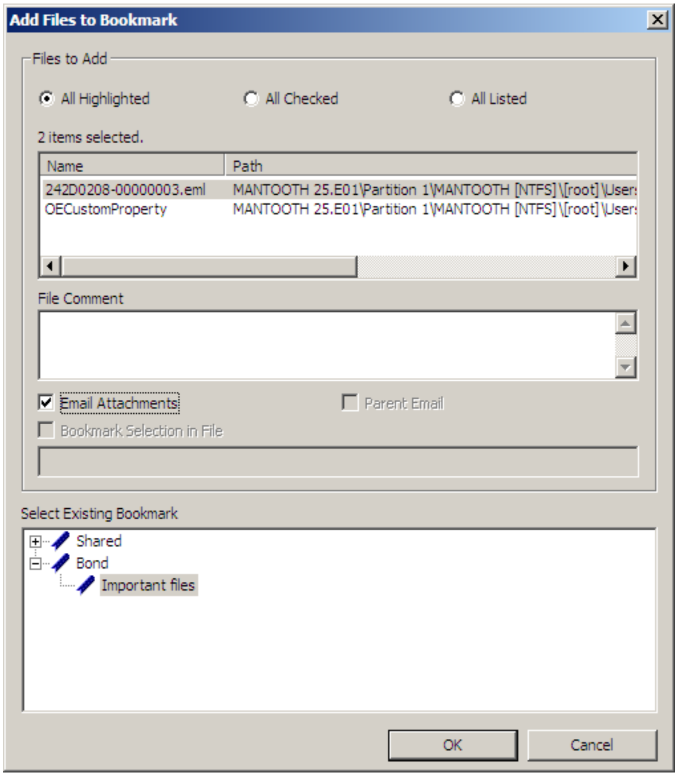
Select Bookmark Parent

- Shared
- Bond
  - Important files

ADDING EMAIL AND EMAIL ATTACHMENTS TO BOOKMARKS

To add an email to a bookmark, select the email to add, then right-click on the email and choose Add To Bookmark. (For more information see, “Adding to an Existing Bookmark” on page 134). 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 6-18 Add Files to Bookmark with Email Attachments Selected



Add Files to Bookmark

Files to Add

● All Highlighted ○ All Checked ○ All Listed

2 items selected.

Name	Path
242D0208-00000003.eml	MANTOOTH 25.E01\Partition 1\MANTOOTH [NTFS]\[root]\User:
OECustomProperty	MANTOOTH 25.E01\Partition 1\MANTOOTH [NTFS]\[root]\User:

File Comment

☑ Email Attachments □ Parent Email

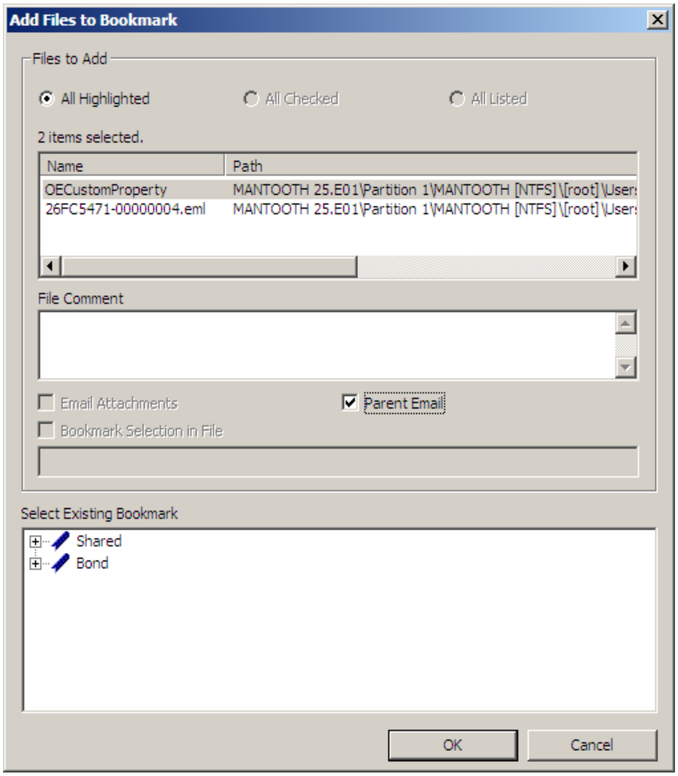
□ Bookmark Selection in File

Select Existing Bookmark

- Shared
- Bond
  - Important files

If only an attachment of an email is needed to be added to the bookmark, select the attachment and follow the instructions for adding to a bookmark. (For more information on adding to bookmarks, see, “Adding to an Existing Bookmark” on page 134.) 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 6-19 Add Files to Bookmark with Parent Email Selected



Add Files to Bookmark

Files to Add

● All Highlighted ○ All Checked ○ All Listed

2 items selected.

Name	Path
OECustomProperty	MANTOOTH 25.E01\Partition 1\MANTOOTH [NTFS]\[root]\User:
26FC5471-00000004.eml	MANTOOTH 25.E01\Partition 1\MANTOOTH [NTFS]\[root]\User:

File Comment

☐ Email Attachments ☑ Parent Email

☐ Bookmark Selection in File

Select Existing Bookmark

Moving a Bookmark

The following steps detail how to move a bookmark:

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

Deleting a Bookmark

Use the following steps to delete a bookmark:

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

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

DELETING FILES FROM A BOOKMARK

Use the following steps to delete files from bookmarks:

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

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

The following table describes the features of the Bookmark tab.

SEARCH TABS

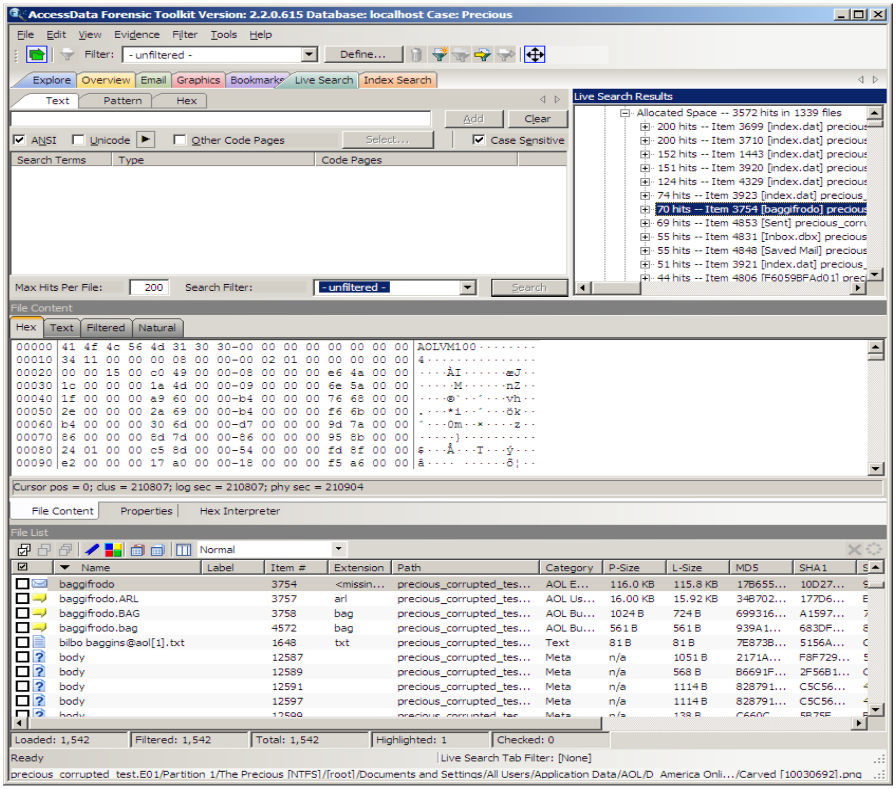
The Search Tabs allow the user to conduct an indexed search or a live search on the evidence. An indexed search is faster, while a live search is more flexible and powerful.

The results of each search appear as line items in the search results list. Click the plus icon (+) next to a search line to expand the search results branch. To view a specific item, select the file in the search results or file lists. All search terms are highlighted in the file. For information on searching, see "Chapter 7 Searching a Case" on page 143.

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 6-20   Live Search Tab


AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost Case: Precious
File Edit View Evidence Filter Tools Help
Filter: - unfiltered -
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search
Text Pattern Hex
Add Clear
☑ ANSI ☐ Unicode ☐ Other Code Pages Select... ☑ Case Sensitive
Search Terms Type Code Pages
Search
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal

Max Hits Per File: 200   Search Filter: - unfiltered -

Live Search Results

```
Allocated Space -- 3572 hits in 1339 files
  200 hits -- Item 3699 [index.dat] precious
  200 hits -- Item 3710 [index.dat] precious
  152 hits -- Item 1443 [index.dat] precious
  151 hits -- Item 3920 [index.dat] precious
  124 hits -- Item 4329 [index.dat] precious
  74 hits -- Item 3923 [index.dat] precious_
  70 hits -- Item 3754 [baggifrodo] precious
  69 hits -- Item 4853 [Sent] precious_corru
  55 hits -- Item 4831 [Inbox.dbx] precious
  55 hits -- Item 4848 [Saved Mail] precious
  51 hits -- Item 3921 [index.dat] precious_
  44 hits -- Item 4806 [F6059BFAd01] preci
```

```
00000 41 4f 4c 56 4d 31 30 30-00 00 00 00 00 00 00 00 AOLVM100········
00010 34 11 00 00 00 08 00 00-00 02 01 00 00 00 00 00 4···············
00020 00 00 15 00 c0 49 00 00-08 00 00 00 e6 4a 00 00 ····ÀI······æJ··
00030 1c 00 00 00 1a 4d 00 00-09 00 00 00 6e 5a 00 00 ·····M······nZ··
00040 1f 00 00 00 a9 60 00 00-b4 00 00 00 76 68 00 00 ····©`··´···vh··
00050 2e 00 00 00 2a 69 00 00-b4 00 00 00 f6 6b 00 00 .···*i··´···ök··
00060 b4 00 00 00 30 6d 00 00-d7 00 00 00 9d 7a 00 00 ´···0m··×····z··
00070 86 00 00 00 8d 7d 00 00-86 00 00 00 95 8b 00 00 ·····}··········
00080 24 01 00 00 c5 8d 00 00-54 00 00 00 fd 8f 00 00 $···Å···T···ý···
00090 e2 00 00 00 17 a0 00 00-18 00 00 00 f5 a6 00 00 â····  ······õ¦··
```

Cursor pos = 0; clus = 210807; log sec = 210807; phy sec = 210904

☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	S
☐	baggifrodo		3754	<missin...	precious_corrupted_tes...	AOL E...	116.0 KB	115.8 KB	17B655...	10D27...	S
☐	baggifrodo.ARL		3757	arl	precious_corrupted_tes...	AOL Us...	16.00 KB	15.92 KB	34B702...	177D6...	E
☐	baggifrodo.BAG		3758	bag	precious_corrupted_tes...	AOL Bu...	1024 B	724 B	699316...	A1597...	7
☐	baggifrodo.bag		4572	bag	precious_corrupted_tes...	AOL Bu...	561 B	561 B	939A1...	683DF...	8
☐	bilbo baggins@aol[1].txt		1648	txt	precious_corrupted_tes...	Text	81 B	81 B	7E873B...	5156A...	C
☐	body		12587		precious_corrupted_tes...	Meta	n/a	1051 B	2171A...	F8F729...	5
☐	body		12589		precious_corrupted_tes...	Meta	n/a	568 B	B6691F...	2F56B1...	C
☐	body		12591		precious_corrupted_tes...	Meta	n/a	1114 B	828791...	C5C56...	4
☐	body		12597		precious_corrupted_tes...	Meta	n/a	1114 B	828791...	C5C56...	4
☐	body		12599		precious_corrupted_tes	Meta	n/a	138 B	C660C	5B75E	F

Loaded: 1,542   Filtered: 1,542   Total: 1,542   Highlighted: 1   Checked: 0

Ready   Live Search Tab Filter: [None]

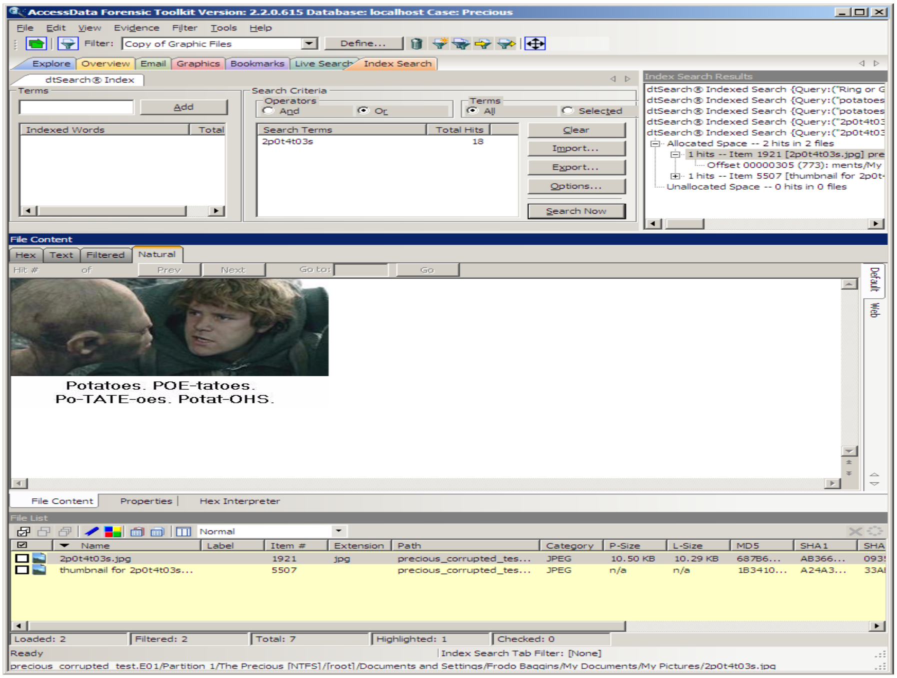
precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/All Users/Application Data/AOL/D America Onli.../Carved [10030692].png

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 6-21 Index Search Tab


AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost Case: Precious
File Edit View Evidence Filter Tools Help
Filter: Copy of Graphic Files
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search
dtSearch® Index
Terms
Add
Indexed Words
Total
Search Criteria
Operators
○ And
● Or
Terms
● All
○ Selected
Search Terms
Total Hits
Clear
Import...
Export...
Options...
Search Now
Index Search Results
File Content
Hex Text Filtered Natural
Hit # of Prev Next Go to: Go
Default
Web
Potatoes. POE-tatoes.
Po-TATE-oes. Potat-OHS.
File Content Properties Hex Interpreter
File List
Normal

Search Terms	Total Hits
2p0t4t03s	18

```
dtSearch® Indexed Search {Query:("Ring or G
dtSearch® Indexed Search {Query:("potatoes
dtSearch® Indexed Search {Query:("potatoes
dtSearch® Indexed Search {Query:("2p0t4t03
dtSearch® Indexed Search {Query:("2p0t4t03
⊟ Allocated Space -- 2 hits in 2 files
   ⊟ 1 hits -- Item 1921 [2p0t4t03s.jpg] pre
      Offset 00000305 (773): ments/My
   ⊞ 1 hits -- Item 5507 [thumbnail for 2p0t-
  Unallocated Space -- 0 hits in 0 files
```

☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA
□	2p0t4t03s.jpg		1921	jpg	precious_corrupted_tes...	JPEG	10.50 KB	10.29 KB	687B6...	AB366...	093
□	thumbnail for 2p0t4t03s...		5507		precious_corrupted_tes...	JPEG	n/a	n/a	1B3410...	A24A3...	33A

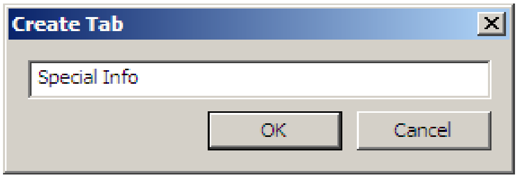
```
Loaded: 2 | Filtered: 2 | Total: 7 | Highlighted: 1 | Checked: 0
Ready | Index Search Tab Filter: [None]
precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/My Pictures/2p0t4t03s.jpg
```

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 6-22 Create Tab Dialog



Special Info

For more information on tab creation, see “Creating Custom Tabs” on page 213.

Chapter 7 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 process involving a bit-by-bit, item-by-item comparison of the search term against all evidence items contained in the case. A live search is flexible because it can find patterns of non-alphanumeric characters. Allow ample time for any live search to complete.

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 146.

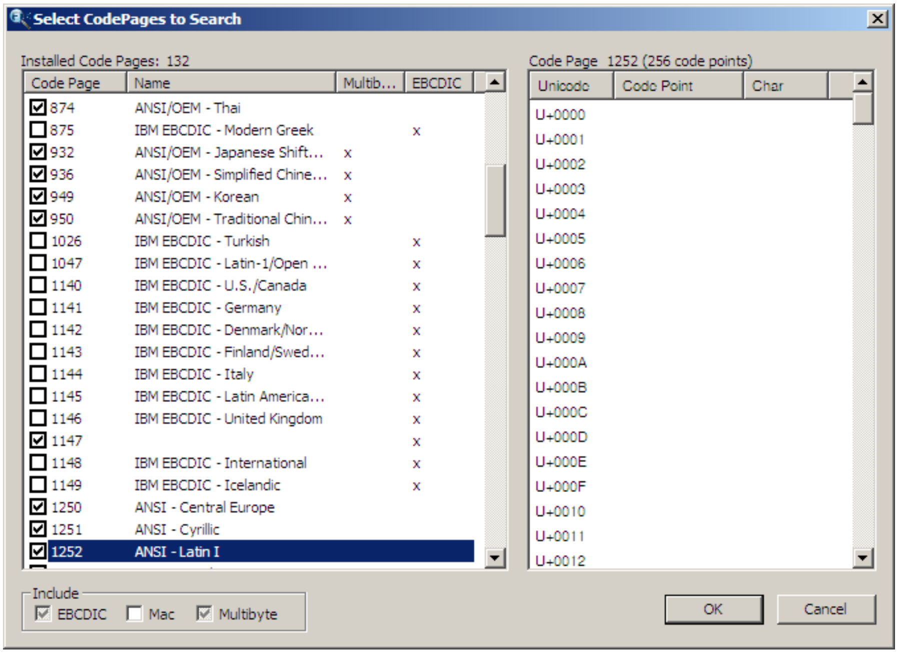
AccessData recommends live searching for items an index search cannot find.

To perform a live search, perform the following steps:

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

   In the *Text* or *Pattern* tabs, mark the character sets to include in the search. If Unicode is selected, and you need to include sets other than ANSI and Unicode, mark the box for *Other Code Pages*, scroll to the code page you need, then click to select it.

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.



Select CodePages to Search

Installed Code Pages: 132

Code Page	Name	Multib...	EBCDIC
☑ 874	ANSI/OEM - Thai		
□ 875	IBM EBCDIC - Modern Greek		x
☑ 932	ANSI/OEM - Japanese Shift...	x	
☑ 936	ANSI/OEM - Simplified Chine...	x	
☑ 949	ANSI/OEM - Korean	x	
☑ 950	ANSI/OEM - Traditional Chin...	x	
□ 1026	IBM EBCDIC - Turkish		x
□ 1047	IBM EBCDIC - Latin-1/Open ...		x
□ 1140	IBM EBCDIC - U.S./Canada		x
□ 1141	IBM EBCDIC - Germany		x
□ 1142	IBM EBCDIC - Denmark/Nor...		x
□ 1143	IBM EBCDIC - Finland/Swed...		x
□ 1144	IBM EBCDIC - Italy		x
□ 1145	IBM EBCDIC - Latin America...		x
□ 1146	IBM EBCDIC - United Kingdom		x
☑ 1147			x
□ 1148	IBM EBCDIC - International		x
□ 1149	IBM EBCDIC - Icelandic		x
☑ 1250	ANSI - Central Europe		
☑ 1251	ANSI - Cyrillic		
☑ 1252	ANSI - Latin I		

Code Page 1252 (256 code points)

Unicode	Code Point	Char
U+0000		
U+0001		
U+0002		
U+0003		
U+0004		
U+0005		
U+0006		
U+0007		
U+0008		
U+0009		
U+000A		
U+000B		
U+000C		
U+000D		
U+000E		
U+000F		
U+0010		
U+0011		
U+0012		

Include

☑ EBCDIC □ Mac ☑ Multibyte

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* in the *Live Search* > *Text* tab 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. Cancelling will return all results found so far.

12. Select the results you wish to view from the Live Search Results pane. Click the plus icon (+) next to a search line to expand the branch. Individual search results are listed in the Live Search Results pane, and the corresponding files are listed in the File List. To view a specific item, select the file in the search results. All search results are highlighted in the Hex View tab.

    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 7-1 Right-Click Options in Live Search Results Pane

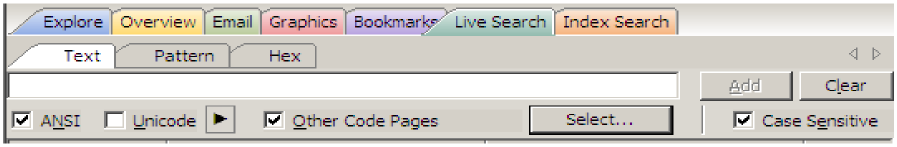
Option	Description
Create Bookmark	Opens the Create New Bookmark dialog.
Copy to Clipboard	Opens a new context-sensitive menu. Options are: • All Hits In Case • All Hist In Search • All File Stats In Case • All File Stats In Search
Export to File	Opens a new context-sensitive menu. Options are: • All Hits In Case • All Hist In Search • All File Stats In Case • All File Stats In Search
Set Context Data Width	Opens the Data Export Options window. Allows you to set a context width from 32 to 2000 characters within which to find and display the search hit.
Delete All Search Results	Deletes all search results from the Live Search Results pane.
Delete this Line	Deletes only the highlighted search results line from the Live Search Results pane.

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 7-1 Live Search Tabs



☑ ANSI □ Unicode ☑ Other Code Pages ☑ Case Sensitive

For more information on customizing the FTK user interface, see “Chapter 11 Customizing the Interface” on page 207.

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 7-2 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 symbol characters.

Simple Pattern Searches

A simple pattern search can be made up entirely of operands. For example, the pattern search *dress* causes the search engine to return a list of all files that contain the sequence of characters *d r e s s*. The pattern search *dress* corresponds to a very specific and restricted pattern of text, that is, sequences of text that contain the sub-string *dress*. Files containing the words “dress,” “address,” “dressing,” and “dresser,” are returned in a search for the pattern search *dress*.

The search engine searches left to right. So in searching the pattern search *dress,* the search engine opens each file and scans its contents line by line, looking for a *d,* followed by an *r*, followed by an *e*, and so on.

Complex Pattern Searches

Operators allow regular expressions to search patterns of data rather than specific values. For example, the operators in the following expression enables the FTK search engine to find all Visa and MasterCard credit card numbers in case evidence files:

```
\<((\d\d\d\d)[\– ]){3}\d\d\d\d\>
```

Without the use of operators, the search engine could look for only one credit card number at a time.

The following table identifies the components in the Visa and MasterCard regular expression:

TABLE 7-3 Visa and MasterCard Regular Expressions

Component	Example
Operands	\–, spacebar space
Operators	\, <, ( ), [ ], {3}, \>

TABLE 7-3 Visa and MasterCard Regular Expressions

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 comprise a sub-expression, that is, a sequence of characters contained within the parentheses 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 know 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 correlation 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.

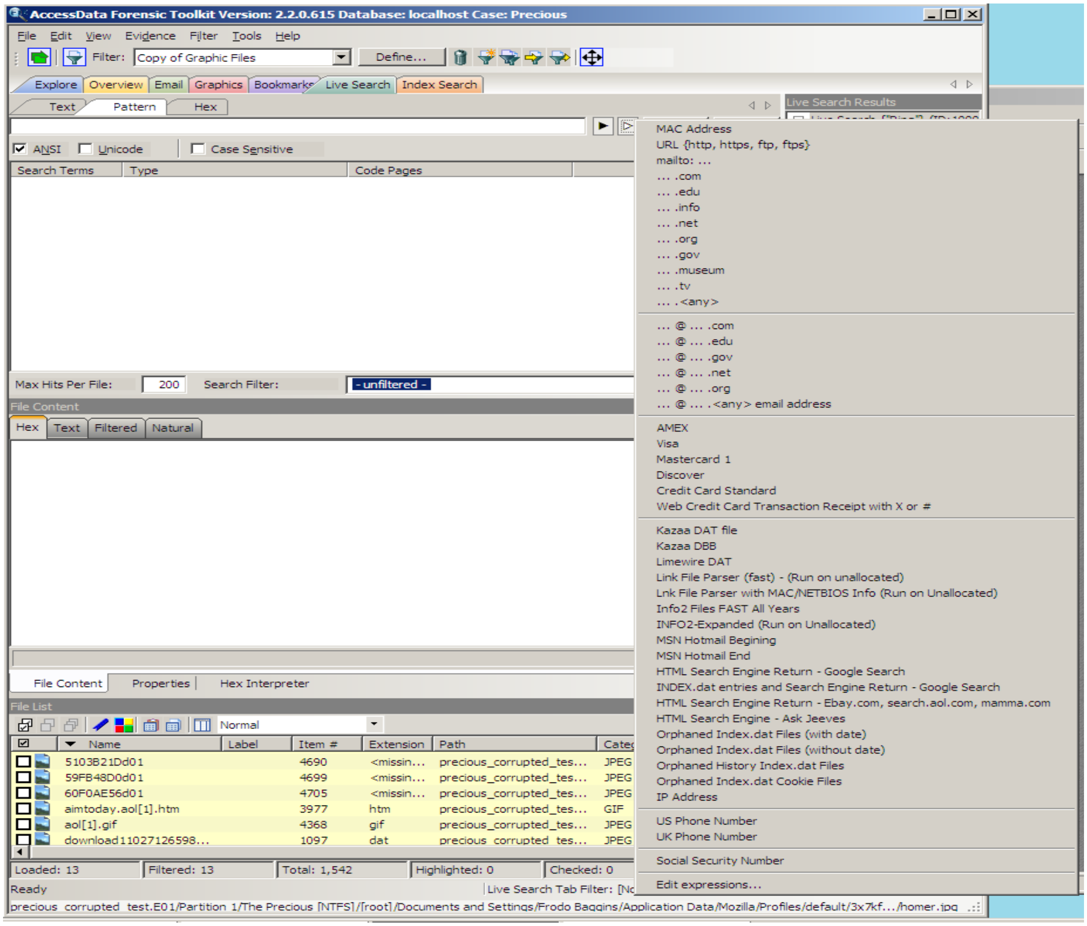
Predefined Regular Expressions

FTK provides several predefined regular expressions to be used in pattern searches.

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

- To access the Predefined Regular Expressions, click the white arrow ▷ . This will display the predefined regular expressions list, as shown in the following figure:

Figure 7-2 Pre-defined Regular Expressions List


AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost Case: Precious
File Edit View Evidence Filter Tools Help
Filter: Copy of Graphic Files
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search
Text Pattern Hex
Live Search Results
☑ ANSI □ Unicode □ Case Sensitive
Search Terms Type Code Pages
Max Hits Per File: 200 Search Filter: - unfiltered -
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal
MAC Address
URL {http, https, ftp, ftps}
mailto: ...
... .com
... .edu
... .info
... .net
... .org
... .gov
... .museum
... .tv
... .<any>
... @ ... .com
... @ ... .edu
... @ ... .gov
... @ ... .net
... @ ... .org
... @ ... .<any> email address
AMEX
Visa
Mastercard 1
Discover
Credit Card Standard
Web Credit Card Transaction Receipt with X or #
Kazaa DAT file
Kazaa DBB
Limewire DAT
Link File Parser (fast) - (Run on unallocated)
Lnk File Parser with MAC/NETBIOS Info (Run on Unallocated)
Info2 Files FAST All Years
INFO2-Expanded (Run on Unallocated)
MSN Hotmail Begining
MSN Hotmail End
HTML Search Engine Return - Google Search
INDEX.dat entries and Search Engine Return - Google Search
HTML Search Engine Return - Ebay.com, search.aol.com, mamma.com
HTML Search Engine - Ask Jeeves
Orphaned Index.dat Files (with date)
Orphaned Index.dat Files (without date)
Orphaned History Index.dat Files
Orphaned Index.dat Cookie Files
IP Address
US Phone Number
UK Phone Number
Social Security Number
Edit expressions...

