



**AccessData<sup>®</sup>**

**FTK 4/5**

**Narrow the focus  
Searching  
Filters**

# Narrow the Focus

- **Narrowing Evidence Items**

- KFF Management

- Can identify and ignore 40-70% of the files in a case
- Can identify “bad” files

- Checked Items

- Ignored / Privileged Items

- **Searching**

- Indexed Search

- Import Lists

- Live Search

- Regular Expressions

# KFF Management, FTK $\geq$ 4.2

- KFF libraries is maintained by the KFF Server
- Hash sets (or libraries) are imported from many sources
- Duplicate hash values are allowed
- Sets/libraries are placed in groups to run against the data
- Available sets/libraries may be assigned to more than one group

# KFF Management

## Default Groups Contain

- NSRL from NIST (National Institute of Standards and Technology)
- HashKeeper from NDIC (National Drug Intelligence Center) and DHS

The screenshot displays the KFF Admin Case: precious2 interface. The 'Defined Groups' table is highlighted with a red box and contains the following data:

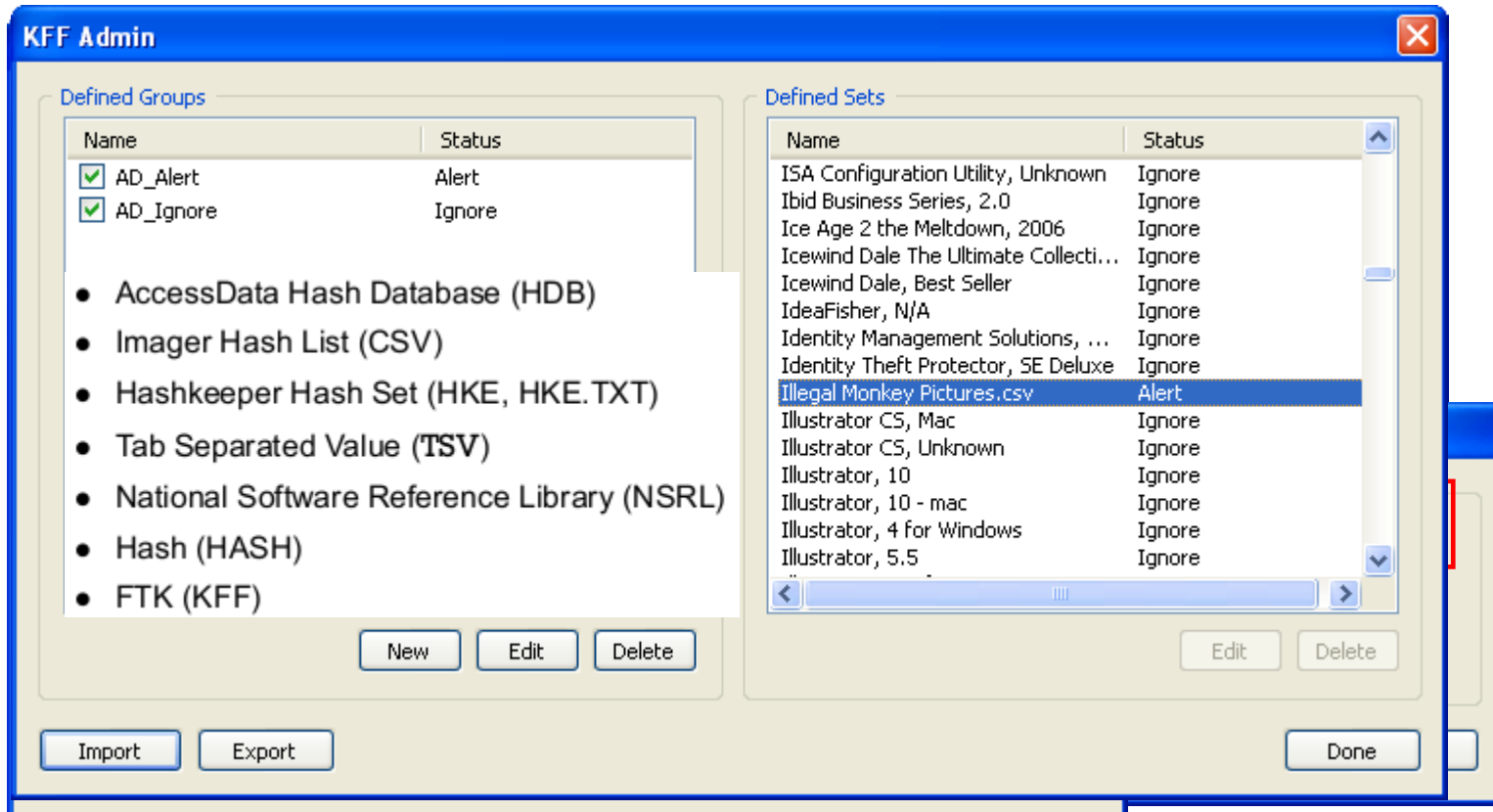
Name	Status	Default	Closed
<input checked="" type="checkbox"/> NSRL_Alert	Alert	*	YES
<input checked="" type="checkbox"/> NSRL_Ignore	Ignore	*	YES

The 'Defined Sets' table lists various software vendors and their status:

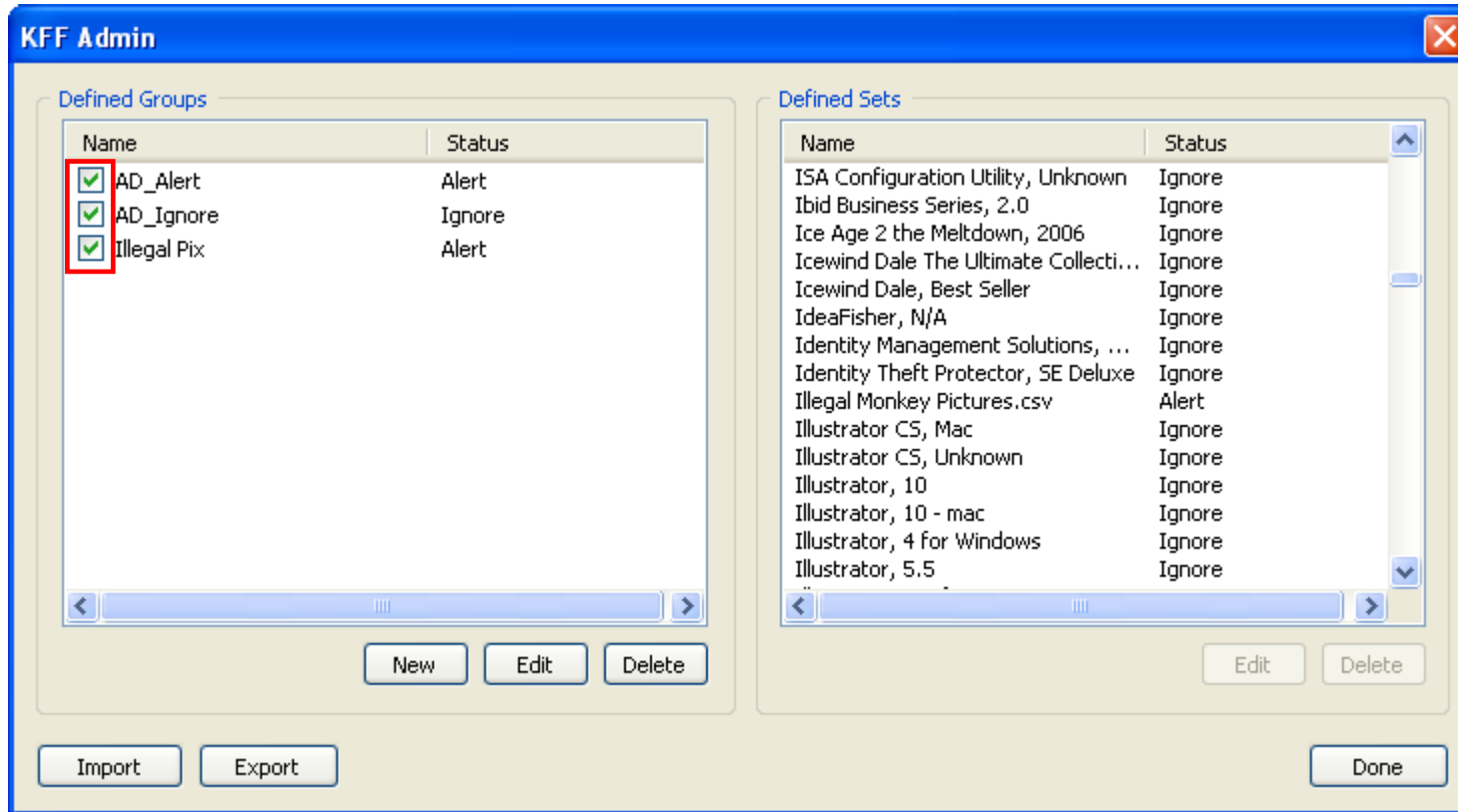
Name	Status	Source Vendor
Absolute Disk Wiper	Alert	National Software Reference Lib.
AccessData Ultimate Toolkit	Alert	National Software Reference Lib.
Active@Eraser Professional 4.1	Alert	National Software Reference Lib.
Active@KillDisk Professional Suite ...	Alert	National Software Reference Lib.
All In One Keylogger	Alert	National Software Reference Lib.
American Management Associatio...	Alert	National Software Reference Lib.
Anti-Hacker Toolkit	Alert	National Software Reference Lib.
Anti-Keylogger	Alert	National Software Reference Lib.
A_DIAL.ZIP	Alert	National Software Reference Lib.
CAC Developer Kit (CDK)	Alert	National Software Reference Lib.
Corporate Cd-rom	Alert	National Software Reference Lib.
Crime Scene	Alert	National Software Reference Lib.
DIAdem	Alert	National Software Reference Lib.

Buttons at the bottom include: Set As Defaults, New, Edit, Delete, Import, Export Groups, and Done. A note states: 'Closed KFF groups and sets cannot be edited or deleted.'

