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

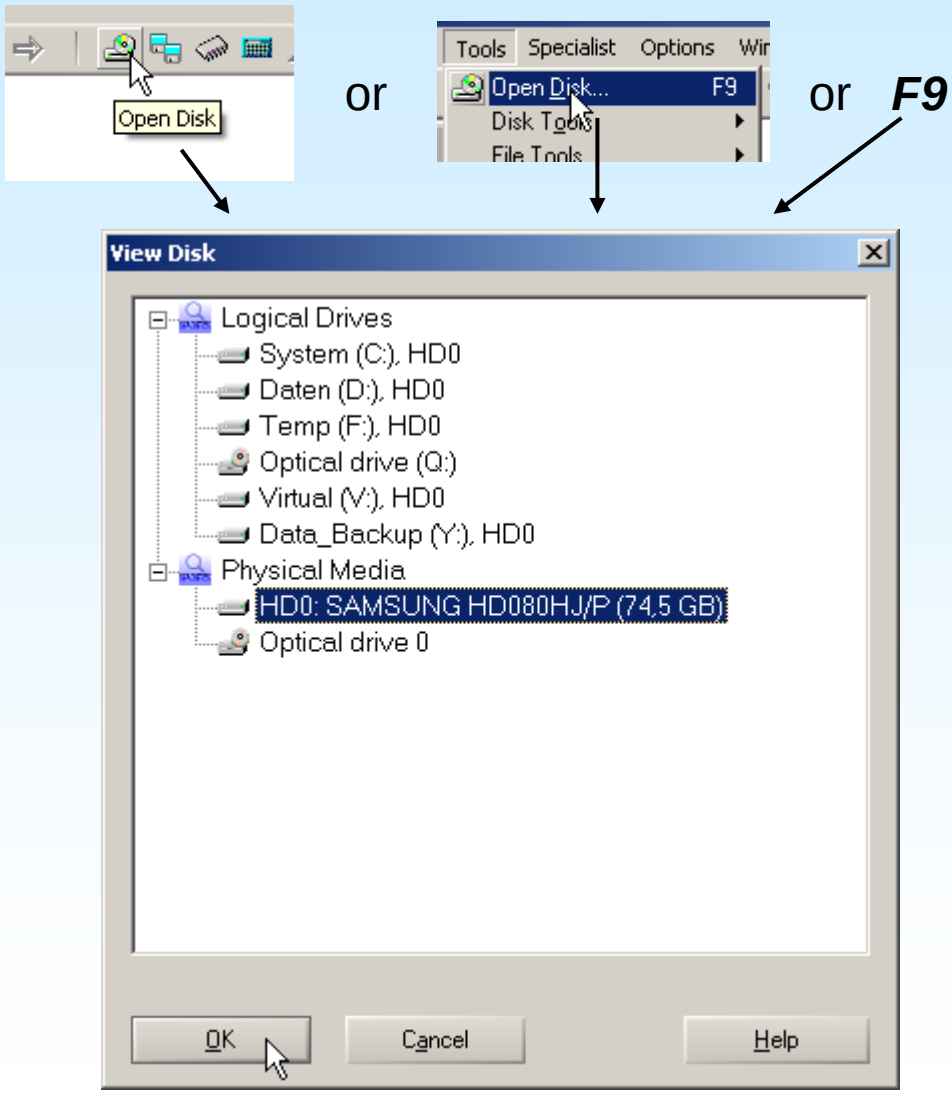
Phone: +49-221-420 486 5

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

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



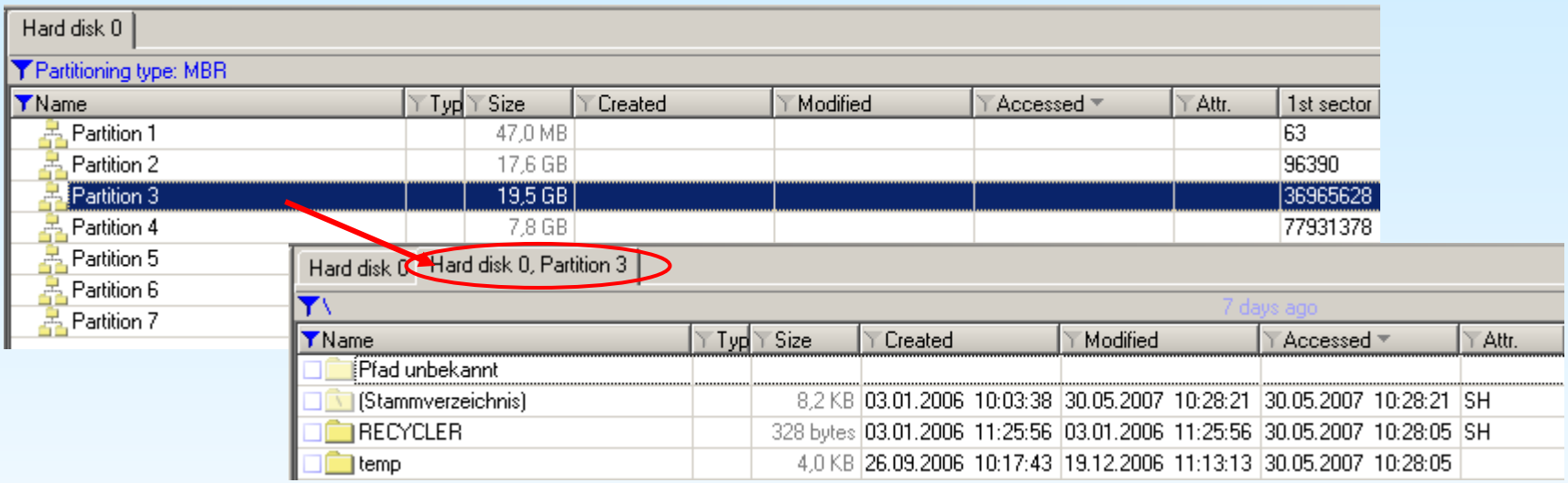
Step 1: Open medium to image

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.