☑	Name	Label	Item #	Extension	Path	Categ
□	5103B21Dd01		4690	<missin...	precious_corrupted_tes...	JPEG
□	59FB48D0d01		4699	<missin...	precious_corrupted_tes...	JPEG
□	60F0AE56d01		4705	<missin...	precious_corrupted_tes...	JPEG
□	aimtoday.aol[1].htm		3977	htm	precious_corrupted_tes...	GIF
□	aol[1].gif		4368	gif	precious_corrupted_tes...	JPEG
□	download1102712 6598...		1097	dat	precious_corrupted_tes...	JPEG

Loaded: 13 | Filtered: 13 | Total: 1,542 | Highlighted: 0 | Checked: 0

Ready | Live Search Tab Filter: [Nc

precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/Application Data/Mozilla/Profiles/default/3x7kf.../homer.jpg

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

TABLE 7-4 Predefined Pattern Searches

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

TABLE 7-4 Predefined Pattern Searches

... .gov	... .museum
... .tv	... .<any>
...@... .com	...@... .edu
...@... .gov	...@... .net
...@... .org	...@... .<any> email address
AMEX	Visa
Mastercard 1	Discover
Credit Card Standard	Web Credit Card Transaction Receipt with X or #
Kazaa DAT file	Kazaa DBB
Limewire DAT	Link File Parser (fast) - (Run on Unallocated)
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.

Creating Custom Regular Expressions

Create your own customized regular expressions using the following list of common operators:

TABLE 7-5 Common Regular Expressions Operators

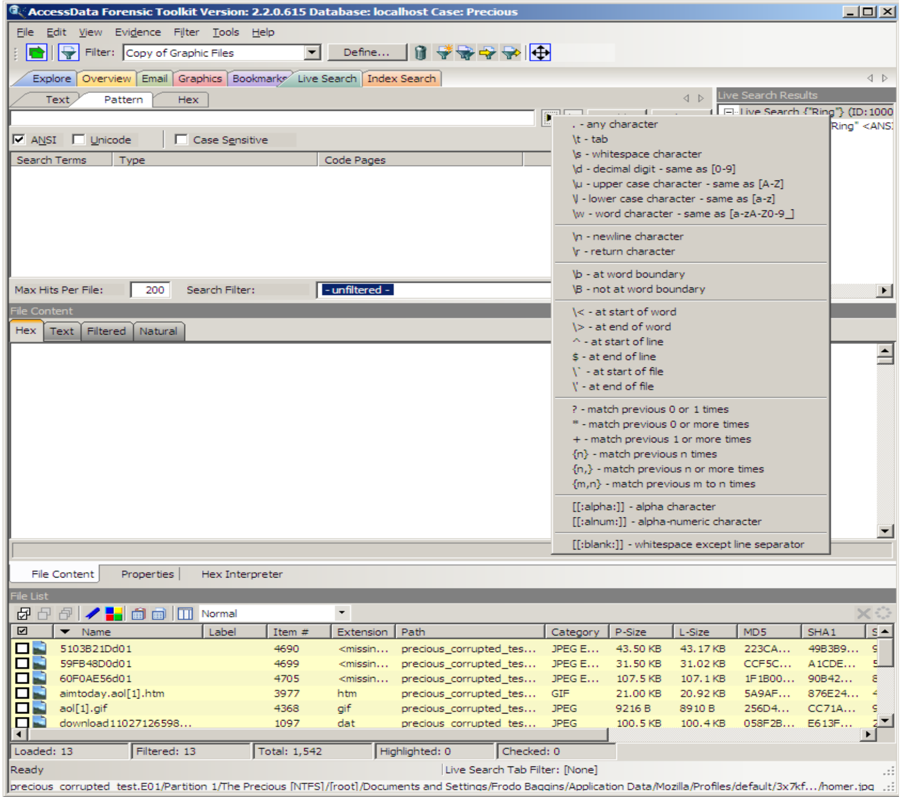
Operators	Description
+	Matches the preceding sub-expression one or more times. For example, “ba+” will find all instances of “ba,” “baa,” “baaa,” and so forth; but it will not find “b.”
$	Matches the end of a line.
*	Matches the preceding sub-expression zero or more times. For example, “ba*” will find all instances of “b,” “ba,” “baa,” “baaa,” and so forth.
?	Matches the preceding sub-expression zero or one times.

TABLE 7-5 Common Regular Expressions Operators

Operators	Description
[ ]	Matches any single value within the square brackets. For example, “ab[xyz]” will find “abx,” “aby,” and “abz.” A hyphen (-) specifies ranges of characters with the brackets. For example, “ab[0-3]” will find “ab0,” “ab1,” “ab2,” and “ab3.” You can also specify case specific ranges such as [a-r], or [B-M].
’	(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].
^	Matches the start of a line.
[[:alpha:]]	Matches any alpha character (short for the [a-z A-Z] operator).
[[:alnum:]]	Matches any alpha numerical character (short for the [a-z A-Z 0-9] operator).
[[:blank:]]	Matches any whitespace, except for line separators.
{*n*,*m*}	Matches the preceding sub-expression at least *n* times, but no more than *m* times.

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 7-3 Defining Customized Regular Expressions


AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost Case: Precious
File Edit View Evidence Filter Tools Help
Filter: Copy of Graphic Files
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search
Text Pattern Hex
Live Search Results
Live Search {"Ring"} (ID: 1000
"Ring" <ANSI
☑ ANSI ☐ Unicode ☐ Case Sensitive
Search Terms Type Code Pages
Max Hits Per File: 200 Search Filter: - unfiltered -
File Content
Hex Text Filtered Natural
File Content Properties Hex Interpreter
File List
Normal

. - any character
\t - tab
\s - whitespace character
\d - decimal digit - same as [0-9]
\u - upper case character - same as [A-Z]
\l - lower case character - same as [a-z]
\w - word character - same as [a-zA-Z0-9_]

\n - newline character
\r - return character

\b - at word boundary
\B - not at word boundary

\< - at start of word
> - at end of word
^ - at start of line
$ - at end of line
\` - at start of file
\' - at end of file

? - match previous 0 or 1 times
* - match previous 0 or more times
+ - match previous 1 or more times
{n} - match previous n times
{n,} - match previous n or more times
{m,n} - match previous m to n times

[[:alpha:]] - alpha character
[[:alnum:]] - alpha-numeric character

[[:blank:]] - whitespace except line separator

☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	S
☐	5103B21Dd01		4690	<missin...	precious_corrupted_tes...	JPEG E...	43.50 KB	43.17 KB	223CA...	49B3B9...	9
☐	59FB48D0d01		4699	<missin...	precious_corrupted_tes...	JPEG E...	31.50 KB	31.02 KB	CCF5C...	A1CDE...	5
☐	60F0AE56d01		4705	<missin...	precious_corrupted_tes...	JPEG E...	107.5 KB	107.1 KB	1F1B00...	90B42...	8
☐	aimtoday.aol[1].htm		3977	htm	precious_corrupted_tes...	GIF	21.00 KB	20.92 KB	5A9AF...	876E24...	4
☐	aol[1].gif		4368	gif	precious_corrupted_tes...	JPEG	9216 B	8910 B	256D4...	CC71A...	9
☐	download11027126598...		1097	dat	precious_corrupted_tes...	JPEG	100.5 KB	100.4 KB	058F2B...	E613F...	2

Loaded: 13 | Filtered: 13 | Total: 1,542 | Highlighted: 0 | Checked: 0

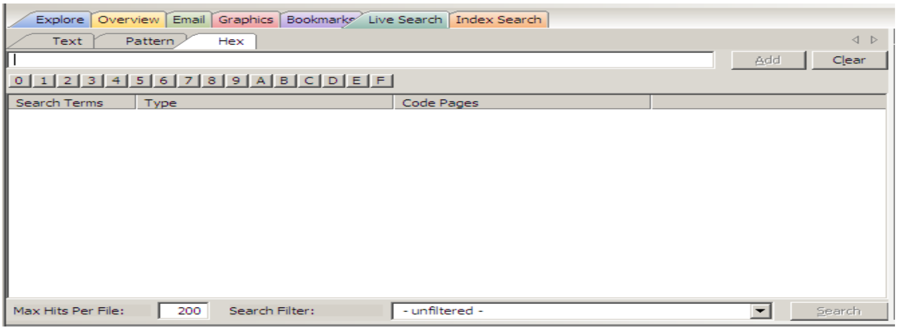
Ready | Live Search Tab Filter: [None]

precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/Application Data/Mozilla/Profiles/default/3x7kf.../homer.jpg

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 7-4 Hex Search Tab



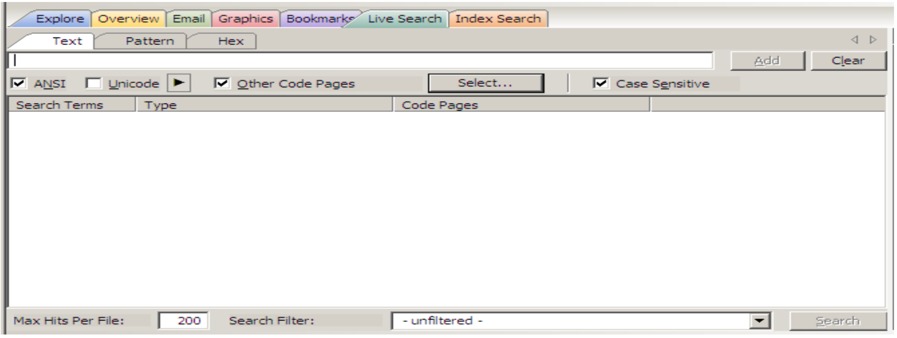
Max Hits Per File: 200 Search Filter: - unfiltered -

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 146.

Conducting Text Searches

The difference between a Pattern search and a Text search is that a text search searches for the exact typed text, there are no operands so the results return exactly as typed. For example, a Pattern search allows you to find all strings that match a certain pattern, such as for any 10-digit phone number (*nnn-nnn-nnnn*), or a nine-digit social security number (*nnn-nn-nnnn*). A Text search finds all strings that match an exact entry, such as a specific phone number (801-377-5410). When conducting a Live Text Search, there are no arrows to click for operand selection, as displayed in the following graphic.

Figure 7-5 Live Search: Text Search Tab



☑ ANSI ☐ Unicode ▶ ☑ Other Code Pages ☑ Case Sensitive

Max Hits Per File: 200 Search Filter: - unfiltered -

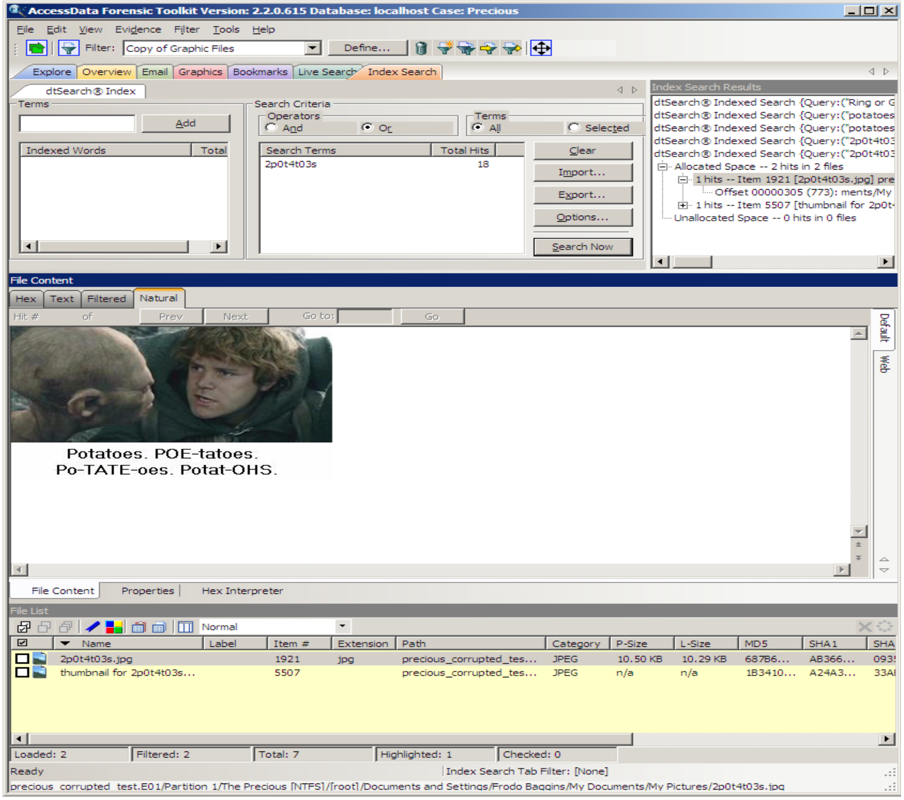
Otherwise apply the instructions for the pattern search to this search. For more information on conducting a pattern search see “Conducting a Pattern Search” on page 146.

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 61. The following figure displays the FTK window with the Index Seach tab selected.

Figure 7-6 Index Search Tab



AccessData Forensic Toolkit Version: 2.2.0.615 Database: localhost Case: Precious

Filter: Copy of Graphic Files

Search Criteria — Operators: ○ And ● Or — Terms: ● All ○ Selected

Search Terms	Total Hits
2p0t4t03s	18

Index Search Results

```
dtSearch® Indexed Search {Query:("Ring or G
dtSearch® Indexed Search {Query:("potatoes
dtSearch® Indexed Search {Query:("potatoes
dtSearch® Indexed Search {Query:("2p0t4t03
dtSearch® Indexed Search {Query:("2p0t4t03
⊟ Allocated Space -- 2 hits in 2 files
   ⊟ 1 hits -- Item 1921 [2p0t4t03s.jpg] pre
      Offset 00000305 (773): ments/My
   ⊞ 1 hits -- Item 5507 [thumbnail for 2p0t
  Unallocated Space -- 0 hits in 0 files
```

File List — Normal

☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA
□	2p0t4t03s.jpg		1921	jpg	precious_corrupted_tes...	JPEG	10.50 KB	10.29 KB	687B6...	AB366...	093
□	thumbnail for 2p0t4t03s...		5507		precious_corrupted_tes...	JPEG	n/a	n/a	1B3410...	A24A3...	33A

Loaded: 2 | Filtered: 2 | Total: 7 | Highlighted: 1 | Checked: 0

Ready | Index Search Tab Filter: [None]

precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/My Pictures/2p0t4t03s.jpg

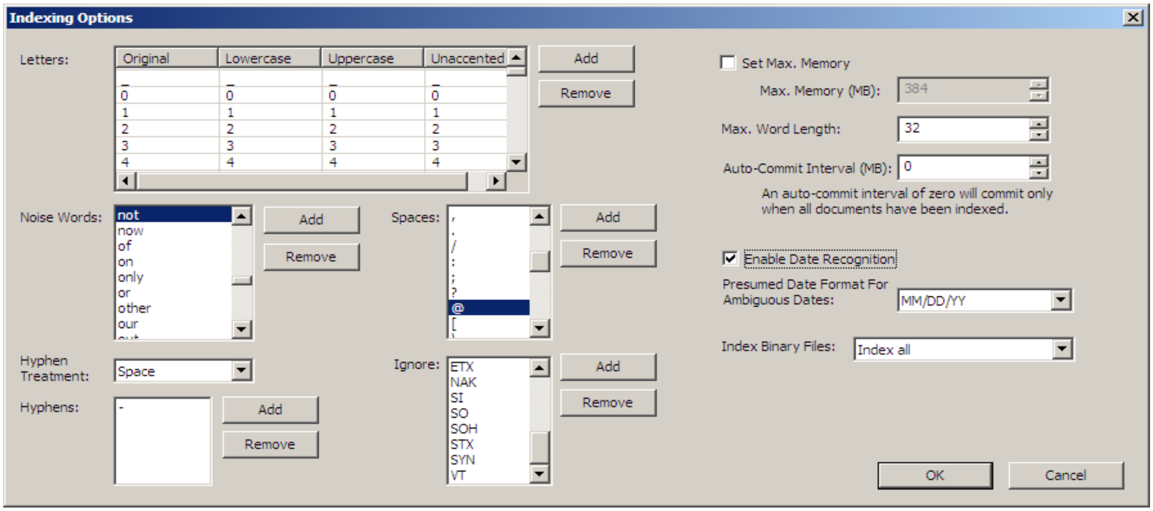
File Edit View Evidence Filter Tools Help
Define...
Explore Overview Email Graphics Bookmarks Live Search Index Search
dtSearch® Index
Terms
Add
Indexed Words Total
Clear
Import...
Export...
Options...
Search Now
File Content
Hex Text Filtered Natural
Hit # of Prev Next Go to: Go
Potatoes. POE-tatoes.
Po-TATE-oes. Potat-OHS.
Default Web
File Content Properties Hex Interpreter

The index files contain all discrete words or number strings found in both the allocated and unallocated space in the case evidence. FTK2.2 allows you to define nearly every aspect of indexing, include that of spaces and special characters or symbols, including the following:

. , : ; " ’ ~ ! # $ % ^ & @ = + .

The following figure shows the Indexing Options dialog:

Figure 7-7   New Indexing Options Dialog



Indexing Options

Letters:

Original	Lowercase	Uppercase	Unaccented
_	_	_	_
0	0	0	0
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4

Noise Words: not, now, of, on, only, or, other, our

Spaces: , . / : ; ? @ [

Hyphen Treatment: Space

Hyphens: -

Ignore: ETX, NAK, SI, SO, SOH, STX, SYN, VT

☐ Set Max. Memory

Max. Memory (MB): 384

Max. Word Length: 32

Auto-Commit Interval (MB): 0

An auto-commit interval of zero will commit only when all documents have been indexed.

☑ Enable Date Recognition

Presumed Date Format For Ambiguous Dates: MM/DD/YY

Index Binary Files: Index all

These options must be set prior to case creation. To set them globally, in Case Management, click *Tools* > *Create Options File* to bring up the Detailed Options dialog. In the Evidence Processing screen, mark the *dtSearch Text Index* box, then click *Indexing Options* to bring up the Indexing Options screen shown in the figure above.

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

TABLE 7-6 dtSearch Indexing Options

Option	Description
Letters	Specifies the letters and numbers to index. Specifies Original, Lowercase, Uppercase, and Unaccented. Choose *Add* or *Remove* to customize the list.
Noise Words	A list of words to be considered "noise" and ignored during indexing. Choose Add or Remove to customize the list. **Note:** The best way to use the ignore words box is to add and remove your own characters/symbols. When doing an index search those characters/symbols are ignored; when typing your search in you shouldn't included the character or symbol you chose to ignore. For example, add ! in the ignore box; in the case there is a term trus!t, in index search term type trust and you will get the hit.
Hyphen Treatment	Specifies how hyphens are to be treated in the index. Options are: • Ignore • Hyphen • Space • All
Hyphens	Specifies which characters are to be treated as hyphens. You can add standard keyboard characters, or control characters. You can remove items as well.
Spaces	Specifies which special characters should be treated as spaces. Remove characters from this list to have them indexed as any other text. Choose *Add* or *Remove* to customize the list.
Ignore	Specifies which control characters or other characters to ignore.
Set Max. Memory	Allows you to set a maximum size for the index.
Max. Word Length	Allows you to set a maximum word length to be indexed
Auto-Commit interval (MB)	Allows you to specify an Auto-Commit Interval while indexing the case. When the index reaches the specified size, the indexed data is saved to the index. The size resets, and indexing continues until it reaches the maximum size, and saves again, and so forth.

TABLE 7-6 dtSearch Indexing Options

Option	Description
Enable Date Recognition	Choose to enable or disable this option
Presumed Date Format For Ambiguous Dates	If date recognition is enables, specify how ambiguous dates should be formatted when enountered during indexing.
Index Binary Files	Specify how binary file should be treated in the index. Options are: • Index all • Skip • Index all (Unicode)

When finished setting Detailed Options, click *OK* to close the dialog, complete the New Case Options dialog, then click *OK* to create the case.

In addition to performing searches within the case, you can also use the index as a basis for a custom dictionary for password recovery processes in the Password Recovery Toolkit (PRTK). You can export the contents of 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.

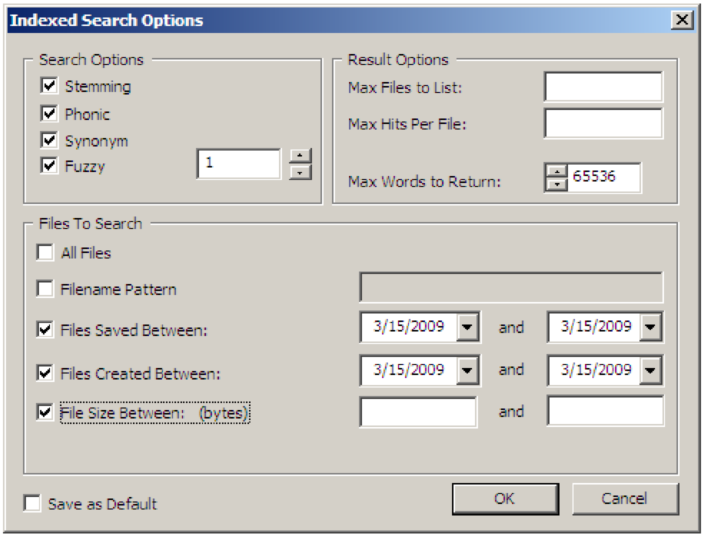
Click *Export* to save a set of search terms, then save the file.

Click *Import* to import a set of search terms then select and apply the imported 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 7-8 Index Search Options Dialog



Indexed Search Options

Search Options

☑ Stemming

☑ Phonic

☑ Synonym

☑ Fuzzy 1

Result Options

Max Files to List:

Max Hits Per File:

Max Words to Return: 65536

Files To Search

□ All Files

□ Filename Pattern

☑ Files Saved Between: 3/15/2009 and 3/15/2009

☑ Files Created Between: 3/15/2009 and 3/15/2009

☑ File Size Between: (bytes) and

□ Save as Default

The following tables review the individual search and result options:

TABLE 7-7 Individual Search and Result Options

Option	Result
Stemming	Words that contain the same root, such as *raise* and *raising*.
Phonic	Words that sound the same, such as *raise* and *raze*.
Synonym	Words that have similar meanings, such as *raise* and *lift*.
Fuzzy	Words that have similar spellings, such as *raise* and *raize*. Click the arrows to increase or decrease the number of letters in a word that can be different from the original search term.

TABLE 7-8 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. Searches limited by changing from the default 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. 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.
Max. Words to Return	The maximum number of words to be returned by the search.

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 7-9 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. Operator characters can be used to fill in for unknown characters. The pattern can include "?" to match any single character or "*" to match zero or more characters. The asterisk (*) and question-mark (?) operators are the only characters allowed in the search. For example, if you set the filename pattern to "d?ugl*", the search could return results from files named "douglas," "douglass", or "druglord." To enter a filename pattern: 1. Check the box. 2. In the field, type the filename pattern to search for.
Files Saved Between	Beginning and ending dates for the last time a file was saved. Do the following to set these parameters: 1. Check the box. 2. In the date fields, enter the beginning and ending dates to search.
Files Created Between	Beginning and ending dates for the creation of a file. Do the following to set these parameters: 1. Check the box. 2. In the date fields, enter the beginning and ending dates that you want to search.
File Size Between	Minimum and maximum file sizes, specified in bytes. Check the box. 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 your settings apply to all index searches.
OK	Saves the Indexed Search Options you have selected, and exits the dialog.
Cancel	Cancels the Indexed Search Options dialog without saving settings.

When search criteria are prepared and you are ready to perform the search, click OK to save your selected options, then 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 7-10 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.

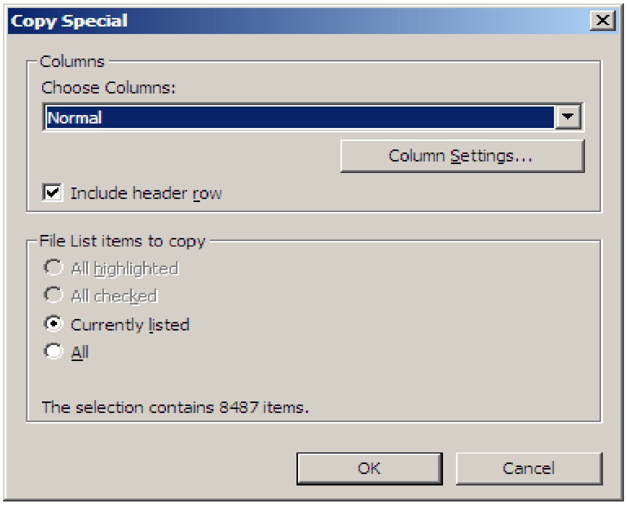
USING COPY SPECIAL TO DOCUMENT SEARCH RESULTS

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*.



Copy Special

Columns

Choose Columns: Normal

Column Settings...

☑ Include header row

File List items to copy

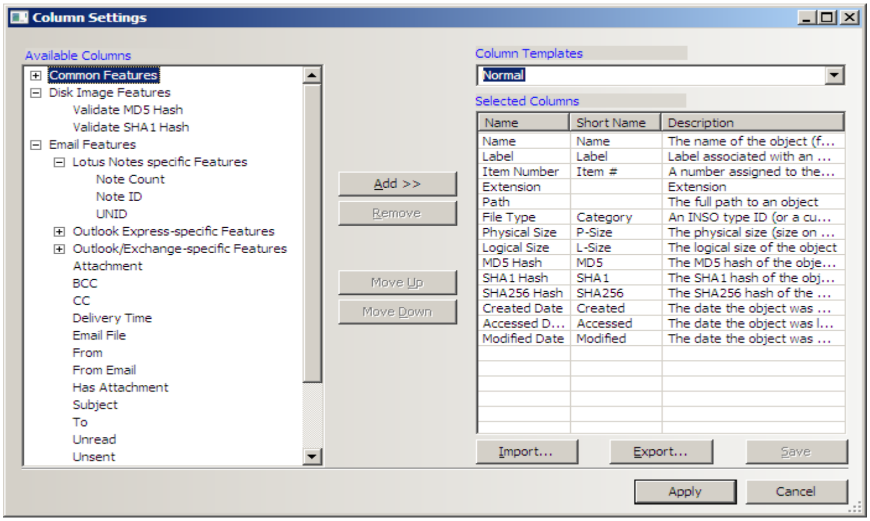
○ All highlighted
○ All checked
● Currently listed
○ All

The selection contains 8487 items.

OK Cancel

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.

Figure 7-9 Select Column Settings to Export with Copy Special



Column Templates: Normal

Selected Columns

Name	Short Name	Description
Name	Name	The name of the object (f...
Label	Label	Label associated with an ...
Item Number	Item #	A number assigned to the...
Extension		Extension
Path		The full path to an object
File Type	Category	An INSO type ID (or a cu...
Physical Size	P-Size	The physical size (size on ...
Logical Size	L-Size	The logical size of the object
MD5 Hash	MD5	The MD5 hash of the obje...
SHA1 Hash	SHA1	The SHA1 hash of the obj...
SHA256 Hash	SHA256	The SHA256 hash of the ...
Created Date	Created	The date the object was ...
Accessed D...	Accessed	The date the object was l...
Modified Date	Modified	The date the object was ...

5a. Modify the column template in the Column Settings Manager. For more information on customizing column templates, see “Customizing File List Columns” on page 213.

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 129.
4. Click *OK*.

The bookmark now appears in the Bookmark tab.

Chapter 8 Using Filters

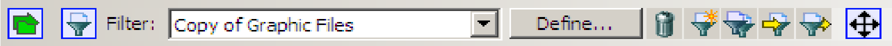
AccessData Forensic Toolkit (FTK) can filter files by their metadata to find specific evidence. For example, FTK can filter a large number of graphics by creation date to see only those made during a certain time frame.

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


Filter: Copy of Graphic Files

For an explanation of the filter toolbar and its components, see “QuickPicks Filter” on page 101.

APPLYING AN EXISTING FILTER

FTK contains the following predefined filters:

TABLE 8-1 Pre-defined Filters

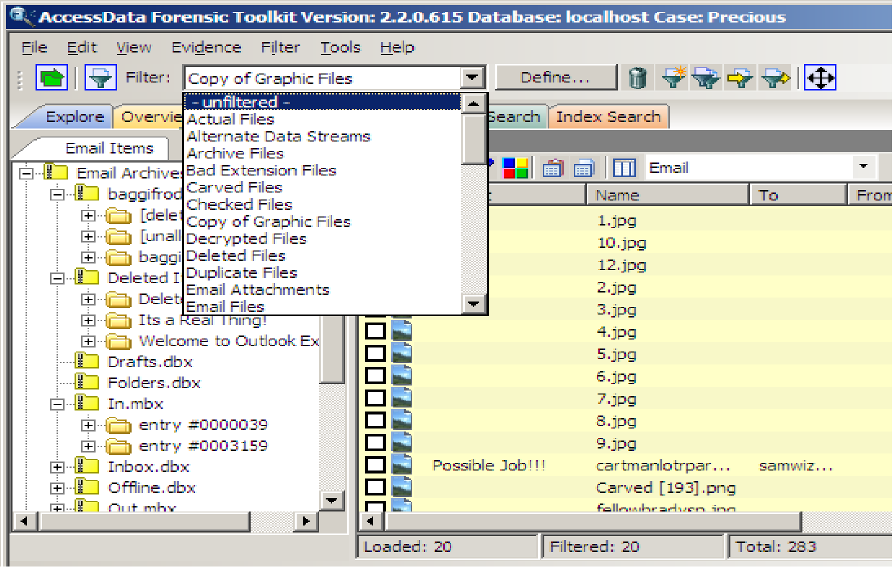
Filter	Description
Archive Files	Shows only archive file items.
Bad Extension Files	Shows only the files with extensions that don't match the detected file type.
Carved Files	Shows only the items that have been carved.
Checked Files	Shows only the items that you have selected with a checkmark.
Decrypted 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 occurs more than once in the case.
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, items encrypted by other means, and compressed files.
Evidence Items	Shows all items added as evidence without their descendents.
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 itemsfound in one of the system recycle bin folders.
Graphic Files	Show only those items that have been identified as graphics.
KFF Alert Files	Shows items flagged Alert by the KFF..
Microsoft Office Files	Show Word, Access, PowerPoint, and Excel files.
KFF Ignore Files	Shows items flagged ignore by the KFF.
No Deleted	Shows all items that do not have Deleted status.