# Importing Hash Sets



# Defining Groups

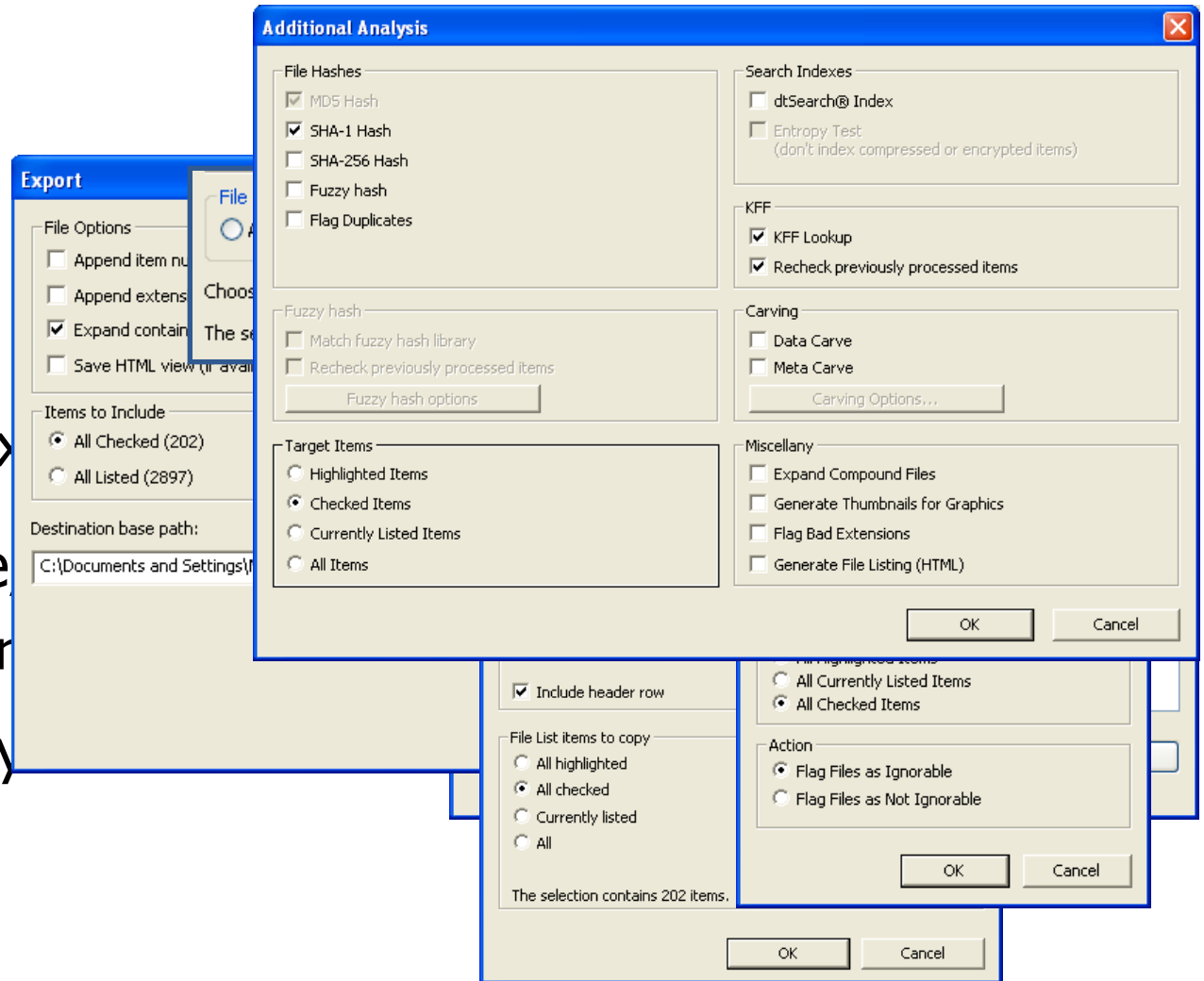


**You must check it to use it!**

# Checked Items

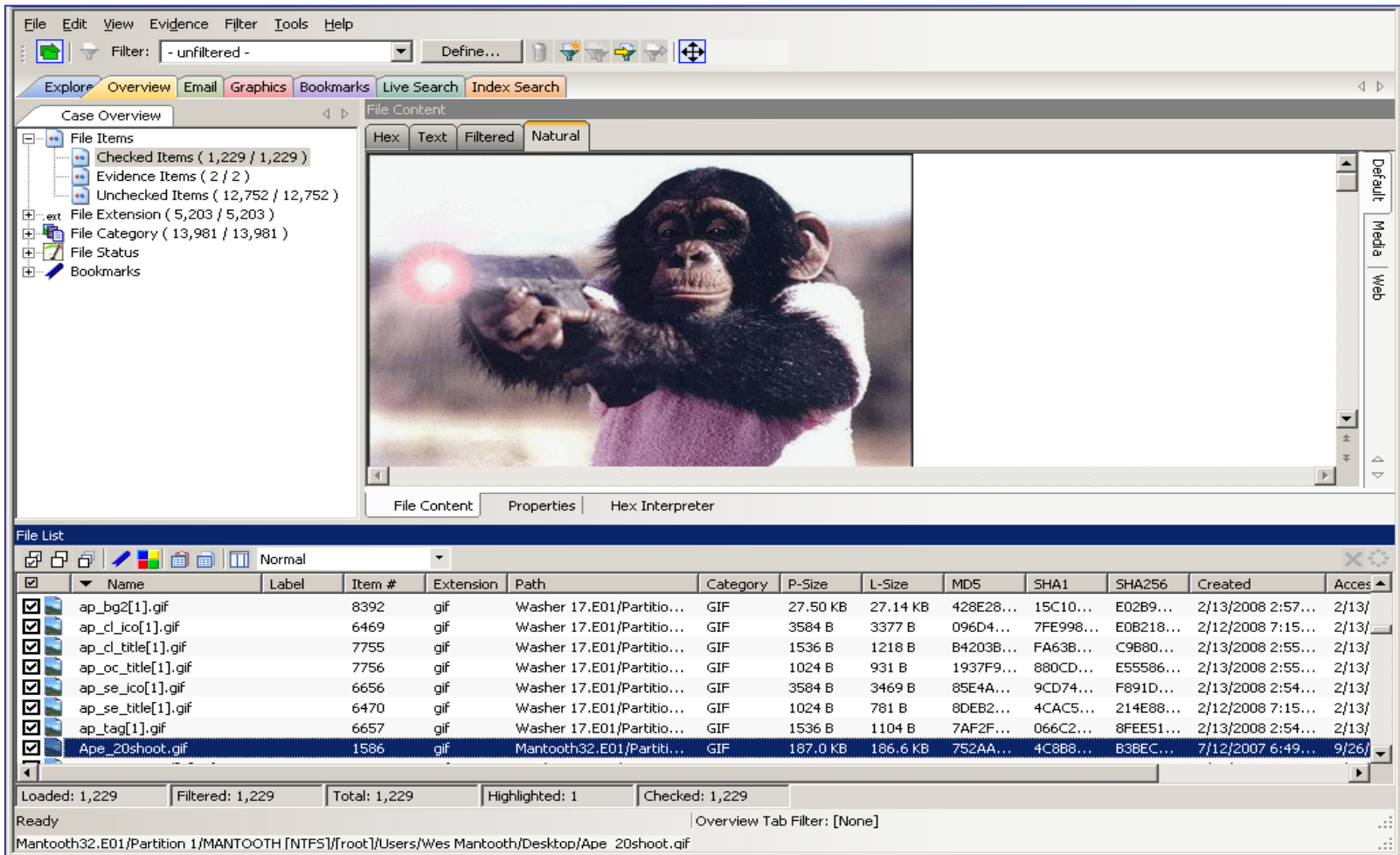
## Use Checked Items to perform special functions

- Bookmarking
- Searching
- Exporting
- Copy Special/Export
- Flag Ignoreable
  - Use with filter
- Additional Analy



# Checked Items

## Review Checked Files in the Case Overview Tab > File Items > Checked Items



The screenshot displays a forensic software interface with a 'Case Overview' tab. The 'File Items' section is expanded to show 'Checked Items (1,229 / 1,229)'. A file list at the bottom shows the following items:

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Access
ap_bg2[1].gif		8392	gif	Washer 17.E01/Partitio...	GIF	27.50 KB	27.14 KB	428E28...	15C10...	E02B9...	2/13/2008 2:57...	2/13/
ap_c_ico[1].gif		6469	gif	Washer 17.E01/Partitio...	GIF	3584 B	3377 B	096D4...	7FE998...	E0B218...	2/12/2008 7:15...	2/13/
ap_c_title[1].gif		7755	gif	Washer 17.E01/Partitio...	GIF	1536 B	1218 B	B4203B...	FA63B...	C9B80...	2/13/2008 2:55...	2/13/
ap_oc_title[1].gif		7756	gif	Washer 17.E01/Partitio...	GIF	1024 B	931 B	1937F9...	880CD...	E55586...	2/13/2008 2:55...	2/13/
ap_se_ico[1].gif		6656	gif	Washer 17.E01/Partitio...	GIF	3584 B	3469 B	85E4A...	9CD74...	F891D...	2/13/2008 2:54...	2/13/
ap_se_title[1].gif		6470	gif	Washer 17.E01/Partitio...	GIF	1024 B	781 B	8DEB2...	4CAC5...	214E88...	2/12/2008 7:15...	2/13/
ap_tag[1].gif		6657	gif	Washer 17.E01/Partitio...	GIF	1536 B	1104 B	7AF2F...	066C2...	8FEES1...	2/13/2008 2:54...	2/13/
Ape_20shoot.gif		1586	gif	Mantooth32.E01/Partiti...	GIF	187.0 KB	186.6 KB	752AA...	4C8B8...	B3BEC...	7/12/2007 6:49...	9/26/

The main preview area shows a GIF image of a chimpanzee pointing. The interface includes a menu bar (File, Edit, View, Evidence, Filter, Tools, Help), a toolbar, and a 'File List' section at the bottom with a table of file details and summary statistics.

Summary Statistics:  
Loaded: 1,229 | Filtered: 1,229 | Total: 1,229 | Highlighted: 1 | Checked: 1,229

Ready | Overview Tab Filter: [None]

Mantooth32.E01/Partition 1/MANTTOOTH [NTFS][root]/Users/Wes Mantooth/Desktop/Ape\_20shoot.gif



# Indexed Searching

Check "Accumulate Results" to get result from Operators at once!

The screenshot displays a forensic search application interface. At the top, there is a menu bar (File, Edit, View, Evidence, Filter, Tools, Help) and a toolbar with a 'Filter' dropdown set to '- unfiltered -' and a 'Define...' button. Below the menu is a tabbed interface with 'Index Search' selected. The main window is divided into several sections:

- Terms:** A text input field contains 'washing' with an 'Add' button. Below it is a table of indexed words and their total hits.
- Search Criteria:** A section for defining search operators and terms. The 'Operators' section has 'And' selected. The 'Terms' section has 'All' selected. A checkbox labeled 'Accumulate Results' is checked. Below this is a table of search terms and their total hits.
- Index Search Results:** A list of search results, each showing the number of hits and the item name. The results are: 10 hits -- Item 2981 [images[1].htm] M..., 10 hits -- Item 3127 [images[1].htm] M..., 10 hits -- Item 3285 [images[3].htm] M..., 7 hits -- Item 3264 [chapter3[1].htm] M..., 7 hits -- Item 7729 [search[2]] Washer, 3 hits -- Item 2476 [history.dat] Manto..., 2 hits -- Item 3534 [RE: Whats up in D I...], 2 hits -- Item 3642 [Re: Whats up in D I...].
- File Content:** A section showing the content of the selected file. It displays an email header and body text.
- File List:** A table listing files found in the search. The columns are Name, Label, Item #, and Ext. The file 'Re: Whats up in D town?' is selected.

