

X-Ways Forensics

Quick Guide

X-Ways Software Technology AG
Carl-Diem-Str. 32
32257 Bünde
Germany

Web: <http://www.x-ways.net>

X-Ways Software Technology AG
Agrippastr. 37-39
50676 Köln
Germany

E-mail: mail@x-ways.com

Phone: +49-221-420 486 5

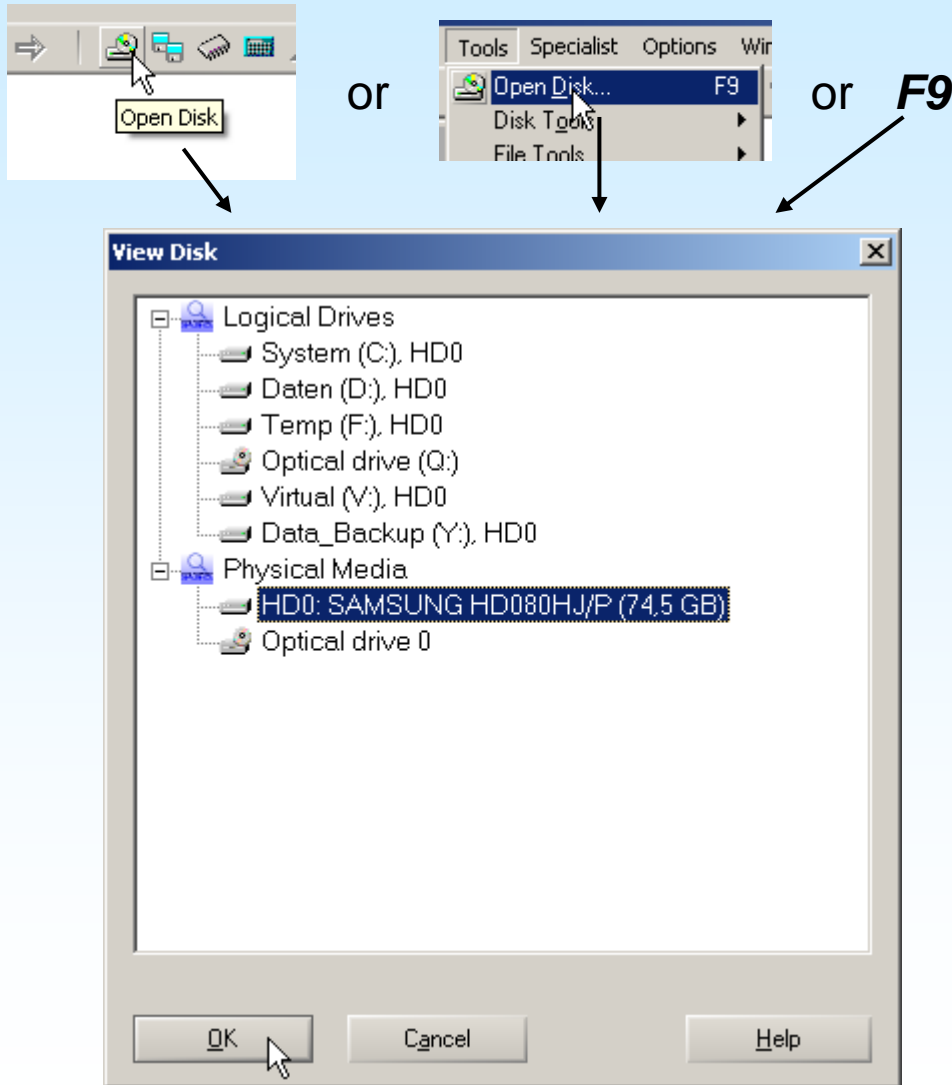
Based on v16.7. Please subscribe to the newsletter to stay informed of updates to the software.

All rights including but not limited to reproduction reserved.

Contents

1: Image Creation.....	3
2: Case Creation, Adding Images.....	6
3: Report Noteworthy Files.....	11
4: Filtering (Ex. Deleted JPEG Files).....	16
5: Refine Volume Snapshot.....	21
6: Office Metadata.....	23
7: Search (Ex. "John" and "Smith").....	27
8: Copying Files.....	31
9: Evidence File Container.....	33

1: Image Creation



Step 1: Open medium to image

Either click the "Open Disk" button in the tool bar or the menu command from the Tools menu or simply hit the F9 key to call the View Disk dialog.

You can select either full physical media or choose a logical drive letter.

1: Image Creation

(Optional) Step 1a: Open desired partition on the disk

The screenshot shows a disk partitioning interface for 'Hard disk 0'. The partitioning type is MBR. A table lists seven partitions. Partition 3 is selected and highlighted in blue. A red arrow points from the selected partition to a smaller window titled 'Hard disk 0 - Hard disk 0, Partition 3'. This window shows the contents of the selected partition, including folders like 'Pfad unbekannt', '(Stammverzeichnis)', 'RECYCLER', and 'temp'.

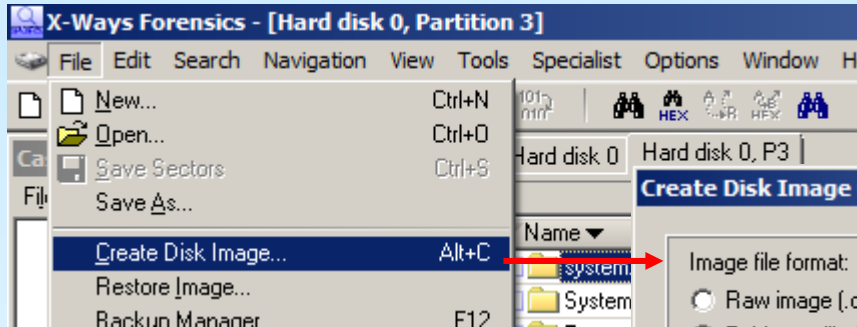
Name	Typ	Size	Created	Modified	Accessed	Attr.	1st sector
Partition 1		47,0 MB					63
Partition 2		17,6 GB					96390
Partition 3		19,5 GB					36965628
Partition 4		7,8 GB					77931378
Partition 5							
Partition 6							
Partition 7							

Hard disk 0 - Hard disk 0, Partition 3							
7 days ago							
Name	Typ	Size	Created	Modified	Accessed	Attr.	
<input type="checkbox"/> Pfad unbekannt							
<input type="checkbox"/> (Stammverzeichnis)		8,2 KB	03.01.2006 10:03:38	30.05.2007 10:28:21	30.05.2007 10:28:21	SH	
<input type="checkbox"/> RECYCLER		328 bytes	03.01.2006 11:25:56	03.01.2006 11:25:56	30.05.2007 10:28:05	SH	
<input type="checkbox"/> temp		4,0 KB	26.09.2006 10:17:43	19.12.2006 11:13:13	30.05.2007 10:28:05		

Select a particular partition and open it. For images of the complete (physical) medium, this is not necessary, of course.

1: Image Creation

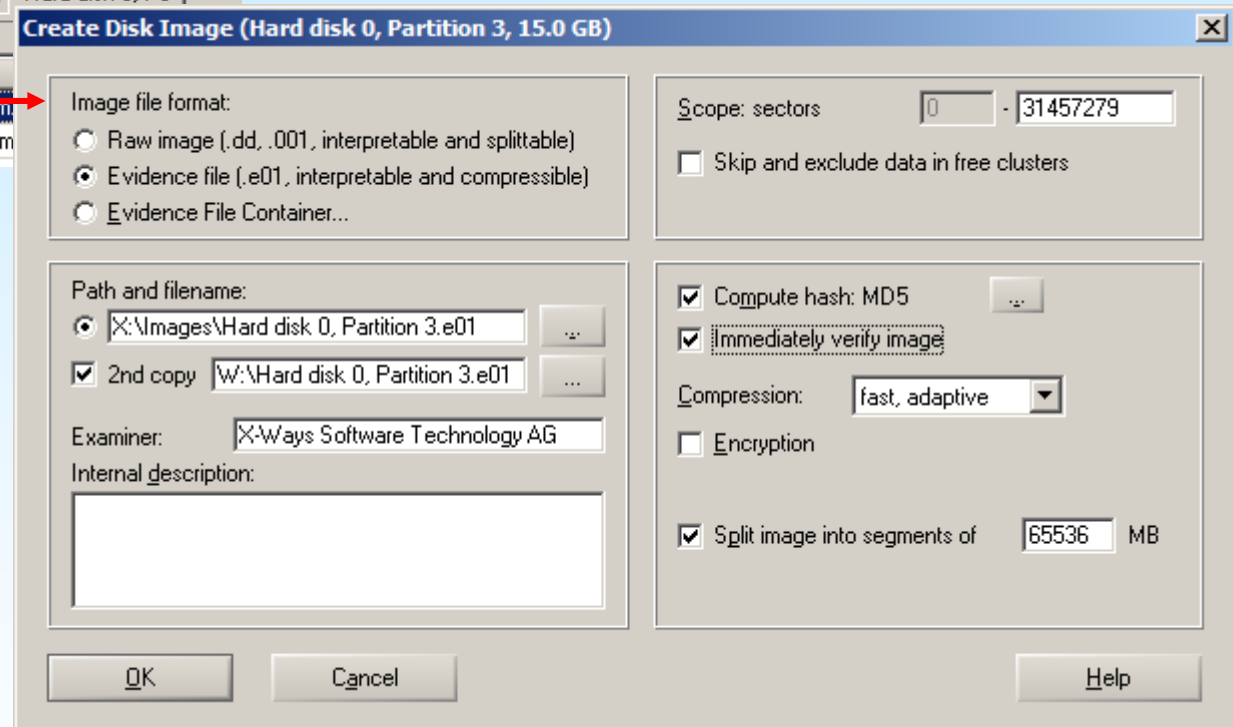
Step 2: Create the disk image



The command always applies to currently active tab within X-Ways Forensics.

Create 2 copies simultaneously if required!

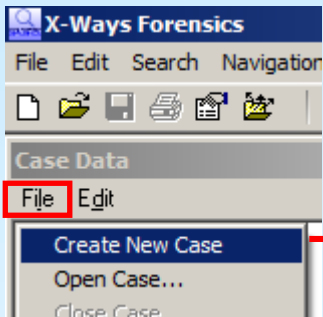
Hash computation allows for later verification of image integrity.



Splitting images helps if you need to store them on CD-Rs or DVD+/-Rs or FAT32 file systems.