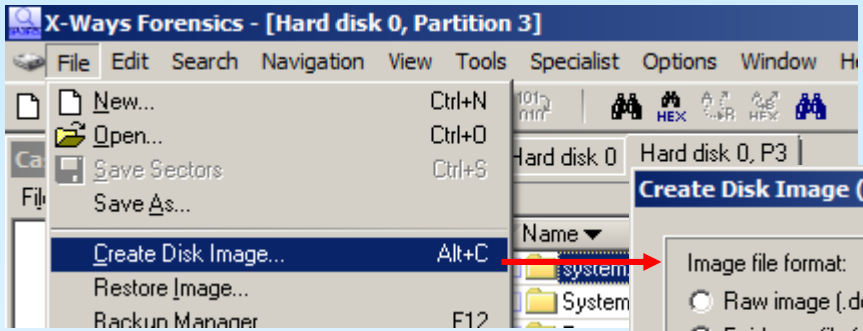
1: Image Creation

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

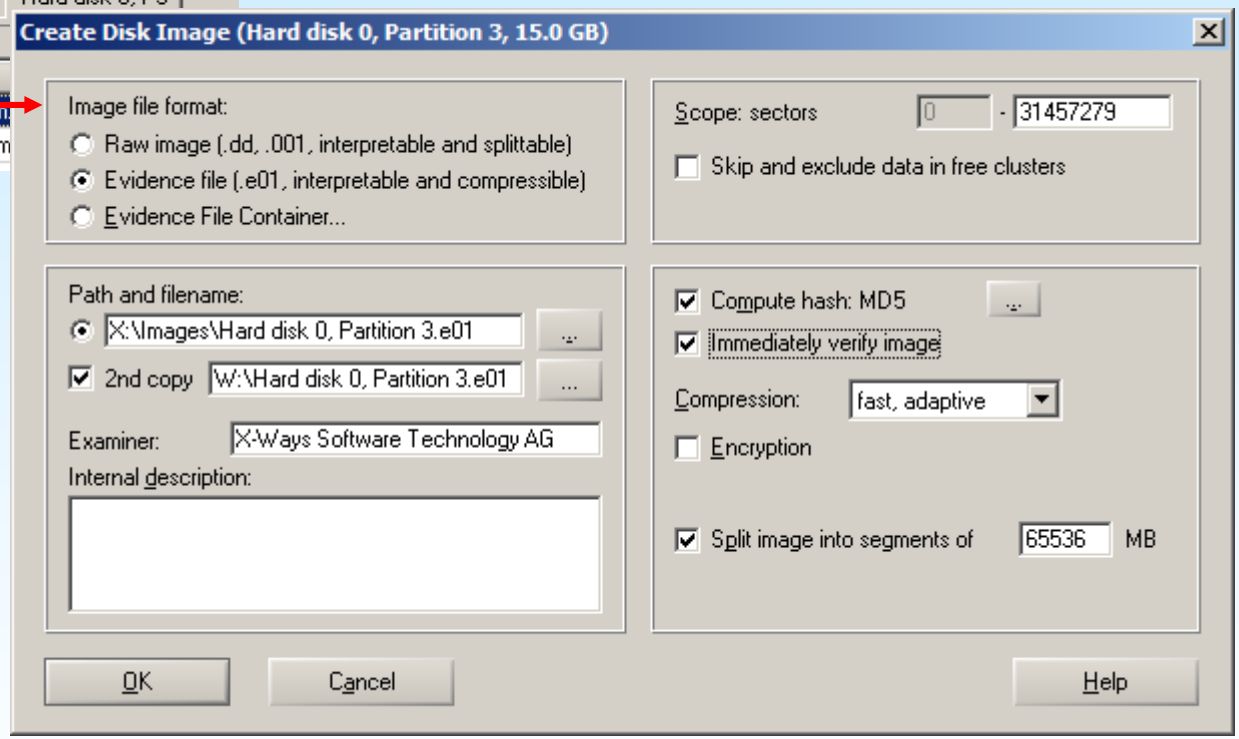


Select a particular partition and open it. For images of the complete (physical) medium, this is not necessary, of course.

1: Image Creation



Step 2: Create the disk image



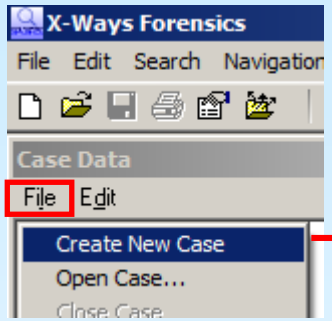
The command always applies to currently active tab within X-Ways Forensics.

Create 2 copies simultaneously if required!

Hash computation allows for later verification of image integrity.

