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-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.**

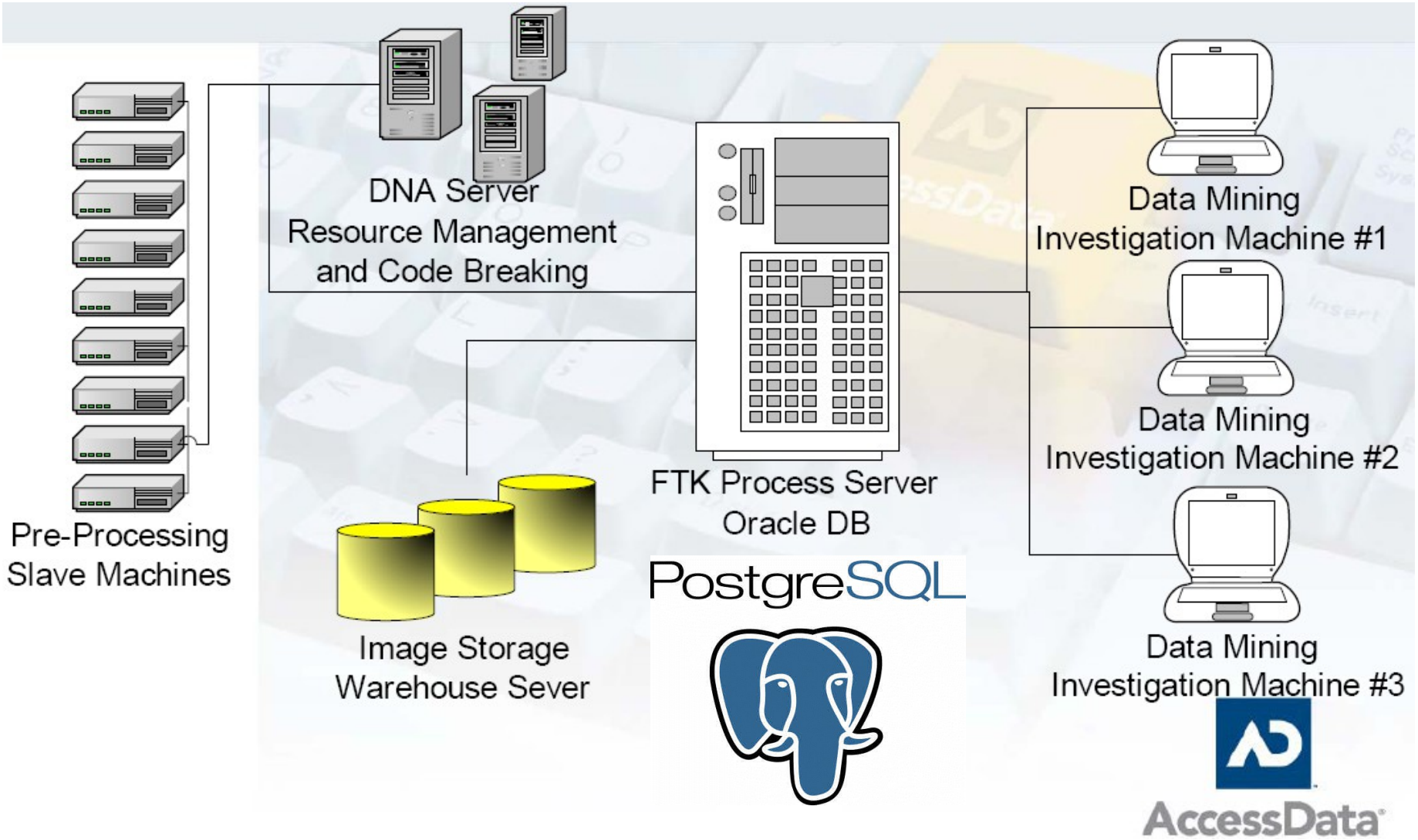
POWERED BY ORACLE

PostgreSQL

Microsoft® SQL Server®

AccessData

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

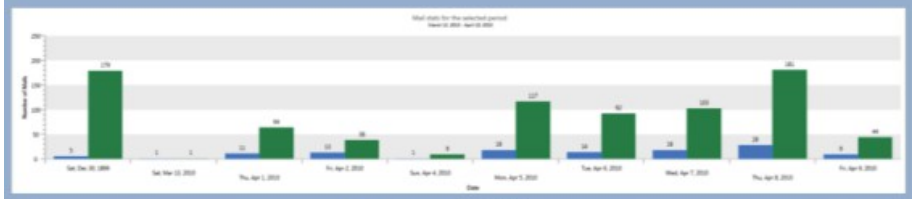


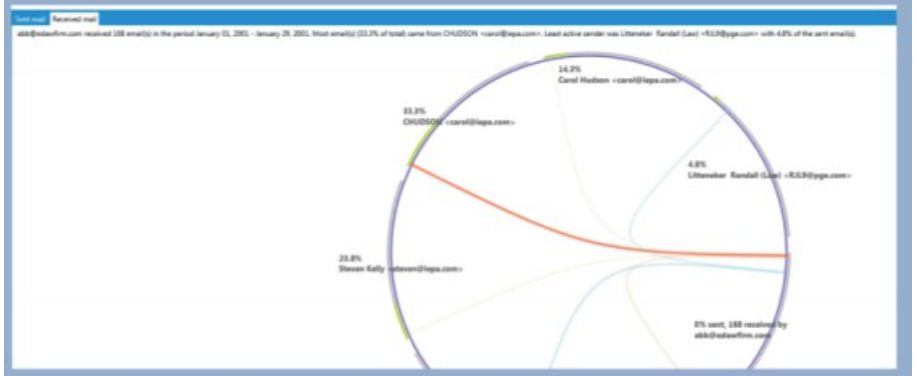
Many FTK 4/5 improvements

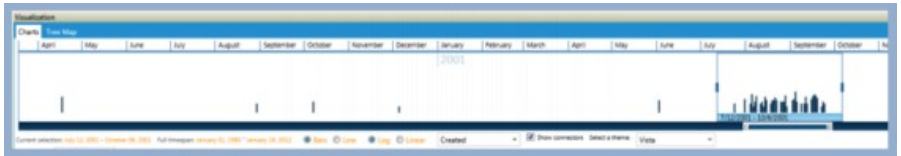
http://accessdata.com/products/computer-forensics/ftk

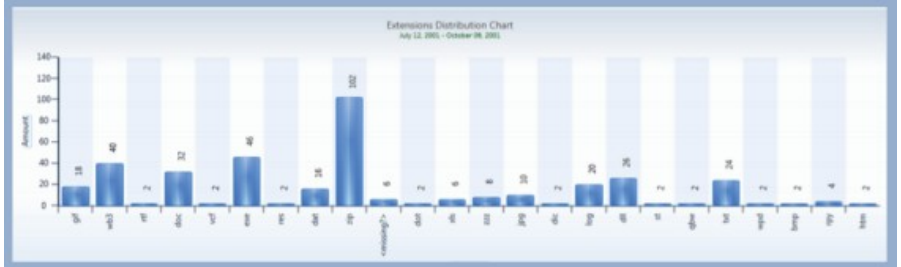
- Most of the improvements are **not** listed here!
- Real DBMS (FTK 2) – Oracle, PostgreSQL
  - GUI is separated from analysis process – crash proof?
- QuickPicks (FTK 2)
  - A feature that lets users view the contents of all subfolders
- Simultaneous multiple user case access (FTK 2)
- Mobile Phone 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

