



**AccessData<sup>®</sup>**

FTK 4 and FTK 5

Working with FTK 4 or 5

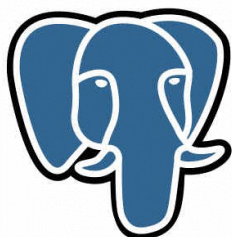
# FTK 2.x, 3.x summary

## ➤ Advantages

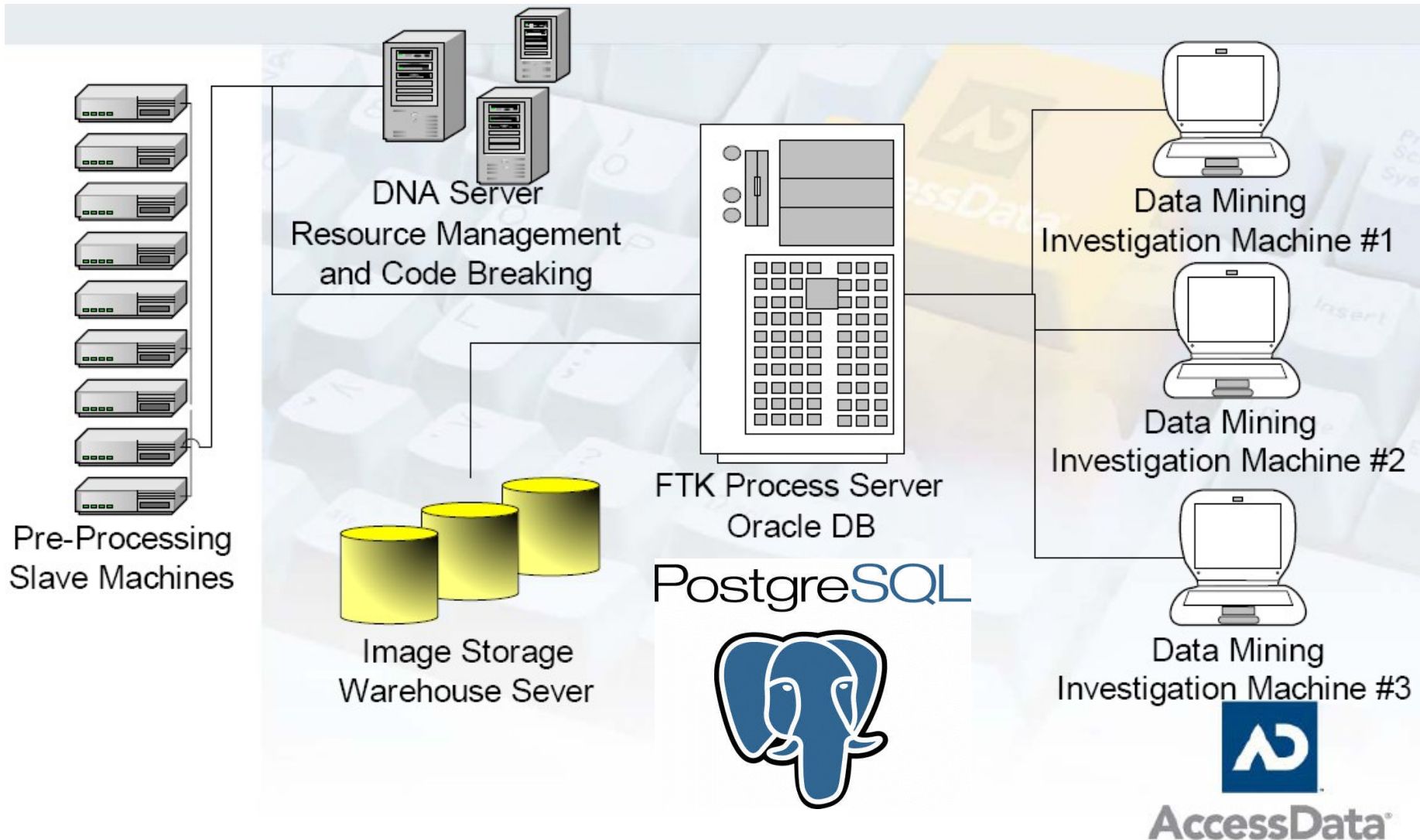
- Client / Server Architecture
- Oracle database capable of managing numerous HD's per case.
- Multi-treaded processing compared to FTK 1.x's serial process.
- Immediate access to data.
- The order of evidence pre-processing and the building of index records is directed by the examiner. (My Documents 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

Figure 1: Timeline, distribution, and network of the 188 spam emails received by the FBI.

The figure is divided into three main sections:

- Timeline (Top):** A line graph showing the arrival of 188 spam emails from April 13 to July 1, 2006. The x-axis represents time in weeks, and the y-axis represents the number of emails. A blue box highlights the period from April 27 to April 29, 2006, indicating the time when the FBI received the 188 spam emails.
- Distribution (Middle):** A bar chart showing the number of spam emails received per day from April 13 to April 29, 2006. The x-axis represents the date, and the y-axis represents the number of emails. The distribution shows a peak of 128 emails on April 13, 2006, and a total of 188 emails received over the period.
- Network (Bottom):** A network diagram showing the distribution of spam emails to various recipients. The nodes represent email addresses, and the edges represent the flow of spam. The network is centered around the email address 'littenraker@fbi.gov', which is the source of the spam. The network shows a high degree of connectivity, with many nodes receiving multiple emails.





# 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.

File List

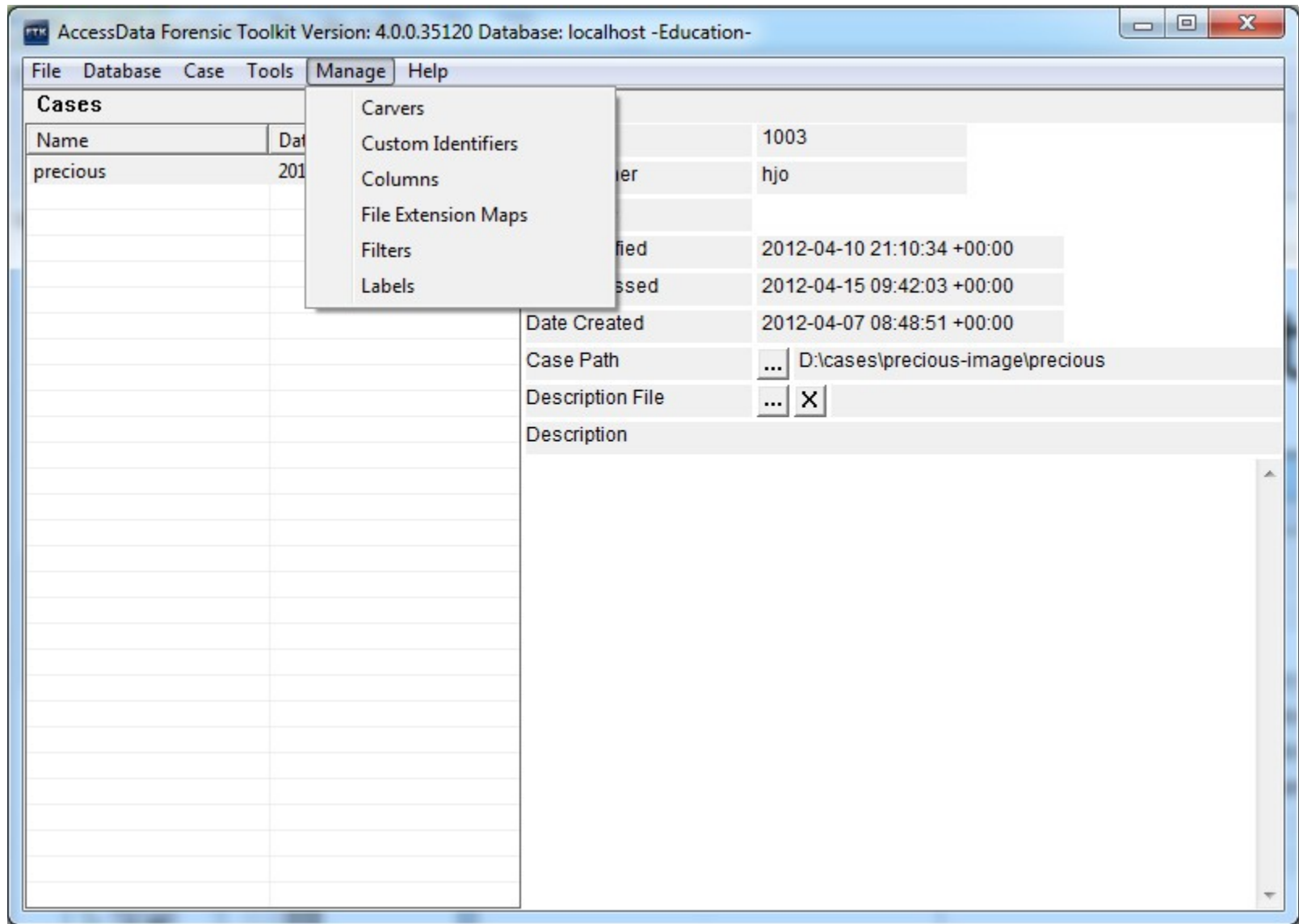
Explicit Material

Day Time Zone: Mountain Daylight Time (From local machine)

Name	La	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
bik4687.jpg		99	99	99	99
centerfold001.jpg	JPG	0	99	99	0
cot2.jpg	JPEG	56	99	99	56
d2445.jpg	JPEG	0	99	99	0
des456375c52.jpg	JPEG	0	99	99	0
fg_ashleybond4.jpg	Explicit JPEG	99	99	99	99
group1.jpg	JPEG	1	99	99	1
landd2503.jpg	JPEG	11	99	99	11
lat12p.jpg	JPEG	0	99	99	0
veg99f5.jpg	JPEG	11	99	99	11
IMG00229 - Copy.jpg	JPEG E...	63	97	97	63
IMG00229.inn	IPFG F...	63	97	97	63

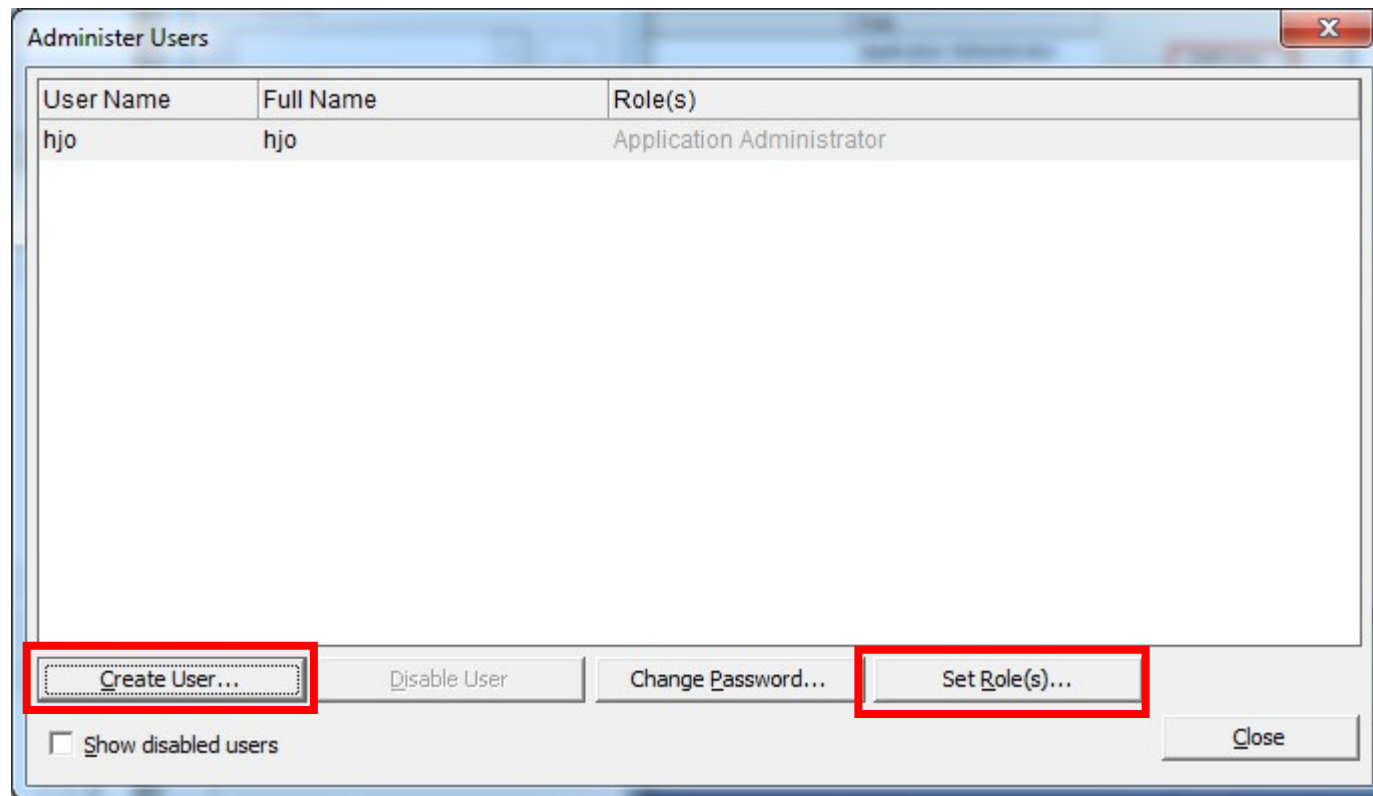
Loaded: 235   Filtered: 235   Total: 21,769   Highlighted: 1   Checked: 0

# Case Manager Interface



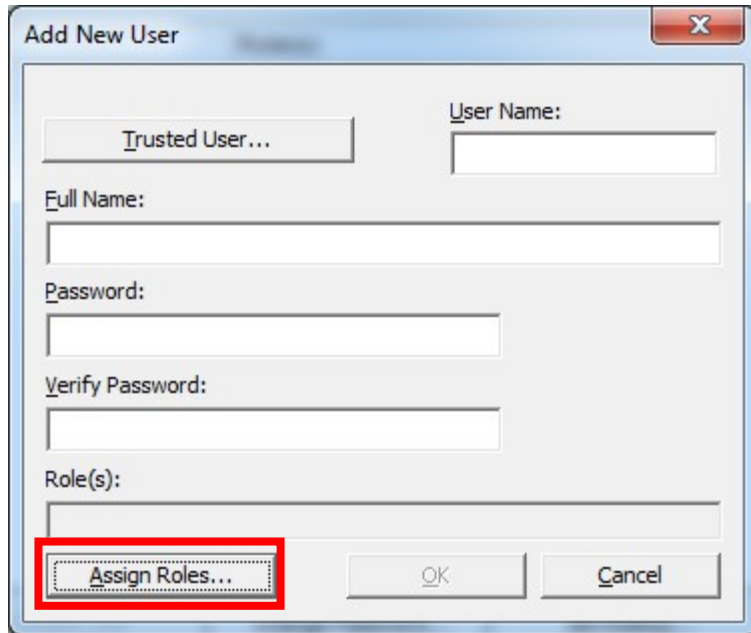
# Administer Users 1

- The first user account is the Application Administrator





# Administer Users 2



The 'Add New User' dialog box contains the following fields and buttons:

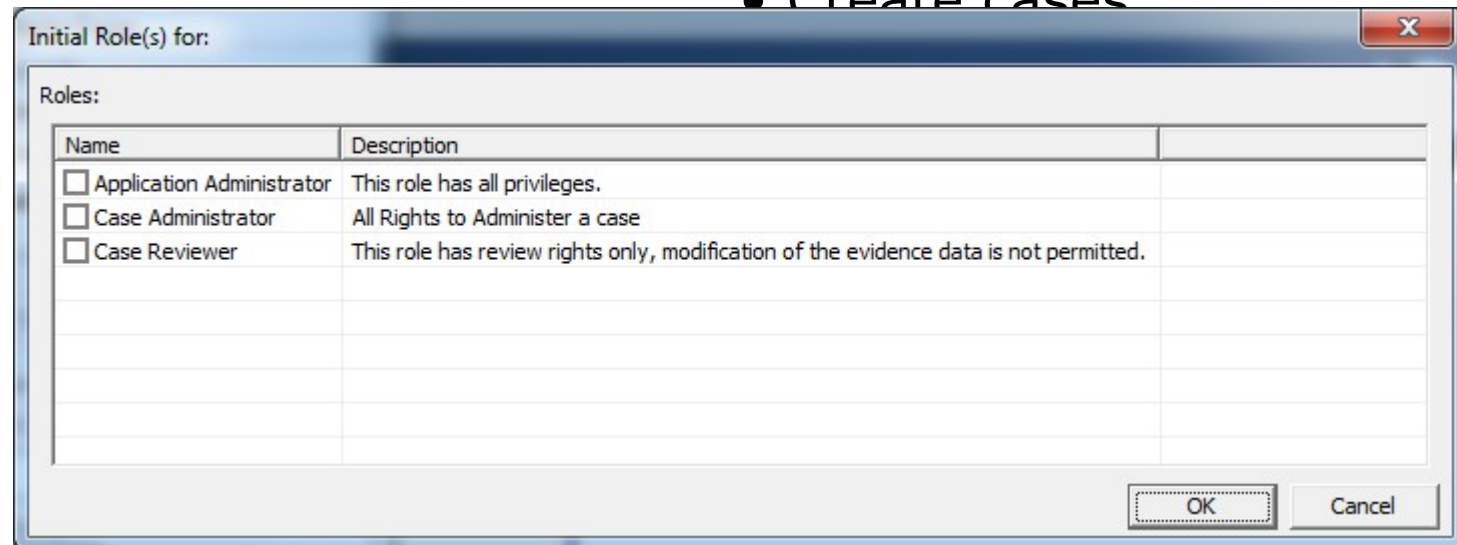
- Trusted User...**: A button to select a trusted user.
- User Name:**: A text input field.
- Full Name:**: A text input field.
- Password:**: A text input field.
- Verify Password:**: A text input field.
- Role(s):**: A text input field.
- Assign Roles...**: A button highlighted with a red rectangle.
- OK**: A button.
- Cancel**: A button.

## Application Administrator

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

## Case Administrator

- Create cases



The 'Initial Role(s) for:' dialog box displays a table of roles with checkboxes for selection.

Name	Description
<input type="checkbox"/> Application Administrator	This role has all privileges.
<input type="checkbox"/> Case Administrator	All Rights to Administer a case
<input type="checkbox"/> Case Reviewer	This role has review rights only, modification of the evidence data is not permitted.

Buttons: **OK**, **Cancel**

cases

# 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

Default Media Web

File Content Properties Hex Interpreter

File List

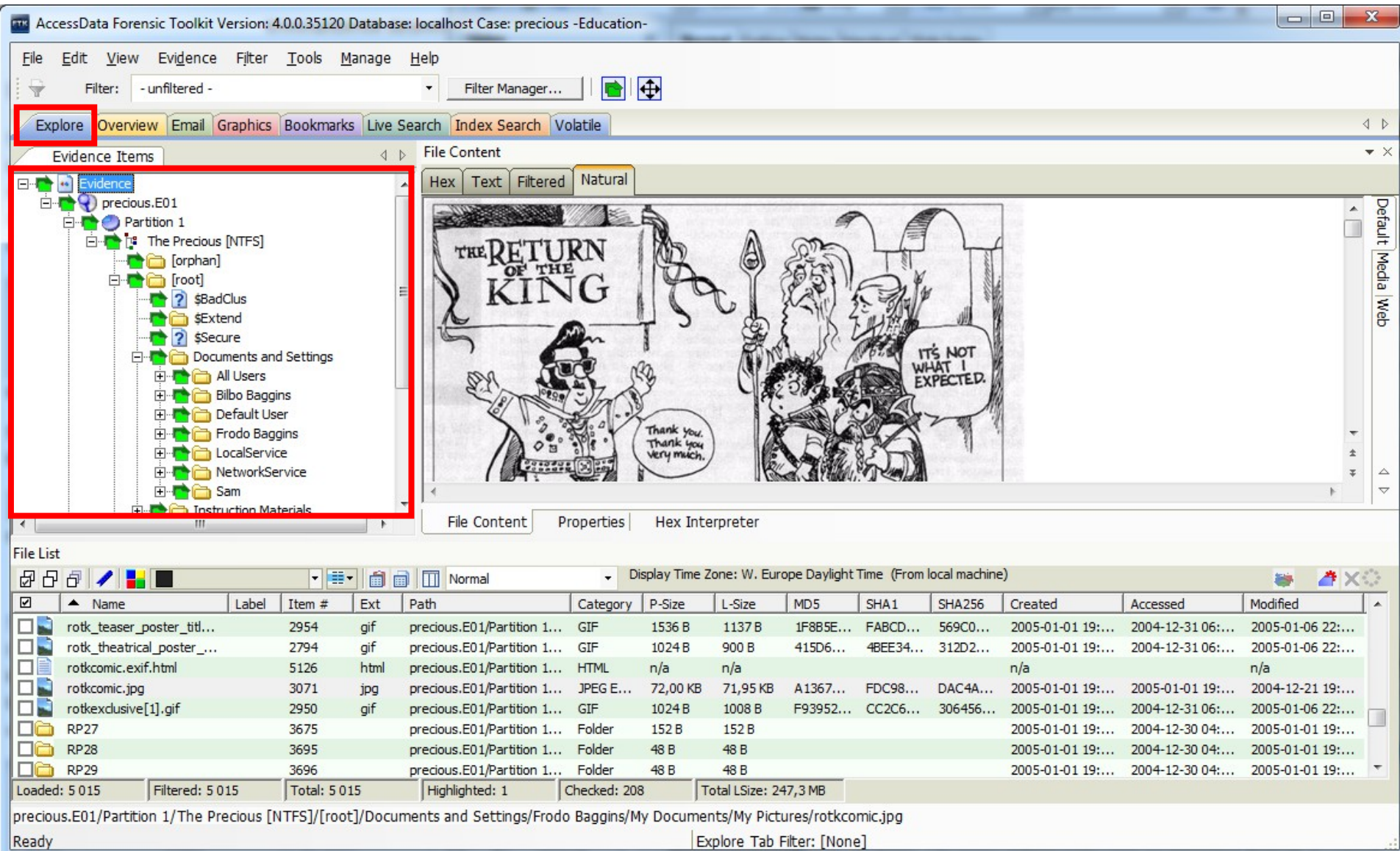
Normal Display Time Zone: W. Europe Daylight Time (From local machine)

<input checked="" type="checkbox"/>	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
<input type="checkbox"/>	rotk_teaser_poster_titl...		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:...
<input type="checkbox"/>	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:...
<input type="checkbox"/>	rotkcomic.exif.html		5126	html	precious.E01/Partition 1...	HTML	n/a	n/a				n/a		n/a
<input type="checkbox"/>	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:...
<input type="checkbox"/>	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:...
<input type="checkbox"/>	RP27		3675		precious.E01/Partition 1...	Folder	152 B	152 B				2005-01-01 19:...	2004-12-30 04:...	2005-01-01 19:...
<input type="checkbox"/>	RP28		3695		precious.E01/Partition 1...	Folder	48 B	48 B				2005-01-01 19:...	2004-12-30 04:...	2005-01-01 19:...
<input type="checkbox"/>	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 shows a file explorer application with a 'View' menu open. The 'Filter Bar' and 'Explorer Tree' options are highlighted with red boxes. The 'File List' pane at the bottom displays a table of files and folders.

**View Menu Options:**

- Refresh (F5)
- ☒ 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

**Properties Panel:**

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

**General Info:**

- File Size**
  - Physical Size: 38,912 bytes (38.00 KB)
  - Logical Size: 38,473 bytes (37.57 KB)
- File Dates**
  - Date Created: 3/5/2007 7:44:22 PM (2007-03-06 01:44:22 UTC)
  - Date Accessed: 7/13/2007 1:44:40 PM (2007-07-13 18:44:40 UTC)
  - Date Modified: 3/5/2007 7:20:00 PM (2007-03-06 01:20:00 UTC)
- File Attributes**
  - General**
    - Actual File: True

**File List Table:**

	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed
<input type="checkbox"/>	Apple_guy.gif		1600	gif	Mantooth32.E01/Partiti...	GIF	8704 B	8483 B	FA79F...	A3B07...	872482...	4/12/2007 7:56...	7/13/
<input type="checkbox"/>	beer.gif		1601	gif	Mantooth32.E01/Partiti...	GIF	7168 B	6892 B	D669C...	11FFC...	9C3DB...	4/12/2007 7:56...	7/13/
<input type="checkbox"/>	Car Titles		1602		Mantooth32.E01/Partiti...	Folder	408 B	408 B	288B5...	6ACEA...	21B049...	3/5/2007 8:01...	7/2/2
<input type="checkbox"/>	Checks		1603		Mantooth32.E01/Partiti...	Folder	56 B	56 B	35ED3...	A9420...	518691...	3/5/2007 8:01...	7/2/2
<input type="checkbox"/>	ClassicVisaFern.gif		1604	gif	Mantooth32.E01/Partiti...	GIF	38.00 KB	37.57 KB	EF250B...	238CD...	903A6...	3/5/2007 7:44...	7/13/
<input type="checkbox"/>	CRACK_ME		1605	<missin...	Mantooth32.E01/Partiti...	Text	1024 KB	1024 KB	5A4F0...	C5EE4...	099975...	4/10/2007 8:27...	6/20/
<input type="checkbox"/>	Dear Sweetie.doc		1606	doc	Mantooth32.E01/Partiti...	Microso...	63.50 KB	63.50 KB	954418...	B79149...	F5393...	7/12/2007 6:51...	7/13/

Loaded: 34 | Filtered: 34 | Total: 34 | Highlighted: 1 | Checked: 0

Ready | Explore Tab Filter: [None]

Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/ClassicVisaFern.gif

# Tabs and Panes

File Edit View Evidence Filter Tools Help

Refresh F5

Define...

Live Search Index Search

File Content

Hex Text Filtered Natural

Tab Layout

- Lock
- Add...
- Remove
- Save
- Save All Layouts
- Restore
- Reset To Default

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

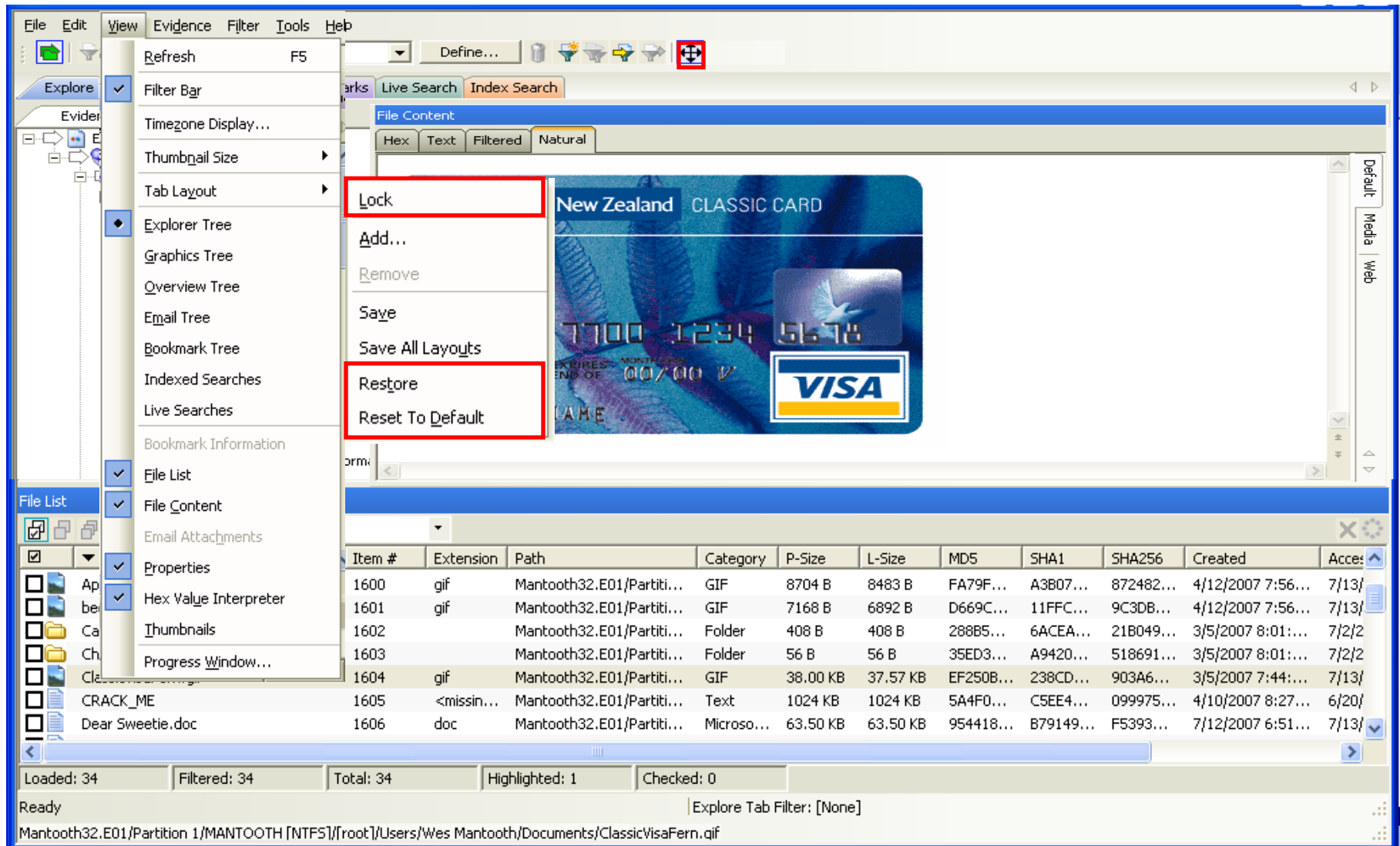
Index	Extension	Name	Type	Size	Size	FA79F...	A3807...	872482...	4/12/2007 7:56...	7/13/
1600	gif	Mantooth32.E01/Partiti...	GIF	8704 B	8483 B	FA79F...	A3807...	872482...	4/12/2007 7:56...	7/13/
1601	gif	Mantooth32.E01/Partiti...	GIF	7168 B	6892 B	D669C...	11FFC...	9C3DB...	4/12/2007 7:56...	7/13/
1602		Mantooth32.E01/Partiti...	Folder	408 B	408 B	28885...	6ACEA...	218049...	3/5/2007 8:01...	7/2/2
1603		Mantooth32.E01/Partiti...	Folder	56 B	56 B	35ED3...	A9420...	518691...	3/5/2007 8:01...	7/2/2
1604	gif	Mantooth32.E01/Partiti...	GIF	38.00 KB	37.57 KB	EF250B...	238CD...	903A6...	3/5/2007 7:44...	7/13/
1605	<missin...	Mantooth32.E01/Partiti...	Text	1024 KB	1024 KB	5A4F0...	C5EE4...	099975...	4/10/2007 8:27...	6/20/
1606	doc	Mantooth32.E01/Partiti...	Microso...	63.50 KB	63.50 KB	954418...	B79149...	F5393...	7/12/2007 6:51...	7/13/

Loaded: 34 Filtered: 34 Total: 34 Highlighted: 1 Checked: 0

Ready Explore Tab Filter: [None]

Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Documents/ClassicVisaFern.gif

# Tabs and Panes





# 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-

Explore Overview Email Graphics Bookmarks Live S

Evidence Items

Evidence

- precious.E01
  - Partition 1
    - The Precious [NTFS]
      - [orphan]
      - [root]
        - \$BadClus
        - \$Extend
        - \$Secure
        - Documents and Settings
          - All Users
          - Bilbo Baggins
          - Default User
          - Frodo Baggins
          - LocalService
          - NetworkService
          - Sam
          - Instruction Materials
          - Mv Music

Hex Text Filtered Natural

THE RETURN OF THE KING

Thank you, Thank you very much.