2: Case Creation, Adding Images

Step 1: Create New Case



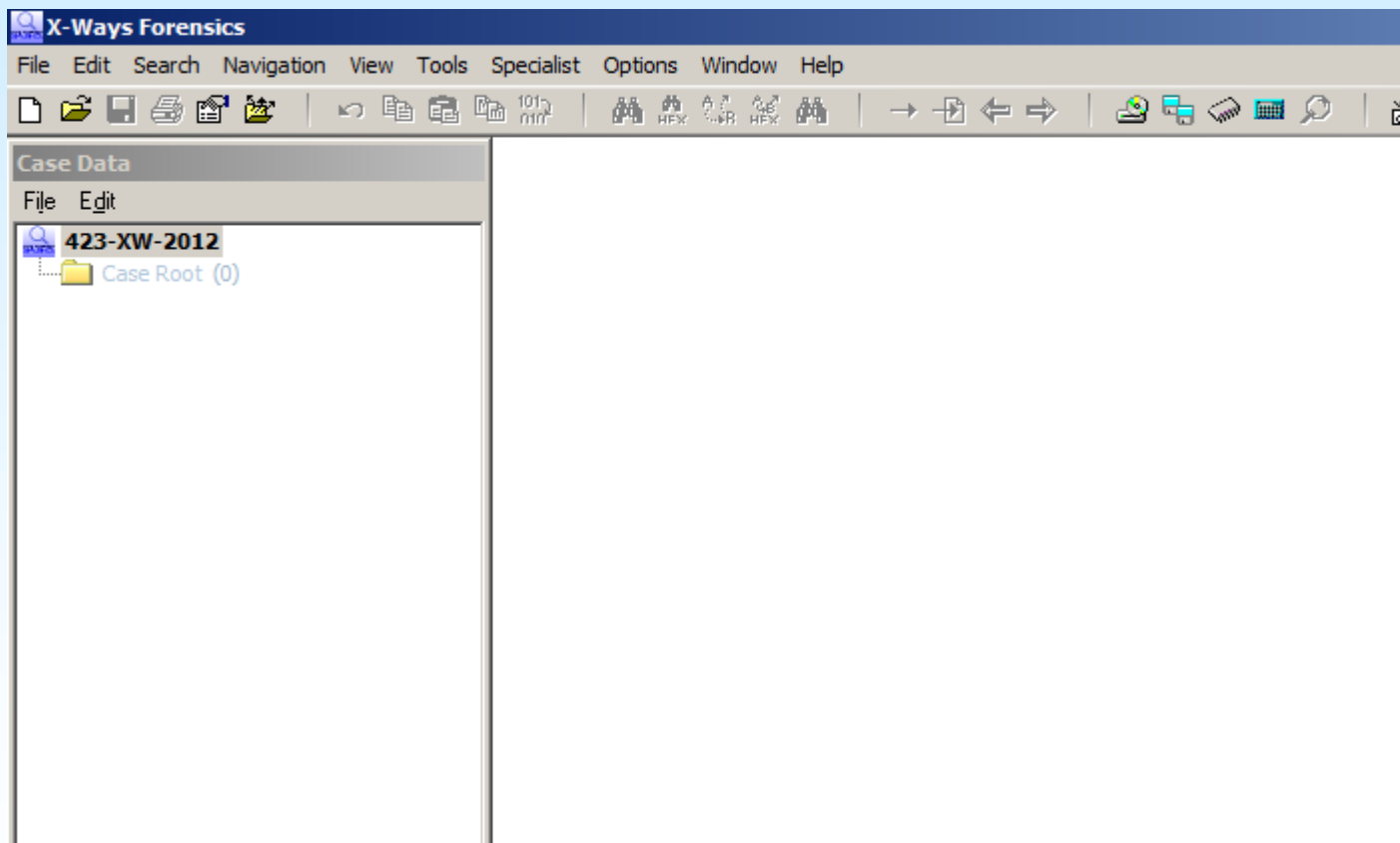
Select the case data window's "Create New Case" command and fill in the resulting dialog:

The 'Properties' dialog box is shown with the following fields and options:

- Case title/number: 432-XW-2012
- Creation time: 17.10.2012 17:43:07
- Directory: E:\cases
- Description: System seized in connection with the investigation against John Doe
- Examiner, organization, address: Det. John Milton LAPD
- Log general activity
- Log Recover/Copy command
- Include screenshots in log
- Default to evidence object folders for output
- Log: 0 B
- Delete... msglog.txt... copylog.html...
- Code pages suitable for processing this case:
 - *** 1252 ANSI - Latin I ***
 - *** 1252 ANSI - Latin I ***
- Report (Options)... Display time zone...
- Auto save interval in min. 10
- Add disk partitions to the case automatically as well
- No. of case file backups: 5
- Protect case file against opening³
- RVS: Protect against duplicates of crasher files

2: Case Creation, Adding Images

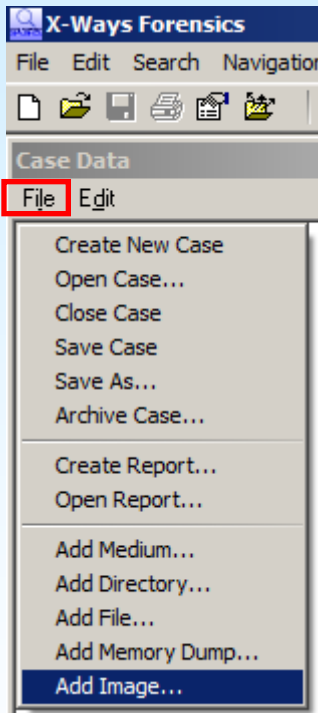
Once you select OK, a new case will be created and opened in X-Ways Forensics:



Images need to be added to work with.

2: Case Creation, Adding Images

Step 2: Adding image files as evidence objects



In the Case Data window's **File** menu, there are commands to add evidence objects to the case. Select **Add Image...**

In the resulting Open File dialog, you may select raw (.dd/.001) images, evidence files (.e01) or virtual hard disks (.vhd or .vmdk), which will then be interpreted.

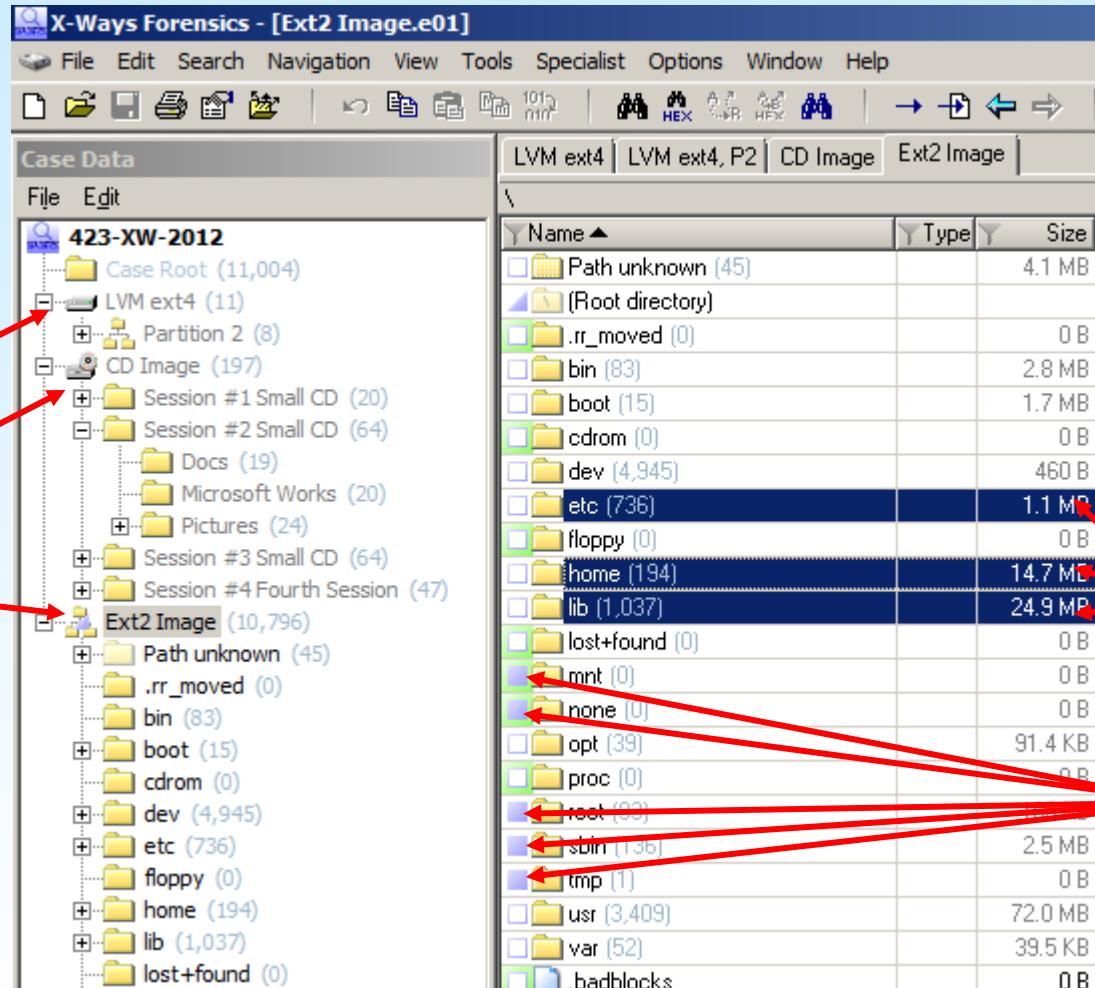
2: Case Creation, Adding Images

Images of:

Physical media

Optical media

Partitions/
Volumes

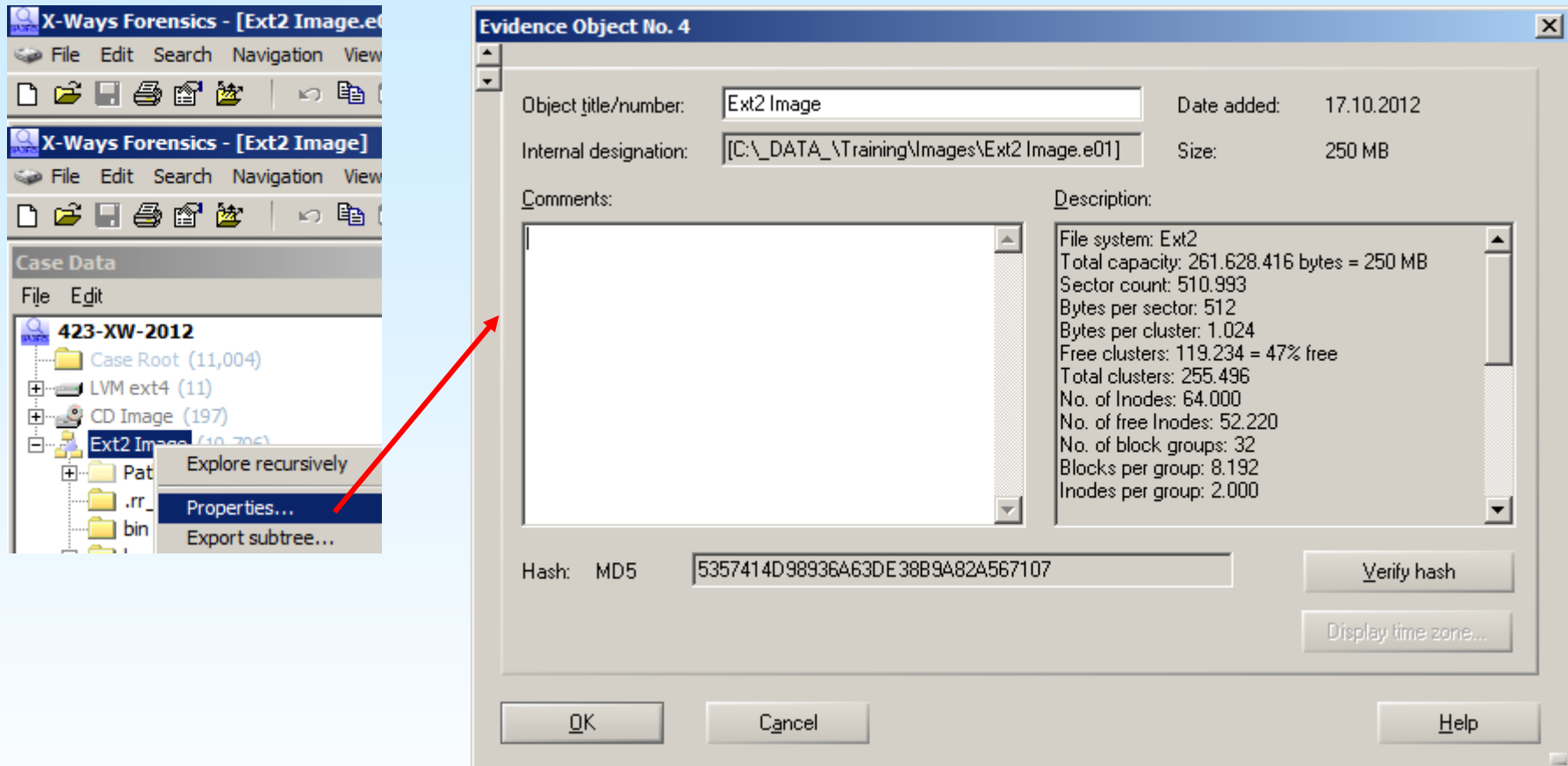


"Selected"

"Tagged"

Segmented images will automatically be recognized if they have identical names and are numbered in their extensions: .e01, .e02,... or .dd, .002,... or .001, .002,...