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 except those flagged ignore by the KFF..
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 except 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.
No Unimportant OLE Streams	Shows all items not affected by Unimportant OLE Streams Filter.
Unimportant OLE Streams	Shows all items from OLE Streams that are in the set of categories in the Unimportant OLE Stream Categories (UOSC).
Unimportant OLE Stream Categories	Shows all items in their Unimportant OLE Streams Categories.

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.)

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.

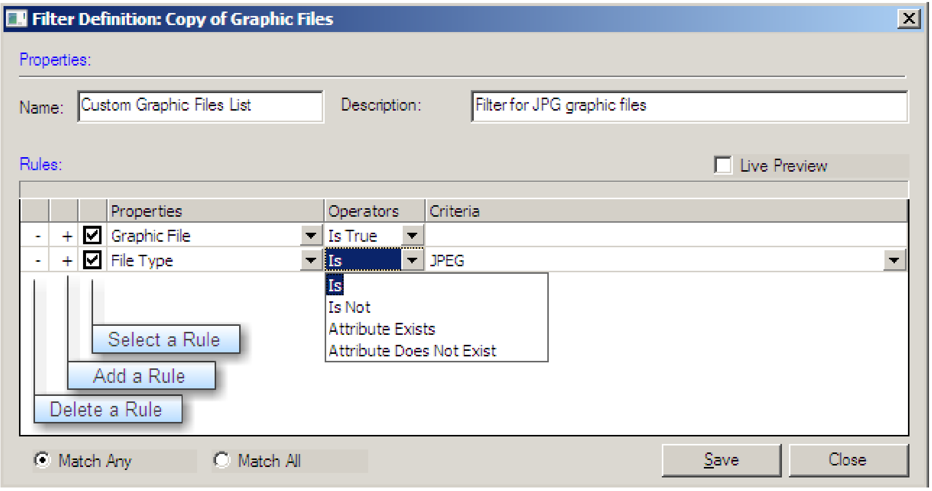
7. Select the *Match Any* operator to filter out data that satisfies any one of the filter rules or the *Match All* operator to filter out data that satisfies all rules of the filter.
8. Click *Save*. The filter you just created is now the active filter.
9. Click *Close*.

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



Filter Definition: Copy of Graphic Files

Properties:

Name: Custom Graphic Files List

Description: Filter for JPG graphic files

Rules:

□ Live Preview

			Properties	Operators	Criteria
-	+	☑	Graphic File	Is True	
-	+	☑	File Type	Is	JPEG

● Match Any ○ Match All

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*.
5. Select the newly created filter from the Filter drop-down in the toolbar to apply it.

Deleting a Filter

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

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) is a utility that uses a database of hash values of known files to filter the files found in the evidence. The purpose of the KFF is to eliminate unimportant files, or to identify and alert the user to known files with illicit content. It also checks for duplicate files. When you add evidence to the case, select KFF to 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

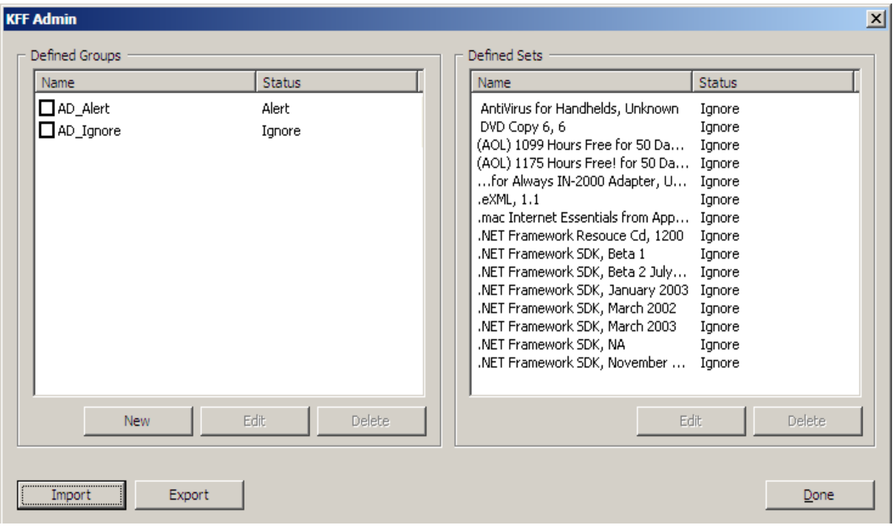
FTK includes hashes from two major reporting agencies, The National Institute of Standards and Technology (NIST), and Hashkeeper, created and maintained by the National Drug Intelligence Center (NDIC). The toolkit also provides a mechanism for the addition of hashes from other sources to the KFF database. 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:

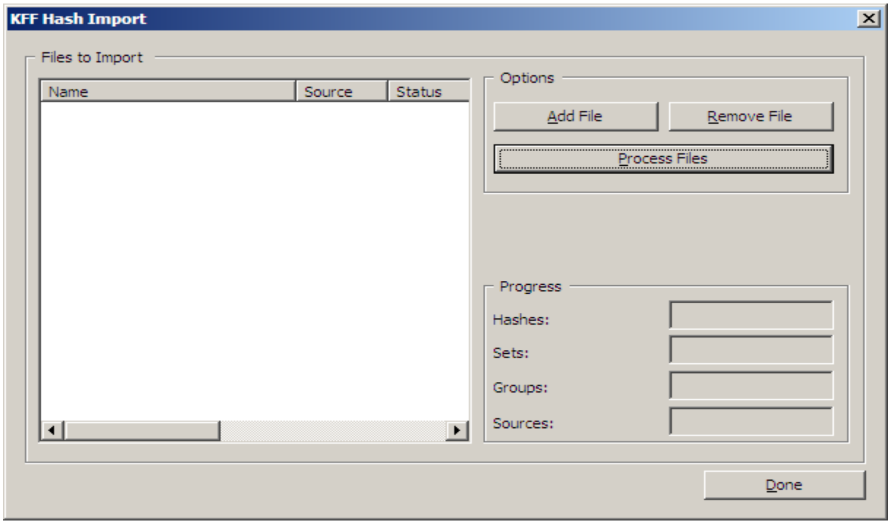
1. Click *Tools* > *KFF* > *Manage* to open the KFF Administration dialog.



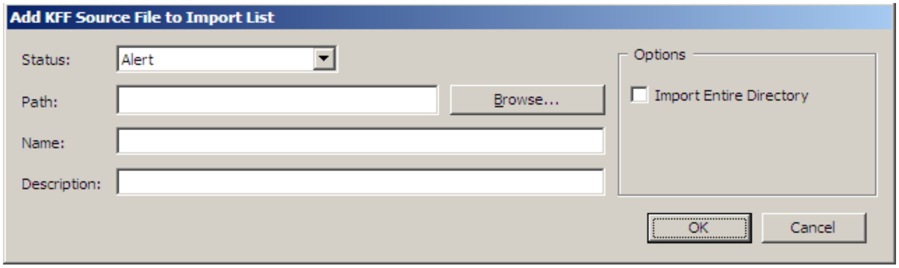
Name	Status
☐ AD_Alert	Alert
☐ AD_Ignore	Ignore

Name	Status
AntiVirus for Handhelds, Unknown	Ignore
DVD Copy 6, 6	Ignore
(AOL) 1099 Hours Free for 50 Da...	Ignore
(AOL) 1175 Hours Free! for 50 Da...	Ignore
...for Always IN-2000 Adapter, U...	Ignore
.eXML, 1.1	Ignore
.mac Internet Essentials from App...	Ignore
.NET Framework Resouce Cd, 1200	Ignore
.NET Framework SDK, Beta 1	Ignore
.NET Framework SDK, Beta 2 July...	Ignore
.NET Framework SDK, January 2003	Ignore
.NET Framework SDK, March 2002	Ignore
.NET Framework SDK, March 2003	Ignore
.NET Framework SDK, NA	Ignore
.NET Framework SDK, November ...	Ignore

2. Click *Import* to open the KFF Hash Import dialog.



3. Click *Add File*. In the Add KFF Source File to Import List dialog you can choose to import any 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)



Add KFF Source File to Import List

Status: Alert

Path:

Name:

Description:

3a. Click the Status drop-down list to select either Alert or Ignore status for the list you are importing.

3b. Browse to the path where the new source file is found.

3c. Type a name for the new source.

3d. Include a description of the new source file.

3e. Mark the *Import Entire Directory* box if all the files in the source path are to be included in this import.

3f. Click *OK* to close this dialog and return to the KFF Hash Import dialog keeping the new source files, or click *Cancel* to close this dialog without adding the new source files.

4. In the KFF Hash Import dialog verify the files to import, and click *Process Files*.

   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 and User Created.

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.
User Created	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 it's 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.

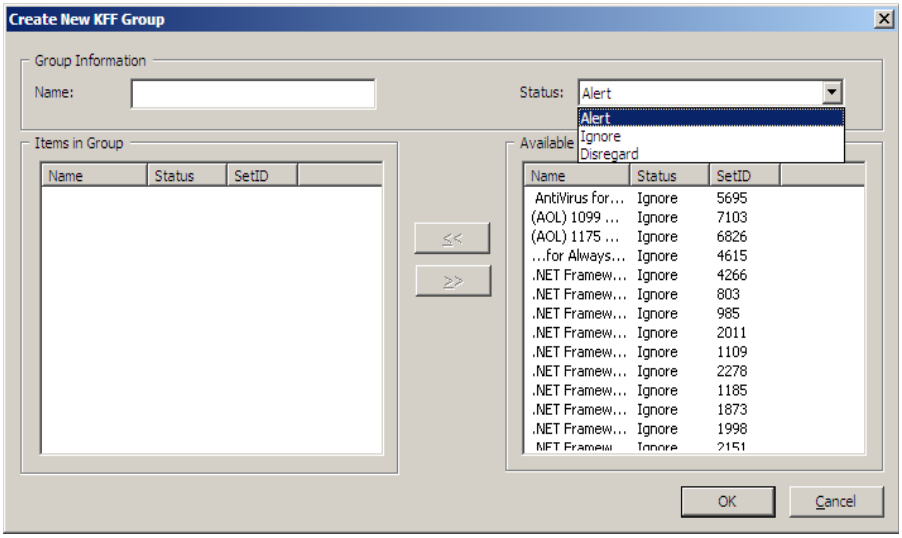
If you have included the same set in two different groups, FTK prioritizes the status and returns the highest priority status:

1. Disregard
2. Alert
3. Ignore

CREATING SETS AND GROUPS

To create sets and organize them into groups, follow these steps:

1. Select *Tools* > *KFF* > *Manage.*
2. Click *New.*



Name:

Status: Alert

Alert
Ignore
Disregard

Name	Status	SetID

Name	Status	SetID
AntiVirus for...	Ignore	5695
(AOL) 1099 ...	Ignore	7103
(AOL) 1175 ...	Ignore	6826
...for Always...	Ignore	4615
.NET Framew...	Ignore	4266
.NET Framew...	Ignore	803
.NET Framew...	Ignore	985
.NET Framew...	Ignore	2011
.NET Framew...	Ignore	1109
.NET Framew...	Ignore	2278
.NET Framew...	Ignore	1185
.NET Framew...	Ignore	1873
.NET Framew...	Ignore	1998
.NET Framew...	Ignore	2151

3. Name the group.
4. Assign the group a status.
5. Select the sets you want in the group from the Available Sets list and move them to the Items in Group list by clicking the arrow button.
6. Click *Apply* to create the group without closing the Create New KFF dialog.
7. Click *OK* to save the group and close.

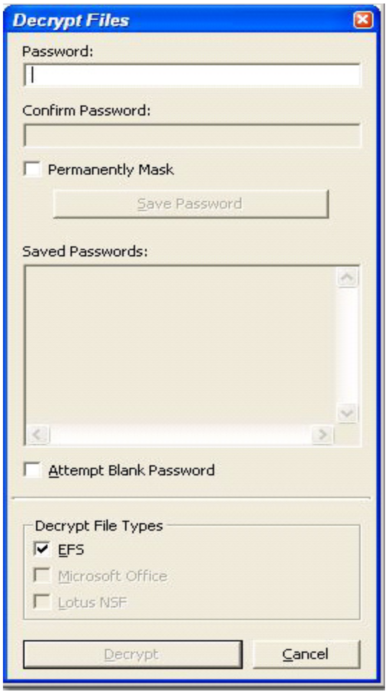
Chapter 9 Decrypting Encrypted Files

Decrypting Files and Folders

FTK 2.2 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 FTK2.2.

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 2.2 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.

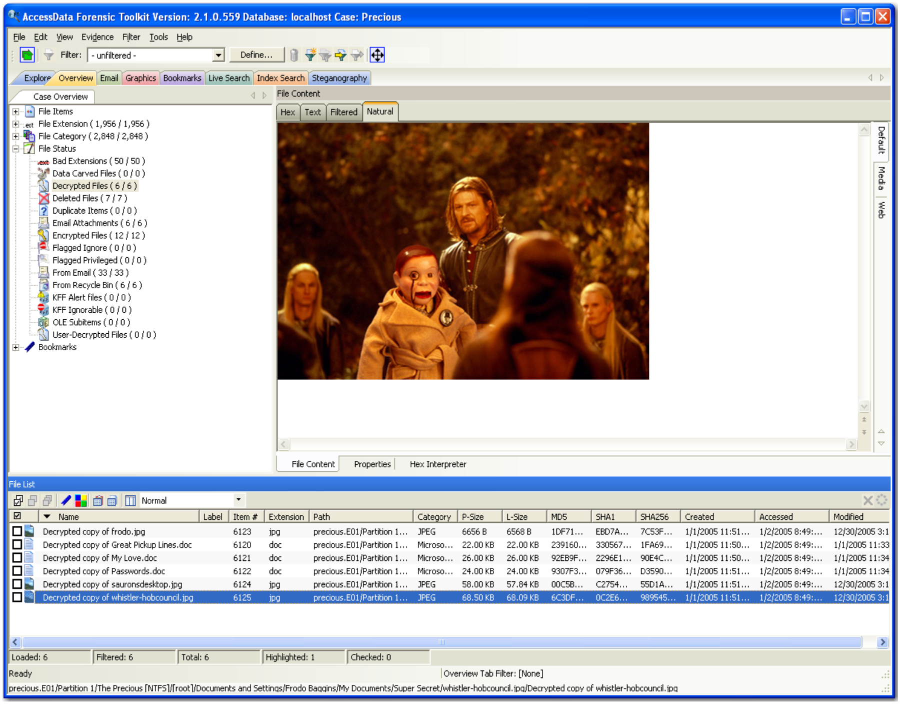
There are certain files that cannot be encrypted, including system files, NTFS compressed files, and files in the [*drive*]:\[*Windows_System_Root*] and its subdirectories.

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



Filter: - unfiltered -

- File Items
- File Extension (1,956 / 1,956)
- File Category (2,848 / 2,848)
- File Status
  - Bad Extensions (50 / 50)
  - Data Carved Files (0 / 0)
  - Decrypted Files (6 / 6)
  - Deleted Files (7 / 7)
  - Duplicate Items (0 / 0)
  - Email Attachments (6 / 6)
  - Encrypted Files (12 / 12)
  - Flagged Ignore (0 / 0)
  - Flagged Privileged (0 / 0)
  - From Email (33 / 33)
  - From Recycle Bin (6 / 6)
  - KFF Alert files (0 / 0)
  - KFF Ignorable (0 / 0)
  - OLE Subitems (0 / 0)
  - User-Decrypted Files (0 / 0)
- Bookmarks

Normal

☑	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
□	Decrypted copy of frodo.jpg		6123	jpg	precious.E01/Partition 1...	JPEG	6656 B	6568 B	1DF71...	EBD7A...	7C53F...	1/1/2005 11:51...	1/2/2005 8:49:...	12/30/2005 3:1
□	Decrypted copy of Great Pickup Lines.doc		6120	doc	precious.E01/Partition 1...	Microso...	22.00 KB	22.00 KB	239160...	330567...	1FA69...	1/1/2005 11:50...	1/2/2005 8:49:...	1/1/2005 11:33
□	Decrypted copy of My Love.doc		6121	doc	precious.E01/Partition 1...	Microso...	26.00 KB	26.00 KB	92EB9F...	2296E1...	90E4C...	1/1/2005 11:50...	1/2/2005 8:49:...	1/1/2005 11:34
□	Decrypted copy of Passwords.doc		6122	doc	precious.E01/Partition 1...	Microso...	24.00 KB	24.00 KB	9307F3...	079F36...	D3590...	1/1/2005 11:51...	1/2/2005 8:49:...	1/1/2005 11:34
□	Decrypted copy of saurونsdesktop.jpg		6124	jpg	precious.E01/Partition 1...	JPEG	58.00 KB	57.84 KB	00C5B...	C2754...	55D1A...	1/1/2005 11:51...	1/2/2005 8:49:...	12/30/2005 3:1
□	Decrypted copy of whistler-hobcouncil.jpg		6125	jpg	precious.E01/Partition 1...	JPEG	68.50 KB	68.09 KB	6C3DF...	0C2E6...	989545...	1/1/2005 11:51...	1/2/2005 8:49:...	12/30/2005 3:1

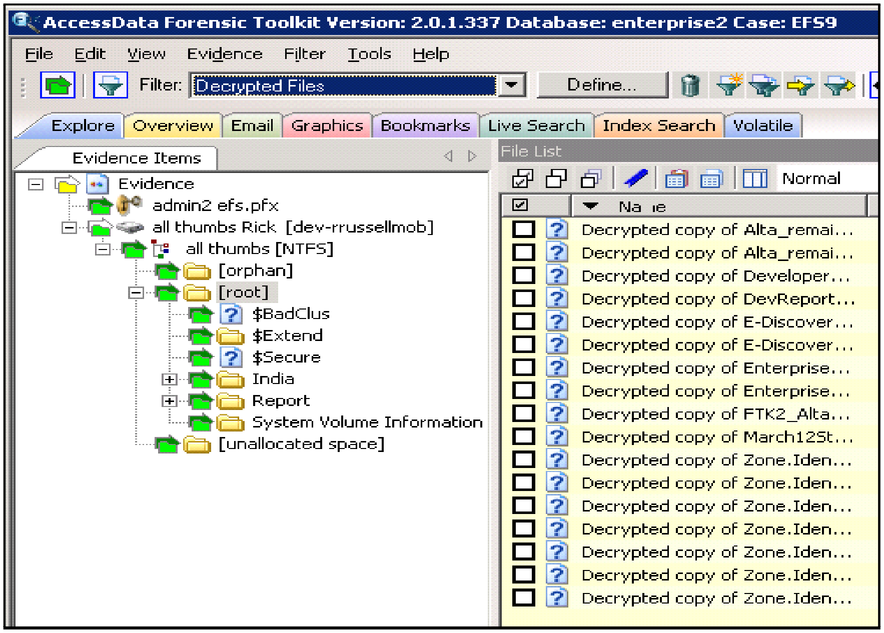
Loaded: 6 | Filtered: 6 | Total: 6 | Highlighted: 1 | Checked: 0

Ready | Overview Tab Filter: [None]

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/Super Secret/whistler-hobcouncil.jpg/Decrypted copy of whistler-hobcouncil.jpg

Note: Regardless of the encryption type, once decrypted, the files will appear in the File List Name column as "Decrypted copy of [*filename*]," as seen in the following figure:

Figure 9-3 File List showing Decrypted Files



Filter: Decrypted Files

☑	Na e
□	Decrypted copy of Alta_remai...
□	Decrypted copy of Alta_remai...
□	Decrypted copy of Developer...
□	Decrypted copy of DevReport...
□	Decrypted copy of E-Discover...
□	Decrypted copy of E-Discover...
□	Decrypted copy of Enterprise...
□	Decrypted copy of Enterprise...
□	Decrypted copy of FTK2_Alta...
□	Decrypted copy of March12St...
□	Decrypted copy of Zone.Iden...
□	Decrypted copy of Zone.Iden...
□	Decrypted copy of Zone.Iden...
□	Decrypted copy of Zone.Iden...
□	Decrypted copy of Zone.Iden...
□	Decrypted copy of Zone.Iden...
□	Decrypted copy of Zone.Iden...

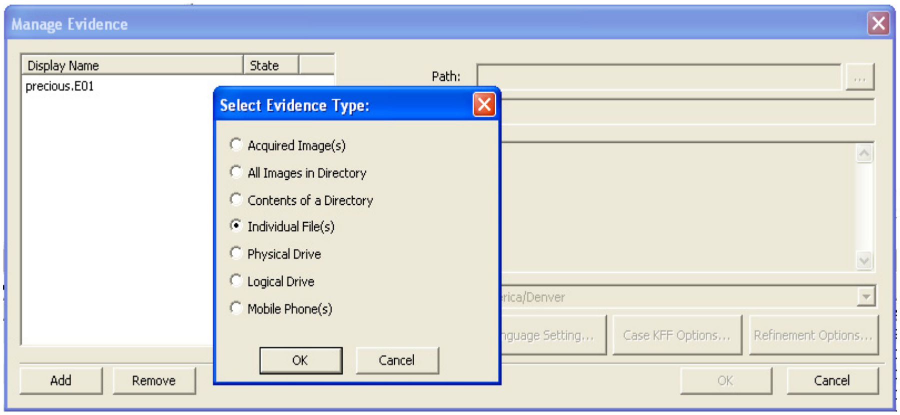
DECRYPTING DOMAIN ACCOUNT EFS FILES

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.*



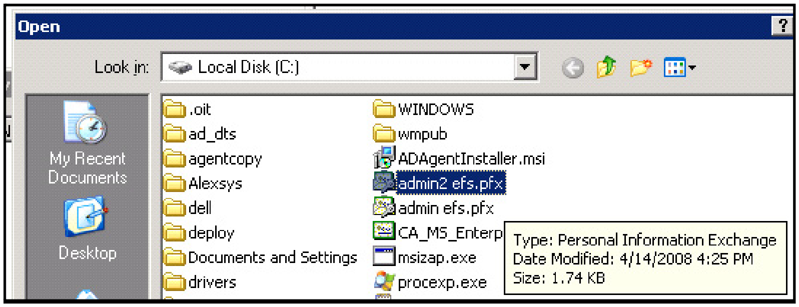
precious.E01

○ Acquired Image(s)
○ All Images in Directory
○ Contents of a Directory
● Individual File(s)
○ Physical Drive
○ Logical Drive
○ Mobile Phone(s)

rica/Denver

3. Click *Add.*
4. Select *Individual File(s).*
5. Click *OK.*
6. Navigate to the PFX path and filename (domain recovery key).

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



Look in: Local Disk (C:)

.oit
ad_dts
agentcopy
Alexsys
dell
deploy
Documents and Settings
drivers
WINDOWS
wmpub
ADAgentInstaller.msi
admin2 efs.pfx
admin efs.pfx
CA_MS_Enterp
msizap.exe
procexp.exe

Type: Personal Information Exchange
Date Modified: 4/14/2008 4:25 PM
Size: 1.74 KB

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.*

   FTK 2.2 begins processing the PFX file and the progress dialog appears.

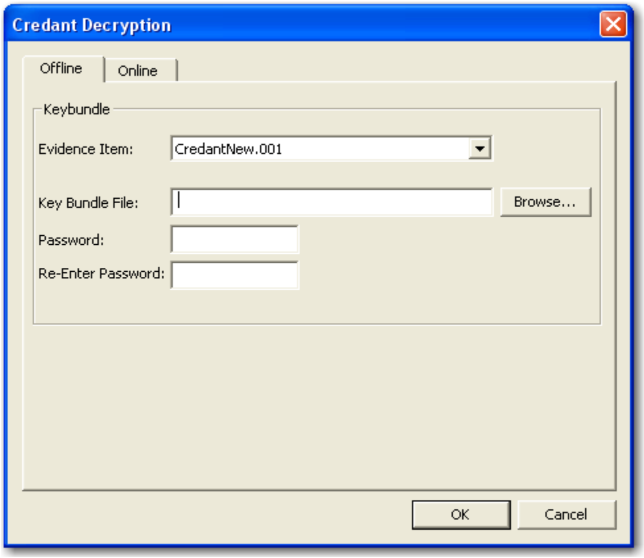
Note:

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



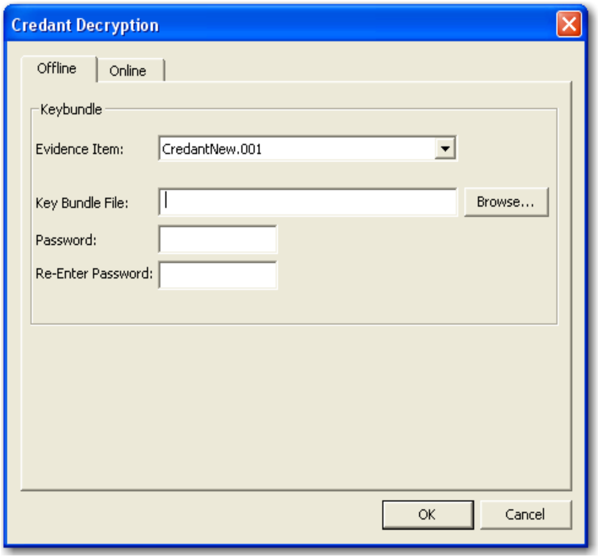
Evidence Item: CredantNew.001

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. 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 local 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. This is detailed in the following steps:

1. Click *Tools* > *Credant Decryption* to open the Credant decryption options dialog.



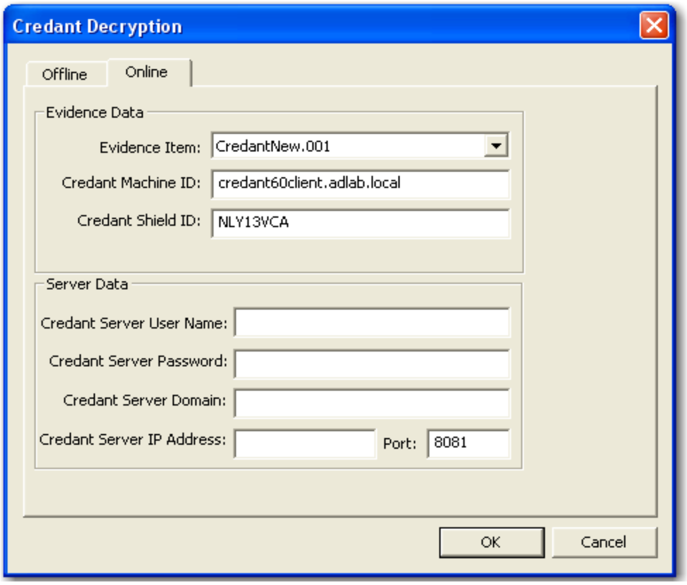
Evidence Item: CredantNew.001

2. Select the key bundle file by entering its location or browsing to it.
3. Enter the password.
4. Re-enter the password.
5. Click *OK*.

Using an Online Key Bundle

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

Figure 9-5 Credant Decryption Online Tab Options



Credant Decryption

Evidence Data

Evidence Item: CredantNew.001

Credant Machine ID: credant60client.adlab.local

Credant Shield ID: NLY13VCA

Server Data

Credant Server User Name:

Credant Server Password:

Credant Server Domain:

Credant Server IP Address:

Port: 8081

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 similar to 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 address. The port should be 8081, and is auto-populated.

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

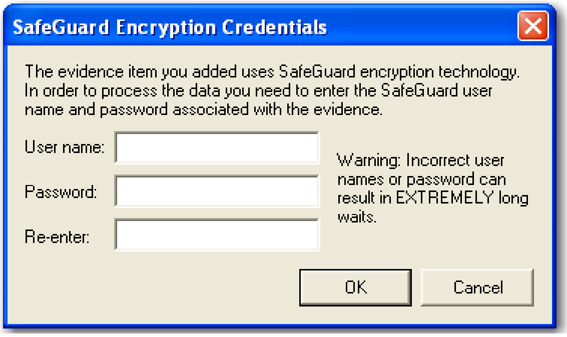
Note that all command line switches are case sensitive. Also, there is no space between the switch and the datatype.

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   Provide the Safeguard Encryption Credentials



SafeGuard Encryption Credentials

The evidence item you added uses SafeGuard encryption technology. In order to process the data you need to enter the SafeGuard user name and password associated with the evidence.

User name:

Password:

Re-enter:

Warning: Incorrect user names or password can result in EXTREMELY long waits.

The Safeguard dialog box appears only when FTK 2.2 reads a valid Utimaco-encrypted image.

