



AccessData®

FTK 4 and FTK 5

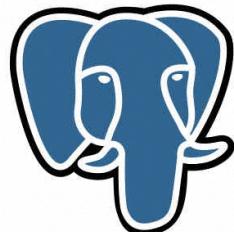
Working with FTK 4 or 5

FTK 2.x, 3.x summary

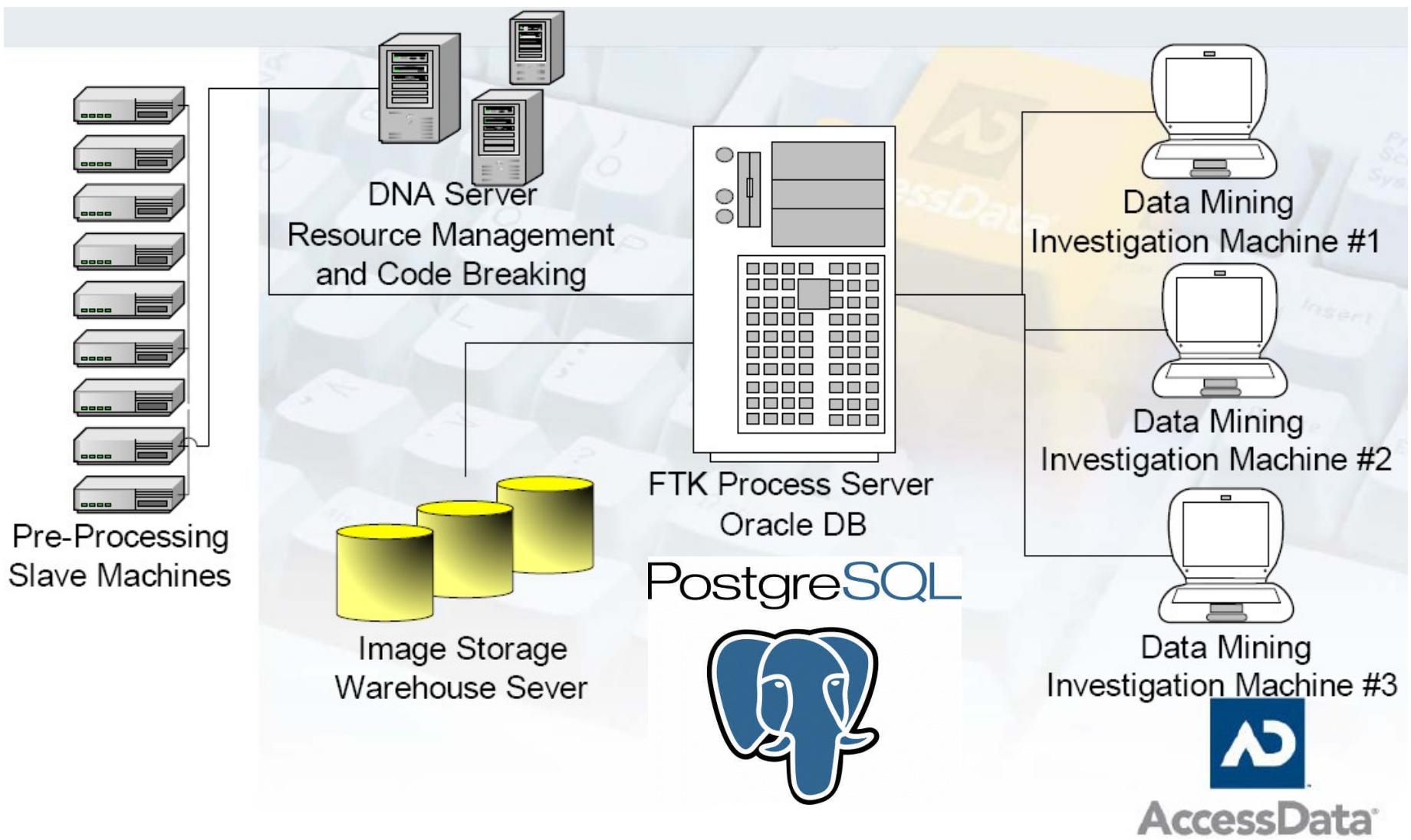
➤ Advantages

- Client / Server Architecture
- Oracle database capable of managing numerous HD's per case.
- Multi-threaded processing compared to FTK 1.x's serial process.
- Immediate access to data.
- The order of evidence pre-processing and the building of index records is directed by the examiner. (My Documents directory, then the e-mail, then the internet history)
- Multi-tier categories, user definable GUI, dock-able windows for multiple monitor support, user definable KFF filters.
- Support of several index based search engines for better searching.
- Full Unicode enabled
- Numerous investigators and examiners can work on the same case at the same time sharing bookmarks, notes, etc.

PostgreSQL



FTK 2.x, 3.x, 4.x, 5.x model

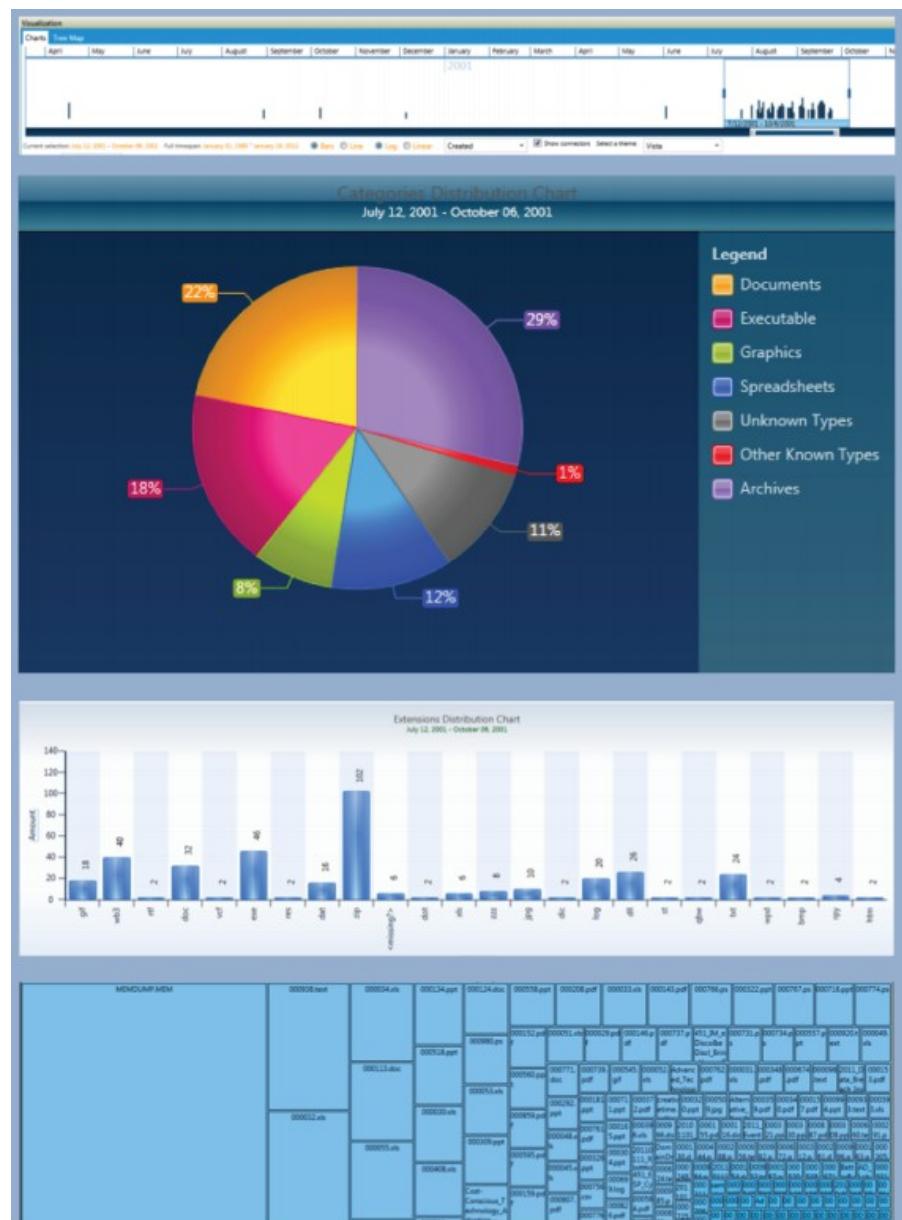


Many FTK 4/5 improvements

<http://accessdata.com/products/computer-forensics/ftk>

- Most of the improvements are **not** listed here!
- Real DBMS (FTK 2) – Oracle, PostgreSQL
 - GUI is separated from analysis process – crash proof?
- QuickPicks (FTK 2)
 - A feature that lets users view the contents of all subfolders
- Simultaneous multiple user case access (FTK 2)
- Mobile Phone Examiner Cell Phone Forensics Software (FTK 2)
- Mac OS X forensic support (FTK 3)
- Single-Node Enterprise (FTK 4) - builds in AD Enterprise (FTK2)
 - Remote forensics via client agents
- Volatile/Memory Analysis (FTK 3)
- Cerberus (FTK 4)
 - Static malware analysis of binary files (manual stage 1 for us)
- Add ons
 - Visualization, Explicit Image Detection (EID), Cerberus full support

Email and File Visualization



Explicit Image Detection

During processing, choose from 4 different options, all of which are shown below.

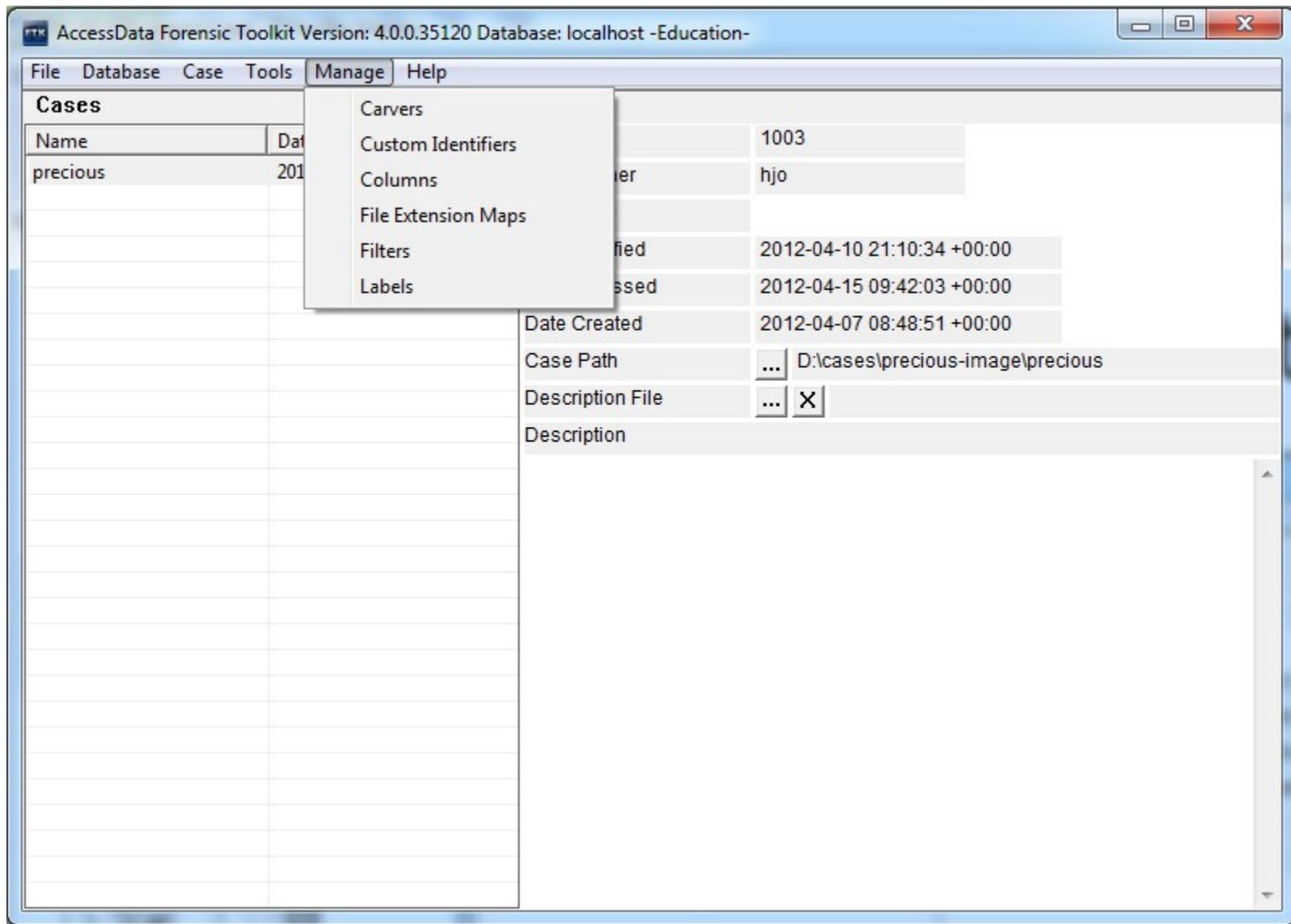
Images are automatically scored from 0 to 100 on their potential to be pornographic.

The screenshot shows the AccessData Forensic Toolkit interface. The top half displays a grid of image thumbnails, with several images having black redaction boxes over them. Below this is a tree view of evidence items, specifically a partition from a Windows XP Professional VM. The bottom half contains two tables. The left table, titled 'File List' and 'Explicit Material Score', lists files with their names and explicit material scores (ranging from 0 to 99). The right table, titled 'Time Zone: Mountain Daylight Time (From local machine)', shows the same files with four different explicit level scores: default, fast, zero false negatives, and zero false positives. A red callout box points to the text about scoring, and another red callout box points to the 'Explicit Material Score' table.