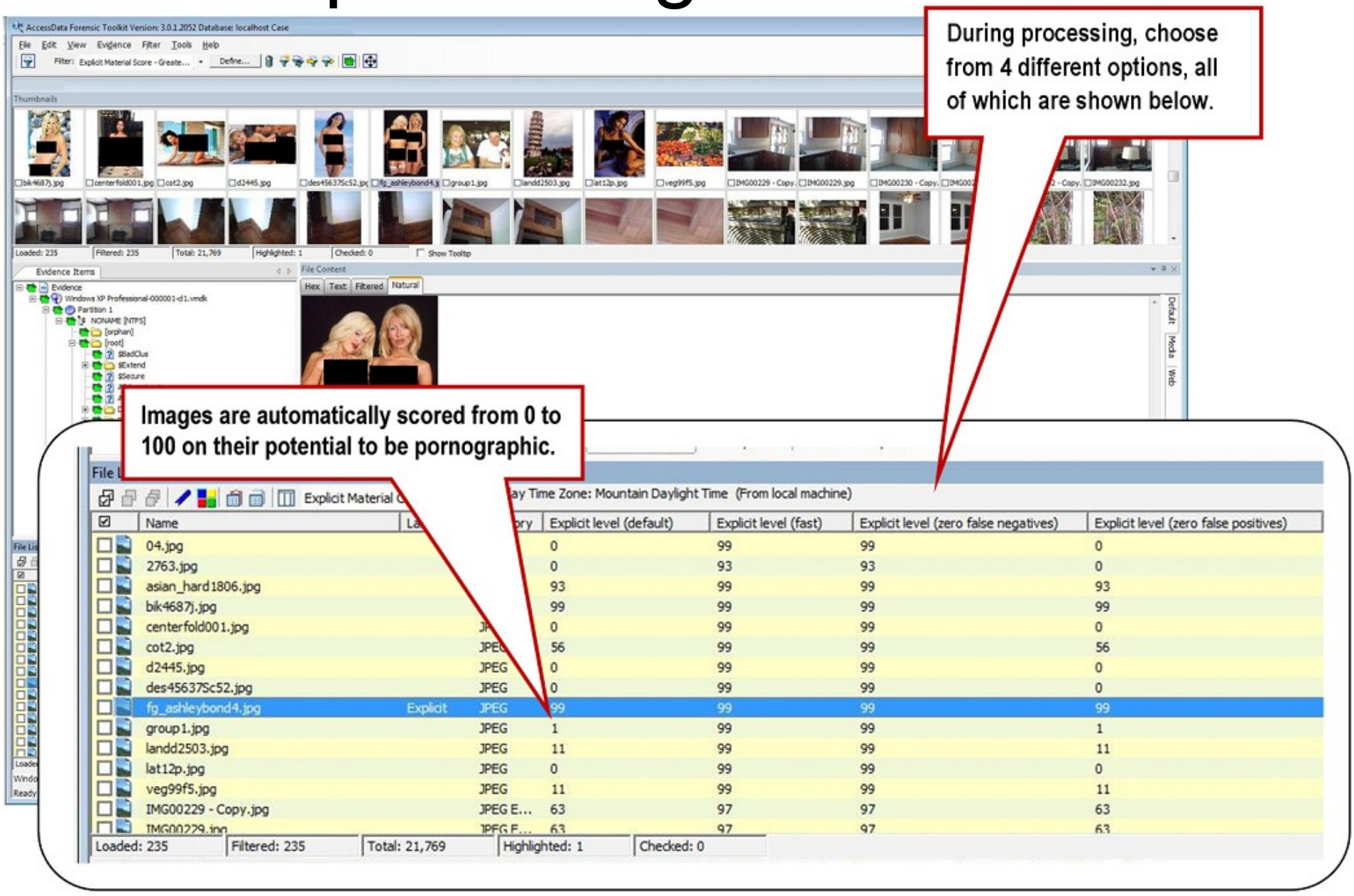




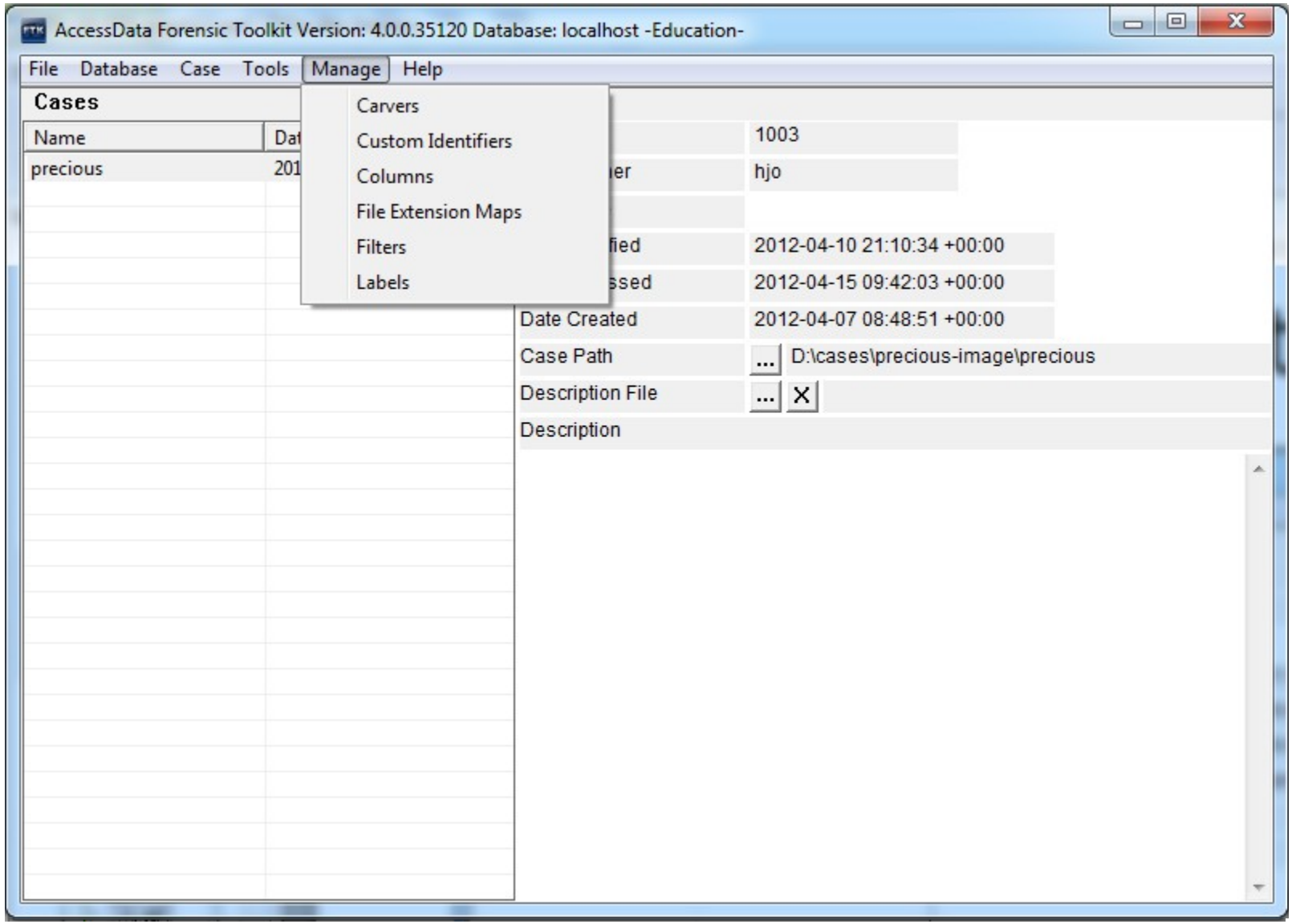




Explicit Image Detection

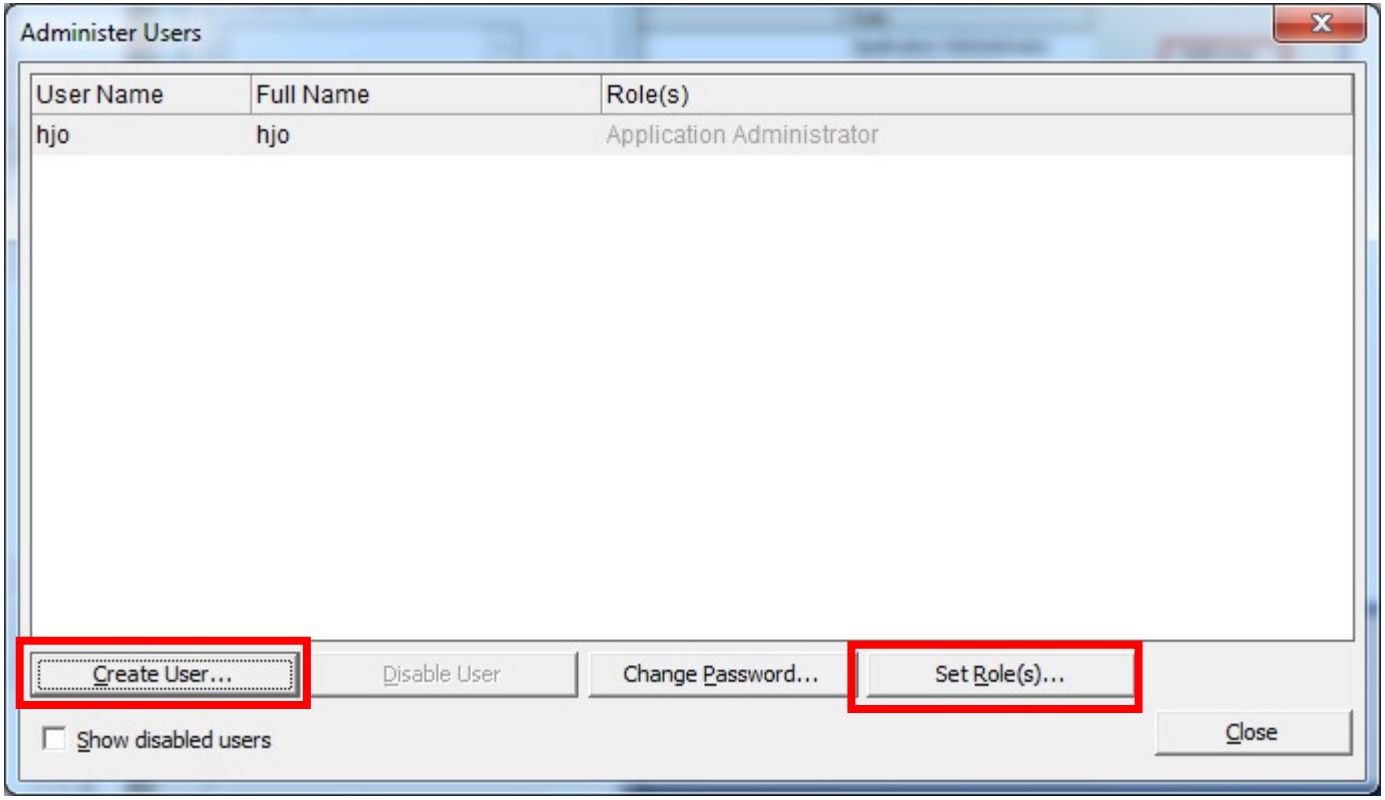


Case Manager Interface

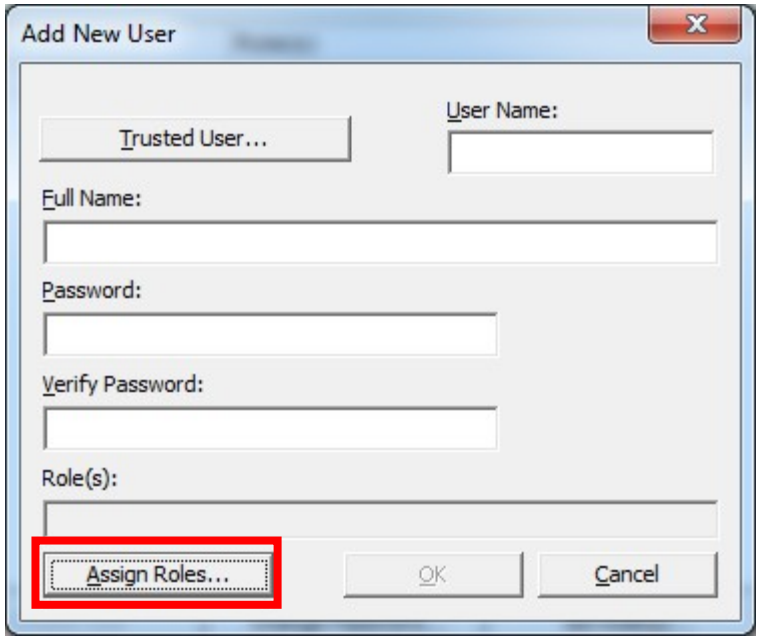


Administer Users 1

- The first user account is the Application Administrator



Administer Users 2

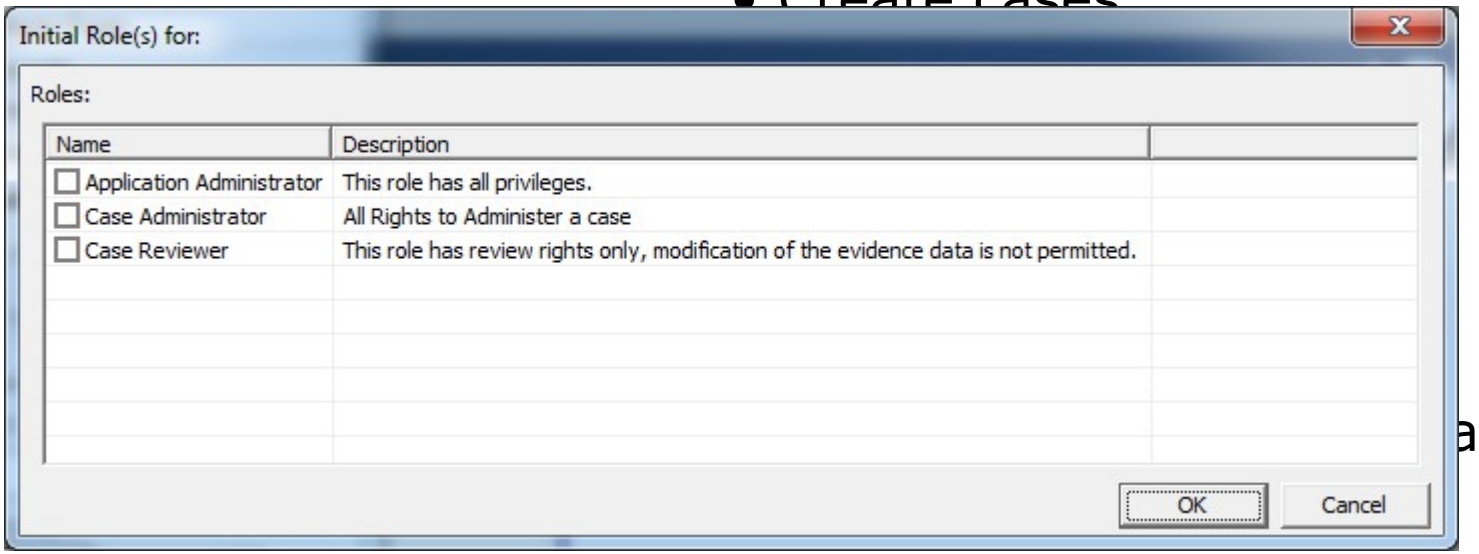


Application Administrator

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

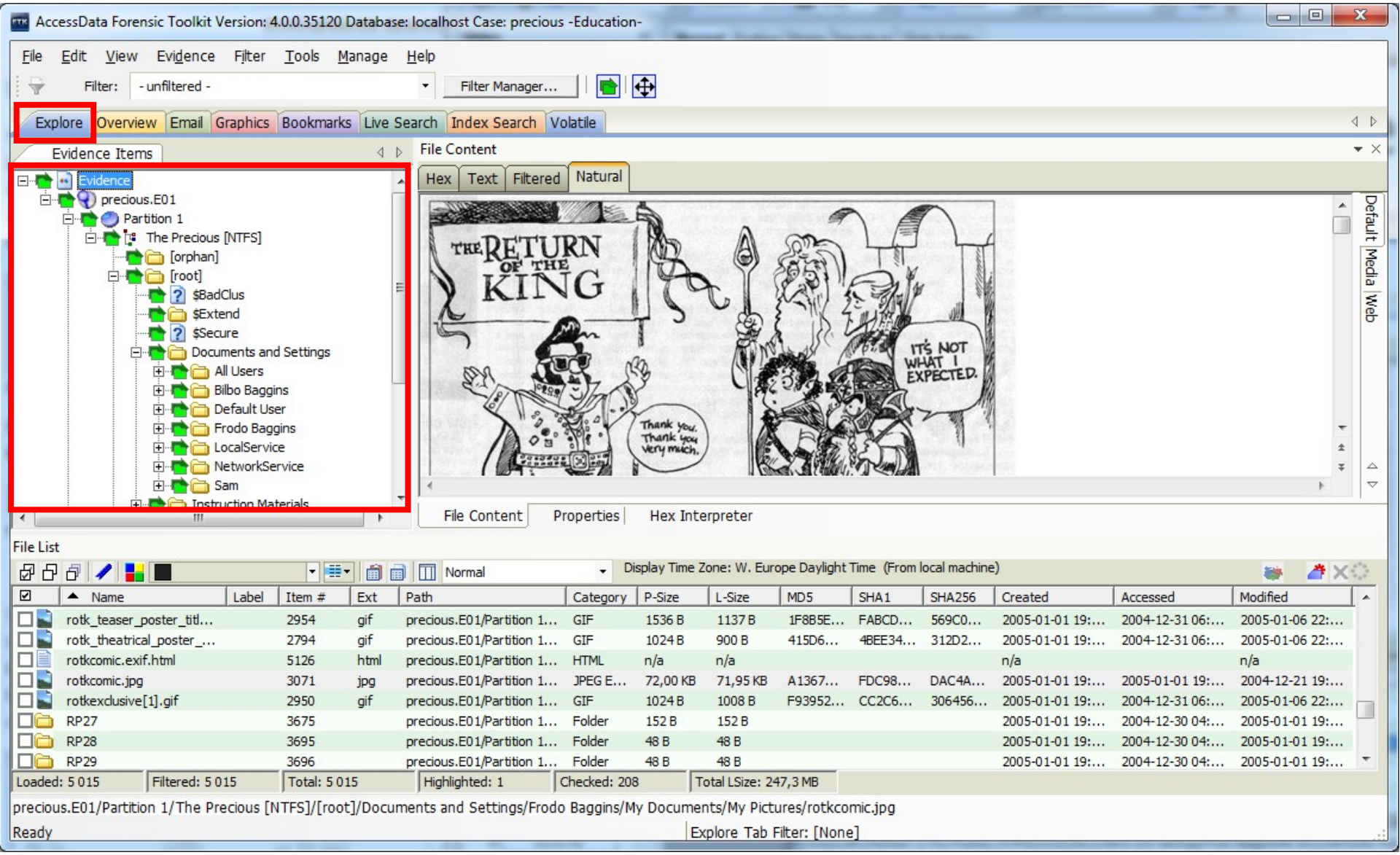
Case Administrator

- Create cases

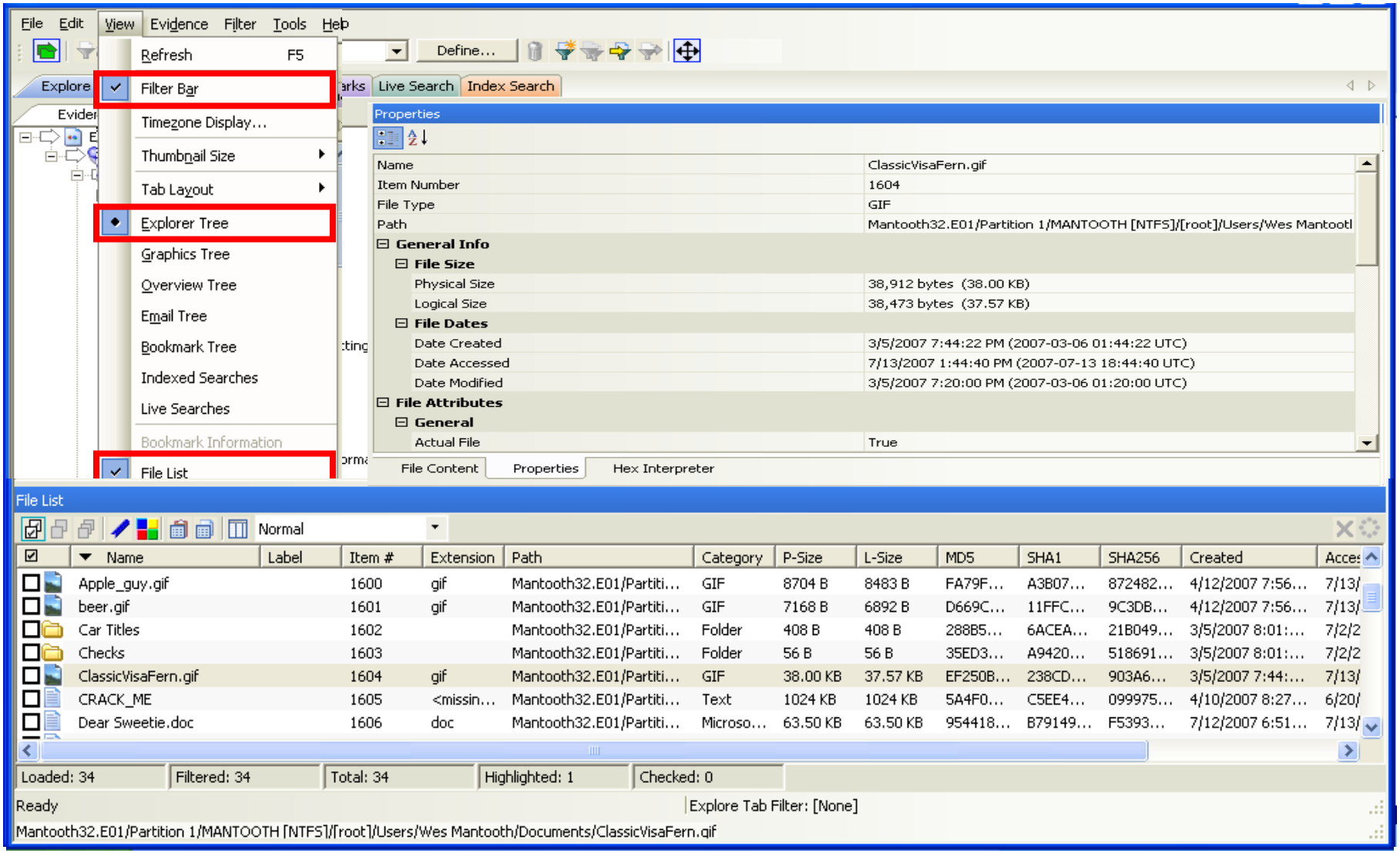


ases

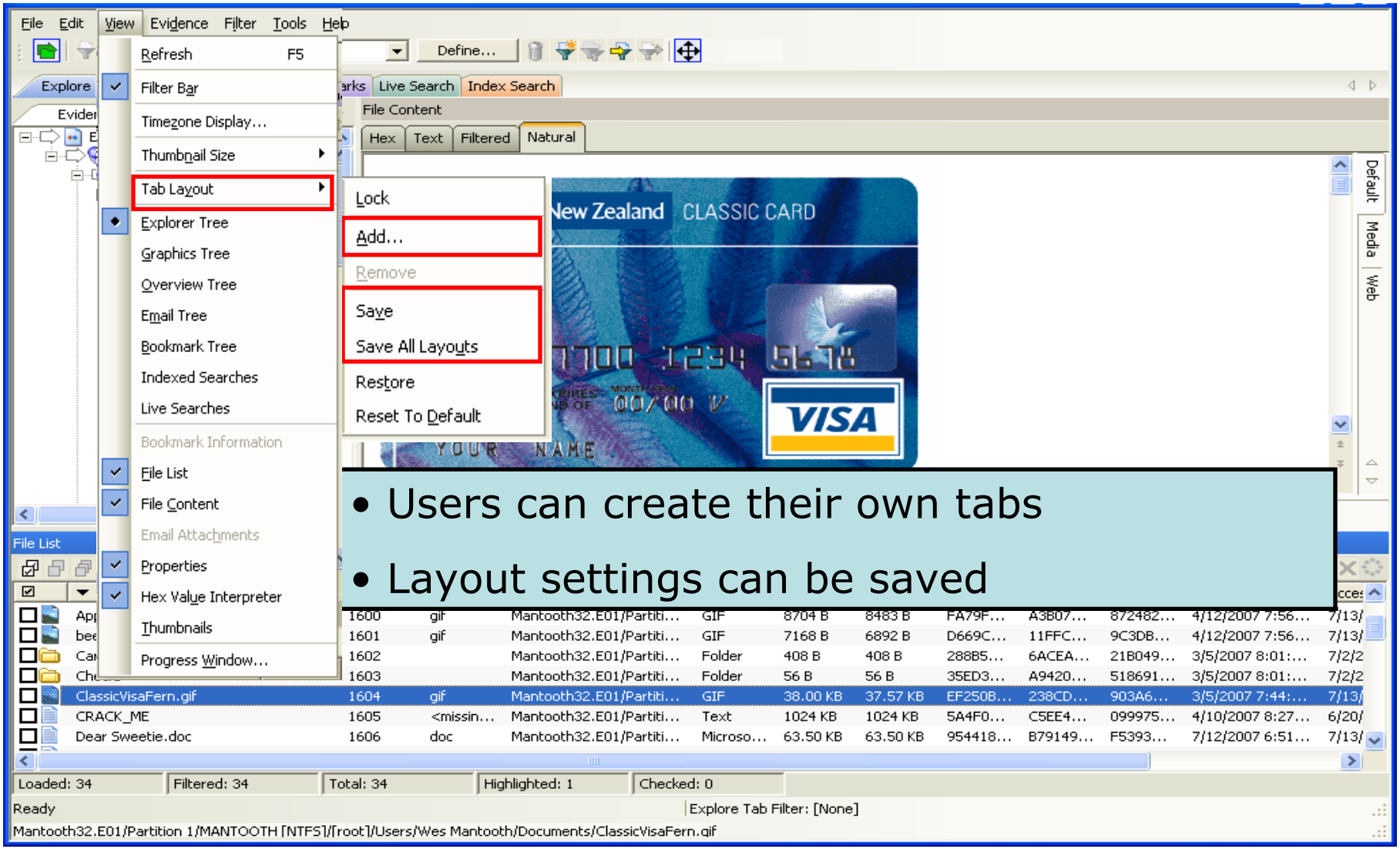
Case Examiner Interface



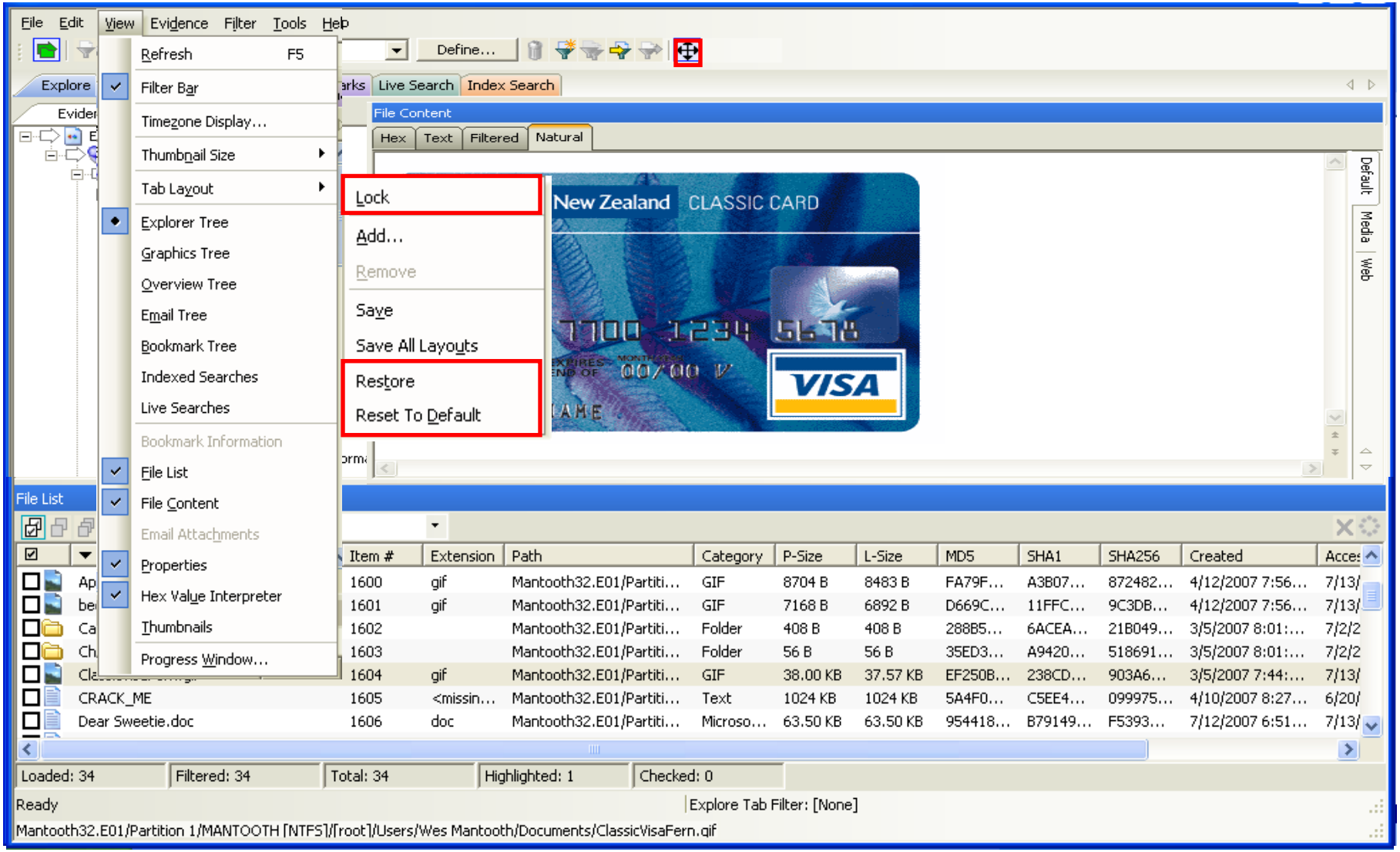
Tabs and Panes



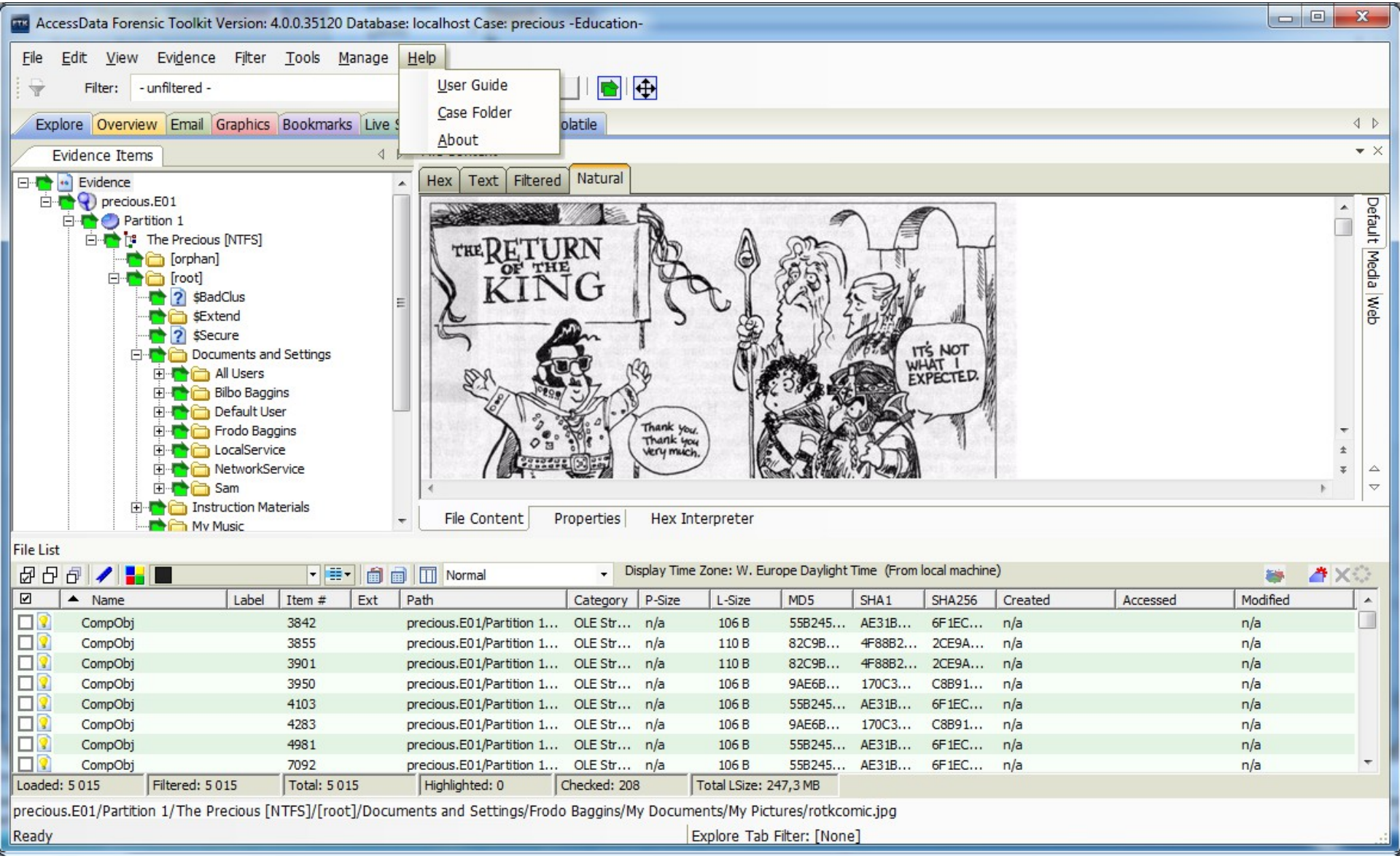
Tabs and Panes