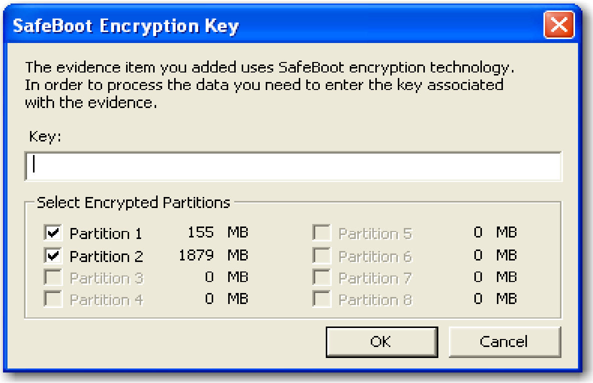
The username and password used to create the encrypted image are required for decryption. Once the credentials have been added, click *OK* to return to the Manage Evidence dialog. Select a time zone from the Time Zone drop-down, then click *OK* to begin processing.

Important: Type the User Name and Password carefully and verify both before clicking *OK*. If this information is entered incorrectly, FTK 2.2 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 FTK 2.2 detects a SafeBoot-encrypted drive or partition, the following dialog is displayed.

Figure 9-7 SafeBoot Encryption Key Entry



SafeBoot Encryption Key

The evidence item you added uses SafeBoot encryption technology. In order to process the data you need to enter the key associated with the evidence.

Key:

Select Encrypted Partitions

☑	Partition 1	155	MB	□	Partition 5	0	MB
☑	Partition 2	1879	MB	□	Partition 6	0	MB
□	Partition 3	0	MB	□	Partition 7	0	MB
□	Partition 4	0	MB	□	Partition 8	0	MB

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 time zone from the Time Zone drop-down, then click *OK* to begin processing.

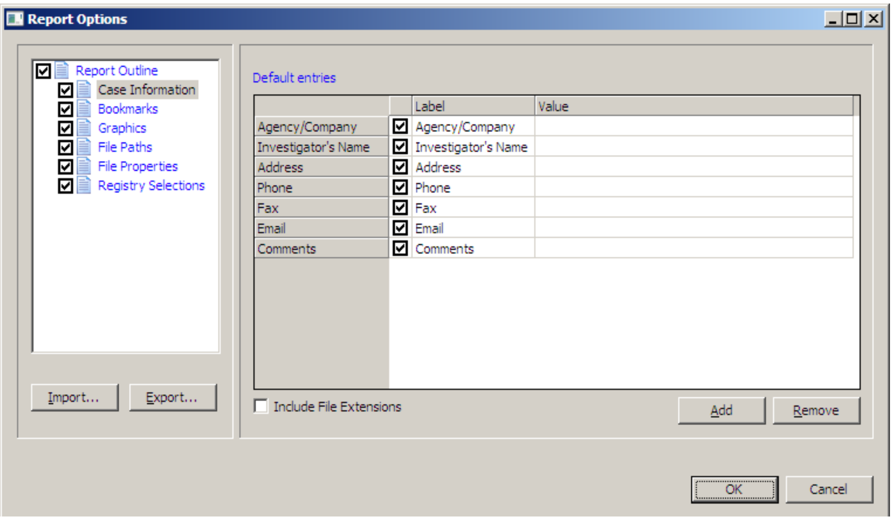
Chapter 10 Working with Reports

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 including one that is viewable in a standard Web browser.

Creating a Report

Create a report with the Report Wizard. Access the Report Wizard by selecting *File > Report*. The Report Wizard is displayed in the following figure:

Figure 10-1 Report Options Dialog



- ☑ Report Outline
  - ☑ Case Information
  - ☑ Bookmarks
  - ☑ Graphics
  - ☑ File Paths
  - ☑ File Properties
  - ☑ Registry Selections

Default entries

	Label	Value
Agency/Company	☑ Agency/Company	
Investigator's Name	☑ Investigator's Name	
Address	☑ Address	
Phone	☑ Phone	
Fax	☑ Fax	
Email	☑ Email	
Comments	☑ Comments	

□ Include File Extensions

To create a report:

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

Each step is discussed in detail in the following sections.

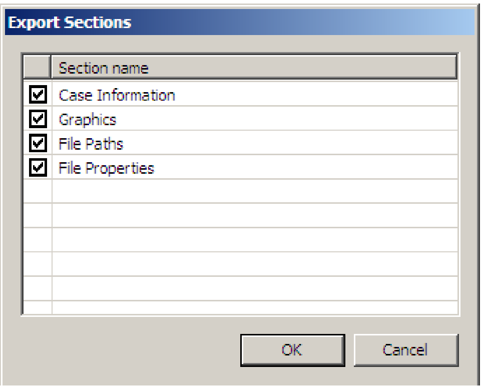
Saving Settings

Report settings are auromatically 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.



Export Sections

	Section name
☑	Case Information
☑	Graphics
☑	File Paths
☑	File Properties

2. Check the Section Names to include in the exported settings file.
3. Click *OK*.
4. Type a name for the exported settings file.
5. Click *OK* to save the settings as an .XML file.

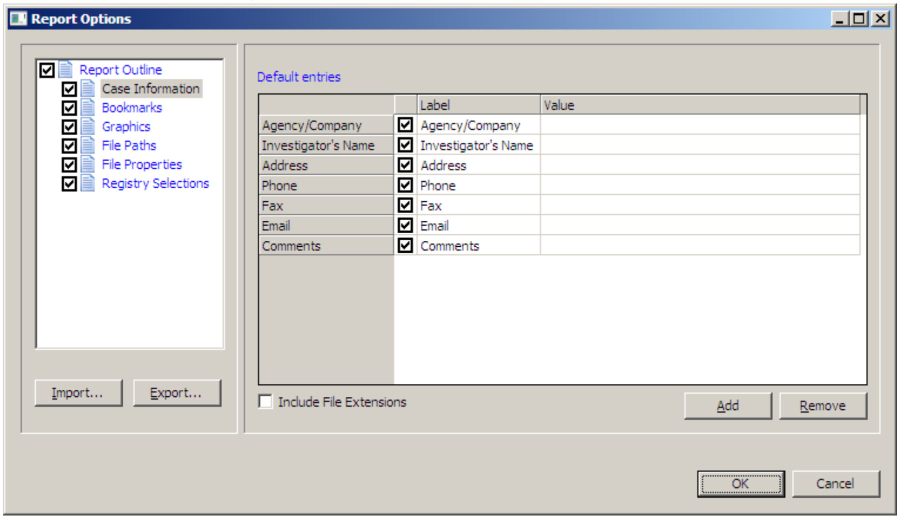
To import settings to a new report in this or another case, perform the following steps:

1. Open a this case or a different case.
1. Click *File* > *Report* > *Import*.
2. Browse to and select the exported settings .XML 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



- ☑ Report Outline
  - ☑ Case Information
  - ☑ Bookmarks
  - ☑ Graphics
  - ☑ File Paths
  - ☑ File Properties
  - ☑ Registry Selections

Default entries

		Label	Value
Agency/Company	☑	Agency/Company	
Investigator's Name	☑	Investigator's Name	
Address	☑	Address	
Phone	☑	Phone	
Fax	☑	Fax	
Email	☑	Email	
Comments	☑	Comments	

□ Include File Extensions

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 include a File Extensions List and count in the File Overview portion of the report.

Important: The default setting is intentionally unchecked, as the File Extensions List is long and may span many pages. If you intend to print the file, this may not be desirable.

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*.

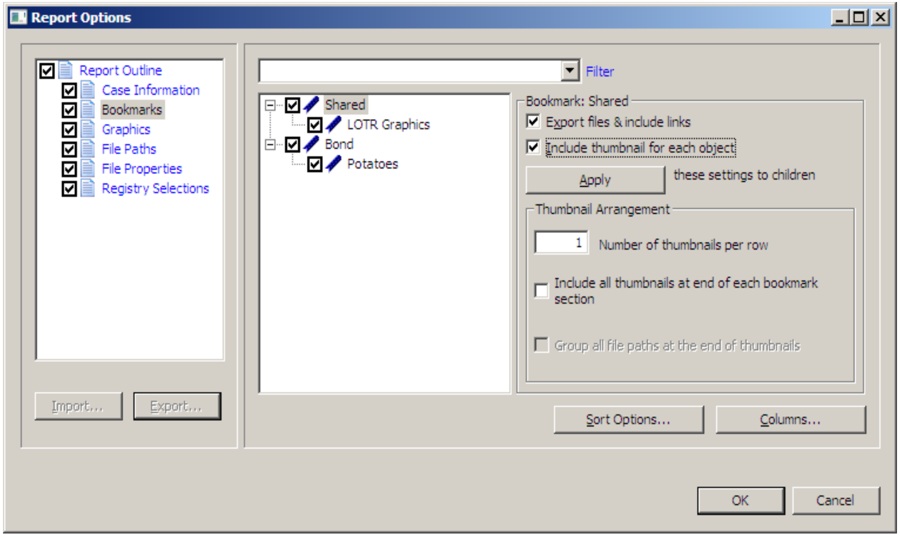
Important: Below the Case Information Pane there is a new button, *Include File Extensions.* This box is unmarked by default. If you wish to include in the report a list of file extensions such as is found in *Overview > File Extensions*, mark the Include File Extensions box. The list of file extensions will appear in the report under Case Information, after File Items and File Category, and before File Status.

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



Report Options

- ☑ Report Outline
  - ☑ Case Information
  - ☑ Bookmarks
  - ☑ Graphics
  - ☑ File Paths
  - ☑ File Properties
  - ☑ Registry Selections

- ☑ Shared
  - ☑ LOTR Graphics
- ☑ Bond
  - ☑ Potatoes

Bookmark: Shared

☑ Export files & include links

☑ Include thumbnail for each object

Thumbnail Arrangement

1 Number of thumbnails per row

□ Include all thumbnails at end of each bookmark section

□ Group all file paths at the end of thumbnails

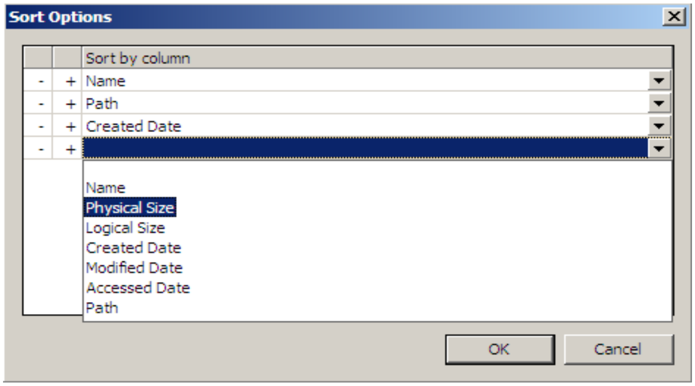
Mark the boxes to include Shared and/or User bookmarks.

- Choose whether to export the files and include links to them in the report when it is generated.
- Choose 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.



Sort Options

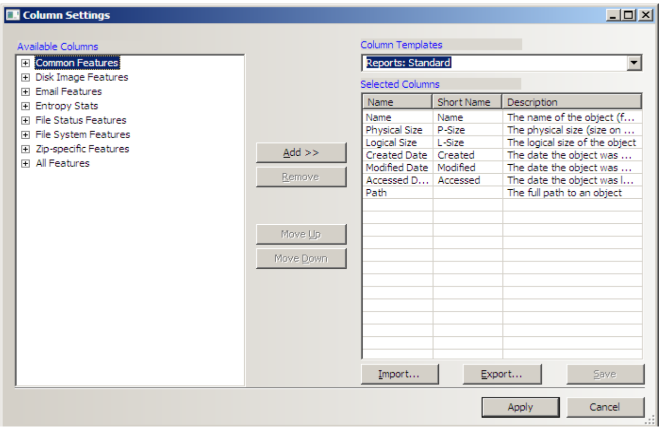
		Sort by column
-	+	Name
-	+	Path
-	+	Created Date
-	+	

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



Column Templates: Reports: Standard

Selected Columns

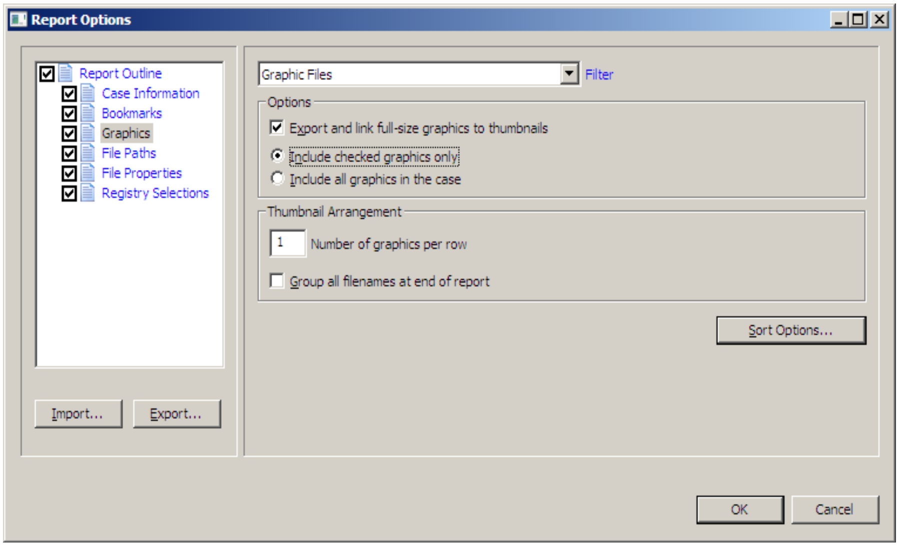
Name	Short Name	Description
Name	Name	The name of the object (f...
Physical Size	P-Size	The physical size (size on ...
Logical Size	L-Size	The logical size of the object
Created Date	Created	The date the object was ...
Modified Date	Modified	The date the object was ...
Accessed D...	Accessed	The date the object was l...
Path		The full path to an object

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 213.

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



- ☑ Report Outline
  - ☑ Case Information
  - ☑ Bookmarks
  - ☑ Graphics
  - ☑ File Paths
  - ☑ File Properties
  - ☑ Registry Selections

Graphic Files

Options

☑ Export and link full-size graphics to thumbnails

● Include checked graphics only

○ Include all graphics in the case

Thumbnail Arrangement

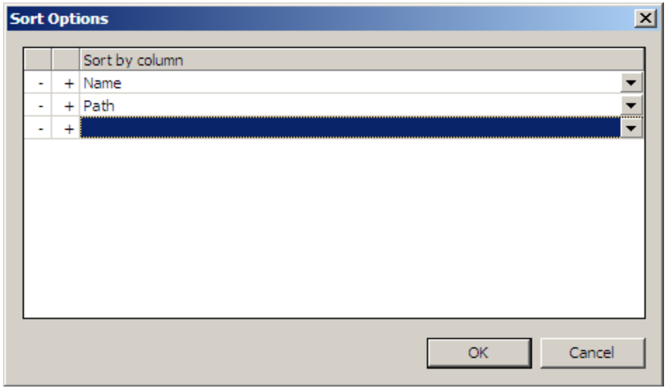
1 Number of graphics per row

□ Group all filenames at end of report

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 checked graphics only
   - Include all graphics in the case
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



Sort Options

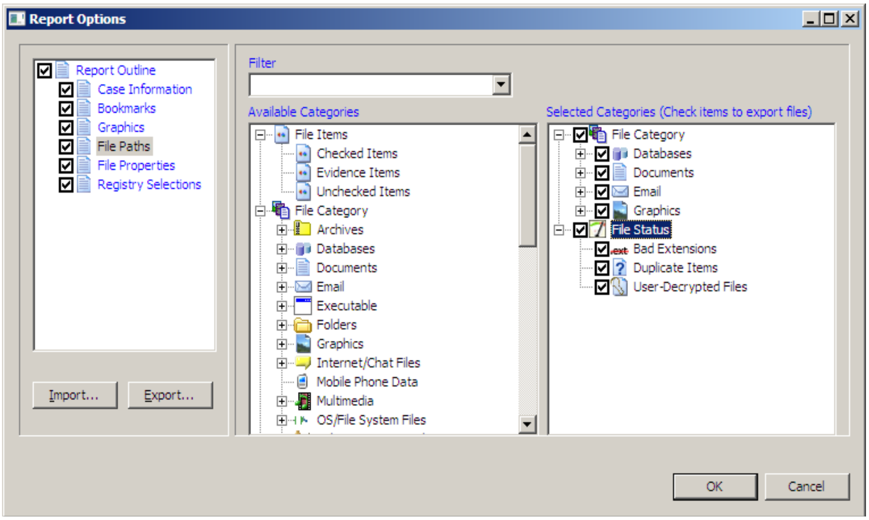
		Sort by column
-	+	Name
-	+	Path
-	+	

7. Set the desired sort options (note that only two options, Name and Path, 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

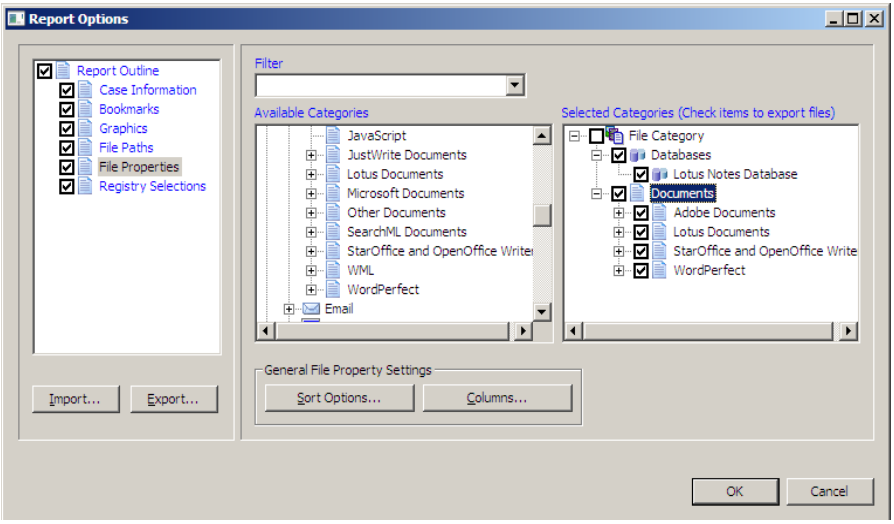


Drag and drop an item from the Available Categories pane to the *Selected Categories* pane to copy an item and its parent category. You can then check a category item to export its contents to the report. Checking a parent item automatically selects the child files and folders of that parent item.

SELECTING A FILE PROPERTIES LIST

The File Properties options allow the creation of 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* list to the *Selected Categories* list. Check items in Selected Categories to export them to the report. Checking a parent item automatically selects the child files and folders contained in the parent item.

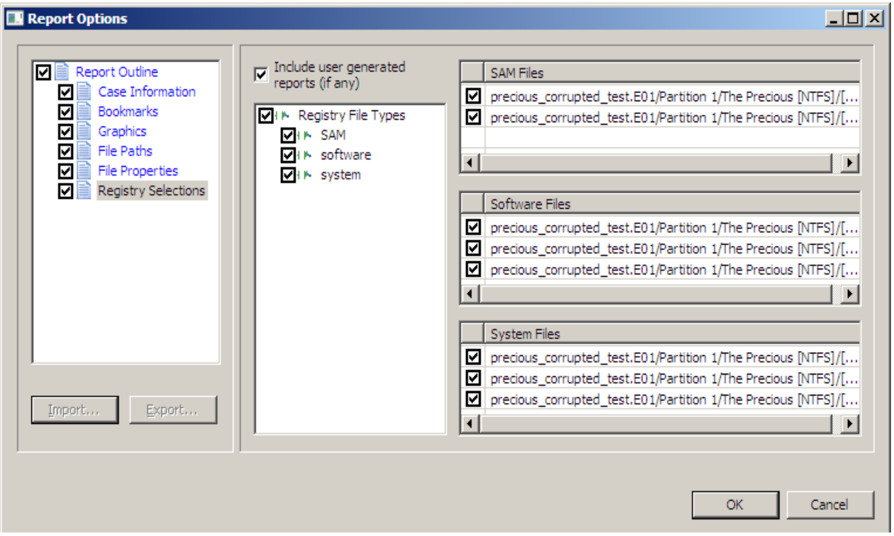
To modify the Sort Options, click *Sort Options*. For more information on modifying the Sort Options, see “Selecting Sort Options” on page 196.

To modify column settings, click *Columns*. The Column Settings dialog opens. For more information on setting columns, see “Customizing File List Columns” on page 213.

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



☑ Report Outline
- ☑ Case Information
- ☑ Bookmarks
- ☑ Graphics
- ☑ File Paths
- ☑ File Properties
- ☑ Registry Selections

☑ Include user generated reports (if any)

☑ Registry File Types
- ☑ SAM
- ☑ software
- ☑ system

SAM Files
- ☑ precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[...
- ☑ precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[...

Software Files
- ☑ precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[...
- ☑ precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[...
- ☑ precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[...

System Files
- ☑ precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[...
- ☑ precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[...
- ☑ precious_corrupted_test.E01/Partition 1/The Precious [NTFS]/[...

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

Check the *Include user generated reports (if any)* box if you have AccessData Registry Viewer reports generated and you want to create FTK report links to the Registry Viewer reports.

Checking this box without the Registry Viewer report(s) having been previously generated will create an empty link.

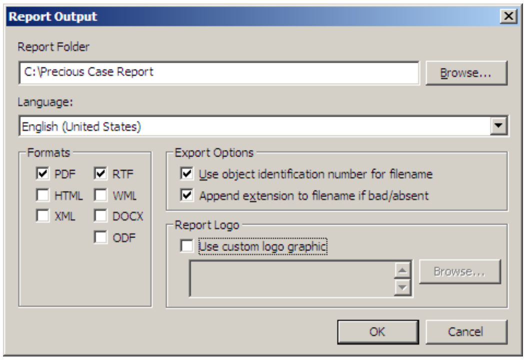
Running the Report

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, report file output type(s), and the selection of a custom logo for the HTML format report.

Figure 10-10 Report Output Dialog



Report Folder: C:\Precious Case Report

Language: English (United States)

Formats:
☑ PDF ☑ RTF
☐ HTML ☐ WML
☐ XML ☐ DOCX
☐ ODF

Export Options:
☑ Use object identification number for filename
☑ Append extension to filename if bad/absent

Report Logo:
☐ Use custom logo graphic

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(s) to generate the report to.
4. Select the Export Options for the report. These are not required. You can choose either, neither, or both. Options are:
   - Use object identification number for filename.
   - Append extension to filename if bad/absent.
5. To add a custom graphic or company logo you want to include in the HTML format of the report, mark the *Use custom logo graphic* checkbox, then browse to and select the graphic file to use. The selected custom graphic will be used in the HTML report.
6. When output selections have been made, click *OK* to begin report generation.

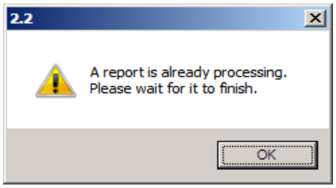
Creating the Report

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, you are prompted to wait, as in the following dialog.

Figure 10-11 A Report is Processing. Please Wait

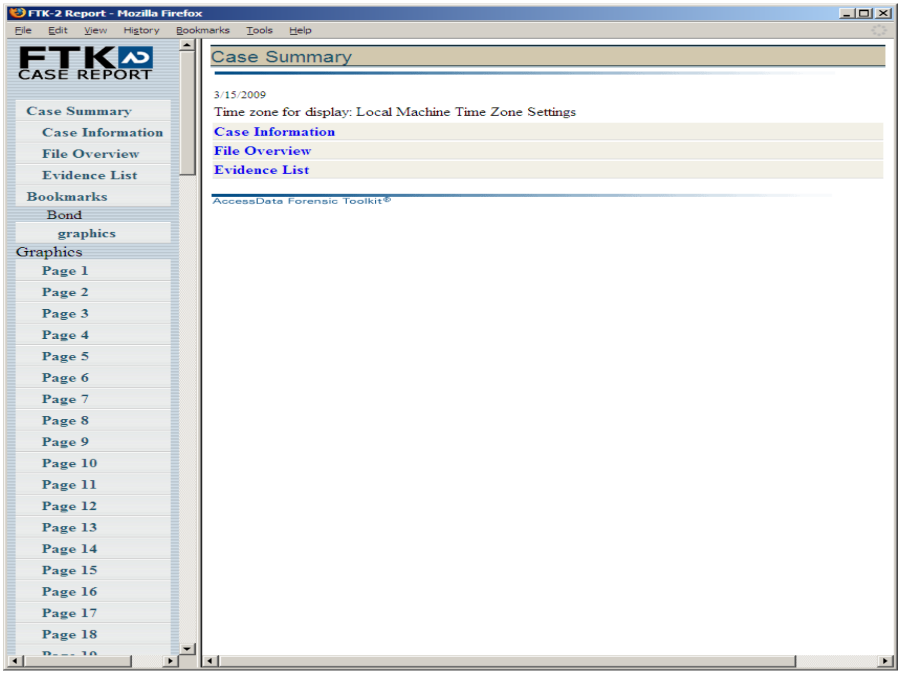


A report is already processing.
Please wait for it to finish.

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



Case Summary

3/15/2009

Time zone for display: Local Machine Time Zone Settings

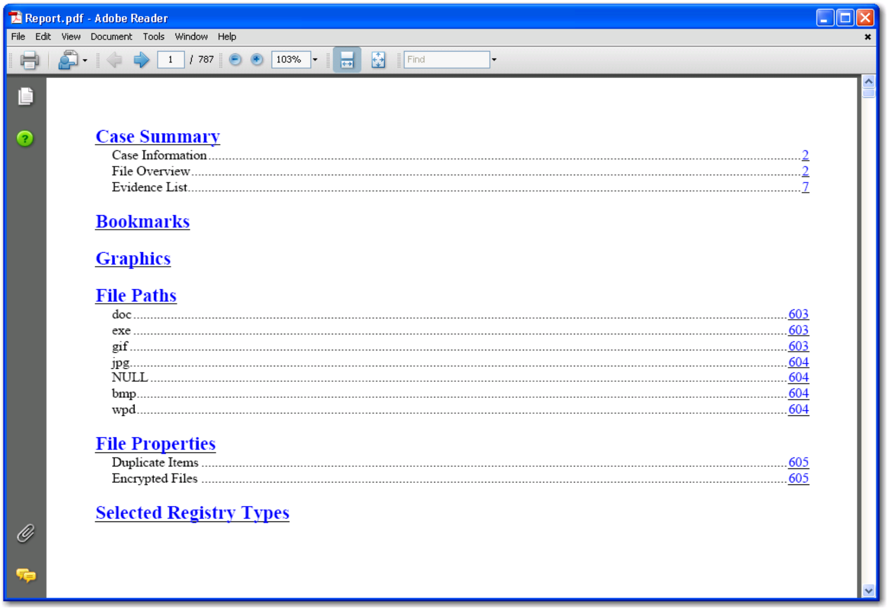
Case Information

File Overview

Evidence List

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

Figure 10-13 PDF Report


Report.pdf - Adobe Reader
File Edit View Document Tools Window Help
1 / 787
103%
Find

Case Summary

Case Information 2
File Overview 2
Evidence List 7

Bookmarks

Graphics

File Paths

doc 603
exe 603
gif 603
jpg 604
NULL 604
bmp 604
wpd 604

File Properties

Duplicate Items 605
Encrypted Files 605

Selected Registry Types

To view the report without opening it from FTK, browse to 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

When a report is generated, the date and time stamp are in the preferred format for the computer that generated the report. For example, a date 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.

Important: To avoid confusion, notify recipients of the date and time format of the computer that generated the report. There is currently no specific option to change this.

Modifying a Report

Once a report is generated, it cannot be edited or modified as you would a word-processing document. You must recreate the report with the added evidence or changed report settings to properly 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. This chapter discusses customizing 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 hovering over a border with your mouse until you see a double-arrow. Then click and drag the window to a new size.

Rearrange the order of the tabs by clicking on a tab, then dragging and dropping it in the desired order.

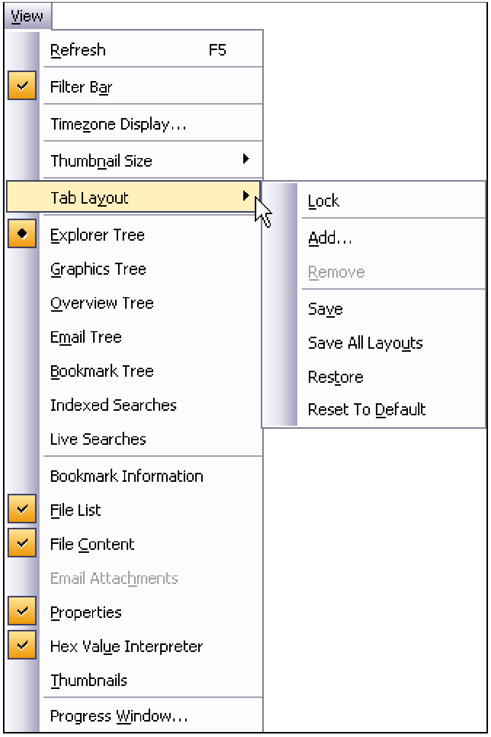
Add or remove panes from the current tab using the View menu. Click *View* and click the pane you would like to add to the current view. a check mark next to the view item means it is being displayed in the current view. Checking and re-checking toggles the setting on or off.

