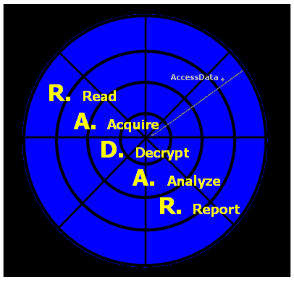
AccessData®

Forensic Toolkit

Sales and Promotional Summary



ACCESSDATA, ON YOUR RADAR

What is AccessData's Forensic Toolkit®?

Also known as FTK®, this application enables you to perform complete and thorough computer forensic examinations. FTK features powerful filtering and search functionality, and is recognized by law enforcement and corporate security professionals as the leading forensic tool for e-mail analysis.

We'll Help Your Investigation

AccessData's Forensic Toolkit advances your investigation by giving you more time, power, and insight to each case. FTK provides you the following advantages:

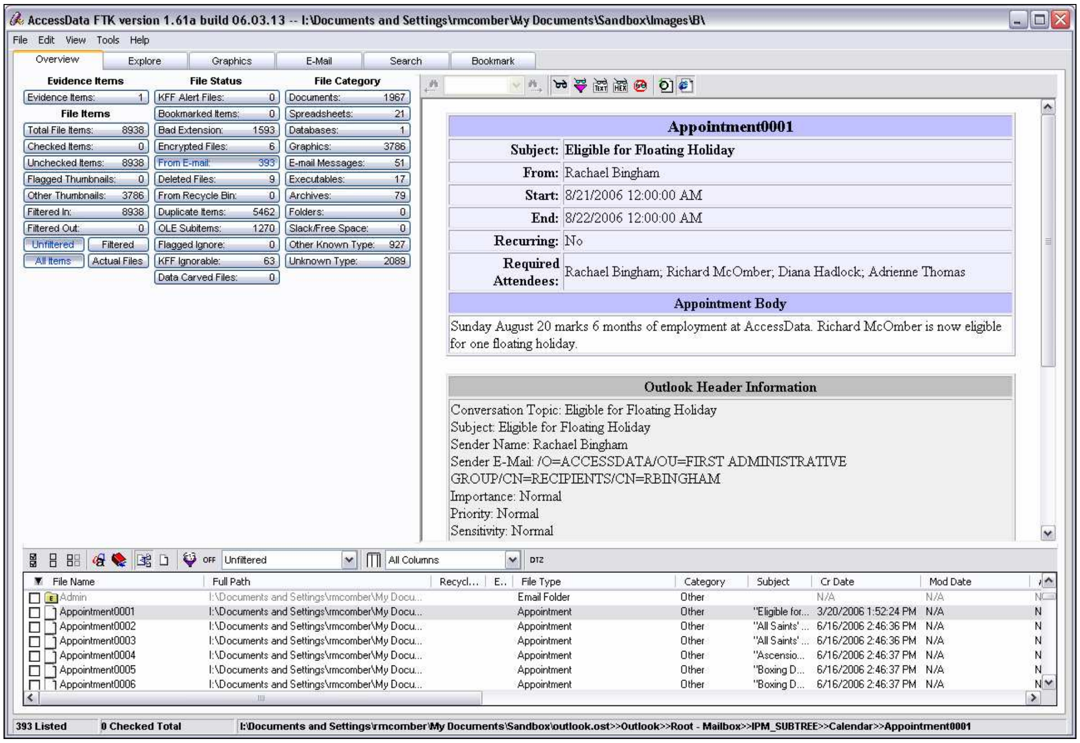
- Simple Users' Interface
- Fast Searching
- EFS Decryption
- Bookmarking
- Reporting
- Password Dictionary Creation

Uncomplicated Users' Interface

FTK makes evidence and easy to analyze. Our database architecture sorts and categorizes all graphics, e-mails, bad extensions, and encrypted files more quickly and simply.

A click of the mouse on the Graphics category, for example, allows you to see a list of every graphic found on the hard drive.

E-mail Display
Most forensic software requires yet another utility to allow the investigator to view emails in readable HTML format. FTK allows you to view e-mail in a user-friendly HTML. You can view native formats such as AOL IP addresses, POP3 servers, and view attachments. You can also document them in HTML reports.