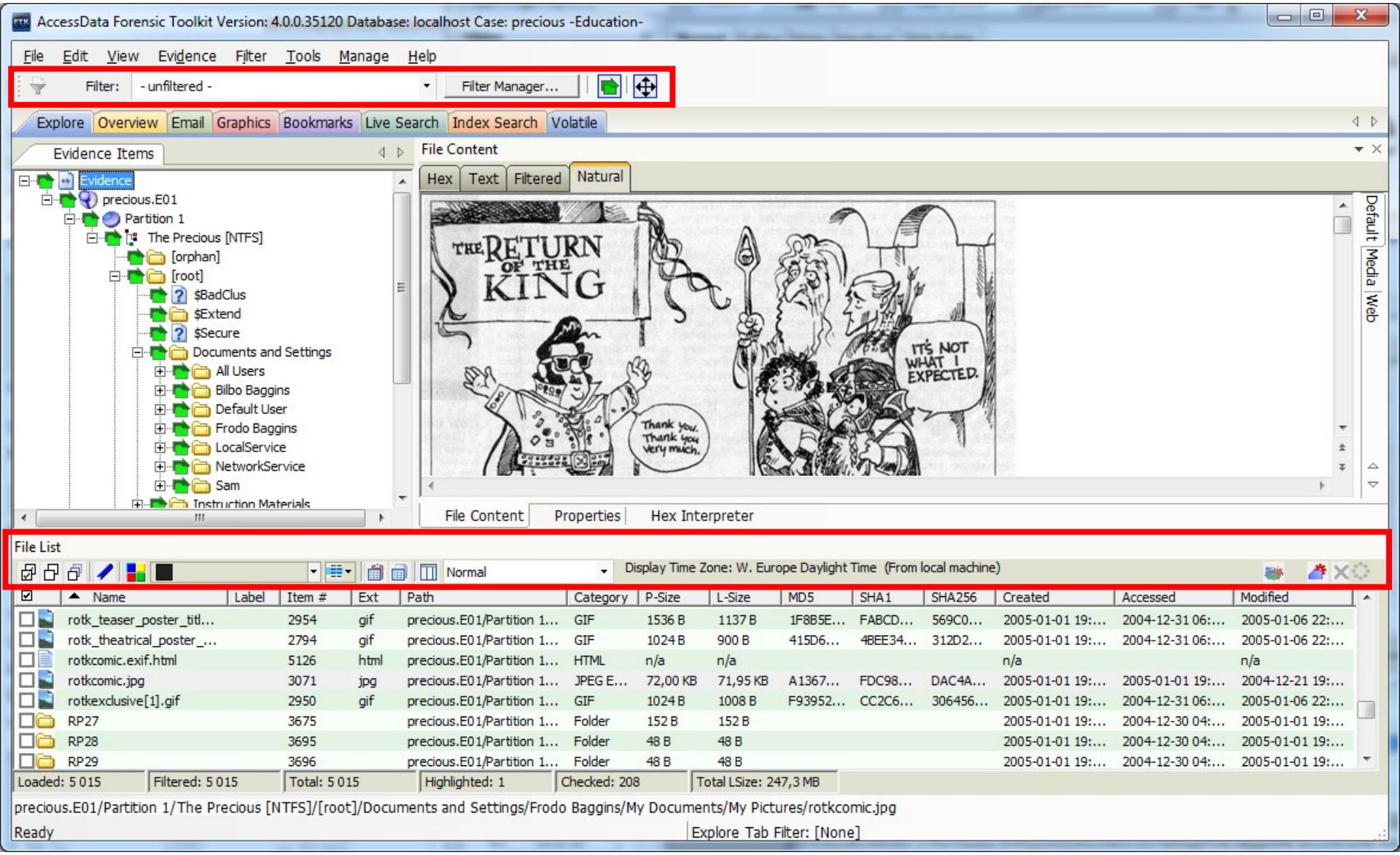
Tabs and Panes



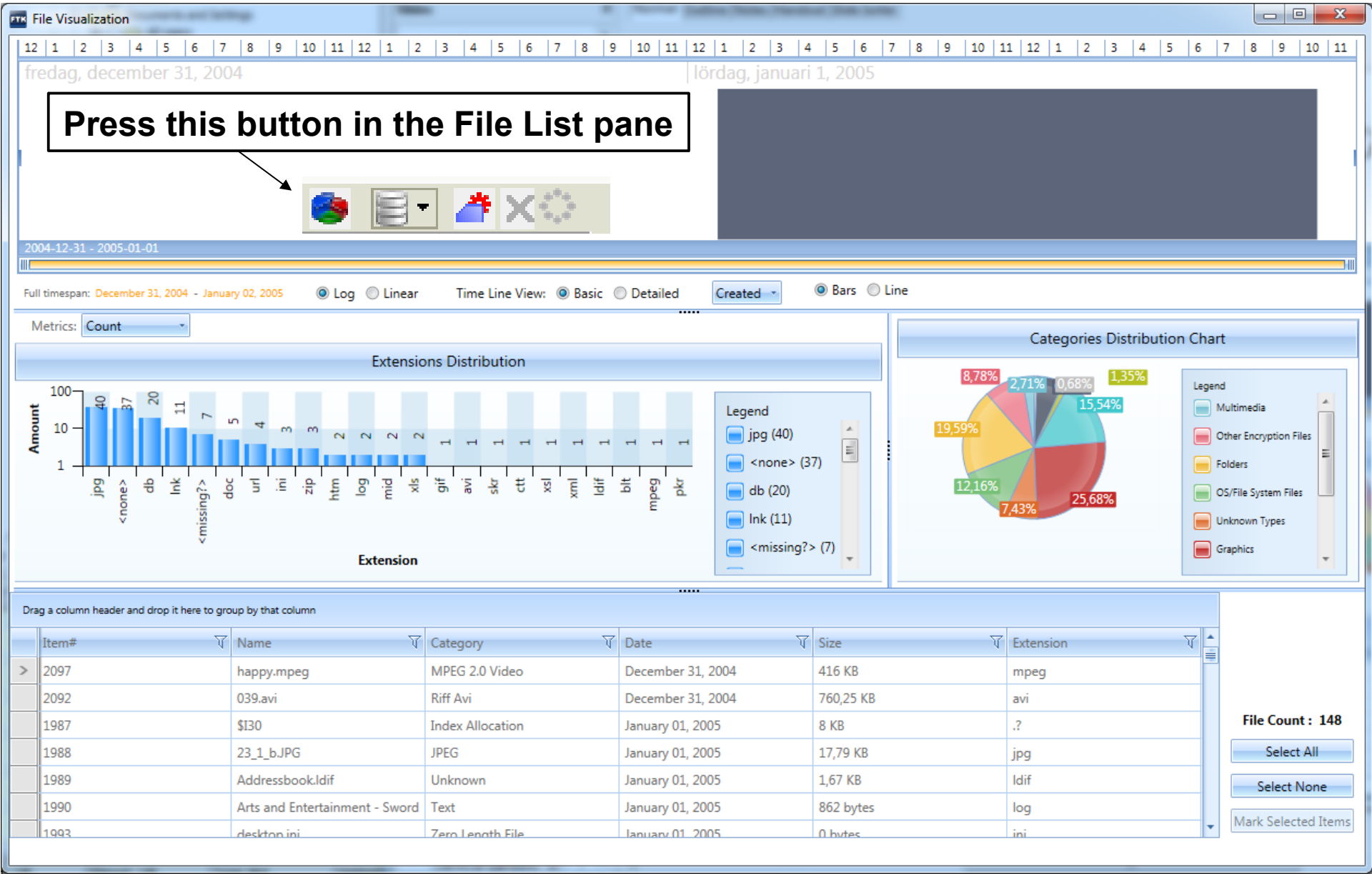
Case Examiner Interface



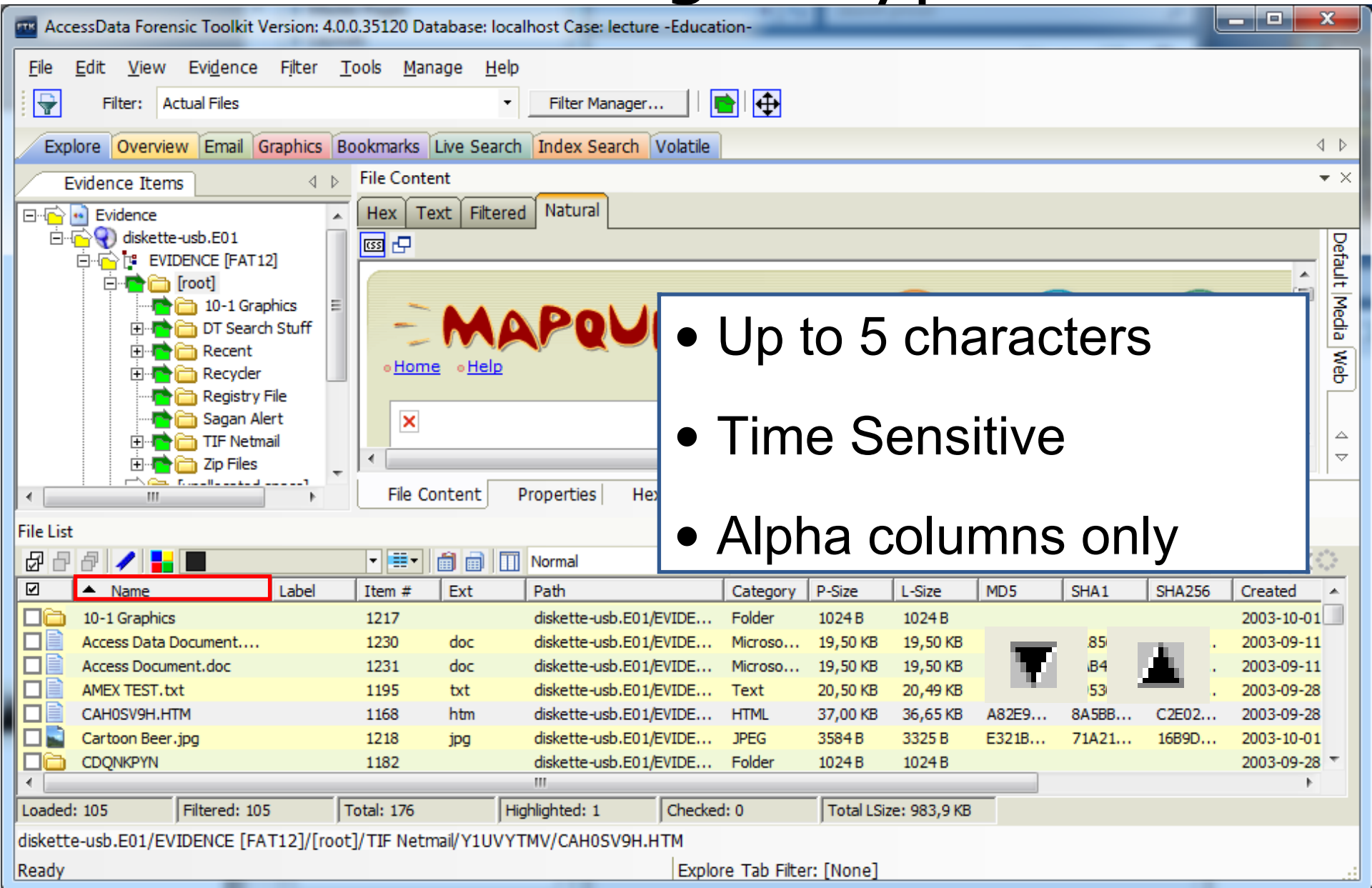
Toolbars


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
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
File Content
Hex Text Filtered Natural
THE RETURN OF THE KING
IT'S NOT WHAT I EXPECTED.
Thank you. Thank you very much.
Default Media Web
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
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:...
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

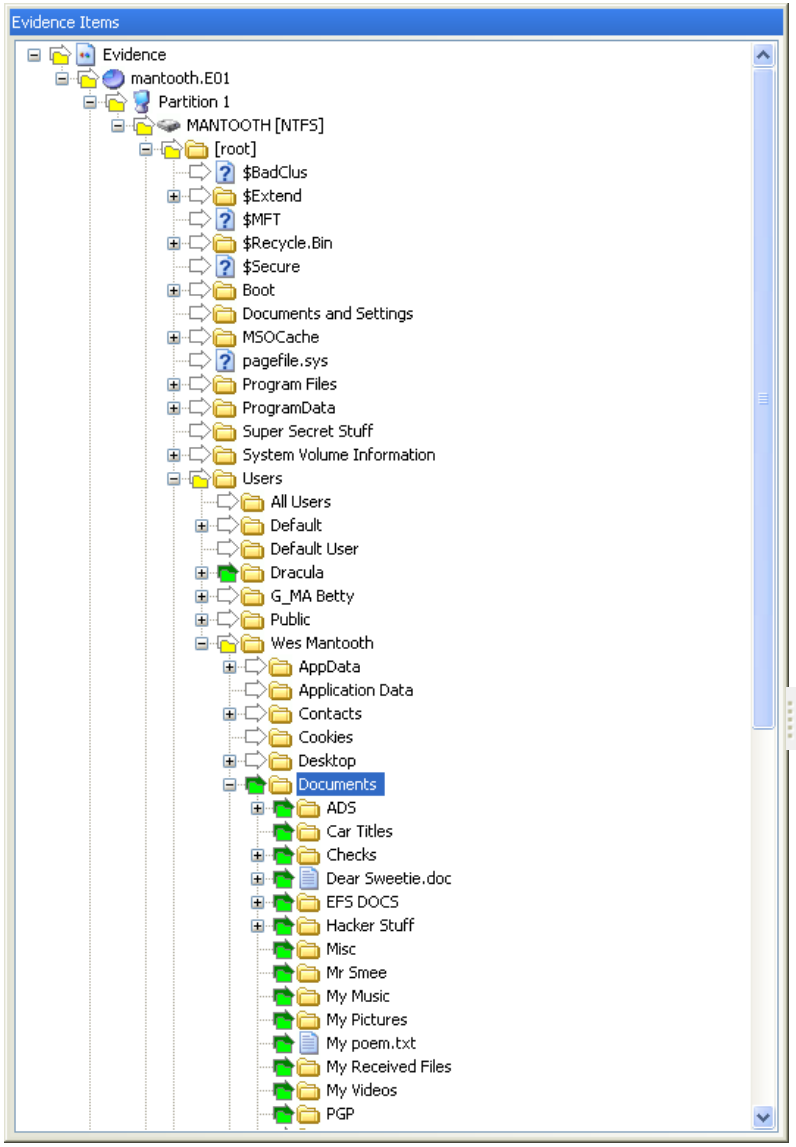


Column Sorting & Type-Down



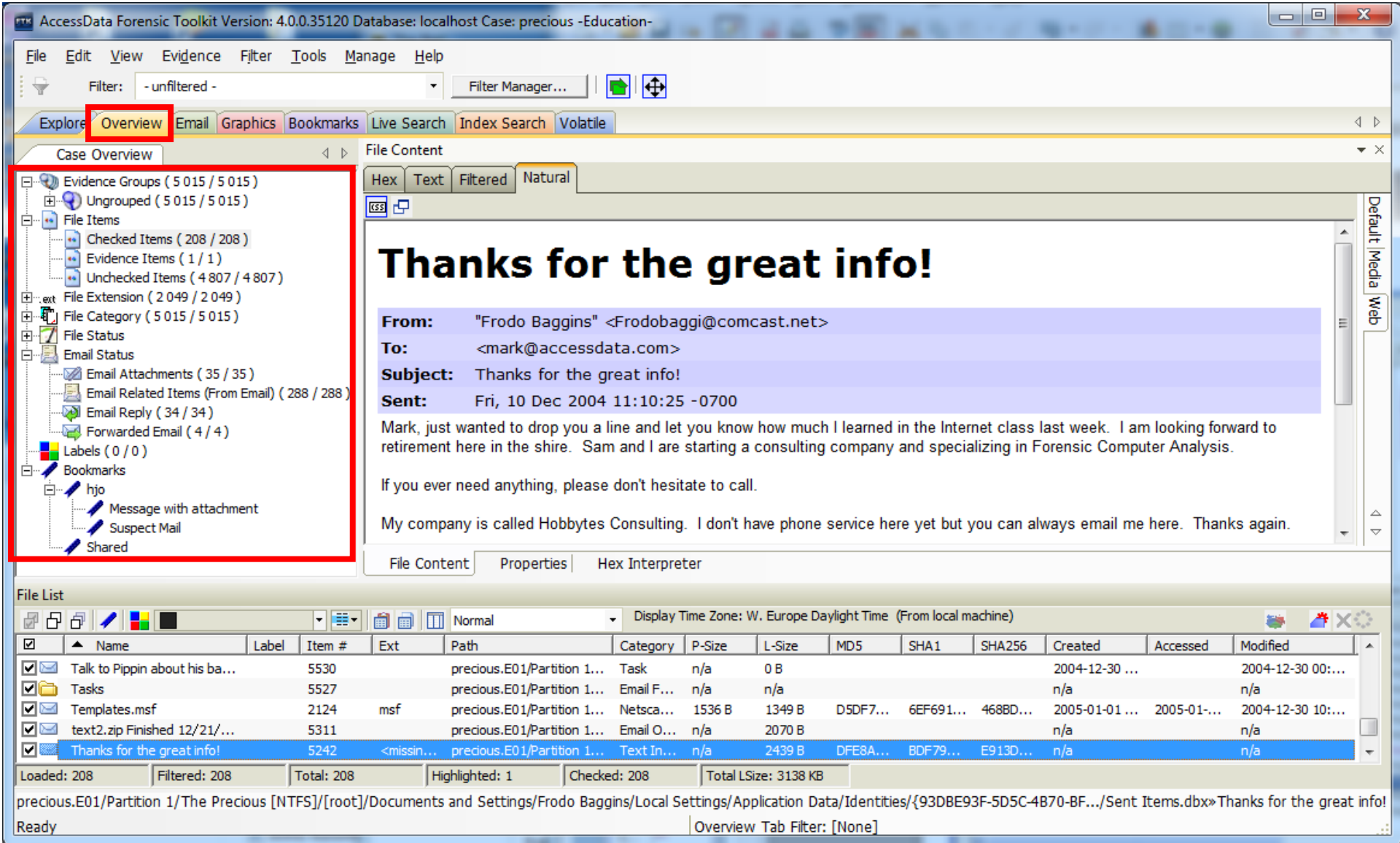
- Up to 5 characters
- Time Sensitive
- Alpha columns only