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:

TABLE 11-1 View Menu Options and Sub-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:
- Bookmark Tree
- Index Searches
- Live searches.
- Bookmark Information

TABLE 11-1 View Menu Options and Sub-options

•Large - default •Medium •Small •Tiny	• File List
• Customize the Tab Layout. Options are:	• File Content
•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.	• Email Attachments
• Explorer Tree	• Properties
• Graphics Tree	• Hex Value Interpreter
• Overview Tree	• Thumbnails
• Email Tree	• 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 select the pane to add. A checkmark next to a pane indicates it is included in the current view. Clicking again toggles the option off. Options are described in the table below:

TABLE 11-2 View Panes Available from the View Menu

View Pane	Description
Bookmark Information	In the Bookmark tab, select to display the Bookmark Informaiton, suhc as the bookmark's name, the creator's name, and comments, and so forth.
File List	Adds the File List Pane to the current tab.

TABLE 11-2 View Panes Available from the View Menu

View Pane	Description
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 Pane 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:

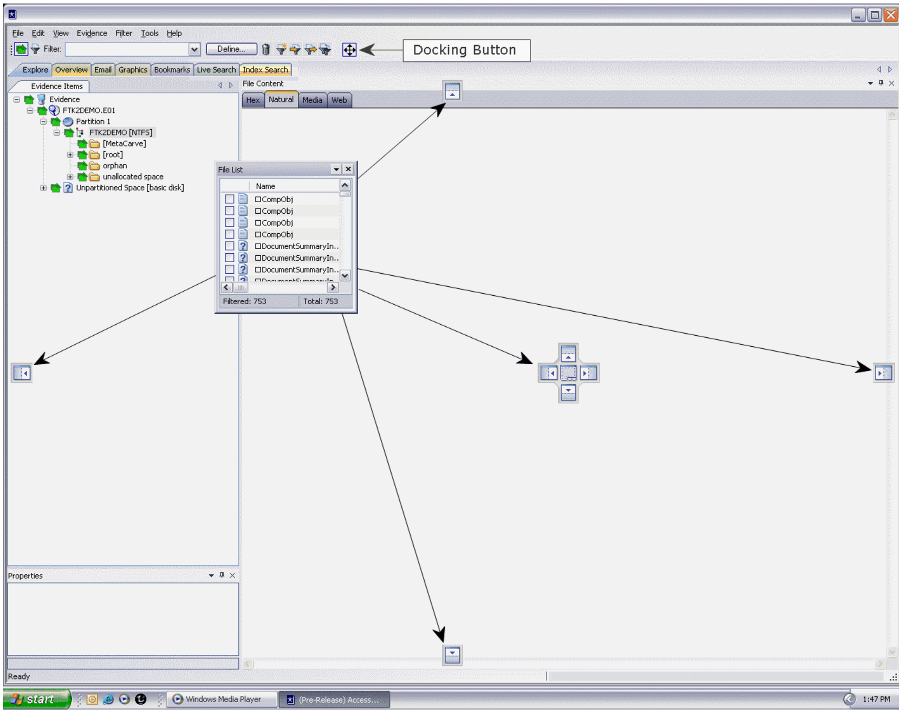
TABLE 11-3 Tab Layout Menu Options

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 copies the layout of the current active tab.
Remove	Removes the active tab from the FTK window.
Save	Saves the changes made to the active tab.
Save All Layouts	Saves the changes made to all tabs.
Restore	Restores all tabs to the settings from the last saved layout. Custom settings can be restored.
Reset to Default	Resets all tabs to the settings 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, then 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

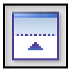
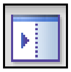
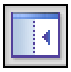
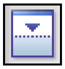
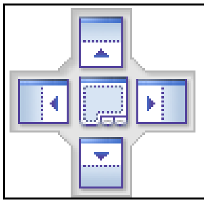
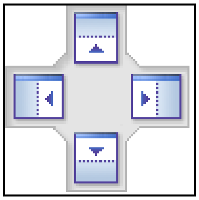
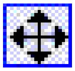


To place the view pane at a specific location in the current tab:

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 11-4 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 lower 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, making them immovable. When the lock is applied, the blue box turns grey. Toggles when clicked, from locked to unlocked, and back.

CREATING CUSTOM TABS

Create custom tabs 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 on an existing tab to use as a template for the new tab.
2. Click *View > Tab Layout > Add.*
3. Enter a name for the new tab and click *OK*. The resulting tab is a copy of the tab your were on when you created the new one.
4. From the View menu, select the features you need in your new tab.

Note: Features marked with diamonds are mutually exclusive, only one can exist on a tab at a time. Features with check marks can co-exist in more than one instance on a tab.

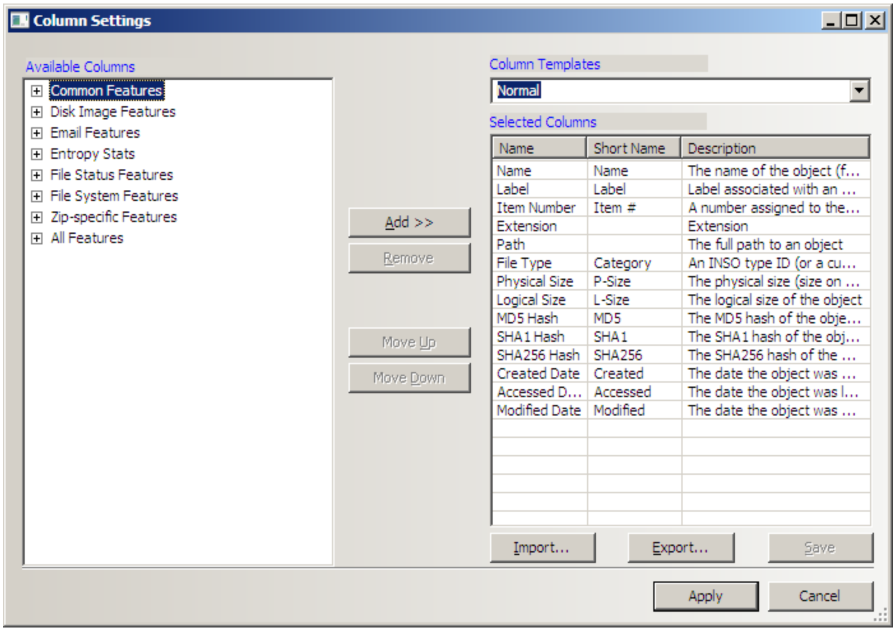
5. When satisfied with your new tab's content, click *Save* to save the current tab's settings, or *View > Tab Layout > Save.*
6. (Optional) Click *View > Tab Layout > Save All* to save all changed and added features**.**
7. To remove tabs, click *View > Tab Layout > Remove.*

CUSTOMIZING FILE LIST COLUMNS

The Column Settings dialog allows the modification of existing definitions, or the creation of new definitions for the colums that display in the File List, and the order in which they display. Column settings are also used to define what file information appears in the Bookmark and 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 Settings Options



Available Columns

- Common Features
- Disk Image Features
- Email Features
- Entropy Stats
- File Status Features
- File System Features
- Zip-specific Features
- All Features

Column Templates: Normal

Selected Columns

Name	Short Name	Description
Name	Name	The name of the object (f...
Label	Label	Label associated with an ...
Item Number	Item #	A number assigned to the...
Extension		Extension
Path		The full path to an object
File Type	Category	An INSO type ID (or a cu...
Physical Size	P-Size	The physical size (size on ...
Logical Size	L-Size	The logical size of the object
MD5 Hash	MD5	The MD5 hash of the obje...
SHA1 Hash	SHA1	The SHA1 hash of the obj...
SHA256 Hash	SHA256	The SHA256 hash of the ...
Created Date	Created	The date the object was ...
Accessed D...	Accessed	The date the object was l...
Modified Date	Modified	The date the object was ...

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 create or modify 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 which tab and which columns template is selected.

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 beginning with 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 11-5 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 on a FAT system.

TABLE 11-5 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 extension does not match its header.
Carved	Indicates whether the object is carved from another object.
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	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	Indicates whether, based on file hashes, the file is a duplicate of another file in the case. Options are blank if not a duplicate, Primary if it was the first instance of the file encountered in processing, or Secondary, if not the first instance. Any duplicate file can be elevated to Primary status, and the original Primary automatically becomes Secondary status.
Encrypted	Indicates whether the object is encrypted. Only set on files.
Extension	Displays the object's extension.
File Class	An internal enumberation describing what kind of object it is.
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	Fuzzy hash of the object's contents.
Fuzzy hash blocksize	Fuzzy hash blocksize

TABLE 11-5 Common Column Headings

Column	Description
Fuzzy hash library group	Fuzzy hash library group
Fuzzy hash library score	Fuzzy hash match score
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 11-6 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 11-7 Common Email Column Headings

Column	Description
Lotus Notes-specific features	Options include: • **Note ID**: The Lotus Notes NOTE_ID (unique to the NSF file). • **UNID**: The Lotus Notes Universal Note ID (globally unique).
Outlook Express-specific Features	See below, table titled **Microsoft Outlook Express Column Headings**
Outlook/Exchange-specific Features	See below, table titled **Microsoft Outlook/Exchange Column Headings**
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 11-8 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 (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 othewise. Only set on emails from Outleook 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 Outleook Express.
Recipient Address	Lists the addresses in the email's recipient field. Only set for Outleook Express.
Recipient Name	Lists the names in the email's recipient field. Only set for Outleook Express.
Sender Address	Lists the addresses in the email's sender field. Only set for Outleook Express.
Sender Address and Name	Lists the addresses and names in the email's sender field. Only set for Outleook Express.

TABLE 11-8 Microsoft Outlook Express Column Headings

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

MICROSOFT OUTLOOK/EXCHANGE HEADINGS

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

TABLE 11-9 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 11-9 Microsoft Outlook/Exchange Column Headings

Column	Description
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 11-10 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. 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 11-11 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.
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 that one set, the status with the height value is used. For more information, see “Chapter 8 Using Filters” on page 167.

FILE SYSTEM FEATURES

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

TABLE 11-12 File Status Column Headings

Column	Description
DOS Features	See below, in the table titled **DOS File System Column Headings**.
ext2 Features	See below, in the table titled **ext2 File System Column Headings.**
HFS Features	See below, in the table titled **HFS File System Column Headings**
NTFS Features	See below, in the table titled **NTFS File System Column Headings**
Unix Security Features	See below, in the table titled **Unix Security File System Column Headings**
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 11-13 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 11-14 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	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. There are a set number of inodes, which indicates the maximum number of files the system can hold. A file's inode number can be found using the ls -i command, while the ls -l command will retrieve other inode information.

HFS FILE SYSTEMS

These column headings list information specific to HFS.

TABLE 11-15 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 11-16 NTFS File System Column Headings

Column	Description
Alternate Date 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.
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 11-17 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 hedings list information specific to files where steganography is found:

TABLE 11-18 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 steganograpyhic payload.

Zip-Specific Features

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

TABLE 11-19 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.

Appendix A File Systems and Drive Image Formats

This appendix lists the file systems and image formats that FTK 2.2 analyzes.

File Systems

TABLE A-1 Recognized File System

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

Hard Disk Image Formats

TABLE A-2 Supported Hard Disk Image Formats

- Encase
- Safeback 2.0 and under
- Linux DD
- Ghost (forensic images only)
- AccessData Logical Image (AD1)
- SnapBack
- Expert Witness
- ICS
- SMART

CD and DVD Image Formats

TABLE A-3 Supported CD and DVD Image Formats

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

Appendix B Recovering Deleted Material

FTK 2.2 finds deleted files on supported file systems by their file header.

FAT 12, 16, AND 32

When parsing FAT directories, FTK 2.2 identifies deleted files by their names. In a deleted file, the first character of the 8.3 filename is replaced by the hex character 0xE5.

The file's directory entry provides the files's starting cluster (C) and size. From the size of the file and the starting cluster, FTK 2.2 computes the total number of clusters (N) occupied by the file.

FTK 2.2 then examines the File Allocation Table (FAT) and counts the number of unallocated clusters starting at C (U). It then assigns the recovered file [min (N, U)] clusters starting at C.

If the deleted file was fragmented, the recovered file is likely to be incorrect and incomplete because the information that is needed to find subsequent fragments was wiped from the FAT system when the file was deleted.

FTK 2.2 uses the long filename (LFN) entries, if present, to recover the first letter of the deleted file's short filename. If the LFN entries are incomplete or absent, it uses an exclamation mark ("!") as the first letter of the filename.

FTK 2.2 meta carves, or searches the volume free space for deleted directories that have been orphaned. An orphaned directory is a directory whose parent directory or whose entry in its parent directory has been overwritten.

NTFS

FTK 2.2 examines the Master File Table (MFT) to find files that are marked deleted because the allocation byte in a record header indicates a deleted file or folder. It then recovers the file's data using the MFT record's data attribute extent list if the data is non-resident.

If the deleted file's parent directory exists, the recovered file is shown in the directory where it originally existed. Deleted files whose parent directories were deleted are shown in their proper place as long as their parent directory's MFT entry has not been recycled.

EXT2

FTK 2.2 searches to find inodes that are marked deleted: the link count is zero and the deletion timestamp is nonzero.

For each deleted inode, FTK 2.2 processes the block pointers as it does for a normal file and adds blocks to the deleted file. However, if an indirect block is marked allocated or references an invalid block number, the recovered file is truncated at that point because the block no longer contains a list of blocks for the file that the application is attempting to recover.

FTK 2.2 does not recover the filenames for files deleted on ext2 systems. Instead, deleted files are identified by inode number because ext2 uses variable-length directory entries organized in a linked list structure. When a file is deleted, its directory entry is unlinked from the list, and the space it occupied becomes free to be partially or completely overwritten by new directory entries. There is no reliable way to identify and extract completely deleted directory entries.

EXT3

FTK 2.2 does not recover deleted files from ext3 volumes because ext3 zeroes out a file's indirect block pointers when it is deleted.

HFS

FTK 2.2 does not recover deleted files from HFS.

Appendix C Program Files

The following tables list key FTK 2.2 files and folders, their functions, and their locations.

FILES AND FOLDERS FOR THE APPLICATION

These files and folders exist on the computer running FTK 2.2.

TABLE C-1 FTK 2.2 Folders and File Locations

File or Folder	Location	Function
FTK2-Data (shared)	Root of system drive or partition [*drive*]:\ftk2-data\	Contains all case data not stored in the database.
summary_install_log_2.2.txt	[*drive*]:\Program Files\AccessData\Forensic Toolkit\2.2\logs\	Points to a set of log files including a summary installation log to help Technical Support with troubleshooting.
KFF Logs	[*drive*]:\Program Files\AccessData\KFF Library FTK 2.2	Records whether the Known File Filter was added to the schema.
FTK.exe	[*drive*]:\Program Files\AccessData\Forensic Toolkit\2.2\bin\	Program executable

TABLE C-1 FTK 2.2 Folders and File Locations

File or Folder	Location	Function
FTK2_log.txt	[*drive*]:\Program Files\ AccessData\ Forensic Toolkit\ 2.2\	Log file recording information specific to the application.
FTK2crash[timestamp].dmp	[*drive*]:\Program Files\AccessData\AccessData Forensic Toolkit\2. 2\	Dump file with the timestamp from an FTK crash.

FILES AND FOLDERS FOR THE DATABASE

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

TABLE C-2 Oracle Database File Locations

File or Folder	Location	Function
ftk2	[*drive*]:\Oracle	Contains files FTK 2.2 uses to work with the Oracle database, such as JRE, libraries, configuration scripts, etc.
logs	[*drive*]:\Program Files\Oracle\Inventory	Contains installation logs intended to help Technical Support with installation troubleshooting.
FTK2_KFF.DBF	[*drive*]:\Oracle\ftk2\database	Contains the hashes that make up the AccessData Known File Filter.

CHANGING REGISTRY OPTIONS

The following sections cover small changes that can be made to items in the registry to aid in the functionality and desired efficiency of FTK.

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 are read during the startup process only.

CHATTY WORKER

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

Appendix D Gathering Windows Registry Evidence

This appendix contains information about the Windows Registry and what information can be gathered for evidence.

UNDERSTANDING THE WINDOWS REGISTRY

For forensic work, registry files are particularly useful because they can contain important information such as the following:

- Usernames and passwords for programs, email, and Internet sites
- A history of Internet sites accessed, including dates and times
- A record of Internet queries (i.e., searches performed on Internet search engines like Google, Yahoo, etc.)
- Lists of recently accessed files (e.g., documents, images, etc.)
- A list of all programs installed on the system

AccessData Registry Viewer allows you to view the contents of Windows operating system registries. Unlike the standard Windows Registry Editor, which only displays the current system's registry, Registry Viewer lets you examine registry files from any system or user. Registry Viewer also provides access to a registry's protected storage, which contains passwords, usernames, and other information not accessible from within Windows Registry Editor.

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

WINDOWS 9X REGISTRY FILES

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

TABLE D-1 Windows 9x Registry files

Filename	Location	Contents
system.dat	\Windows	• Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet 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. • Lists installed programs, their settings, and any usernames and passwords associated with them. • Contains the System settings.
user.dat	\Windows If there are multiple user accounts on the system, each user has a user.dat file located in \Windows\profiles\user account	• 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. • User preference settings (desktop configuration, etc.).

Windows NT and Windows 2000 Registry Files

The following table describes each item in the Windows NT and Windows 2000 registry files:

TABLE D-2 Windows NT and Windows 2000 Registry Files

Filename	Location	Contents
NTUSER.DAT	\Documents and Settings\[*user account*] If there are multiple user accounts on the system, each user has an ntuser.dat file.	• Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet 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. • All installed programs, their settings, and any usernames and passwords associated with them. • User preference settings (desktop configuration, etc.)
default	\Winnt\system32\config	System settings
SAM	\Winnt\system32\config	User account management and security settings
SECURITY	\Winnt\system32\config	Security settings
software	\Winnt\system32\config	All installed programs, their settings, and any usernames and passwords associated with them
system	\Winnt\system32\config	System settings

WINDOWS XP REGISTRY FILES

The following table describes each item in the Windows XP registry files:

TABLE D-3 Windows XP Registry Files

Filename	Location	Contents
NTUSER.DAT	\Documents and Settings\[*user account*] If there are multiple user accounts on the system, each user has an ntuser.dat file.	• Protected storage for all users on the system. Protected Storage is an access-restricted area of the registry that stores confidential user information including usernames and passwords for Internet 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. • All installed programs, their settings, and any usernames and passwords associated with them. • User preference settings (desktop configuration, etc.)
default	\Winnt\system32\config	System settings
SAM	\Winnt\system32\config	User account management and security settings
SECURITY	\Winnt\system32\config	Security settings
software	\Winnt\system32\config	All installed programs, their settings, and any usernames and passwords associated with them
system	\Winnt\system32\config	System settings

The logical registry is organized into the following tree structure:

The top level of the tree is divided into hives. A hive is a discrete body of keys, subkeys, and values that is rooted at the top of the registry hierarchy. On Windows XP systems, the registry hives are as follows:

- HKEY_CLASSES_ROOT (HKCR)
- HKEY_CURRENT_USER (HKCU)

- HKEY_LOCAL_MACHINE (HKLM)
- HKEY_USERS (HKU)
- HKEY_CURRENT_CONFIG (HKCC)
- HKEY_DYN_DATA (HKDD)

HKEY_LOCAL_MACHINE and HKEY_USERS are the root hives. They contain information that is used to create the HKEY_CLASSES_ROOT, HKEY_CURRENT_USER, and HKEY_CURRENT_CONFIG hives.

HKEY_LOCAL_MACHINE is generated at startup from the system.dat file and contains all the configuration information for the local machine. For example, it might have one configuration if the computer is docked, and another if the computer is not docked. Based on the computer state at startup, the information in HKEY_LOCAL_MACHINE is used to generate HKEY_CURRENT_CONFIG and HKEY_CLASSES_ROOT.

HKEY_USERS is generated at startup from the system User.dat files and contains information for every user on the system.

Based on who logs in to the system, the information in HKEY_USERS is used to generate HKEY_CURRENT_USER, HKEY_CURRENT_CONFIG, and HKEY_CLASSES_ROOT.

Keys and sub-keys are used to divide the registry tree into logical units off the root.

When you select a key, Registry Editor displays the key's values; that is, the information associated with that key. Each value has a name and a data type, followed by a representation of the value's data. The data type tells you what kind of data the value contains as well as how it is represented. For example, values of the REG_BINARY type contain raw binary data and are displayed in hexadecimal format.

POSSIBLE DATA TYPES

The following table lists the Registry's possible data types:

TABLE D-4 Possible Data Types

Data Type	Name	Description
REG_BINARY	Binary Value	Raw binary data. Most hardware component information is stored as binary data and is displayed in hexadecimal format.
REG_DWORD	DWORD Value	Data represented by a number that is 4 bytes long (a 32-bit integer). Many parameters for device drivers and services are this type and are displayed in binary, hexadecimal, or decimal format. Related values are REG_DWORD_LITTLE_ENDIAN (least significant byte is at the lowest address) and REG_DWORD_BIG_ENDIAN (least significant byte is at the highest address).
REG_EXPAND_SZ	Expandable String Value	A variable-length data string. This data type includes variables that are resolved when a program or service uses the data.
REG_MULTI_SZ	Multi-String Value	A multiple string. Values that contain lists or multiple values in a format that people can read are usually this type. Entries are separated by spaces, commas, or other marks.
REG_SZ	String Value	A text string of any length.
REG_RESOURCE_LIST	Binary Value	A series of nested arrays designed to store a resource list used by a hardware device driver or one of the physical devices it controls. This data is detected by the system and is displayed in hexadecimal format as a Binary Value.
REG_RESOURCE_REQUIREMENTS_LIST	Binary Value	A series of nested arrays designed to store a device driver's list of possible hardware resources that it, or one of the physical devices it controls, can use. This data is detected by the system and is displayed in hexadecimal format as a Binary Value.
REG_FULL_RESOURCE_DESCRIPTOR	Binary Value	A series of nested arrays deigned to store a resource list used by a physical hardware device. This data is displayed in hexadecimal format as a Binary Value.

TABLE D-4 Possible Data Types

Data Type	Name	Description
REG_NONE	None	Data with no particular type. This data is written to the registry by the system or applications and is displayed in hexadecimal format as a Binary Value.
REG_LINK	Link	A Unicode string naming a symbolic link.
REG_QWORD	QWORD Value	Data represented by a number that is a 64-bit integer.

ADDITIONAL CONSIDERATIONS

If there are multiple users on a single machine, you must be aware of the following issues when conducting a forensic investigation:

- If there are individual profiles for each user on the system, you need to locate the USER.DAT file for the suspect(s).
- If all the users on the system are using the same profile, everyone's information is stored in the same USER.DAT file. Therefore, you will have to find other corroborating evidence because you cannot associate evidence in the USER.DAT file with a specific user profile.
- On Windows 9*x* systems, the USER.DAT file for the default user is used to create the USER.DAT files for new user profiles. Consequently, the USER.DAT files for new profiles can inherit a lot of junk.

To access the Windows registry from an image of the suspect's drive, you can do any of the following:

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

  Note: The problem with this method is that you can only view the registry as text. Registry Editor displays everything in ASCII so you can't see hex or binary values in the registry.
- Use Registry Viewer. Registry Viewer integrates seamlessly with FTK 2.2 to display registry files within the image and create reports.

Important: Registry Viewer shows everything you normally see in live systems using the Windows Registry Editor. However, unlike Registry Editor and other tools that use the Windows API, Registry Viewer decrypts protected storage information so it displays values in the Protected Storage System Provider key (PSSP). Registry Viewer also shows information that is normally hidden in null-terminated keys.

SEIZING WINDOWS SYSTEMS

Information stored in the registry—Internet Messenger sessions, Microsoft Office MRU lists, usernames and passwords for Internet Web sites accessed through Internet Explorer, and so forth—are temporarily stored in HKEY_CURRENT_USER. When the user closes an application or logs out, the hive's cached information is pulled out of memory and written to the user's corresponding USER.DAT.

Note: Passwords and MRU lists are not saved unless these options are enabled.

Important: Because normal seizure procedures require that there be no alteration of the suspect's computer in any way, you must be able to articulate why you closed any active applications before pulling the plug on the suspect's computer. Sometimes it is better to simply pull the plug on the computer; other times, it makes more sense to image the computer in place while it is on. It may depend on what is the most important type of data expected to be found on the computer.

For example, Windows updates some program information in the registry when the changes are made. Other information is not updated until a program is closed. Also, if the computer's drive is encrypted and you cannot decrypt it or don't have the Key or password, you may have no choice except to image the live drive.

The Registry Quick Find Chart gives more information.

REGISTRY QUICK FIND CHART

The following charts discuss common locations where you can find data of forensic interest in the Windows Registry.

System Information

TABLE D-5 System Information From HKLM

Information	File or Key	Location	Description
Registered Owner	Software	Microsoft\Windows NT\CurrentVersion	This information is entered during installation, but can be modified later.
Registered Organization	Software	Microsoft\Windows NT\CurrentVersion	This information is entered during installation, but can be modified later.
Run	Software	Microsoft\Windows\CurrentVersion\Run	Programs that appear in this key run automatically when the system boots.
Logon Banner Message	Software	Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeText	This is a banner that users must click through to log on to a system.
Mounted Devices	System	MountedDevices	Database of current and prior mounted devices that received a drive letter.
Current Control Set	System	Select	Identifies which control set is current.
Shutdown Time	System	ControlSetXXX\Control\Windows	System shutdown time.
Event Logs	System	ControlSetXXX\Services\Eventlog	Location of Event logs.
Dynamic Disk	System	ControlSetXXX\Services\DMIO\Boot Info\Primary Disk Group	Identifies the most recent dynamic disk mounted in the system.
Pagefile	System	ControlSetXXX\Control\Session Manager\Memory Management	Location, size, set to wipe, etc.
Last User Logged In	Software	Microsoft\Windows NT\CurrentVersion\Winlogon	Last user logged in - can be a local or domain account.
Product ID	Software	Microsoft\Windows NT\CurrentVersion	
O\S Version	Software	Microsoft\Windows NT\CurrentVersion	
Logon Banner Title	Software	Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	User-defined data.
Logon Banner Message	Software	Microsoft\Windows\CurrentVersion\Policies\System\LegalNoticeCaption	User-defined data.
Time Zone	System	ControlSet001(or002)\Control\TimeZoneInformation\StandardName	This information is entered during installation, but can be modified later.

NETWORKING

TABLE D-6 Registry Networking Information

Information	File or Key	Location	Description
Map Network Drive MRU	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\Map Network Drive MRU	Most recently used list of mapped network drives.
TCP\IP data	System	ControlSetXXX\Services\TCPIP\Parameters	Domain, hostname data.
TCP\IP Settings of a Network Adapter	System	ControlSetXXX\Services\adapter\Parameters\TCPIP	IP address, gateway information.
Default Printer	NTUSER.DAT	Software\Microsoft\Windows NT\CurrentVersion\Windows	Current default printer.
Default Printer	NTUSER.DAT	\printers	Current default printer.
Local Users	SAM	Domains\Account\Users\Names	Local account security identifiers.
Local Groups	SAM	Domains\Builtin\Aliases\Names	Local account security identifiers.
Profile list	Software	Microsoft\Windows NT\CurrentVersion\ProfileList	Contains user security identifiers (only users with profile on the system).
Network Map	NTUSER.DAT	Documents and Settings\username	Browser history and last-viewed lists attributed to the user.

USER DATA

TABLE D-7 Registry User Data Information

Information	File or Key	Location	Description
Run	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Run	Programs that appear in this key run automatically when the user logs on.
Media Player Recent List	NTUSER.DAT	Software\Microsoft\Media Player\Player\ RecentFileList	This key contains the user's most recently used list for Windows Media Player.
O\S Recent Docs	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs	MRU list pointing to shortcuts located in the recent directory.

TABLE D-7 Registry User Data Information

Information	File or Key	Location	Description
Run MRU	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU	MRU list of commands entered in the "run" box.
Open And Save As Dialog Boxes MRU	NTUSER.DAT	\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32	MRU lists of programs\files opened with or saved with the "open" or "save as" dialog box(es).
Current Theme	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Themes	Desktop theme\wallpaper.
Last Theme	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Themes\Last Theme	Desktop theme\wallpaper.
File Extensions\Program Association	NTUSER.DAT	Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts	Identifies associated programs with file extensions.

USER APPLICATION DATA

TABLE D-8 Registry User Application Data Information

Information	File or Key	Location	Description
Word User Info	NTUSER.DAT	Software\Microsoft\office\version\Common\UserInfo	This information is entered during installation, but can be modified later.
Word Recent Docs	NTUSER.DAT	Software\Microsoft\office\version\Common\Data	Microsoft word recent documents.
IE Typed URLs	NTUSER.DAT	Software\Microsoft\Internet Explorer\TypedURLs	Data entered into the URL address bar.
IE Auto- Complete Passwords	NTUSER.DAT	\Software\Microsoft\Internet Explorer\IntelliForms	Web page auto complete password-encrypted values.
IE Auto-Complete Web Addresses	NTUSER.DAT	\Software\Microsoft\Protected Storage System Provider	Lists Web pages where auto complete was used.
IE Default Download Directory	NTUSER.DAT	Software\Microsoft\Internet Explorer	Default download directory when utilizing Internet Explorer.
Outlook Temporary Attachment Directory	NTUSER.DAT	Software\Microsoft\office\version\Outlook\Security	Location where attachments are stored when opened from Outlook.