AccessData FTK version 1.61a build 06.03.13 -- I:\Documents and Settings\rmcomber\My Documents\Sandbox\Images\B\
File Edit View Tools Help
Overview
Explore
Graphics
E-Mail
Search
Bookmark
OFF
Unfiltered
All Columns
DTZ

Evidence Items		File Status		File Category	
Evidence Items:	1	KFF Alert Files:	0	Documents:	1967
File Items		Bookmarked Items:	0	Spreadsheets:	21
Total File Items:	8938	Bad Extension:	1593	Databases:	1
Checked Items:	0	Encrypted Files:	6	Graphics:	3786
Unchecked Items:	8938	From E-mail:	393	E-mail Messages:	51
Flagged Thumbnails:	0	Deleted Files:	9	Executables:	17
Other Thumbnails:	3786	From Recycle Bin:	0	Archives:	79
Filtered In:	8938	Duplicate Items:	5462	Folders:	0
Filtered Out:	0	OLE Subitems:	1270	Slack/Free Space:	0
Unfiltered	Filtered	Flagged Ignore:	0	Other Known Type:	927
All Items	Actual Files	KFF Ignorable:	63	Unknown Type:	2089
		Data Carved Files:	0		

Appointment0001	
Subject:	**Eligible for Floating Holiday**
From:	Rachael Bingham
Start:	8/21/2006 12:00:00 AM
End:	8/22/2006 12:00:00 AM
Recurring:	No
Required Attendees:	Rachael Bingham; Richard McOmber; Diana Hadlock; Adrienne Thomas

Appointment Body

Sunday August 20 marks 6 months of employment at AccessData. Richard McOmber is now eligible for one floating holiday.

Outlook Header Information

Conversation Topic: Eligible for Floating Holiday
Subject: Eligible for Floating Holiday
Sender Name: Rachael Bingham
Sender E-Mail: /O=ACCESSDATA/OU=FIRST ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=RBINGHAM
Importance: Normal
Priority: Normal
Sensitivity: Normal

File Name	Full Path	Recycl...	E..	File Type	Category	Subject	Cr Date	Mod Date	
□ Admin	I:\Documents and Settings\rmcomber\My Docu...			Email Folder	Other		N/A	N/A	N
□ Appointment0001	I:\Documents and Settings\rmcomber\My Docu...			Appointment	Other	"Eligible for...	3/20/2006 1:52:24 PM	N/A	N
□ Appointment0002	I:\Documents and Settings\rmcomber\My Docu...			Appointment	Other	"All Saints' ...	6/16/2006 2:46:36 PM	N/A	N
□ Appointment0003	I:\Documents and Settings\rmcomber\My Docu...			Appointment	Other	"All Saints' ...	6/16/2006 2:46:36 PM	N/A	N
□ Appointment0004	I:\Documents and Settings\rmcomber\My Docu...			Appointment	Other	"Ascensio...	6/16/2006 2:46:37 PM	N/A	N
□ Appointment0005	I:\Documents and Settings\rmcomber\My Docu...			Appointment	Other	"Boxing D...	6/16/2006 2:46:37 PM	N/A	N
□ Appointment0006	I:\Documents and Settings\rmcomber\My Docu...			Appointment	Other	"Boxing D...	6/16/2006 2:46:37 PM	N/A	N

393 Listed | 0 Checked Total | I:\Documents and Settings\rmcomber\My Documents\Sandbox\outlook.ost>>Outlook>>Root - Mailbox>>IPM_SUBTREE>>Calendar>>Appointment0001

FTK can print or export e-mail messages and all associated attachments. It recognizes the source of the e-mail messages based on e-mail archives and special headers.