Quick Picks



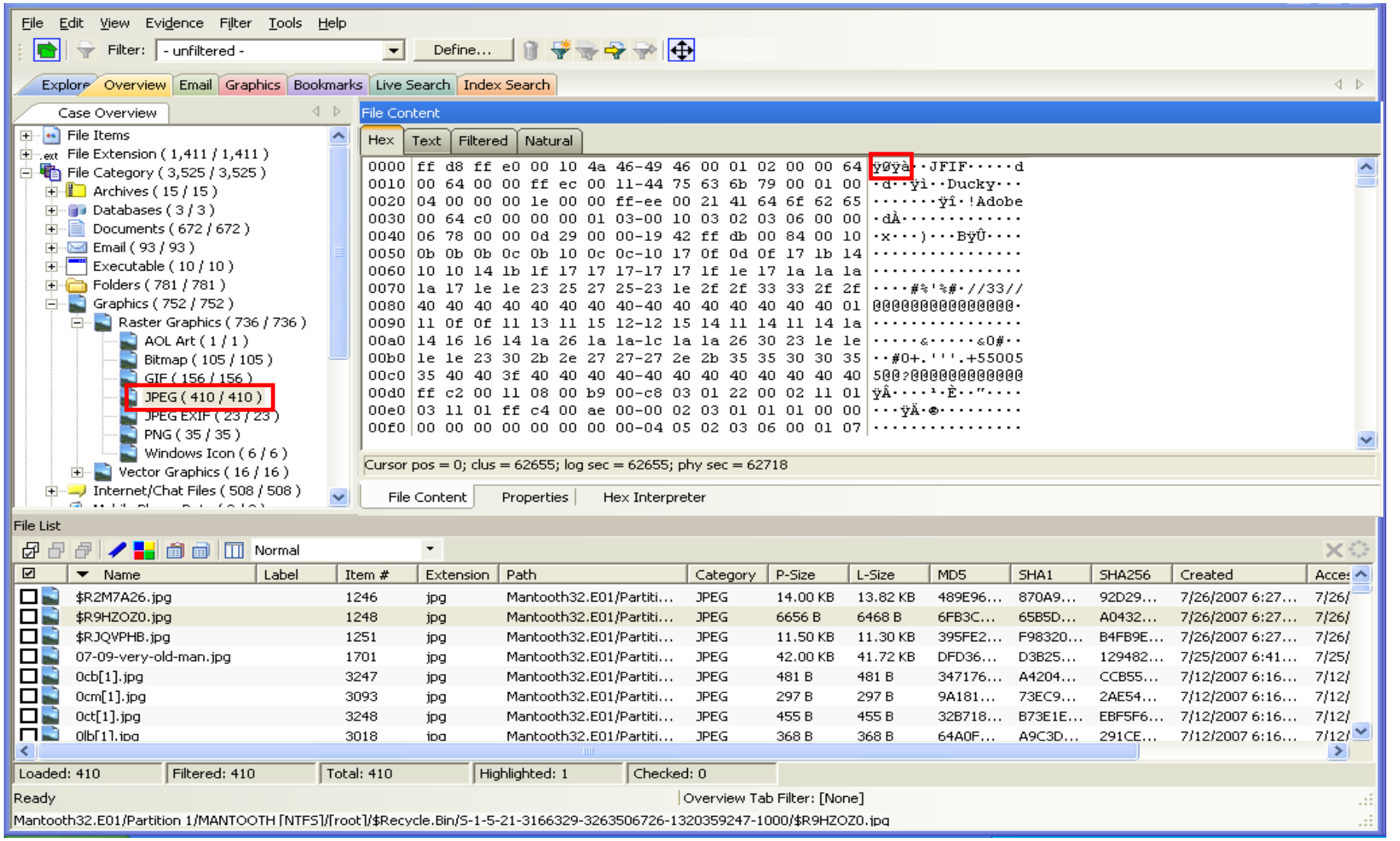
- Allows user selectable focus
- Icons show selected status
- Can be suspended via the Quickpicks suspend button located on the toolbar