TABLE D-8 Registry User Application Data Information

Information	File or Key	Location	Description
AIM	NTUSER.DAT	Software\America Online\AOL Instant Messenger\ CurrentVersion\Users\username	IM contacts, file transfer information, etc.
Word User Info	NTUSER.DAT	Software\Microsoft\office\ version\Common\UserInfo	This information is entered during installation, but can be modified later.
ICQ	NTUSER.DAT	\Software\Mirabilis\ICQ\*	IM contacts, file transfer information, etc.
MSN Messenger	NTUSER.DAT	Software\Microsoft\MSN Messenger\ListCache\.NET MessngerService*	IM contacts, file transfer information, etc.
Kazaa	NTUSER.DAT	Software\Kazaa\*	Configuration, search, download, IM data, etc.
Yahoo	NTUSER.DAT	Software\Yahoo\Pager\ Profiles*	IM contacts, file transfer information, etc.
Google Client History	NTUSER.DAT	Software\Google\NavClient\ 1.1\History	
Adobe	NTUSER.DAT	Software\Adobe\*	Acrobat, Photo deluxe, etc.

Appendix E Troubleshooting

FTK 2.2 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 Knowledge Base.

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 *Knowledge Base*
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 or 801-377-5410. For complete AccessData contact information, see "Appendix G AccessData Corporate Contact Information" on page 307.

TROUBLESHOOTING TABLES

The following table provides limited, basic information for troubleshooting FTK 2.2.

TABLE E-1 FTK 2.2 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 *View* > *Refresh* to manually update the view.
The installer cannot connect to your Oracle database. **Note:** When you change the name or domain affiliation of the Oracle host, the Oracle instance on that host will not work.	Check to see if the Oracle host has been changed. Test connectivity at port 1521. Verify that the SYS password is entered correctly. Changing the Host name or Domain affiliation causes the FTK2.exe 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. Log in to the host running Oracle. Stop the listener control program by entering "lsnrctl stop" at a command prompt. From a text editor, open the file: c:\Oracle\ftk2\NETWORK\ADMIN\listener.ora. 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)) Save the change and exit the text editor. Restart the listener service by entering "lsnrctl start" at a command prompt.

TABLE E-1 FTK 2.2 Troubleshooting

Problem	Suggested Resolution
The file names listed in the 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 FTK 2.2 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 2.2 using an NLS license. Error message reads: "No more user licenses are available."	FTK 2.2 is looking on the local CmStick for a license. To correct the problem, remove the local CmStick. Launch FTK 2.2, and locate the NLS server. Reattach the local CmStick to allow other applications to access it.

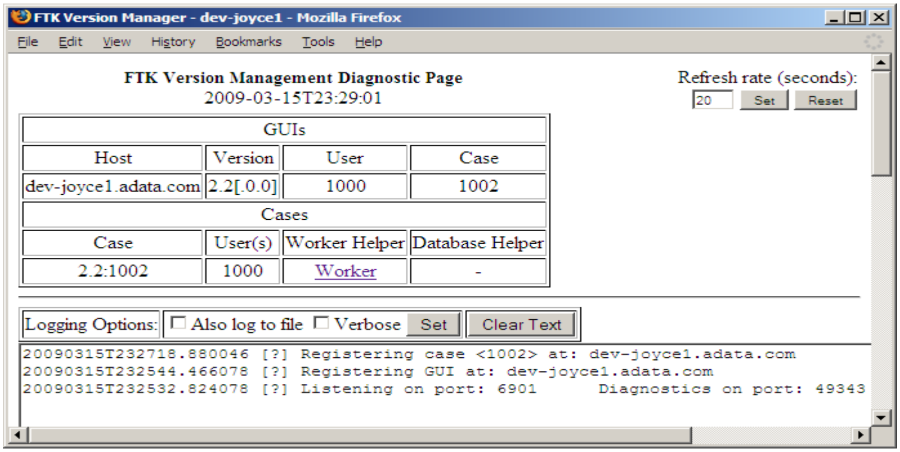
DIAGNOSTICS TOOLS

FTK provides a Diagnostics tool to help troubleshoot problems with evidence processing. It 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.



FTK Version Management Diagnostic Page
2009-03-15T23:29:01

Refresh rate (seconds): 20 Set Reset

GUIs			
Host	Version	User	Case
dev-joyce1.adata.com	2.2[.0.0]	1000	1002
Cases			
Case	User(s)	Worker Helper	Database Helper
2.2:1002	1000	Worker	-

Logging Options: □ Also log to file □ Verbose Set Clear Text

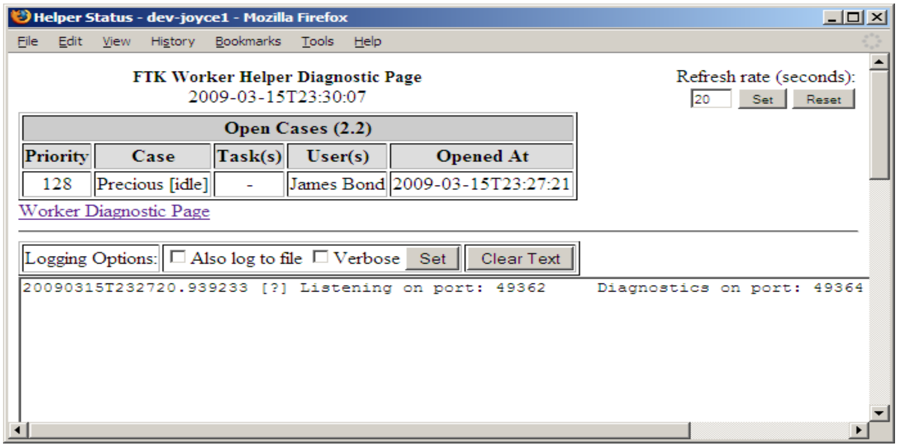
```
20090315T232718.880046 [?] Registering case <1002> at: dev-joyce1.adata.com
20090315T232544.466078 [?] Registering GUI at: dev-joyce1.adata.com
20090315T232532.824078 [?] Listening on port: 6901      Diagnostics on port: 49343
```

2. The FTK Version Management Diagnostics page opens. The page displays the following information:

TABLE E-2 FTK Version Management Diagnostic Page

Information Category and Related Data
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
Cases Information
• Case Number(s) • User GUID logged in to work on that case • Worker Helper Link • Database Helper Link
Logging options
Time and date at which the case was opened, in the following format: MM/DD/YYYY Hours:Minutes:DecimalSeconds AM/PM +/- UTC.

3. Click the Worker link. The Worker Helper Diagnostics Page opens.



FTK Worker Helper Diagnostic Page
2009-03-15T23:30:07

Refresh rate (seconds): 20 Set Reset

Open Cases (2.2)				
Priority	Case	Task(s)	User(s)	Opened At
128	Precious [idle]	-	James Bond	2009-03-15T23:27:21

Worker Diagnostic Page

Logging Options: □ Also log to file □ Verbose Set Clear Text

```
20090315T232720.939233 [?] Listening on port: 49362     Diagnostics on port: 49364
```

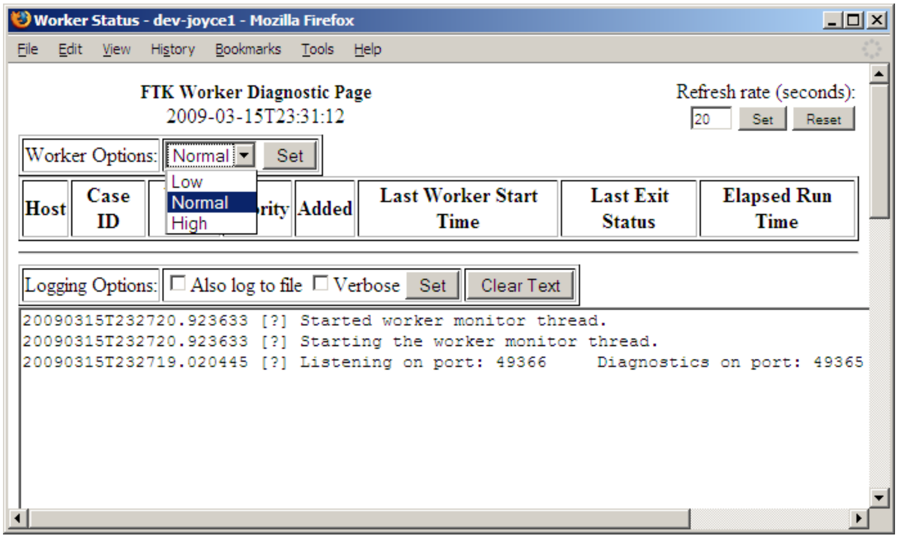
The page displays the following information:

TABLE E-3 FTK Worker Helper Diagnostic Page Information

Information Category and Related Data	
Page Title	
Time and Date in UTC	
Refresh Rate.	
Open cases for this version of FTK.	
• Case Priority • Case Name • Current Task(s)	• User(s) assigned to this case • Date and Time case was opened • Logging Options: •**Also log to file** •**Verbose** •**Set** •**Clear Text** •**Log Entries**

Click the Worker Diagnostic Page to see more information specific to the current worker.

Figure E-1 FTK Worker Diagnostic Page


Worker Status - dev-joyce1 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Set
Reset
Set
Low
Normal
High
Set
Clear Text

FTK Worker Diagnostic Page
2009-03-15T23:31:12

Refresh rate (seconds): 20

Worker Options: Normal

Host	Case ID	rity	Added	Last Worker Start Time	Last Exit Status	Elapsed Run Time

Logging Options: □ Also log to file □ Verbose

```
20090315T232720.923633 [?] Started worker monitor thread.
20090315T232720.923633 [?] Starting the worker monitor thread.
20090315T232719.020445 [?] Listening on port: 49366     Diagnostics on port: 49365
```

The FTK Worker Diagnostic Page appears. The following information is displayed:

TABLE E-4

Information Category and Related Data
Date and Time in UTC
Refresh Rate
Worker Options
• Low, Normal, or High Priority / Set • Host • Case ID • Case PriorityAdded • Last Worker Start Time • Last Exit Status • Elapsed Run Time
Logging Options
• Also log to file • Verbose • Set • Clear Text
Logged data

UNINSTALLING FTK 2.2 AND THE ORACLE DATABASE

If for any reason you need to uninstall FTK, and in particular in the case of a failed FTK 2.2 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.

AUTOMATED UNINSTALL

Try uninstalling in Add or Remove Programs in the Windows Control Panel. If for any reason this process fails, move contact AccessData Support, or refer to the instructions for Manually Uninstalling the Database on our website, www.accessdata.com/support.

Appendix F Managing Security Devices and Licenses

This chapter acquaints you with the managing AccessData product licenses. Here you will find details regarding the LicenseManager interface and how to manage licenses and update products using LicenseManager.

NLS Support

Beginning with the PRTK 6.4 and DNA 3.4 release, AccessData's Network License Service (NLS)is supported. If you have NLS, you should also have documentation on how to install and implement it.

Installing and Managing Security Devices

Before you can manage licenses with LicenseManager, you must install the proper security device software and/or drivers. This section explains installing and using the Wibu CodeMeter Runtime software and USB CmStick, as well as the Keylok USB dongle drivers and dongle device.

Installing the Security Device

As discussed previously, AccessData products require a licensing security device that communicates with the program to verify the existence of a current license. The device can be the older Keylok dongle, or the newer Wibu CmStick. Both are USB devices, and both require specific software to be installed prior to connecting the devices and running your AccessData products. You will need:

- The Wibu CodeMeter Runtime software with a Wibu CodeMeter (CmStick)
- The Wibu CodeMeter Runtime software, and the AccessData Dongle Drivers with a Keylok dongle

  Note: The Codemeter Runtime software and either a silver Wibu CmStick or a green Keylok dongle are required to run PRTK or DNA. Without them, you can run PRTK or DNA in Demo mode only.

The CmStick or dongle should be stored in a secure location when not in use.

You can install PRTK and the CodeMeter software from the shipping CD or from downloadable files available on the AccessData website at www.accessdata.com. Click *Support* > *Downloads*, and browse to the product to download. Click the download link and save the file locally prior to running the installation files.

For solutions to commonly asked installation questions, see "Chapter 11 Troubleshooting" on page 189.

Installing the CodeMeter Runtime Software

When you purchase the full PRTK package, AccessData provides a USB CmStick with the product package. The green Keylok dongles are no longer provided, but can be purchased separately through your AccessData Sales Representative.

To use the CmStick, you must first install the CodeMeter Runtime software, either from the shipping CD, or from the setup file downloaded from the AccessData Web site.

Locating the Setup File

To install the CodeMeter Runtime software from the CD, you can browse to the setup file, or select it from the Autorun menu.

To download the CodeMeter Runtime software, go to www.accessdata.com and do the following:

1. Click *Support* > *Downloads.*
2. Find

   2a. CodeMeter Runtime 3.30a (32 bit)

   MD5: 9F299EC832152E593D9E8D76F199C723

(MD5 hash applies only to this version)

OR

2b. CodeMeter Runtime 3.30a (64 bit)

MD5: 1140085cbbd0f15ade393f632b56d00c

(MD5 hash applies only to this version)

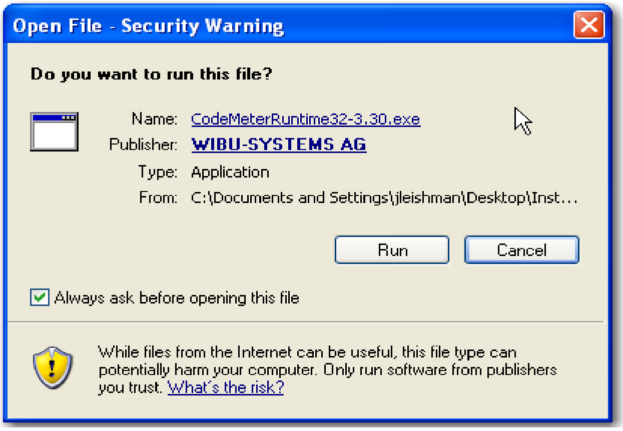
3. Click the *Download* link.
4. Save the file to your PC and run after the download is complete.

When the download is complete, double-click on the CodeMeterRuntime32-3.30.exe or the CodeMeterRuntime64-3.30.exe.

Running the CodeMeter Runtime Setup

Whichever way you choose to access the CodeMeter Runtime setup file, when you run it you will see the following:

1. The CodeMeter Runtime Open File Security Warning will appear to allow you to verify that you really want to open this file.



Open File - Security Warning

Do you want to run this file?

Name: CodeMeterRuntime32-3.30.exe

Publisher: WIBU-SYSTEMS AG

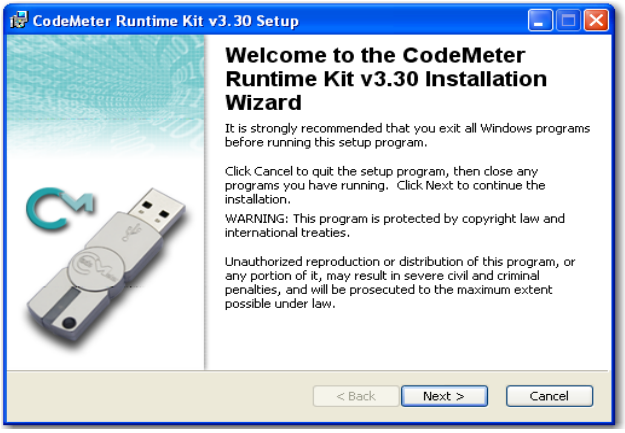
Type: Application

From: C:\Documents and Settings\jleishman\Desktop\Inst...

☑ Always ask before opening this file

While files from the Internet can be useful, this file type can potentially harm your computer. Only run software from publishers you trust. What's the risk?

2. Click *Run*.



Welcome to the CodeMeter Runtime Kit v3.30 Installation Wizard

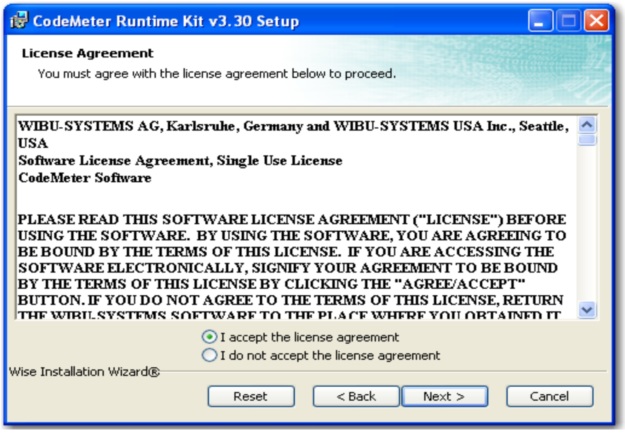
It is strongly recommended that you exit all Windows programs before running this setup program.

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

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

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

3. On the Welcome screen, click *Next*.



License Agreement

You must agree with the license agreement below to proceed.

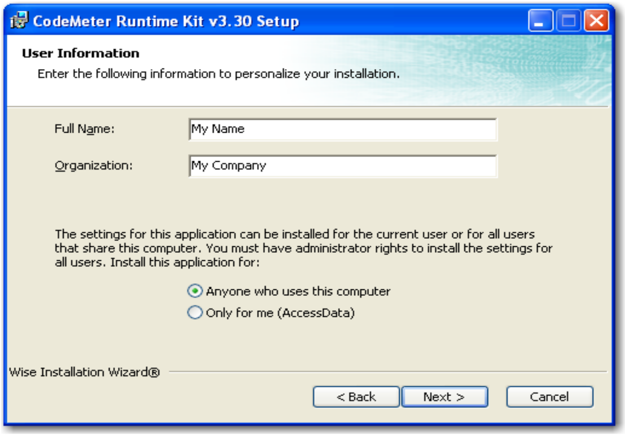
WIBU-SYSTEMS AG, Karlsruhe, Germany and WIBU-SYSTEMS USA Inc., Seattle, USA
Software License Agreement, Single Use License
CodeMeter Software

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") BEFORE USING THE SOFTWARE. BY USING THE SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. IF YOU ARE ACCESSING THE SOFTWARE ELECTRONICALLY, SIGNIFY YOUR AGREEMENT TO BE BOUND BY THE TERMS OF THIS LICENSE BY CLICKING THE "AGREE/ACCEPT" BUTTON. IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, RETURN THE WIBU-SYSTEMS SOFTWARE TO THE PLACE WHERE YOU OBTAINED IT

● I accept the license agreement
○ I do not accept the license agreement

4. Accept the License Agreement.

5. Click *Next*.



CodeMeter Runtime Kit v3.30 Setup

User Information

Enter the following information to personalize your installation.

Full Name: My Name

Organization: My Company

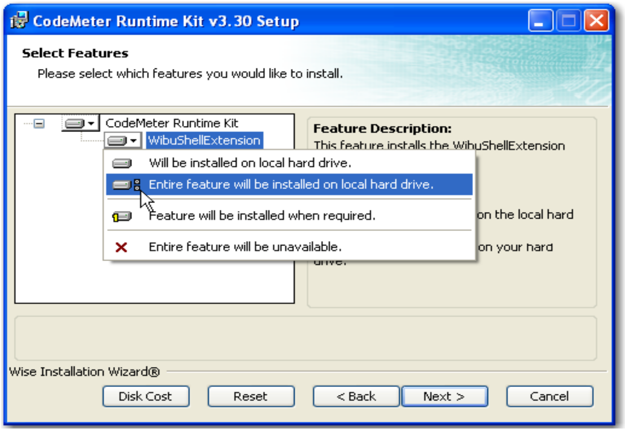
The settings for this application can be installed for the current user or for all users that share this computer. You must have administrator rights to install the settings for all users. Install this application for:

● Anyone who uses this computer
○ Only for me (AccessData)

6. In the User Information screen, enter your name and your company name.

7. Specify whether this application should be available only when you log in, or for anyone who uses this computer.

8. Click *Next*.



CodeMeter Runtime Kit v3.30 Setup

Select Features

Please select which features you would like to install.

CodeMeter Runtime Kit
WibuShellExtension

Will be installed on local hard drive.
Entire feature will be installed on local hard drive.
Feature will be installed when required.
✕ Entire feature will be unavailable.

Feature Description:

This feature installs the WibuShellExtension

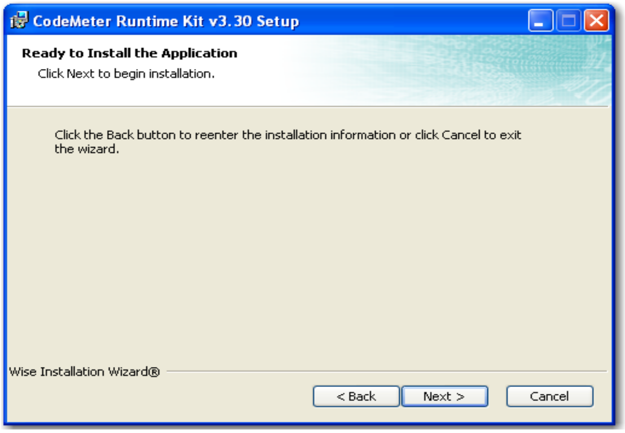
on the local hard

on your hard

drive.

9. Select the features you want to install.

10. Click *Next.*



CodeMeter Runtime Kit v3.30 Setup

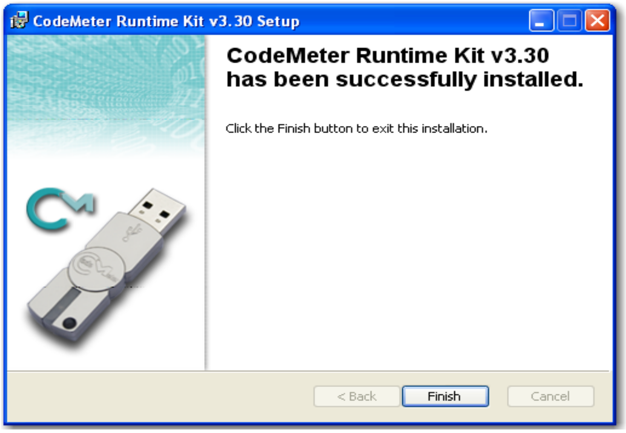
Ready to Install the Application

Click Next to begin installation.

Click the Back button to reenter the installation information or click Cancel to exit the wizard.

Wise Installation Wizard®

11. When you are satisfied with the options you have selected, click *Next.*



CodeMeter Runtime Kit v3.30 Setup

CodeMeter Runtime Kit v3.30 has been successfully installed.

Click the Finish button to exit this installation.

12. Installation will run its course. When complete, you will see the "CodeMeter Runtime Kit v3.30 has been successfully installed" screen. Click *Finish* to exit the installation.

The CodeMeter Control Center

When the CodeMeter Runtime installation is complete, the CodeMeter Control Center pops up. This is a great time to connect the CmStick and verify that the device is recognized and is Enabled. Once verified, you can close the control center and run your AccessData product(s).

For the most part there is nothing you need to do with this control center, and you need make no changes using this tool with very few exceptions. If you have problems with your CmStick, contact AccessData Support and an agent will walk you through any troubleshooting steps that may need to be performed.

INSTALLING KEYLOK DONGLE DRIVERS

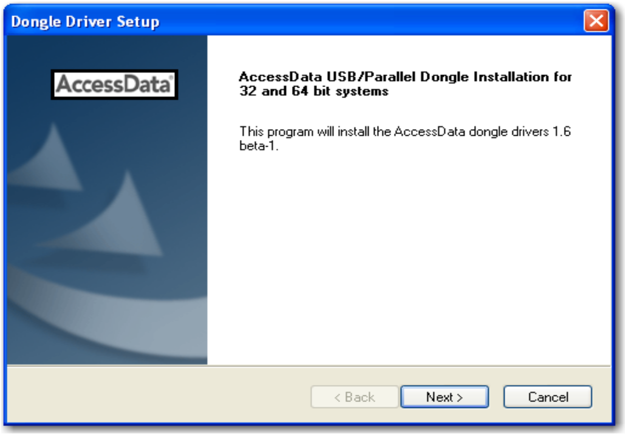
To install the Keylok USB dongle drivers do the following:

1. If installing from CD, insert the CD into the CD-ROM drive and click *Install the Dongle Drivers*.

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

   OR

1. If installing from a file downloaded from the AccessData Web site, locate the Dongle_driver_1.6.exe setup file, and double-click it.

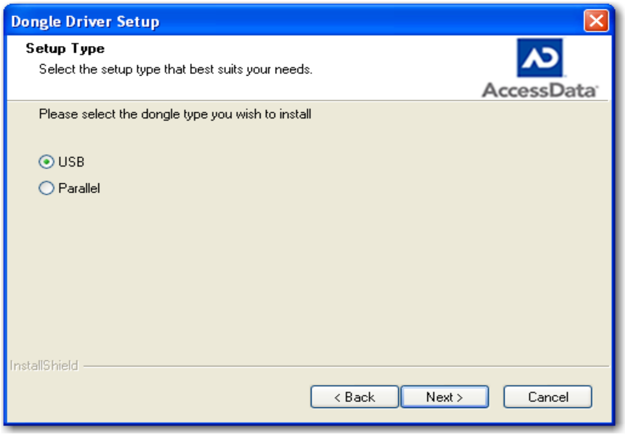


Dongle Driver Setup

AccessData USB/Parallel Dongle Installation for 32 and 64 bit systems

This program will install the AccessData dongle drivers 1.6 beta-1.

2. Click *Next*.



Dongle Driver Setup

Setup Type

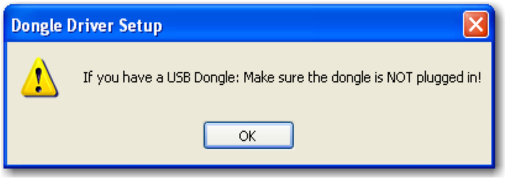
Select the setup type that best suits your needs.

Please select the dongle type you wish to install

● USB

○ Parallel

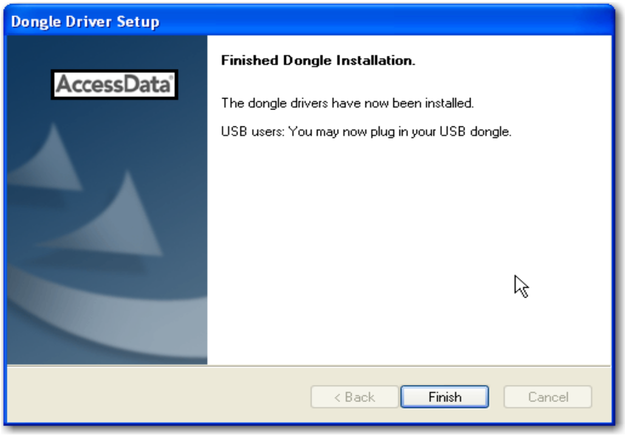
3. Select the type of dongle to install the drivers for.
4. Click *Next*.



Dongle Driver Setup

If you have a USB Dongle: Make sure the dongle is NOT plugged in!

5. If you have a USB dongle, verify that it is not connected.
6. Click *Next*.



Dongle Driver Setup

Finished Dongle Installation.

The dongle drivers have now been installed.

USB users: You may now plug in your USB dongle.

7. Click *Finish*.

8. Connect the USB dongle. Wait for the Windows Found New Hardware wizard, and follow the prompts.

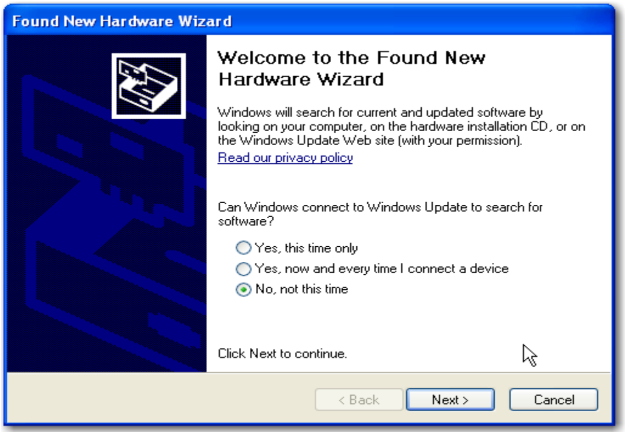
Important: If the Windows Found New Hardware wizard appears, complete the wizard. Do not close without completing, or the dongle driver will not be installed.

Windows Found New Hardware Wizard

When you connect the dongle after installing the dongle drivers, you should wait for the Windows Found New Hardware Wizard to come up. It is not uncommon for users to disregard this wizard, and then find that the dongle is not recognized and their AccessData software will not run.

When the Found New Hardware Wizard pops up, do the following:

1. When prompted whether to connect to Windows Update to search for software, choose, “No, not this time”.



Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

Windows will search for current and updated software by looking on your computer, on the hardware installation CD, or on the Windows Update Web site (with your permission).