IT'S NOT WHAT I EXPECTED.

File Content Properties Hex Interpreter

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
☐	💡	CompObj		3855		precious.E01/Partition 1...	OLE Str...	n/a	110 B	82C9B...	4F88B2...	2CE9A...	n/a		n/a
☐	💡	CompObj		3901		precious.E01/Partition 1...	OLE Str...	n/a	110 B	82C9B...	4F88B2...	2CE9A...	n/a		n/a
☐	💡	CompObj		3950		precious.E01/Partition 1...	OLE Str...	n/a	106 B	9AE6B...	170C3...	C8B91...	n/a		n/a
☐	💡	CompObj		4103		precious.E01/Partition 1...	OLE Str...	n/a	106 B	55B245...	AE31B...	6F1EC...	n/a		n/a
☐	💡	CompObj		4283		precious.E01/Partition 1...	OLE Str...	n/a	106 B	9AE6B...	170C3...	C8B91...	n/a		n/a
☐	💡	CompObj		4981		precious.E01/Partition 1...	OLE Str...	n/a	106 B	55B245...	AE31B...	6F1EC...	n/a		n/a
☐	💡	CompObj		7092		precious.E01/Partition 1...	OLE Str...	n/a	106 B	55B245...	AE31B...	6F1EC...	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

File Content Properties Hex Interpreter

File List

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

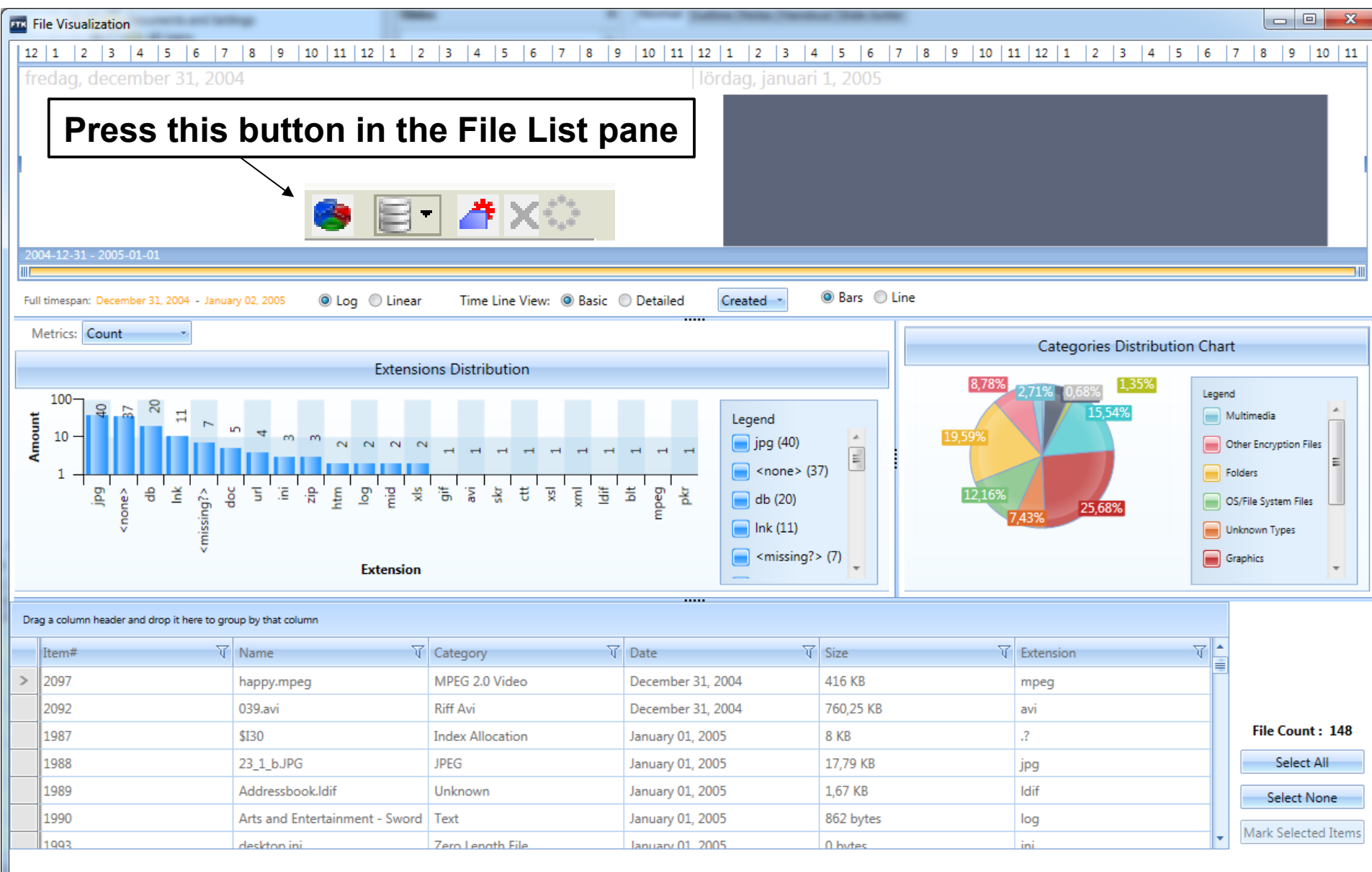
	Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed	Modified
<input checked="" type="checkbox"/>	rotk_teaser_poster_titl...		2954	gif	precious.E01/Partition 1...	GIF	1536 B	1137 B	1F8B5E...	FABCD...	569C0...	2005-01-01 19:...	2004-12-31 06:...	2005-01-06 22:...
<input type="checkbox"/>	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:...
<input type="checkbox"/>	rotkcomic.exif.html		5126	html	precious.E01/Partition 1...	HTML	n/a	n/a				n/a		n/a
<input type="checkbox"/>	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:...
<input type="checkbox"/>	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:...
<input type="checkbox"/>	RP27		3675		precious.E01/Partition 1...	Folder	152 B	152 B				2005-01-01 19:...	2004-12-30 04:...	2005-01-01 19:...
<input type="checkbox"/>	RP28		3695		precious.E01/Partition 1...	Folder	48 B	48 B				2005-01-01 19:...	2004-12-30 04:...	2005-01-01 19:...
<input type="checkbox"/>	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





# Column Sorting & Type-Down

The screenshot displays the AccessData Forensic Toolkit (FTK) Version: 4.0.0.35120. The interface includes a menu bar (File, Edit, View, Evidence, Filter, Tools, Manage, Help), a toolbar with a filter dropdown set to 'Actual Files', and a tabbed interface with 'Explore', 'Overview', 'Email', 'Graphics', 'Bookmarks', 'Live Search', 'Index Search', and 'Volatile'. The 'Evidence Items' pane on the left shows a tree structure for 'diskette-usb.E01' containing 'EVIDENCE [FAT12]' and '[root]'. The 'File Content' pane shows a preview of a file with the text 'MAPQU'. A callout box with a blue border contains the following list:

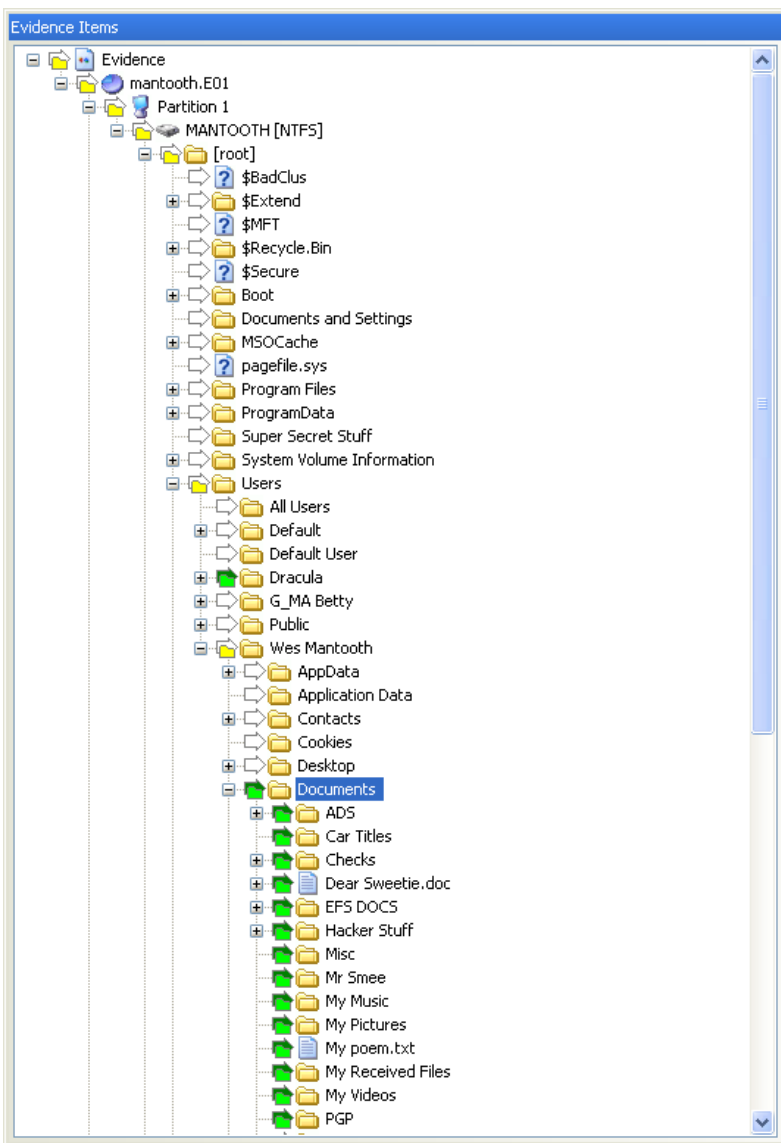
- Up to 5 characters
- Time Sensitive
- Alpha columns only

The 'File List' pane at the bottom shows a table of files with columns: Name, Label, Item #, Ext, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, and Created. The 'Name' column is highlighted with a red box. The table contains the following data:

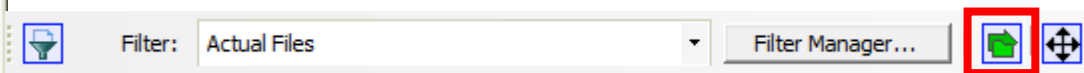
Name	Label	Item #	Ext	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created
10-1 Graphics		1217		diskette-usb.E01/EVIDE...	Folder	1024 B	1024 B				2003-10-01
Access Data Document....		1230	doc	diskette-usb.E01/EVIDE...	Microso...	19,50 KB	19,50 KB		85		2003-09-11
Access Document.doc		1231	doc	diskette-usb.E01/EVIDE...	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

At the bottom, the status bar shows: Loaded: 105, Filtered: 105, Total: 176, Highlighted: 1, Checked: 0, Total LSize: 983,9 KB. The path bar shows: diskette-usb.E01/EVIDENCE [FAT12]/[root]/TIF Netmail/Y1UVYTMV/CAH0SV9H.HTM. The status bar also indicates 'Ready' and '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 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 Hobbytes 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
<input checked="" type="checkbox"/>	Talk to Pippin about his ba...		5530		precious.E01/Partition 1...	Task	n/a	0 B				2004-12-30 ...		2004-12-30 00:...
<input checked="" type="checkbox"/>	Tasks		5527		precious.E01/Partition 1...	Email F...	n/a	n/a				n/a		n/a
<input checked="" type="checkbox"/>	Templates.msfc		2124	msf	precious.E01/Partition 1...	Netsca...	1536 B	1349 B	D5DF7...	6EF691...	468BD...	2005-01-01 ...	2005-01-...	2004-12-30 10:...
<input checked="" type="checkbox"/>	text2.zip Finished 12/21/...		5311		precious.E01/Partition 1...	Email O...	n/a	2070 B				n/a		n/a
<input checked="" type="checkbox"/>	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

The screenshot displays a file analysis application with the following components:

- File List (Left Pane):** A tree view showing file categories. 'JPEG (410 / 410)' is highlighted under 'Raster Graphics'.
- File Content (Main Pane):** A hex dump of a file header. The first two bytes, 'ff d8', are highlighted with a red box, indicating the start of a JPEG file. The text on the right shows the ASCII representation of the header, including 'JFIF'.
- File List (Bottom Pane):** A table listing files with columns for Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Accessed. The files listed are:

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed
\$R2M7A26.jpg		1246	jpg	Mantooth32.E01/Partiti...	JPEG	14.00 KB	13.82 KB	489E96...	870A9...	92D29...	7/26/2007 6:27...	7/26/...
\$R9HZO20.jpg		1248	jpg	Mantooth32.E01/Partiti...	JPEG	6656 B	6468 B	6FB3C...	65B5D...	A0432...	7/26/2007 6:27...	7/26/...
\$R3QVPHB.jpg		1251	jpg	Mantooth32.E01/Partiti...	JPEG	11.50 KB	11.30 KB	395FE2...	F98320...	B4FB9E...	7/26/2007 6:27...	7/26/...
07-09-very-old-man.jpg		1701	jpg	Mantooth32.E01/Partiti...	JPEG	42.00 KB	41.72 KB	DFD36...	D3B25...	129482...	7/25/2007 6:41...	7/25/...
0cb[1].jpg		3247	jpg	Mantooth32.E01/Partiti...	JPEG	481 B	481 B	347176...	A4204...	CCB55...	7/12/2007 6:16...	7/12/...
0cm[1].jpg		3093	jpg	Mantooth32.E01/Partiti...	JPEG	297 B	297 B	9A181...	73EC9...	2AE54...	7/12/2007 6:16...	7/12/...
0ct[1].jpg		3248	jpg	Mantooth32.E01/Partiti...	JPEG	455 B	455 B	32B718...	B73E1E...	EBF5F6...	7/12/2007 6:16...	7/12/...
0lb[1].ico		3018	ico	Mantooth32.E01/Partiti...	JPEG	368 B	368 B	64A0F...	A9C3D...	291CE...	7/12/2007 6:16...	7/12/...