FTK supports these e-mail applications:

- AOL[*]
- Earthlink
- Eudora
- Hotmail
- MSN E-mail
- Netscape
- Outlook
- Outlook Express
- Yahoo

FTK can recover encrypted instant messaging chat logs and additional information such as buddy lists. FTK supports these instant messaging applications:

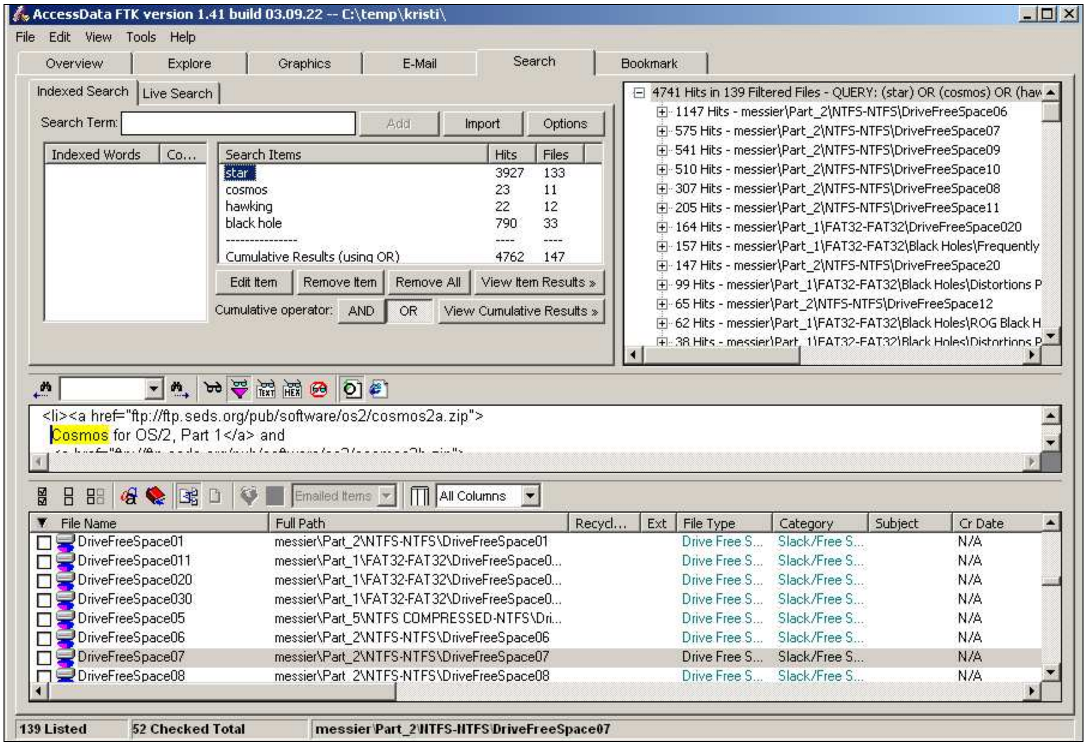
- AOL Instant Messenger
- Yahoo MessengerReporting

Fast Searching

Full-text indexing makes searching for keywords instantaneous. The index file is a

[*] FTK includes extended support for AOL, including buddy lists, global settings, user history, URL history, thumbnail extraction, and address book extraction.

the case evidence. The indexed search uses the index file to find the search term. Evidence items may be indexed when they are first added to the case, or later on.



Indexed Words	Co...

Search Items	Hits	Files
star	3927	133
cosmos	23	11
hawking	22	12
black hole	790	33
---------------	----	----
Cumulative Results (using OR)	4762	147

```
⊟ 4741 Hits in 139 Filtered Files - QUERY: (star) OR (cosmos) OR (haw
    ⊞ 1147 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace06
    ⊞ 575 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace07
    ⊞ 541 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace09
    ⊞ 510 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace10
    ⊞ 307 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace08
    ⊞ 205 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace11
    ⊞ 164 Hits - messier\Part_1\FAT32-FAT32\DriveFreeSpace020
    ⊞ 157 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Frequently
    ⊞ 147 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace20
    ⊞ 99 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Distortions P
    ⊞ 65 Hits - messier\Part_2\NTFS-NTFS\DriveFreeSpace12
    ⊞ 62 Hits - messier\Part_1\FAT32-FAT32\Black Holes\ROG Black H
    ⊞ 38 Hits - messier\Part_1\FAT32-FAT32\Black Holes\Distortions P
```

```
<li><a href="ftp://ftp.seds.org/pub/software/os2/cosmos2a.zip">
  Cosmos for OS/2, Part 1</a> and
```