Name	Category	Explicit level (default)	Explicit level (fast)	Explicit level (zero false negatives)	Explicit level (zero false positives)
04.jpg		0	99	99	0
2763.jpg		0	93	93	0
asian_hard1806.jpg		93	99	99	93
bik4687j.jpg		99	99	99	99
centerfold001.jpg		JPEG	0	99	0
cot2.jpg		JPEG	56	99	99
d2445.jpg		JPEG	0	99	0
des45637Sc52.jpg		JPEG	0	99	0
fg_ashleybond4.jpg	Explicit	JPEG	99	99	99
group1.jpg		JPEG	1	99	1
landd2503.jpg		JPEG	11	99	11
lat12p.jpg		JPEG	0	99	0
veg99f5.jpg		JPEG	11	99	11
IMG00229 - Copy.jpg		JPEG E...	63	97	63
IMG00229.inn		JPEG F...	63	97	63

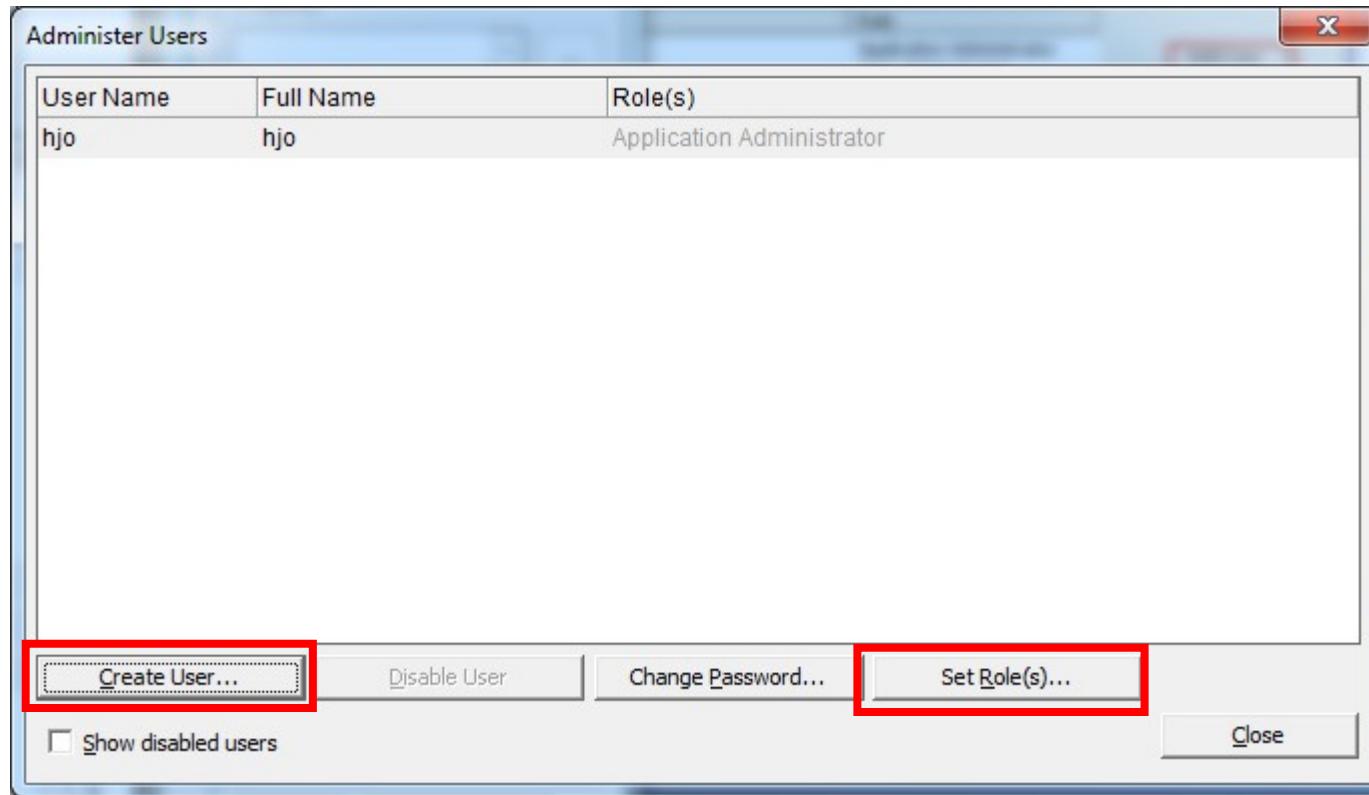
Name	Category	Explicit level (default)	Explicit level (fast)	Explicit level (zero false negatives)	Explicit level (zero false positives)
04.jpg		0	99	99	0
2763.jpg		0	93	93	0
asian_hard1806.jpg		93	99	99	93
bik4687j.jpg		99	99	99	99
centerfold001.jpg		JPEG	0	99	0
cot2.jpg		JPEG	56	99	99
d2445.jpg		JPEG	0	99	0
des45637Sc52.jpg		JPEG	0	99	0
fg_ashleybond4.jpg	Explicit	JPEG	99	99	99
group1.jpg		JPEG	1	99	1
landd2503.jpg		JPEG	11	99	11
lat12p.jpg		JPEG	0	99	0
veg99f5.jpg		JPEG	11	99	11
IMG00229 - Copy.jpg		JPEG E...	63	97	63
IMG00229.inn		JPEG F...	63	97	63

Case Manager Interface

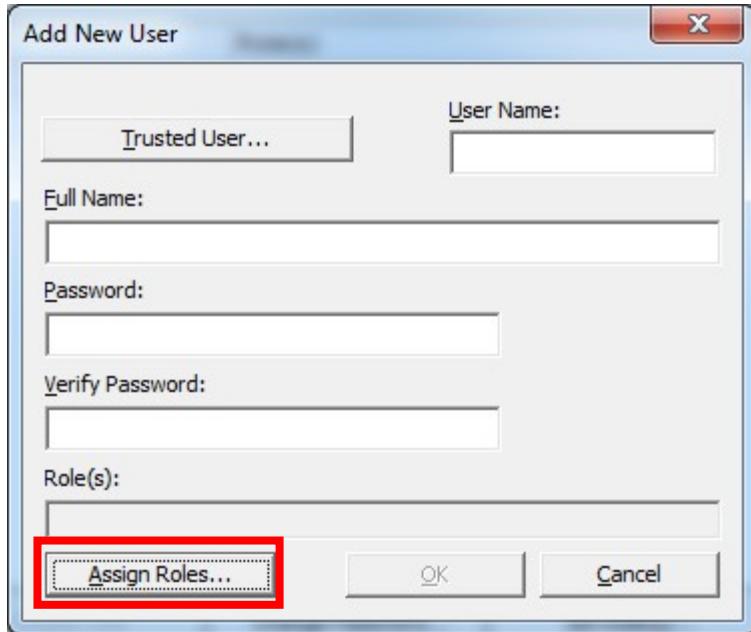


Administer Users 1

- The first user account is the Application Administrator



Administer Users 2

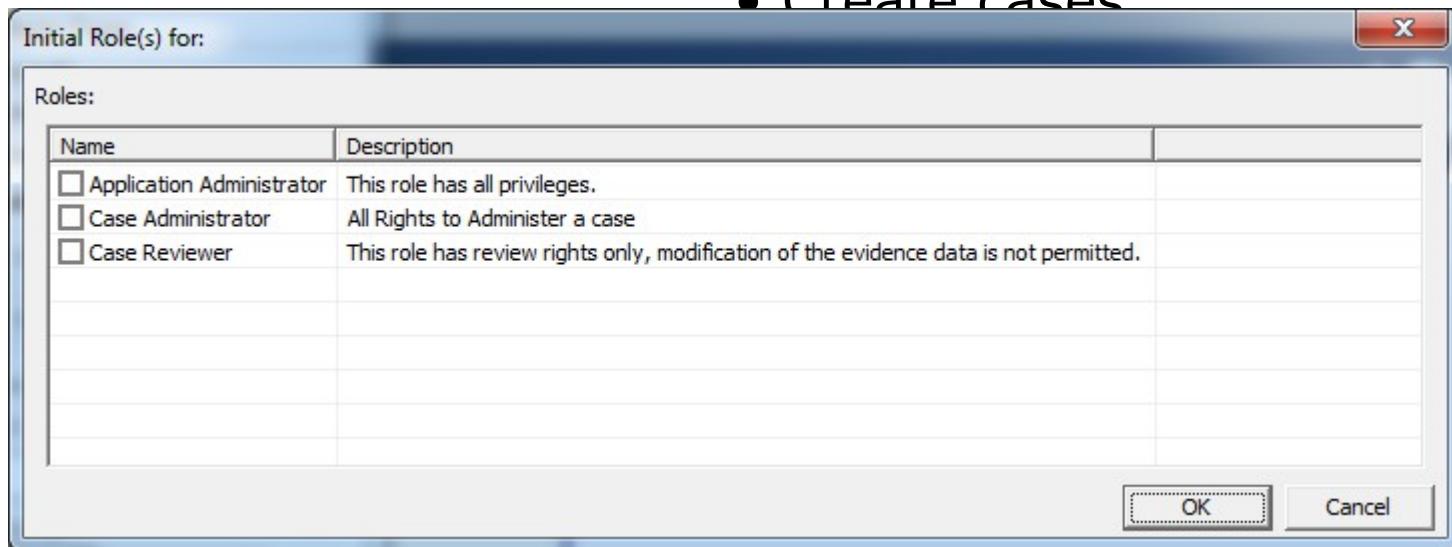


Application Administrator

- Create other users
- Create cases
- Assign rights to cases
- Change User Passwords

Case Administrator

- Create cases



ases

Case Examiner Interface

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Evidence Items

File Content

Hex Text Filtered Natural

THE RETURN OF THE KING
Frodo: Thank you. Thank you very much.
Gandalf: IT'S NOT WHAT I EXPECTED.

Default Media Web

File List

Display Time Zone: W. Europe Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
rotk_teaser_poster_tit...		2954	gif	precious.E01/Partition 1...	GIF	1536 B	1137 B	1F8B5E...	FABCD...	569C0...	2005-01-01 19...	2004-12-31 06...	2005-01-06 22...
rotk_theatrical_poster_...		2794	gif	precious.E01/Partition 1...	GIF	1024 B	900 B	415D6...	4BEE34...	312D2...	2005-01-01 19...	2004-12-31 06...	2005-01-06 22...
rotkcomic.exif.html		5126	html	precious.E01/Partition 1...	HTML	n/a	n/a				n/a		
rotkcomic.jpg		3071	jpg	precious.E01/Partition 1...	JPEG E...	72,00 KB	71,95 KB	A1367...	FDC98...	DAC4A...	2005-01-01 19...	2005-01-01 19...	2004-12-21 19...
rotkexclusive[1].gif		2950	gif	precious.E01/Partition 1...	GIF	1024 B	1008 B	F93952...	CC2C6...	306456...	2005-01-01 19...	2004-12-31 06...	2005-01-06 22...
RP27		3675		precious.E01/Partition 1...	Folder	152 B	152 B				2005-01-01 19...	2004-12-30 04...	2005-01-01 19...
RP28		3695		precious.E01/Partition 1...	Folder	48 B	48 B				2005-01-01 19...	2004-12-30 04...	2005-01-01 19...
RP29		3696		precious.E01/Partition 1...	Folder	48 B	48 B				2005-01-01 19...	2004-12-30 04...	2005-01-01 19...

Loaded: 5 015 Filtered: 5 015 Total: 5 015 Highlighted: 1 Checked: 208 Total LSize: 247,3 MB

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

Ready Explore Tab Filter: [None]

Tabs and Panes

The screenshot displays a digital forensic analysis interface with several windows and tabs.

Top Navigation Bar: File, Edit, View, Evidence, Filter, Tools, Help.

View Menu: Refresh (F5), Define..., Filter Bar, Timezone Display..., Thumbnail Size, Tab Layout, Explorer Tree, Graphics Tree, Overview Tree, Email Tree, Bookmark Tree, Indexed Searches, Live Searches, Bookmark Information, File List.

Filter Bar: Marks, Live Search, Index Search.

Properties Window: Shows file details for "ClassicVisaFern.gif".

Name	Item Number	File Type	Path
ClassicVisaFern.gif	1604	GIF	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth

File Details: General Info, File Size, File Dates, File Attributes, General.

File List: Shows a list of files with columns: Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed.

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed
Apple_guy.gif		1600	gif	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth	GIF	8704 B	8483 B	FA79F...	A3B07...	872482...	4/12/2007 7:56...	7/13/2007 1:44:22 PM (2007-03-06 01:44:22 UTC)
beer.gif		1601	gif	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth	GIF	7168 B	6892 B	D669C...	11FFC...	9C3DB...	4/12/2007 7:56...	7/13/2007 1:44:22 PM (2007-03-06 01:44:22 UTC)
Car Titles		1602		Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth	Folder	408 B	408 B	288B5...	6ACEA...	21B049...	3/5/2007 8:01...	7/2/2007 1:44:22 PM (2007-03-06 01:44:22 UTC)
Checks		1603		Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth	Folder	56 B	56 B	35ED3...	A9420...	518691...	3/5/2007 8:01...	7/2/2007 1:44:22 PM (2007-03-06 01:44:22 UTC)
ClassicVisaFern.gif		1604	gif	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth	GIF	38.00 KB	37.57 KB	EF250B...	238CD...	903A6...	3/5/2007 7:44...	7/13/2007 1:44:22 PM (2007-03-06 01:44:22 UTC)
CRACK_ME		1605	<missing>	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth	Text	1024 KB	1024 KB	5A4F0...	C5EE4...	099975...	4/10/2007 8:27...	6/20/2007 1:44:22 PM (2007-03-06 01:44:22 UTC)
Dear Sweetie.doc		1606	doc	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth	Microsoft Word Document	63.50 KB	63.50 KB	954418...	B79149...	F5393...	7/12/2007 6:51...	7/13/2007 1:44:22 PM (2007-03-06 01:44:22 UTC)

Status Bar: Loaded: 34, Filtered: 34, Total: 34, Highlighted: 1, Checked: 0.

Bottom Status: Ready, Explore Tab Filter: [None], Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/ClassicVisaFern.qif

Tabs and Panes

The screenshot shows a digital forensic analysis software interface. On the left, there's a vertical toolbar with icons for File List, Evidence, Filter Bar, Timezone Display..., Thumbnail Size, Tab Layout, Explorer Tree, Graphics Tree, Overview Tree, Email Tree, Bookmark Tree, Indexed Searches, Live Searches, and Bookmark Information. Below this is a file browser pane showing files like 'ClassicVisaFern.gif', 'CRACK_ME', and 'Dear Sweetie.doc'. The main workspace has several tabs: 'File Content' (selected), 'Hex', 'Text', 'Filtered', and 'Natural'. A context menu is open over a Visa card image, with options like Lock, Add..., Remove, Save, Save All Layouts, Restore, and Reset To Default. At the bottom, a status bar displays 'Loaded: 34 | Filtered: 34 | Total: 34 | Highlighted: 1 | Checked: 0' and the path 'Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/root/Users/Wes Mantooth/Documents/ClassicVisaFern.qif'.

- Users can create their own tabs
- Layout settings can be saved

Tabs and Panes

Screenshot of a digital forensic tool interface illustrating tabs and panes.