2: Case Creation, Adding Images

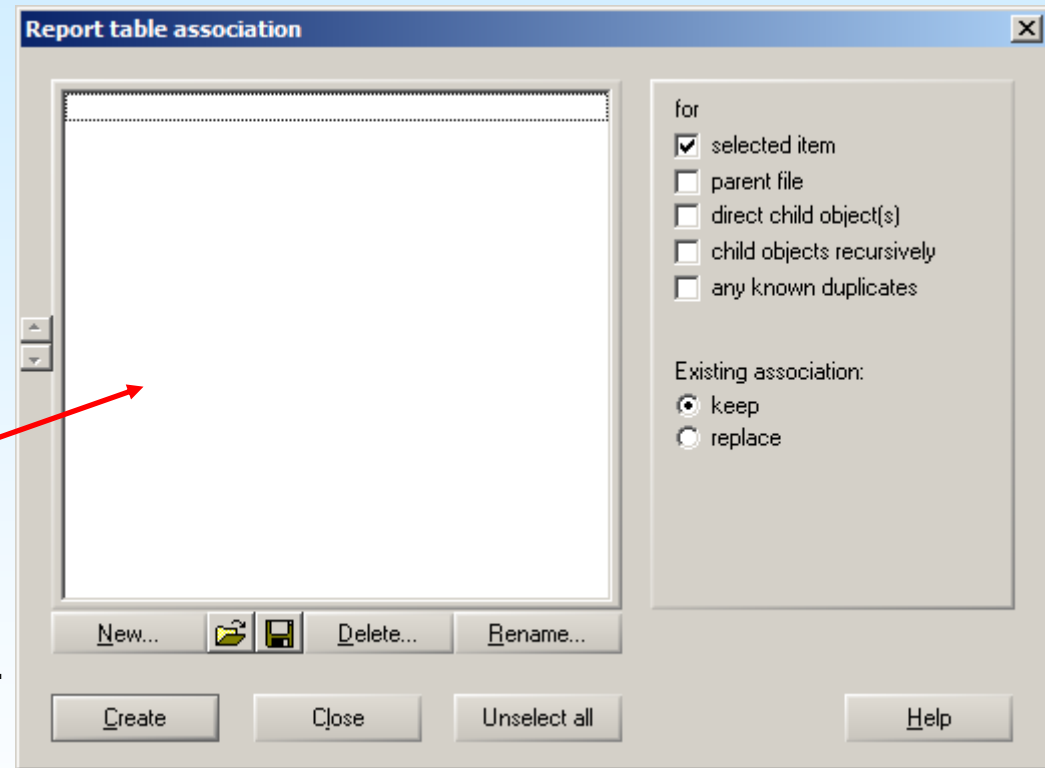
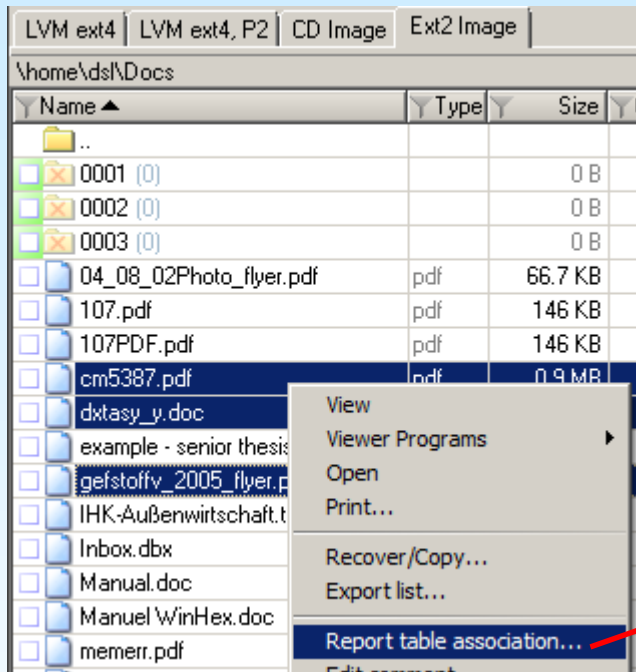


Properties of an image can be accessed via the context menu in the Case Data window.

There you can have X-Ways Forensics verify the image's hash value as well.

3: Report Noteworthy Files

Step 1: Report table association



Select the files and directories in question and right-click the selection. In the context menu, use “Report table association...”, which will bring up the list of currently available report tables.

At first use of this functionality no report tables exist yet – they must first be created.

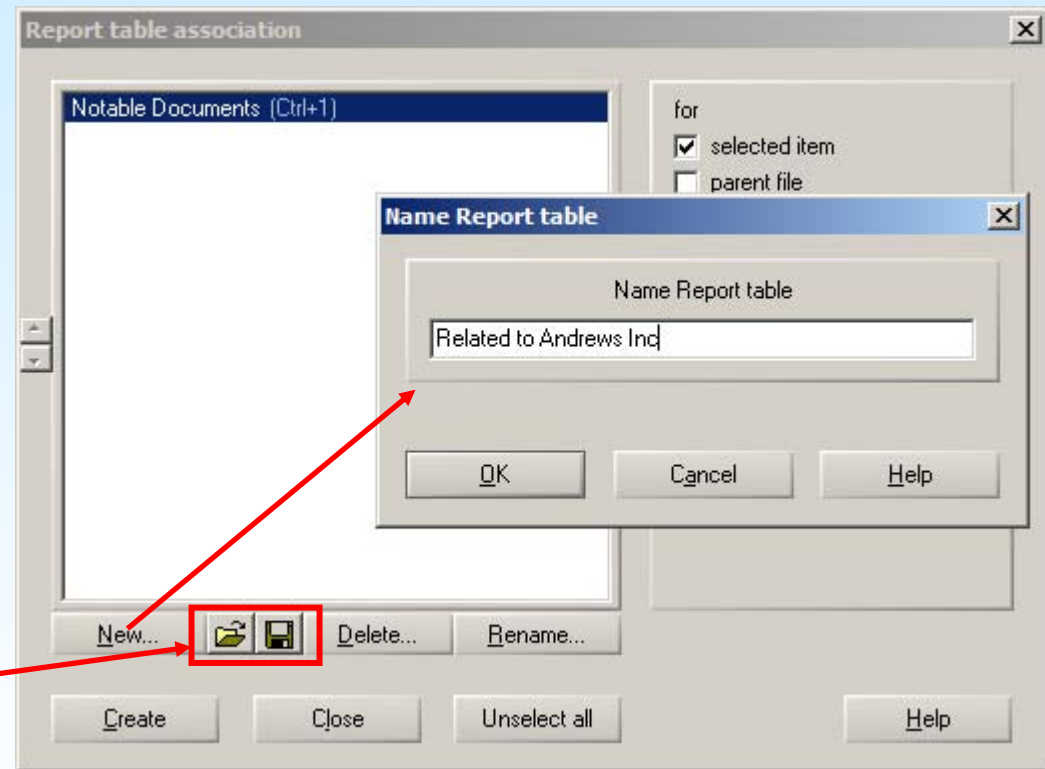
3: Report Noteworthy Files

Step 1a: New report table

(Step only required if the desired report table does not yet exist)

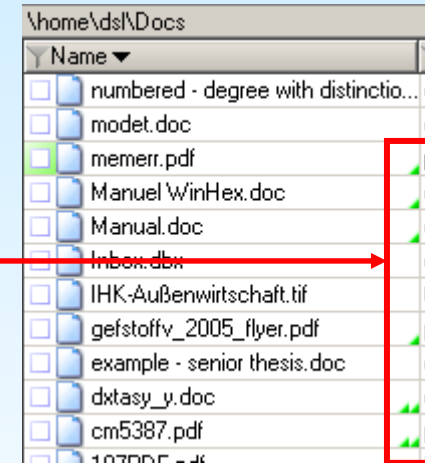
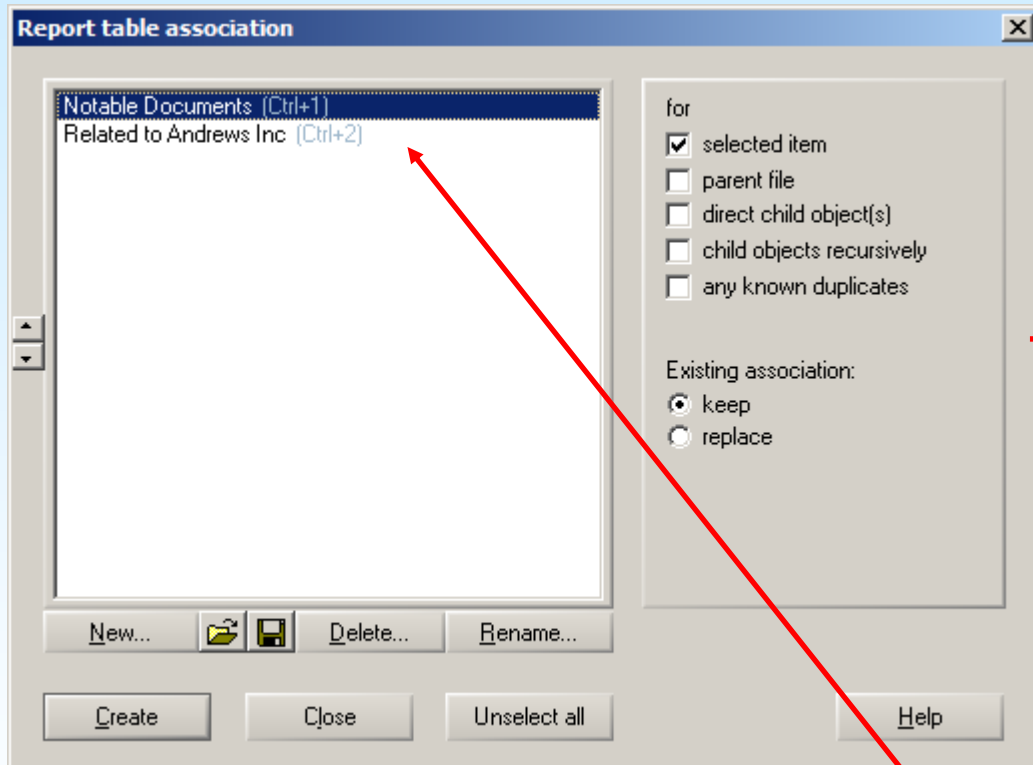
Create as many tables as you need – the list can be added to at any time.

Alternatively, you can save a list of report tables, once created, and simply load that list for the next case.



3: Report Noteworthy Files

Step 1b: Report table association



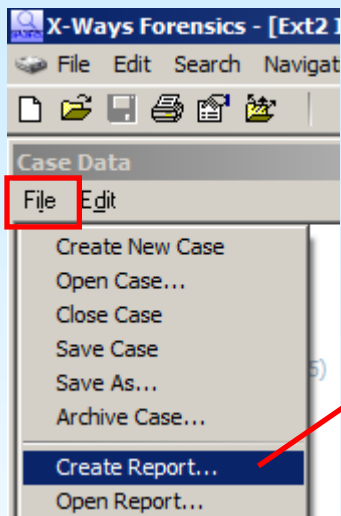
The green triangle identifies files presently in a report table (two triangles: two report tables)

Choose the required table and click *Create*, to add the previously selected files and directories to the report table.

Note the keyboard shortcuts (e.g. Ctrl+1), which allow adding items to report tables without using the context menu.

3: Report Noteworthy Files

Step 2: Create Report



Select the option “Make copy of files for inclusion in report...”. Ensure that “Include report tables” is checked. Also select the fields to output according to your preferences.

Report (Options)

Create basic report

Optional logo:
 ...

left center right

Optional report header:

left center right

Optional preface:

In selected evidence objects ...

Output activity log
 Include times
 Include screenshots in log
 Font size:

Include report tables³

Notable Documents (8)
 Related to Andrews Inc (2)

New... Delete... Rename...