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

Ready | Overview Tab Filter: [None]

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

# Viewing Options

The screenshot displays a file analysis application with a menu bar (File, Edit, View, Evidence, Filter, Tools, Help) and a toolbar. The 'View' menu is open, showing options like 'Hex', 'Text', 'Filtered', and 'Natural'. The 'Text' view is selected, showing the content of a file named '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'. The content is displayed in a text editor with a cursor at position 0. The left pane shows a file tree with categories like Documents, Email, Executable, Folders, Graphics, Internet/Chat Files, Mobile Phone Data, Multimedia, OS/File System Files, Other Encryption Files, and Other Known Types. The bottom pane shows a file list with columns for Name, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Accessed. The status bar at the bottom indicates 'Ready' and 'Overview Tab Filter: [None]'.

File Content

Hex Text Filtered Natural

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 2f 77 77 77 2e 61-70 70 6c 69 65 64 6c 61 ://www.appliedia  
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-7f 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

Cursor pos = 0

File Content Properties Hex Interpreter

File List

Name	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/...
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/Partitio...	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/...

Loaded: 23 Filtered: 23 Total: 23 Highlighted: 1 Checked: 0

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

Notepad View

# Viewing File/Folder Properties

The screenshot displays a file management application with a menu bar (File, Edit, View, Evidence, Filter, Tools, Help) and a toolbar. The left pane shows a tree view of folders and files, including 'Documents (2,001 / 2,001)', 'Adobe Documents (5 / 5)', 'HTML and XML (518 / 518)', 'Lotus Documents (4 / 4)', '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 right pane shows the 'Properties' dialog for the selected file 'Confidential Business Letter.doc'. The 'General Info' section includes 'Name', 'Item Number', 'File Type', and 'Path'. The 'File Size' section shows 'Physical Size' and 'Logical Size'. The 'File Dates' section shows 'Date Created', 'Date Accessed', and 'Date Modified'. The 'File Attributes' section includes 'General' attributes like 'Actual File', 'Duplicate File', 'From Email', and 'File Type'. The bottom pane shows a 'File List' table with columns for Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Accessed. The table lists four files: 'Astral.doc', 'Confidential Business Letter.doc', 'Confidential Business Letter.doc', and 'Dear Sweetie.doc'. The status bar at the bottom shows 'Loaded: 23', 'Filtered: 23', 'Total: 23', 'Highlighted: 1', 'Checked: 0', and 'Overview Tab Filter: [None]'. The bottom-most text shows the full path of the selected file: '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'.

File Edit View Evidence Filter Tools Help

Filter: - unfiltered - Define...

Explore Overview Email Graphics Bookmarks Live Search Index Search

Case Overview

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 / 3)
    - Microsoft Word 2002 (1 / 1)
    - Microsoft Word 2003 (2 / 2)
    - Microsoft Word 6.0 (8 / 8)
- 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)

Other Known Types (150 / 150)

Properties

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 Content Properties Hex Interpreter

File List

	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Accessed
<input type="checkbox"/>	Astral.doc		1222	doc	Mantooth32.E01/Partiti...	Microso...	38.00 KB	38.00 KB	7CED6...	59B829...	7850A...	2/12/2008 4:53...	2/12/...
<input type="checkbox"/>	Confidential Business Le...		3789	doc	Mantooth32.E01/Partiti...	Microso...	n/a	29.15 KB	8C778...	3D9EC...	1D554...	n/a	n/a
<input type="checkbox"/>	Confidential Business Le...		15274	doc	Washer 17.E01/Partiti...	Microso...	39.69 KB	29.00 KB	8C778...	3D9EC...	1D554...	n/a	n/a
<input type="checkbox"/>	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/...

Loaded: 23 Filtered: 23 Total: 23 Highlighted: 1 Checked: 0

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

Evidence

- diskette-usb.E01
  - EVIDENCE [FAT12]
    - [root]
      - 10-1 Graphics
      - DT Search Stuff
      - Recent
      - Recycler
      - Registry File
      - Sagan Alert
      - TIF Netmail
      - Zip Files

File Content

Hex Text Filtered Natural

0000 3C 73 63 72 69 70 74 20-6C 61 6E 67 75 61 67 65 <script language  
0010 3D 4A 61 76 61 53 63 72-69 70 74 3E 0A 20 20 20 =JavaScript>.  
0020 20 20 20 20 20 64 6F 63-75 6D 65 6E 74 2E 63 6F document.co  
0030 6F 6B 69 65 20 3D 20 22-4A 53 45 6E 61 62 6C 65 okie = "JSEnable  
0040 64 3D 31 22 20 20 0A 20-20 20 20 3C 2F 73 63 72 d=1" . </scr  
0050 69 70 74 3E 0A 0A 0A 0A-0A 0A 0A 0A 0A 20 3C ipt>.....<  
0060 68 74 6D 6C 3E 0A 20 20-20 20 3C 68 65 61 64 3E html> . <head>  
0070 0A 20 20 20 20 20 20 20-20 20 20 20 20 20 20 . <title>MapQ  
0080 75 64 65 64 64 64 64 64-64 64 64 64 64 64 64 uest: Driving Di

Cursor pos =

File Content

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
0 KB 19,50 KB	652F15...	21856F...	9FA62...		2003-09-11
0 KB 19,50 KB	027A5...	9AB4E...	324D2...		2003-09-11
0 KB 20,49 KB	155230...	7953C...	1EC8E...		2003-09-28
0 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

The screenshot displays the Hex Interpreter application interface. The top menu bar includes File, Edit, View, Evidence, Filter, Tools, and Help. Below the menu is a toolbar with icons for file operations and a search filter set to "-unfiltered-". The main window is divided into three panes. The left pane, titled "Case Overview", shows a tree view of file categories such as File Items, File Extension, File Category, Archives, Databases, Documents, Email, Executable, Folders, Graphics, Internet/Chat Files, Mobile Phone Data, Multimedia, OS/File System Files, and Other Encryption Files. The middle pane, titled "Hex Interpreter", displays a table of file metadata. The right pane, titled "File Content", shows the hex data for the selected file. The bottom pane, titled "File List", shows a table of file entries with columns for Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Accessed. The status bar at the bottom indicates "Ready" and "Overview Tab Filter: [None]".

File Extension ( 5,248 / 5,248 )  
File Category ( 14,077 / 14,077 )  
Archives ( 170 / 170 )  
Databases ( 3 / 3 )  
Documents ( 2,001 / 2,001 )  
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 )  
Disk Image ( 3 / 3 )  
File System ( 4 / 4 )  
Index Allocation ( 266 / 266 )  
Partition ( 3 / 3 )  
Recycle Bin Index ( 5 / 5 )  
Windows NT Registry ( 23 / 23 )  
Windows Shortcut ( 242 / 242 )  
Other Encryption Files ( 29 / 29 )  
Other Known Types ( 150 / 150 )  
Presentations ( 16 / 16 )

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 +	MLJ

Byte order: ☒ Little endian ☐ Big endian

File Content | Properties | Hex Interpreter

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:...	8/3/2
INFO2		5427	<missin...	Washer 17.E01/Partitio...	Recycl...	1024 B	820 B	FB4B0...	244FC...	5535C...	8/3/2007 6:40:...	8/3/2
INFO2		5432	<missin...	Washer 17.E01/Partitio...	Recycl...	2560 B	2420 B	584428...	8D098...	5BF20B...	8/3/2007 6:39:...	8/3/2
INFO2		5436	<missin...	Washer 17.E01/Partitio...	Recycl...	2048 B	1620 B	FD4F8...	6D946...	F40009...	8/3/2007 6:35:...	8/3/2

Loaded: 5 | Filtered: 5 | Total: 5 | Highlighted: 1 | Checked: 0

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 displays a forensic analysis tool interface. The left pane shows a tree view of file system components, with 'Slack/Free Space (92 / 92)' expanded and its sub-items 'File System Slack (1 / 1)', 'Slack Space (44 / 44)', 'Unallocated Space (46 / 46)', and 'Unpartitioned Space (1 / 1)' visible. The main pane shows a hex dump of data, with a red box highlighting the text 'Cursor pos = 0; clus = 6350; log sec = 6350; phy sec = 6413'. The bottom pane shows a file list with columns for Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Access. The file '006350' is highlighted in the list.

File Content

Hex Text Filtered Natural

0000 49 4e 44 58 28 00 09 00-98 4b 88 01 00 00 00 00 INDX{...K...  
0010 00 00 00 00 00 00 00 00-28 00 00 00 78 0d 00 00 .....(..x..  
0020 e8 0f 00 00 00 00 00 00-20 00 01 00 c7 01 01 00 è.....Ç..  
0030 01 00 01 00 01 00 00 00-00 00 00 00 00 00 00 00 .....P..  
0040 7f 06 00 00 00 00 01 00-60 00 50 00 00 00 00 00 .....`P..  
0050 7e 06 00 00 00 00 01 00-07 3b 27 09 db c0 c7 01 ~.....;'.ÛÀÇ.  
0060 2e 39 a7 09 db c0 c7 01-18 9f bc 14 b8 6d c8 01 .9S·ÛÀÇ···x·,mE·  
0070 44 11 27 b3 ca 6d c8 01-00 00 00 00 00 00 00 00 D·'·ÊmE·····  
0080 00 00 00 00 00 00 00 00-22 20 00 10 00 00 00 00 ....."  
0090 07 03 41 00 70 00 70 00-44 00 61 00 74 00 61 00 ··A·p·p·D·a·t·a·  
00a0 f2 06 00 00 00 00 01 00-78 00 62 00 00 00 00 00 ò.....x·b·...  
00b0 7e 06 00 00 00 00 01 00-96 62 24 0a db c0 c7 01 ~.....bç·ÛÀÇ·  
00c0 b5 64 d2 a5 b3 5a c7 01-da 8a c8 14 b8 6d c8 01 µdÖW·ZÇ·Û·Ê·,mE·  
00d0 ac 9a 30 b3 ca 6d c8 01-00 00 00 00 00 00 00 00 ¬·0·ÊmE·····  
00e0 00 00 00 00 00 00 00-00 00 00 10 00 00 00 00 .....  
00f0 10 01 41 00 70 00 70 00-6c 00 69 00 63 00 61 00 ··A·p·p·l·i·c·a·

Cursor pos = 0; clus = 6350; log sec = 6350; phy sec = 6413

File List

Item #	Name	Label	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Access
1177	000001			Mantooth32.E01/Unpar...	Unalloc...	31.00 KB	31.00 KB				n/a	n/a
1179	006318			Mantooth32.E01/Partiti...	Unalloc...	12.00 KB	12.00 KB				n/a	n/a
1180	006350			Mantooth32.E01/Partiti...	Unalloc...	12.00 KB	12.00 KB				n/a	n/a
1181	007770			Mantooth32.E01/Partiti...	Unalloc...	354.5 KB	354.5 KB				n/a	n/a
1182	018270			Mantooth32.E01/Partiti...	Unalloc...	512.0 KB	512.0 KB				n/a	n/a
1183	023498			Mantooth32.E01/Partiti...	Unalloc...	512 B	512 B				n/a	n/a
1208	0302			Mantooth32.E01/Partiti...	Unalloc...	211.0 KB	211.0 KB				n/a	n/a
1184	043782			Mantooth32.E01/Partiti...	Unalloc...	980.0 KB	980.0 KB				n/a	n/a

Loaded: 46 Filtered: 46 Total: 46 Highlighted: 1 Checked: 0

Ready Overview Tab Filter: [None]

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 Status
- 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 List

	Subject	Name	To	From	CC	BCC	Submit ...	Deliver...	Unread	Unsent	Has Att...	Created
<input checked="" type="checkbox"/>	frodbaggi, ge...	1/2/2005 eBay...	baggifr...	eBay@...			2005-0...	2005-0...	False		False	n/a
<input checked="" type="checkbox"/>	You want it, eB...	12/23/2004 eB...	baggifr...	eBay@...			2004-1...	2004-1...	False		False	n/a
<input checked="" type="checkbox"/>	frodbaggi sen...	4/29/2005 bag...	samwiz...	baggifr...			2005-0...	2005-0...	False		False	n/a
<input checked="" type="checkbox"/>	RE: HELP!	4/29/2005 jpar...	Baggifr...	jparry...			2005-0...	2005-0...	False		False	n/a
<input checked="" type="checkbox"/>	RE: Southeast ...	4/29/2005 swa...	Baggifr...	swater...			2005-0...	2005-0...	False		False	n/a

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

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

Email Attachments

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

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/All Users/.../baggifrodo»baggifrodo»Mail»Incoming»Saved Mail»4292005 swaters@accessda RE: Southeast Cybercrime Summit

Ready

Email Tab Filter: Email Files and Attachments

# 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].jpg 0601\_top03[1].jpg 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 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
<input type="checkbox"/>		040_fp0993_a[1].jpg		2682	jpg	precious.E01/Partition 1...	JPEG	2048 B	1791 B	F48EEB...	19B318...	AA5F1...	2005-01-01
<input type="checkbox"/>		040102_alfred.jpg		3038	jpg	precious.E01/Partition 1...	JPEG	20,00 KB	19,52 KB	E56408...	85EDE...	E18B2...	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

File Content

Hex Text Filtered Natural

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
<input checked="" type="checkbox"/>	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 Possible Job!!!