File Name	Full Path	Recycl...	Ext	File Type	Category	Subject	Cr Date
□ DriveFreeSpace01	messier\Part_2\NTFS-NTFS\DriveFreeSpace01			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace011	messier\Part_1\FAT32-FAT32\DriveFreeSpace0...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace020	messier\Part_1\FAT32-FAT32\DriveFreeSpace0...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace030	messier\Part_1\FAT32-FAT32\DriveFreeSpace0...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace05	messier\Part_5\NTFS COMPRESSED-NTFS\Dri...			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace06	messier\Part_2\NTFS-NTFS\DriveFreeSpace06			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace07	messier\Part_2\NTFS-NTFS\DriveFreeSpace07			Drive Free S...	Slack/Free S...		N/A
□ DriveFreeSpace08	messier\Part_2\NTFS-NTFS\DriveFreeSpace08			Drive Free S...	Slack/Free S...		N/A

139 Listed | 52 Checked Total | messier\Part_2\NTFS-NTFS\DriveFreeSpace07

Full-text indexing makes searching much more efficient. All keyboard-related characters in the case evidence are indexed, allowing you to data carve and search by Internet keywords.

KFF Database

The Known File Filter (KFF) is an FTK utility that compares file hashes of your evidence against a database of hashes from files known to be irrelevant (such as known system and program files). It also checks for duplicate files.

- You can expand the power of your KFF by importing hashes from other databases, or updating the KFF database.
- A KFF Alert Editor allows you to edit the Alert/Ignore status of every hash set contained within the KFF library.
- KFF includes the NDIC/NIST database, which is updated periodically and is available for download on the FTK update page (http://www.accessdata.com/downloads.htm).

EFS Decryption

The Encrypting File System, or EFS is part of the Microsoft NTFS file system. EFS is a transparent public key encryption technology that works in conjunction with the user’s logon process to grant and deny users access to files and folders in Windows NT (excluding NT4), 2000, XP (excluding XP Home Edition) and Vista operating systems.

Important: FTK requires the PRTK license to decrypt EFS files.

EFS uses a public key and a private key for encryption. If the user does not have a key pair, the EFS generates one automatically. Files can be encrypted individually, or a folder can be designated as encrypted so that any file written to that folder is automatically encrypted. Because EFS's encryption technology integrates into the file system, once initiated it is transparent to the user as it is based on the logon authentication. These EFS encrypted 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. Forensic Toolkit (FTK) can break the file encryption so that additional evidence can be uncovered.

When evidence is added to a case and Decrypt EFS Files is selected in the New Case Wizard, FTK launches PRTK and decrypts EFS files.

Windows 2000 and XP Systems Prior to SP1
FTK automatically decrypts EFS files on Windows 2000 systems and Windows XP systems prior to Service Pack 1. Select the Decrypt EFS Files option when adding evidence to a case and FTK will launch PRTK and decrypt the EFS files.