The 'File Content' section shows the following text:

Re: Whats up in D town?  
Re: Whats up in D town?  
From:  
John Washer  
To:  
Wes Mantooth  
Subject:  
Re: Whats up in D town?  
Sent:  
6/21/2007 9:09:28 PM +00:00

So.. how are you going to get the writing off these? The usual method? Does it work the same with scripts as checks? <http://celtickane.com/projects/washing/>  
----- Original Message ----- From: Wes Mantooth To: 'John Washer' Sent: Thursday, June 21, 2007 3:06 PM Subject: RE: Whats up in D town?

The 'File List' section shows the following table:

Name	Label	Item #	Ext
history.dat		2476	dat
images[1].htm		2981	htm
images[1].htm		3127	htm
images[3].htm		3285	htm
mime part 0 (text/plain)		15285	<mi
mime part 0 (text/plain)		15354	<mi
mime part 1 (text/html)		15286	<mi
mime part 1 (text/html)		15355	<mi
RE: Whats up in D town?		3534	
Re: Whats up in D town?		3642	
RE: Whats up in D town?		3646	
search[2]		7729	<mi
search[3]		7299	<mi
Untitled0		14803	<mi

At the bottom of the interface, there is a status bar showing 'Loaded: 25', 'Filtered: 25', and 'Total: 25'. The bottom-most text indicates the current file path: 'Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/Outlook.pst/Personal Folders/Top of Personal Folders/Inbox/Re: Whats up in D town?'.

# Indexed Search Options

The screenshot displays the 'Indexed Search Options' dialog box over a search application interface. The dialog box is titled 'Indexed Search Options' and contains the following sections:

- Search Options:**
  - Stemming
  - Phonic
  - Synonym
  - Fuzzy
- Result Options:**
  - Max Files to List: [ ]
  - Max Hits Per File: [ ]
  - Max Words to Return: [ 65536 ]
- Files To Search:**
  - All Files
  - Filename Pattern: [ ]
  - Files Saved Between: [ 6/23/2009 ] and [ 6/23/2009 ]
  - Files Created Between: [ 6/23/2009 ] and [ 6/23/2009 ]
  - File Size Between: (bytes) [ ] and [ ]
- Save as Default
- Buttons: OK, Cancel

The background application shows an 'Index Search' tab with a search term 'washing'. The 'Index Search Results' pane on the right lists search results, with the 'Options...' button highlighted in red. Below the search results is a 'File List' table:

Name	Label	Item #	Ext
history.dat		2476	dat
images[1].htm		2981	htm
images[1].htm		3127	htm
images[3].htm		3285	htm
mime part 0 (text/plain)		15285	<mi
mime part 0 (text/plain)		15354	<mi
mime part 1 (text/html)		15286	<mi
mime part 1 (text/html)		15355	<mi
RE: Whats up in D town?		3534	
RE: Whats up in D town?		3642	
RE: Whats up in D town?		3646	
search[2]		7729	<mi
search[3]		7299	<mi
Untitled0		14803	<mi

At the bottom of the application, the status bar shows: 'Loaded: 25', 'Filtered: 25', 'Total: 25'. The system tray at the bottom indicates the search filter is '[None]' and the current path is 'Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/Users/Wes Mantooth/AppData/Local/Microsoft/Outlook/Outlook.pst/Personal Folders/Top of Personal Folders/Inbox/Re: Whats up in D town?'.

# Indexed Search Options

- Stemming
  - Ord med samma rot, jobb, jobbar
- Phonic
  - Ord som låter lika
- Synonym
  - Ord med samma betydelse
- Fuzzy
  - Ord med liknande stavning

The screenshot shows a dialog box titled "Index Search Options" with a close button (X) in the top right corner. The dialog is divided into three main sections: "Search Options", "Result Options", and "Files To Search".

**Search Options:** This section contains four checkboxes: "Stemming" (checked), "Phonic", "Synonym", and "Fuzzy". To the right of the "Fuzzy" checkbox is a small numeric spinner control set to the value "1".

**Result Options:** This section contains three input fields: "Max Files to List:" (empty), "Max Hits Per File:" (empty), and "Max Words to Return:" (set to "65536").

**Files To Search:** This section contains a checked checkbox for "All Files" and three unchecked checkboxes: "File Name Pattern", "Files Saved Between:", and "Files Created Between:". To the right of these checkboxes are input fields for file names and date ranges. The "Files Saved Between:" and "Files Created Between:" fields are both set to "2012-04-10" with dropdown arrows. The "File Size Between:" field is currently empty.

At the bottom of the dialog, there is a "Reset to Factory Defaults" button, a "Save as Defaults" checkbox (unchecked), and "OK" and "Cancel" buttons.

# Import Lists

The screenshot displays a forensic search application interface. At the top, there is a menu bar (File, Edit, View, Evidence, Filter, Tools, Help) and a toolbar with various icons. Below the menu is a navigation bar with tabs: Explore, Overview, Email, Graphics, Bookmarks, Live Search, and Index Search. The main window is divided into several sections:

- Search Criteria:** Shows operators (And, Or) and terms (All, Selected). A table lists search terms and their total hits.
- Index Search Results:** A list of search results with details like item numbers and offsets.
- File Content:** Displays the content of a selected file, showing a letterhead and a business proposal.
- File List:** A table listing files with their names, labels, item numbers, and extensions.

**Search Criteria Table:**

Search Terms	Total Hits
dog	263
cat	269
check	414
washing	125
wes	4542
mantooth	7878

**Index Search Results:**

- 7 hits -- Item 2739 [1Table] Mantooth3
- 7 hits -- Item 2744 [C:\Users\Wes Manl
- 7 hits -- Item 3376 [mime part 23 (appli
- 7 hits -- Item 3789 [Confidential Busine

**File Content:**

Lagos, Nigeria.  
Attention: The President/CEO  
Dear Sir,

Confidential Business Proposal  
Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers Of Commerce and Industry, I have the privilege to request your assistance to transfer the sum of

**File List:**

Name	Label	Item #	Ex...
RevelationHelper.dll		1817	dll
Vampire Terminology.doc		1050	doc
Vampire.doc		1051	doc
Exhume.doc		1221	doc
Astral.doc		1222	doc
Arabic Text.doc		1578	doc
Japanese text.doc		1579	doc
Dear Sweetie.doc		1606	doc
russ_4_ящеркой.doc		1779	doc
C money plates.doc		1804	doc
John.doc		1806	doc
Wes.doc		1807	doc
Confidential Business Le...		3789	doc
News Report.doc		4371	doc

Loaded: 3,690 | Filtered: 3,690 | Total: 3,690

# Searching Checked Items

The screenshot displays a search application window with the following components:

- Menu Bar:** File, Edit, View, Evidence, Filter, Tools, Help
- Filter:** - unfiltered -
- Navigation Tabs:** Explore, Overview, Email, Graphics, Bookmarks, Live Search, Index Search
- Search Criteria:**
  - Operators:  Add,  Or
  - Terms:  All,  Selected
  - Search Terms Table:

Search Terms	Total Hits
check	414
washing	125
- Index Search Results:**
  - dtSearch@ Indexed Search {Query: ("check an
  - Allocated Space -- 46 hits in 7 files
    - 16 hits -- Item 14803 [Untitled0] Wash
    - 15 hits -- Item 7299 [search[3]] Washe
    - 7 hits -- Item 7729 [search[2]] Washer
    - 2 hits -- Item 15285 [mime part 0 (text
    - 2 hits -- Item 15286 [mime part 1 (text
    - 2 hits -- Item 15354 [mime part 0 (text
    - 2 hits -- Item 15355 [mime part 1 (text
  - Unallocated Space -- 0 hits in 0 files
- File List:**

Checked	Name	Label	Item #	Ex...
<input checked="" type="checkbox"/>	search[3]		7299	<missin...
<input checked="" type="checkbox"/>	search[2]		7729	<missin...
<input checked="" type="checkbox"/>	Untitled0		14803	<missin...
<input checked="" type="checkbox"/>	mime part 0 (text/plain)		15285	<missin...
<input checked="" type="checkbox"/>	mime part 1 (text/html)		15286	<missin...
<input checked="" type="checkbox"/>	mime part 0 (text/plain)		15354	<missin...
<input checked="" type="checkbox"/>	mime part 1 (text/html)		15355	<missin...
- File Content:** Hex, Text, Filtered, Natural
- Status Bar:** Loaded: 7, Filtered: 7, Total: 25, Highli
- Index Search Tab Filter:** Checked Files

# Live Search

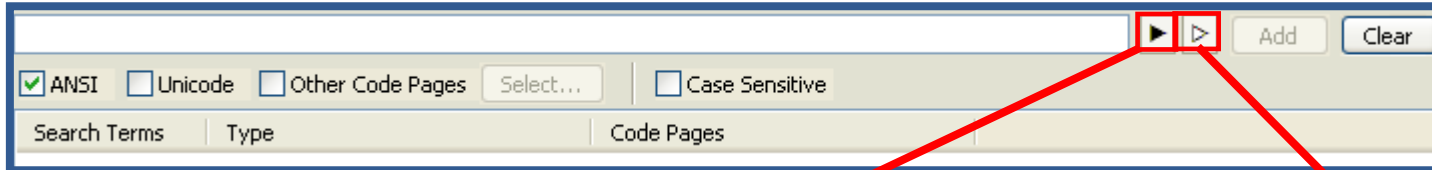
The screenshot shows a forensic software interface with the following components:

- Menu Bar:** File, Edit, View, Evidence, Filter, Tools, Help
- Filter:** - unfiltered -
- Navigation:** Explore, Overview, Email, Graphics, Bookmarks, Live Search, Index Search
- Search Options:** Text, Pattern, Hex; ANSI, Unicode, Case Sensitive
- Search Terms Table:**

Search Terms	Type	Code Pages
- Search Parameters:** Max Hits Per File: 200; Search Filter: Checked Files
- File Content:** Hex, Text, Filtered, Natural views. The hex dump shows data from offset 0c10 to 0d30. The text column contains fragments of an email or document, with search results highlighted in blue.
- Live Search Results (Right Sidebar):**
  - Allocated Space -- 14 hits in 8 files
  - 3 hits -- Item 5579 [SLIST.doc] Washer
  - 3 hits -- Item 15227 [SLIST.doc] Washer
    - Item 15227, Offset 34d0 (13520): <
    - Item 15227, Offset 44f8 (17656): <
    - Item 15227, Offset 678c (26508): <
  - 2 hits -- Item 15242 [News Report.doc]
    - Item 15242, Offset 0ce0 (3296): ige
    - Item 15242, Offset 0d2d (3373): , T
  - 2 hits -- Item 15447 [WordDocument1.W...
- File List (Bottom Right):**