Ready

Bookmarks Tab Filter: [None]

Bookmark Information

Bookmark Name: Message with attachment

Creator Name: hjo

Bookmark Comment:

Supplementary Files:

File Comment:

Attach File Remove File

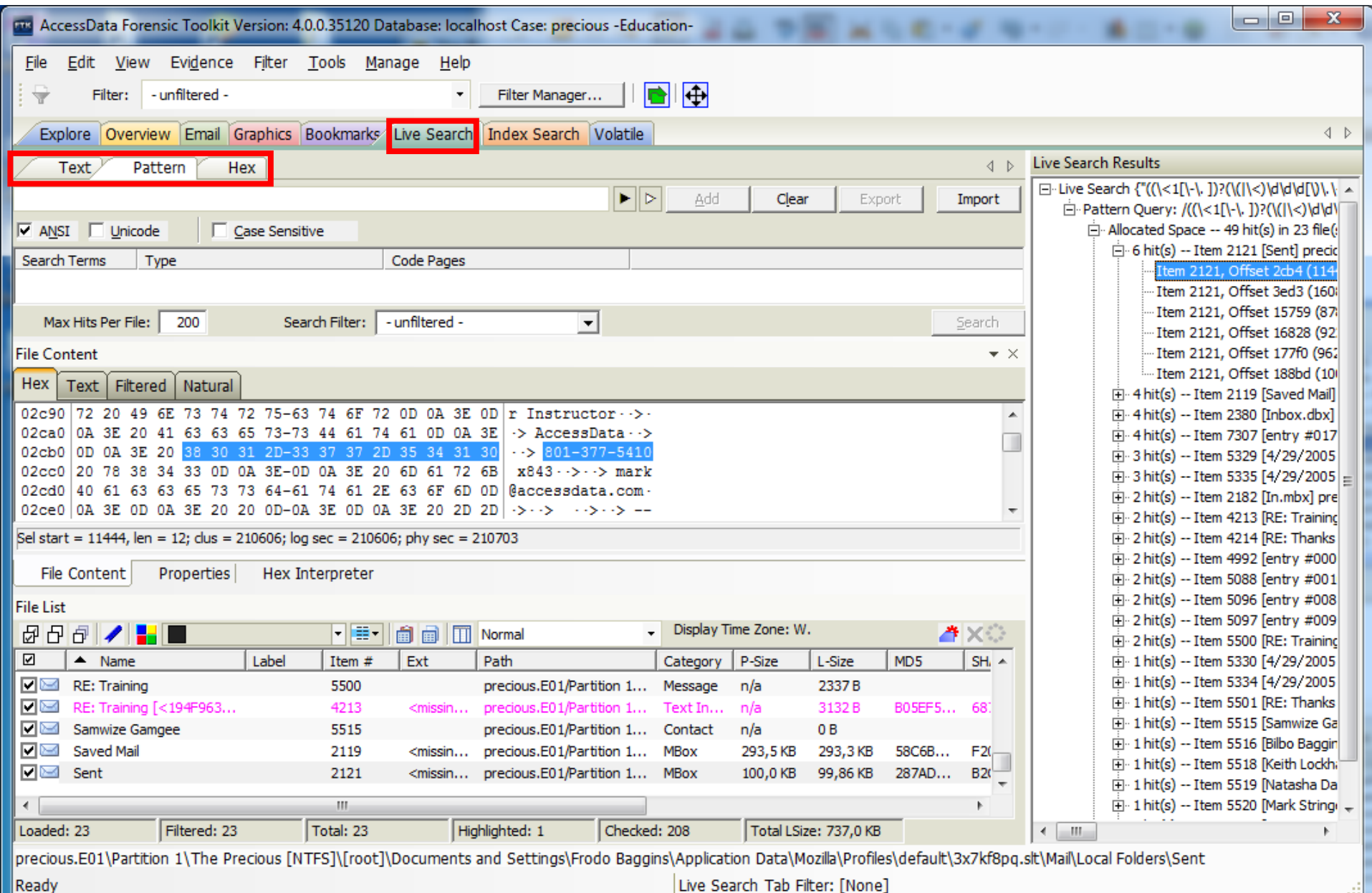
Selection(s):

Selection Comment:

Save Changes Clear Changes Add Selection Remove Selection



# Live Search Tab



# 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

kill Add

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	Total Hits
kill	20

Clear Import... Export... Options... Search Now

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 #
    - [+] 80% - 3 hit(s) -- Item 4096 [entry #
    - [+] 40% - 1 hit(s) -- Item 7215 [entry #
    - [+] 40% - 1 hit(s) -- Item 5969 [entry #
    - [+] 40% - 1 hit(s) -- Item 5965 [entry #
    - [+] 40% - 1 hit(s) -- Item 4074 [entry #
  - [-] 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
  - [-] 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
    - [+] 40% - 1 hit(s) -- Item 2077 [CACHE
- [-] Unallocated Space -- 0 hit(s) in 0 file(s)

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 / center expanded \$ long timer \$! won't close if you moved back on < New TM

File Content Properties Hex Interpreter

File List

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

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\D\_America Online 9.0\idx\main.idx

Ready

Index Search Tab Filter: [None]

# 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.

The 'New Case Options' dialog box is shown with the following fields and settings:

- Owner: Hans Jones
- Case Name: lecturecase
- Reference: (empty)
- Description: This is a lecture test case
- Description File: (empty)
- Case Folder Directory: D:\cases
- Database Directory: (empty)
- ☐ In the case folder
- Processing Profile: AD Standard
- Custom...** (highlighted with a red box)
- ☒ Open the case

The 'Detailed Options' dialog box is shown with the 'Evidence Processing' tab selected. The 'Evidence Processing' section is highlighted with a red box. The following options are visible:

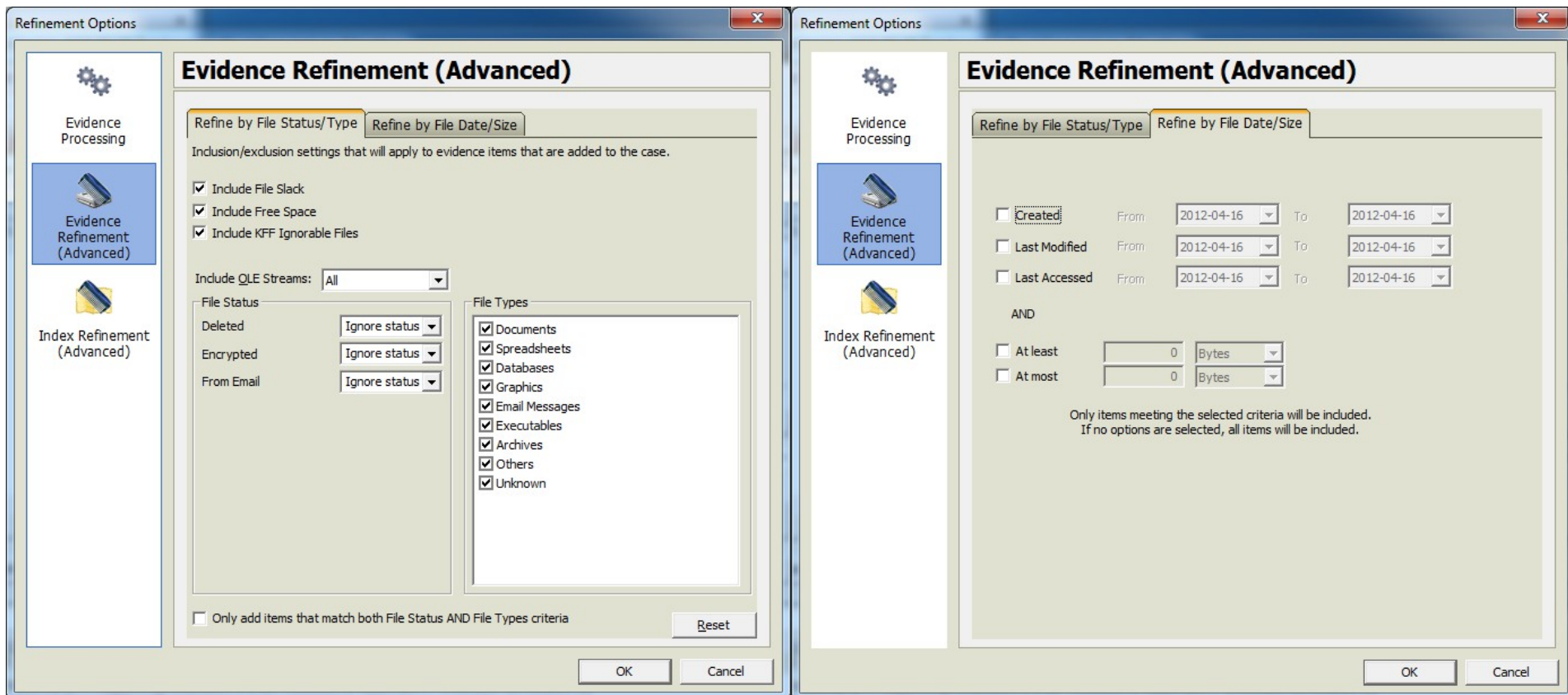
- Evidence Processing** (highlighted with a red box)
- Evidence Refinement (Advanced)
- Index Refinement (Advanced)
- Custom File Identification

The 'Evidence Processing' section includes the following options:

- ☒ Generate File Hashes (flag duplicates)
  - ☒ MD5 Hash
  - ☒ SHA-1 Hash
  - ☒ SHA-256 Hash
  - ☐ Fuzzy Hash
  - ☐ Match Fuzzy Hash Library
  - ☐ Flag Duplicate Files
  - ☐ KFF
  - ☐ PhotoDNA
- ☒ Expand Compound Files
- ☒ File Signature Analysis
- ☒ Flag Bad Extensions
- ☒ Entropy Test
- ☒ dSearch® Text Index
- ☒ Create Thumbnails for Graphics
- ☐ Create Thumbnails for Videos
- ☐ Generate Common Video File
- ☐ HTML File Listing
- ☐ CSV File Listing
- ☐ Data Carve
- ☐ Meta Carve
- ☐ Optical Character Recognition
- ☐ Exploit Image Detection
- ☐ Registry Reports
- ☒ Include Deleted Files
- ☐ Cerberus Analysis
- ☐ Send Email Alert on Job Completion
- ☐ Decrypt Credent Files
- ☐ Process Internet Browser History for Visualization
- ☐ Cache Common Filters
- ☐ Perform Automatic Decryption
- ☐ Language Identification

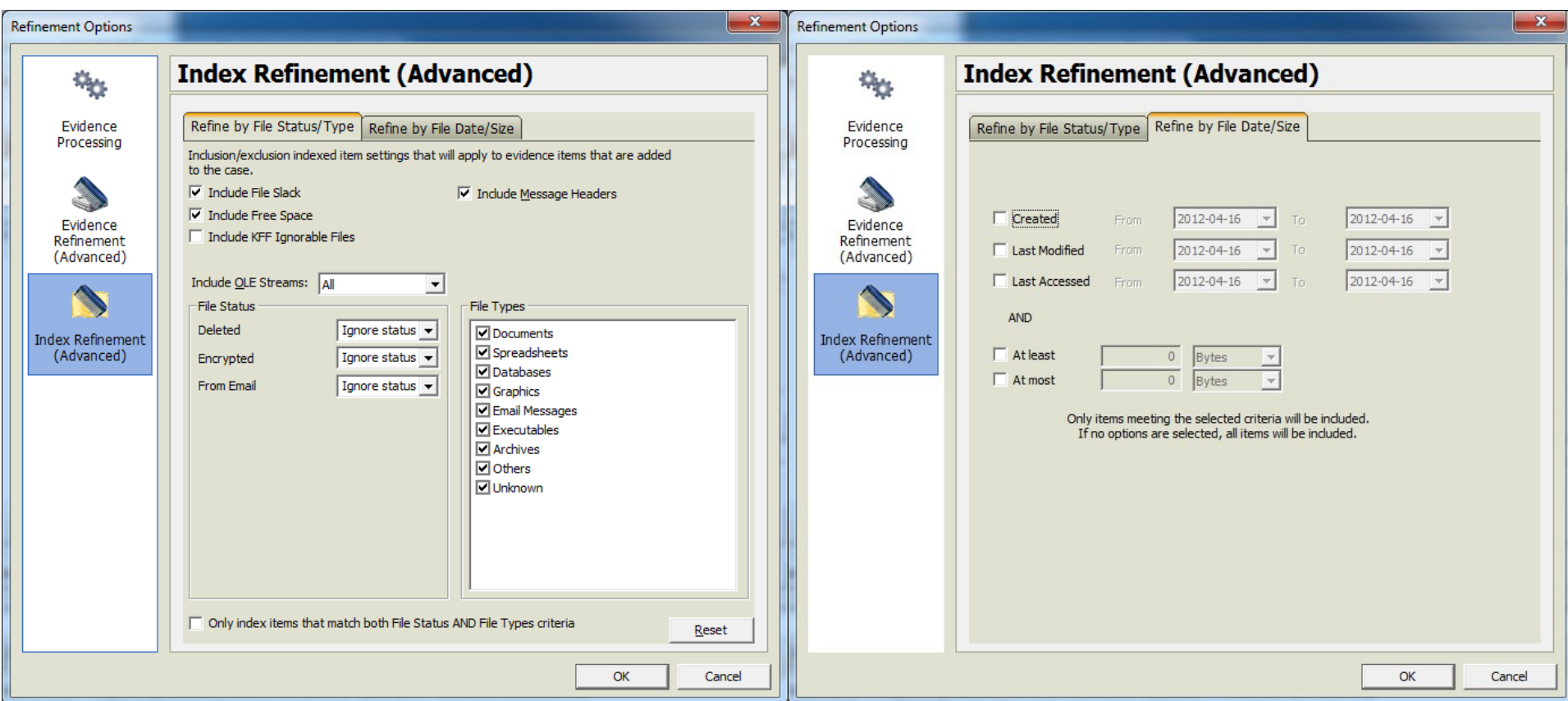
# Refining Case Evidence

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



# Defining Index Parameters

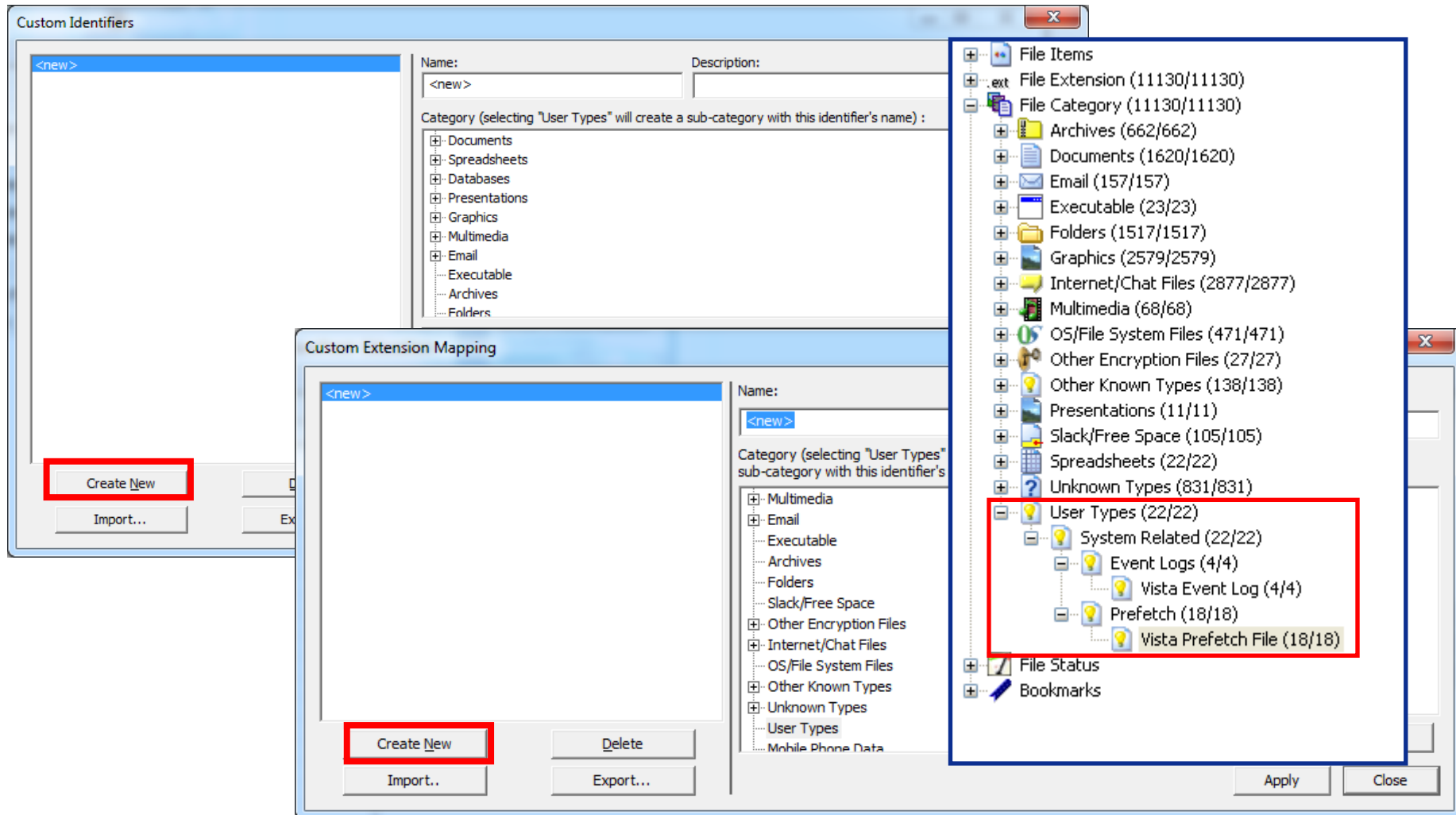
- Usually not needed to modify these parameters
- Refine by: Type, Status, Date/Size