Sort files by evidence object and int. ID
 Order as they are currently listed in the case root

3 files per line Font size: 10
 Page break after x table rows for printing: 4
 Border width: 1 Cell padding: 3

Make copy of files for inclusion in report³
 Maximum filename length: 127

Rename .eml for viewing directly in browser
 Embed attachments in parent .eml file
 Embed pictures in HTML as inline code (Firefox)

Max. dimension of pictures: 250 × 185
 Max. number of pictures per HTML file: 500

Fields to output:

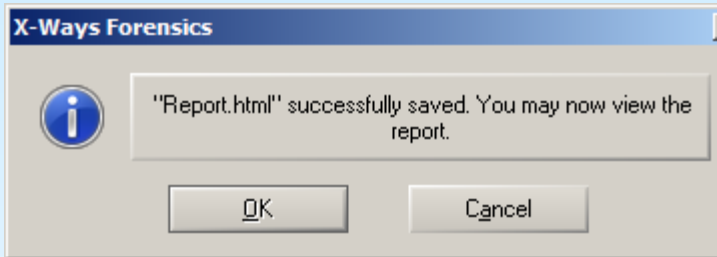
Name
Description
Ext.
Type
Type status
Type descr.
Category
Evidence object
Path
Parent name
Child objects
Sender
Recipients

Field names

Max. cell width: 250

3: Report Noteworthy Files

Step 2a: View Report



Clicking OK will call the HTML viewing application specified in Options | Viewer Programs... (none specified: default browser).

The report tables will be included with links for non-picture files while pictures will be embedded directly. (cf. scaling options at the report creation stage).

423-XW-2012

Creation time: 17.10.2012 16:30:43

Case file: E:\cases\423-XW-2012.xfc

Time zone UTC +00:00 London, Lisbon, Dublin

Report generated by X-Ways Forensics 16.7 SR-3

Description System seized in connection with the investigation against John Doe

Examiner, organization, address: Det. John Milton

LAPD

Evidence objects:

[Ext2 Image](#)

Notable Documents (8 items)

Name: **new-york-9400020.jpg**

Type: jpg

Evidence object: Ext2 Image

Path: \home\ds1\Pictures\0003

Size: 18.6 KB



Name: **Manuel WinHex.doc**

Type: doc

Evidence object: Ext2 Image

Path: \home\ds1\Docs

Size: 438 KB

[Link](#)

Name: **cm**

Type: pdf

Evidence

Path: \hor

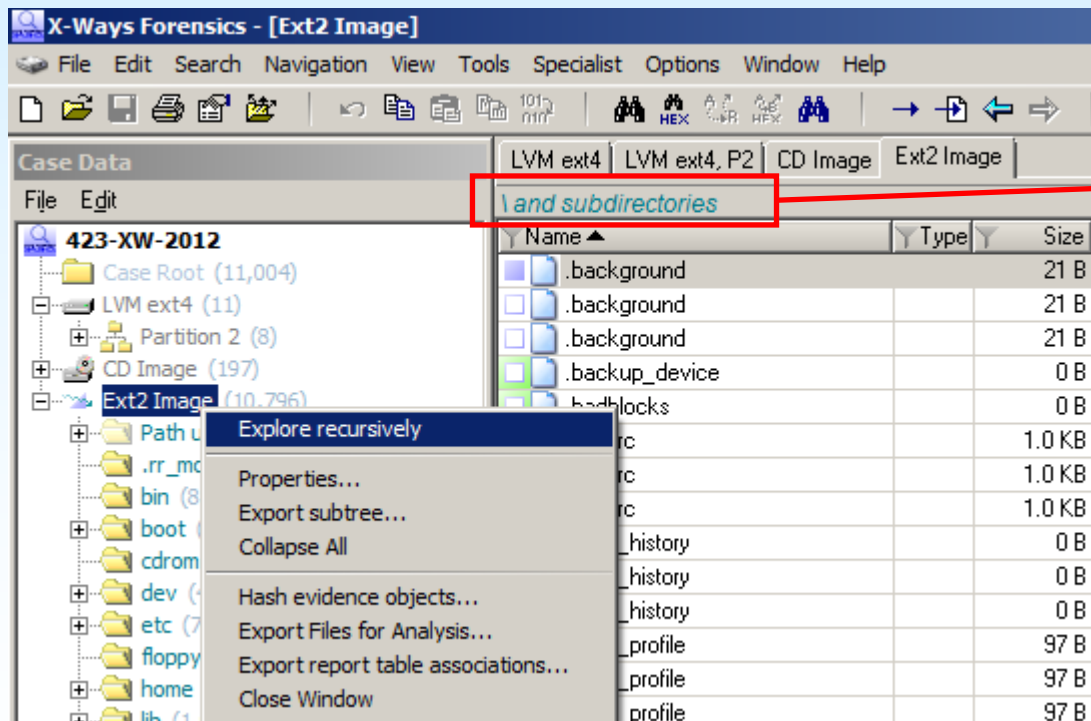
Size: 0.9 M

[Link](#)

4: Filtering (Ex. Deleted JPEG Files)

Step 1: Explore recursively

Right-click the volume in the directory tree and select “Explore recursively” from the context menu. This will generate a list of all files in all subdirectories.

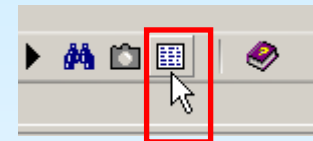
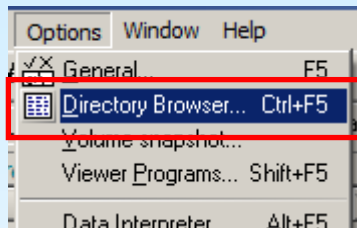


“and subdirectories” denotes recursive listings!

\ represents a partition's root directory

4: Filtering (Ex. Deleted JPEG Files)

Step 2: Open the directory browser options



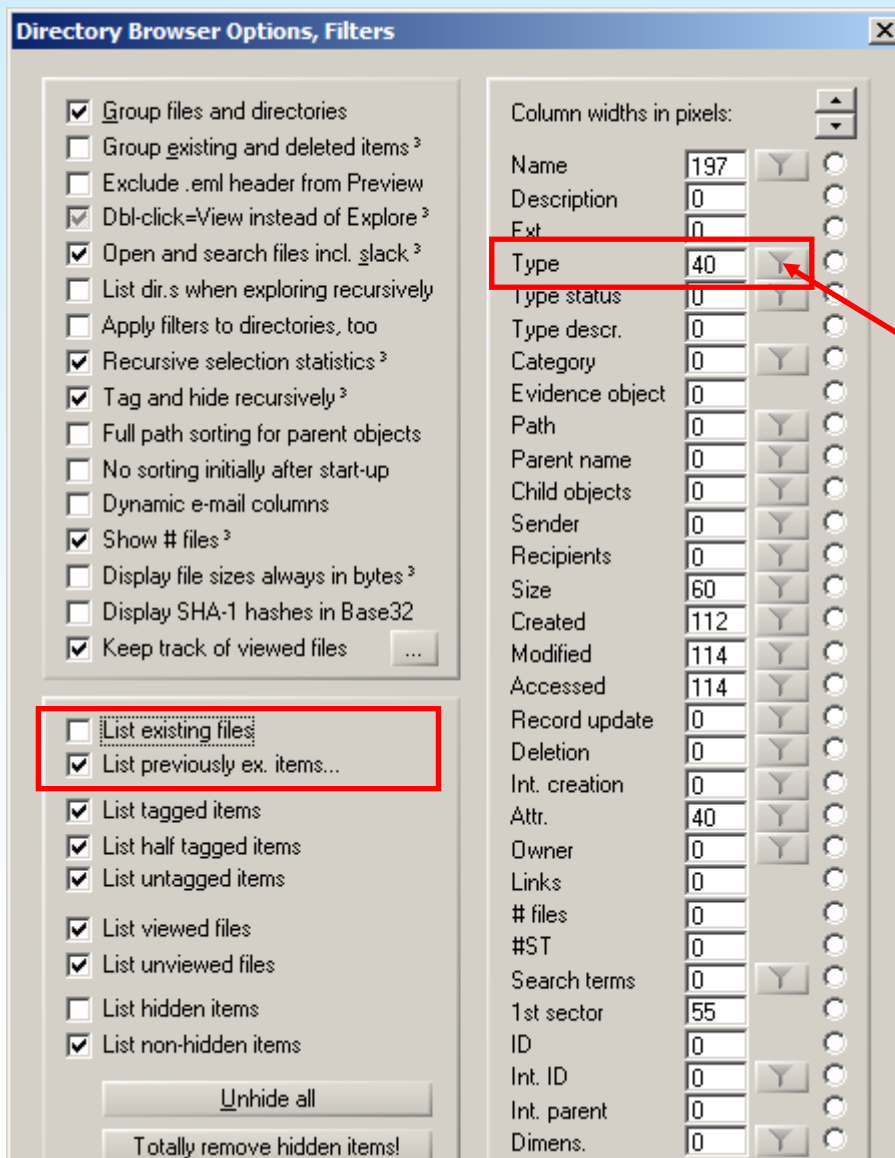
The directory browser options can be called either via their entry in the “Options” menu, the corresponding button in the toolbar or simply by clicking the directory browser’s title bar.

 A screenshot of a file browser window titled '[Ext2 Image.e01]'. The window shows a table of files and subdirectories. A red circle highlights the mouse cursor hovering over the 'Size' column header.

Filename ^	Type	Size	Modified	Accessed	Attr.	ID
.background		21 bytes	11/07/2005 20:43:37	12/14/2005 17:51:17	rw-rw...	24058
.background		21 bytes	11/07/2005 20:43:37	12/14/2005 17:54:19	rw-rw...	20267
.background		21 bytes	11/07/2005 20:43:37	12/14/2005 17:54:18	rw-rw...	2218
.backup_device		0 bytes	08/10/2004 06:54:14	12/14/2005 17:51:17	rw-rw...	32106

4: Filtering (Ex. Deleted JPEG Files)

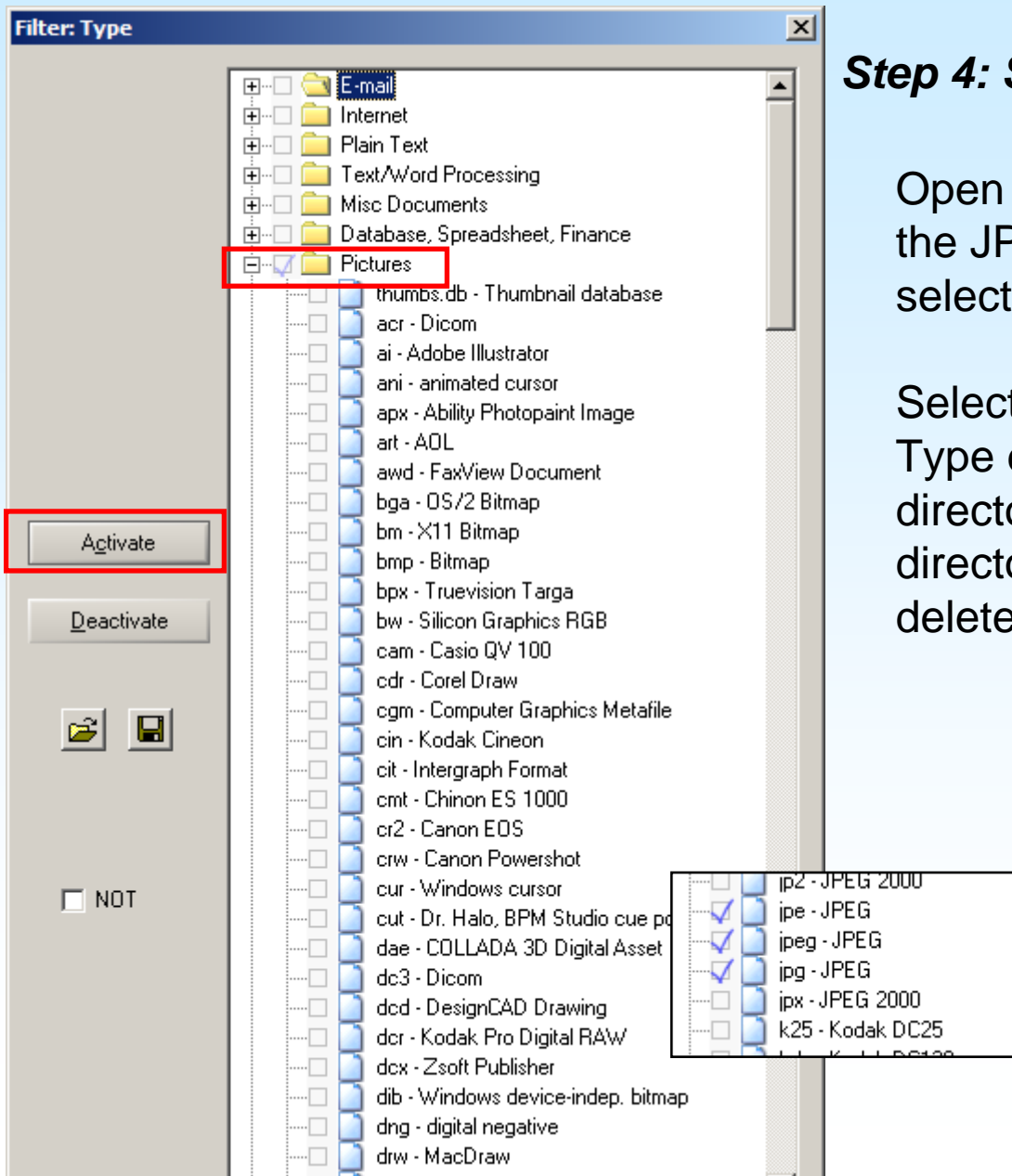
Step 3: Directory browser options



To see deleted files *only*, uncheck the option “List existing files”.