Overview Tab

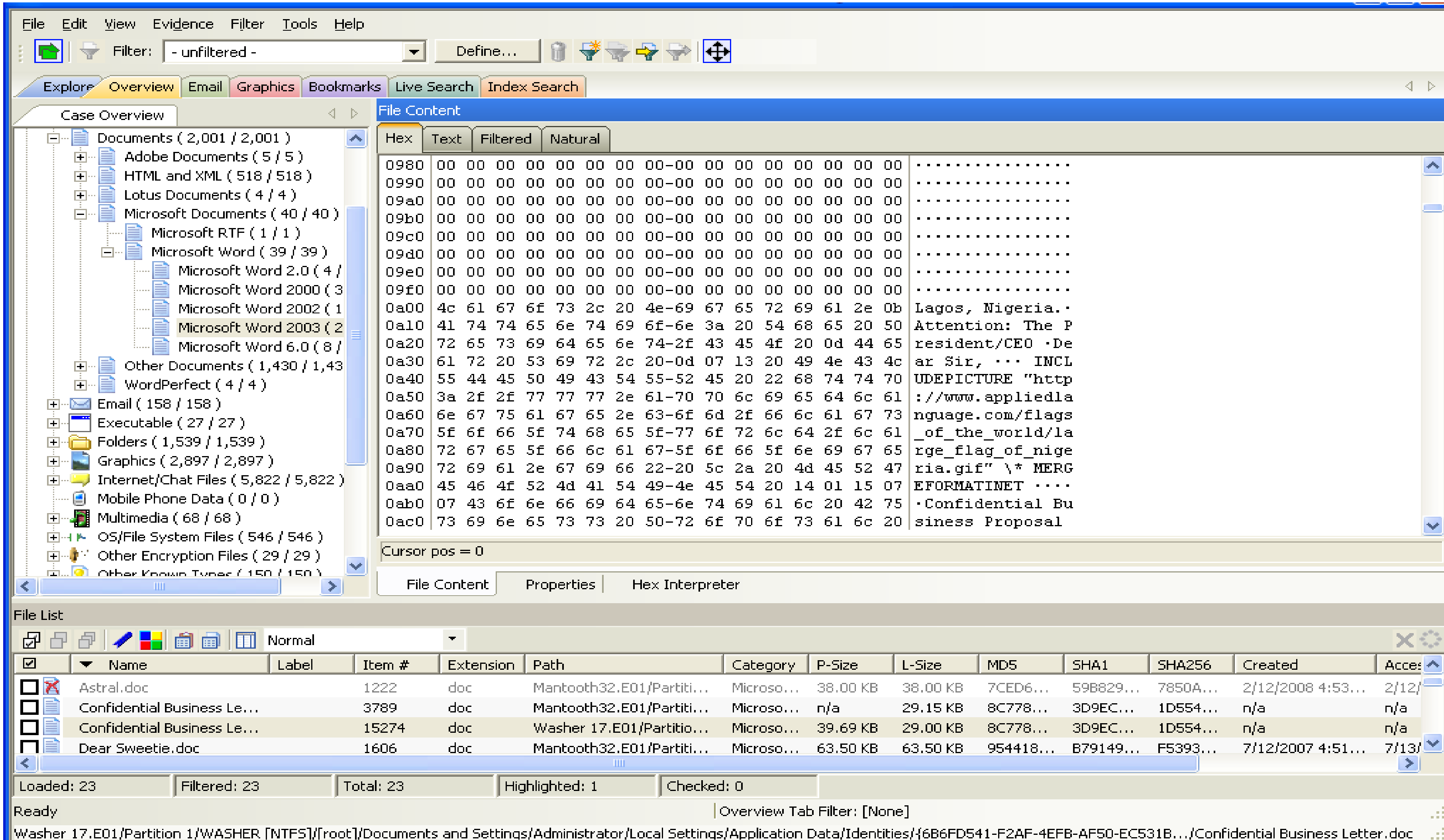


Overview Tab

Files are identified by header, not by extension

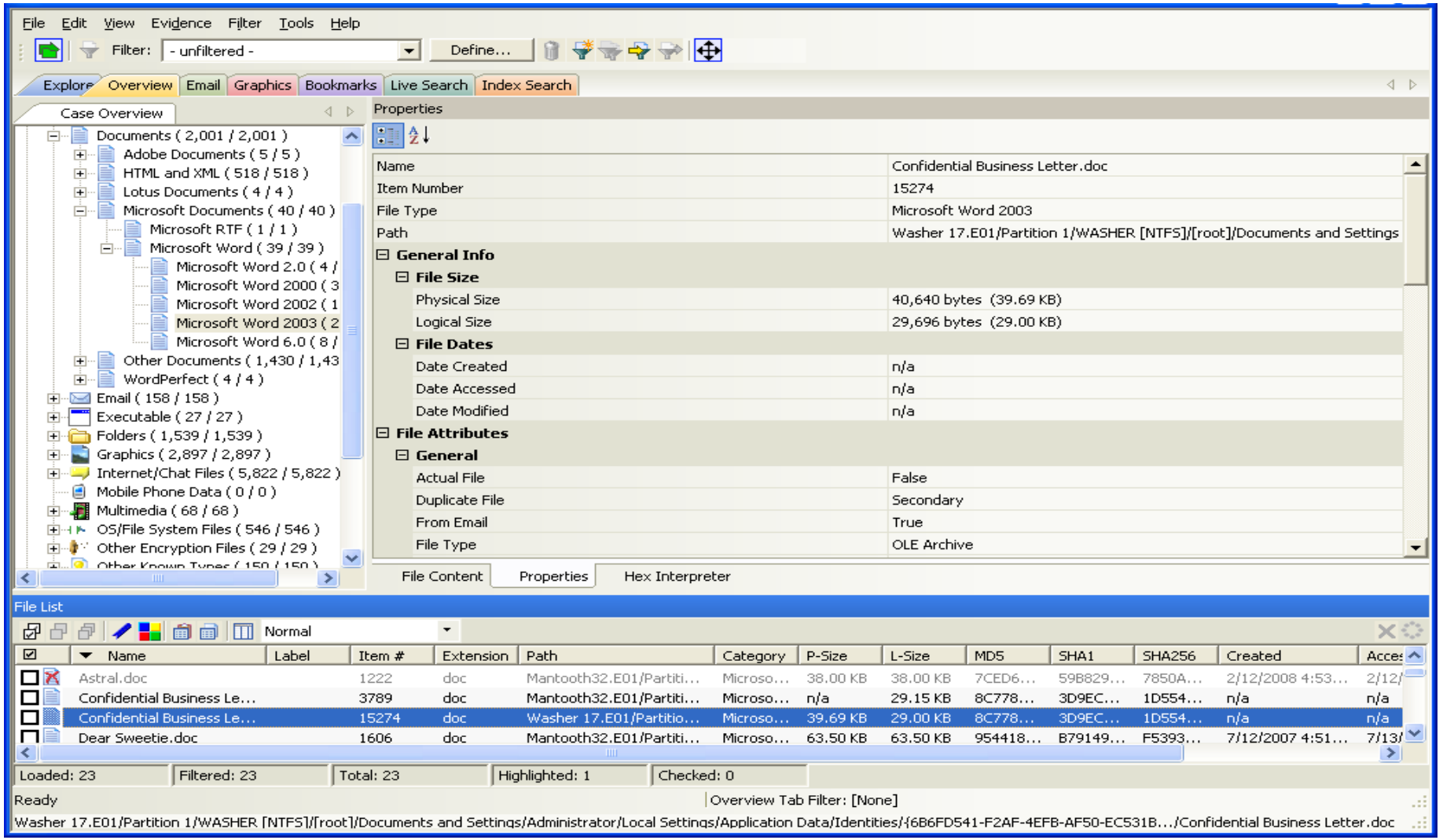


Viewing Options

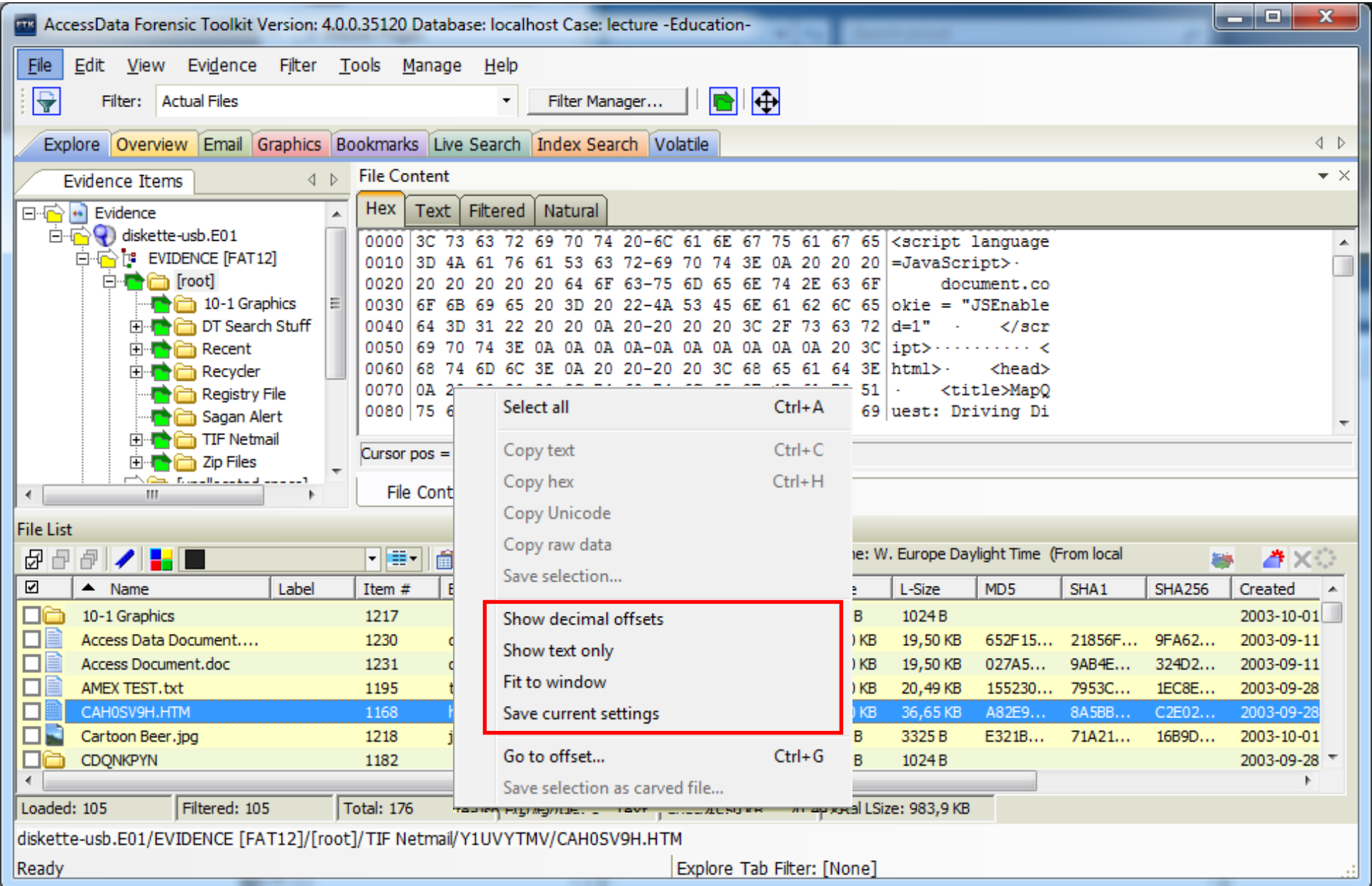


Natural View / Text View / Filtered View

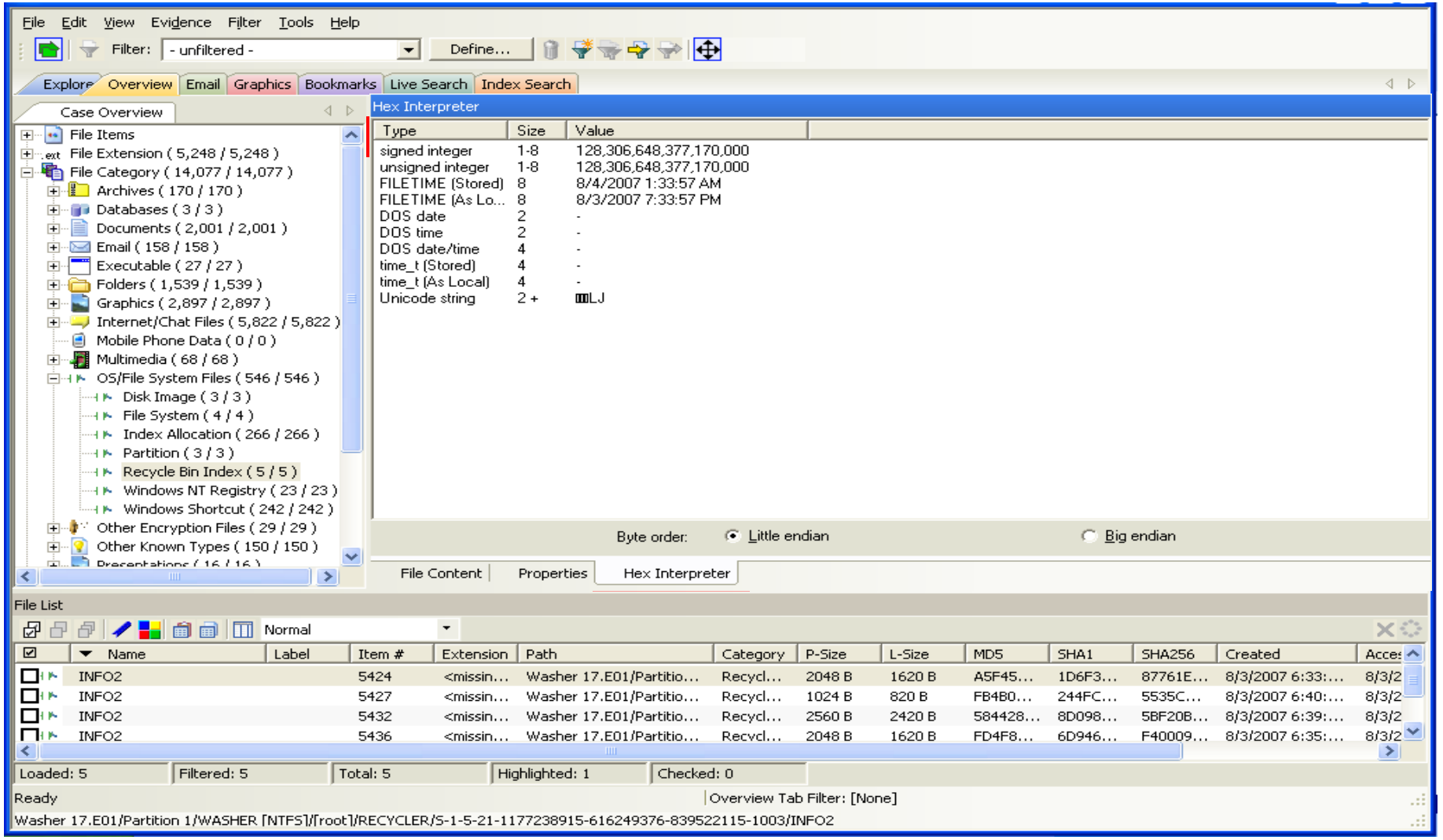
Viewing File/Folder Properties



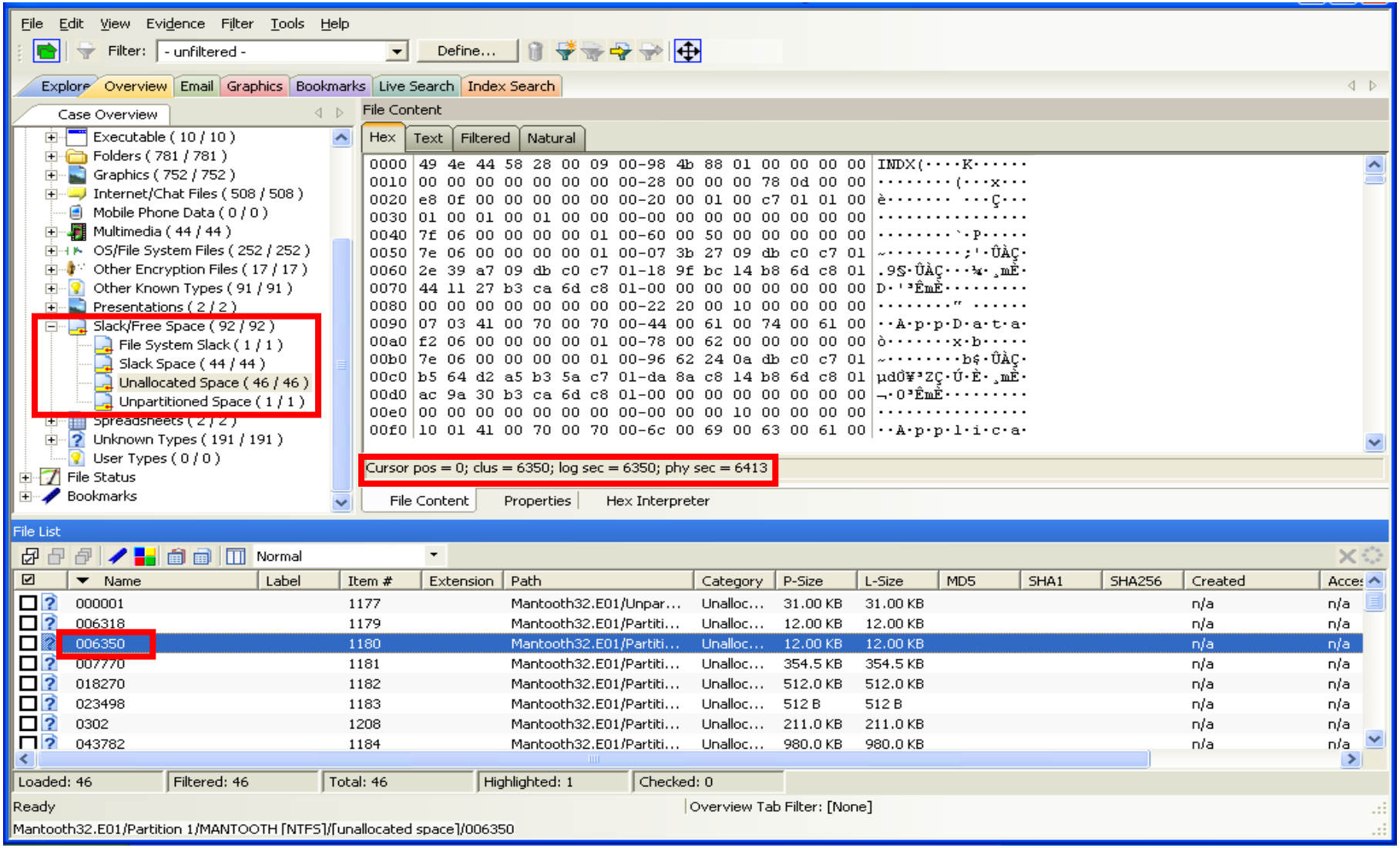
Hex View Settings



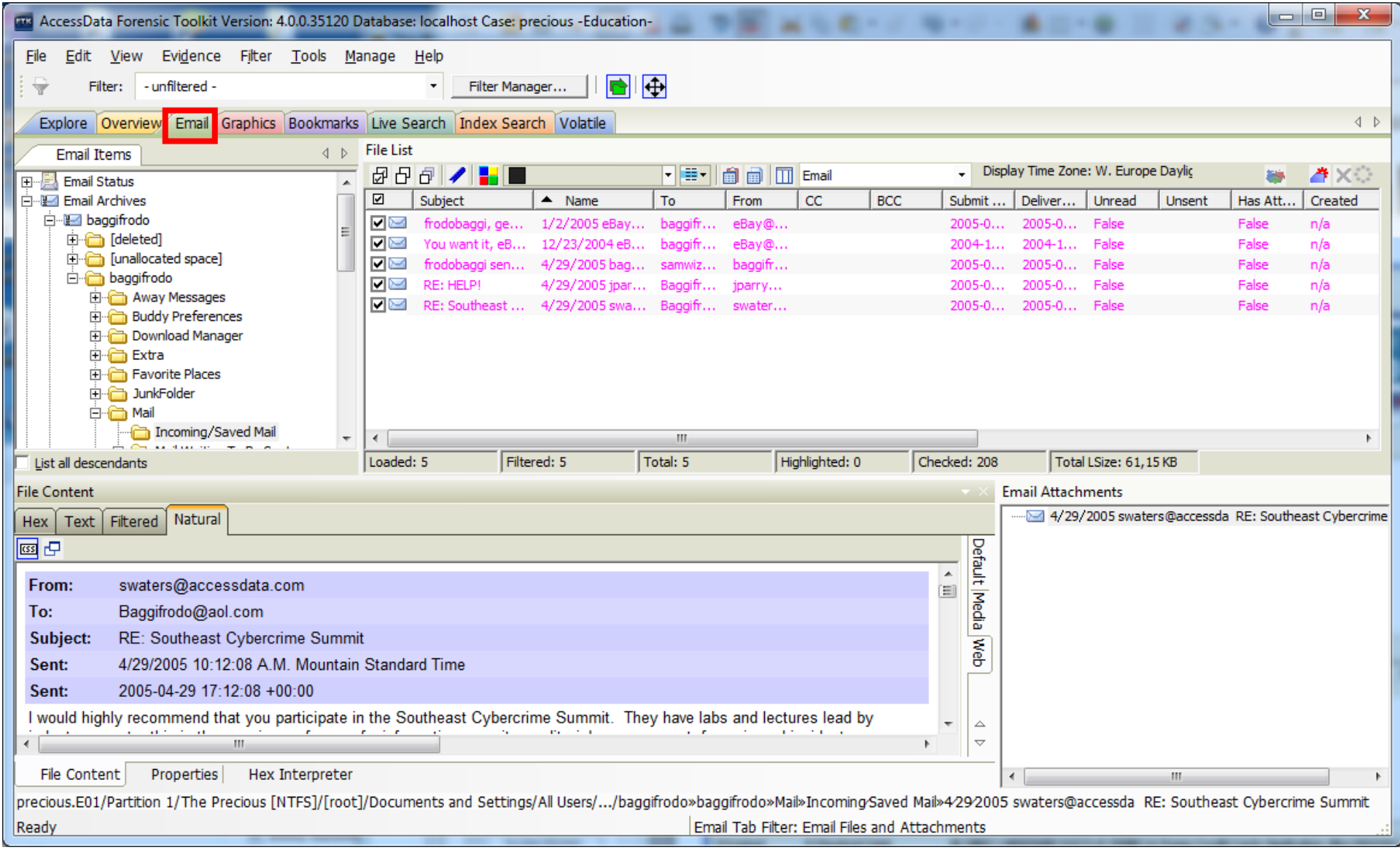
Hex Interpreter



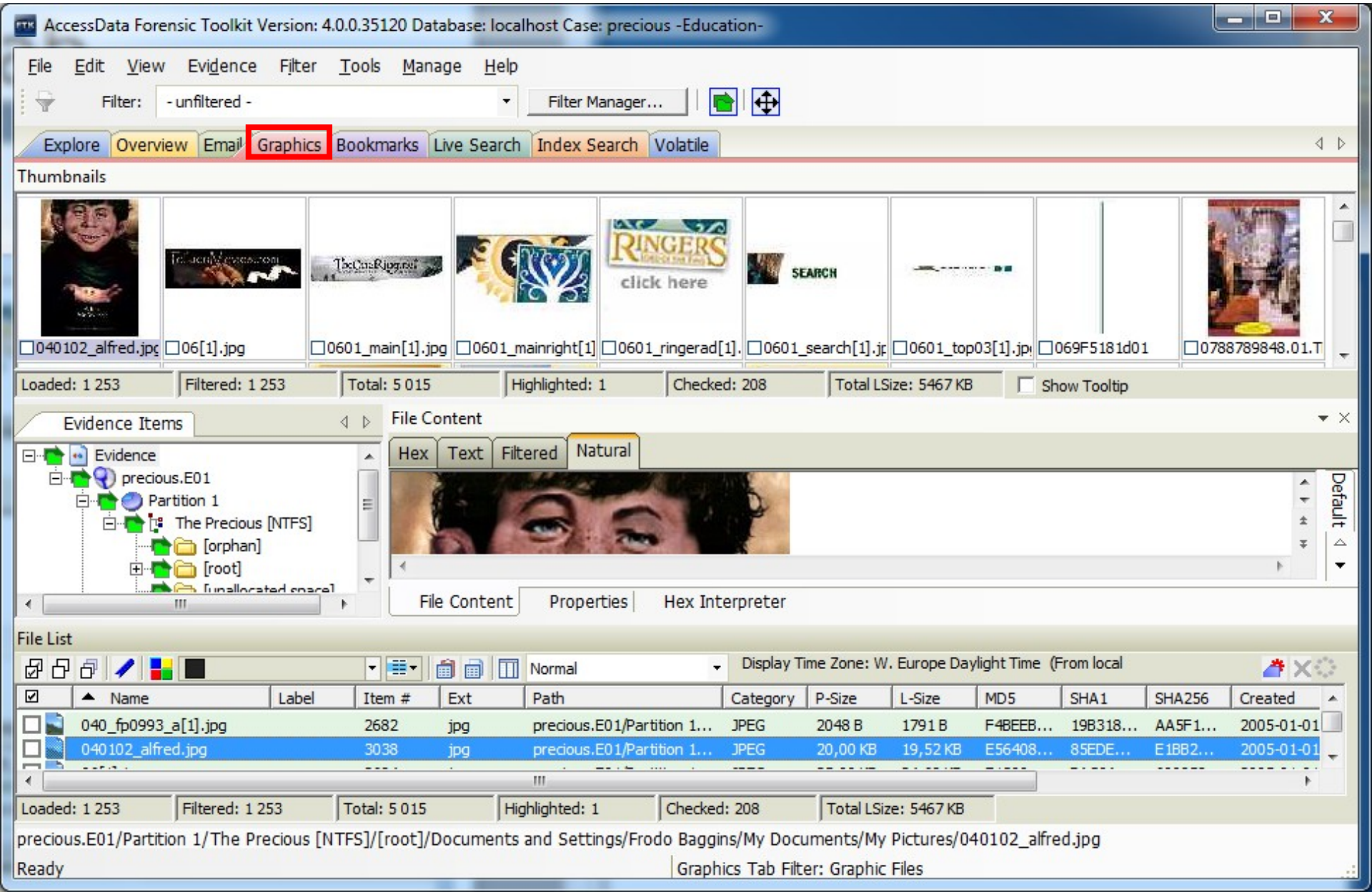
Drive Free Space



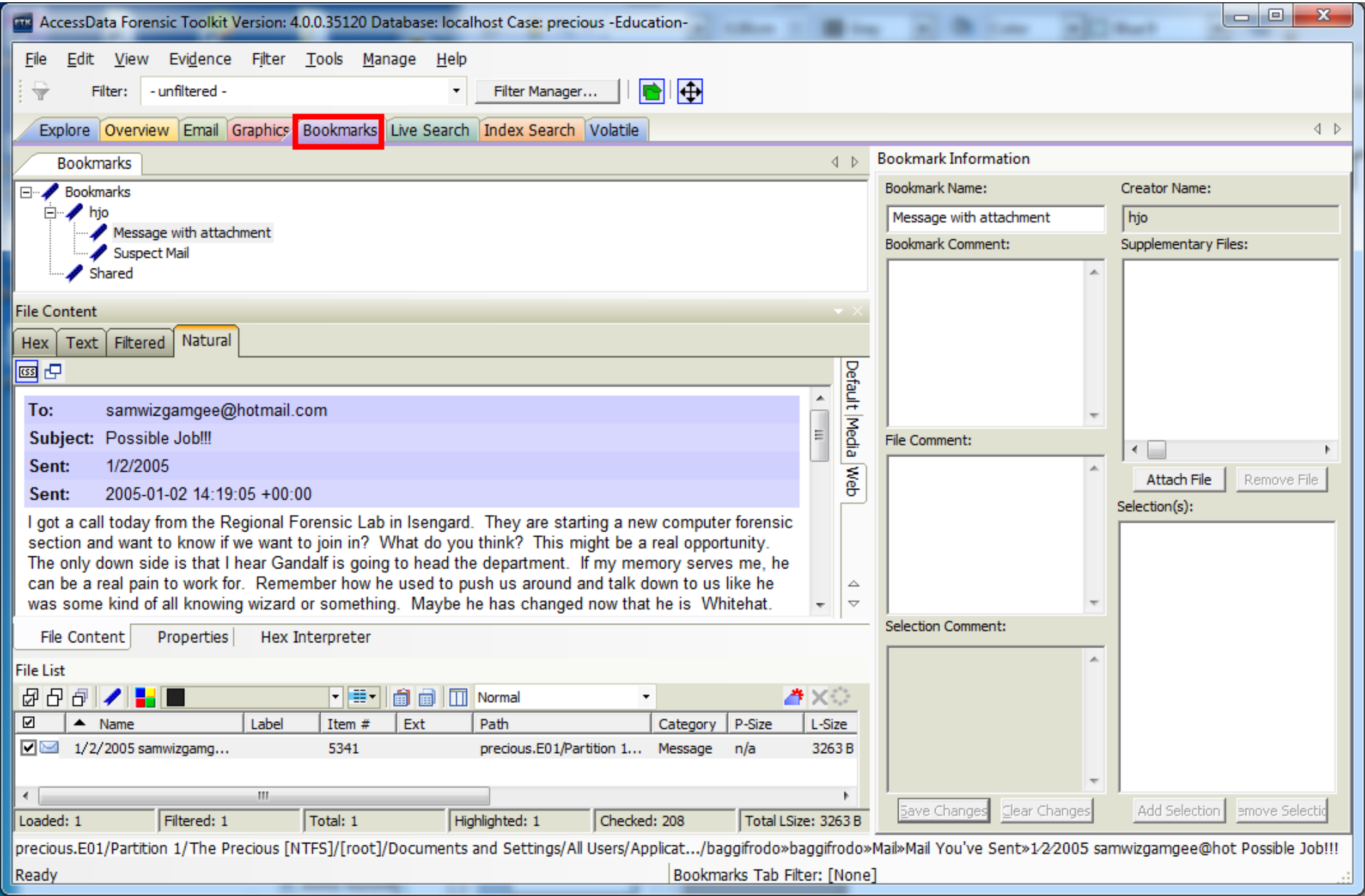
Email Tab


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
Email
Display Time Zone: W. Europe Daylig
Subject Name To From CC BCC Submit ... Deliver... Unread Unsent Has Att... Created
frodobaggi, ge... 1/2/2005 eBay... baggifr... eBay@... 2005-0... 2005-0... False False n/a
You want it, eB... 12/23/2004 eB... baggifr... eBay@... 2004-1... 2004-1... False False n/a
frodobaggi sen... 4/29/2005 bag... samwiz... baggifr... 2005-0... 2005-0... False False n/a
RE: HELP! 4/29/2005 jpar... Baggifr... jparry... 2005-0... 2005-0... False False n/a
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
Default Media Web
Email Attachments
4/29/2005 swaters@accessda RE: Southeast Cybercrime
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