Name	Label	Item #
DocumentSummaryIn...		9311
DocumentSummaryIn...		15439
SummaryInformation		9312
SummaryInformation		15440
088432		5283
News Report.doc		15242
SLIST.doc		5579
SLIST.doc		15227
WordDocument		15447
- Status Bar:** Loaded: 9, Filtered: 9, Total: 9

# Regular Expressions



<code>\t</code> - tab
<code>\s</code> - whitespace character
<code>\d</code> - decimal digit - same as <code>[0-9]</code>
<code>\u</code> - upper case character - same as <code>[A-Z]</code>
<code>\l</code> - lower case character - same as <code>[a-z]</code>
<code>\w</code> - word character - same as <code>[a-zA-Z0-9_]</code>
<code>\n</code> - newline character
<code>\r</code> - return character
<code>\b</code> - at word boundary
<code>\B</code> - not at word boundary
<code>\&lt;</code> - at start of word
<code>\&gt;</code> - at end of word
<code>^</code> - at start of line
<code>\$</code> - at end of line
<code>\`</code> - at start of file
<code>\'</code> - at end of file
<code>[[alpha:]]</code> - alpha character
<code>[[alnum:]]</code> - alpha-numeric character
<code>[[blank:]]</code> - whitespace except line separator

- Left select helps to write them live
- Right, select from list or Edit Expressions

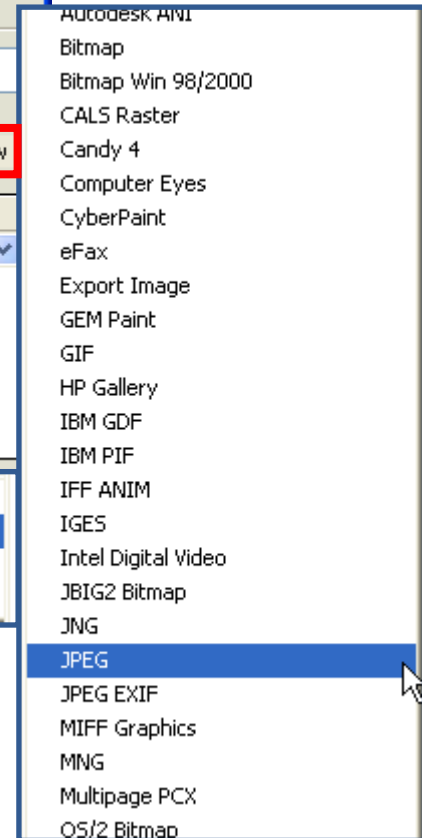
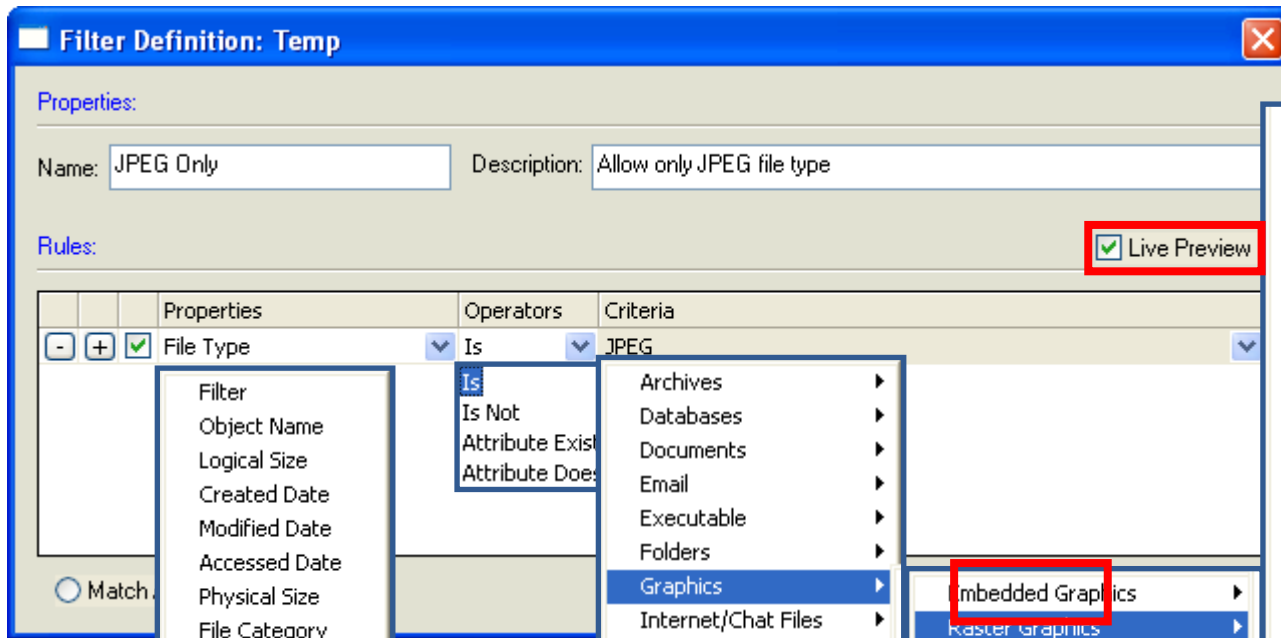
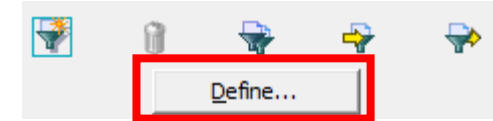
Page with many examples!  
<http://accessdata.com/regular-expressions>

Visa card `(xxxx-xxxx-xxxx-xxxx)`  
`\<((\d\d\d\d)[\s- ]){3}\d\d\d\d\>`

US Phone Number
UK Phone Number
Credit Card Number
American Express
Diner's Club
Discover
MasterCard/Visa
Social Security Number
IP Address
MAC Address
URL {http, https, ftp, ftps}
mailto: ...
... .com
... .edu
... .info
... .net
... .org
... .gov
... .museum
... .tv
... .<any>
... @ ... .com
... @ ... .edu
... @ ... .gov
... @ ... .net
... @ ... .org
... @ ... .<any> email address
Kazaa DBB
Kazaa DAT file
Limewire DAT
Edit expressions...

# Defining a Filter

Filter > New  
OR



**Live Preview lets you see the results as you tweak your filter!**



# Adding Rules

<input checked="" type="checkbox"/>	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Access
<input type="checkbox"/>	Dock.jpg		1645	jpg	Mantooth32.E01/Partiti...	JPEG E...	309.5 KB	309.5 KB	8A572...	939C4...	68D34...	7/14/2007 1:04...	7/13/
<input type="checkbox"/>	Dotted_Lines.emf		2096	emf	Mantooth32.E01/Partiti...	Windo...	4096 B	3792 B	3B2C6...	FD180...	C84E5...	7/7/2007 5:52:...	7/7/2
<input type="checkbox"/>	DSC00252.JPG		1587	jpg	Mantooth32.E01/Partiti...	JPEG E...	2169 KB	2169 KB	EA55F...	BA352...	5D160...	7/7/2007 6:38:...	9/26/
<input type="checkbox"/>	electronic-checks.jpg		1795	jpg	Mantooth32.E01/Partiti...	JPEG	24.00 KB	23.56 KB	3E613B...	AF298...	3DEC7...	3/5/2007 7:52:...	7/13/
<input type="checkbox"/>	enlg_z146.gif		1796	gif	Mantooth32.E01/Partiti...	GIF	112.0 KB	111.7 KB	F97152...	9F1BC...	B01654...	3/5/2007 7:52:...	7/13/
<input type="checkbox"/>	ERROR.BMP		1810	bmp	Mantooth32.E01/Partiti...	Bitmap	1024 B	888 B	1FE84...	06C61...	724CE...	7/14/2007 1:02...	7/13/
<input type="checkbox"/>	funny.png		1609	png	Mantooth32.E01/Partiti...	PNG	66.00 KB	65.70 KB	E15385...	2D33A...	7C25A...	3/5/2007 7:52:...	7/13/
<input type="checkbox"/>	Garden.jpg		2098	jpg	Mantooth32.E01/Partiti...	JPEG	23.50 KB	23.31 KB	4A35A...	EEDED...	6D2CC...	7/7/2007 5:52:...	7/7/2
<input type="checkbox"/>	Genko_1.emf		2099	emf	Mantooth32.E01/Partiti...	Windo...	5632 B	5524 B	41C3E...	E80F0...	BDFC3...	7/7/2007 5:52:...	7/7/2
<input type="checkbox"/>	Genko_2.emf		2100	emf	Mantooth32.E01/Partiti...	Windo...	10.50 KB	10.10 KB	27B578...	3ADAB...	EB8A9...	7/7/2007 5:52:...	7/7/2
<input type="checkbox"/>	gift_certif_sample.jpg		1610	jpg	Mantooth32.E01/Partiti...	JPEG	17.50 KB	17.48 KB	B8B19...	2992C...	3D4C8...	3/5/2007 7:52:...	7/13/
<input type="checkbox"/>	Graph.emf		2101	emf	Mantooth32.E01/Partiti...	Windo...	114.0 KB	114.0 KB	387CA...	65B161...	AF08E...	7/7/2007 5:52:...	7/7/2
<input type="checkbox"/>	GreenBubbles.jpg		2103	jpg	Mantooth32.E01/Partiti...	JPEG	6656 B	6406 B	EF7814...	88DF4...	9E7582...	7/7/2007 5:52:...	7/7/2
<input type="checkbox"/>	grid_cm.wmf		2104	wmf	Mantooth32.E01/Partiti...	Windo...	3072 B	2920 B	88AAC...	25BDF...	165DC...	7/7/2007 5:52:...	7/7/2