The interface includes the following components:

- File List:** A pane on the left showing file navigation and properties. It displays items like "App", "be", "Ca", "Ch", "Cl", "CRACK_ME", and "Dear Sweetie.doc".
- File Content:** A central pane showing the content of a selected file, specifically a Visa card image titled "Classic Card".
- Properties:** A sub-pane under "File List" showing file details for selected items.
- Hex Value Interpreter:** A sub-pane under "File List" showing hex values for selected items.
- thumbnails:** A sub-pane under "File List" showing thumbnails for selected items.
- Progress Window...:** A sub-pane under "File List" showing progress for selected items.
- File List Filter:** A toolbar at the top of the "File List" pane.
- View:** A menu bar item that has been expanded, showing options like "Lock", "Add...", "Remove", "Save", "Save All Layouts", "Restore", and "Reset To Default".
- File Content Filter:** A toolbar at the top of the "File Content" pane with buttons for "Hex", "Text", "Filtered", and "Natural".
- File Content Tab:** A tab bar at the top of the "File Content" pane with tabs for "File Content", "Hex", "Text", "Filtered", and "Natural".
- File Content Data:** A large pane displaying the content of the selected file, showing a Visa card image with the number 7700 1234 5678 and expiration date 00/00.
- File Content Statistics:** A table below the image showing file statistics for the selected item.
- File Content Filter:** A toolbar at the bottom of the "File Content" pane with buttons for "Default", "Media", and "Web".
- Status Bar:** A bar at the bottom showing "Loaded: 34", "Filtered: 34", "Total: 34", "Highlighted: 1", "Checked: 0", and "Explore Tab Filter: [None]".
- Address Bar:** A bar at the very bottom showing the path "Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/ClassicVisaFern.qif".

Case Examiner Interface

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

User Guide Case Folder About

Explore Overview Email Graphics Bookmarks Live Search

Evidence Items

Hex Text Filtered Natural

The RETURN OF THE KING

Thank you. Thank you very much.

IT'S NOT WHAT I EXPECTED.

Default Media Web

File List

Normal Display Time Zone: W. Europe Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
CompObj		3842		precious.E01/Partition 1...	OLE Str...	n/a	106 B	55B245...	AE31B...	6F1EC...	n/a	n/a	n/a
CompObj		3855		precious.E01/Partition 1...	OLE Str...	n/a	110 B	82C9B...	4F88B2...	2CE9A...	n/a	n/a	n/a
CompObj		3901		precious.E01/Partition 1...	OLE Str...	n/a	110 B	82C9B...	4F88B2...	2CE9A...	n/a	n/a	n/a
CompObj		3950		precious.E01/Partition 1...	OLE Str...	n/a	106 B	9AE6B...	170C3...	C8B91...	n/a	n/a	n/a
CompObj		4103		precious.E01/Partition 1...	OLE Str...	n/a	106 B	55B245...	AE31B...	6F1EC...	n/a	n/a	n/a
CompObj		4283		precious.E01/Partition 1...	OLE Str...	n/a	106 B	9AE6B...	170C3...	C8B91...	n/a	n/a	n/a
CompObj		4981		precious.E01/Partition 1...	OLE Str...	n/a	106 B	55B245...	AE31B...	6F1EC...	n/a	n/a	n/a
CompObj		7092		precious.E01/Partition 1...	OLE Str...	n/a	106 B	55B245...	AE31B...	6F1EC...	n/a	n/a	n/a

Loaded: 5 015 Filtered: 5 015 Total: 5 015 Highlighted: 0 Checked: 208 Total LSize: 247,3 MB

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

Ready Explore Tab Filter: [None]

Toolbars

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...  

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Evidence Items File Content

Hex Text Filtered Natural

Default Media Web

File List

Normal Display Time Zone: W. Europe Daylight Time (From local machine)

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
rotk_teaser_poster_tit...		2954	gif	precious.E01/Partition 1...	GIF	1536 B	1137 B	1F8B5E...	FABCD...	569C0...	2005-01-01 19:...	2004-12-31 06:...	2005-01-06 22:...
rotk_theatrical_poster_...		2794	gif	precious.E01/Partition 1...	GIF	1024 B	900 B	415D6...	4BEE34...	312D2...	2005-01-01 19:...	2004-12-31 06:...	2005-01-06 22:...
rotkcomic.exif.html		5126	html	precious.E01/Partition 1...	HTML	n/a	n/a				n/a		n/a
rotkcomic.jpg		3071	jpg	precious.E01/Partition 1...	JPEG E...	72,00 KB	71,95 KB	A1367...	FDC98...	DAC4A...	2005-01-01 19:...	2005-01-01 19:...	2004-12-21 19:...
rotkexclusive[1].gif		2950	gif	precious.E01/Partition 1...	GIF	1024 B	1008 B	F93952...	CC2C6...	306456...	2005-01-01 19:...	2004-12-31 06:...	2005-01-06 22:...
RP27		3675		precious.E01/Partition 1...	Folder	152 B	152 B				2005-01-01 19:...	2004-12-30 04:...	2005-01-01 19:...
RP28		3695		precious.E01/Partition 1...	Folder	48 B	48 B				2005-01-01 19:...	2004-12-30 04:...	2005-01-01 19:...
RP29		3696		precious.E01/Partition 1...	Folder	48 B	48 B				2005-01-01 19:...	2004-12-30 04:...	2005-01-01 19:...

Loaded: 5 015 Filtered: 5 015 Total: 5 015 Highlighted: 1 Checked: 208 Total LSize: 247,3 MB

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

Ready Explore Tab Filter: [None]

The File Visualization Pane

File Visualization

fredag, december 31, 2004 lördag, januari 1, 2005

Press this button in the File List pane

2004-12-31 - 2005-01-01

Full timespan: December 31, 2004 - January 02, 2005 Log Linear Time Line View: Basic Detailed Created Bars Line

Metrics: Count

Extensions Distribution

Extension	Amount
jpg	40
<none>	37
db	20
Ink	11
<missing?>	7
doc	5
url	4
ini	3
zip	3
htm	2
log	2
mid	2
xls	2
gif	1
avi	1
skr	1
ett	1
xsl	1
xml	1
ldif	1
bit	1
mpeg	1
pkz	1

Legend

- jpg (40)
- <none> (37)
- db (20)
- Ink (11)
- <missing?> (7)

Categories Distribution Chart

Category	Percentage
Multimedia	8,78%
Other Encryption Files	2,71%
Folders	0,68%
OS/File System Files	15,54%
Unknown Types	19,59%
Graphics	12,16%
?	7,43%
Text	25,68%

Legend

- Multimedia
- Other Encryption Files
- Folders
- OS/File System Files
- Unknown Types
- Graphics
- ?
- Text

Drag a column header and drop it here to group by that column

Item#	Name	Category	Date	Size	Extension
2097	happy.mpeg	MPEG 2.0 Video	December 31, 2004	416 KB	mpeg
2092	039.avi	Riff Avi	December 31, 2004	760,25 KB	avi
1987	\$130	Index Allocation	January 01, 2005	8 KB	?
1988	23_1_b.JPG	JPEG	January 01, 2005	17,79 KB	jpg
1989	Addressbook.ldif	Unknown	January 01, 2005	1,67 KB	ldif
1990	Arts and Entertainment - Sword	Text	January 01, 2005	862 bytes	log
1993	desktop.ini	Zero Length File	January 01, 2005	0 bytes	ini

File Count : 148

Select All

Select None

Mark Selected Items

Column Sorting & Type-Down

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: lecture -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: Actual Files Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Evidence Items

File Content

Hex Text Filtered Natural

Default Media Web

File List

Name Label Item # Ext Path Category P-Size L-Size MD5 SHA1 SHA256 Created

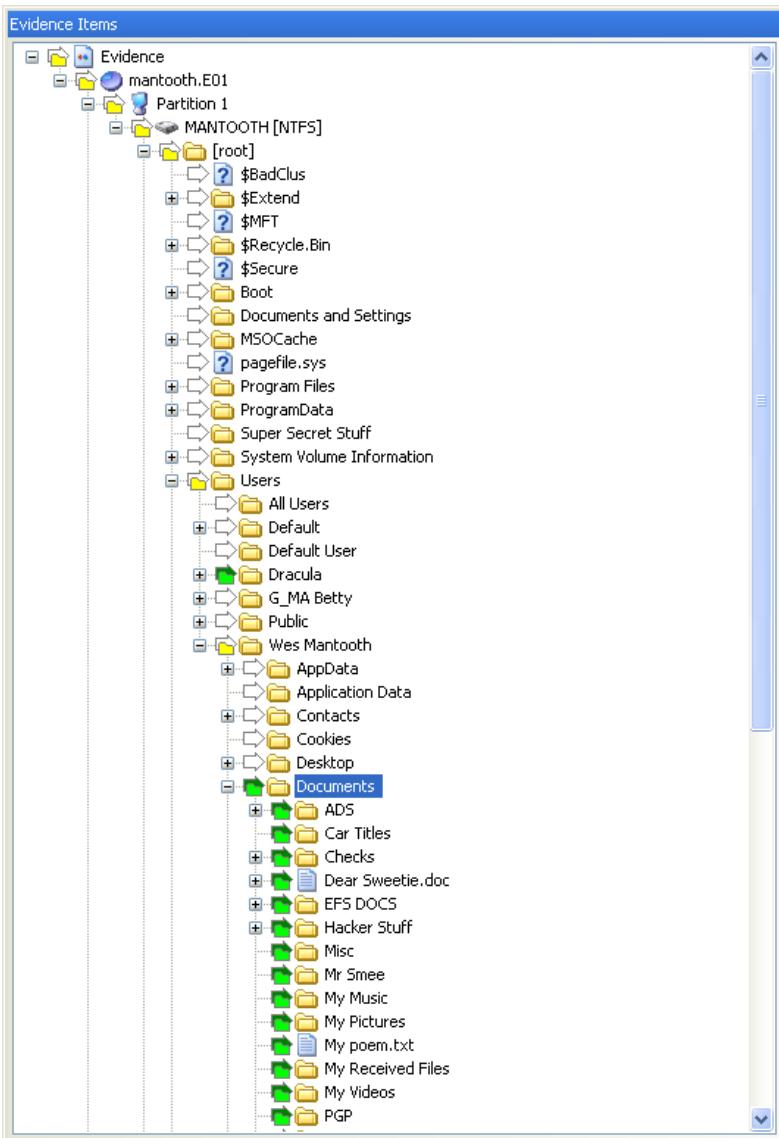
	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
	10-1 Graphics		1217		diskette-usb.E01/EVIDE...	Folder	1024 B	1024 B				2003-10-01
	Access Data Document....		1230	doc	diskette-usb.E01/EVIDE...	Microso...	19,50 KB	19,50 KB		85		2003-09-11
	Access Document.doc		1231	doc	diskette-usb.E01/EVIDE...	Microso...	19,50 KB	19,50 KB		B4		2003-09-11
	AMEX TEST.txt		1195	txt	diskette-usb.E01/EVIDE...	Text	20,50 KB	20,49 KB		53		2003-09-28
	CAH0SV9H.HTM		1168	htm	diskette-usb.E01/EVIDE...	HTML	37,00 KB	36,65 KB	A82E9...	8A5BB...	C2E02...	2003-09-28
	Cartoon Beer.jpg		1218	jpg	diskette-usb.E01/EVIDE...	JPEG	3584 B	3325 B	E321B...	71A21...	16B9D...	2003-10-01
	CDQNKPYN		1182		diskette-usb.E01/EVIDE...	Folder	1024 B	1024 B				2003-09-28

Loaded: 105 Filtered: 105 Total: 176 Highlighted: 1 Checked: 0 Total LSize: 983,9 KB

diskette-usb.E01/EVIDENCE [FAT12]/[root]/TIF Netmail/Y1UVYTMV/CAH0SV9H.HTM

Ready Explore Tab Filter: [None]

Quick Picks



- Allows user selectable focus
- Icons show selected status
- Can be suspended via the Quickpicks suspend button located on the toolbar

Overview Tab

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Case Overview

Evidence Groups (5 015 / 5 015)
+ Ungrouped (5 015 / 5 015)
File Items
+ Checked Items (208 / 208)
Evidence Items (1 / 1)
+ Unchecked Items (4 807 / 4 807)
File Extension (2 049 / 2 049)
File Category (5 015 / 5 015)
File Status
Email Status
+ Email Attachments (35 / 35)
Email Related Items (From Email) (288 / 288)
+ Email Reply (34 / 34)
Forwarded Email (4 / 4)
Labels (0 / 0)
Bookmarks
+ hjo
+ Message with attachment
+ Suspect Mail
+ Shared

File Content Hex Text Filtered Natural

Thanks for the great info!

From: "Frodo Baggins" <Frodobaggi@comcast.net>
To: <mark@accessdata.com>
Subject: Thanks for the great info!
Sent: Fri, 10 Dec 2004 11:10:25 -0700

Mark, just wanted to drop you a line and let you know how much I learned in the Internet class last week. I am looking forward to retirement here in the shire. Sam and I are starting a consulting company and specializing in Forensic Computer Analysis.

If you ever need anything, please don't hesitate to call.

My company is called Hobabytes Consulting. I don't have phone service here yet but you can always email me here. Thanks again.