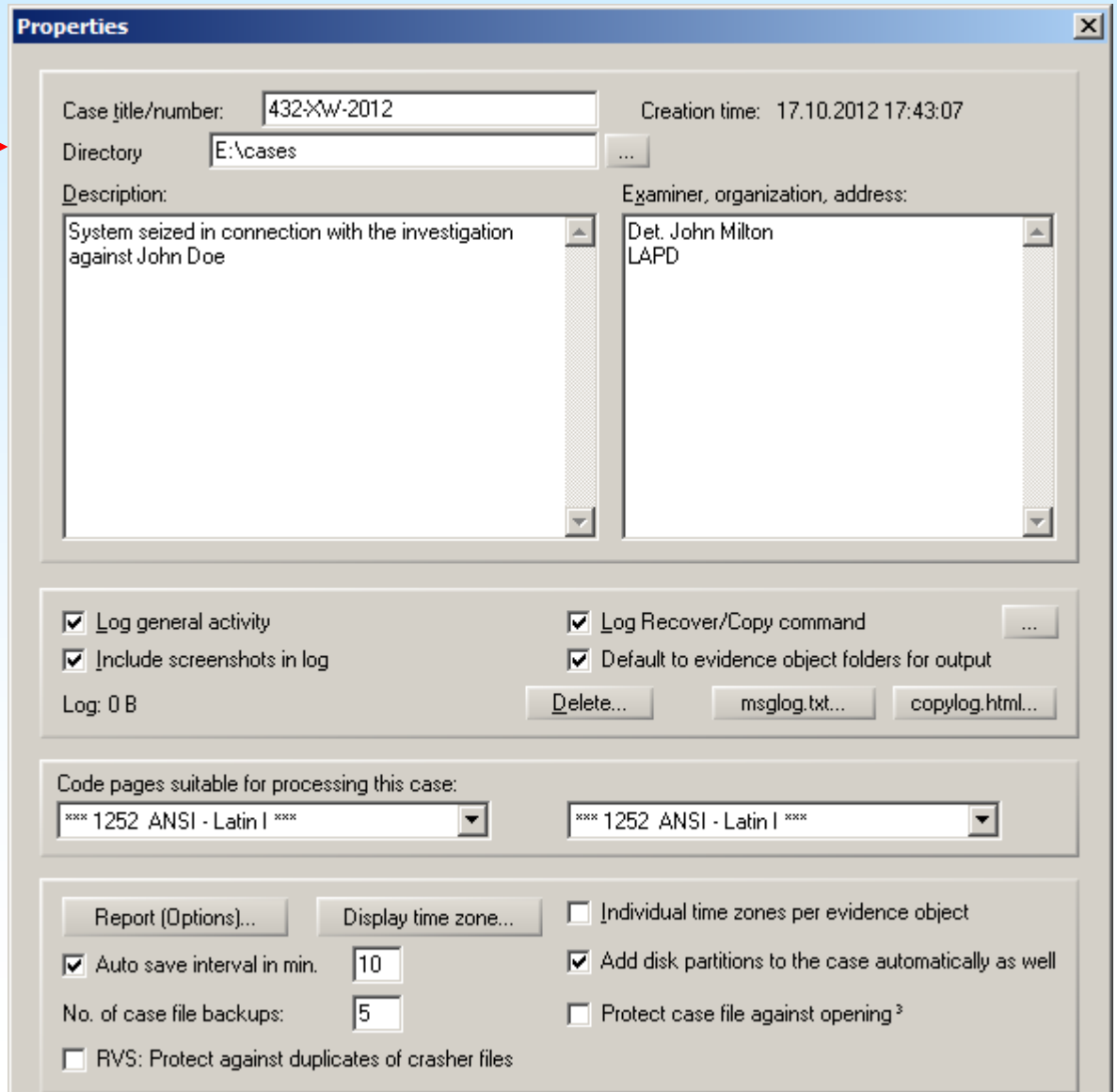
Splitting images helps if you need to store them on CD-Rs or DVD+/-Rs or FAT32 file systems.