Loaded: 87    Filtered: 87    Total: 13,968    Highlighted: 0    Checked: 0

Show only file category graphics

+

Match Owner SID ending in 1000

+

***Match All Rules***

**= Narrow Scope**

# Adding Rules

<input type="checkbox"/>	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Access
<input type="checkbox"/>	#local		3323		Mantooth32.E01/Partiti...	Folder	160 B	160 B	784CF...	5E8ED...	FESAC...	7/7/2007 5:57:...	7/2/2
<input type="checkbox"/>	#Security		1975		Mantooth32.E01/Partiti...	Folder	272 B	272 B	4CFDC...	84E8C...	AE6FB...	7/7/2007 5:57:...	7/2/2
<input type="checkbox"/>	#SharedObjects		1976		Mantooth32.E01/Partiti...	Folder	152 B	152 B	EE68B1...	9569E9...	DCBD2...	7/7/2007 5:57:...	7/2/2
<input type="checkbox"/>	\$EFS		1915		Mantooth32.E01/Partiti...	EFS FE...	1024 B	712 B	6DF8C...	202EC...	ABD72...	3/5/2007 8:14:...	3/5/2
<input type="checkbox"/>	\$EFS		1916		Mantooth32.E01/Partiti...	EFS FE...	1024 B	712 B	C7A6B...	4CBDD...	556173...	3/5/2007 8:14:...	3/5/2
<input type="checkbox"/>	\$EFS		1917		Mantooth32.E01/Partiti...	EFS FE...	1024 B	712 B	83F0E0...	347502...	C6214...	3/5/2007 8:14:...	3/5/2
<input type="checkbox"/>	\$EFS		1918		Mantooth32.E01/Partiti...	EFS FE...	1024 B	712 B	A6665...	2AD2F...	660DB...	3/5/2007 8:14:...	3/5/2
<input type="checkbox"/>	\$I30		1584		Mantooth32.E01/Partiti...	Index ...	4096 B	4096 B	91B044...	005761...	34997F...	7/7/2007 4:09:...	7/2/2
<input type="checkbox"/>	\$I30		1597		Mantooth32.E01/Partiti...	Index ...	12.00 KB	12.00 KB	C4C85...	839711...	D9FE1...	7/7/2007 4:09:...	7/2/2
<input type="checkbox"/>	\$I30		1631		Mantooth32.E01/Partiti...	Index ...	4096 B	4096 B	C9374...	6E8786...	96A54...	7/7/2007 4:09:...	7/2/2
<input type="checkbox"/>	\$I30		1640		Mantooth32.E01/Partiti...	Index ...	4096 B	4096 B	DCDEF...	948D4...	938E4...	7/7/2007 4:09:...	7/2/2
<input type="checkbox"/>	\$I30		1649		Mantooth32.E01/Partiti...	Index ...	4096 B	4096 B	766089...	A7BB7...	522CC...	7/7/2007 4:09:...	7/2/2
<input type="checkbox"/>	\$I30		1759		Mantooth32.E01/Partiti...	Index ...	4096 B	4096 B	A4A0E...	8F65C...	6C73A...	7/7/2007 5:57:...	7/2/2
<input type="checkbox"/>	\$I30		1785		Mantooth32.E01/Partiti...	Index ...	4096 B	4096 B	116F01...	DDDC8...	6F3D4...	3/5/2007 8:01:...	7/2/2

Loaded: 3,393 | Filtered: 3,393 | Total: 13,968 | Highlighted: 0 | Checked: 0

Show only file category graphics

+

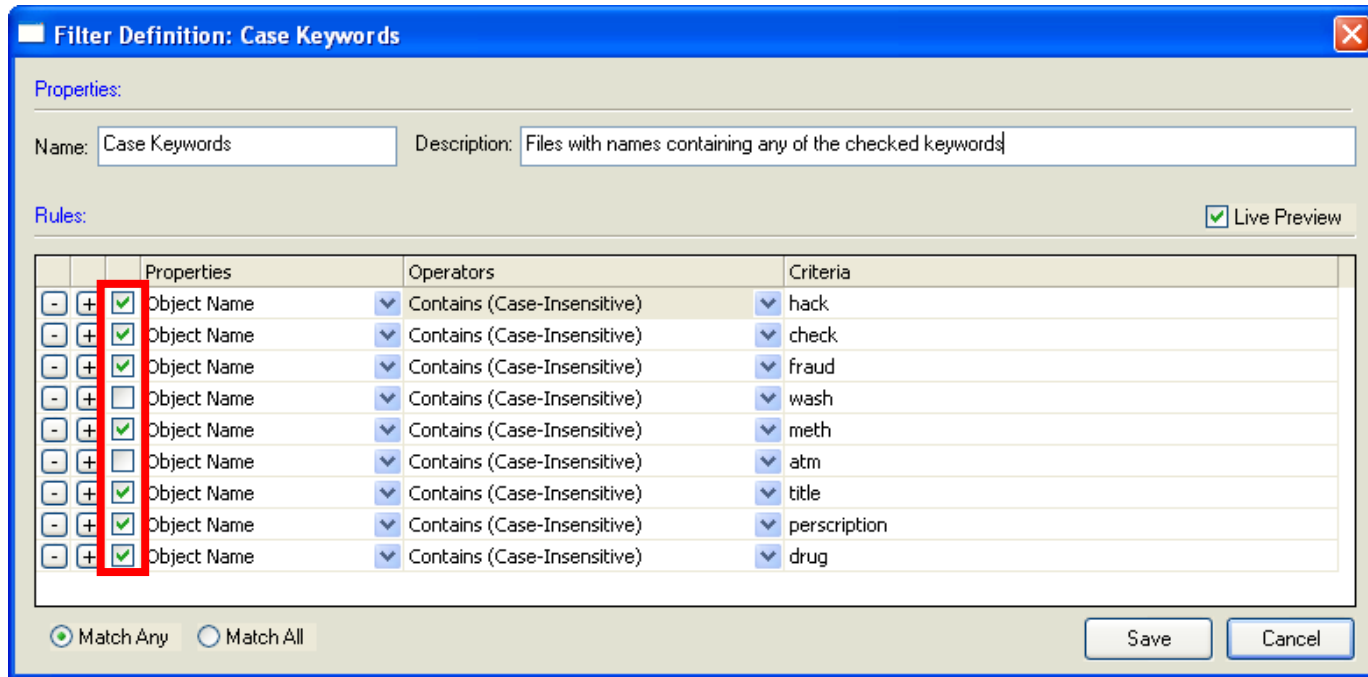
Match Owner SID ending in 1000

= **Broad Scope**

+

***Match Any Rule***

# Adding Rules



**Rules can be inactivated by un-checking them.**

# Nesting Filters

The screenshot shows a dialog box titled "Filter Definition: Temp" with a close button in the top right corner. The dialog is divided into two main sections: "Properties" and "Rules".

**Properties:**

- Name: Nested Filter
- Description: \wD\w! Look at that flexibility!

**Rules:**

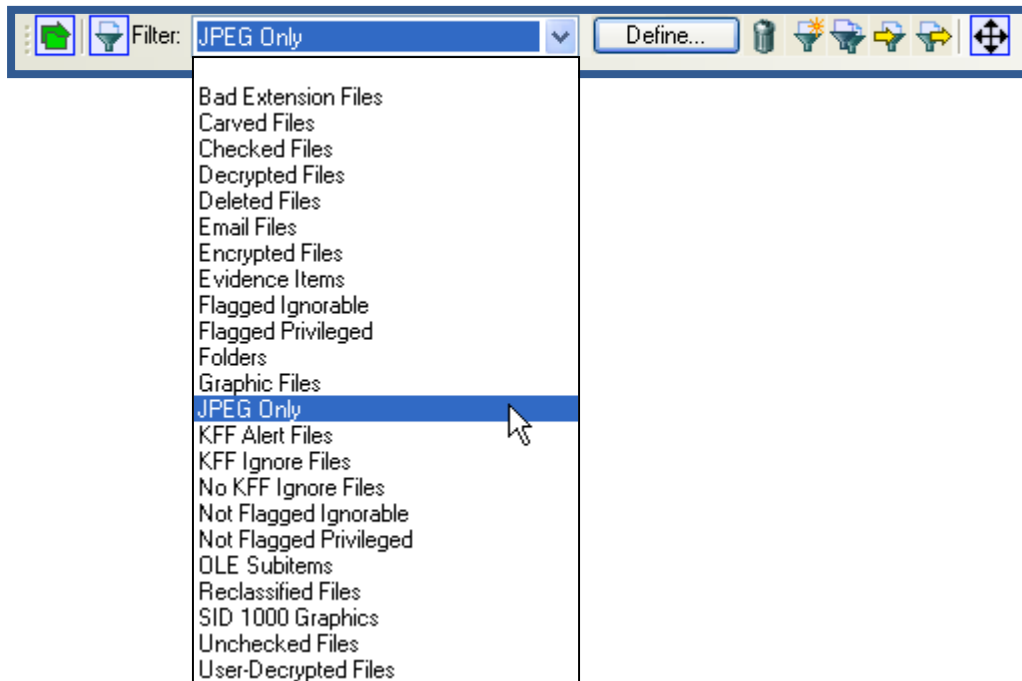
There is a checked checkbox for "Live Preview". Below it is a table with three columns: Properties, Operators, and Criteria.

		Properties	Operators	Criteria
-	+	<input checked="" type="checkbox"/> Filter	Matches	Case Keywords
-	+	<input checked="" type="checkbox"/> Filter	Matches	SID Ending in 1000 Only
-	+	<input checked="" type="checkbox"/> File Category	Is Not a Member of	[Graphics]

At the bottom of the dialog, there are two radio buttons: "Match Any" (unselected) and "Match All" (selected). To the right are "Save" and "Cancel" buttons.

**Filters can be nested for ultimate flexibility**

# Global Filters



Filters applied to the toolbar are global across all the tabs

# Tab Filters

The screenshot shows a file management application with a 'Case Overview' pane on the left and a 'File Content' pane on the right. The 'File Content' pane is displaying a document titled 'THIS WARRANT VOID AFTER AUGUST 24, 2006 Auditor of State of Arkansas'. The 'File List' pane at the bottom shows a list of files with columns for Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Access. A red box highlights the text 'Overview Tab Filter: Graphics by SID 1000' in the status bar.

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Access
08-15-05_arkansas_che...		1786	gif	Mantooth32.E01/Partiti...	GIF	95.00 KB	94.75 KB	AA8B0...	92E276...	C6B2C...	3/5/2007 7:52:...	7/13/
5273501.gif		1585	gif	Mantooth32.E01/Partiti...	GIF	22.00 KB	21.80 KB	9638B...	BBC23...	2AE88...	7/7/2007 6:38:...	7/7/2
5273501.gif		1598	gif	Mantooth32.E01/Partiti...	GIF	22.00 KB	21.80 KB	9638B...	BBC23...	2AE88...	4/12/2007 7:56:...	7/13/
67chev.jpg		1783	jpg	Mantooth32.E01/Partiti...	JPEG	67.00 KB	66.62 KB	7A623...	4D8A7...	41BE56...	6/21/2007 5:18:...	7/13/
81064B.gif		1787	gif	Mantooth32.E01/Partiti...	GIF	49.50 KB	49.08 KB	BEC05...	D5A27...	D0047...	3/5/2007 7:52:...	3/5/2
91064B.gif		1788	gif	Mantooth32.E01/Partiti...	GIF	21.00 KB	20.51 KB	3B594B...	A911C...	5305C...	3/5/2007 7:52:...	3/5/2
AdobeCMapFnt08.lst		2140	lst	Mantooth32.E01/Partiti...	Postscript	512 B	508 B	2FC44...	4A77B...	4A841...	7/7/2007 5:57:...	7/7/2
AdobeSysFnt08.lst		2141	lst	Mantooth32.E01/Partiti...	Postscript	67.00 KB	66.57 KB	A8561...	8C020...	96C96...	7/7/2007 5:57:...	7/7/2
Andromeda Galaxy M31...		1641	jpg	Mantooth32.E01/Partiti...	JPEG	23.50 KB	23.00 KB	9D2FB...	2AB0D...	C94BF...	7/14/2007 1:04:...	7/13/
Ape_20shoot.gif		1586	gif	Mantooth32.E01/Partiti...	GIF	187.0 KB	186.6 KB	752AA...	4C888...	B3BEC...	7/12/2007 6:49:...	9/26/
Apple_guy.gif		1600	gif	Mantooth32.E01/Partiti...	GIF	8704 B	8483 B	FA79F...	A3B07...	872482...	4/12/2007 7:56:...	7/13/
Autumn Leaves.jpg		1642	jpg	Mantooth32.E01/Partiti...	JPEG E...	270.0 KB	269.7 KB	EA649...	D85F6...	44CBC...	7/14/2007 1:04:...	7/13/
Bears.jpg		2091	jpg	Mantooth32.E01/Partiti...	JPEG E...	1536 B	1074 B	40074...	9C1C0...	9E3114...	7/7/2007 5:52:...	7/7/2
beer.gif		1601	gif	Mantooth32.E01/Partiti...	GIF	7168 B	6892 B	D669C...	11FFC...	9C3DB...	4/12/2007 7:56:...	7/13/

Loaded: 87 | Filtered: 87 | Total: 13,968 | Highlighted: 1 | Checked: 0

Overview Tab Filter: Graphics by SID 1000

A filter applied as a tab filter applies to ONLY that tab!