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
Talk to Pippin about his ba...		5530		precious.E01/Partition 1...	Task	n/a	0 B				2004-12-30 ...		2004-12-30 00:...
Tasks		5527		precious.E01/Partition 1...	Email F...	n/a	n/a				n/a		n/a
Templates.msf		2124	msf	precious.E01/Partition 1...	Netsca...	1536 B	1349 B	D5DF7...	6EF691...	468BD...	2005-01-01 ...	2005-01-...	2004-12-30 10:...
text2.zip Finished 12/21/...		5311		precious.E01/Partition 1...	Email O...	n/a	2070 B				n/a		n/a
Thanks for the great info!		5242	<missin...	precious.E01/Partition 1...	Text In...	n/a	2439 B	DFE8A...	BDF79...	E913D...	n/a		n/a

Loaded: 208 Filtered: 208 Total: 208 Highlighted: 1 Checked: 208 Total LSize: 3138 KB

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/Local Settings/Application Data/Identities/{93DBE93F-5D5C-4B70-BF...}/Sent Items.dbx»Thanks for the great info! Ready | Overview Tab Filter: [None]

Overview Tab

Files are identified by header, not by extension

File Edit View Evidence Filter Tools Help

Filter: - unfiltered - Define... |

Explore Overview Email Graphics Bookmarks Live Search Index Search

Case Overview

File Items

- + ext File Extension (1,411 / 1,411)
- File Category (3,525 / 3,525)
 - + Archives (15 / 15)
 - + Databases (3 / 3)
 - + Documents (672 / 672)
 - + Email (93 / 93)
 - + Executable (10 / 10)
 - + Folders (781 / 781)
 - + Graphics (752 / 752)
 - + Raster Graphics (736 / 736)
 - + AOL Art (1 / 1)
 - + Bitmap (105 / 105)
 - + GIF (156 / 156)
 - + JPEG (410 / 410) **Red Box**
 - + JPEG EXIF (23 / 23)
 - + PNG (35 / 35)
 - + Windows Icon (6 / 6)
 - + Vector Graphics (16 / 16)
 - + Internet/Chat Files (508 / 508)

Hex Text Filtered Natural

0000 ff d8 ff e0 00 10 4a 46-49 46 00 01 02 00 00 64 **ÿþÿà** JFIF.....d
0010 00 64 00 00 ff ec 00 11-44 75 63 6b 79 00 01 00 ..d..ÿi..Ducky...
0020 04 00 00 00 1e 00 00 ff-ee 00 21 41 64 6f 62 65ÿi..!Adobe
0030 00 64 c0 00 00 00 01 03-00 10 03 02 03 06 00 00 ..dÀ.....
0040 06 78 00 00 0d 29 00 00-19 42 ff db 00 84 00 10 ..x...)..ByÙ...
0050 0b 0b 0b 0b 10 0c 0c-10 17 0f 0d 0f 17 1b 14
0060 10 10 14 1b 1f 17 17 17-17 17 1f 1e 17 1a 1a 1a
0070 1a 17 1e 23 27 25-27 25 1e 2f 2f 33 33 2f 2f#%!%#/33//
0080 40 40 40 40 40 40 40-40 40 40 40 40 40 40 40 01 00000000000000000000
0090 11 0f 0f 11 13 11 15 12-12 15 14 11 14 11 14 1a
00a0 14 16 16 14 1a 26 1a 1a-1c 1a 1a 26 30 23 1e 1e&.....&0#..
00b0 1e 1e 23 30 2b 2e 27 27-27 2e 2b 35 35 30 30 35 ..#0+.!!!.+55005
00c0 35 40 40 3f 40 40 40-40 40 40 40 40 40 40 40 40 500?00000000000000
00d0 ff c2 00 11 08 00 b9 00-c8 03 01 22 00 02 11 01 ÿÀ.....È....
00e0 03 11 01 ff c4 00 ae 00-00 02 03 01 01 01 00 00 ..ÿÀ..@.....
00f0 00 00 00 00 00 00 00-04 05 02 03 06 00 01 07 ..
Cursor pos = 0; clus = 62655; log sec = 62655; phy sec = 62718

File Content Properties Hex Interpreter

File List

	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed
<input type="checkbox"/>	\$R2M7A26.jpg		1246	jpg	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg	JPEG	14.00 KB	13.82 KB	489E96...	870A9...	92D29...	7/26/2007 6:27...	7/26/2007 6:27...
<input type="checkbox"/>	\$R9HZO20.jpg		1248	jpg	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg	JPEG	6656 B	6468 B	6FB3C...	65B5D...	A0432...	7/26/2007 6:27...	7/26/2007 6:27...
<input type="checkbox"/>	\$RJQVPHB.jpg		1251	jpg	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg	JPEG	11.50 KB	11.30 KB	395FE2...	F98320...	B4FB9E...	7/26/2007 6:27...	7/26/2007 6:27...
<input type="checkbox"/>	07-09-very-old-man.jpg		1701	jpg	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg	JPEG	42.00 KB	41.72 KB	DFD36...	D3B25...	129482...	7/25/2007 6:41...	7/25/2007 6:41...
<input type="checkbox"/>	Ocb[1].jpg		3247	jpg	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg	JPEG	481 B	481 B	347176...	A4204...	CCB55...	7/12/2007 6:16...	7/12/2007 6:16...
<input type="checkbox"/>	Ocm[1].jpg		3093	jpg	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg	JPEG	297 B	297 B	9A181...	73EC9...	2AE54...	7/12/2007 6:16...	7/12/2007 6:16...
<input type="checkbox"/>	Oct[1].jpg		3248	jpg	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg	JPEG	455 B	455 B	32B718...	B73E1E...	EBF5F6...	7/12/2007 6:16...	7/12/2007 6:16...
<input type="checkbox"/>	Obf[1].ico		3018	ico	Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg	JPEG	368 B	368 B	64A0F...	A9C3D...	291CE...	7/12/2007 6:16...	7/12/2007 6:16...

Loaded: 410 Filtered: 410 Total: 410 Highlighted: 1 Checked: 0

Overview Tab Filter: [None]

Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$R9HZO20.jpg

Viewing Options

The screenshot shows the FTK File Recovery software interface. The main window has a menu bar with File, Edit, View, Evidence, Filter, Tools, and Help. Below the menu is a toolbar with icons for search, filter, and file operations. The top navigation bar includes tabs for Explore, Overview, Email, Graphics, Bookmarks, Live Search, and Index Search, with Overview selected.

The left pane displays a tree view of file types: Documents (2,001 / 2,001), Microsoft Documents (40 / 40), Microsoft Word (39 / 39), Other Documents (1,430 / 1,430), WordPerfect (4 / 4), Email (158 / 158), Executable (27 / 27), Folders (1,539 / 1,539), Graphics (2,897 / 2,897), Internet/Chat Files (5,822 / 5,822), Mobile Phone Data (0 / 0), Multimedia (68 / 68), OS/File System Files (546 / 546), Other Encryption Files (29 / 29), and Other Known Types (150 / 150).

The central pane is titled "File Content" and contains four tabs: Hex, Text, Filtered, and Natural. The Hex tab shows a hex dump of a file, with the first few lines being:

```
0980 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  
0990 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  
09a0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  
09b0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  
09c0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  
09d0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  
09e0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  
09f0 00 00 00 00 00 00 00-00 00 00 00 00 00 00 00 00  
0a00 4c 61 67 6f 73 2c 20 4e-69 67 65 72 69 61 2e 0b Lagos, Nigeria..  
0a10 41 74 74 65 6e 74 69 6f-6e 3a 20 54 68 65 20 50 Attention: The P  
0a20 72 65 73 69 64 65 6e 74-2f 43 45 4f 20 0d 44 65 resident/CEO .De  
0a30 61 72 20 53 69 72 2c 20-0d 07 13 20 49 4e 43 4c ar Sir, ... INCL  
0a40 55 44 45 50 49 43 54 55-52 45 20 22 68 74 74 70 UDEPICTURE "http  
0a50 3a 2f 77 77 77 2e 61-70 70 6c 69 65 64 6c 61 ://www.appliedla  
0a60 6e 67 75 61 67 65 2e 63-6f 6d 2f 66 6c 61 67 73 nguage.com/flags  
0a70 5f 6f 66 5f 74 68 65 5f-77 6f 72 6c 64 2f 6c 61 _of_the_world/la  
0a80 72 67 65 5f 66 6c 61 67-5f 6f 66 5f 6e 69 67 65 rge_flag_of_nige  
0a90 72 69 61 2e 67 69 66 22-20 5c 2a 20 4d 45 52 47 ria.gif" \* MERG  
0aa0 45 46 4f 52 4d 41 54 49-4e 45 54 20 14 01 15 07 EFORMATINET ....  
0ab0 07 43 6f 6e 66 69 64 65-6e 74 69 61 6c 20 42 75 .Confidential Bu  
0ac0 73 69 6e 65 73 73 20 50-72 6f 70 6f 73 61 6c 20 siness Proposal
```

The bottom status bar shows "Cursor pos = 0".

The bottom pane is titled "File List" and shows a table of files with columns: Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Accessed. The table includes rows for "Astral.doc", "Confidential Business Le...", "Dear Sweetie.doc", and others.

At the bottom, there are status indicators: "Loaded: 23", "Filtered: 23", "Total: 23", "Highlighted: 1", "Checked: 0", and "Ready". The status bar also shows the full path: "Washer 17.E01/Partition 1/WASHER [NTFS]/root/Documents and Settings/Administrator/Local Settings/Application Data/Identities/{6B6FD541-F2AF-4EFB-AF50-EC531B...}/Confidential Business Letter.doc".

Viewing File/Folder Properties

The screenshot displays a digital forensic analysis tool with the following interface elements:

- Menu Bar:** File, Edit, View, Evidence, Filter, Tools, Help.
- Toolbar:** Includes icons for Filter, Define..., Delete, Copy, Paste, and others.
- Tab Bar:** Explore, Overview, Email, Graphics, Bookmarks, Live Search, Index Search. The "Overview" tab is selected.
- Case Overview:** A tree view of file types and counts:
 - Documents (2,001 / 2,001)
 - Adobe Documents (5 / 5)
 - HTML and XML (518 / 518)
 - Lotus Documents (4 / 4)
 - Microsoft Documents (40 / 40)
 - Microsoft RTF (1 / 1)
 - Microsoft Word (39 / 39)
 - Microsoft Word 2.0 (4 / 4)
 - Microsoft Word 2000 (3)
 - Microsoft Word 2002 (1)
 - Microsoft Word 2003 (2)
 - Microsoft Word 6.0 (8 / 8)
 - Other Documents (1,430 / 1,430)
 - Email (158 / 158)
 - WordPerfect (4 / 4)
 - Executable (27 / 27)
 - Folders (1,539 / 1,539)
 - Graphics (2,897 / 2,897)
 - Internet/Chat Files (5,822 / 5,822)
 - Mobile Phone Data (0 / 0)
 - Multimedia (68 / 68)
 - OS/File System Files (546 / 546)
 - Other Encryption Files (29 / 29)
 - Other Known Types (150 / 150)
 - Properties Panel:** Shows detailed information for a selected file, "Confidential Business Letter.doc".

Name	Confidential Business Letter.doc
Item Number	15274
File Type	Microsoft Word 2003
Path	Washer 17.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings
General Info	
File Size	
Physical Size	40,640 bytes (39.69 KB)
Logical Size	29,696 bytes (29.00 KB)
File Dates	
Date Created	n/a
Date Accessed	n/a
Date Modified	n/a
File Attributes	
General	
Actual File	False
Duplicate File	Secondary
From Email	True
File Type	OLE Archive
 - File List:** A table showing a list of files with columns: Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Accessed.

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed
Astral.doc		1222	doc	Mantooth32.E01/Partiti...	Microso...	38.00 KB	38.00 KB	7CED6...	59B829...	7850A...	2/12/2008 4:53...	2/12/2008 4:53...
Confidential Business Le...		3789	doc	Mantooth32.E01/Partiti...	Microso...	n/a	29.15 KB	8C778...	3D9EC...	1D554...	n/a	n/a
Confidential Business Le...		15274	doc	Washer 17.E01/Partiti...	Microso...	39.69 KB	29.00 KB	8C778...	3D9EC...	1D554...	n/a	n/a
Dear Sweetie.doc		1606	doc	Mantooth32.E01/Partiti...	Microso...	63.50 KB	63.50 KB	954418...	B79149...	F5393...	7/12/2007 4:51...	7/13/2007 10:41...
 - Status Bar:** Loaded: 23, Filtered: 23, Total: 23, Highlighted: 1, Checked: 0.
 - Bottom Status:** Ready, Overview Tab Filter: [None], Washer 17.E01/Partition 1/WASHER [NTFS]/[root]/Documents and Settings/Administrator/Local Settings/Application Data/Identities/{6B6FD541-F2AF-4EFB-AF50-EC531B...}/Confidential Business Letter.doc

Hex View Settings

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: lecture -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: Actual Files Filter Manager...  

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Evidence Items

Hex Text Filtered Natural

diskette-usb.E01

EVIDENCE [FAT12]

[root]

10-1 Graphics DT Search Stuff Recent Recycler Registry File Sagan Alert TIF Netmail Zip Files

0000 3C 73 63 72 69 70 74 20-6C 61 6E 67 75 61 67 65 <script language=JavaScript>

0010 3D 4A 61 76 61 53 63 72-69 70 74 3E 0A 20 20 20 document.co

0020 20 20 20 20 64 6F 63-75 6D 65 6E 74 2E 63 6F okie = "JSEnable

0030 6F 6B 69 65 20 3D 20 22-4A 53 45 6E 61 62 6C 65 d=1" . </scr

0040 64 3D 31 22 20 20 0A 20-20 20 20 3C 2F 73 63 72 ipt>..... <

0050 69 70 74 3E 0A 0A 0A-0A 0A 0A 0A 0A 0A 20 3C html> . <head>

0060 68 74 6D 6C 3E 0A 20 20-20 20 3C 68 65 61 64 3E 51 . <title>MapQuest: Driving Di

0070 0A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 69 uest: Driving Di

0080 75 6

Select all Ctrl+A

Copy text Ctrl+C

Copy hex Ctrl+H

Copy Unicode

Copy raw data

Save selection...

Show decimal offsets

Show text only

Fit to window

Save current settings

Go to offset... Ctrl+G

Save selection as carved file...

File List

Name	Label	Item #
10-1 Graphics		1217
Access Data Document....		1230
Access Document.doc		1231
AMEX TEST.txt		1195
CAH0SV9H.HTM		1168
Cartoon Beer.jpg		1218
CDQNKPYN		1182

Loaded: 105 Filtered: 105 Total: 176

diskette-usb.E01/EVIDENCE [FAT12]/[root]/TIF Netmail/Y1UVYTMV/CAH0SV9H.HTM

Ready Explore Tab Filter: [None]

	L-Size	MD5	SHA1	SHA256	Created
B	1024 B				2003-10-01
) KB	19,50 KB	652F15...	21856F...	9FA62...	2003-09-11
) KB	19,50 KB	027A5...	9AB4E...	324D2...	2003-09-11
) KB	20,49 KB	155230...	7953C...	1EC8E...	2003-09-28
) KB	36,65 KB	A82E9...	8A5BB...	C2E02...	2003-09-28
B	3325 B	E321B...	71A21...	16B9D...	2003-10-01
B	1024 B				2003-09-28

Hex Interpreter

Screenshot of a digital forensic tool interface showing the "Hex Interpreter" tab selected.