Read our privacy policy

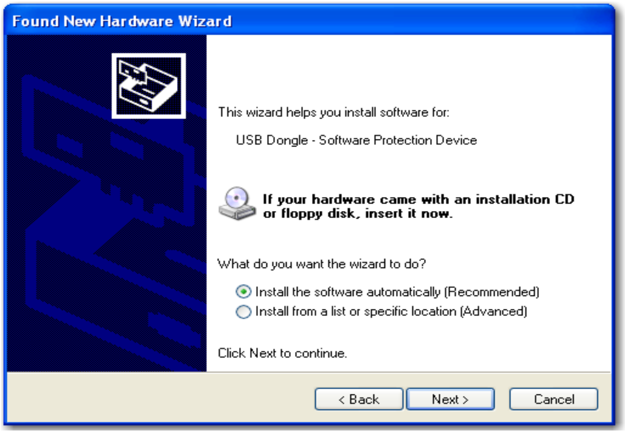
Can Windows connect to Windows Update to search for software?

○ Yes, this time only
○ Yes, now and every time I connect a device
● No, not this time

Click Next to continue.

2. Click *Next*.

3. When prompted whether to install the software automatically or to install from a list of specific locations, choose, "Install the software automatically (Recommended)".



Found New Hardware Wizard

This wizard helps you install software for:

USB Dongle - Software Protection Device

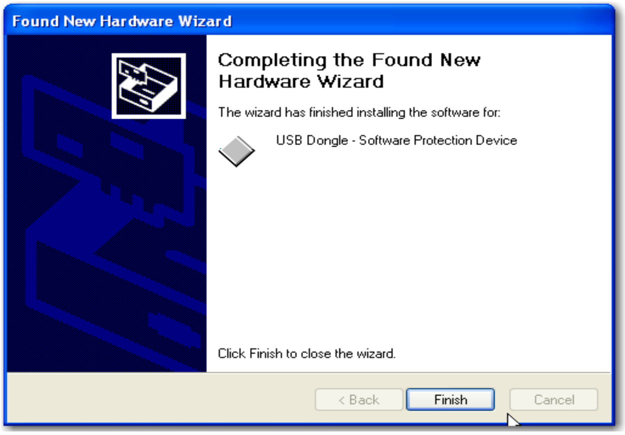
If your hardware came with an installation CD or floppy disk, insert it now.

What do you want the wizard to do?

● Install the software automatically (Recommended)
○ Install from a list or specific location (Advanced)

Click Next to continue.

4. Click *Next*.
5. Click *Finish* to close the wizard.



Found New Hardware Wizard

Completing the Found New Hardware Wizard

The wizard has finished installing the software for:

USB Dongle - Software Protection Device

Click Finish to close the wizard.

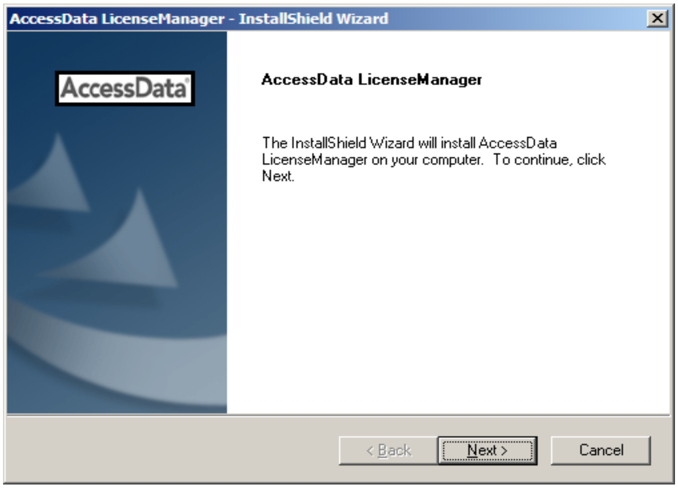
Once you have installed the dongle drivers and connected the dongle and verified that Windows recognizes it, you can use LicenseManager to manage product licenses.

INSTALLING LICENSEMANAGER

LicenseManager lets you manage product and license subscriptions using a security device or device packet file.

To install LicenseManager from the downloadable file:

1. Go to the AccessData download page at http://www.accessdata.com/downloads.htm.
2. On the download page, click the LicenseManager *Download* link.
3. Save the installation file (currently lm-license_manager-2.2.4.exe) to a temporary directory on your drive.
4. To launch the installation program, go to the temporary directory and double-click the installation file you downloaded in step 3.
5. Click *Next* on the Welcome screen.

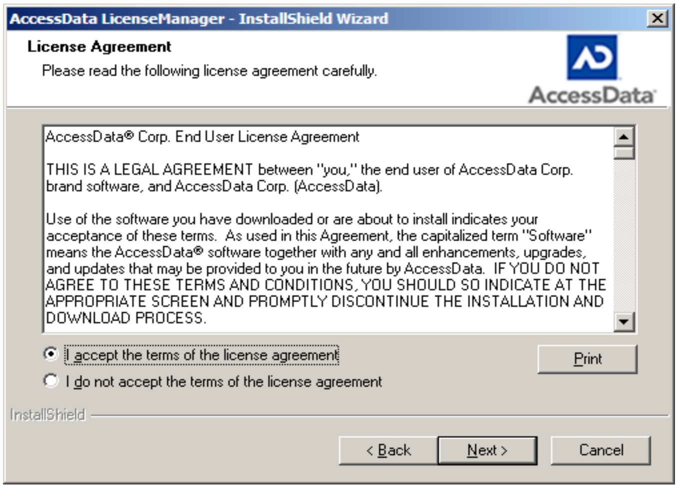


AccessData LicenseManager - InstallShield Wizard

AccessData LicenseManager

The InstallShield Wizard will install AccessData LicenseManager on your computer. To continue, click Next.

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



AccessData LicenseManager - InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

AccessData® Corp. End User License Agreement

THIS IS A LEGAL AGREEMENT between "you," the end user of AccessData Corp. brand software, and AccessData Corp. (AccessData).

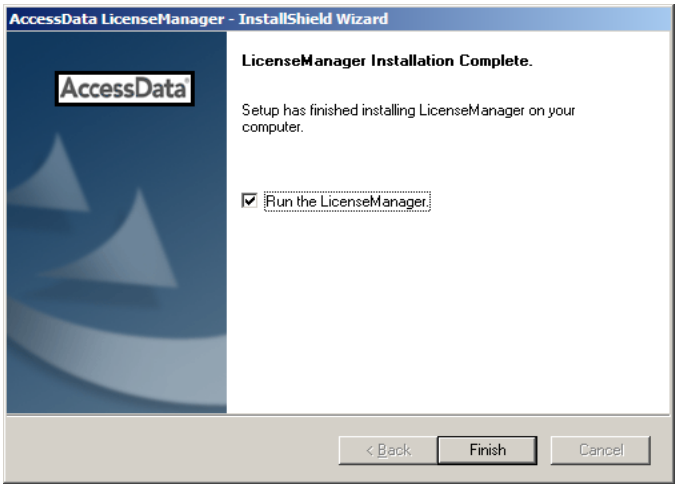
Use of the software you have downloaded or are about to install indicates your acceptance of these terms. As used in this Agreement, the capitalized term "Software" means the AccessData® software together with any and all enhancements, upgrades, and updates that may be provided to you in the future by AccessData. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, YOU SHOULD SO INDICATE AT THE APPROPRIATE SCREEN AND PROMPTLY DISCONTINUE THE INSTALLATION AND DOWNLOAD PROCESS.

● I accept the terms of the license agreement

○ I do not accept the terms of the license agreement

7. Wait while the installation completes.

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



AccessData LicenseManager - InstallShield Wizard

LicenseManager Installation Complete.

Setup has finished installing LicenseManager on your computer.

☑ Run the LicenseManager.

Run LicenseManager later by selecting
Start >Programs > AccessData > LicenseManager > LicenseManager
or by double-clicking the LicenseManager icon on your desktop .

MANAGING LICENSES WITH LICENSEMANAGER

LicenseManager manages AccessData product licenses on a Keylok dongle or Wibu CodeMeter Stick security device, or in a security device packet file. LicenseManager and the CodeMeter Stick installation are no longer integrated with FTK2 installation.

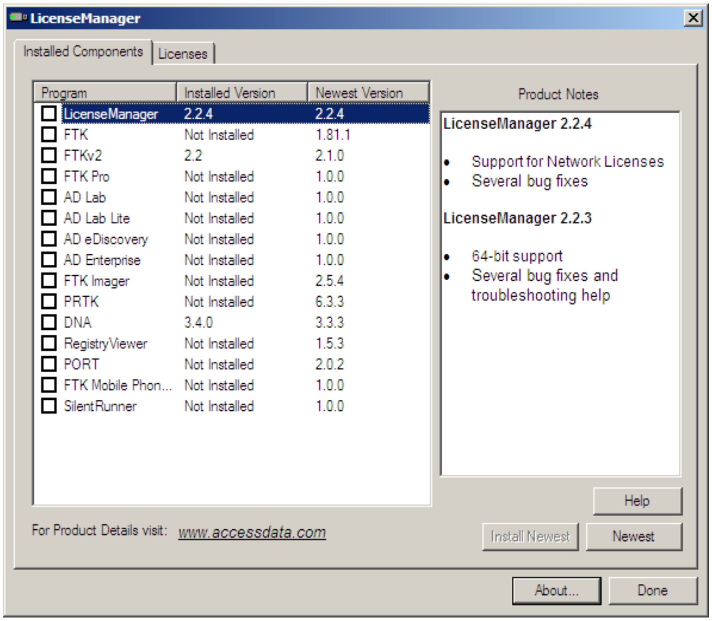
LicenseManager displays license information, allows you to add or remove existing licenses to a dongle or CmStick. LicenseManager can also be used to export a security device packet file. Packet files can be saved and reloaded onto the dongle or CmStick, or sent via email to AccessData support.

In addition, you can use LicenseManager to check for product updates and download the latest product versions.

LicenseManager displays CodeMeter Stick information (including packet version and serial number) and licensing information for all AccessData products. The Purchase Licenses button connects directly to the AccessData website and allows you to browse the site for information about products you may wish to purchase. Contact AccessData by phone to speak with a Sales Representative for answers to product questions, and to purchase products and renew licenses and subscriptions.

LicenseManager provides information as displayed in the following figures:

Figure 6-1 LicenseManager Installed Components Tab



Program	Installed Version	Newest Version
☐ LicenseManager	2.2.4	2.2.4
☐ FTK	Not Installed	1.81.1
☐ FTKv2	2.2	2.1.0
☐ FTK Pro	Not Installed	1.0.0
☐ AD Lab	Not Installed	1.0.0
☐ AD Lab Lite	Not Installed	1.0.0
☐ AD eDiscovery	Not Installed	1.0.0
☐ AD Enterprise	Not Installed	1.0.0
☐ FTK Imager	Not Installed	2.5.4
☐ PRTK	Not Installed	6.3.3
☐ DNA	3.4.0	3.3.3
☐ RegistryViewer	Not Installed	1.5.3
☐ PORT	Not Installed	2.0.2
☐ FTK Mobile Phon...	Not Installed	1.0.0
☐ SilentRunner	Not Installed	1.0.0

Product Notes

LicenseManager 2.2.4

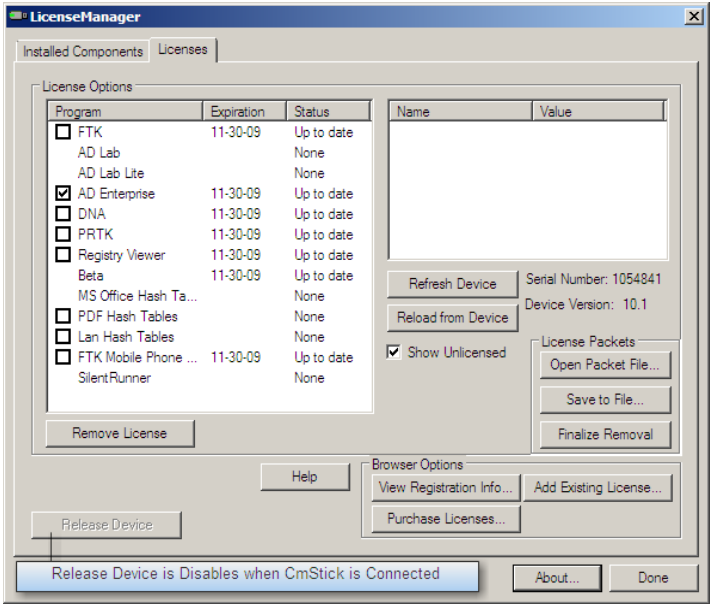
- Support for Network Licenses
- Several bug fixes

LicenseManager 2.2.3

- 64-bit support
- Several bug fixes and troubleshooting help

For Product Details visit: www.accessdata.com

Figure 6-2 LicenseManager Licenses Tab



Program	Expiration	Status
☐ FTK	11-30-09	Up to date
AD Lab		None
AD Lab Lite		None
☑ AD Enterprise	11-30-09	Up to date
☐ DNA	11-30-09	Up to date
☐ PRTK	11-30-09	Up to date
☐ Registry Viewer	11-30-09	Up to date
Beta	11-30-09	Up to date
MS Office Hash Ta...		None
☐ PDF Hash Tables		None
☐ Lan Hash Tables		None
☐ FTK Mobile Phone ...	11-30-09	Up to date
SilentRunner		None

Name	Value

Serial Number: 1054841

Device Version: 10.1

☑ Show Unlicensed

Release Device is Disables when CmStick is Connected

STARTING LICENSEMANAGER

LicenseManager.exe is located in C:\Program Files\AccessData\Common Files\AccessData LicenseManager\. You can execute the program from this location if you wish.

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

OR

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

OR

From some AccessData programs, you can run LicenseManager from the *Tools > Other Applications* menu. This option is not available in PRTK or DNA.

The LicenseManager program opens.

When starting LicenseManager, License Manager reads licensing and subscription information from the installed and connected Wibu CodeMeter Stick, or Keylok dongle.

If using a Keylok dongle, and LicenseManager either does not open or displays the message, "Device Not Found", do the following:

1. Make sure the correct dongle driver is installed on your computer.
2. With the dongle connected, check in Windows Device Manager to make sure the device is recognized. If it has an error indicator, right click on the device and choose Uninstall.
3. Remove the dongle after the device has been uninstalled.
4. Reboot your computer.
5. After the reboot is complete, and all startup processes have finished running, connect the dongle.
6. Wait for Windows to run the Add New Hardware wizard. If you already have the right dongle drivers installed, do not browse the internet, choose, "No, not this time."
7. Click *Next* to continue.
8. On the next options screen, choose, "Install the software automatically (Recommended)

9. Click Next to continue.
10. When the installation of the dongle device is complete, click Finish to close the wizard.
11. You still need the CodeMeter software installed, but will not need a CodeMeter Stick to run LicenseManager.

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

1. Make sure the CodeMeter Runtime 3.30a software is installed. It is available at www.accessdata.com/support. Click Downloads and browse to the product. Click on the download link. You can Run the product from the Website, or Save the file locally and run it from your PC. Once the CodeMeter Runtime software is installed and running, you will see a gray icon in your system tray: .
2. Make sure the CodeMeter Stick is connected to the USB port. When the CmStick is then connected, you will see the icon change to look like this: .

If the CodeMeter Stick is not connected, LicenseManager still lets you to manage licenses using a security device packet file if you have exported and saved the file previously.

To open LicenseManager without a CodeMeter Stick installed:

1. Click *Tools* > *LicenseManager*.

   LicenseManager displays the message, “Device not Found”.
2. Click *OK*, then browse for a security device packet file to open.

Note: Although you can run LicenseManager using a packet file, FTK 2.2 will not run with a packet file alone. You must have the CmStick connected to the computer to run FTK 2.2.

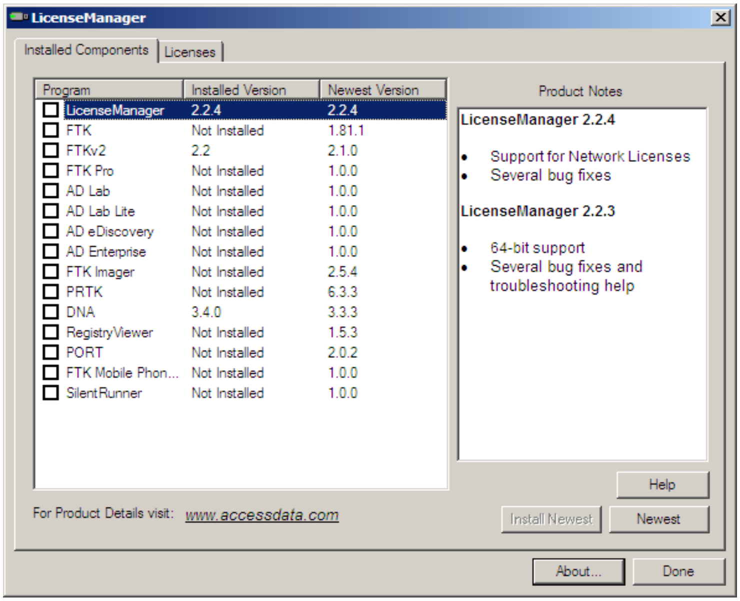
The LicenseManager Interface

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

The Installed Components Tab

The Installed Components tab lists the AccessData programs installed on the machine. The Installed Components tab is displayed in the following figure.

Figure 6-3 LicenceManager Installed Components



Program	Installed Version	Newest Version
□ LicenseManager	2.2.4	2.2.4
□ FTK	Not Installed	1.81.1
□ FTKv2	2.2	2.1.0
□ FTK Pro	Not Installed	1.0.0
□ AD Lab	Not Installed	1.0.0
□ AD Lab Lite	Not Installed	1.0.0
□ AD eDiscovery	Not Installed	1.0.0
□ AD Enterprise	Not Installed	1.0.0
□ FTK Imager	Not Installed	2.5.4
□ PRTK	Not Installed	6.3.3
□ DNA	3.4.0	3.3.3
□ RegistryViewer	Not Installed	1.5.3
□ PORT	Not Installed	2.0.2
□ FTK Mobile Phon...	Not Installed	1.0.0
□ SilentRunner	Not Installed	1.0.0

LicenseManager 2.2.4

- Support for Network Licenses
- Several bug fixes

LicenseManager 2.2.3

- 64-bit support
- Several bug fixes and troubleshooting help

For Product Details visit: www.accessdata.com

The following information is displayed on the Installed Components tab:

TABLE 6-1 LicenseManager Installed Components Tab Features

Item	Description
Program	Lists all AccessData products installed on the host.
Installed Version	Displays the version of each AccessData product installed on the host.
Newest Version	Displays the latest version available of each AccessData product installed on the host. Click Newest to refresh this list.
Product Notes	Displays notes and information about the product selected in the program list.
AccessData Link	Links to the AccessData product page where you can learn more about AccessData products.

The following buttons provide additional functionality from the Installed Components tab:

TABLE 6-2 LicenseManager Installed Components Buttons

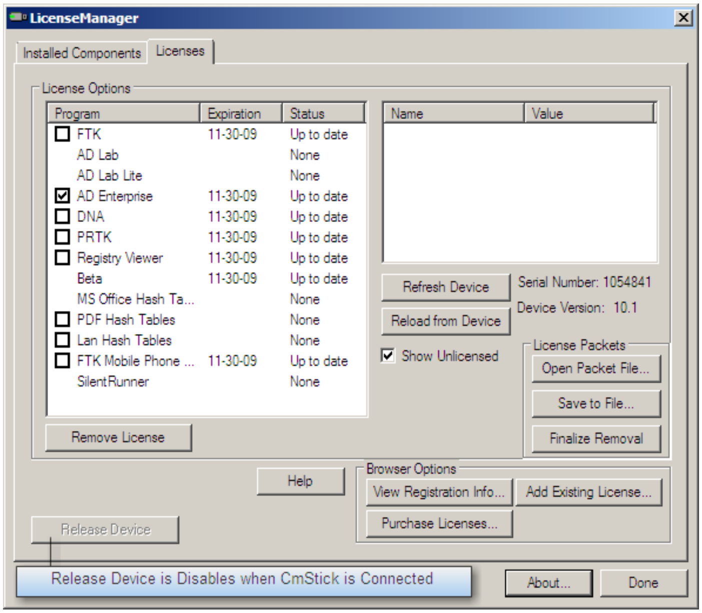
Button	Function
Help	Opens the LicenseManager Help web page.
Install Newest	Installs the newest version of the programs checked in the product window, if that program is available for download. You can also get the latest versions from our website using your Internet browser.
Newest	Updates the latest version information for your installed products.
About	Displays the About LicenseManager screen. Provides version, copyright, and trademark information for LicenseManager.
Done	Closes LicenseManager.

Use the Installed Components tab to manage your AccessData products and stay up to date on new releases.

THE LICENSES TAB

The Licenses tab displays CodeMeter Stick information for the current security device packet file and licensing information for AccessData products available to the owner of the CodeMeter Stick, as displayed in the following figure.

Figure 6-4 LicenseManager Licenses Tab



Program	Expiration	Status
☐ FTK	11-30-09	Up to date
AD Lab		None
AD Lab Lite		None
☑ AD Enterprise	11-30-09	Up to date
☐ DNA	11-30-09	Up to date
☐ PRTK	11-30-09	Up to date
☐ Registry Viewer	11-30-09	Up to date
Beta	11-30-09	Up to date
MS Office Hash Ta...		None
☐ PDF Hash Tables		None
☐ Lan Hash Tables		None
☐ FTK Mobile Phone ...	11-30-09	Up to date
SilentRunner		None

Serial Number: 1054841

Device Version: 10.1

☑ Show Unlicensed

Release Device is Disables when CmStick is Connected

The Licenses tab provides the following information:

TABLE 6-3 LicenseManager Licenses Tab Features

Column	Description
Program	Shows the owned licenses for AccessData products.
Expiration Date	Shows the date on which your current license expires.
Status	Shows these status of that product's license: • **None**: the product license is not currently owned • **Days Left**: displays when less than 31 days remain on the license. • **Never**: the license is permanently owned. This generally applies to Hash Tables and Portable Office Rainbow Tables.
Name	Shows the name of additional parameters or information a product requires for its license.

TABLE 6-3 LicenseManager Licenses Tab Features

Column	Description
Value	Shows the values of additional parameters or information a product contained in or required for its license.
Show Unlicensed	When checked, the License window displays all products, whether licensed or not.

The following license management actions can be performed using buttons found on the License tab:

TABLE 6-4 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. 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 6-4 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 Dongle Packet Files

You can open or save dongle packet files using LicenseManager. When started, LicenseManager attempts to read licensing and subscription information from the dongle. If you do not have a dongle installed, LicenseManager lets you browse to open a dongle packet file. You must have already created and saved a dongle packet file to be able to browse to and open it.

To save a security device packet file:

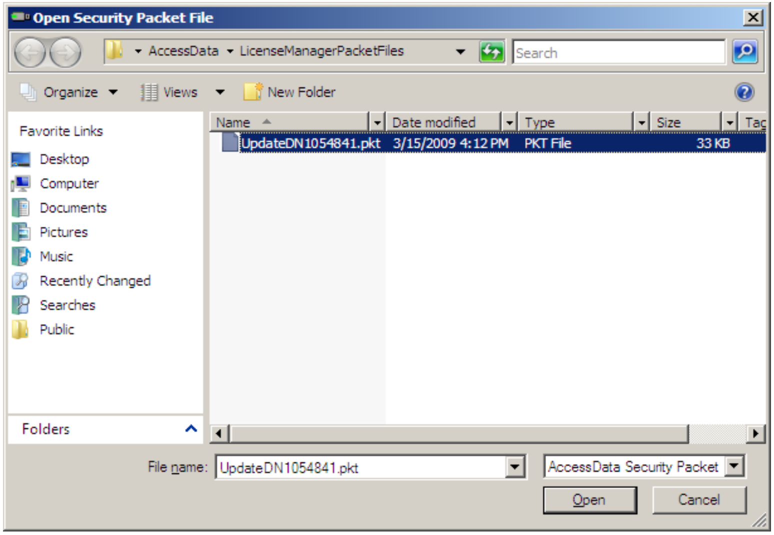
1. Click the *Licenses* tab, then under License Packets, click *Save to File*.
2. Browse to the desired folder and accept the default name of the .pkt file; then click *Save*.

Note: In general, the best place to save the .pkt files is in the AccessData LicenseManager folder. The default path is C:\Program Files\AccessData\Common Files\AccessData LicenseManager\.

To open a security device packet file:

1. Select the *Licenses* tab, then under License Packets, click *Open Packet File*.
2. Browse for a dongle packet file to open. Select the file, then click *Open*.

Figure 6-5 LicenseManager Open Packet File



Name	Date modified	Type	Size	Tag
UpdateDN1054841.pkt	3/15/2009 4:12 PM	PKT File	33 KB	

File name: UpdateDN1054841.pkt

AccessData Security Packet

Adding and Removing Product Licenses

On a computer with an Internet connection, LicenseManager lets you add available product licenses to, or remove them from, a dongle.

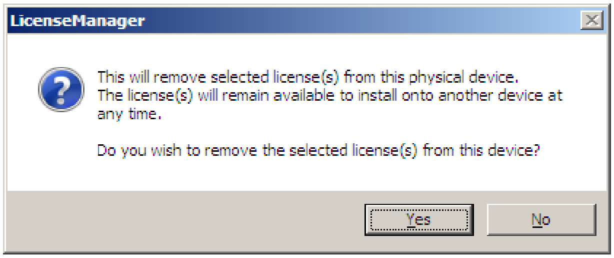
To move a product license from one dongle to another dongle, first remove the product license from the first dongle. You must release that dongle, and connect the second dongle before continuing. When the second dongle is connected and recognized by Windows and LicenseManager, click on the Licenses tab to add the product license to the second dongle.

Remove a License

To remove (unassociate) a product license:

1. From the Licenses tab, mark the program license to remove. This action activates the Remove License button below the Program list box.
2. Click *Remove License*. This connects your machine to the AccessData License Server through the Internet.

3. You will be prompted to confirm the removal of the selected license(s) from the device.



LicenseManager

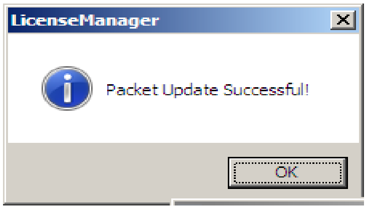
This will remove selected license(s) from this physical device.
The license(s) will remain available to install onto another device at any time.

Do you wish to remove the selected license(s) from this device?

Click *Yes* to continue, or *No* to cancel.

4. You will see some screens indicating the connection and activity on the License Server, and when the license removal is complete, you will see the following screen:

Figure 6-6 Packet Update Successful



LicenseManager

Packet Update Successful!

5. Click OK to close the message box. You will then see an Internet browser screen from LicenseManager with a message that says, "The removal of your license(s) from Security Device was successful!" You may close this box at any time.

ADD A LICENSE

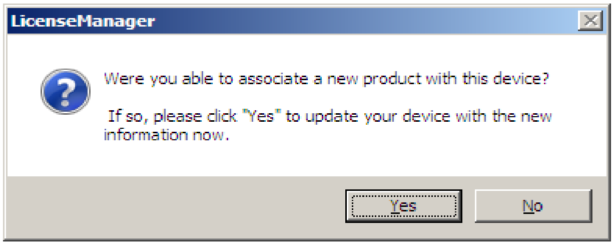
To add a new or released license:

1. From the Licenses tab, under Browser Options, click *Add Existing License.*

   The AccessData LicenseManager Web page opens, listing the licenses currently bound to the connected security device, and below that list, you will see the licenses that currently are not bound to any security device. Mark the box in the Bind column for the product you wish to add to the connected device, then click *Submit.*

2. An AccessData LicenseManager Web page will open, displaying the following message, "The AccessData product(s) that you selected has been bound to the record for Security Device *nnnnnnn* within the Security Device Database.

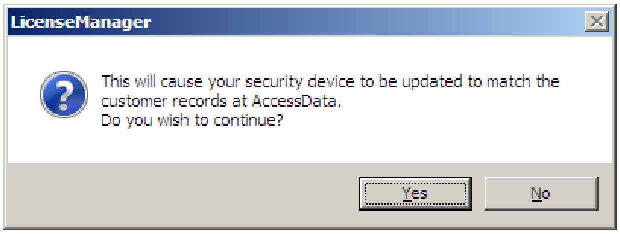
"Please run LicenseManager's "Refresh Device" feature in order to complete the process of binding these product license(s) to this Security Device." You may close this window at any time.


LicenseManager

Were you able to associate a new product with this device?

If so, please click "Yes" to update your device with the new information now.

3. Click *Yes* if LicenseManager prompts, "Were you able to associate a new product with this device?"
4. Click *Refresh Device* in the Licenses tab of LicenseManager. Click *Yes* when prompted.


LicenseManager

This will cause your security device to be updated to match the customer records at AccessData.
Do you wish to continue?

You will see the newly added license in the License Options list.