# Using Filters

The screenshot shows a forensic software interface with a menu bar (File, Edit, View, Evidence, Filter, Tools, Help) and a toolbar. A dropdown menu for filters is open, showing '- unfiltered -' selected. Below the toolbar are tabs for 'Explore', 'Overview', 'Email', 'Graphics', 'Bookmarks', 'Live Search', and 'Index Search'. The 'Graphics' tab is active, displaying a grid of image thumbnails. The first four thumbnails are labeled with file names: '\$R2M7A26.jpg', '\$R9HZOZ0.jpg', '\$RJQVPHB.jpg', and '\$RKY3FVP.gif'. The '\$RKY3FVP.gif' thumbnail is highlighted with a blue border. Below the thumbnails is a status bar showing 'Loaded: 2,854', 'Filtered: 2,854', 'Total: 13,968', 'Highlighted: 1', and 'Checked: 0'. The main window is divided into 'Evidence Items' and 'File Content' sections. The 'Evidence Items' section shows a tree view of the file system. The 'File Content' section displays the content of the selected file, which is a GIF image. The status bar at the bottom of the window shows 'Loaded: 2,854', 'Filtered: 2,854', 'Total: 13,968', 'Highlighted: 1', and 'Checked: 0'. A tooltip is visible over the status bar, displaying 'Graphics Tab Filter: Graphic Files'.

Filter: - unfiltered -

Explore Overview Email Graphics Bookmarks Live Search Index Search

Thumbnails

Loaded: 2,854 Filtered: 2,854 Total: 13,968 Highlighted: 1 Checked: 0 Show Tooltip

Evidence Items File Content

Hex Text Filtered Natural

File List

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Acces
\$R2M7A26.jpg		1246	jpg	Mantooth32.E01/Partiti...	JPEG	14.00 KB	13.82 KB	489E96...	870A9...	92D29...	7/26/2007 6:27...	7/26/
\$R9HZOZ0.jpg		1248	jpg	Mantooth32.E01/Partiti...	JPEG	6656 B	6468 B	6FB3C...	65B5D...	A0432...	7/26/2007 6:27...	7/26/
\$RJQVPHB.jpg		1251	jpg	Mantooth32.E01/Partiti...	JPEG	11.50 KB	11.30 KB	395FE2...	F98320...	B4FB9E...	7/26/2007 6:27...	7/26/
\$RKY3FVP.gif		1252	gif	Mantooth32.E01/Partiti...	GIF	7168 B	6798 B	5733C...	04BF35...	12BEA...	7/26/2007 6:27...	7/26/

Loaded: 2,854 Filtered: 2,854 Total: 13,968 Highlighted: 1 Checked: 0

Graphics Tab Filter: Graphic Files

Mantooth32.E01/Partition 1/MANTOOTH [NTFS]/[root]/\$Recycle.Bin/S-1-5-21-3166329-3263506726-1320359247-1000/\$RKY3FVP.gif

Tab filters can be used with global filters

# Using Filters

The screenshot shows a forensic software interface with a global filter set to "SID ending in 1000" and a tab filter set to "Graphic Files". The interface includes a menu bar, a toolbar, a thumbnails view, a file list, and a file content viewer.

**Global Filter:** Filter: SID ending in 1000

**Tab Filter:** Graphics Tab Filter: Graphic Files

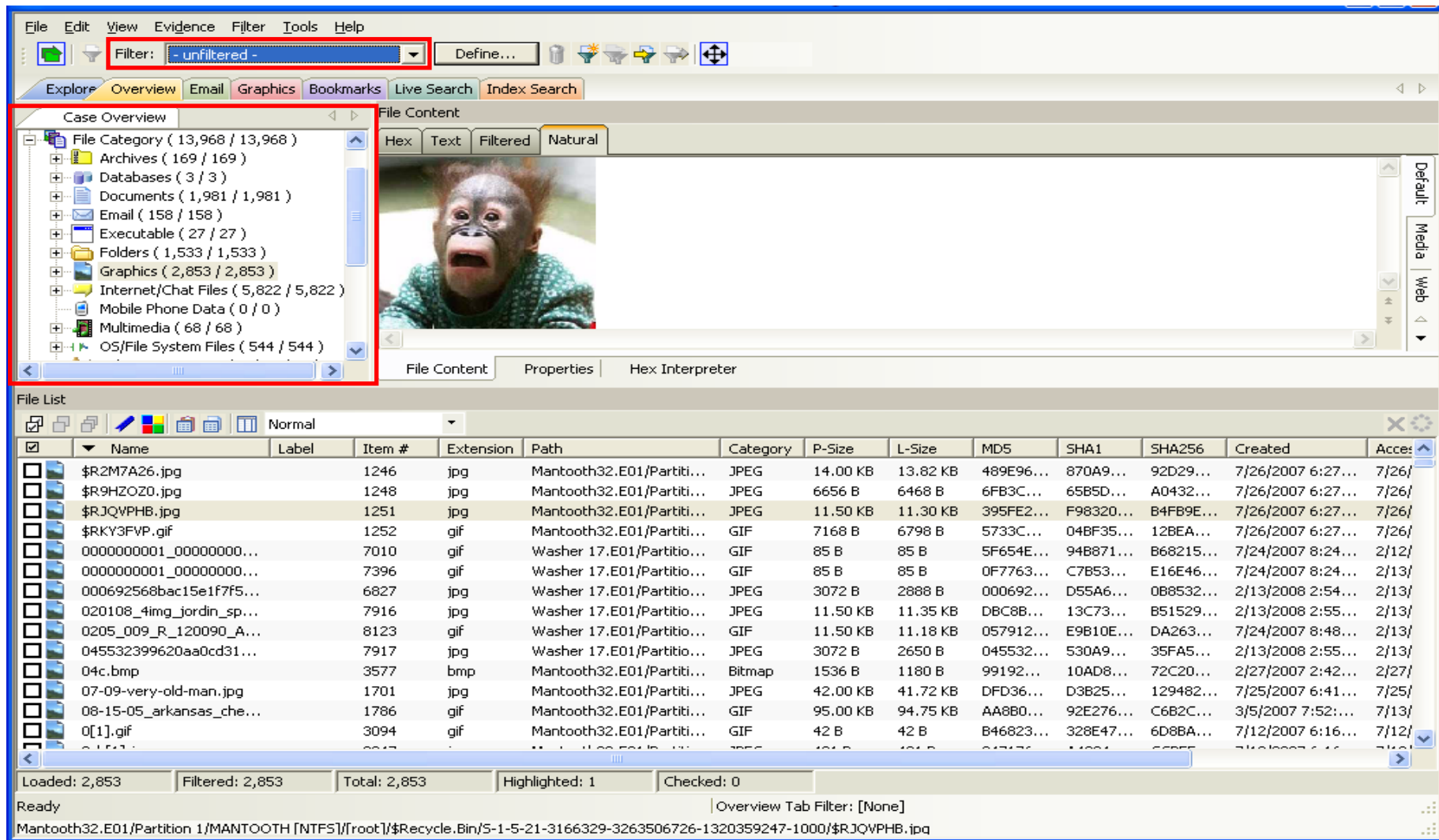
**File List:**

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Acces
AdobeCMapFnt08.lst		2140	lst	Mantooth32.E01/Partiti...	Postscript	512 B	508 B	2FC44...	4A77B...	4A841...	7/7/2007 5:57:...	7/7/2
AdobeSysFnt08.lst		2141	lst	Mantooth32.E01/Partiti...	Postscript	67.00 KB	66.57 KB	A8561...	8C020...	96C96...	7/7/2007 5:57:...	7/7/2
Andromeda Galaxy M31...		1641	jpg	Mantooth32.E01/Partiti...	JPEG	23.50 KB	23.00 KB	9D2FB...	2AB0D...	C94BF...	7/14/2007 1:04...	7/13/
Ape_20shoot.gif		1586	gif	Mantooth32.E01/Partiti...	GIF	187.0 KB	186.6 KB	752AA...	4C8B8...	B3BEC...	7/12/2007 6:49...	9/26/

Tab filters can be used with global filters



# Using Filters



The screenshot displays a file analysis application interface. At the top, a menu bar includes 'File', 'Edit', 'View', 'Evidence', 'Filter', 'Tools', and 'Help'. Below the menu, a toolbar contains a 'Filter:' dropdown menu set to '- unfiltered -', a 'Define...' button, and several icons. The main window is divided into several panes. On the left, a 'Case Overview' pane shows a tree view of file categories: File Category (13,968 / 13,968), Archives (169 / 169), Databases (3 / 3), Documents (1,981 / 1,981), Email (158 / 158), Executable (27 / 27), Folders (1,533 / 1,533), Graphics (2,853 / 2,853), Internet/Chat Files (5,822 / 5,822), Mobile Phone Data (0 / 0), Multimedia (68 / 68), and OS/File System Files (544 / 544). The 'Graphics' category is highlighted. The main pane shows 'File Content' with tabs for 'Hex', 'Text', 'Filtered', and 'Natural'. A preview image of a baby orangutan is displayed. Below the main pane is a 'File List' table with columns: Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Access. The table lists various files, including images and executables. At the bottom, a status bar shows 'Loaded: 2,853', 'Filtered: 2,853', 'Total: 2,853', 'Highlighted: 1', and 'Checked: 0'. The 'Overview Tab Filter: [None]' is also visible.

Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Access
\$R2M7A26.jpg		1246	jpg	Mantooth32.E01/Partiti...	JPEG	14.00 KB	13.82 KB	489E96...	870A9...	92D29...	7/26/2007 6:27...	7/26/
\$R9HZOZ0.jpg		1248	jpg	Mantooth32.E01/Partiti...	JPEG	6656 B	6468 B	6FB3C...	65B5D...	A0432...	7/26/2007 6:27...	7/26/
\$RJQVPHB.jpg		1251	jpg	Mantooth32.E01/Partiti...	JPEG	11.50 KB	11.30 KB	395FE2...	F98320...	B4FB9E...	7/26/2007 6:27...	7/26/
\$RKY3FVP.gif		1252	gif	Mantooth32.E01/Partiti...	GIF	7168 B	6798 B	5733C...	04BF35...	12BEA...	7/26/2007 6:27...	7/26/
0000000001_00000000...		7010	gif	Washer 17.E01/Partitio...	GIF	85 B	85 B	5F654E...	94B871...	B68215...	7/24/2007 8:24...	2/12/
0000000001_00000000...		7396	gif	Washer 17.E01/Partitio...	GIF	85 B	85 B	0F7763...	C7B53...	E16E46...	7/24/2007 8:24...	2/13/
000692568bac15e1f7f5...		6827	jpg	Washer 17.E01/Partitio...	JPEG	3072 B	2888 B	000692...	D55A6...	0B8532...	2/13/2008 2:54...	2/13/
020108_4img_jordin_sp...		7916	jpg	Washer 17.E01/Partitio...	JPEG	11.50 KB	11.35 KB	DBC8B...	13C73...	B51529...	2/13/2008 2:55...	2/13/
0205_009_R_120090_A...		8123	gif	Washer 17.E01/Partitio...	GIF	11.50 KB	11.18 KB	057912...	E9B10E...	DA263...	7/24/2007 8:48...	2/13/
045532399620aa0cd31...		7917	jpg	Washer 17.E01/Partitio...	JPEG	3072 B	2650 B	045532...	530A9...	35FA5...	2/13/2008 2:55...	2/13/
04c.bmp		3577	bmp	Mantooth32.E01/Partiti...	Bitmap	1536 B	1180 B	99192...	10AD8...	72C20...	2/27/2007 2:42...	2/27/
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/
08-15-05_arkansas_che...		1786	gif	Mantooth32.E01/Partiti...	GIF	95.00 KB	94.75 KB	AA8B0...	92E276...	C6B2C...	3/5/2007 7:52:...	7/13/
0[1].gif		3094	gif	Mantooth32.E01/Partiti...	GIF	42 B	42 B	B46823...	328E47...	6D8BA...	7/12/2007 6:16...	7/12/

**Filters can be used in conjunction with containers**

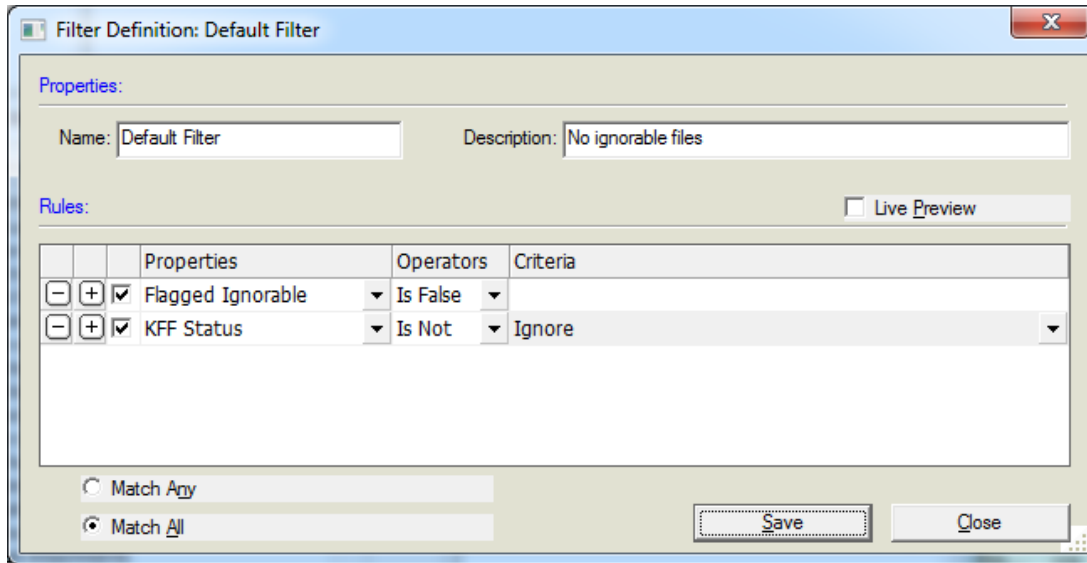
# Using Filters

The screenshot displays a forensic software interface with a 'Filter' dropdown menu set to 'Email Attachments'. The 'Case Overview' pane on the left shows a tree view of file categories, with 'Email (0 / 158)' highlighted. The main 'File Content' pane shows a preview of a document. The 'File List' pane at the bottom displays a table of files with columns for Name, Label, Item #, Extension, Path, Category, P-Size, L-Size, MD5, SHA1, SHA256, Created, and Access. The table shows a list of files, including 'Camera.bmp' and 'Cover Plate.bmp', which are highlighted in blue. The status bar at the bottom indicates 'Loaded: 172', 'Filtered: 172', 'Total: 2,853', 'Highlighted: 1', and 'Checked: 0'.

File List	Name	Label	Item #	Extension	Path	Category	P-Size	L-Size	MD5	SHA1	SHA256	Created	Access
<input type="checkbox"/>	aboutIconRollover.jpg		15504	jpg	Washer 17.E01/Partitio...	JPEG E...	n/a	17.65 KB	72799...	C792A...	C3F90...	n/a	n/a
<input type="checkbox"/>	AMEX.jpg		15484	jpg	Washer 17.E01/Partitio...	JPEG	n/a	7594 B	72E589...	8F0176...	C8C03...	n/a	n/a
<input type="checkbox"/>	AMEXGR.jpg		15485	jpg	Washer 17.E01/Partitio...	JPEG	n/a	6677 B	8A88D...	B22372...	06D3F...	n/a	n/a
<input type="checkbox"/>	BEACH.jpg		15486	jpg	Washer 17.E01/Partitio...	JPEG	n/a	37.50 KB	77CED...	509D7...	B60CC...	n/a	n/a
<input type="checkbox"/>	BEACH_VALID.jpg		15487	jpg	Washer 17.E01/Partitio...	JPEG	n/a	40.75 KB	B6806E...	8EFC0...	B5CC7...	n/a	n/a
<input type="checkbox"/>	Camera.bmp		4365	bmp	Mantooth32.E01/Partiti...	Bitmap	501.2 KB	366.2 KB	C708C...	5C030...	FD292...	n/a	n/a
<input type="checkbox"/>	Camera.bmp		4385	bmp	Mantooth32.E01/Partiti...	Bitmap	501.2 KB	366.2 KB	C708C...	5C030...	FD292...	n/a	n/a
<input type="checkbox"/>	Camera.bmp		15217	bmp	Washer 17.E01/Partitio...	Bitmap	501.2 KB	366.2 KB	C708C...	5C030...	FD292...	n/a	n/a
<input type="checkbox"/>	Cover Plate.bmp		4364	bmp	Mantooth32.E01/Partiti...	Bitmap	543.7 KB	397.3 KB	989D3...	6BB101...	66A56...	n/a	n/a
<input type="checkbox"/>	Cover Plate.bmp		4384	bmp	Mantooth32.E01/Partiti...	Bitmap	543.7 KB	397.3 KB	989D3...	6BB101...	66A56...	n/a	n/a
<input type="checkbox"/>	Cover Plate.bmp		15216	bmp	Washer 17.E01/Partitio...	Bitmap	543.7 KB	397.3 KB	989D3...	6BB101...	66A56...	n/a	n/a
<input type="checkbox"/>	DCI.jpg		15488	jpg	Washer 17.E01/Partitio...	JPEG	n/a	8889 B	AD365...	A8BF4...	F1BB64...	n/a	n/a
<input type="checkbox"/>	DCIGR.jpg		15489	jpg	Washer 17.E01/Partitio...	JPEG	n/a	8070 B	E18626...	2912F5...	9BCC8...	n/a	n/a
<input type="checkbox"/>	DCP_1415.JPG		15344	jpg	Washer 17.E01/Partitio...	JPEG E...	607.0 KB	443.6 KB	6A990...	4E7832...	32B234...	n/a	n/a

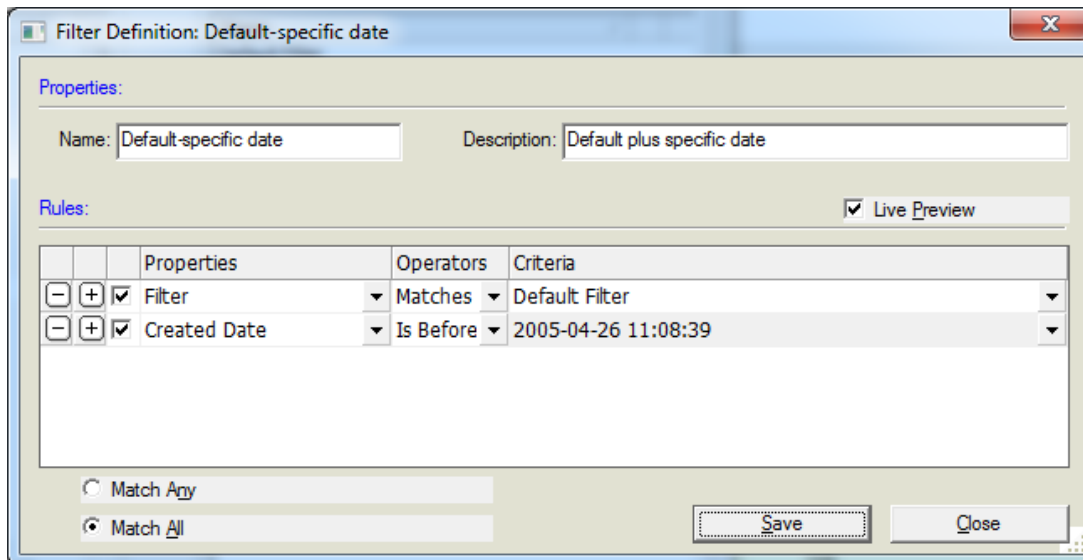
**Filters can be used in conjunction with containers**

# Default Filter



Removes:

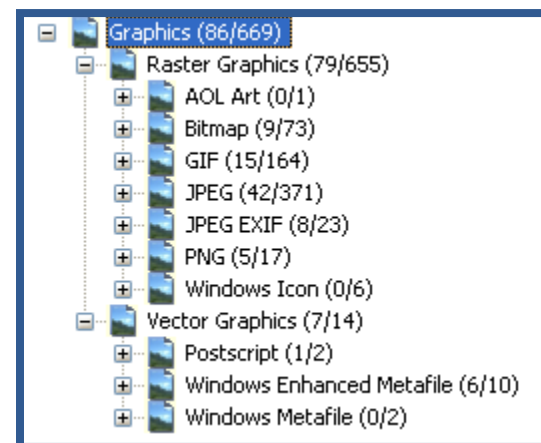
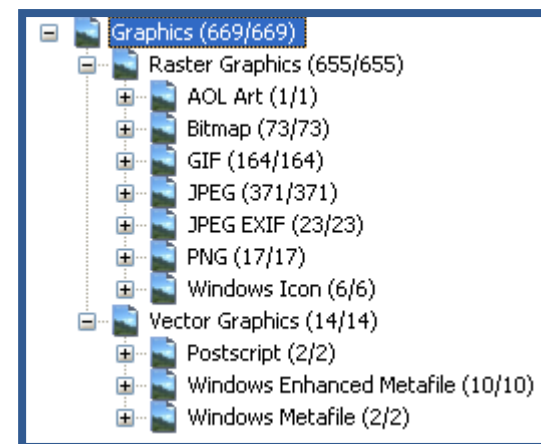
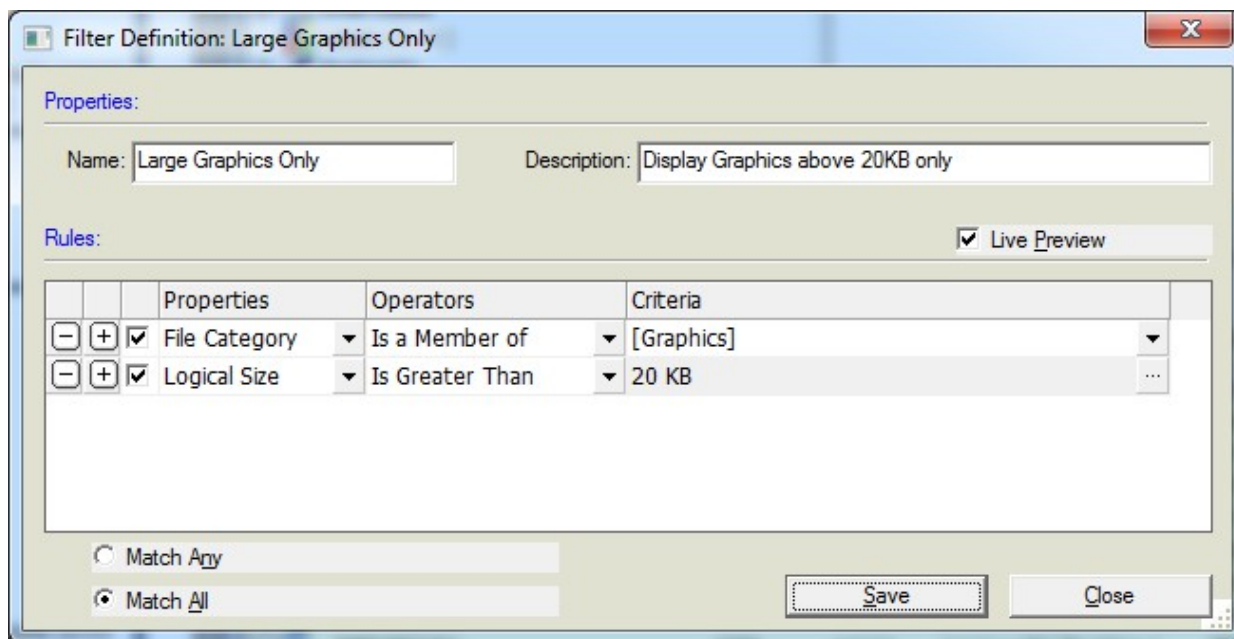
- Flagged Ignore
- KFF Ignorable



Use it as a  
starting point  
for other filters!

# Large Graphic Filter

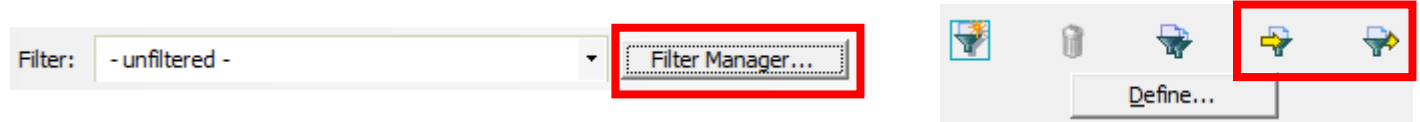
Used to eliminate small Internet graphics



# Importing and Exporting

Filter > New

OR

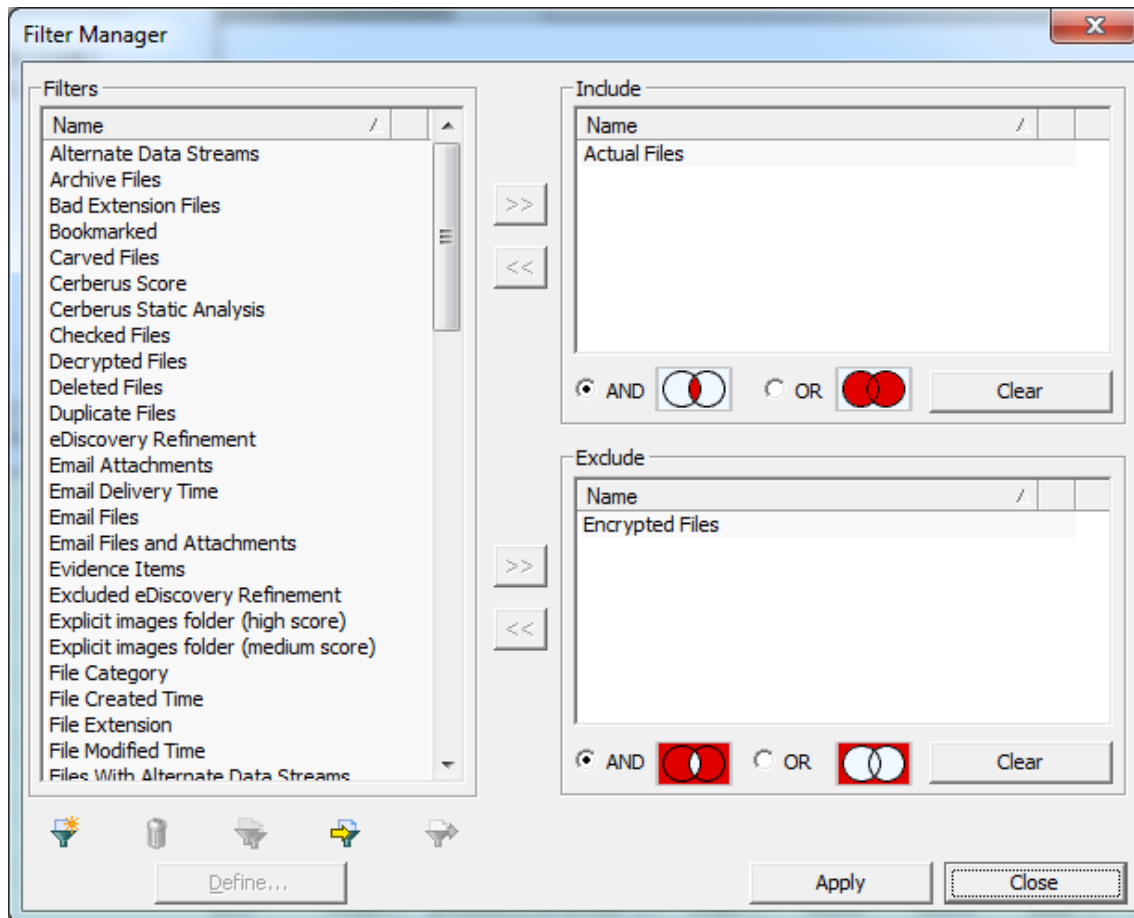


- Cross-case filters should be exported
- Results in an XML file
- Must be imported once for each case

# Filterer Manager

The Filter Manager allow multiple filters to be selected and applied concurrently. These are known as **Compound filters**.

In addition, the Filter Manager dialog allows you to either **include** by filter, or **exclude** by filter. You can also choose **AND/OR** options



# Video Tab

The Video Tab may have a to restrictive Tab Filter? Set it to Actual Files to show actual content!

AccessData Forensic Toolkit Version: 4.2.1.22 Database: localhost Case: precious2 -Education-

File Edit View Evidence Filter Tools Manage Help

Filter: -unfiltered- Filter Manager...

Explore Overview Email Graphics Video Bookmarks Live Search Index Search Volatile

Video Video Thumbnails

Multimedia (46 / 46)

login.swf

Loaded: 46 Filtered: 46 Total: 46 Highlighted: 1 Checked: 0 Total LSize: 2139 KB Show Tooltip

File List

Name	Label	Item #	Ext	Path
BD671779d01		1021	<missin...	precious.E01/Partition 1/The Precious [NTF...
C5BBA629d01		1026	<missin...	precious.E01/Partition 1/The Precious [NTF...
CD8D2990d01		1033	<missin...	precious.E01/Partition 1/The Precious [NTF...
CE488001d01		1034	<missin...	precious.E01/Partition 1/The Precious [NTF...
D512B2BFd01		1041	<missin...	precious.E01/Partition 1/The Precious [NTF...
DAD66F61d01		1043	<missin...	precious.E01/Partition 1/The Precious [NTF...
DB34CD8Cd01		1044	<missin...	precious.E01/Partition 1/The Precious [NTF...
DC441E10d01		1046	<missin...	precious.E01/Partition 1/The Precious [NTF...
DCC98A85d01		1047	<missin...	precious.E01/Partition 1/The Precious [NTF...
E056D4A0d01		1050	<missin...	precious.E01/Partition 1/The Precious [NTF...
EF569BACd01		1061	<missin...	precious.E01/Partition 1/The Precious [NTF...
F6572BE3d01		1068	<missin...	precious.E01/Partition 1/The Precious [NTF...
happy.mpeg		2097	mpeg	precious.E01/Partition 1/The Precious [NTF...
login.swf		2633	swf	precious.E01/Partition 1/The Precious [NTF...
Qirien - The Lord of the ...		2070	mid	precious.E01/Partition 1/The Precious [NTF...
Qirien - To Isengard.mid		2071	mid	precious.E01/Partition 1/The Precious [NTF...
sndrec.wav		2498	wav	precious.E01/Partition 1/The Precious [NTF...
sndrec.wav		2730	wav	precious.E01/Partition 1/The Precious [NTF...

File Content

Hex Text Filtered Natural

Paused 00:17

File Content Properties Hex Interpreter

precious.E01/Partition 1/The Precious [NTFS]/[root]/Documents and Settings/Frodo Baggins/My Documents/My Received Files/happy.mpeg

Ready

Video Tab Filter: Actual Files