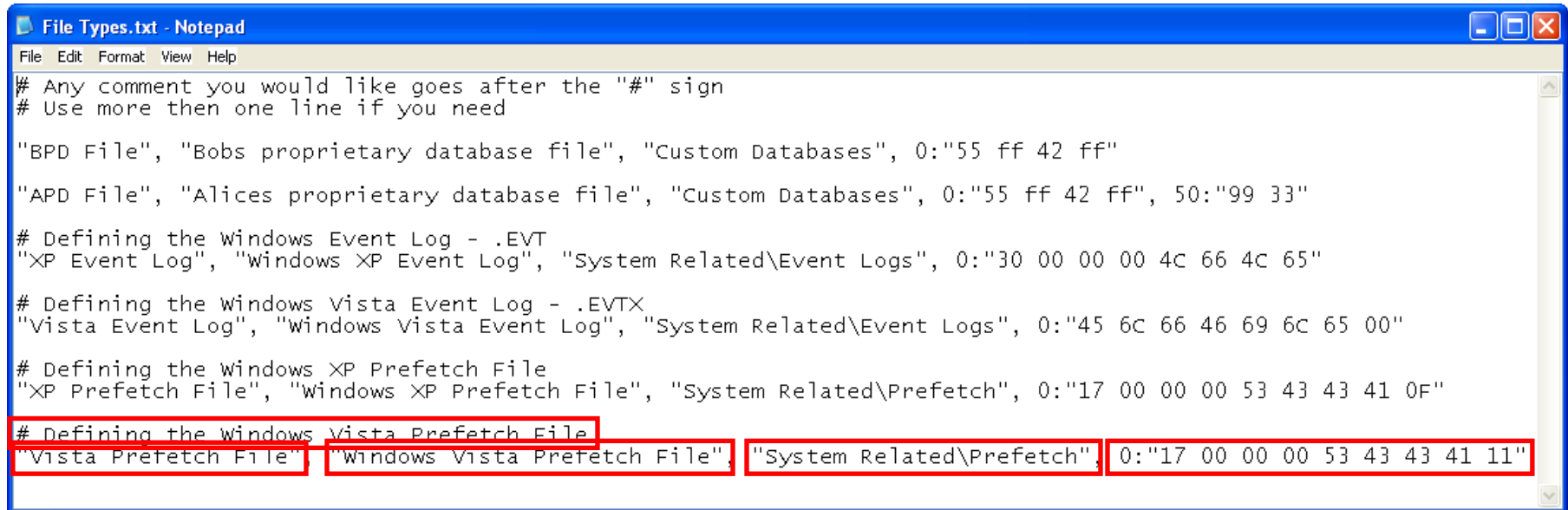
# Custom File Identification

- Allows user-defined file identification for header and suffix



# Custom File Identification

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



```
# Any comment you would like goes after the "#" sign
# Use more then 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"
```

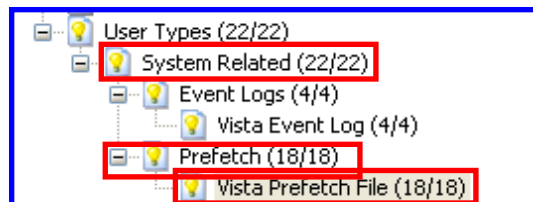
**# = Comments (ignored)**

**File type label**

**Description = For reference only**

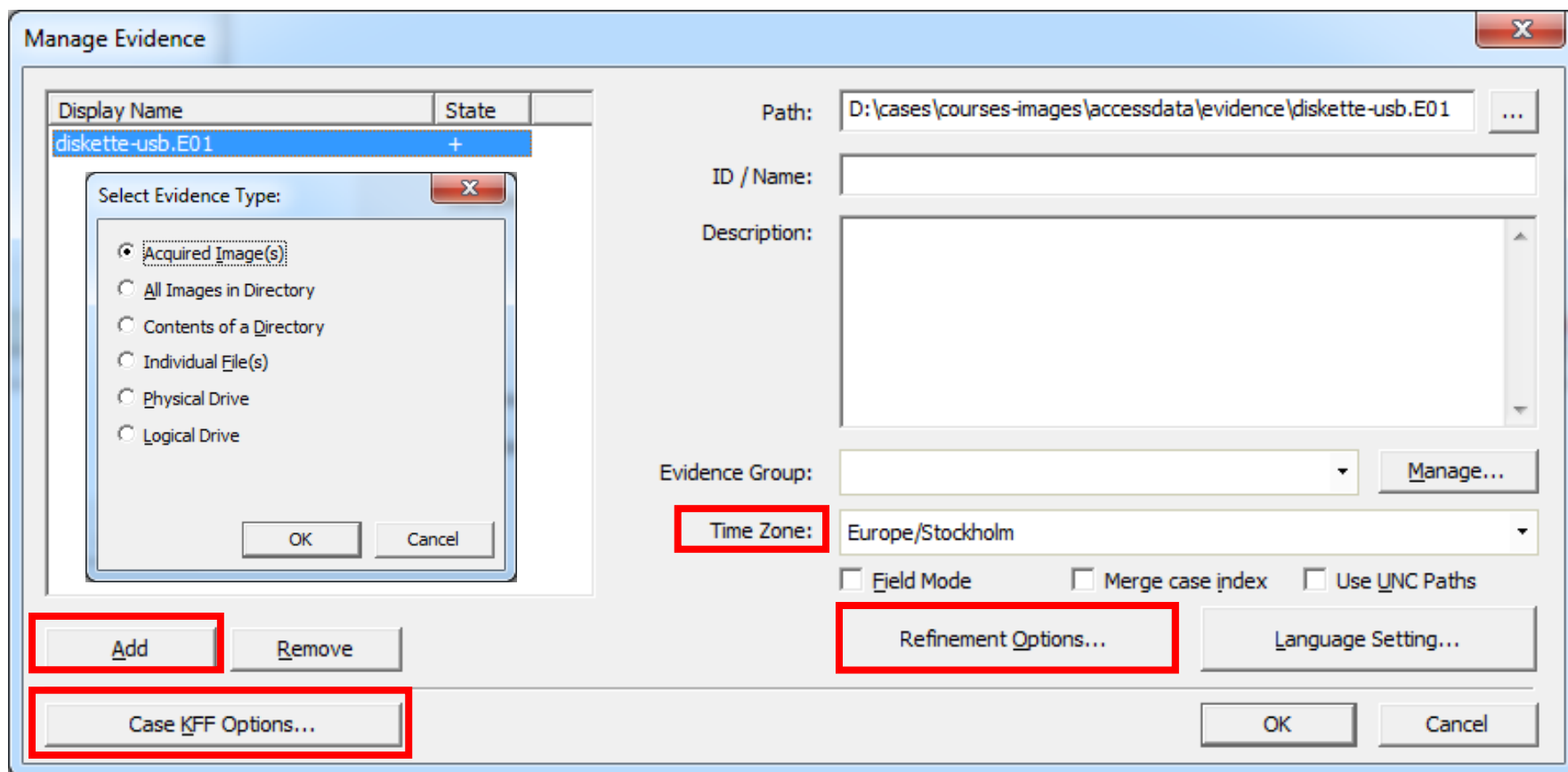
**Category path relative to "User Types"**

**Offset and hex values (AND/OR)**

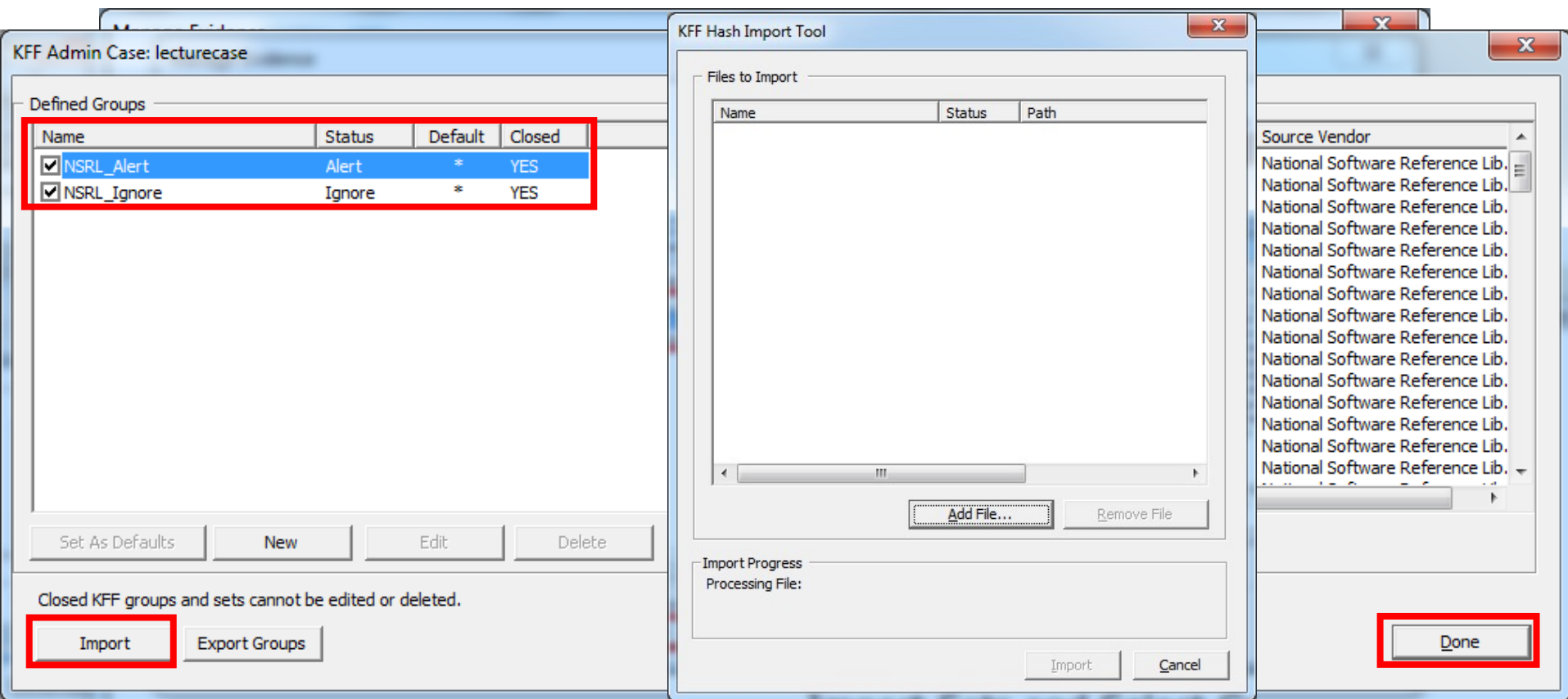


# Creating a New Case cont.

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



# KFF Processing



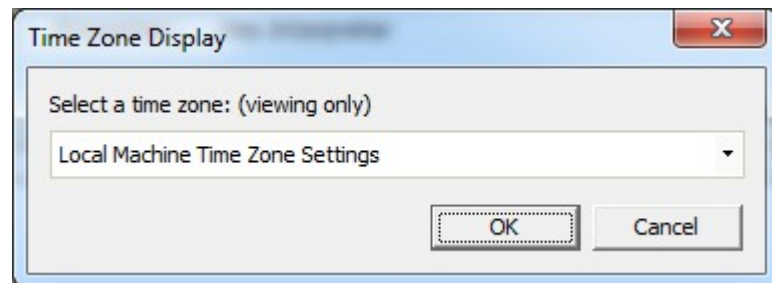
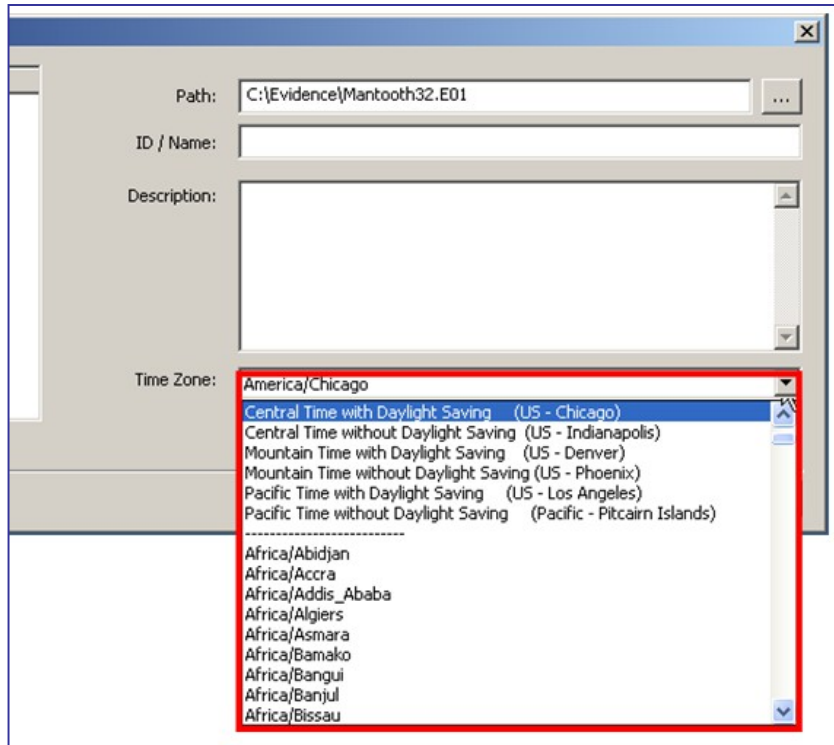
## Import Sets and Select Groups