Adding and Removing Product Licenses Remotely

While LicenseManager requires an Internet connection to use some features, you can add or remove licenses from a dongle packet file for a dongle that resides on a computer, such as a forensic lab computer, that does not have an Internet connection.

If you cannot connect to the Internet, the easiest way to move licenses from one dongle to another is to physically move the dongle to a computer with an Internet connection, add or remove product licenses as necessary using LicenseManager, and then physically move the dongle back to the original computer. However, if you cannot move the dongle—due to organization policies or a need for forensic soundness—then transfer the packet files and update files remotely.

ADD A LICENSE REMOTELY

To remotely add (associate) a product license:

1. On the computer where the security device resides:

   1a. Run LicenseManager.

   1b. From the *Licenses* tab, click *Reload from Device* to read the dongle license information.

   1c. Click *Save to File* to save the dongle packet file to the local machine.

2. Copy the dongle packet file to a computer with an Internet connection.

3. On the computer with an Internet connection:

   3a. Remove any attached security device.

   3b. Launch LicenseManager. You will see a notification, "No security device found".

   3c. Click *OK*.

   3d. An "Open" dialog box will display. Highlight the `.pkt` file, and click *Open*.

   3e. Click on the Licenses tab.

   3f. Click *Add Existing License*.

   3g. Complete the process to add a product license on the Website page.

   3h. Click *Yes* when the LicenseManager prompts, "Were you able to associate a new product with this dongle?"

   3i. When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted to save the update file, `[serial#].wibuCmRaU`.

   3j. Save the update file to the local machine.

4. After the update file is downloaded, copy the update file to the computer where the dongle resides:

5. On the computer where the dongle resides:

   5a. Run the update file by double-clicking it. (It is an executable file.)

   5b. After an update file downloads and installs, click *OK*.

   5c. Run LicenseManager.

   5d. From the Licenses tab, click *Reload from Device* to verify the product license has been added to the dongle.

REMOVE A LICENSE REMOTELY

To remotely remove (unassociate) a product license:

1. On the computer where the dongle resides:

   1a. Run LicenseManager.

   1b. From the Licenses tab, click *Reload from Device* to read the dongle license information.

   1c. Click *Save to File* to save the dongle packet file to the local machine.

2. Copy the file to a computer with an Internet connection.

3. On the computer with an Internet connection:

   3a. Launch LicenseManager. You will see a notification, “No security device found”.

   3b. Click *OK*.

   3c. An “Open” dialog box will display. Highlight the `.pkt` file, and click *Open*.

   3d. Click on the Licenses tab.

   3e. Mark the box for the product license you want to unassociate; then click *Remove License*.

   3f. When prompted to confirm the removal of the selected license from the dongle, click *Yes*.

   When LicenseManager does not detect a dongle or the serial number of the dongle does not match the serial number in the dongle packet file, you are prompted save the update file.

   3g. Click *Yes* to save the update file to the local computer.

   The Step 1 of 2 dialog details how to use the dongle packet file to remove the license from a dongle on another computer.

   3h. Save the update file to the local machine.

4. After the update file is downloaded, copy the update file to the computer where the dongle resides.

5. On the computer where the dongle resides:

   5a. Run the update file by double-clicking it. This runs the executable update file and copies the new information to the security device.

   5b. Run LicenseManager

   5c. On the Licenses tab, click *Reload from Device* in LicenseManager to read the security device and allow you to verify the product license is removed from the dongle.

5d. Click *Save to File* to save the updated dongle packet file to the local machine.

6. Copy the file to a computer with an Internet connection.

Updating Products

You can use LicenseManager to check for product updates and download the latest product versions.

For more information on the general features of the subscription service, see the AccessData Website at http://www.accessdata.com/subscription_renewal.htm.

Check for Product Updates

To check for product updates, on the Installed Components tab, click *Newest*. This refreshes the list to display what version you have installed, and the newest version available.

Download Product Updates

To install the newest version, mark the box next to the product to install, then click Install Newest.

Note: Some products, such as FTK 2.x, Enterprise, and others, are too large to download, and are not available. A notification displays if this is the case.

To download a product update:

1. Ensure that LicenseManager displays the latest product information by clicking the Installed Components tab. Click *Newest* to refresh the list showing the latest releases, then compare your installed version to the latest release.

   If the latest release is newer than your installed version, you may be able to install the latest release from our Website.
2. Ensure that the program you want to install is not running.
3. Mark the box next to the program you want to download; then click *Install Newest*.
4. When prompted, click *Yes* to download and install the latest install version of the product.
5. If installing the update on a remote computer, copy the product update file to another computer.

6. Install the product update.

For information about installing the product update, refer to the installation information for the product. You may need to restart your computer after the update is installed.

Purchase Product Licenses

Use LicenseManager to link to the AccessData Web site to find information about all our products.

Purchase product licenses through your AccessData Sales Representative. Call 801-377-5410 and follow the prompt for Sales, or send an email to sales@accessdata.com.

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

Send a Dongle Packet File to Support

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

To create a dongle packet file, do the following:

1. Run LicenseManager
2. Click on the Licenses tab.
3. Click *Load from Device.*
4. Click *Refresh Device* if you need to get the latest info from AD's license server.
5. Click *Save to File*, and note or specify the location for the saved file.
6. Attach the dongle packet file to an e-mail and send it to:
   support@accessdata.com.

Note: For a more complete list of AccessData Corporation's contact information, see "Appendix G AccessData Corporate Contact Information" on page 307.

AccessData Glossary

A

AccessData Recovery Session

In PRTK, selecting one or more files and starting the password recovery process is called an AccessData Recovery (ADR) session. Typically, each case has one session unless you have a large number of encrypted files.

Address

A location of data, usually in main memory or on a disk. You can think of computer memory as an array of storage boxes, each of which is one byte in length. Each cstorage box has an address (a unique number) assigned to it. By specifying a memory address, programmers can access a particular byte of data. Disks are divided into tracks and sectors, each of which has a unique address.

Advanced Encryption Standard

A common symmetric encryption system that has replaced Data Encryption Standard as the encryption standard. It uses a 128, 192, or 256-bit key.

Application Administrator

The first user created in an AccessData FTK2 system. The Application Administrator has all rights within the application, including adding users and assigning roles.

Application Administrators can assign the role of Application Administrator to new users as they are created.

Asymmetric Encryption

A type of encryption in which the encryption and decryption keys are different. Asymmetric encryption uses a public key (which can be posted on an Internet site or made “public” through other means) and a private key, which remains secret. In this system, something that has been encrypted with the private key can be decrypted only by the public key, and vice versa. Asymmetric algorithms are slower than symmetric algorithms, but can nonetheless be very useful. They are often used in combination with symmetric algorithms, as with EFS Encryption.

The number of possible key values refers to the actual number of different key words or passwords that can exist, based on the particular algorithm used to create the key value in question. A n-bit key has 2n possible values. For example, a 40-bit key has 240 possible values, or 1,099,511,627,776 possibilities.

The security of an algorithm should rely on the secrecy of the key only, not the secrecy of the algorithm.

Do not compare key sizes between symmetric and asymmetric algorithms. For example, a 128-bit symmetric key is approximately as strong as a 512-bit asymmetric key.

B

BestCrypt

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

TABLE Glossary-1 BestCrypt Hash Functions and Encryption Algorithms

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

Binary

Pertaining to a number system that has just two unique digits. Computers are based on the binary numbering system, which consists of just two unique numbers, 0 and 1. All operations that are possible in the decimal system (addition, subtraction, multiplication, and division) are equally possible in the binary system.

BIOS

Acronym for Basic Input/Output System. The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

Bit-stream Image

See "Forensic Image" on page 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.

C

Chunk Size

The number of passwords the supervisor machine can process in the amount of time specified.

Cluster

Fixed-length blocks that store files on the FAT media. Each cluster is assigned a unique number by the computer operating system. Only the part of the partition called the "data area" is divided into clusters. The remainder of the partition are defined as sectors. Files and directories store their data in these clusters. The size of one cluster is specified in a structure called the Boot Record, and can range from a single sector to 128 sectors. The operating system assigns a unique number to each cluster and the keeps track of files according to which cluster they use.

CMOS

Short for Complementary Metal Oxide Semiconductor. Pronounced SEE-moss, CMOS is a widely used type of semiconductor. CMOS semiconductors use both NMOS (negative polarity) and PMOS (positive polarity) circuits. Since only one of the circuit types is on at any given time, CMOS chips require less power than chips using just one type of transistor. This makes them particularly attractive for use in battery-powered devices, such as portable computers. Personal computers also contain a small amount of battery-powered CMOS memory to hold the date, time, and system setup parameters.

CRC

Short for Cyclical Redundancy Check. It performs a complex calculation on every byte in the file, generating a unique number for the file in question. If so much as a single byte in the file being checked were to change, the cyclical redundancy check value for that file would also change. If the CRC value is known for a file before it is downloaded, you can compare it with the CRC value generated by this software after the file has been downloaded to ascertain whether the file was damaged in transit. The odds of two files having the same CRC value are even longer than the odds of winning a state-run lottery—along the lines of one in 4,294,967,296.

Cylinder

A single-track location on all the platters making up a hard disk. For example, if a hard disk has four platters, each with 600 tracks, then there will be 600 cylinders, and each cylinder will consist of 8 tracks (assuming that each platter has tracks on both sides).

D

dd

(Linux) Makes a copy of a input file (STDIN) using the specified conditions, and sends the results to the output file (STDOUT).

Data Carving

Data carving is the process of extracting a collection of data from a larger data set. Data carving techniques frequently occur during a digital investigation when the unallocated file system space is analyzed to extract files. The files are "carved" from the unallocated space using file type-specific header and footer values. File system structures are not used during the process.

Data Encryption Standard

A 56-bit symmetric encryption system that is considered weak by current standards. It has been broken in a distributed environment.

Device

Any machine or component that attaches to a computer. Examples of devices include disk drives, printers, mice, and modems. These particular devices fall into the category of peripheral devices because they are separate from the main computer.

Most devices, whether peripheral or not, require a program called a device driver that acts as a translator, converting general commands from an application into specific commands that the device understands.

Disk

A round plate on which data can be encoded. There are two basic types of disks: magnetic disks and optical disks.

E

Encrypting File System (EFS)

EFS is a file system driver that provides filesystem-level encryption in Microsoft Windows (2000 and later) operating systems, except Windows XP Home Edition, Windows Vista Basic, and Windows Vista Home Premium. The technology enables files to be transparently encrypted on NTFS file systems to protect confidential data from attackers with physical access to the computer.

EnScript (also "e script")

EnScript is a language and API that has been designed to operate within the EnCase environment. EnScript is compatible with the ANSI C++ standard for expression evaluation and operator meanings but contains only a small subset of C++ features. In other words, EnScript uses the same operators and general syntax as C++ but classes and functions are organized differently.

Evidence Item

A physical drive, a logical drive or partition, or drive space not included in any partitioned virtual drive.

F

File Allocation Table (FAT)

A table that the operating system uses to locate files on a disk. A file may be divided into many sections that are scattered around the disk. The FAT keeps track of all these pieces.

There is a field in the Boot Record that specifies the number of FAT copies. With FAT12 and FAT16, MS-DOS uses only the first copy, but the other copies are synchronized. FAT32 was enhanced to specify which FAT copy is the active one in a 4-bit value part of a Flags field.

Think of the FAT as a singly linked list. Each of the chains in the FAT specify which parts of the disk belong to a given file or directory.

A file allocation table is a simple array of 12-bit, 16-bit, or 32-bit data elements. Usually there will be two identical copies of the FAT.

FAT12: The oldest type of FAT uses a 12-bit binary number to hold the cluster number. A volume formatted using FAT12 can hold a maximum of 4,086 clusters, which is 2^{12} minus a few values (to allow for reserved values to be used in the FAT). FAT12 is most suitable for very small volumes, and is used on floppy disks and hard disk partitions smaller than about 16 MB (the latter being rare today.)

FAT16: The FAT used for older systems, and for small partitions on modern systems, uses a 16-bit binary number to hold cluster numbers. When you see someone refer to a FAT volume generically, they are usually referring to FAT16, because it is the de facto standard for hard disks, even with FAT32 now more popular than FAT16. A volume using FAT16 can hold a maximum of 65,526 clusters, which is 2^{16} less a few values (again for reserved values in the FAT). FAT16 is used for hard disk volumes ranging in size from 16 MB to 2,048 MB. VFAT is a variant of FAT16.

FAT32: The newest FAT type, FAT32 is supported by newer versions of Windows, including Windows 95's OEM SR2 release, as well as Windows 98, Windows ME, and Windows 2000. FAT32 uses a 28-bit binary cluster number—not 32 because 4 of the 32 bits are reserved. 28 bits is still enough to permit very large volumes—FAT32 can theoretically handle volumes with over 268 million clusters, and will theoretically support drives up to 2 TB in size. To do this, however, the size of the FAT grows very large.

VFAT features the following key improvements compared to FAT12 and FAT16:

- **Long File Name Support**: Prior to Windows 95, FAT was limited to the eleven-character (8.3) file name restriction. VFAT's most important accomplishment enabled the use of long file names by the Windows 95 operating system and applications written for it, while maintaining compatibility with older software that had been written before VFAT was implemented.
- **Improved Performance**: The disk access and file system management routines for VFAT were rewritten using 32-bit protected-mode code to improve

performance. At the same time, 16-bit code was maintained, for use when required for compatibility.

- **Better Management Capabilities**: Special support was added for techniques like disk locking to allow utilities to access a disk in exclusive mode without fear of other programs using it in the meantime.

File Header

The data at the beginning of a file that identifies the file type: .gif, .doc, .txt, etc.

File Footer

The data at the end of the file signifying the file is complete and allows the file to be understood by the operating system.

File Item

Any item FTK can parse from the evidence. This includes complete files as well as sub-elements such as graphics, files, or OLE objects embedded in other files; deleted items recovered from unallocated space; and so forth.

File Slack

Unused space. Operating systems store files in fixed-length blocks called clusters. Because few files are a size that is an exact multiple of the cluster size, there is typically unused space between the end of the file and the end of the last cluster used by that file.

Forensic Image

A process where all areas of a physical disk are copied, sector by sector, to storage media. This image may be a raw file, as in the case of the Linux utility DD, or it may be a forensically correct copy, such as SPADA provides. These images replicate exactly all sectors on a given storage device. All files, unallocated data areas, and areas not normally accessible to a user are copied.

Forensically Prepared Media

Digital media (such as a diskette, tape, CD, hard drive) that is sanitized (wiped clean) of all data. This means computer media that may be sanitized up to the Department of

Defense standards 5220.22-M (National Industrial Security Program Operating Manual Supplement) using software wipe utilities such as Dan Mares (Maresware) Declassify, New Technologies Inc (NTI) Disk Scrub or M-Sweep Pro or Symantec (Norton) WipeInfo to remove all data by overwriting the existing data with random or predefined characters. The Linux OS may also be used to write out a value of zero (0) to a device.

The media is then examined using tools to determine that no data exists (MD5, SHA-1 or Diskedit). The partition information is removed and the media is sanitized from the physical address of (cylinder/head/sector) 0/0/1 to the physical (versus logical) end of the media.

This process involves using a program such as I-wipe, Encase, Linux, Drivespy, SPADA or any program capable of writing multiple passes of a single character over the entire drive.

Checksum is a form of redundancy check, a very simple measure for protecting the integrity of data by detecting errors in data. It works by adding up the basic components of a message, typically the bytes, and storing the resulting value. Later, anyone can perform the same operation on the data, compare the result to the authentic checksum and (assuming that the sums match) conclude that the message was probably not corrupted.

Redundancy check is extra data added to a message for the purposes of error detection and error correction.

The value of the checksum of forensically prepared media will be zero (0) provided the write process is done using zeros.

G

Graphic Image Files

Computer graphic image files such as photos, drawings, etc. Come in various standard formats. Some of the most common file types include but are not limited to Joint Photographic Experts Group (JPEG, JPG), Bitmap (BMP), Graphics Interchange Format (GIF, JFIF) and AOL image file (ART).

Golden Dictionary

The Golden Dictionary file, ADPasswords.dat, contains all recovered passwords for all PRTK sessions on the current computer. It is stored in the AccessData program directory (C:\Program Files\AccessData\Recovery\). Recovered passwords are used as the first level of attack in all password recovery sessions. Most people use the same password for different files, so recovering the password for a simple file often opens the door to more difficult files.

Graphic Interchange Format (GIF)

A common graphics format that can be displayed on almost all Web browsers. GIFs typically display in 256 colors and have built-in compression. Static or animated GIF images are the most common form of banner creation.

H

Hard Disk (Drive)

A magnetic disk on which you can store computer data. The term hard is used to distinguish it from a soft or floppy disk. Hard disks hold more data and are faster than floppy disks. A hard disk, for example, can store anywhere from 10gigabytes to several terabytes, whereas most floppies have a maximum storage capacity of 1.4 megabytes.

Hashing

Generating a unique alphanumeric value based on a file's contents. The alphanumeric value can be used to prove that a file copy has not been altered in any way from the original. It is statistically impossible for an altered file to generate the same hash number.

Head

The mechanism that reads data from or writes data to a magnetic disk or tape. Hard disk drives have many heads, usually two for each platter.

Hexadecimal

The base-16 number system, which consists of 16 unique symbols: the numbers zero through nine and the letters A to F. For example, the decimal number 15 is represented as F in the hexadecimal numbering system. The hexadecimal system is useful because it can represent every byte (eight bits) as two consecutive hexadecimal digits. It is easier for humans to read hexadecimal numbers than binary numbers.

K

Known File Filter (KFF)

The KFF is a database utility that compares the hash values of case files to a database of hash values from known files. The KFF can significantly reduce the amount of time you spend analyzing files by eliminating unimportant files such as system and application files, or identifying alert files such as known child pornograhy images. After you compare case files to the KFF database, FTK and Enterprise place unimportant files (known system and application files) in the KFF Ignorable container and alert files (known criminal files) in the KFF Alert Files container within the Overview tab.

M

Markov Permutation

The Markov permutation records the times certain words, letters, punctuation, and spaces occur together in a given amount of text, then generates random output that has the same distribution of groups.

For example: if you were to scan through the text and create a huge frequency table of what words come after the words “up the,” you might find “tree,” “ladder,” and “creek” most often. You would then generate output from the words “up the,” and get the results “up the tree,” “up the creek,” and “up the ladder” randomly.

If the words “up the” were followed most frequently by the word “creek” in your sample text, the phrase “up the creek” would occur most frequently in your random output.

Andrey Andreyevich Markov (June 14, 1856–July 20, 1922) was a Russian mathematician.

Memory

Internal storage areas in the computer. The term memory identifies data storage that comes in the form of chips; the word storage is used for memory that exists on tapes or disks. Moreover, the term memory is usually used as shorthand for physical memory, which refers to the actual chips capable of holding data.

Message Digest 5

A 128-bit digital fingerprint based on a file's content. An algorithm created in 1991 by Professor Ronald Rivest of RSA that is used to create digital signatures, or a 128-bit digital fingerprint based on a file's content. Message Digest 5 (MD5) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a hash or digest. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest. When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been changed. This comparison is called a hash check. The number is derived from the input in such a way that it is computationally infeasible to derive any information about the input from the hash. It is also computationally infeasible to find another file that will produce the same output.

MD5 hashes are used by the KFF to identify known files.

Metadata

Literally data about data. Metadata describes how, when, and by whom a particular set of data was collected and how the data is formatted. Metadata is essential for understanding information stored in data warehouses and has become increasingly important in XML-based Web applications.

Mount

To make a mass storage device available to the OS, or to a user or user group. In may also mean to make a device physically accessible. In a Unix environment, the mount command attaches discs or directories logically rather than physically. The Unix mount command makes a directory accessible by attaching a root directory of one file system to another directory, which makes all the file systems usable as if they were subdirectories of the file system they are attached to. Unix recognizes devices by their location, while Windows recognizes them by their names (C: drive, for example). Unix organizes directories in a tree-like structure in which directories are attached by mounting them on the branches of the tree. The file system location where the device is attached is called a mount point. Mounts may be local or remote. A local mount connects disk drives on one machine so that they behave as one logical system. A remote mount uses Network File System (NFS) to connect to directories on other machines so that they can be used as if they were all part of the user's file system.

N

NT File System (NTFS)

One of the file systems for the Windows NT operating system (Windows NT also supports the FAT file system). NTFS has features to improve reliability, such as transaction logs to help recover from disk failures. To control access to files, you can set permissions for directories or individual files. NTFS files are not accessible from other operating systems, such as DOS. For large applications, NTFS supports spanning volumes, which means files and directories can be spread out across several physical disks.

P

Pagefile (.sys)

The paging file is the area on the hard disk that Windows uses as if it were random access memory (RAM). This is sometimes known as virtual memory. By default, Windows stores this file on the same partition as the Windows system files.

Parallel Framework Extensions (PFX)

PFX is a managed concurrency library being developed by a collaboration between Microsoft Research and the CLR team at Microsoft. It is composed of two parts: **Parallel LINQ (PLINQ)** and **Task Parallel Ligary (TPL).**

Pretty Good Privacy

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

R

RC4

RC4, or ARC4, is a variable key-length stream cipher designed by RSA. Stream ciphers are key-dependent, pseudo-random number generators whose output is XORed with the data <plaintext> XOR <random-looking stream> = <random-looking ciphertext>. Because XOR is symmetric (in other words, [A XOR B] XOR B = A), XORing the ciphertext with the stream again returns the plaintext. Microsoft Word and Excel use RC4 and a 40-bit key to encrypt their files. An exhaustive key space attack has a much better chance at succeeding with a 40-bit key space.

S

Sector

A sector is a group of bytes within a track and is the smallest group of bytes that can be addressed on a drive. There are normally tens or hundreds of sectors within each track. The number of bytes in a sector can vary, but is almost always 512. The maximum number of sectors in a cluster is 64. CDROMS normally have 2048 bytes per sector. Sectors are numbered sequentially within a track, starting at 1. The numbering restarts on every track, so that “track 0, sector 1” and “track 5, sector 1” refer to different sectors. Modern drives use a system known as Logical Block Addressing (LBA) instead of CHS to track sectors.

During a low-level format, hard disks are divided into tracks and sectors. The tracks are concentric circles around the disk and the sectors are segments within each circle. For example, a formatted disk might have 40 tracks, with each track divided into ten sectors.

Physical sectors are relative to the entire drive. Logical sectors are relative to the partition.

Secure Hash Algorithm

A 160-bit digital fingerprint based on a file's content. Designed by the National Institute of Standards and Technology (NIST), Secure Hash Algorithm (SHA) takes as input an arbitrary-length file and outputs a fixed-length number referred to as a hash or digest. The number is derived from the input in such a way that it is computationally impossible to derive any information about the input from the hash. It is also computationally impossible to find another file that will produce the same output. SHA-1 hashes are used by the KFF to identify known files.

FTK uses SHA-1 and SHA-256. The KFF library contains some A hashes.

SHA

The SHA (Secure Hash Algorithm) family is a set of related cryptographic hash functions. The most commonly used function in the family, SHA-1, is employed in a large variety of popular security applications and protocols, including TLS, SSL, PGP, SSH, S/MIME, and IPSec. SHA-1 is considered to be the successor to MD5, an earlier, widely-used hash function. The SHA algorithms were designed by the National Security Agency (NSA) and published as a US government standard.

The first member of the family, published in 1993, is officially called SHA; however, it is often called SHA-0 to avoid confusion with its successors. Two years later, SHA-1, the first successor to SHA, was published. Four more variants have since been issued with increased output ranges and a slightly different design: SHA-224, SHA-256, SHA-384, and SHA-512—sometimes collectively referred to as SHA-2.

Attacks have been found for both SHA-0 and SHA-1. No attacks have yet been reported on the SHA-2 variants, but since they are similar to SHA-1, researchers are worried, and are developing candidates for a new, better hashing standard.

Spool (spooling, print spool)

Acronym for Simultaneous Peripheral Operations On-Line, spooling refers to putting jobs in a buffer, a special area in memory or on a disk where a device can access them when it is ready. Spooling is useful because devices access data at different rates. The buffer provides a waiting station where data can rest while the slower device catches up.

The most common spooling application is print spooling. In print spooling, documents are loaded into a buffer (usually an area on a disk), and then the printer pulls them off the buffer at its own rate. Because the documents are in a buffer where they can be accessed by the printer, you can perform other operations on the computer while printing takes place in the background. Spooling also lets you place a number of print jobs on a queue instead of waiting for each one to finish before specifying the next one.

Slack (File and RAM)

Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space that exists from the end of the file to the end of the last cluster assigned to the file is called file slack. Cluster sizes vary in length depending on the operating system involved and, in the case of Windows 95, the size of the logical partition involved. Larger cluster sizes mean more file slack and also the waste of storage space when Windows 95 systems are involved.

File slack potentially contains randomly selected bytes of data from computer memory. This happens because DOS/Windows normally writes in 512 byte blocks called sectors. Clusters are made up of blocks of sectors. If there is not enough data in the file to fill the last sector in a file, DOS/Windows makes up the difference by padding the remaining space with data from the memory buffers of the operating system. This randomly selected data from memory is called RAM Slack because it comes from the memory of the computer.

RAM Slack can contain any information that may have been created, viewed, modified, downloaded or copied during work sessions that have occurred since the computer was last booted. Thus, if the computer has not been shut down for several days, the data stored in file slack can come from work sessions that occurred in the past.

RAM slack pertains only to the last sector of a file. If additional sectors are needed to round out the block size for the last cluster assigned to the file, then a different type of slack is created. It is called drive slack and it is stored in the remaining sectors which might be needed by the operating system to derive the size needed to create the last cluster assigned to the file. Unlike RAM slack, which comes from memory, drive slack is padded with what was stored on the storage device before. Such data could contain remnants of previously deleted files or data from the format pattern associated with disk storage space that has yet to be used by the computer.

For example, take a file that is created by writing the word “Hello.” Assuming that this is the only data written in the file and assuming a two sector cluster size for the file, the data stored to disk and written in file slack could be represented as follows:

Hello+++++++|————(EOC)

RAM Slack is indicated by "+"

Drive Slack is indicated by "–"

File Slack is created at the time a file is saved to disk. When a file is deleted under DOS, Windows, Windows 95, Windows 98 and Windows NT/2000/XP, the data associated with RAM slack and drive slack remains in the cluster that was previously assigned to the end of the deleted file. The clusters which made up the deleted file are released by the operating system and they remain on the disk in the form of unallocated storage space until the space is overwritten with data from a new file.

File slack potentially contains data dumped randomly from the computer's memory. It is possible to identify network login names, passwords, and other sensitive information associated with computer usage. File slack can also be analyzed to identify prior uses of the subject computer and such legacy data can help the computer forensics investigator. File slack is not a trivial item. On large hard disk drives, file slack can involve several hundred megabytes of data. Fragments of prior email messages and word processing documents can be found in file slack. From a computer forensic standpoint, file slack is very important as both a source of digital evidence and security risks

String Searches

A string search is a data string containing standard text or non-text data. The term may be a word, phrase or an expression. Keyword searches are designed to aid in the identification of potentially relevant data on the examined media.

Superuser Administrator

Aperson with unlimited access privileges who can perform any and all operations on the computer and within the operating system and file system. These privileges do not necessarily transfer to the applications installed on the computer.

Symmetric Encryption

A type of encryption in which the encryption and decryption keys are the same. Some common symmetric encryption systems are Data Encryption Standard, Triple-DES, Pretty Good Privacy, BestCrypt, and Advanced Encryption Standard.

T

Thumbnail

A smaller-sized version of a graphics image.

U

Unallocated Space

Also called free space, it consists of all the clusters on a drive that are not currently assigned to a file. Some of these clusters may still contain data from files that have been deleted but not yet overwritten by other files.

Until the first file is written to the data storage area of a computer storage device, the clusters are unallocated by the operating system in the File Allocation Table (FAT). These unallocated clusters are padded with format pattern characters and the unallocated clusters are not of interest to the computer forensics specialist until data is written to the clusters. As the computer user creates files, clusters are allocated in the File Allocation Table (FAT) to store the data. When the file is deleted by the computer user, the clusters allocated to the file are released by the operating system so new files and data can be stored in the clusters when needed. However, the data associated with the deleted file remains behind. This data storage area is referred to as unallocated storage space and it is fragile from an evidence preservation standpoint. However, until the unallocated storage space is reassigned by the operating system, the data remains behind for easy discovery and extraction by the computer forensics specialist. Unallocated file space potentially contains intact files, remnants of files and subdirectories and temporary files, which were transparently created and deleted by computer applications and also the operating system. All of such files and data fragments can be sources of digital evidence and also security leakage of sensitive data and information.

URL

Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use and the second part specifies the IP address or the domain name where the resource is located.

V

Volume

A volume refers to a mounted partition. There may be only one volume on a disk, such as a floppy disk or a zip disk. There may be several volumes on a disk as on a partitioned hard drive. A volume is a logical structure, not a physical device. There can be up to 24 of these logical volumes on a disk and they show up as drive "c," "d," or "e" in DOS.

Volume Boot Sector

Since every partition may contain a different file system, each partition contains a volume boot sector which is used to describe the type of file system on the partition and usually contains boot code necessary to mount the file system.