The "Hex Interpreter" pane displays a table of file items with their types, sizes, and values:

Type	Size	Value
signed integer	1-8	128,306,648,377,170,000
unsigned integer	1-8	128,306,648,377,170,000
FILETIME (Stored)	8	8/4/2007 1:33:57 AM
FILETIME (As Local)	8	8/3/2007 7:33:57 PM
DOS date	2	-
DOS time	2	-
DOS date/time	4	-
time_t (Stored)	4	-
time_t (As Local)	4	-
Unicode string	2 +	IIIJ

Below the table, there are options for "Byte order:" with radio buttons for "Little endian" (selected) and "Big endian".

The "File Content" tab is also visible in the bottom navigation bar.

The "File List" pane at the bottom shows a table of four entries, all labeled "INFO2".

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed
INFO2		5424	<missin...	Washer 17.E01/Partitio...	Recycl...	2048 B	1620 B	A5F45...	1D6F3...	87761E...	8/3/2007 6:33:...	8/3/2007
INFO2		5427	<missin...	Washer 17.E01/Partitio...	Recycl...	1024 B	820 B	FB4B0...	244FC...	5535C...	8/3/2007 6:40:...	8/3/2007
INFO2		5432	<missin...	Washer 17.E01/Partitio...	Recycl...	2560 B	2420 B	584428...	8D098...	5BF20B...	8/3/2007 6:39:...	8/3/2007
INFO2		5436	<missin...	Washer 17.E01/Partitio...	Recycl...	2048 B	1620 B	FD4F8...	6D946...	F40009...	8/3/2007 6:35:...	8/3/2007

At the bottom status bar, the text reads: "Ready Overview Tab Filter: [None] Washer 17.E01/Partition 1/WASHER [NTFS]/[root]/RECYCLER/S-1-5-21-1177238915-616249376-839522115-1003/INFO2".

Drive Free Space

The screenshot shows a digital forensic analysis software interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, and Help. Below the menu is a toolbar with various icons. The main window has tabs for Explore, Overview, Email, Graphics, Bookmarks, Live Search, and Index Search, with Index Search selected.

The left pane displays a tree view of the "Case Overview" containing various file types and their counts, such as Executable (10 / 10), Folders (781 / 781), Graphics (752 / 752), Internet/Chat Files (508 / 508), Mobile Phone Data (0 / 0), Multimedia (44 / 44), OS/File System Files (252 / 252), Other Encryption Files (17 / 17), Other Known Types (91 / 91), and Presentations (2 / 2). A red box highlights the "Slack/Free Space (92 / 92)" category, which further branches into File System Slack (1 / 1), Slack Space (44 / 44), Unallocated Space (46 / 46), and Unpartitioned Space (1 / 1).

The central pane is titled "File Content" and contains four tabs: Hex, Text, Filtered, and Natural. The Hex tab shows a hex dump of the data starting at address 0000. The Natural tab shows the corresponding ASCII representation. A status bar at the bottom of this pane indicates: Cursor pos = 0; clus = 6350; log sec = 6350; phy sec = 6413.

The bottom pane is titled "File List" and displays a table of files. The columns include Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Access. One row in the list is highlighted with a red box and is labeled "006350".

At the bottom of the interface, there are status indicators: Loaded: 46, Filtered: 46, Total: 46, Highlighted: 1, Checked: 0, and an Overview Tab Filter: [None]. The footer also shows the path: Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[unallocated space]/006350.

Email Tab

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Email Items

Email Archives

- baggifrodo
 - [deleted]
 - [unallocated space]
 - baggifrodo
 - Away Messages
 - Buddy Preferences
 - Download Manager
 - Extra
 - Favorite Places
 - JunkFolder
 - Mail
 - Incoming/Saved Mail

List all descendants

File Content

Hex Text Filtered Natural

From: swaters@accessdata.com
To: Baggifrodo@aol.com
Subject: RE: Southeast Cybercrime Summit
Sent: 4/29/2005 10:12:08 A.M. Mountain Standard Time
Sent: 2005-04-29 17:12:08 +00:00

I would highly recommend that you participate in the Southeast Cybercrime Summit. They have labs and lectures lead by

File Content Properties Hex Interpreter

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/All Users/.../baggifrodo/baggifrodo/Mail/Incoming/Saved Mail/4/29/2005 swaters@accessda RE: Southeast Cybercrime Summit Ready

Email Tab Filter: Email Files and Attachments

File List

Subject	Name	To	From	CC	BCC	Submit ...	Deliver...	Unread	Unsent	Has Att...	Created
frodobaggi, ge...	1/2/2005 eBay...	baggir...	eBay@...			2005-0...	2005-0...	False	False	n/a	
You want it, eB...	12/23/2004 eB...	baggir...	eBay@...			2004-1...	2004-1...	False	False	n/a	
frodobaggi sen...	4/29/2005 bag...	samwiz...	baggir...			2005-0...	2005-0...	False	False	n/a	
RE: HELP!	4/29/2005 jpar...	Baggir...	jparry...			2005-0...	2005-0...	False	False	n/a	
RE: Southeast ...	4/29/2005 swa...	Baggir...	swater...			2005-0...	2005-0...	False	False	n/a	

Loaded: 5 Filtered: 5 Total: 5 Highlighted: 0 Checked: 208 Total LSize: 61,15 KB

Email Attachments

4/29/2005 swaters@accessda RE: Southeast Cybercrime

Graphics Tab

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email **Graphics** Bookmarks Live Search Index Search Volatile

Thumbnails

040102_alfred.jpg 06[1].jpg 0601_main[1].jpg 0601_mainright[1] 0601_ringerad[1] 0601_search[1].jp 0601_top03[1].jp 069F5181d01 0788789848.01.T

Loaded: 1 253 Filtered: 1 253 Total: 5 015 Highlighted: 1 Checked: 208 Total LSize: 5467 KB Show Tooltip

Evidence Items

- Evidence
- precious.E01
- Partition 1
- The Precious [NTFS]
- [orphan]
- [root]
- Unallocated erased

File Content

Hex Text Filtered Natural

File Content Properties Hex Interpreter

File List

Normal Display Time Zone: W. Europe Daylight Time (From local)

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
040_fp0993_a[1].jpg		2682	jpg	precious.E01/Partition 1...	JPEG	2048 B	1791 B	F4BEEB...	19B318...	AA5F1...	2005-01-01
040102_alfred.jpg		3038	jpg	precious.E01/Partition 1...	JPEG	20,00 KB	19,52 KB	E56408...	85EDE...	E1BB2...	2005-01-01

Loaded: 1 253 Filtered: 1 253 Total: 5 015 Highlighted: 1 Checked: 208 Total LSize: 5467 KB

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/My Pictures/040102_alfred.jpg

Ready Graphics Tab Filter: Graphic Files

Bookmarks Tab

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager... |

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Bookmarks

- Bookmarks
 - hjo
 - Message with attachment
 - Suspect Mail
 - Shared

Bookmark Information

Bookmark Name: Message with attachment Creator Name: hjo

Bookmark Comment:

Supplementary Files:

To: samwizgamgee@hotmail.com
Subject: Possible Job!!!
Sent: 1/2/2005
Sent: 2005-01-02 14:19:05 +00:00

I got a call today from the Regional Forensic Lab in Isengard. They are starting a new computer forensic section and want to know if we want to join in? What do you think? This might be a real opportunity. The only down side is that I hear Gandalf is going to head the department. If my memory serves me, he can be a real pain to work for. Remember how he used to push us around and talk down to us like he was some kind of all knowing wizard or something. Maybe he has changed now that he is Whitehat.

File Content Properties Hex Interpreter

File List

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size
1/2/2005 samwizgam...		5341		precious.E01/Partition 1...	Message	n/a	3263 B

Loaded: 1 Filtered: 1 Total: 1 Highlighted: 1 Checked: 208 Total LSize: 3263 B

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/All Users/Applicat.../baggifrodo»baggifrodo»Mail»Mail You've Sent»1/2/2005 samwizgamgee@hotmail.com Possible Job!!!

Ready Bookmarks Tab Filter: [None]

Live Search Tab

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered - Filter Manager... |

Explore Overview Email Graphics Bookmarks **Live Search** Index Search Volatile

Text **Pattern** Hex

ANSI Unicode Case Sensitive

Search Terms Type Code Pages

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

File Content

Hex Text Filtered Natural

02c90	72 20 49 6E 73 74 72 75-63 74 6F 72 0D 0A 3E 0D	r Instructor-->
02ca0	0A 3E 20 41 63 63 65 73-73 44 61 74 61 0D 0A 3E	-> AccessData->
02cb0	0D 0A 3E 20 38 30 31 2D-33 37 37 2D 35 34 31 30	--> 801-377-5410
02cc0	20 78 38 34 33 0D 0A 3E-0D 0A 3E 20 6D 61 72 6B	x843-->--> mark
02cd0	40 61 63 63 65 73 73 64-61 74 61 2E 63 6F 6D 0D	@accessdata.com->-->-->-->
02ce0	0A 3E 0D 0A 3E 20 20 0D-0A 3E 0D 0A 3E 20 2D 2D	-->-->-->-->-->--

Sel start = 11444, len = 12; clus = 210606; log sec = 210606; phy sec = 210703

File Content Properties Hex Interpreter

File List

<input checked="" type="checkbox"/>	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SH
<input checked="" type="checkbox"/>	RE: Training		5500		precious.E01\Partition 1...	Message	n/a	2337 B		
<input checked="" type="checkbox"/>	RE: Training [<194F963...		4213	<missin...	precious.E01\Partition 1...	TextIn...	n/a	3132 B	B05EF5...	68:
<input checked="" type="checkbox"/>	Samwise Gamgee		5515		precious.E01\Partition 1...	Contact	n/a	0 B		
<input checked="" type="checkbox"/>	Saved Mail		2119	<missin...	precious.E01\Partition 1...	MBox	293,5 KB	293,3 KB	58C6B...	F20:
<input checked="" type="checkbox"/>	Sent		2121	<missin...	precious.E01\Partition 1...	MBox	100,0 KB	99,86 KB	287AD...	B20:

Loaded: 23 Filtered: 23 Total: 23 Highlighted: 1 Checked: 208 Total LSize: 737,0 KB

precious.E01\Partition 1\The Precious [NTFS]\[root]\Documents and Settings\Frodo Baggins\Application Data\Mozilla\Profiles\default\3x7kf8pq.slt\Mail\Local Folders\Sent

Ready Live Search Tab Filter: [None]

Live Search Results

- Live Search {"((\l<1[\-\.\])?(\|)\l<)d\d\|d[\-\.\])}
- Pattern Query: /((\l<1[\-\.\])?(\|)\l<)d\d/
- Allocated Space -- 49 hit(s) in 23 file(s)
- 6 hit(s) -- Item 2121 [Sent] precious
- Item 2121, Offset 2cb4 (114):
 - Item 2121, Offset 3ed3 (160):
 - Item 2121, Offset 15759 (87):
 - Item 2121, Offset 16828 (92):
 - Item 2121, Offset 177f0 (96):
 - Item 2121, Offset 188bd (10):
- 4 hit(s) -- Item 2119 [Saved Mail]
- 4 hit(s) -- Item 2380 [Inbox.dbx]
- 4 hit(s) -- Item 7307 [entry #017]
- 3 hit(s) -- Item 5329 [4/29/2005]
- 3 hit(s) -- Item 5335 [4/29/2005]
- 2 hit(s) -- Item 2182 [In.mbx] precious
- 2 hit(s) -- Item 4213 [RE: Training]
- 2 hit(s) -- Item 4214 [RE: Thanks]
- 2 hit(s) -- Item 4992 [entry #000]
- 2 hit(s) -- Item 5088 [entry #001]
- 2 hit(s) -- Item 5096 [entry #008]
- 2 hit(s) -- Item 5097 [entry #009]
- 2 hit(s) -- Item 5500 [RE: Training]
- 1 hit(s) -- Item 5330 [4/29/2005]
- 1 hit(s) -- Item 5334 [4/29/2005]
- 1 hit(s) -- Item 5501 [RE: Thanks]
- 1 hit(s) -- Item 5515 [Samwise Ga...]
- 1 hit(s) -- Item 5516 [Bilbo Baggins]
- 1 hit(s) -- Item 5518 [Keith Lockhe...]
- 1 hit(s) -- Item 5519 [Natasha Da...]
- 1 hit(s) -- Item 5520 [Mark String]

Index Search Tab

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: precious -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager... |

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

dtSearch® Index

Terms

killed

Indexed Words	Total Hits
kilinks	1
kill	20
kill3	4
killed	13
killer	2
killing	4
killist	2
kills	1

Search Criteria

Operators And Or Terms All Selected Accumulate Results

Search Terms kill Total Hits 20

File Content

Hex Text **Filtered** Natural

to return, in case the previous stream does not hand context back UNLOCK! let this form close CLOSE! Go to Address Book \$) LOCK! protect us from accidental closure \$Oforce context to return, in case the previous stream does not hand context back UNLOCK! let this form close CLOSE! \$ show form \$ hide form \$ resize form get desired height \$# force kill form with a quick timer \$ force close \$A LOCK: tell parent form "don't kill us", mostly during lose_focus UNLOCK \$ PLUS group / address card direct \$ PLUS group / address card button \$PLUS group / entry expanded & long timer still won't close if you mouse over back or < Next TM

File Content Properties Hex Interpreter

File List

Normal Display Time Zone: W.

Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SH
main.idx		1072	idx	precious.E01\Partition 1...	Unknown	12,50 MB	12,50 MB	F1FAF...	F1...
OnThis.d...		2227	20,50 KB	20,50 KB	D2007	20...