# 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

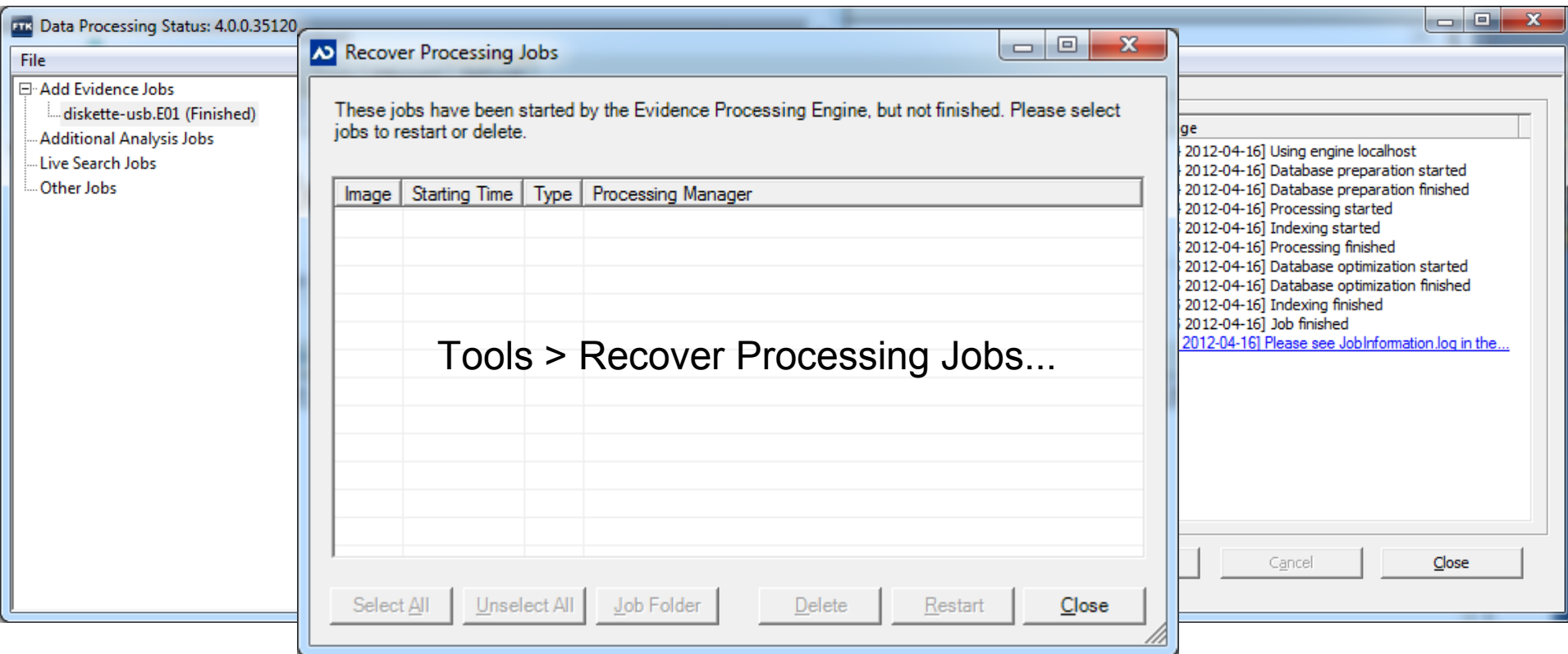
View > Time Zone Display...



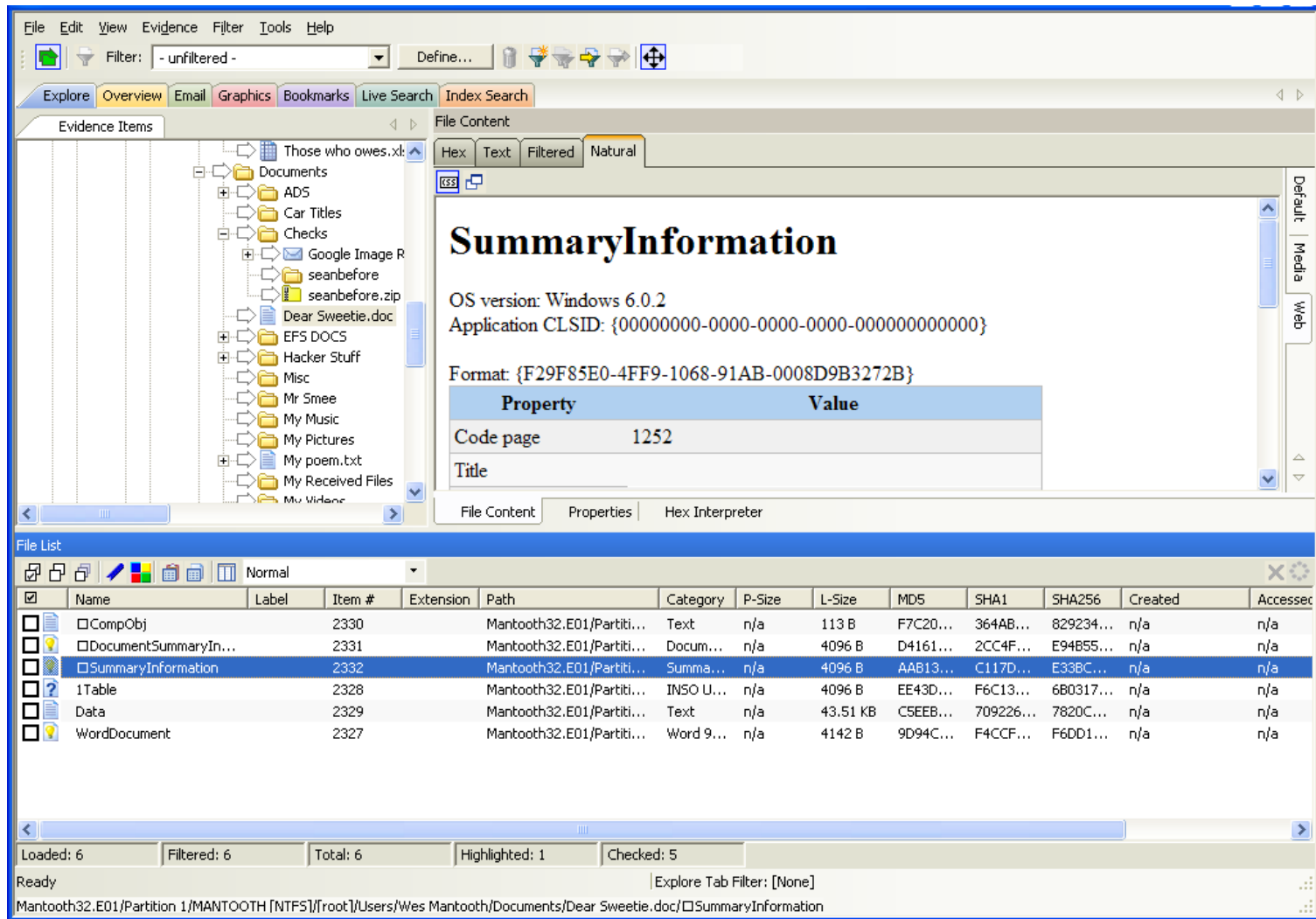


# Jobs and recover jobs

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

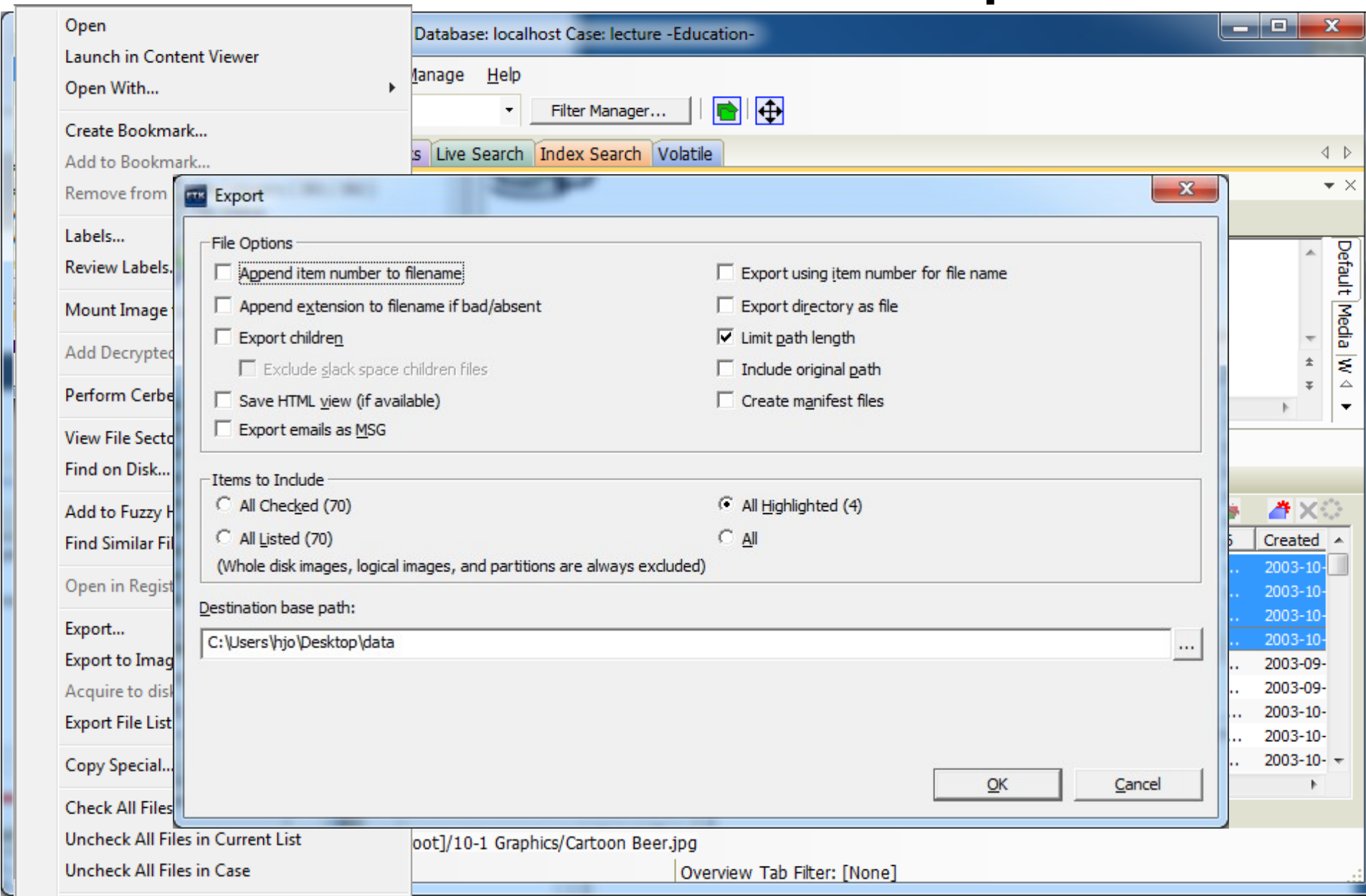


# Compound Files



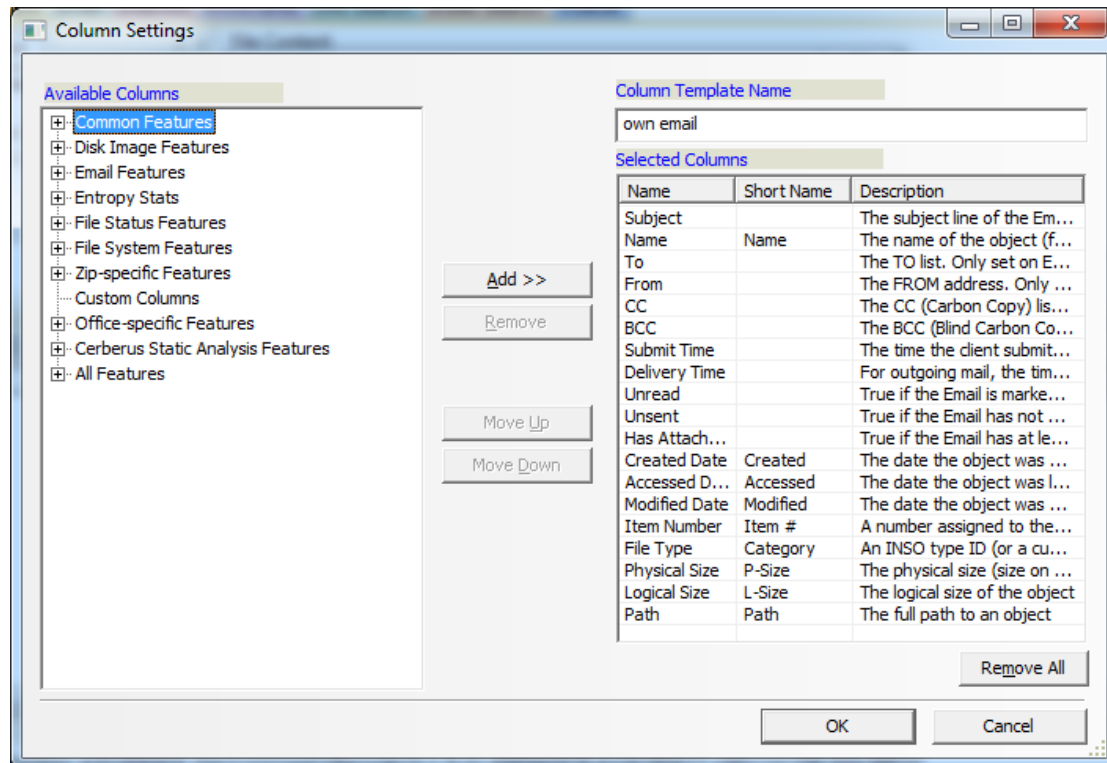
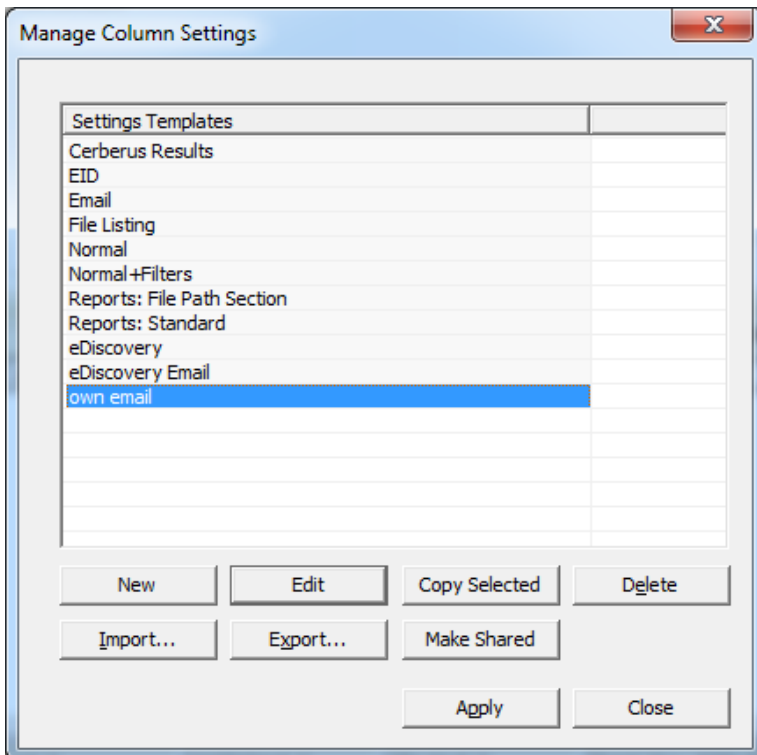
Compound files must also appear in the folder tree so they can be selected - to see their children.