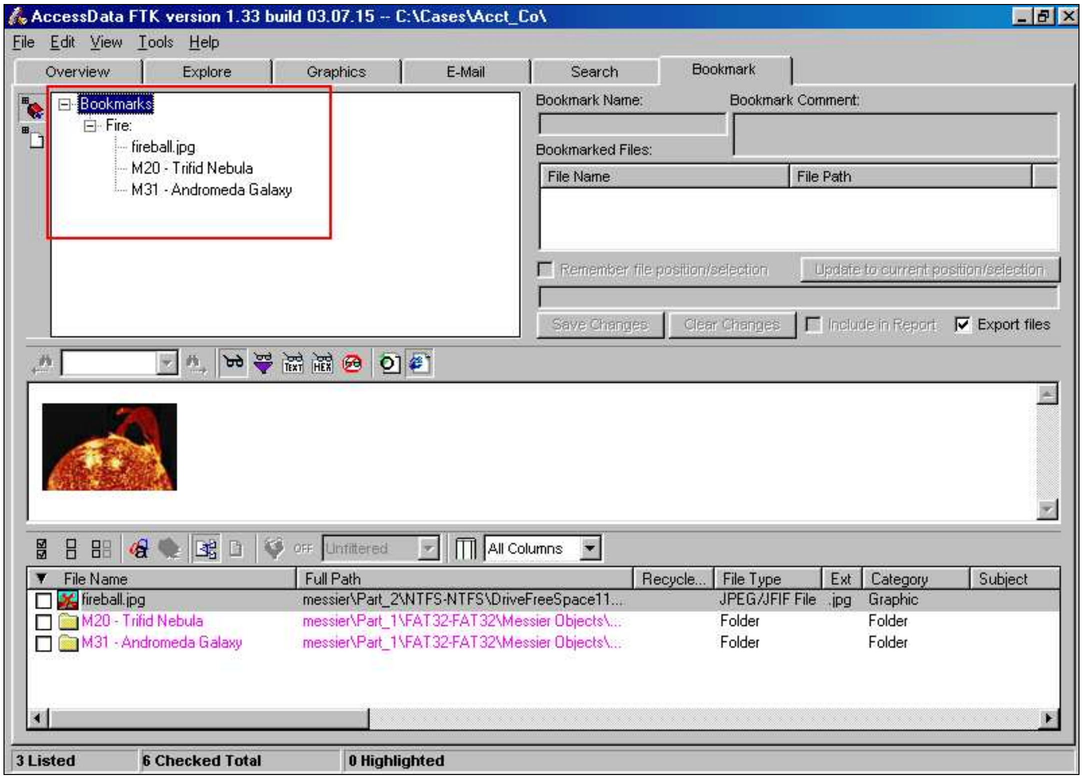
Windows XP SP1 or Later
For Windows XP systems with Service Pack 1 or later, FTK needs the user's or Recovery Agent's password before it can decrypt EFS files.

The decrypted information is displayed in the Explore window. The decrypted file is displayed as a sub-item to the encrypted file. The metadata and full path name is also displayed, including a note that shows that the file is decrypted

For example, if you have a decrypted file named "Jupiter Statistics.xls," then the decrypted version would be "Jupiter Statistics[decrypted].xls" is listed as a child of "Jupiter Statistics.xls" in the File List.

Bookmarking

The end result of a successful investigation is a list of bookmarked data to be used as evidence. A bookmark contains a group of files that you want to reference in your case. Bookmarks help organize the case evidence by grouping related or similar files. For example, you can create a bookmark of graphics that contain similar images.



- Bookmarks
  - Fire:
    - fireball.jpg
    - M20 - Trifid Nebula
    - M31 - Andromeda Galaxy

☑ Export files

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

3 Listed | 6 Checked Total | 0 Highlighted

You can add checked files, highlighted files, and currently listed files simply by right-clicking and selecting “add to bookmark,” FTK will show you a list of current bookmarks to select from.