Loaded: 11 Filtered: 11 Total: 11 Highlighted: 1 Checked: 208 Total LSize: 14,27 MB

precious.E01\Partition 1\The Precious [NTFS]\[root]\Documents and Settings\All Users\Application Data\AOL\America Online 9.0\idb\main.idx

Ready Index Search Tab Filter: [None]

Index Search Results

- dtSearch® Indexed Search {Prefilter:(all files) Q}
- Allocated Space -- 20 hit(s) in 11 file(s)
 - Documents -- 3 hit(s) in 2 file(s)
 - + 60% - 2 hit(s) -- Item 3727 [Options...]
 - + 40% - 1 hit(s) -- Item 2013 [AD9143]
 - Internet/Chat Files -- 10 hit(s) in 6 file(s)
 - + 80% - 3 hit(s) -- Item 5967 [entry #0]
 - + 80% - 3 hit(s) -- Item 4096 [entry #0]
 - + 40% - 1 hit(s) -- Item 7215 [entry #0]
 - + 40% - 1 hit(s) -- Item 5969 [entry #0]
 - + 40% - 1 hit(s) -- Item 5965 [entry #0]
 - + 40% - 1 hit(s) -- Item 4074 [entry #0]
 - Other Known Types -- 2 hit(s) in 1 file(s)
 - + 60% - 2 hit(s) -- Item 4101 [WordDo...]
 - Hit #1: applied to the word "kill".
 - Hit #2: o the word "kill". Kill K
 - Unknown Types -- 5 hit(s) in 2 file(s)
 - + 100% - 4 hit(s) -- Item 1072 [main.id...]
 - Hit #1: oad Tool Bounce Tool Kill
 - Hit #2: ose start a 2 second kill ti
 - Hit #3: ired height \$# force kill fc
 - Hit #4: l parent form "don't kill us"
 - Unallocated Space -- 0 hit(s) in 0 file(s)

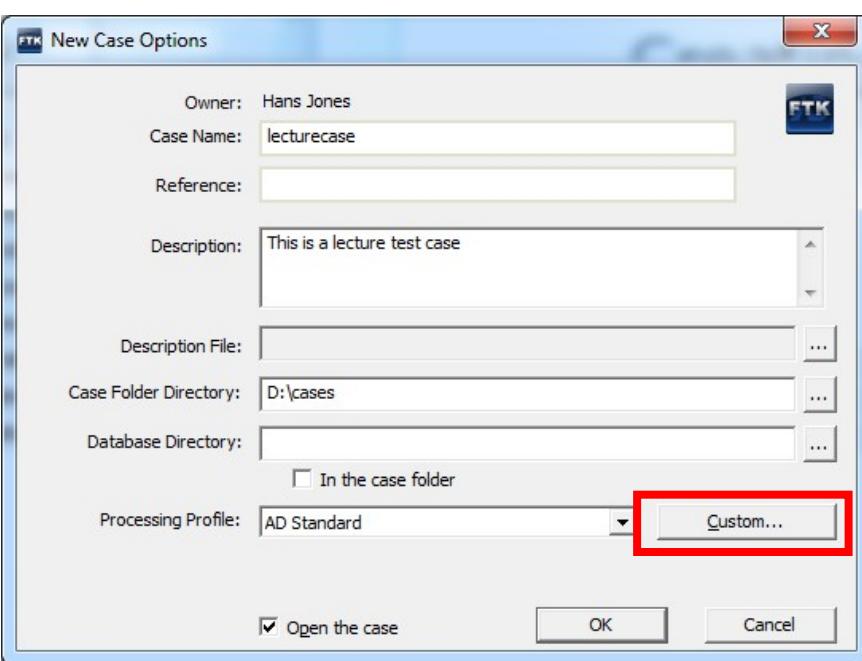
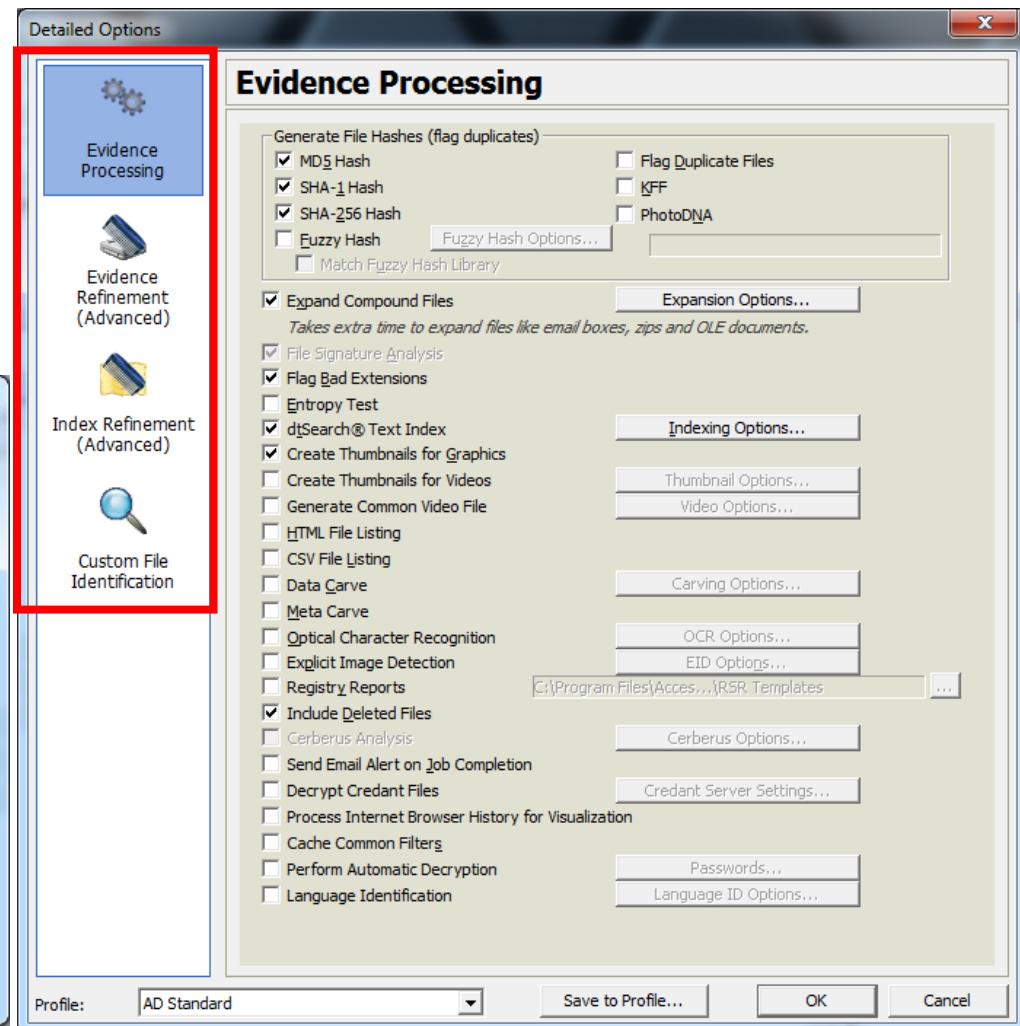
Creating a New Case and Processing Options

- From the Case Manager Interface menu > Case > New

Selections are pre-checked based on case setup.

Can be changed per evidence item later.

Selections can be saved as defaults for future cases.



Refining Case Evidence

- Usually not needed to modify these parameters
- Refine by: Type, Status, Date/Size

The image displays two identical windows titled "Evidence Refinement (Advanced)" side-by-side. Both windows have a blue header bar with the title and a standard Windows-style close button in the top right corner.

Left Window Content:

- Left Sidebar:** Contains icons for "Evidence Processing", "Evidence Refinement (Advanced)" (which is selected and highlighted in blue), and "Index Refinement (Advanced)".
- Main Area:**
 - Top Buttons:** "Refine by File Status/Type" and "Refine by File Date/Size".
 - Inclusion/Exclusion Settings:** A note: "Inclusion/exclusion settings that will apply to evidence items that are added to the case." Below this are three checked checkboxes:
 - Include File Slack
 - Include Free Space
 - Include KFF Ignorable Files
 - OLE Streams:** A dropdown menu set to "All".
 - File Status:** Three dropdown menus: "Deleted" (set to "Ignore status"), "Encrypted" (set to "Ignore status"), and "From Email" (set to "Ignore status").
 - File Types:** A list of checked checkboxes representing various file types:
 - Documents
 - Spreadsheets
 - Databases
 - Graphics
 - Email Messages
 - Executables
 - Archives
 - Others
 - Unknown
 - Bottom Options:** A checkbox: "Only add items that match both File Status AND File Types criteria" and two buttons: "Reset" and "OK".

Right Window Content:

- Left Sidebar:** Contains icons for "Evidence Processing", "Evidence Refinement (Advanced)" (selected), and "Index Refinement (Advanced)".
- Main Area:**
 - Top Buttons:** "Refine by File Status/Type" and "Refine by File Date/Size".
 - File Status Refinement:** Three checkboxes with date pickers:
 - Created: From 2012-04-16 To 2012-04-16
 - Last Modified: From 2012-04-16 To 2012-04-16
 - Last Accessed: From 2012-04-16 To 2012-04-16
 - File Size Refinement:** Two checkboxes with byte input fields:
 - At least 0 Bytes
 - At most 0 Bytes
 - Note:** "Only items meeting the selected criteria will be included. If no options are selected, all items will be included."
 - Bottom Buttons:** "OK" and "Cancel".

Defining Index Parameters

- Usually not needed to modify these parameters
- Refine by: Type, Status, Date/Size

The image shows two identical 'Index Refinement (Advanced)' dialog boxes side-by-side, illustrating the configuration options for refining indexed items.

Left Dialog Box:

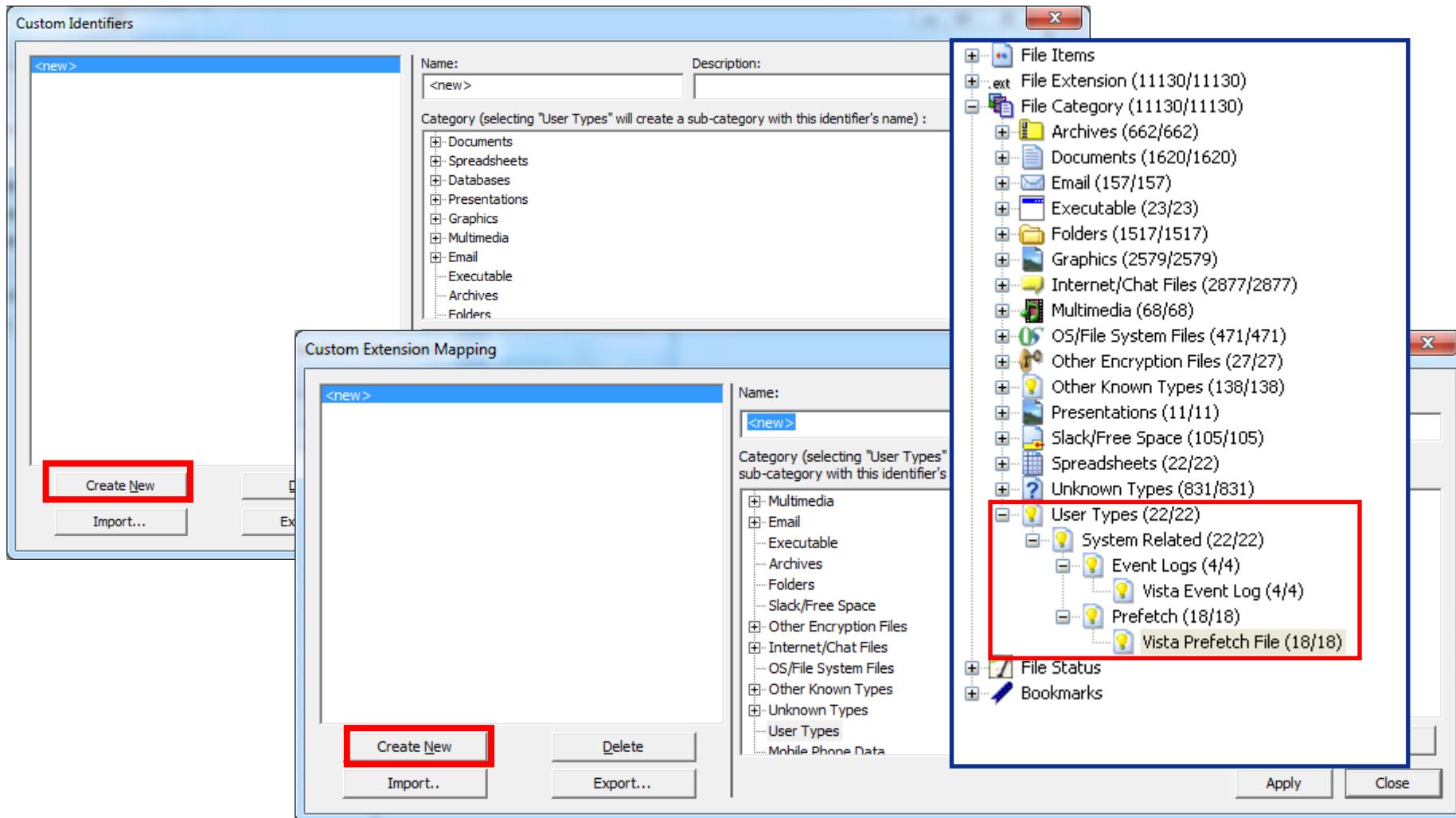
- Refinement Options:** Evidence Processing, Evidence Refinement (Advanced), Index Refinement (Advanced).
- Index Refinement (Advanced) Tab:**
 - Refine by File Status/Type:** Includes checkboxes for 'Include File Slack' (checked), 'Include Free Space' (checked), and 'Include KFF Ignorable Files' (unchecked).
 - Refine by File Date/Size:** Includes checkboxes for 'Include Message Headers' (checked).
 - File Status:** Includes dropdowns for 'Include OLE Streams' (set to 'All'), 'Deleted' (Ignore status), 'Encrypted' (Ignore status), and 'From Email' (Ignore status).
 - File Types:** A list of checked file types: Documents, Spreadsheets, Databases, Graphics, Email Messages, Executables, Archives, Others, and Unknown.
 - Checkboxes:** 'Only index items that match both File Status AND File Types criteria'.
- Buttons:** OK, Cancel, Reset.

Right Dialog Box:

- Refinement Options:** Evidence Processing, Evidence Refinement (Advanced), Index Refinement (Advanced).
- Index Refinement (Advanced) Tab:**
 - Refine by File Status/Type:** Includes checkboxes for 'Created' (unchecked), 'Last Modified' (unchecked), and 'Last Accessed' (unchecked).
 - Refine by File Date/Size:** Includes date range fields for 'From' and 'To' for 'Created' (both set to 2012-04-16), 'Last Modified' (both set to 2012-04-16), and 'Last Accessed' (both set to 2012-04-16).
 - AND:** Includes checkboxes for 'At least' (unchecked) and 'At most' (unchecked), with corresponding byte count fields (both set to 0).
- Note:** Only items meeting the selected criteria will be included. If no options are selected, all items will be included.
- Buttons:** OK, Cancel.