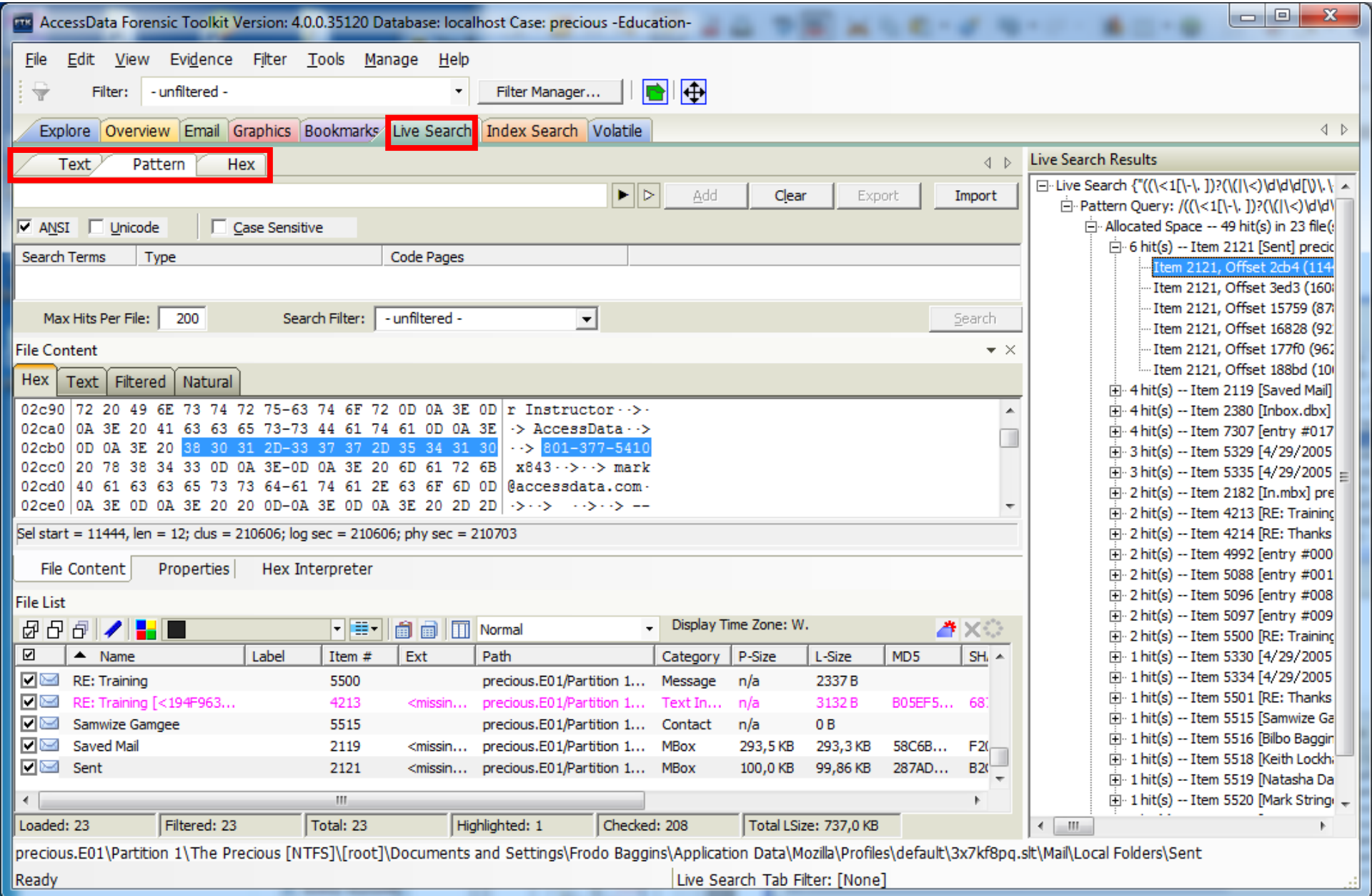
Graphics Tab



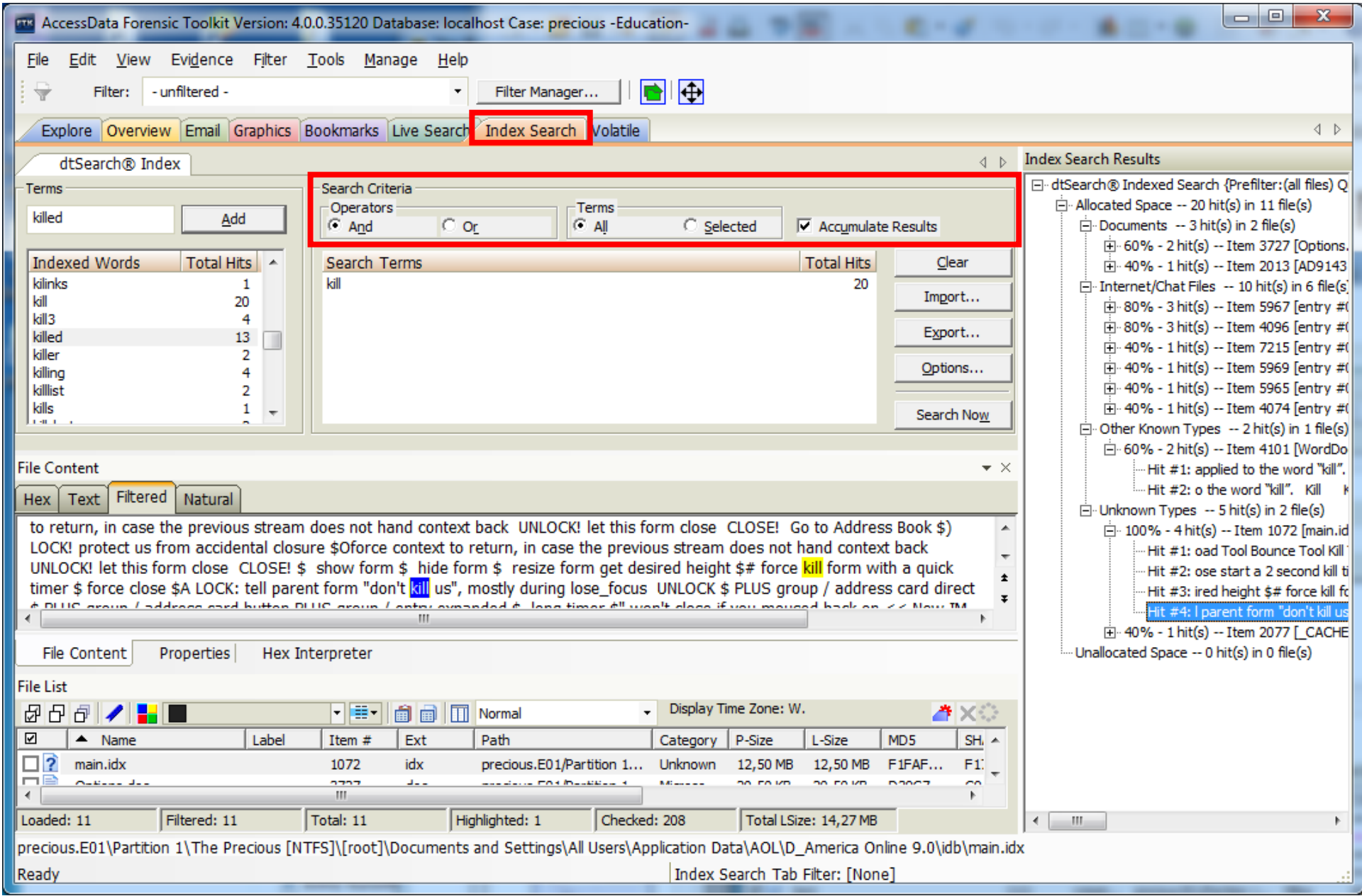
Bookmarks Tab



Live Search Tab



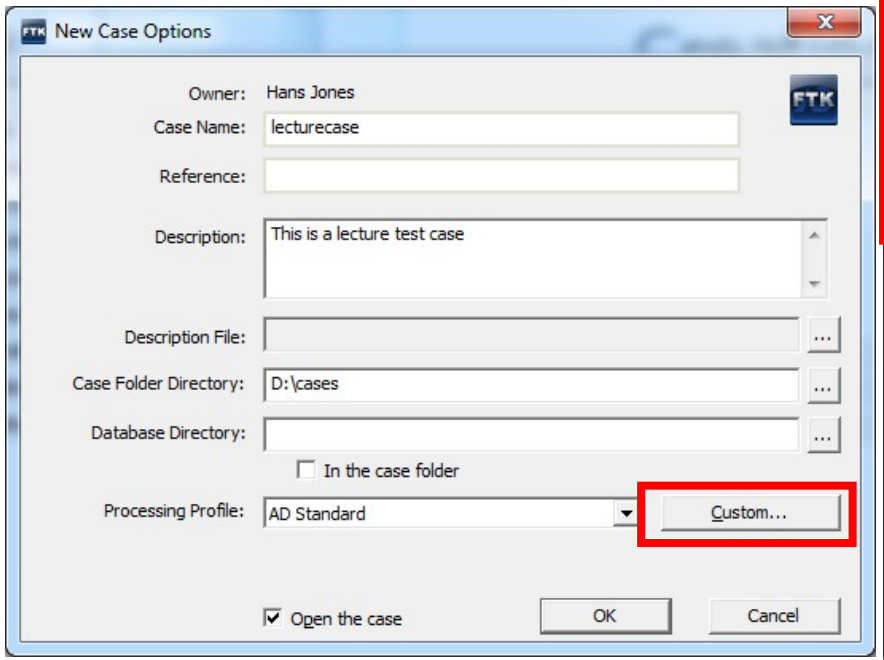
Index Search Tab

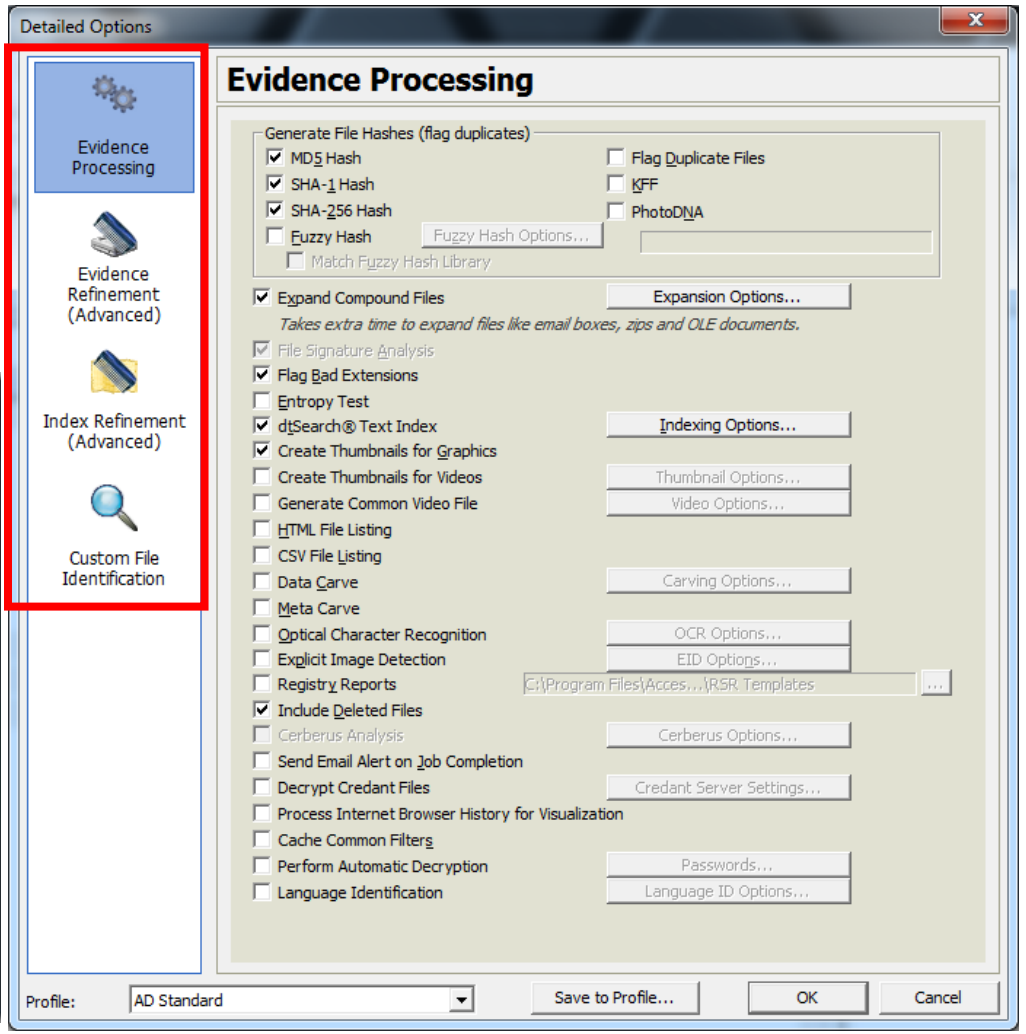


Creating a New Case and Processing Options

- From the Case Manager Interface menu > Case > New

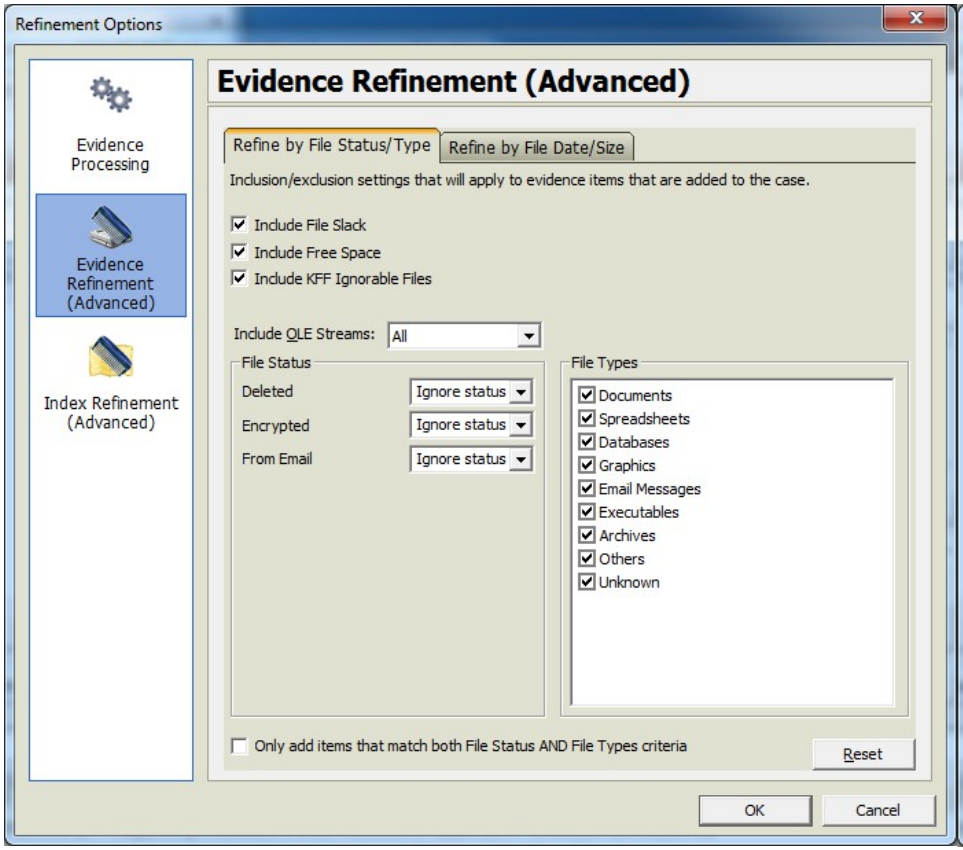
Selections are pre-checked based on case setup.
Can be changed per evidence item later.
Selections can be saved as defaults for future cases.

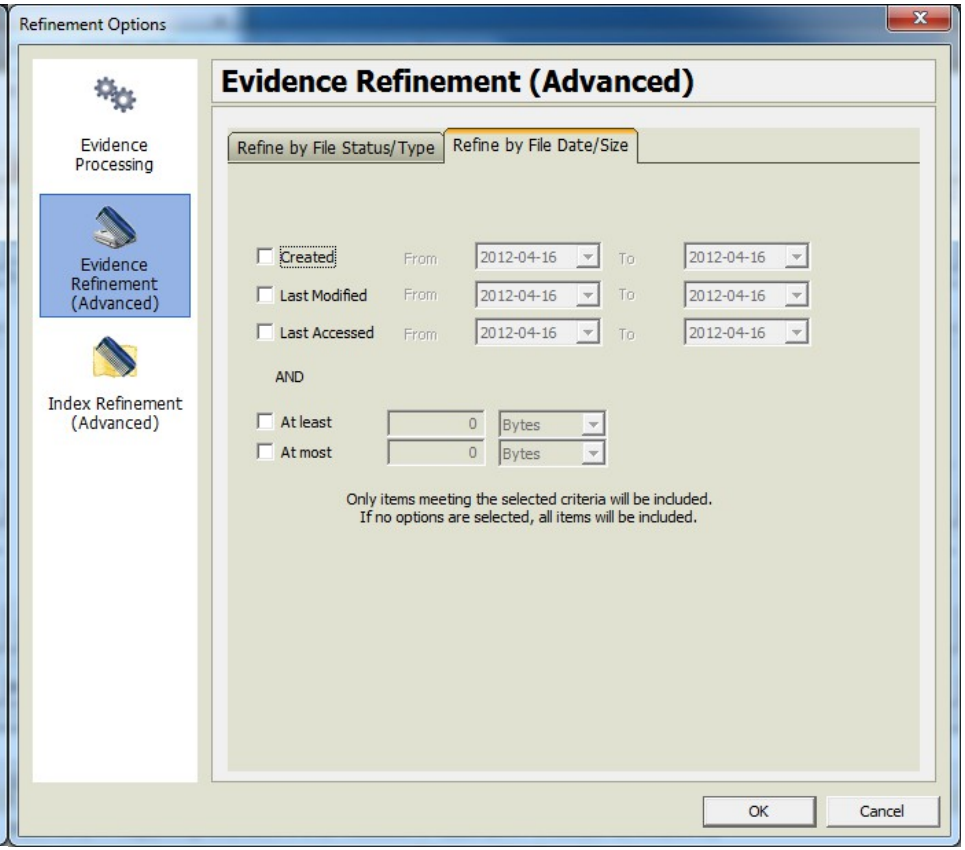




Refining Case Evidence

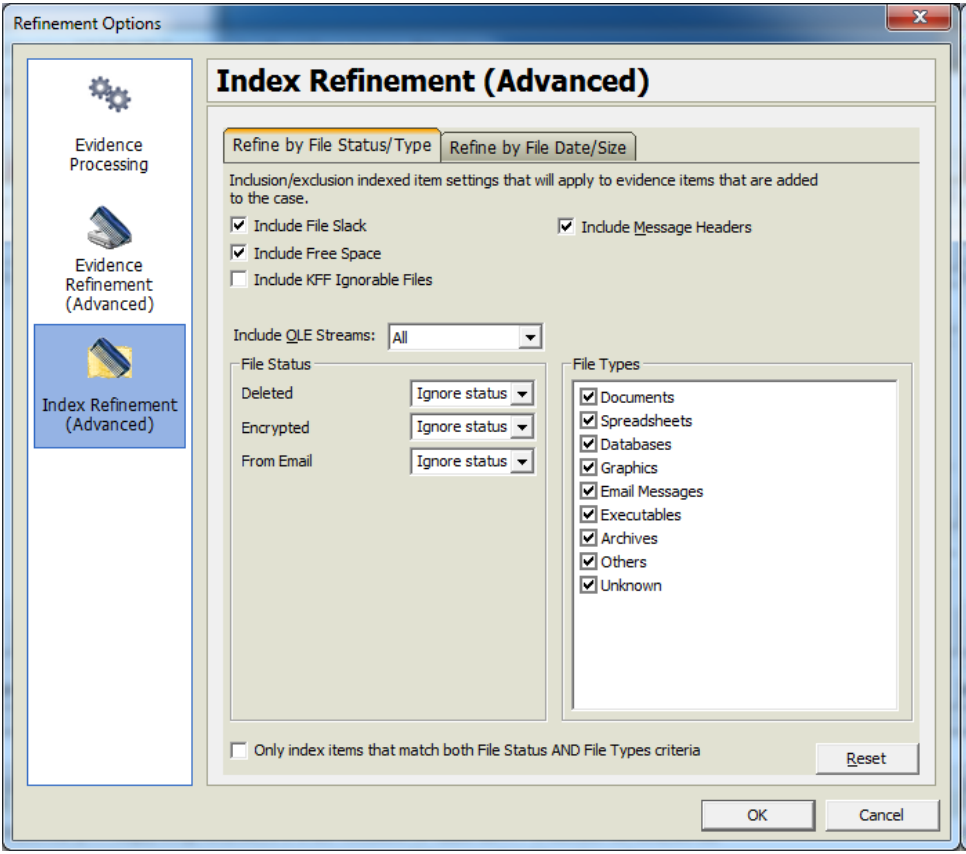
- Usually not needed to modify these parameters
- Refine by: Type, Status, Date/Size

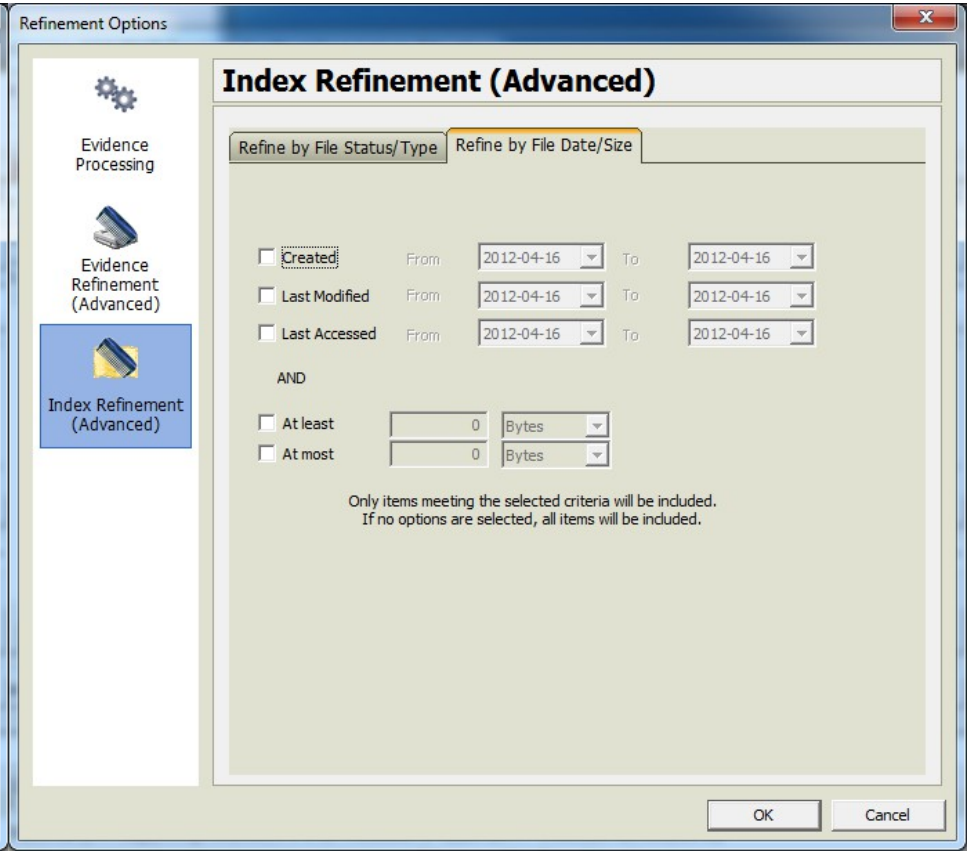




Defining Index Parameters

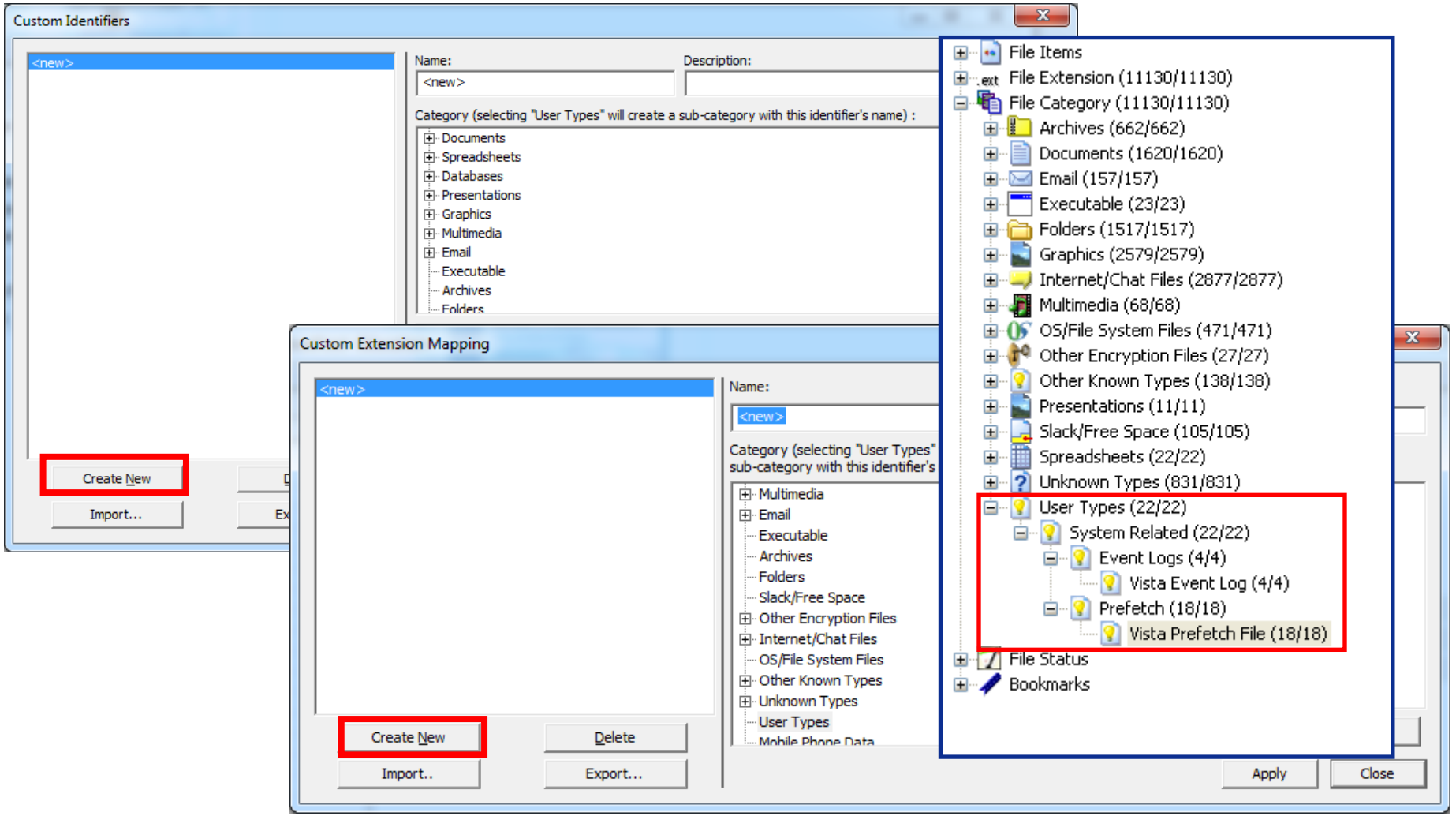
- Usually not needed to modify these parameters
- Refine by: Type, Status, Date/Size