# File and Folder Export

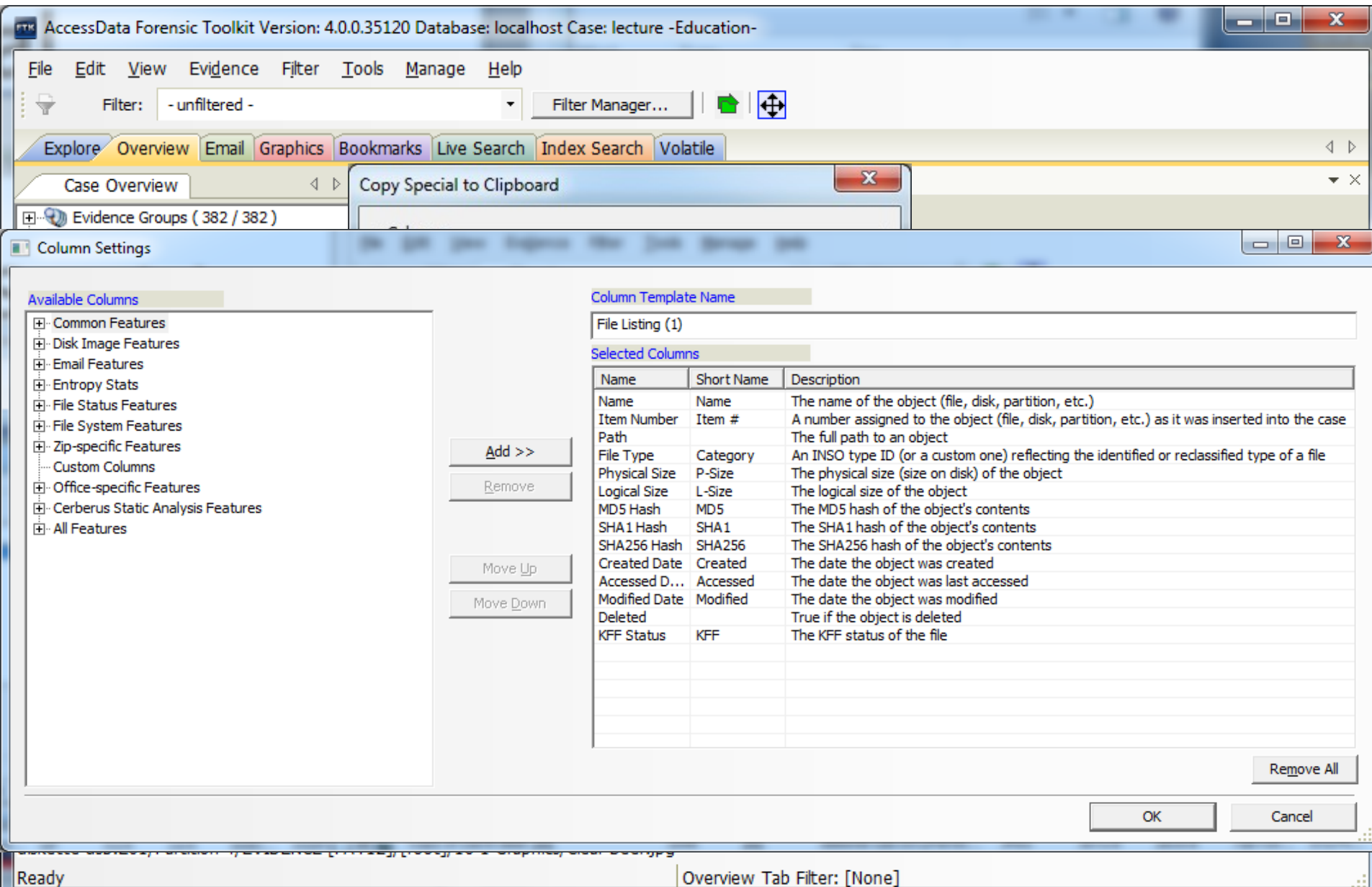


# Column Settings

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

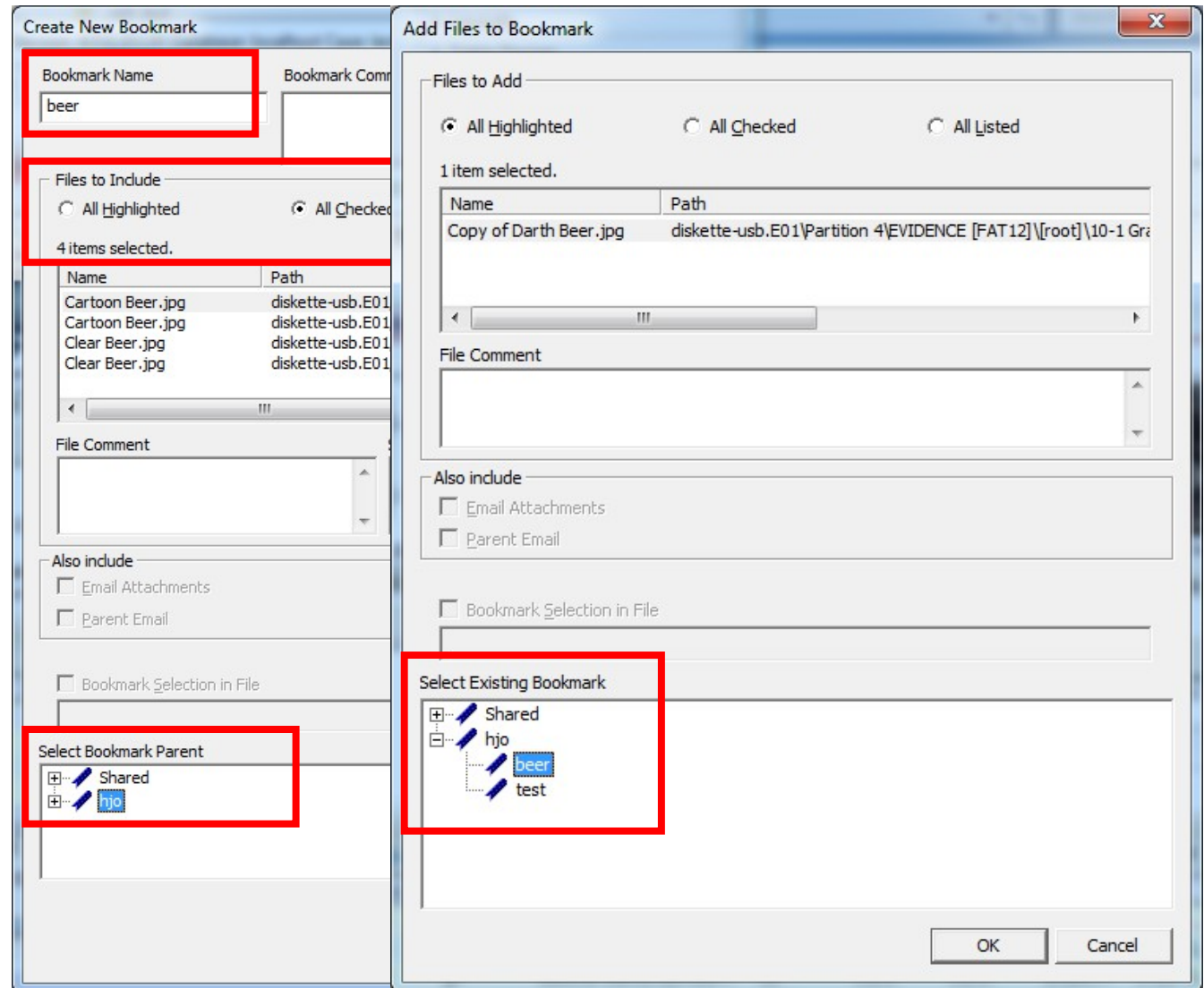
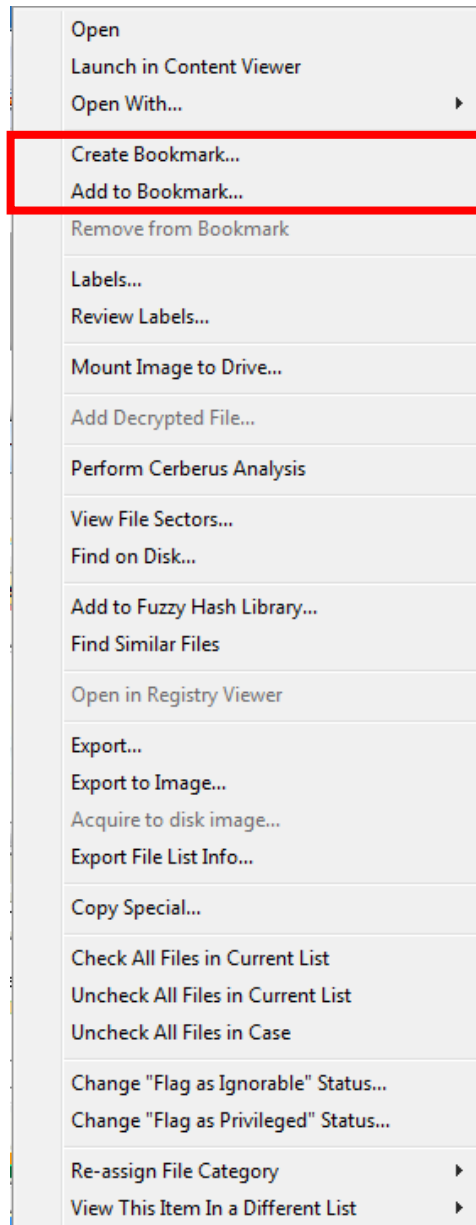


# Copy Special > clipboard





# Create and Add Bookmarks



# Managing Bookmarks

The screenshot shows a software interface with a menu bar (File, Edit, View, Evidence, Filter, Tools, Help) and a toolbar. The main window is divided into several panes:

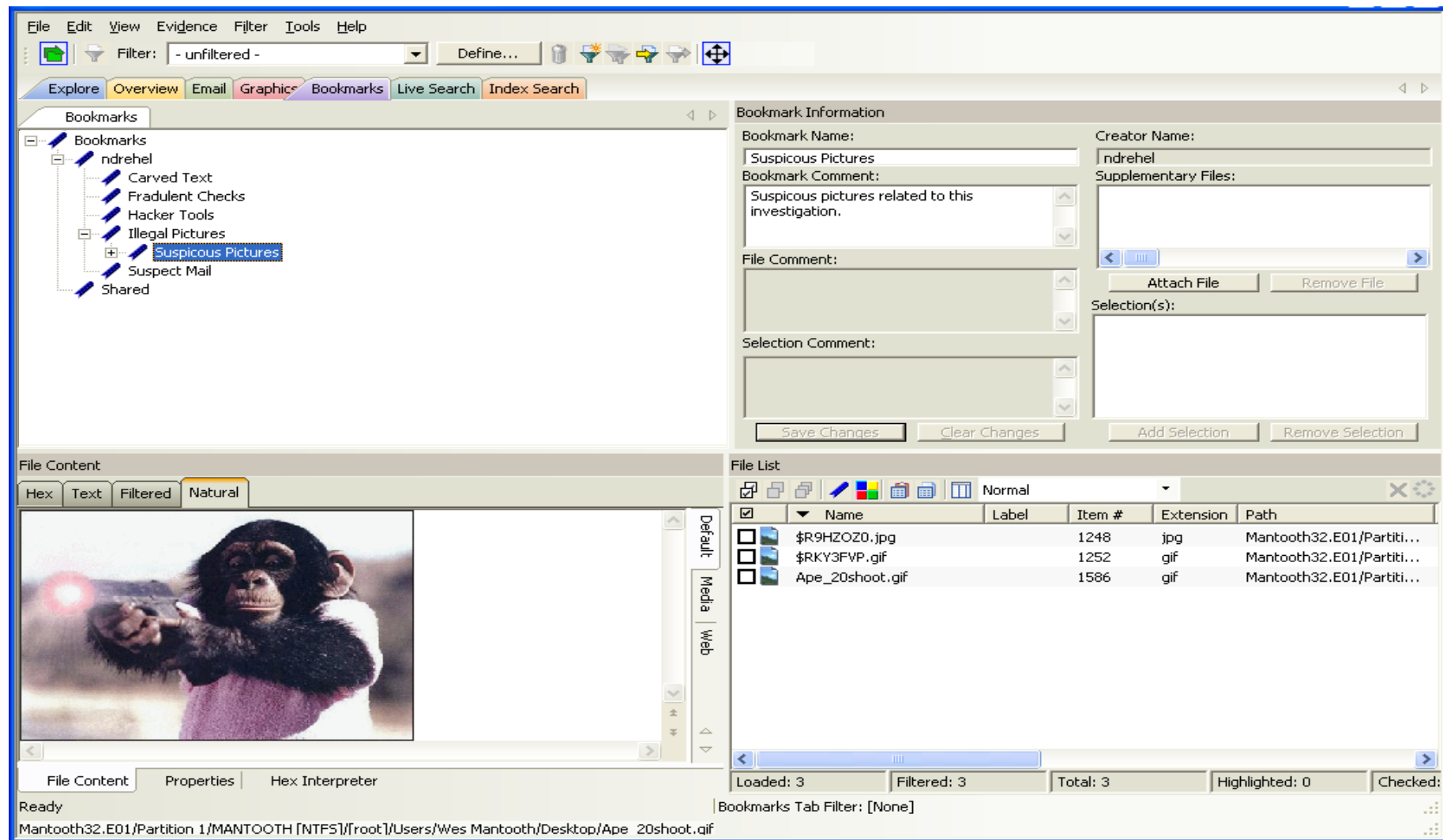
- Bookmarks Pane:** Displays a tree view of bookmarks under the 'Bookmarks' folder. The 'Suspicious Pictures' bookmark is selected.
- Bookmark Information Pane:** Shows details for the selected bookmark.
  - Bookmark Name: Suspicious Pictures
  - Creator Name: ndrehel
  - Bookmark Comment: Suspicious pictures related to this investigation.
  - File Comment: (Empty text area)
  - Selection Comment: (Empty text area)
  - Buttons: Attach File, Remove File, Save Changes, Clear Changes, Add Selection, Remove Selection
- File Content Pane:** Displays the content of the selected file. It shows a photograph of a chimpanzee holding a gun. The pane has tabs for Hex, Text, Filtered, and Natural.
- File List Pane:** Displays a list of files in a table format.

**File List Table:**

	Name	Label	Item #	Extension	Path
<input type="checkbox"/>	\$R9HZOZ0.jpg		1248	jpg	Mantooth32.E01/Partiti...
<input type="checkbox"/>	\$RKY3FVP.gif		1252	gif	Mantooth32.E01/Partiti...
<input checked="" type="checkbox"/>	Ape_20shoot.gif		1586	gif	Mantooth32.E01/Partiti...

At the bottom of the interface, there is a status bar showing 'Ready' and the file path: 'Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/Desktop/Ape\_20shoot.gif'. The status bar also includes a 'Bookmarks Tab Filter: [None]' dropdown.

# Managing Bookmarks



**Bookmarks can be nested when created or later!**