2: Case Creation, Adding Images



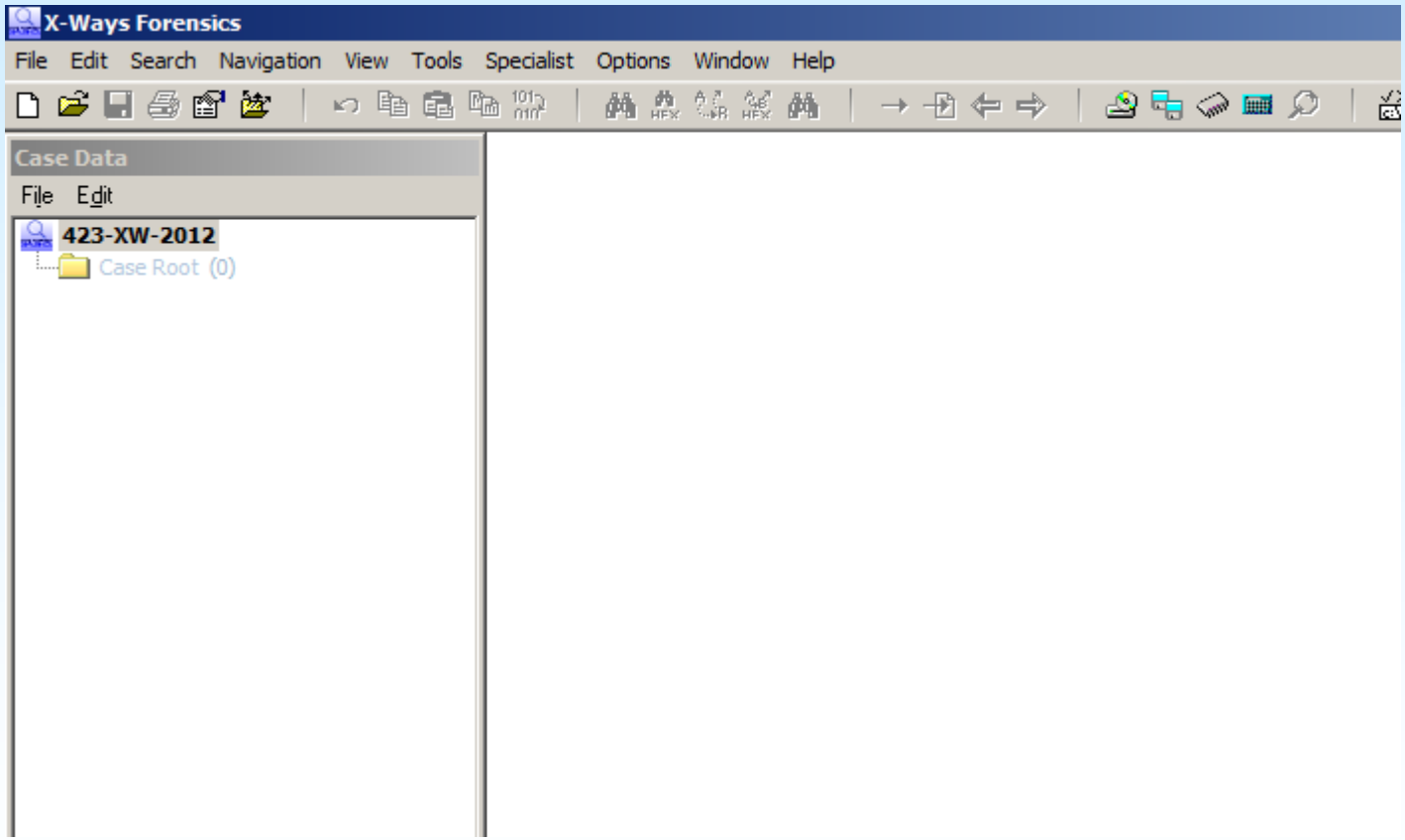
Step 1: Create New Case

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



2: Case Creation, Adding Images

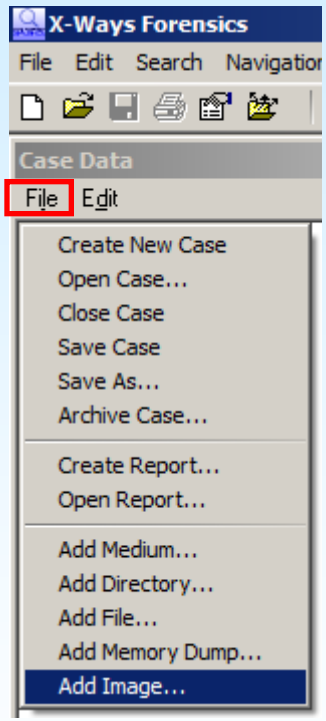
Once you select OK, a new case will be created and opened in X-Ways Forensics:



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.