Then click the filter button for “Type”:
The dialog for step 4 will come up.

4: Filtering (Ex. Deleted JPEG Files)



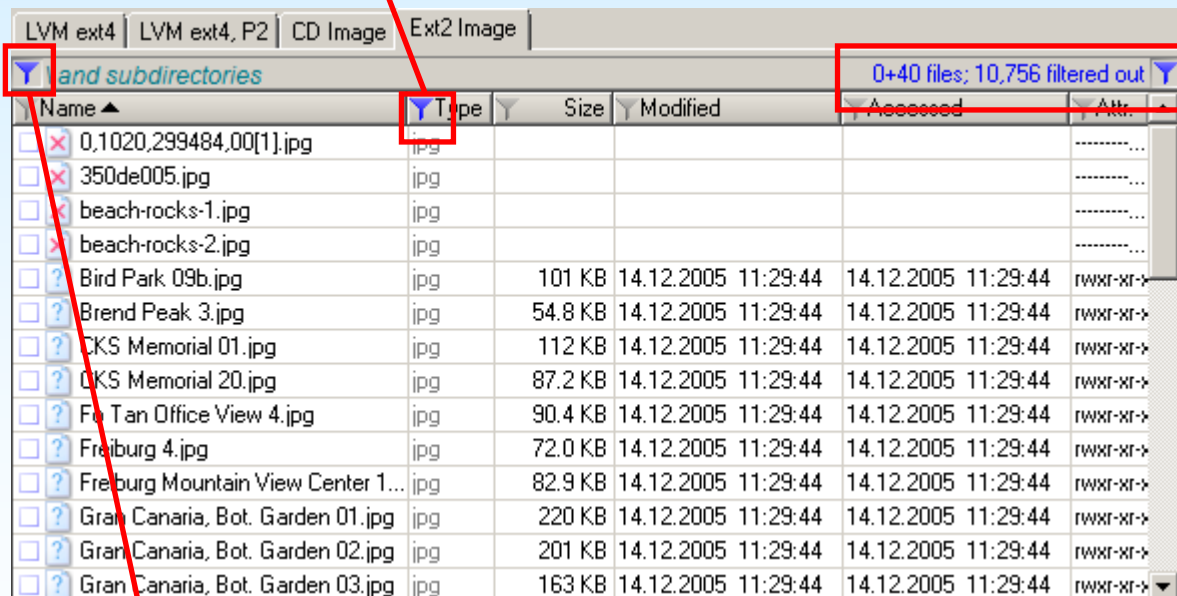
Step 4: Selecting the type

Open category "Pictures" and check the JPEG types. Remove any other selections, if necessary.

Select "Activate" to close the Filter: Type dialog and "OK" to close the directory browser options. The directory browser will now only display deleted files of type JPG/JPEG.

4: Filtering (Ex. Deleted JPEG Files)

Quicker access to the column-based filters (e.g. to deactivate again)



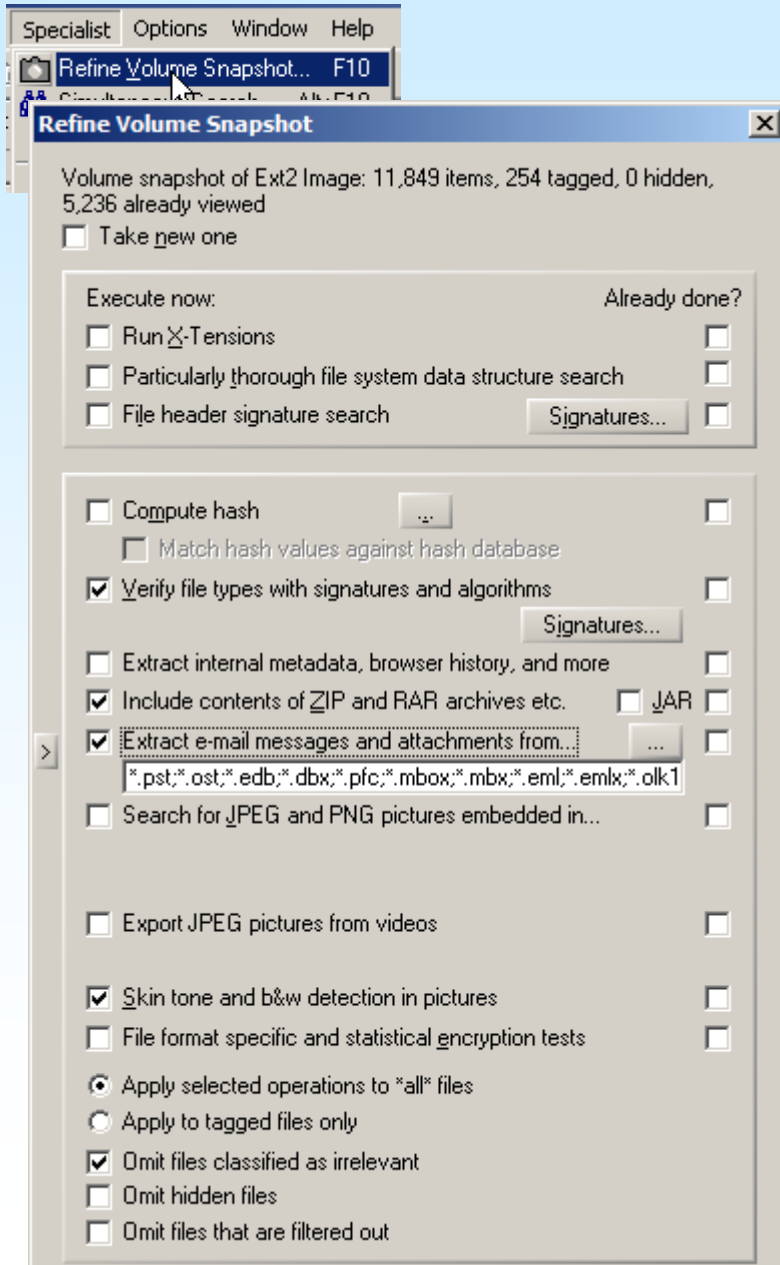
Gives details about the filters' effects:

40 previously existing files are currently displayed (no existing files, no virtual files, no directories).

10,756 files have been filtered out, i.e. are not listed.

Also acts as a "remove all filters" button.

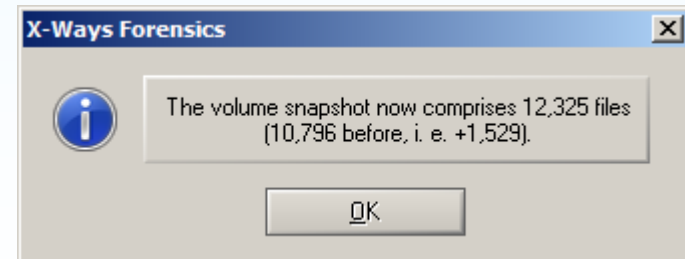
5: Refine Volume Snapshot



Refining the Volume Snapshot first will allow searching compressed files in archives and e-mails in e-mail archives, but also correctly identify file types based on their content, extract internal metadata, recognize skin color and black-and-white pictures, etc.

To that end, press F10 or invoke “Refine Volume Snapshot” from the Specialist menu.

Check the desired options and click ok, which will eventually result in a message like the one below. Acknowledge with OK.



5: Refine Volume Snapshot

Sample Effects of the Refinement

Before:

Name ▲	Type
xyz.abc	abc

File is listed as specified by the file system – *Type* column simply assumes the extension

After:

Name ▲	Type
...xyz.abc (3)	zip

Type has been replaced by type identified from the file contents.

Since the file is an archive and listing their contents was amongst the options chosen, the ... in the icon shows there are now child objects present, the (3) after the name specifies the number of files inside.

Skin color and black-and-white detection:

Name ▲	SC%
makeup3.jpg	26%
makeup4.jpg	61%
Marisandra.jpg	4%
Memorial.jpg	5%
monoster.bmp	b/w
Mydslgui.png	b/w
necklace1.jpg	69%
Neo & Trinity 1.jpg	26%
New York 2.jpg	5%
new-york-9400020.jpg	0%

Color images receive a percentage score with regards to how much of the picture is within skin color range – grayscale images are flagged as **b/w** instead.

6: Office Metadata

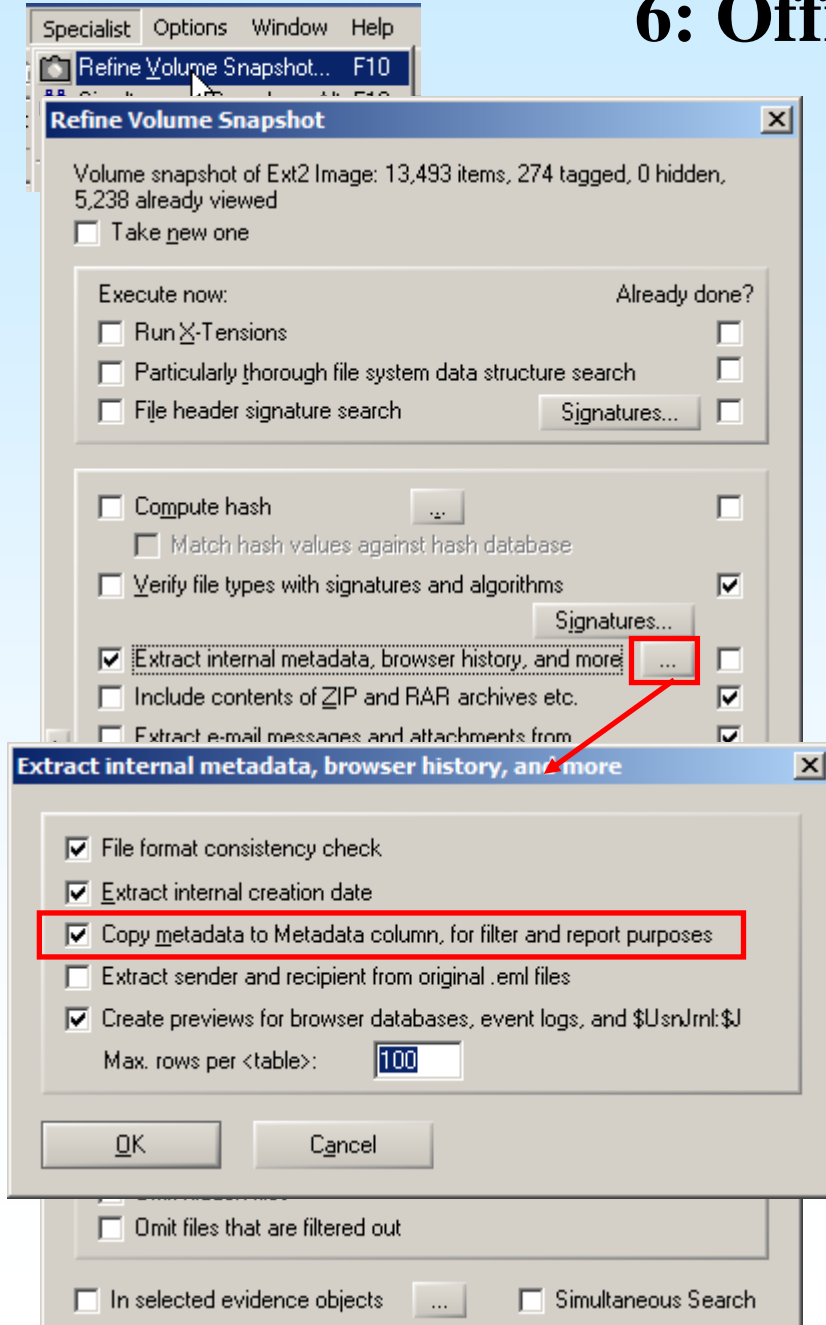
Step 1: Refine Volume Snapshot

Press F10 or invoke "Refine Volume Snapshot" from the Specialist menu.