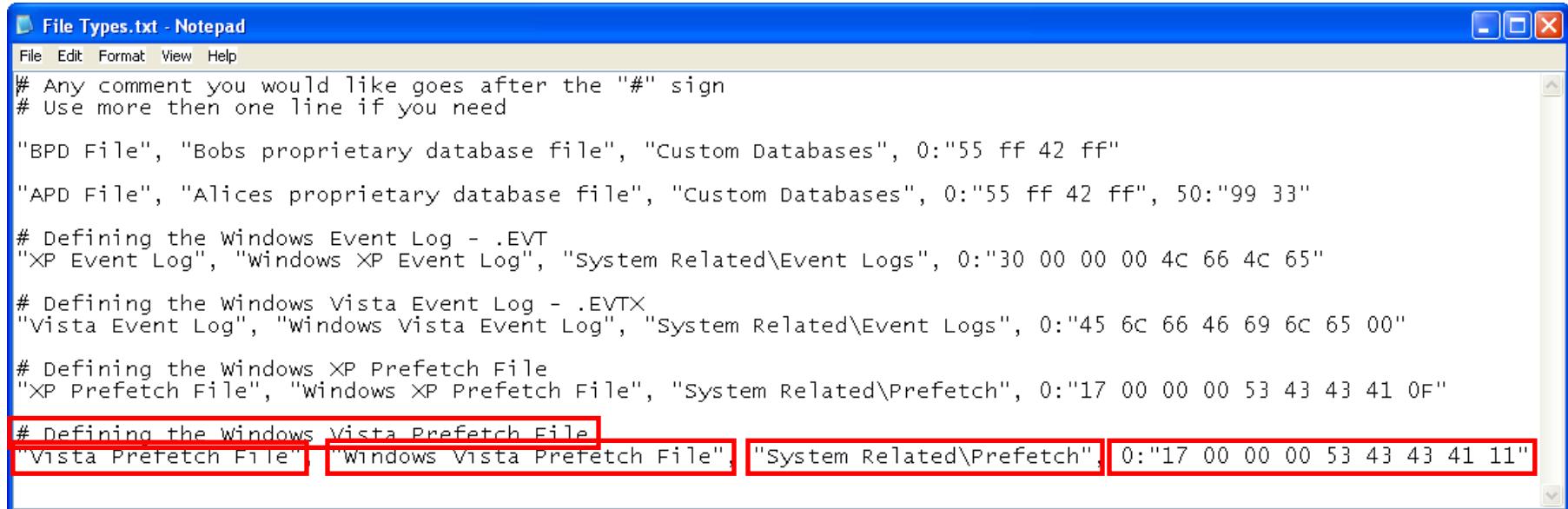
Custom File Identification

- Allows user-defined file identification for header and suffix



Custom File Identification

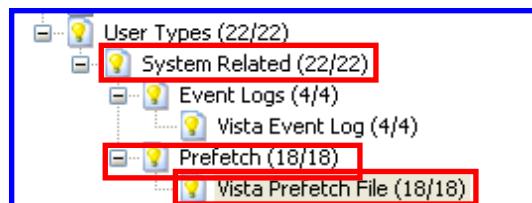
name, description, category[, offset:value [| offset:value]*]+



The screenshot shows a Windows Notepad window titled "File Types.txt - Notepad". The content is a list of file types and their characteristics, separated by commas. Some entries are preceded by a '#' symbol, indicating they are comments. The entries include:

- # Any comment you would like goes after the "#" sign
- # Use more than one line if you need
- "BPD File", "Bobs proprietary database file", "Custom Databases", 0:"55 ff 42 ff"
- "APD File", "Alices proprietary database file", "Custom Databases", 0:"55 ff 42 ff", 50:"99 33"
- # Defining the Windows Event Log - .EVT
- "XP Event Log", "Windows XP Event Log", "System Related\Event Logs", 0:"30 00 00 00 4c 66 4c 65"
- # Defining the Windows Vista Event Log - .EVTX
- "Vista Event Log", "Windows Vista Event Log", "System Related\Event Logs", 0:"45 6c 66 46 69 6c 65 00"
- # Defining the Windows XP Prefetch File
- "XP Prefetch File", "Windows XP Prefetch File", "System Related\Prefetch", 0:"17 00 00 00 53 43 43 41 0F"
- # defining the Windows Vista Prefetch File
- "Vista Prefetch File", "Windows Vista Prefetch File", "System Related\Prefetch", 0:"17 00 00 00 53 43 43 41 11"

= Comments (ignored)



File type label

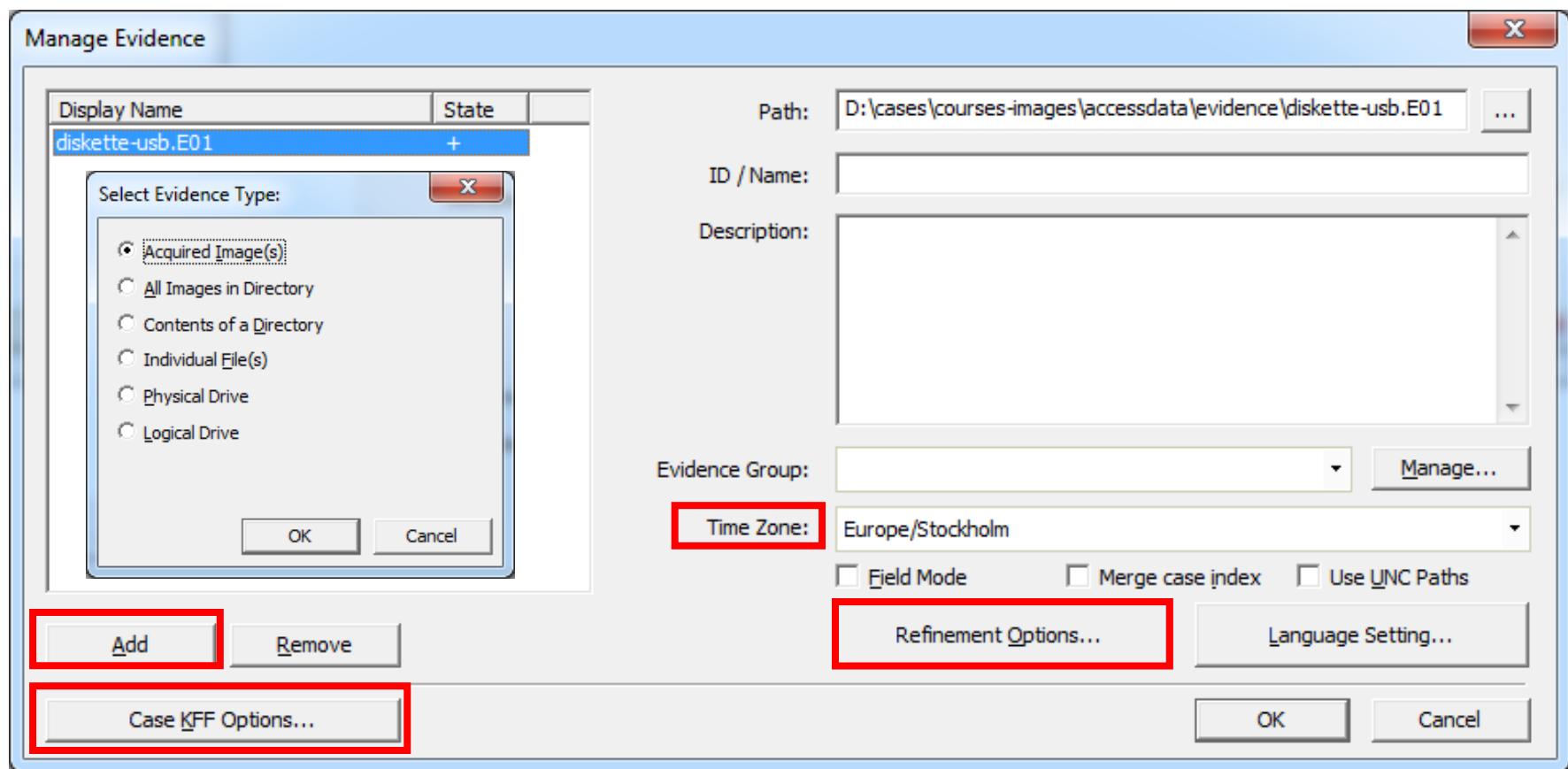
Description = For reference only

Category path relative to “User Types”

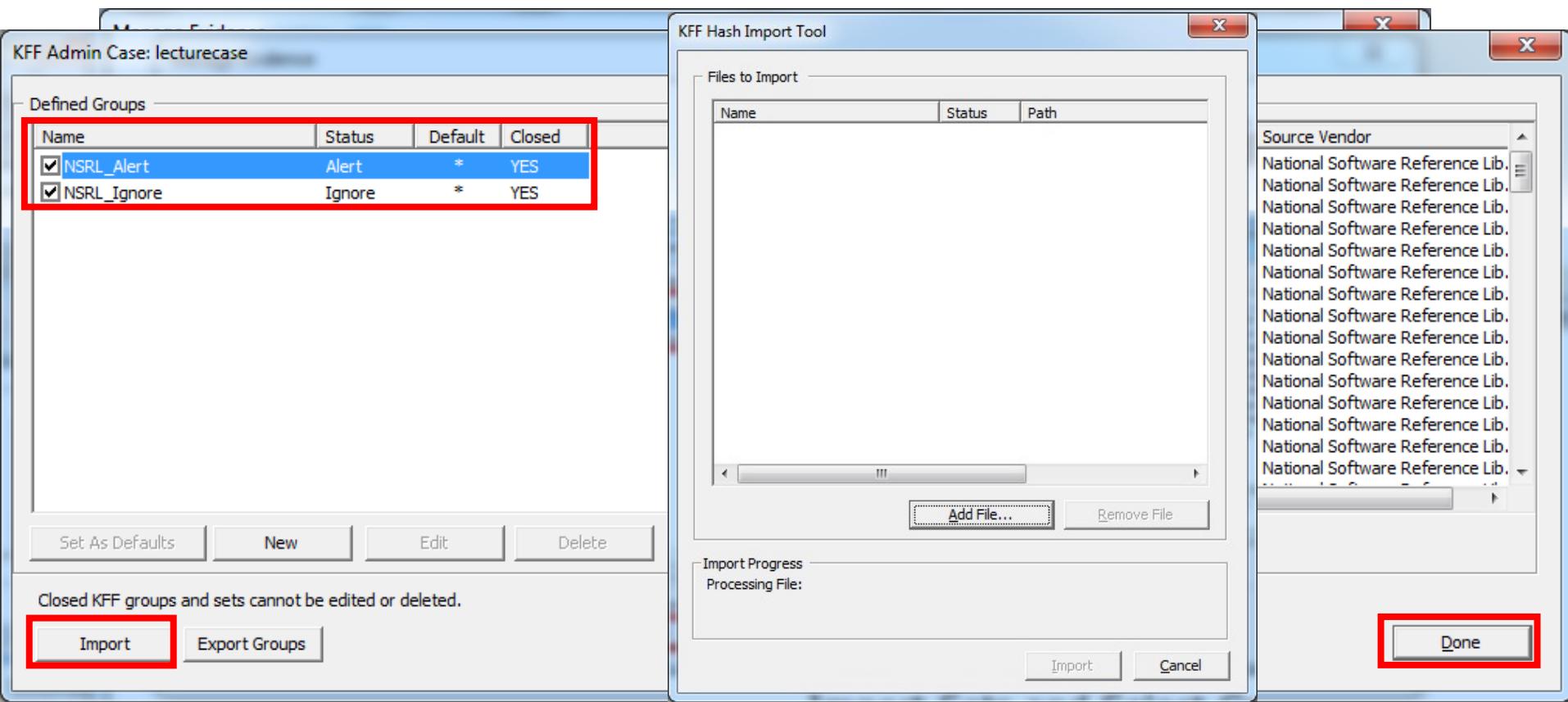
Offset and hex values (AND/OR)

Creating a New Case cont.

- From the Case Examiner Interface menu > Evidence > Add/Remove
- Refinement Options available again, change per item



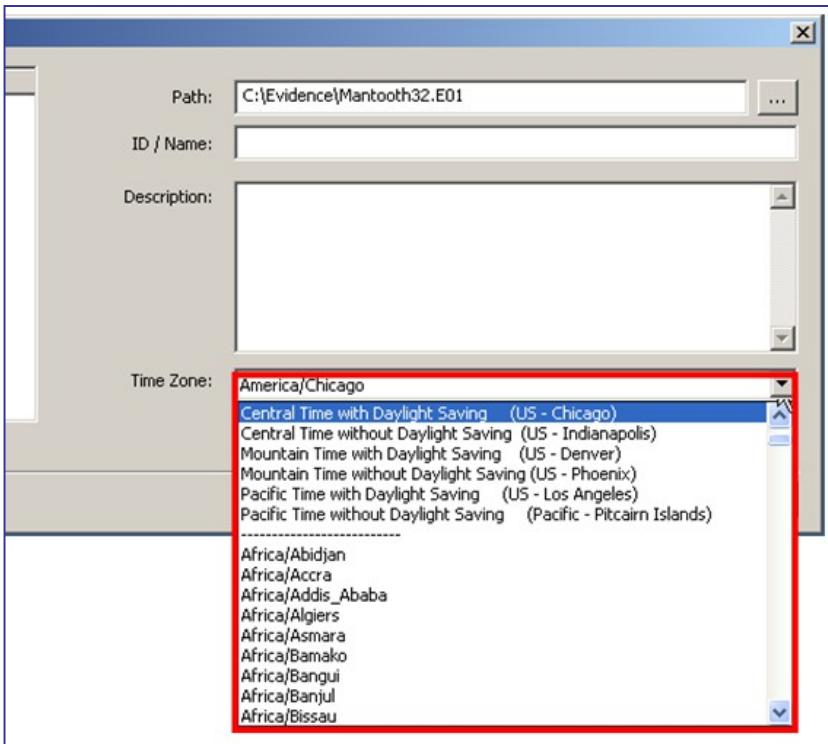
KFF Processing



Import Sets and Select Groups

KFF from National Software Reference Library (NSRL)

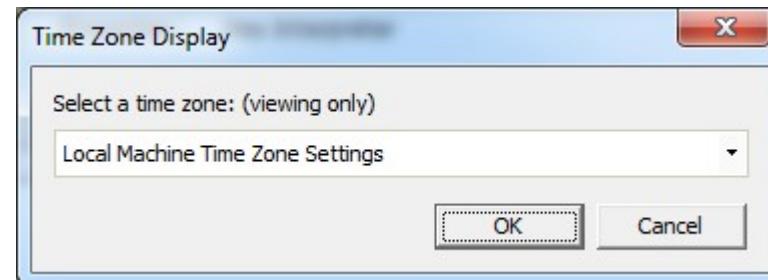
FTK Time Zone Settings



- FTK requires selection of a time zone for all evidence items
- FAT times are converted to GMT in the case database
- Removable Media
 - Should get the settings of associated computers if they exist
 - Use local settings if they do not