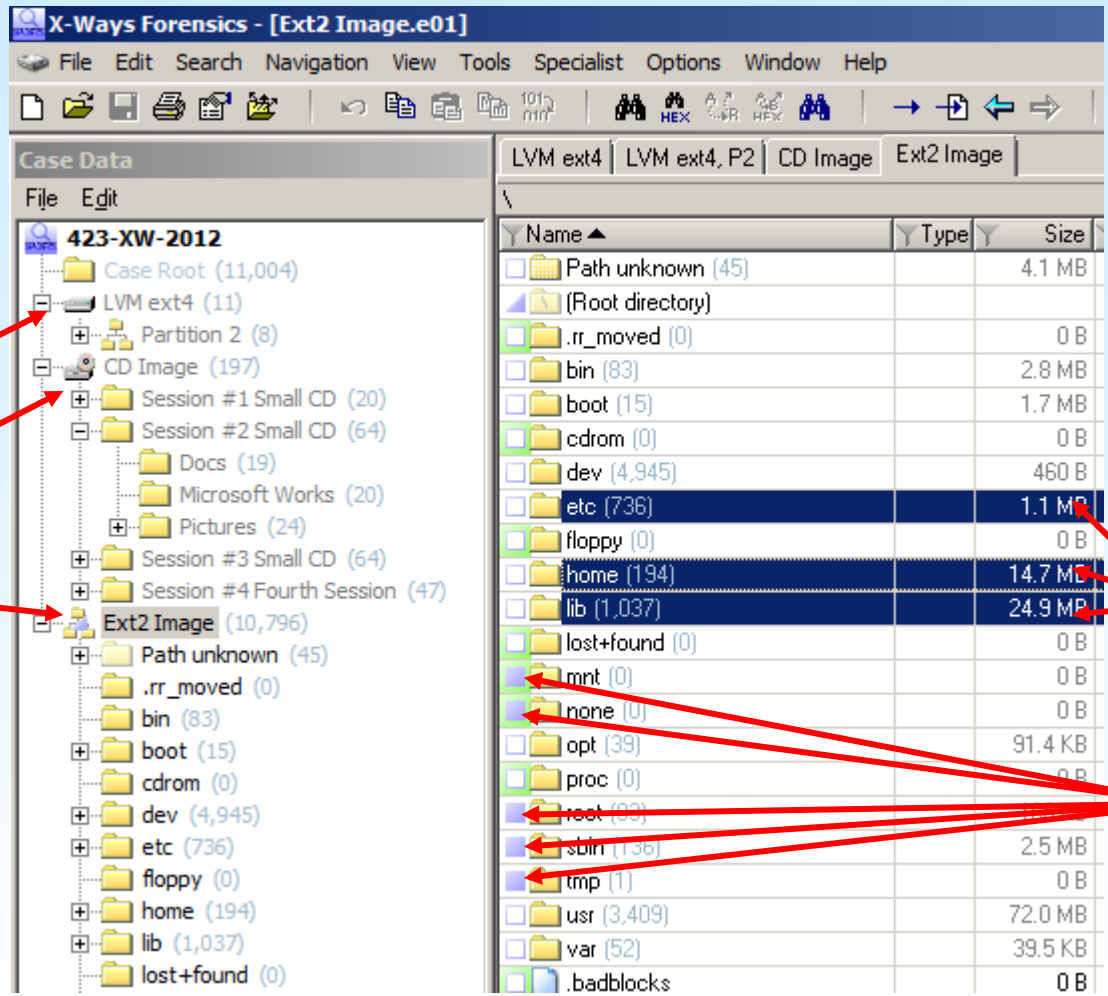
2: Case Creation, Adding Images

Images of:

Physical media

Optical media

Partitions/ Volumes

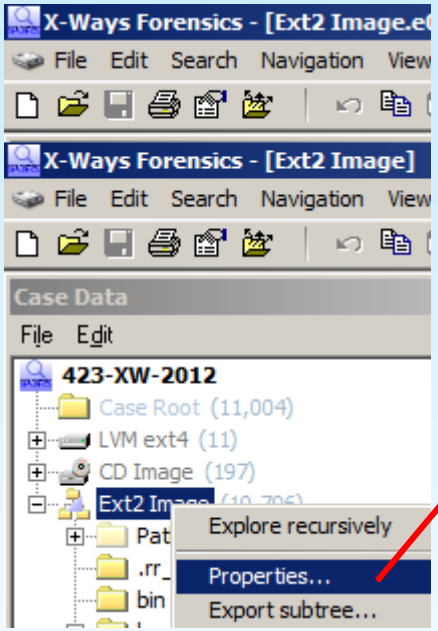


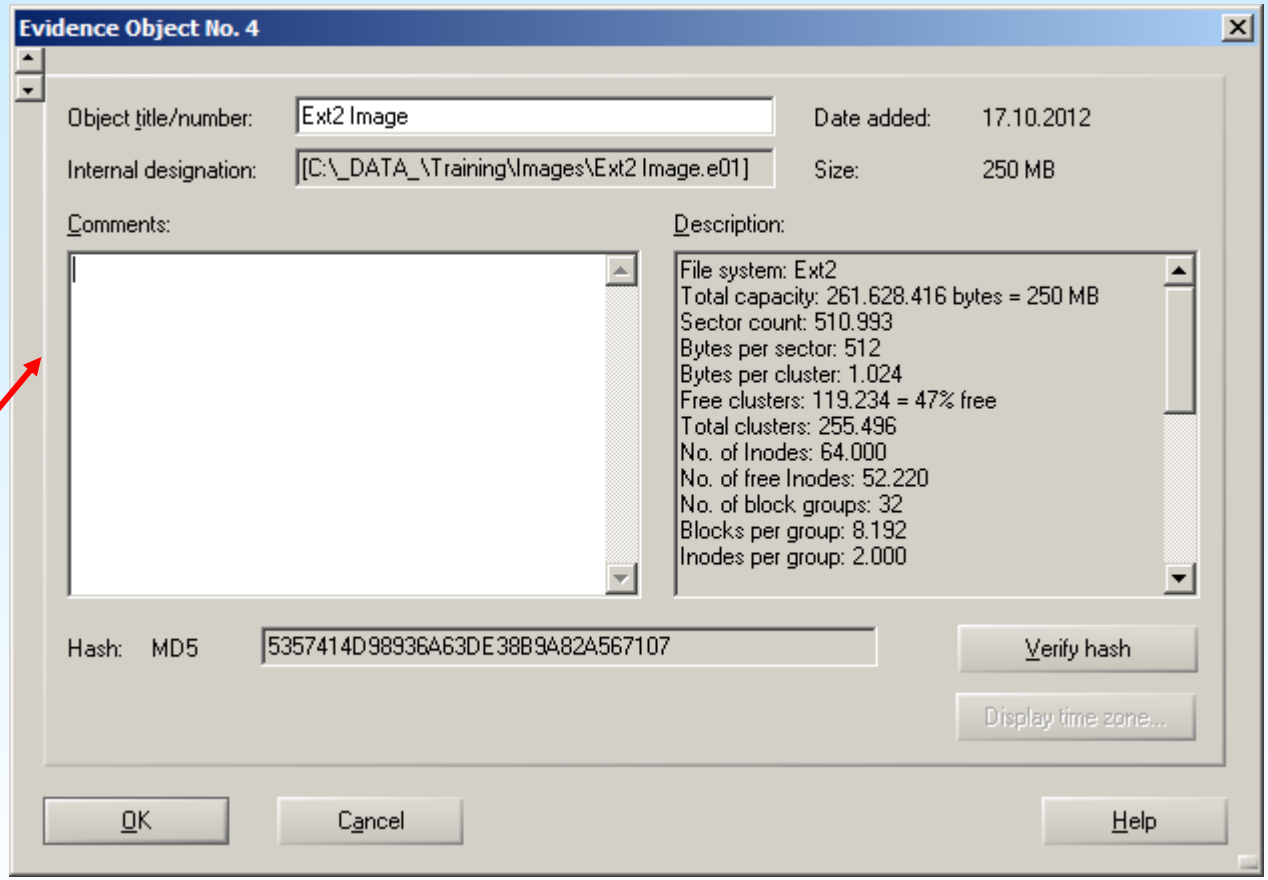