Choose the option "Extract internal metadata, browser history, and more" and click on the button ... that appears to the right of it.

Choose "Copy metadata to Metadata column, for filter and report purposes". [Here you can also have the internal created date added to the corresponding column and for browser databases, etc., a permanent preview can be created.]

Click OK in both dialogue windows to run the refinement process.



6: Office Metadata

<input type="checkbox"/> Exclude .eml header from Preview	Description	0		
<input checked="" type="checkbox"/> Dbl-click=View instead of Explore ³	Ext.	0		
<input checked="" type="checkbox"/> Open and search files incl. slack ³	Type	43	Y	
<input type="checkbox"/> List dir.s when exploring recursively	Type status	0	Y	
<input type="checkbox"/> Apply filters to directories, too	Type descr.	0		
<input checked="" type="checkbox"/> Recursive selection statistics ³	Category	0	Y	
<input checked="" type="checkbox"/> Tag and hide recursively ³	Evidence object	0		
<input type="checkbox"/> Full path sorting for parent objects	Path	0	Y	
<input type="checkbox"/> No sorting initially after start-up	Parent name	0	Y	
<input type="checkbox"/> Dynamic e-mail columns	Child objects	0	Y	
<input checked="" type="checkbox"/> Show # files ³	Sender	0	Y	
<input type="checkbox"/> Display file sizes always in bytes ³	Recipients	0	Y	
<input type="checkbox"/> Display SHA-1 hashes in Base32	Size	60	Y	
<input checked="" type="checkbox"/> Keep track of viewed files	Created	0	Y	
	Modified	114	Y	
	Accessed	114	Y	
	Record update	0	Y	
<input checked="" type="checkbox"/> List existing files	Deletion	0	Y	
<input checked="" type="checkbox"/> List previously ex. items...	Int. creation	0	Y	
<input checked="" type="checkbox"/> List tagged items	Attr.	40	Y	
<input checked="" type="checkbox"/> List half tagged items	Owner	0	Y	
<input checked="" type="checkbox"/> List untagged items	Links	0		
<input checked="" type="checkbox"/> List viewed files	# files	0		
<input checked="" type="checkbox"/> List unviewed files	#ST	0		
<input type="checkbox"/> List hidden items	Search terms	0	Y	
<input checked="" type="checkbox"/> List non-hidden items	1st sector	55		
	ID	0		
	Int. ID	0	Y	
	Int. parent	0		
	Dimens.	0	Y	
	SC%	50	Y	
	Hash	300	Y	
	Hash set	142	Y	
	Hash category	176	Y	
	Report table	0	Y	
	Comment	200	Y	
	Metadata	400	Y	

First scrollable column:

Step 2: Make Metadata column visible

If the Metadata column is already visible in the directory browser, simply skip this step.

Open the directory browser options (cf. chapter 4, step 2).

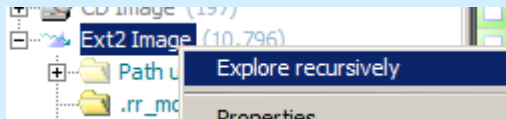
Enter a value in the box for "Metadata", e.g. 400.

[The value entered will be the column width in pixels – the width can be adjusted with the mouse at any time later.]

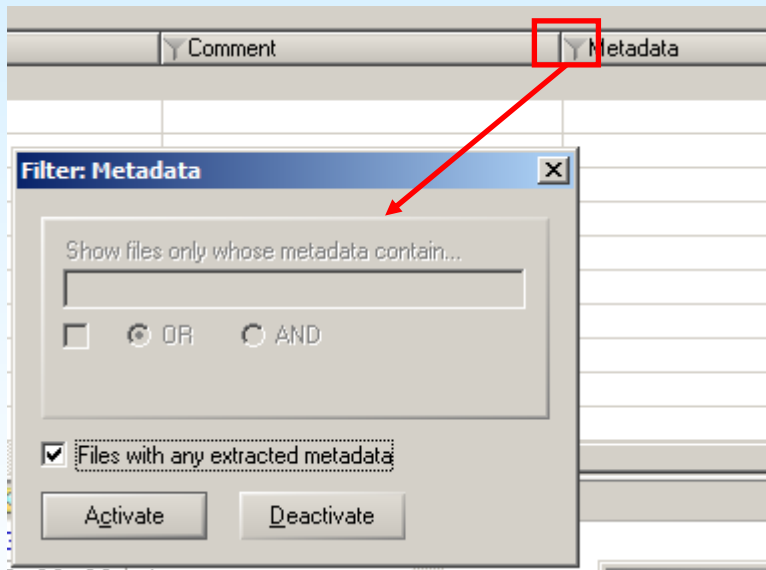
Confirm with OK. The column should appear in the directory browser.

6: Office Metadata

Step 3: Filter: Metadata – any



Explore the partition recursively (cf. chapter 4, step 1).



Click the filter icon in the Metadata column. The Filter: Metadata should appear.

[If you miss the icon and instead click the column header itself, the column will be sorted by.]

Leave "Files with any extracted metadata" checked and click "Activate". The directory browser will then only list files whose Metadata column is not empty.

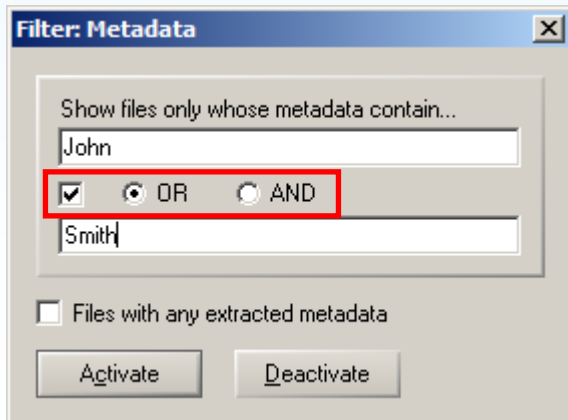
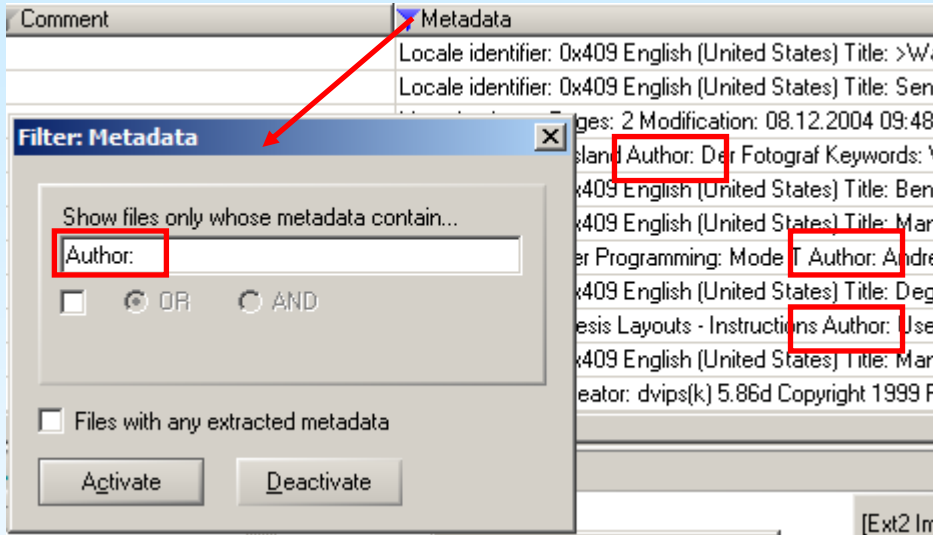
6: Office Metadata

Step 4: Filter: Metadata – specific

Click on the filter icon in the Metadata column. The Filter: Metadata should appear again.

Uncheck "Files with any extracted metadata". As an example enter "Author:" in the text box and click "Activate". The directory browser now only shows files whose Metadata column contains "Author:".

With the check box below the search term you can add a second text box. The two can then be combined with OR (all files whose Metadata field has at least one of the search terms) or AND (all files whose Metadata field contains both search terms) as required.



7: Search (Ex. "John" and "Smith")

Step 1: Enter search terms and options

Via the context menu the search can be limited to selected items, but the options allow changing that to all or tagged items instead.

The screenshot shows a file manager window with a context menu open over the 'home' directory. The 'Simultaneous Search...' option is selected. The 'Simultaneous Search' dialog box is open, showing the search terms 'John' and 'Smith' in a text area. The dialog box has several options and checkboxes:

- Match case
- GREP syntax
- Whole words only
- Alphabet to define word boundaries: ...
- Cond.: offset mod 512 = 0
- Run X-Tensions
- All objects in volume snapshot (267 MB)
- Search all tagged objects (3.6 MB)
- Search all selected objects (10.4 MB)
- Open and search files incl. slack³
- Cover file slack/free space transition
- Decode text in files: *.pdf;*.docx;*.pptx;*.xlsx;*.odt;*.odp;*.oc
- Omit files classified as irrelevant
- Omit hidden files
- Omit files that are filtered out
- Recommendable data reduction
- Omit directories
- 1 hit per file needed only (faster)

At the bottom of the dialog box, there are three checked text encoding options:

- ANSI - Latin I (1252)
- Unicode UTF-16 Little Endian (1200)
- Unicode UTF-8 (65001)

Red boxes and arrows highlight these features:

- A red box around the 'Whole words only' checkbox with an arrow pointing to the text: "Occurrences of 'John' and 'Smith' as whole words only".
- A red box around the text encoding options with an arrow pointing to the text: "Multiple text encodings simultaneously".
- A red box around the search results area with an arrow pointing to the text: "OK will run the search".

The dialog box also has buttons for 'OK', 'Cancel', 'Logical (file-wise)', and 'Help'.