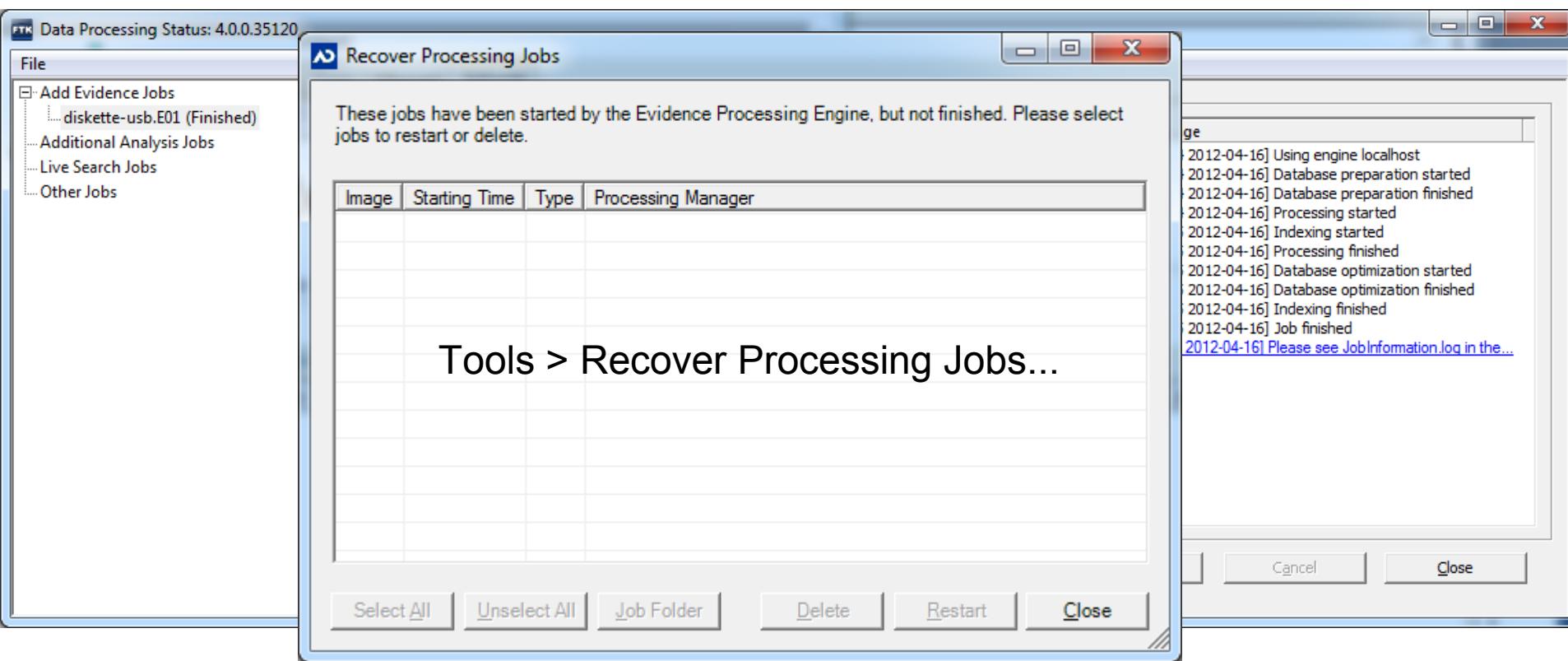
* Time Zone can be adjusted afterwards – visible in case log

View > Time Zone Display...



Jobs and recover jobs

- From the Case Examiner Interface menu > View > Progress Window...
 - Shows all ongoing jobs
 - GUI is separated from processing engine – crash proof?



Compound Files

The screenshot shows the EnCase Evidence Analysis software interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, and Help. The toolbar contains various icons for file operations. The main window has tabs for Explore, Overview, Email, Graphics, Bookmarks, Live Search, and Index Search. The 'Explore' tab is selected. The left pane displays a folder tree under 'Evidence Items'. A node labeled 'Those who owes.xls' is expanded, showing sub-folders like Documents, ADS, Car Titles, Checks, Google Image R, EFS DOCS, Hacker Stuff, Misc, Mr Smee, My Music, My Pictures, My poem.txt, My Received Files, and My Videos. The right pane displays 'SummaryInformation' details:

OS version: Windows 6.0.2
Application CLSID: {00000000-0000-0000-0000-000000000000}
Format: {F29F85E0-4FF9-1068-91AB-0008D9B3272B}

Property	Value
Code page	1252
Title	

The bottom pane shows a 'File List' table with columns: Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, Accessed. The table lists several files, including 'CompObj', 'DocumentSummaryIn...', 'SummaryInformation' (which is selected), '1Table', 'Data', and 'WordDocument'. The status bar at the bottom indicates 'Loaded: 6', 'Filtered: 6', 'Total: 6', 'Highlighted: 1', 'Checked: 5', and the path 'Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/Dear Sweetie.doc/□SummaryInformation'.

Compound files must also appear in the folder tree so they can be selected - to see their children.

File and Folder Export

File Options

- Append item number to filename
- Append extension to filename if bad/absent
- Export children
 - Exclude slack space children files
- Save HTML view (if available)
- Export emails as MSG
- Export using item number for file name
- Export directory as file
- Limit path length
- Include original path
- Create manifest files

Items to Include

- All Checked (70)
- All Highlighted (4)
- All

(Whole disk images, logical images, and partitions are always excluded)

Destination base path:

C:\Users\hjo\Desktop\data

OK Cancel

Database: localhost Case: lecture -Education-

Manage Help Filter Manager... Live Search Index Search Volatile

Labels... Review Labels... Mount Image... Add Decrypted... Perform Cerberus... View File Sector... Find on Disk... Add to Fuzzy Hash... Find Similar Files... Open in Registry... Export... Export to Image... Acquire to disk... Export File List... Copy Special... Check All Files Uncheck All Files in Current List Uncheck All Files in Case

oot]/10-1 Graphics/Cartoon Beer.jpg Overview Tab Filter: [None]

Default Media W

Created

2003-10-20 2003-10-20 2003-10-20 2003-10-20 2003-09-20 2003-09-20 2003-10-20 2003-10-20 2003-10-20

Column Settings

- From the Case Examiner Interface menu > Manage > Columns > Manage Columns...
- Can be used for: Sorting, Reporting, Copy Special / Export File List

The image displays two windows from a software application for managing column settings.

Left Window: Manage Column Settings

- Settings Templates:**
 - Cerberus Results
 - EID
 - Email
 - File Listing
 - Normal
 - Normal+Filters
 - Reports: File Path Section
 - Reports: Standard
 - eDiscovery
 - eDiscovery Email
 - own email** (selected)
- Buttons:** New, Edit, Copy Selected, Delete, Import..., Export..., Make Shared, Apply, Close.

Right Window: Column Settings

- Available Columns:** A tree view showing categories like Common Features, Disk Image Features, Email Features, Entropy Stats, File Status Features, File System Features, Zip-specific Features, Custom Columns, Office-specific Features, Cerberus Static Analysis Features, and All Features. The "Common Features" node is expanded.
- Add >>** Button to move columns from Available to Selected.
- Remove** Button to remove selected columns.
- Move Up** and **Move Down** buttons for reordering selected columns.
- Selected Columns:** A grid table showing the configuration for various columns.

Name	Short Name	Description
Subject	Name	The subject line of the Em...
Name	Name	The name of the object (f...
To		The TO list. Only set on E...
From		The FROM address. Only ...
CC		The CC (Carbon Copy) lis...
BCC		The BCC (Blind Carbon Co...
Submit Time		The time the client submit...
Delivery Time		For outgoing mail, the tim...
Unread		True if the Email is marke...
Unsent		True if the Email has not ...
Has Attach...		True if the Email has at le...
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 ...
Item Number	Item #	A number assigned to the ...
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 obj...
Path	Path	The full path to an object
- Column Template Name:** A text input field containing "own email".
- Buttons:** Remove All, OK, Cancel.

Copy Special > clipboard

AccessData Forensic Toolkit Version: 4.0.0.35120 Database: localhost Case: lecture -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: - unfiltered - Filter Manager...

Explore Overview Email Graphics Bookmarks Live Search Index Search Volatile

Case Overview Evidence Groups (382 / 382)

Column Settings

Copy Special to Clipboard

Available Columns

- + Common Features
- + Disk Image Features
- + Email Features
- + Entropy Stats
- + File Status Features
- + File System Features
- + Zip-specific Features
- Custom Columns
- + Office-specific Features
- + Cerberus Static Analysis Features
- + All Features

Add >> Remove Move Up Move Down

Column Template Name

File Listing (1)

Selected Columns

Name	Short Name	Description
Name	Name	The name of the object (file, disk, partition, etc.)
Item Number	Item #	A number assigned to the object (file, disk, partition, etc.) as it was inserted into the case
Path		The full path to an object
File Type	Category	An INSO type ID (or a custom one) reflecting the identified or reclassified type of a file
Physical Size	P-Size	The physical size (size on disk) of the object
Logical Size	L-Size	The logical size of the object
MD5 Hash	MD5	The MD5 hash of the object's contents
SHA1 Hash	SHA1	The SHA1 hash of the object's contents
SHA256 Hash	SHA256	The SHA256 hash of the object's contents
Created Date	Created	The date the object was created
Accessed Date	Accessed	The date the object was last accessed
Modified Date	Modified	The date the object was modified
Deleted		True if the object is deleted
KFF Status	KFF	The KFF status of the file

Remove All OK Cancel

Ready Overview Tab Filter: [None]

Create and Add Bookmarks

The screenshot illustrates the process of creating and adding bookmarks in a forensic or analytical software environment.

Left Panel (Context Menu):

- Open
- Launch in Content Viewer
- Open With...
- Create Bookmark...** (highlighted with a red box)
- Add to Bookmark...
- Remove from Bookmark
- Labels...
- Review Labels...
- Mount Image to Drive...
- Add Decrypted File...
- Perform Cerberus Analysis
- View File Sectors...
- Find on Disk...
- Add to Fuzzy Hash Library...
- Find Similar Files
- Open in Registry Viewer
- Export...
- Export to Image...
- Acquire to disk image...
- Export File List Info...
- Copy Special...
- Check All Files in Current List
- Uncheck All Files in Current List
- Uncheck All Files in Case
- Change "Flag as Ignorable" Status...
- Change "Flag as Privileged" Status...
- Re-assign File Category
- View This Item In a Different List

Create New Bookmark Dialog:

Bookmark Name: beer

Files to Include:
All Checked (radio button selected)
4 items selected.
Name Path
Cartoon Beer.jpg diskette-usb.E01
Cartoon Beer.jpg diskette-usb.E01
Clear Beer.jpg diskette-usb.E01
Clear Beer.jpg diskette-usb.E01

File Comment:

Also include:
 Email Attachments
 Parent Email
 Bookmark Selection in File

Select Bookmark Parent Dialog:

Shared
hjo
beer
test

Add Files to Bookmark Dialog:

Files to Add:
All Checked (radio button selected)
1 item selected.
Name Path
Copy of Darth Beer.jpg diskette-usb.E01\Partition 4\EVIDENCE [FAT12]\[root]\10-1 Gra

File Comment:

Also include:
 Email Attachments
 Parent Email
 Bookmark Selection in File

Select Existing Bookmark:
Shared
hjo
beer
test

OK Cancel

Managing Bookmarks

File Edit View Evidence Filter Tools Help

Filter: - unfiltered - Define...

Explore Overview Email Graphics Bookmarks Live Search Index Search

Bookmarks

- Bookmarks
 - ndrehel
 - Carved Text
 - Fraudulent Checks
 - Hacker Tools
 - Illegal Pictures
 - Suspect Mail
 - Suspicious Pictures
 - Shared

Bookmark Information

Bookmark Name: Suspicious Pictures
Creator Name: ndrehel
Bookmark Comment: Suspicious pictures related to this investigation.
File Comment:
Selection Comment:

Attach File Remove File

Save Changes Clear Changes Add Selection Remove Selection

File Content

Hex Text Filtered Natural

Default Media Web

File List

Name	Label	Item #	Extension	Path
\$R9H2OZ0.jpg		1248	jpg	Mantooth32.E01/Partiti...
\$RKY3FVP.gif		1252	gif	Mantooth32.E01/Partiti...
Ape_20shoot.gif		1586	gif	Mantooth32.E01/Partiti...

Loaded: 3 Filtered: 3 Total: 3 Highlighted: 1 Checked: 1

Bookmarks Tab Filter: [None]

Ready

Mantooth32.E01/Partition 1/MANTOOOTH [NTFS]/[root]/Users/Wes Mantooth/Desktop/Ape_20shoot.gif

Managing Bookmarks

The screenshot displays a digital forensic analysis software interface. The top navigation bar includes File, Edit, View, Evidence, Filter, Tools, and Help. Below the menu is a toolbar with various icons. The main window has several tabs: Explore, Overview, Email, Graphics, Bookmarks (which is selected and highlighted in purple), Live Search, and Index Search.

Bookmarks Tab: This panel shows a hierarchical tree view of bookmarks. A node labeled "Suspicious Pictures" is currently selected and highlighted in blue. Other nodes include "ndrehel" (which contains "Carved Text", "Fraudulent Checks", "Hacker Tools", "Illegal Pictures", "Shared", and "Suspect Mail"), and "Shared".

Bookmark Information Panel: This panel contains fields for Bookmark Name ("Suspicious Pictures"), Creator Name ("ndrehel"), and Supplementary Files. It also includes sections for File Comment and Selection Comment, along with buttons for Attach File, Remove File, Save Changes, Clear Changes, Add Selection, and Remove Selection.

File Content Tab: This panel shows the file "Ape_20shoot.gif" in its media format. Below the preview are tabs for Hex, Text, Filtered, and Natural. On the right, there are buttons for Default, Media, and Web, along with scroll bars.

File List Panel: This panel displays a list of files found in the current evidence item. The columns are Name, Label, Item #, Extension, and Path. The listed files are:

Name	Label	Item #	Extension	Path
\$R9HZOZO.jpg		1248	jpg	Mantooth32.E01/Partiti...
\$RKY3FVP.gif		1252	gif	Mantooth32.E01/Partiti...
Ape_20shoot.gif		1586	gif	Mantooth32.E01/Partiti...

Status Bar: The bottom status bar shows the path "Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Desktop/Ape_20shoot.gif", the number of loaded files (3), filtered files (3), total files (3), highlighted files (0), and checked files (0).

Bookmarks can be nested when created or later!