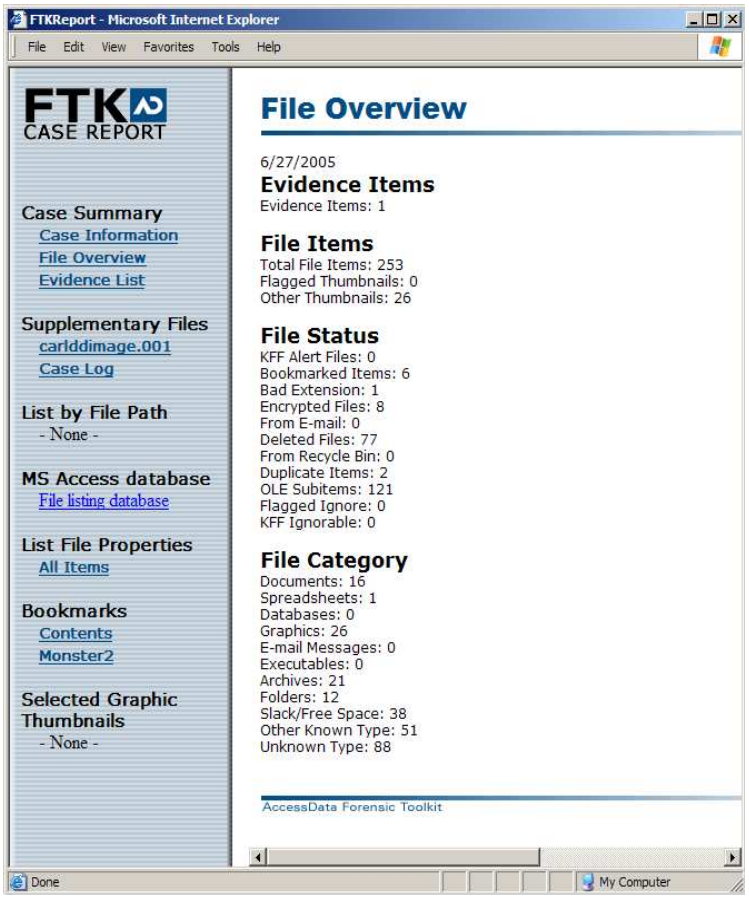
Reporting

After you complete the case investigation, you can create a report that summarizes the relevant evidence of the case.

FTK provides a thorough report wizard that allows customization of reports, including the placement of one’s own logo on the title page. The final report is in HTML format and is viewable in a standard Web browser.

- You can create a section in the report that lists the bookmarks that were created during the case investigation. You can also choose to not create a bookmark section.
- You can create a section in the report that displays thumbnail images of the case graphics.
- You can create a section in the report that lists the file paths of files in selected categories. The List by File Path section simply displays the files and their file paths; it does not contain any additional information. However, you can export and link to the files in the File Path list by checking the Export to the Report box.
- You can create a section in the report that lists file properties for different file types in selected categories.

- You can add files such as supplementary reports, search warrant information, and photos of the crime scene to the report. You can also add the case log to the report. The case log documents activities and events that occur in the case during investigation and analysis.


FTKReport - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Done
My Computer

FTK CASE REPORT

Case Summary
Case Information
File Overview
Evidence List

Supplementary Files
carlddimage.001
Case Log

List by File Path
- None -

MS Access database
File listing database

List File Properties
All Items

Bookmarks
Contents
Monster2

Selected Graphic Thumbnails
- None -

File Overview

6/27/2005

Evidence Items
Evidence Items: 1

File Items
Total File Items: 253
Flagged Thumbnails: 0
Other Thumbnails: 26

File Status
KFF Alert Files: 0
Bookmarked Items: 6
Bad Extension: 1
Encrypted Files: 8
From E-mail: 0
Deleted Files: 77
From Recycle Bin: 0
Duplicate Items: 2
OLE Subitems: 121
Flagged Ignore: 0
KFF Ignorable: 0

File Category
Documents: 16
Spreadsheets: 1
Databases: 0
Graphics: 26
E-mail Messages: 0
Executables: 0
Archives: 21
Folders: 12
Slack/Free Space: 38
Other Known Type: 51
Unknown Type: 88

AccessData Forensic Toolkit

Included files only require that the applications to view them must be installed on the computer the report is being viewed .

Password Dictionary Creation

FTK uses the full-text index for instantaneous keyword results. It can also be exported for use as a dictionary for password recovery processes in the Password Recovery Toolkit (PRTK).

With Full Text Index, you create a dictionary of every alpha numeric string located on the hard drive. This dictionary that you create in FTK becomes pivotal in cracking passwords. Every alpha numeric string ever recorded onto the hard drive is placed into a database for PRTK to search through and decrypt passwords from.

You can export the index by selecting **Tools**, and then **Export Word List**.

Conclusion

FTK Applies a database methodology to digital analysis. With its built in viewers, filters, and other utilities, FTK is very fast and very efficient at case analysis.

Contact Us:

Sales
AccessData
384 South 400 West Suite 200
Lindon, UT 84042
USA

sales@accessdata.com
800.574.5199