7: Search (Ex. "John" and "Smith")

Step 2: Reviewing search hits (Explanations on following slide)

Case Data | LVM ext4 | LVM ext4, P2 | CD Image | Ext2 Image | 16.7 SR-3

File Edit Search Navigation View Tools Specialist Options Window Help

Search hits in \ and subdirectories 18 Search hits

Offset	Rel. ofs.	Descr.	Search hits	Name	Type	Size	#ST
98162715	153627	CP 1252	file or disk. Find "John" [MatchCase Mat	Manual.doc	doc	419 KB	1
98162886	153798	CP 1252	indow for the name John or the hexadecima	Manual.doc	doc	419 KB	1
98585732	144516	CP 1252	disque actif. Find "John" [MatchCase Mat	Manuel WinHex.doc	doc	438 KB	2
98585900	144684	CP 1252	être active le nom John ou les valeurs hex	Manuel WinHex.doc	doc	438 KB	2
98593231	152015	CP 1252	e.g.: Letter to Mr. Smith.doc Invoice*.pdf	Manuel WinHex.doc	doc	438 KB	2
107947537	136721	CP 1252	file or disk. Find "John" [MatchCase Mat	Spanish Manual.doc	doc	394 KB	2
107947708	136892	CP 1252	indow for the name John or the hexadecima	Spanish Manual.doc	doc	394 KB	2
107954449	143633	CP 1252	e.g.: Letter to Mr. Smith.doc Invoice*.pdf	Spanish Manual.doc	doc	394 KB	2
107964172	153356	CP 1252	e words Dear Mr. Smith in a MS Word do	Spanish Manual.doc	doc	394 KB	2
108575010	127266	CP 1252	file or disk. Find "John" [MatchCase Mat	WinHex Manual.doc	doc	378 KB	2
108575181	127437	CP 1252	indow for the name John or the hexadecima	WinHex Manual.doc	doc	378 KB	2
108581785	134041	CP 1252	e.g.: Letter to Mr. Smith.doc Invoice*.pdf	WinHex Manual.doc	doc	378 KB	2
108591481	143737	CP 1252	e words Dear Mr. Smith in a MS Word do	WinHex Manual.doc	doc	378 KB	2
112288433	10929	CP 1252	. We all know that John Carmack has den	dxtasy_y.doc	doc	86.0 KB	1

File Tree (Left): Ext2 Image (12,325) | Path unknown (48) | .rr_moved (0) | bin (83) | boot (15) | cdrom (0) | dev (4,945) | etc (757) | floppy (0) | home (219) | dsl (219) | .dillo (5) | .emelfm (8) | .fluxbox (6) | .index (7) | .sylheed (12) | .xmsm (24)

Notable hits (Bottom Left): John (11) | Smith (7)

Hex View (Bottom): Volume | File | Preview | Details | Gallery | Calendar | Legend | Sync | Selected: 1 Search hits

File Details (Right): [Ext2 Image.e01] 47% free | File system: Ext2 | [Read-only mode] | Alloc. of visible drive space: | Block: 105417 | Spanish Manual.doc | \home\ds\Docs\

Search Parameters (Bottom): Sector 210835 of 510993 | Offset: 107947537 | = 74 | Block: | n/a | Size: n/a

7: Search (Ex. "John" and "Smith")

Step 2: Reviewing search hits (Explanations for previous slide)

- 1 Clicking this button calls the search term and search hit lists.
- 2 This is the search hit list. You can narrow search hits down by
 - selecting sub-directories in the directory tree 3
 - applying filtering methods available in the directory browser 4
- 5 This is the search term list. Selecting one or more search terms allows narrowing the search hits to just the currently desired terms. Double-click a single term or use multiple-selection and the Enter button or key.
- 6 Clicking on a search hit in the list will bring the hit into view in the lower half of the screen.
- 7 Increasing the expected search terms (i.e. different search terms not, not multiple hits for the same one!) per file reduces the search hit list to just those files that meet the condition.



7: Search (Ex. "John" and "Smith")

GREP alternative to Step 1: Enter search terms and options

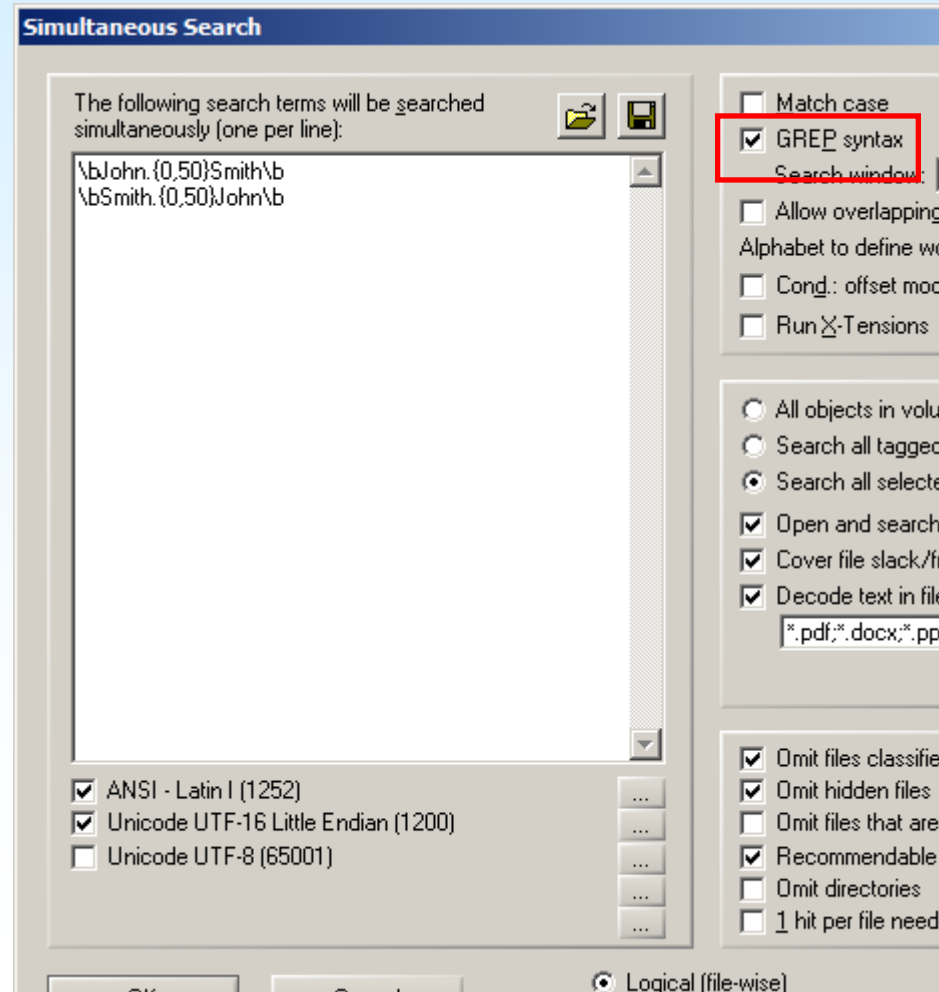
Instead of search for "John" and "Smith" as independent key words, GREP allows running a proximity search, i.e. requiring them to be found close together:

\bJohn.{0,50}Smith\b

\b requires a word boundary, (beginning or end of a word, depending on position) thus repaces "Whole words only"

.{0,50} allows for anything between 0 and 50 random characters (represented by the period), thus allows "John" and "Smith" either as one word or separated by at most 50 random characters.

The second line allows for the two words to occur in opposite order.



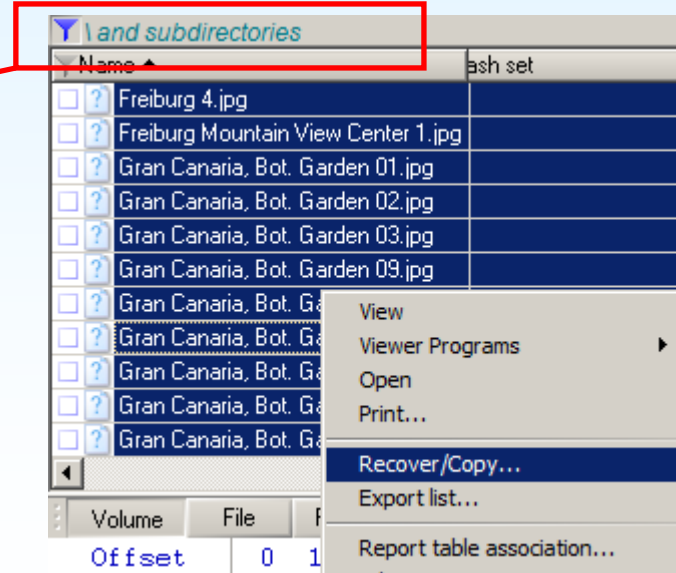
8: Copying Files

Step 1: Select the desired files and/or directories

- individually or as a group, via Ctrl+A the entire current list
- recursively or in regular listing
- using filters of your choice or without filters

As an example, deleted JPEGs are filtered for (as shown in chapter 4) and using Ctrl+A all files are selected that meet the filter criteria. Right-click the selection to see the context menu:

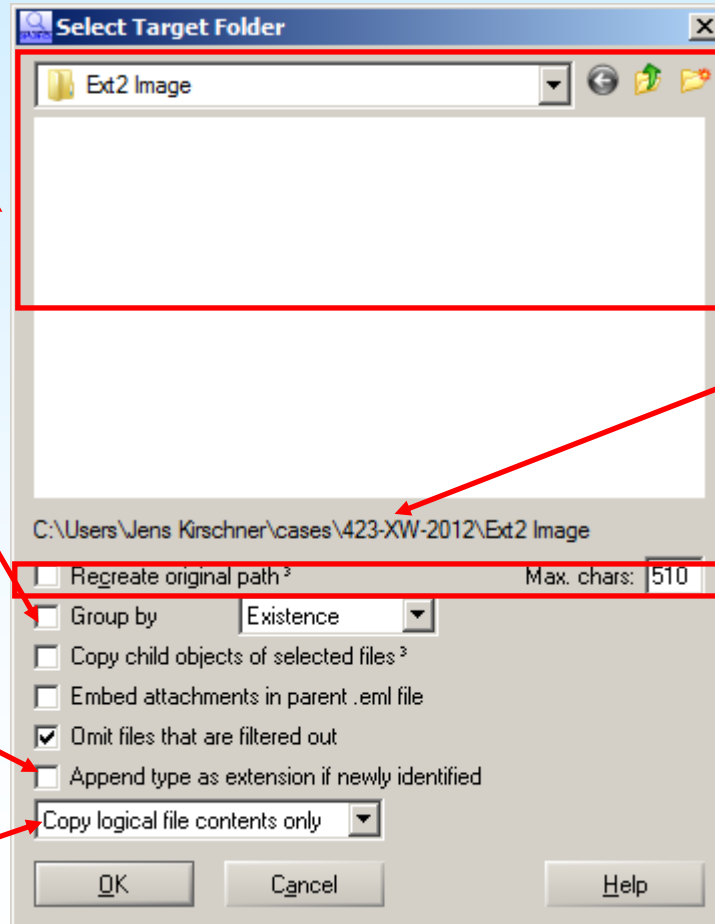
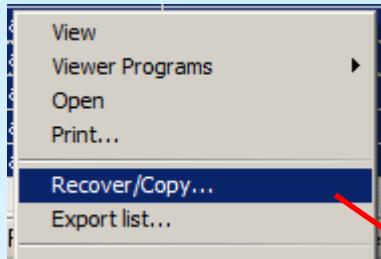
Filter active (in the example: Type filter for JPEGs, existing files not listed) and recursive listing from the root directory ("\\")



8: Copying Files

Step 2: Recover/Copy

In the context menu, select *Recovery/Copy...*



Produces separate output directories, as per the grouping.

Renames files without a useful extension – allows Windows to correctly open the file.

File contents with and without slack – or just slack, if the file itself is of no significance.

Specify output path for the files to be recovered/copied.

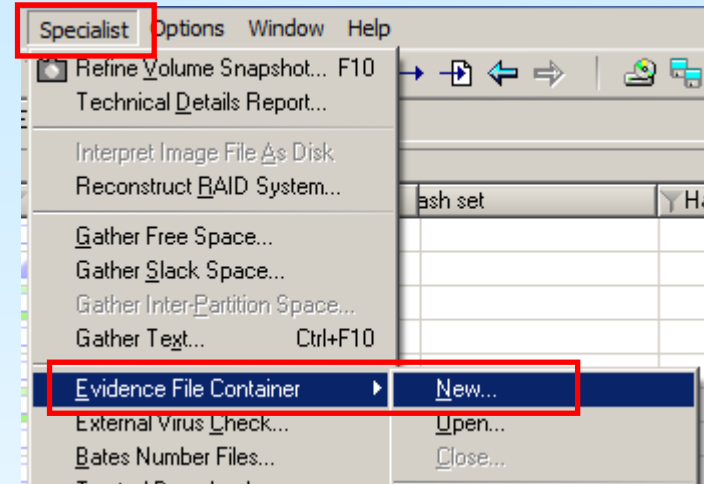
Reproduces within the output directory the paths as found at the origin (provided the maximum length is not exceeded).