Custom File Identification

- Allows user-defined file identification for header and suffix



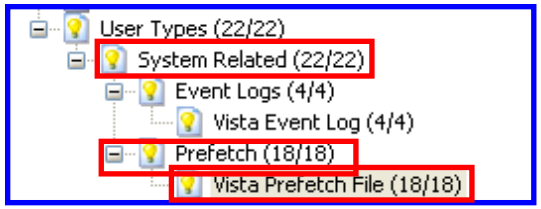
Custom File Identification

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

File Types.txt - Notepad

File Edit Format View Help

```
# 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

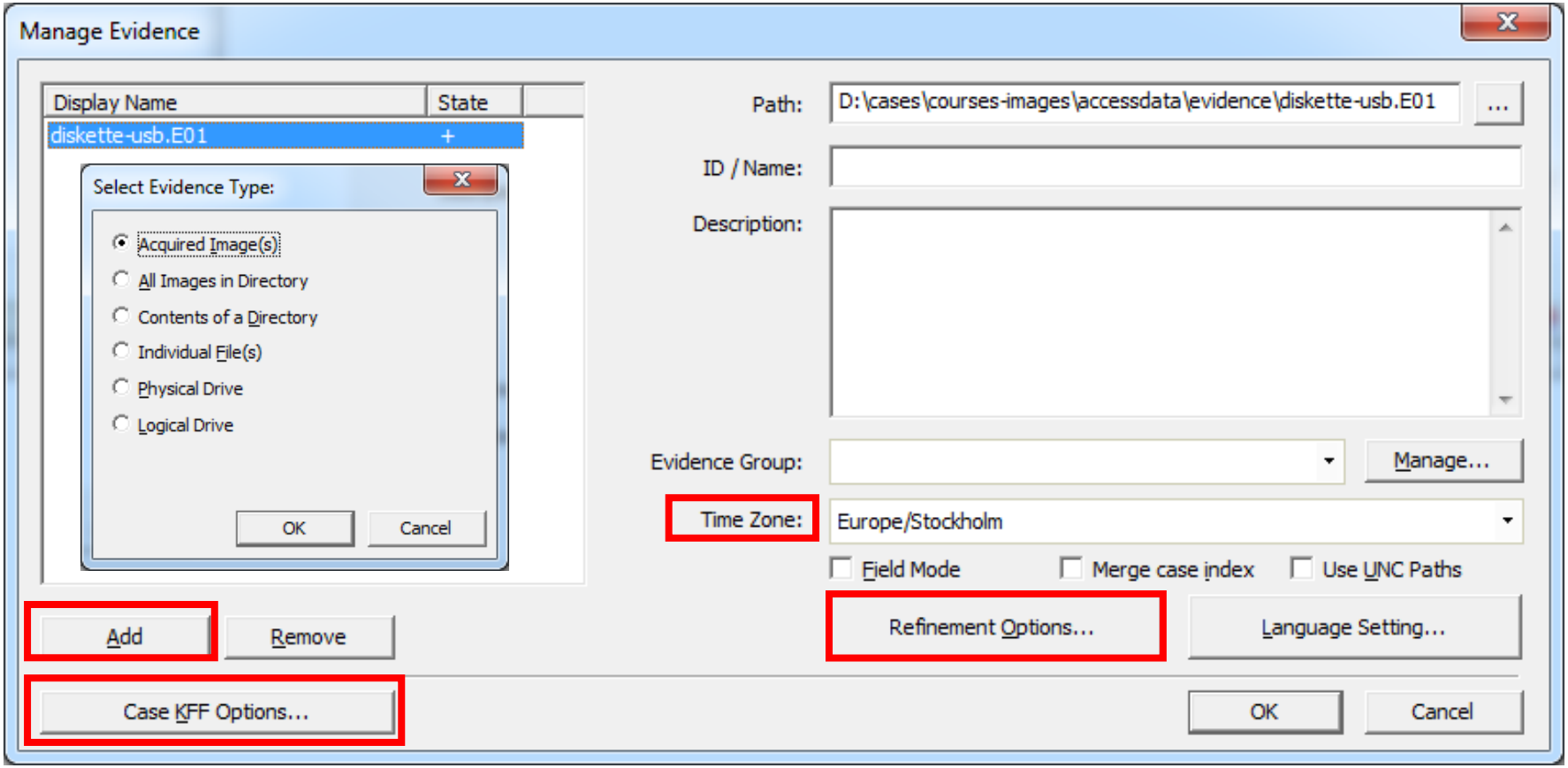
Description = For reference only

Category path relative to "User Types"

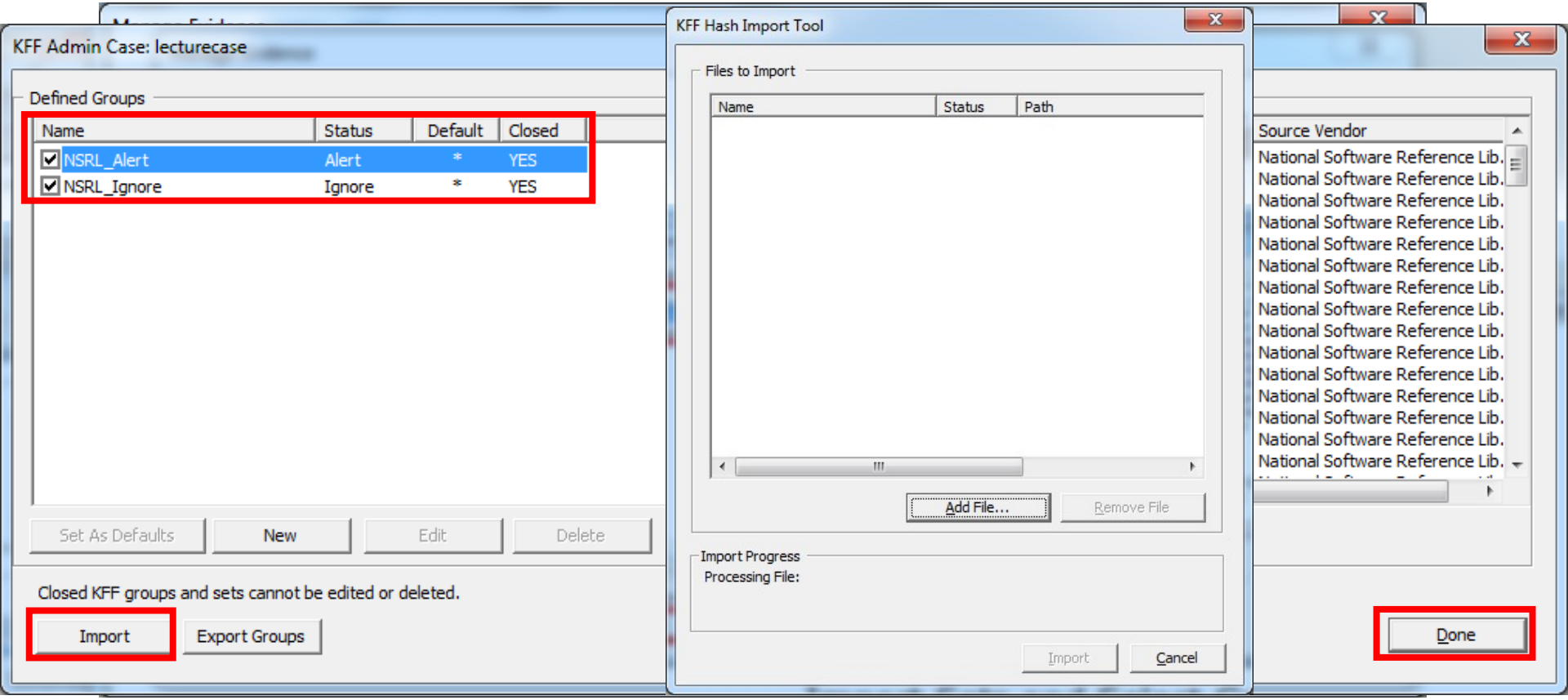
Offset and hex values (AND/OR)

Creating a New Case cont.

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



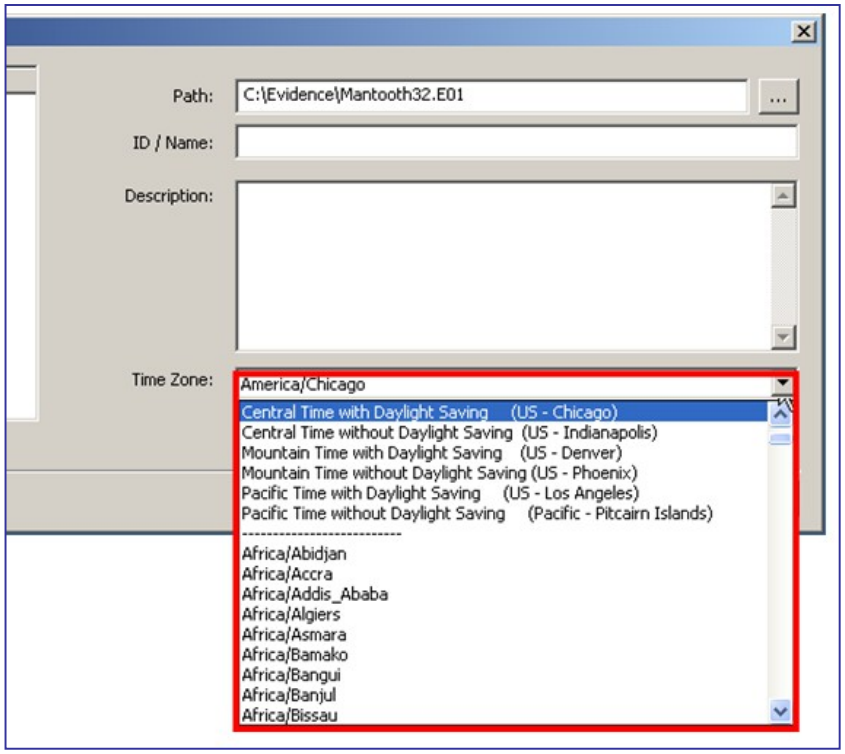
KFF Processing



Import Sets and Select Groups

KFF from National Software Reference Library (NSRL)

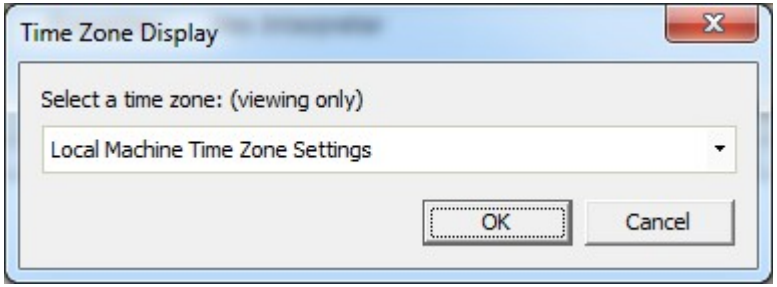
FTK Time Zone Settings



- 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