9: Evidence File Container

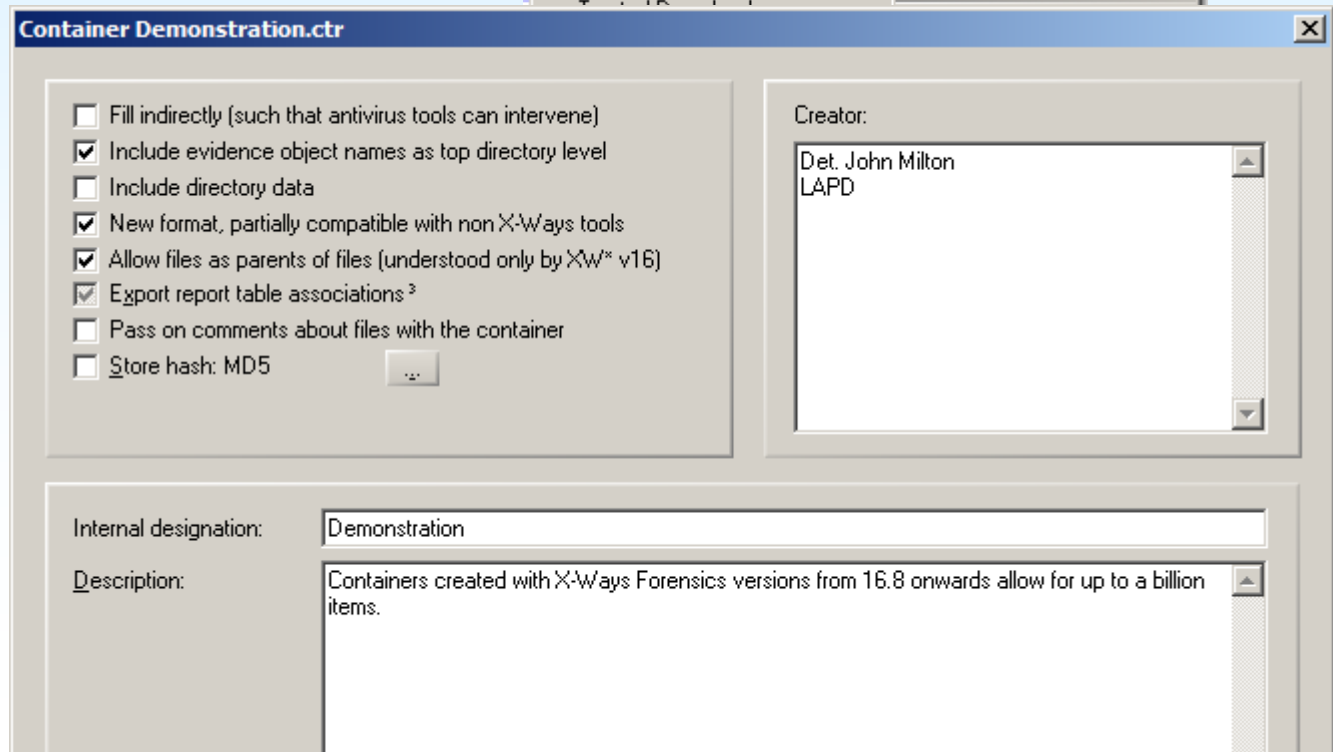
Step 1: Create the Evidence File Container

In the menu, go to *Specialist* → *Evidence File Container* → *New...*

In the following file dialogue, choose the desired path and file name for the container. X-Ways Forensics will add the extension .ctr.

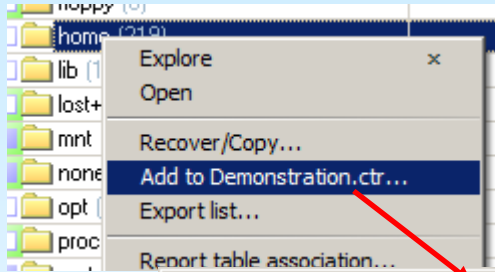


Once the file dialogue is confirmed, X-Ways Forensics will ask for the desired container settings. Keep the settings and enter a description. Click OK.

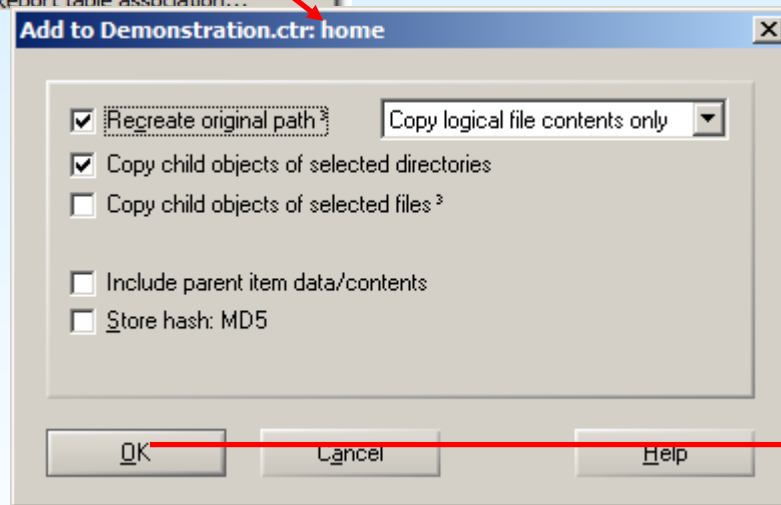


9: Evidence File Container

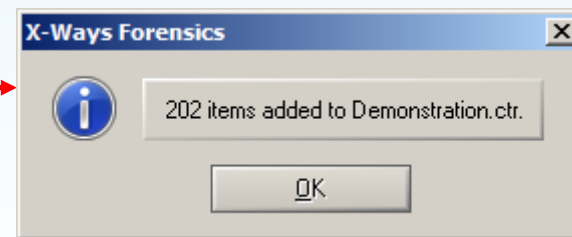
Step 2: Adding files to the container



Use the same methods as for copying files (chapter 8, step 1) to select the desired files. But in the context menu choose *Add to [name of your container]...* instead.



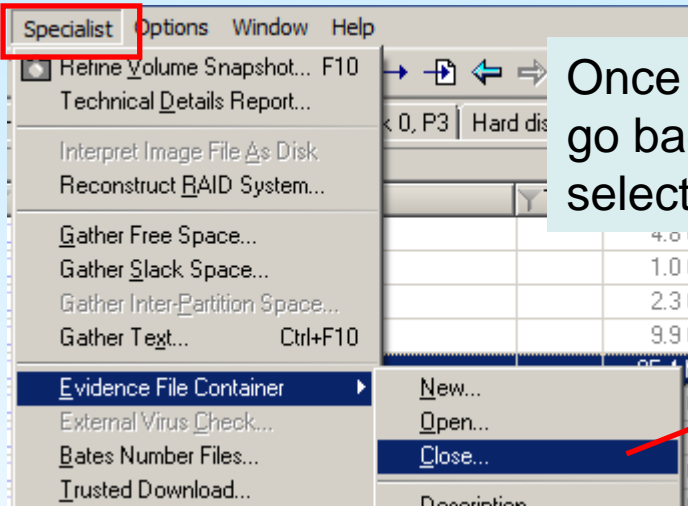
The options are similar to those of *Recover/Copy* as well, but no output directory is required, of course – and all files in the container are protected from interference by the operating system.



You can copy files from various sources into the same container. It does not matter whether the sources are media or images, or whether they are part of a case or have simply been opened standalone.

9: Evidence File Container

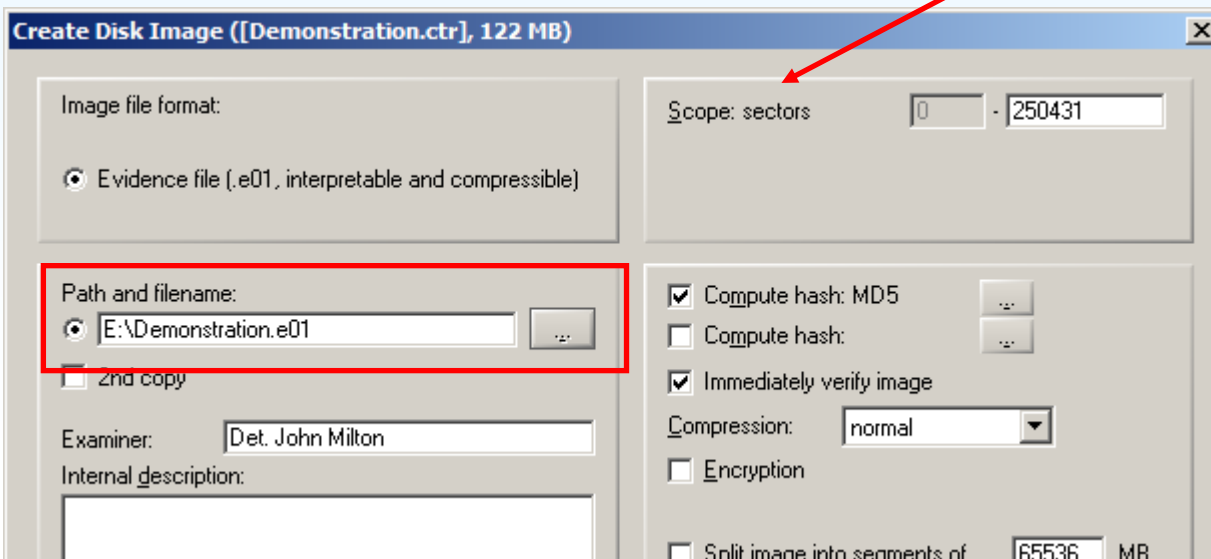
Step 3: Close the container



Once you have added all required items to the container, go back to *Specialist* → *Evidence File Container* and select *Close*.



Click Yes.



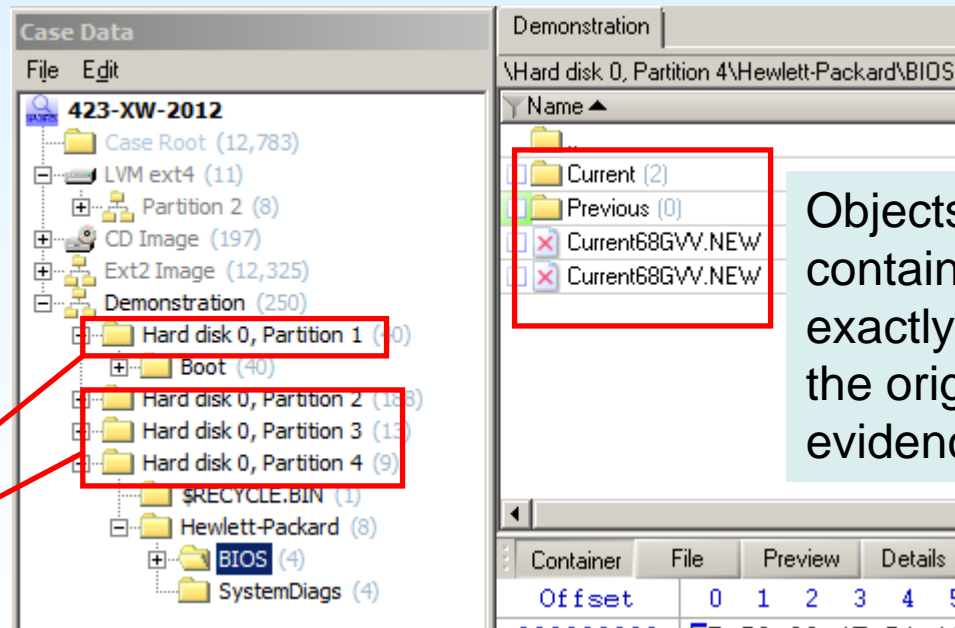
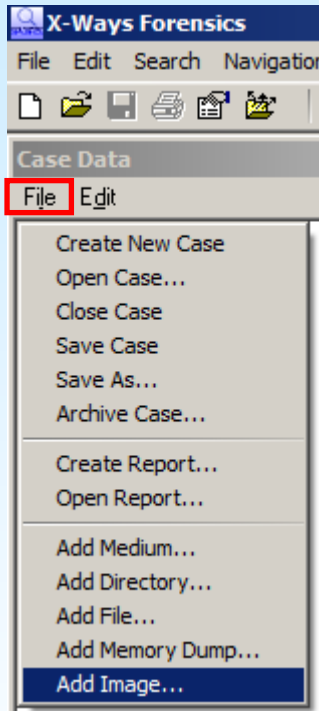
This dialogue is already known from chapter 1, step 2 – except here it is fixed to *Evidence file*.

Specify an appropriate output destination and click OK.

9: Evidence File Container

Step 4: Add container to the case

Containers are treated like ordinary images by X-Ways Forensics – add your container to your case (as in chapter 2, step 2).



Original evidence sources are shown as the top-level directories