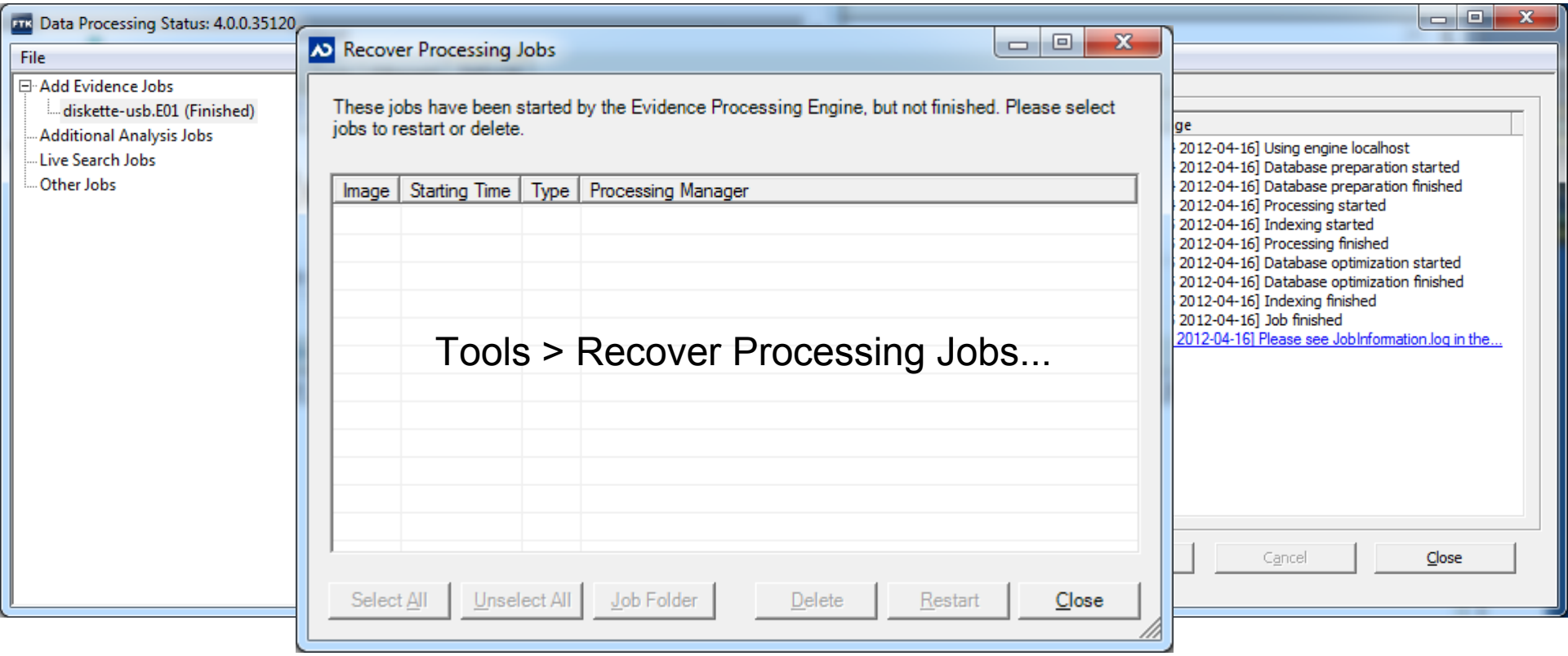
* Time Zone can be adjusted afterwards – visible in case log

View > Time Zone Display...

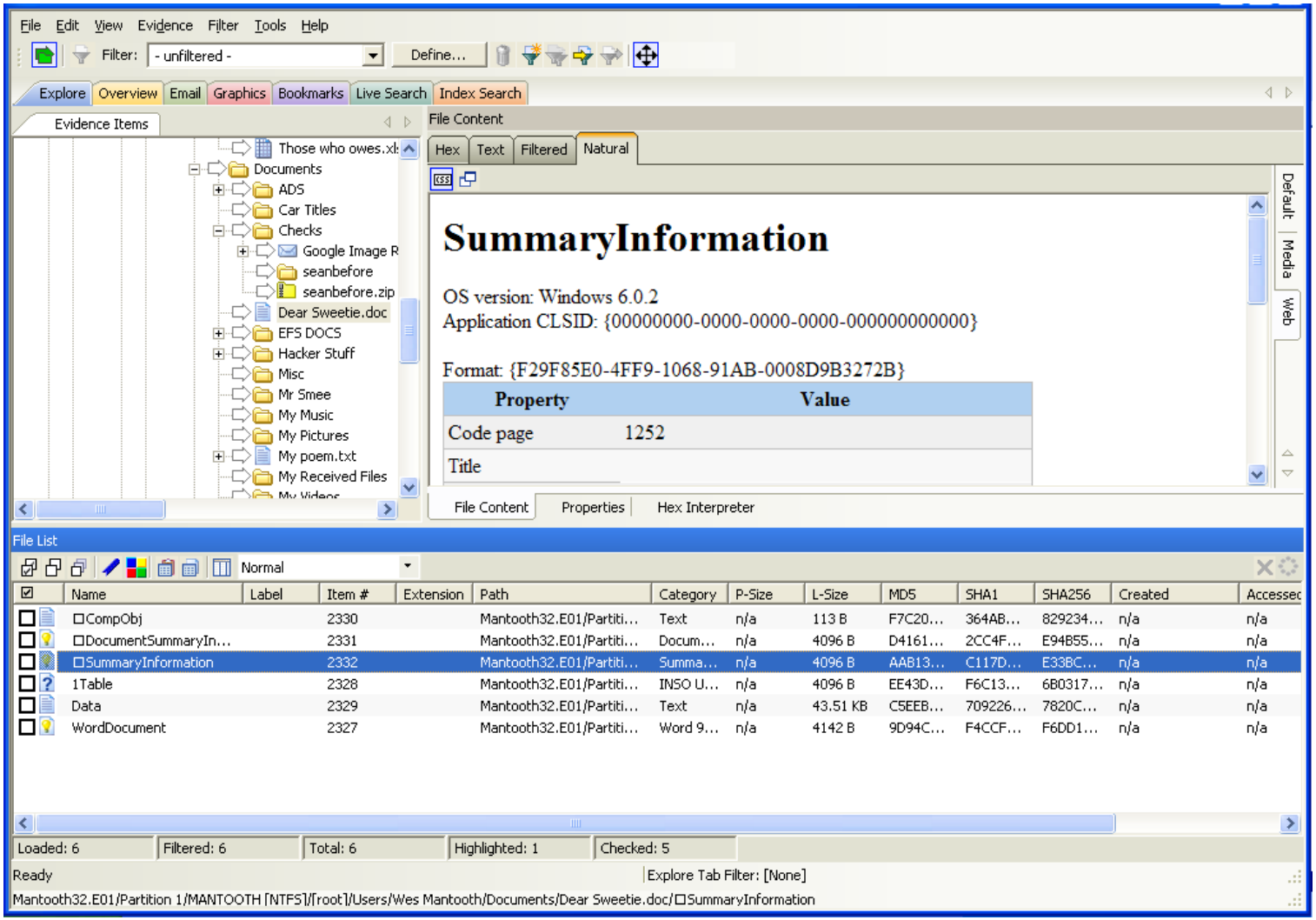


Jobs and recover jobs

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

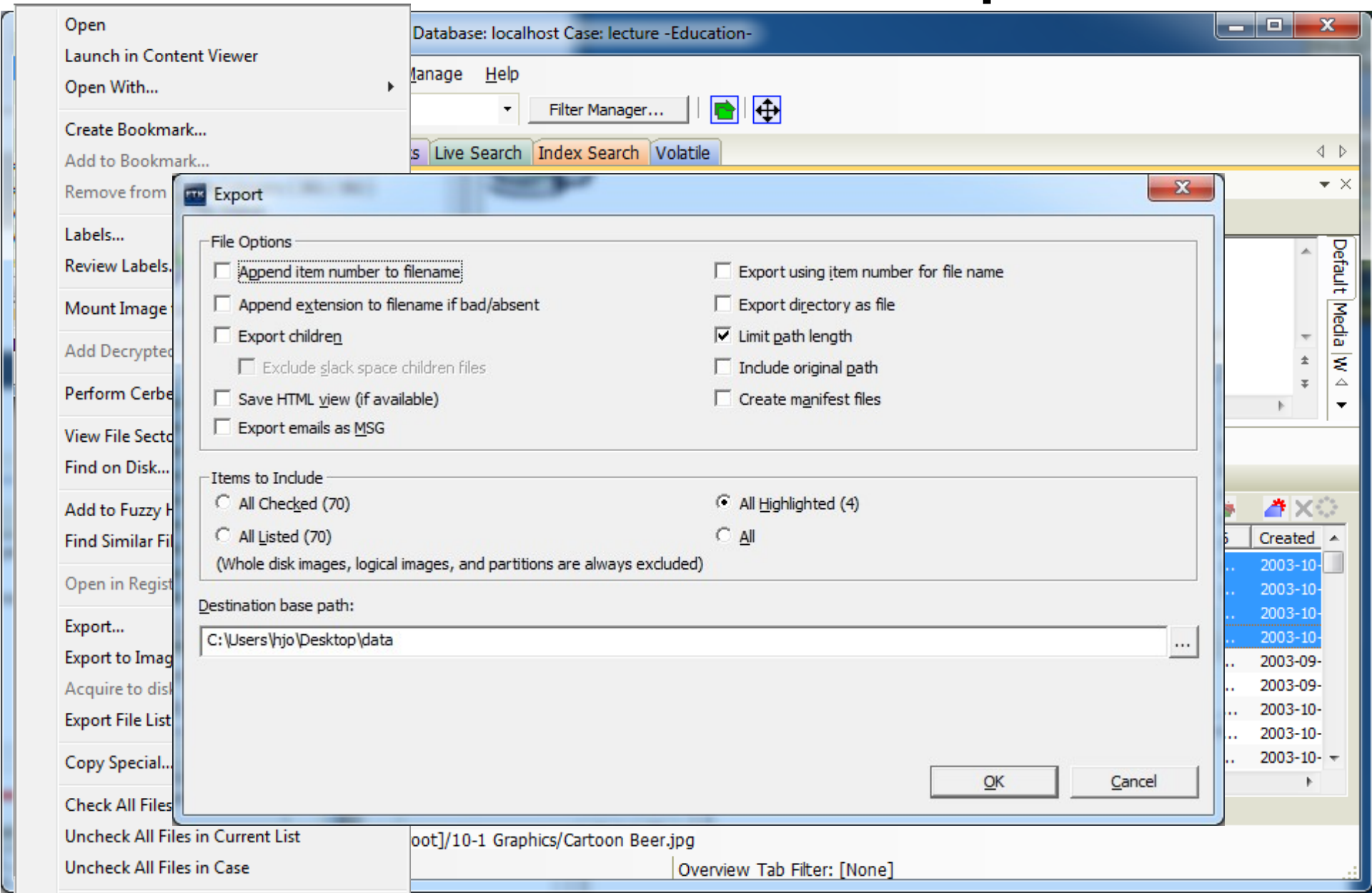


Compound Files



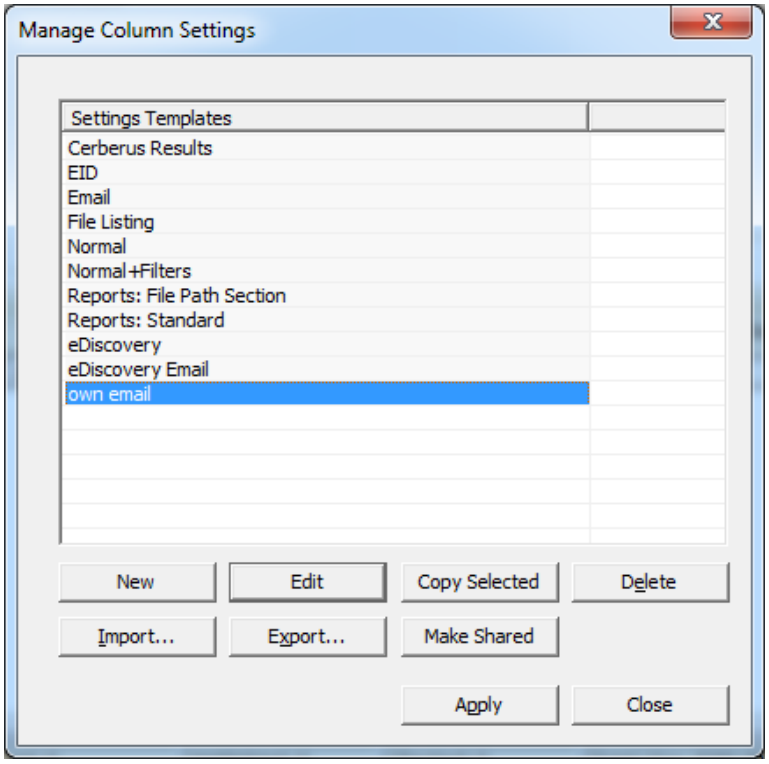
Compound files must also appear in the folder tree so they can be selected - to see their children.

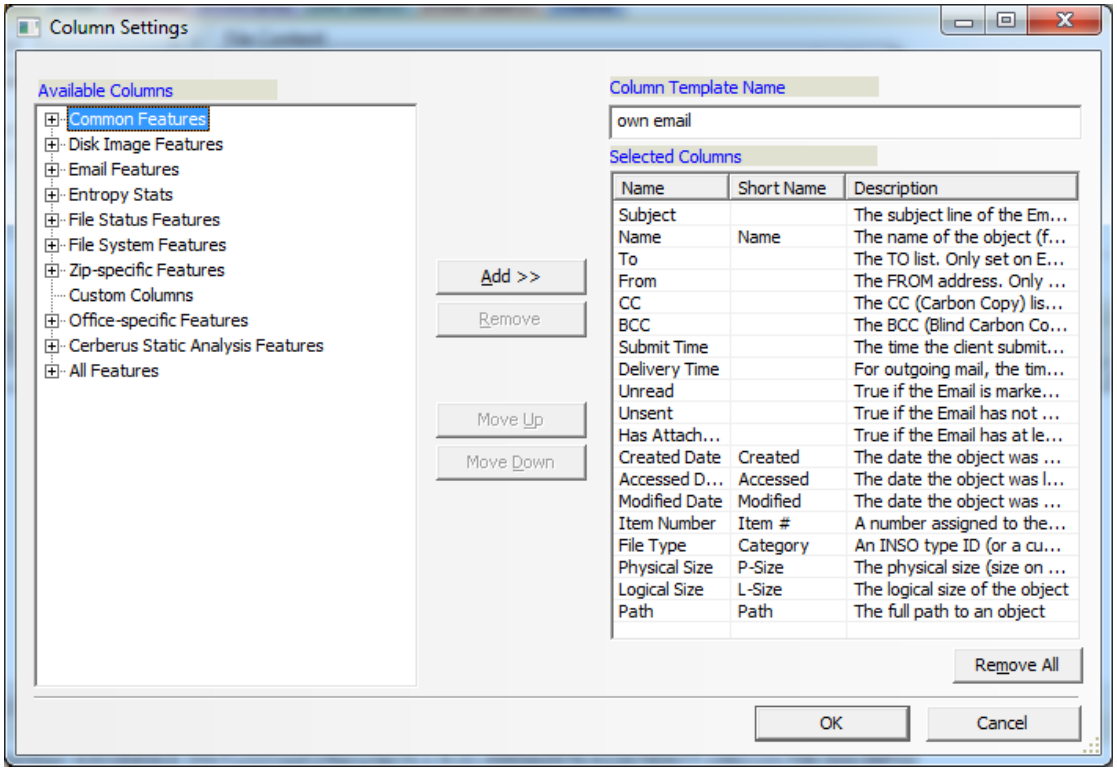
File and Folder Export



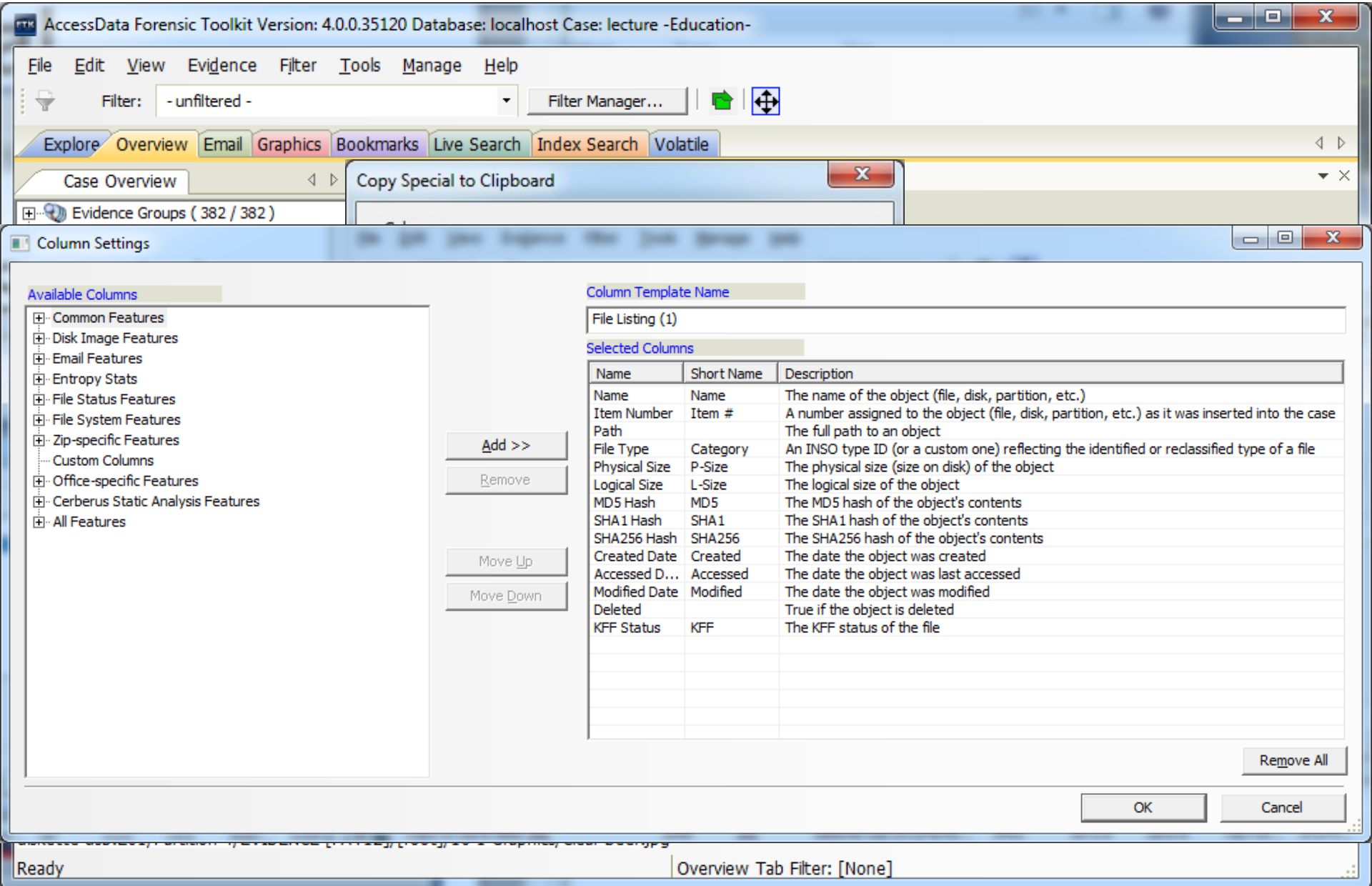
Column Settings

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

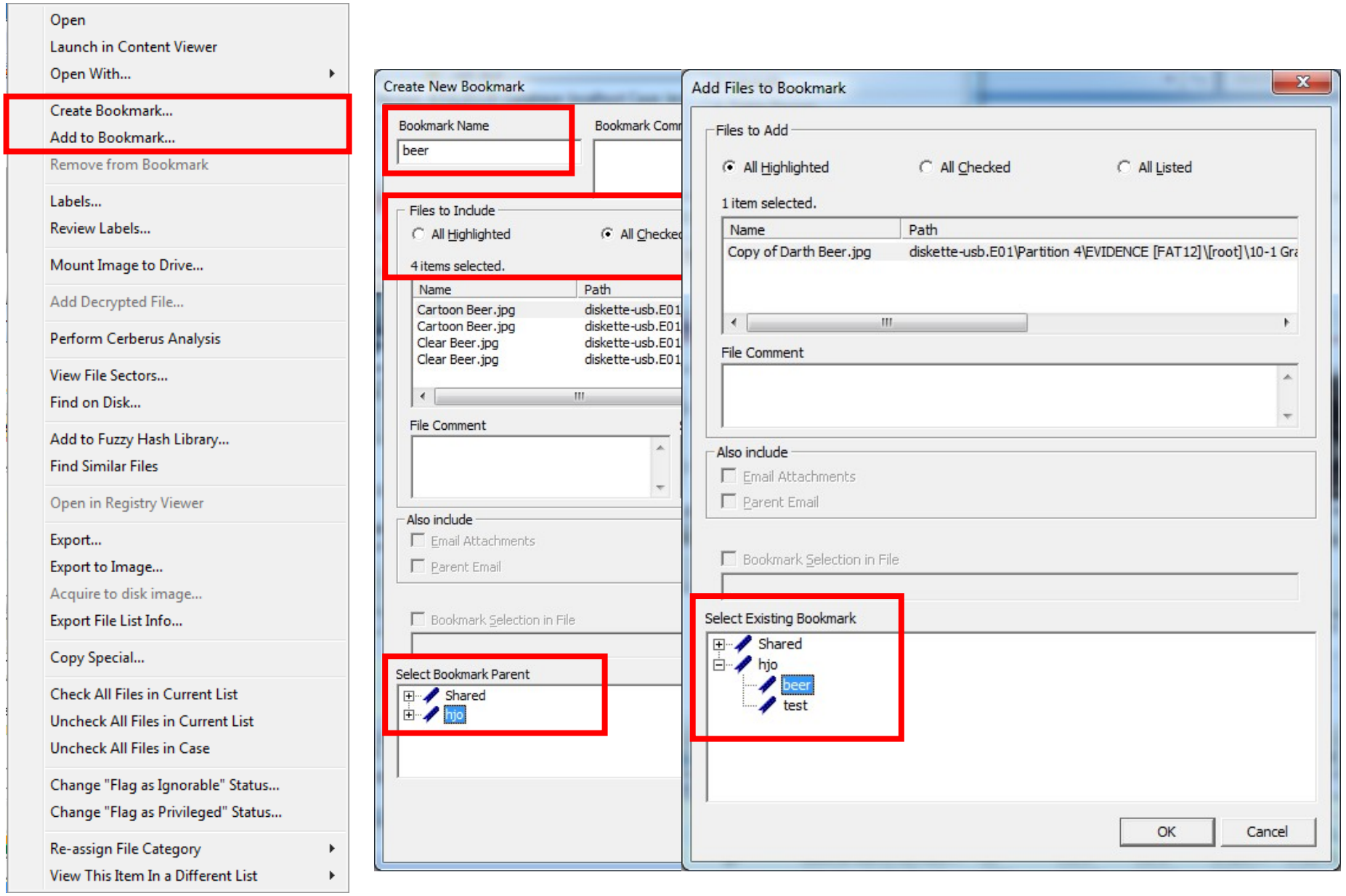




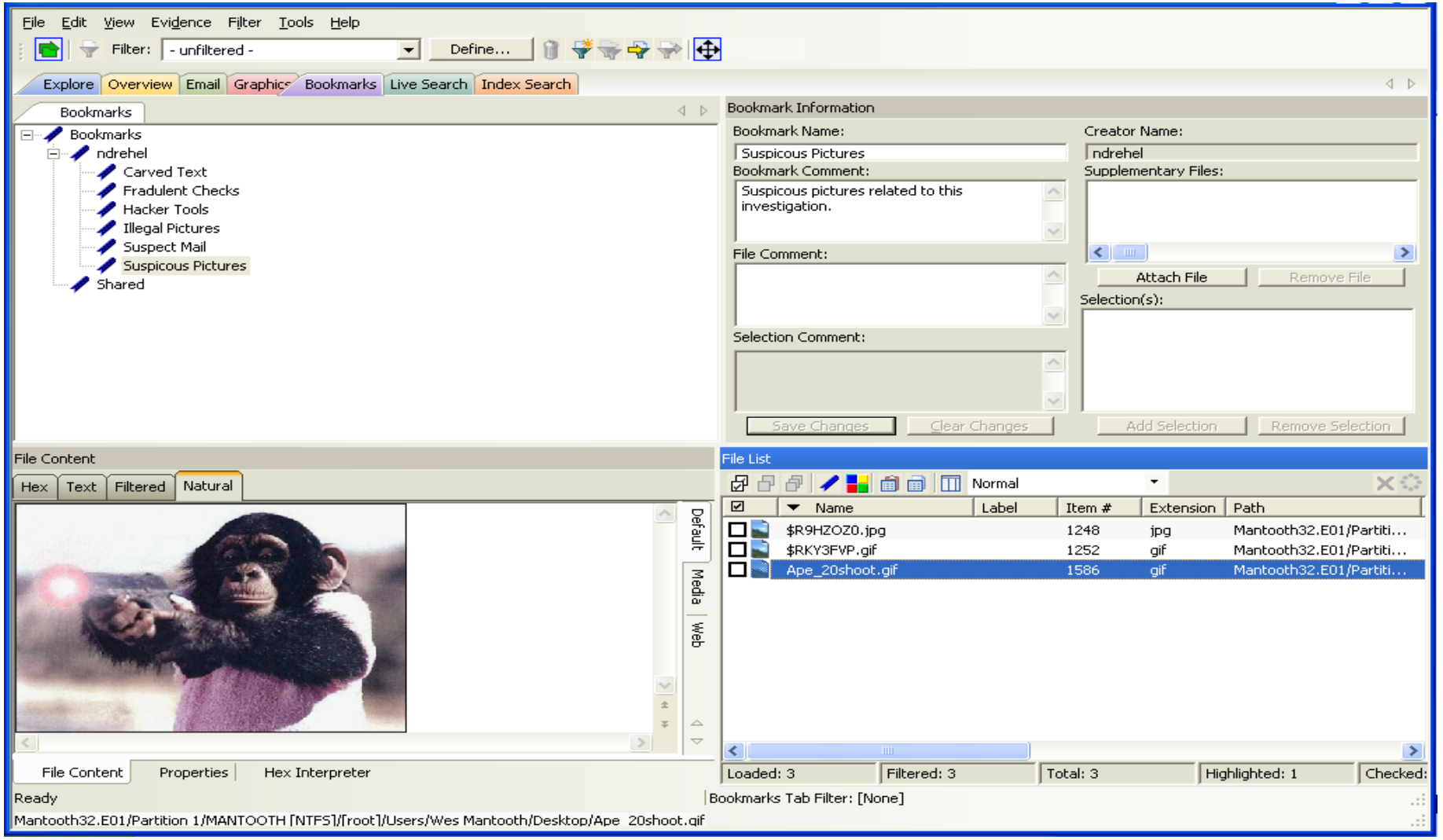
Copy Special > clipboard



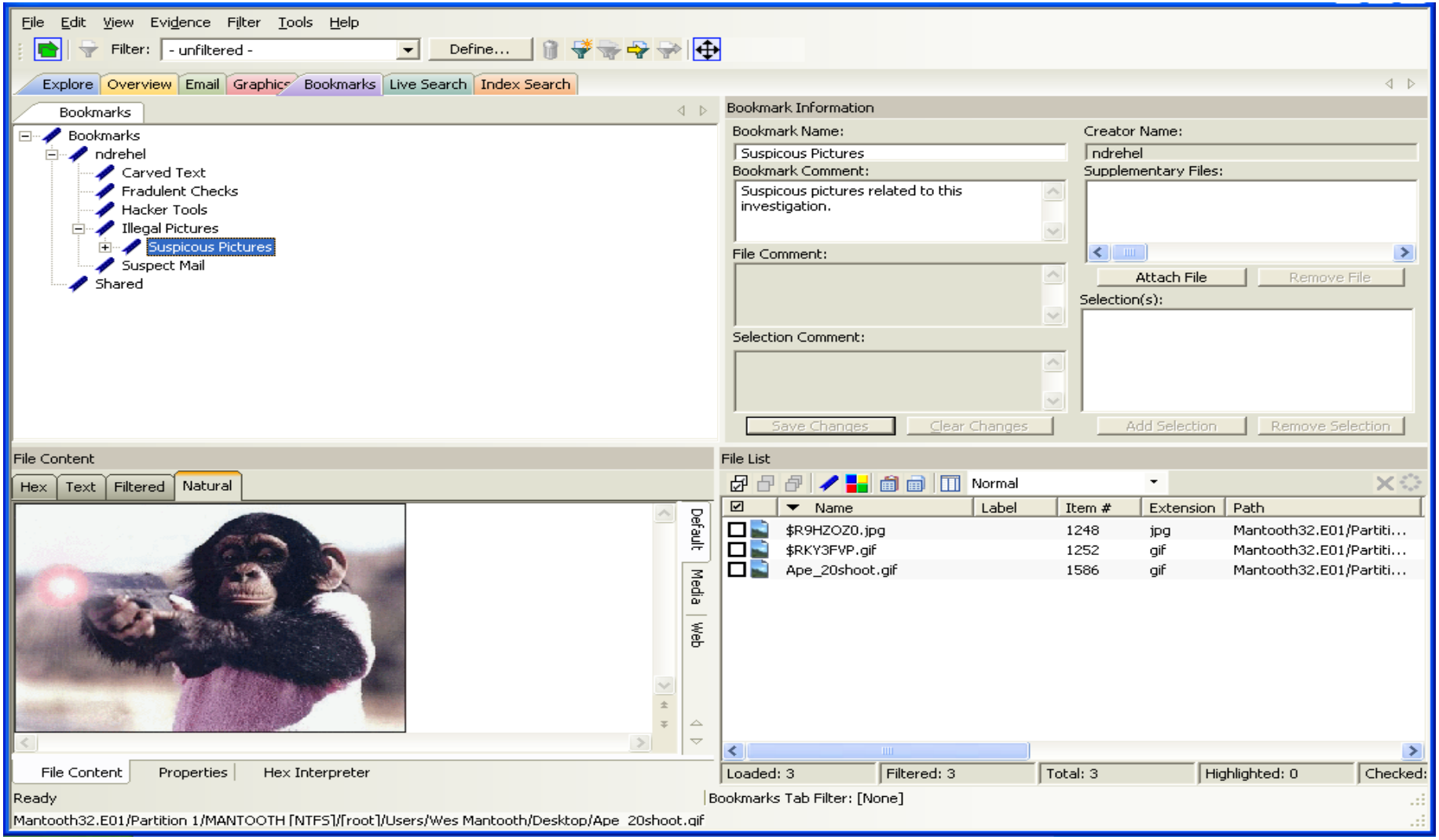
Create and Add Bookmarks



Managing Bookmarks



Managing Bookmarks



Bookmarks can be nested when created or later!