"Selected"

"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,...

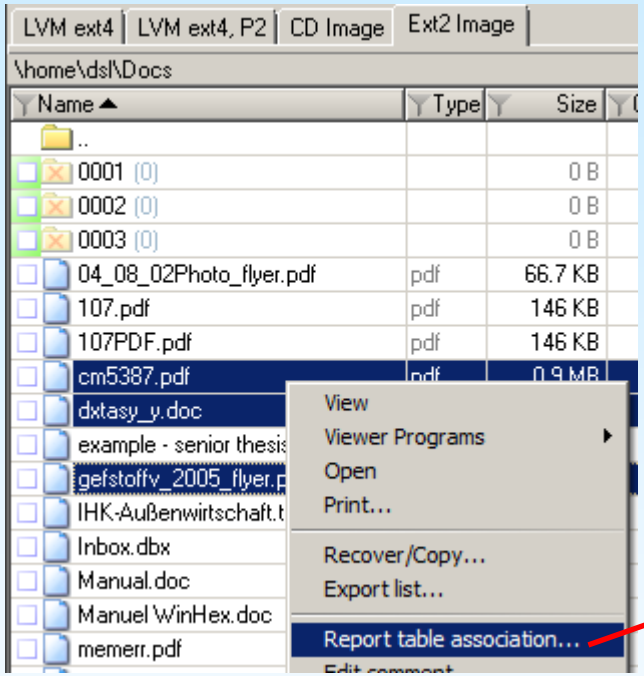
2: Case Creation, Adding Images



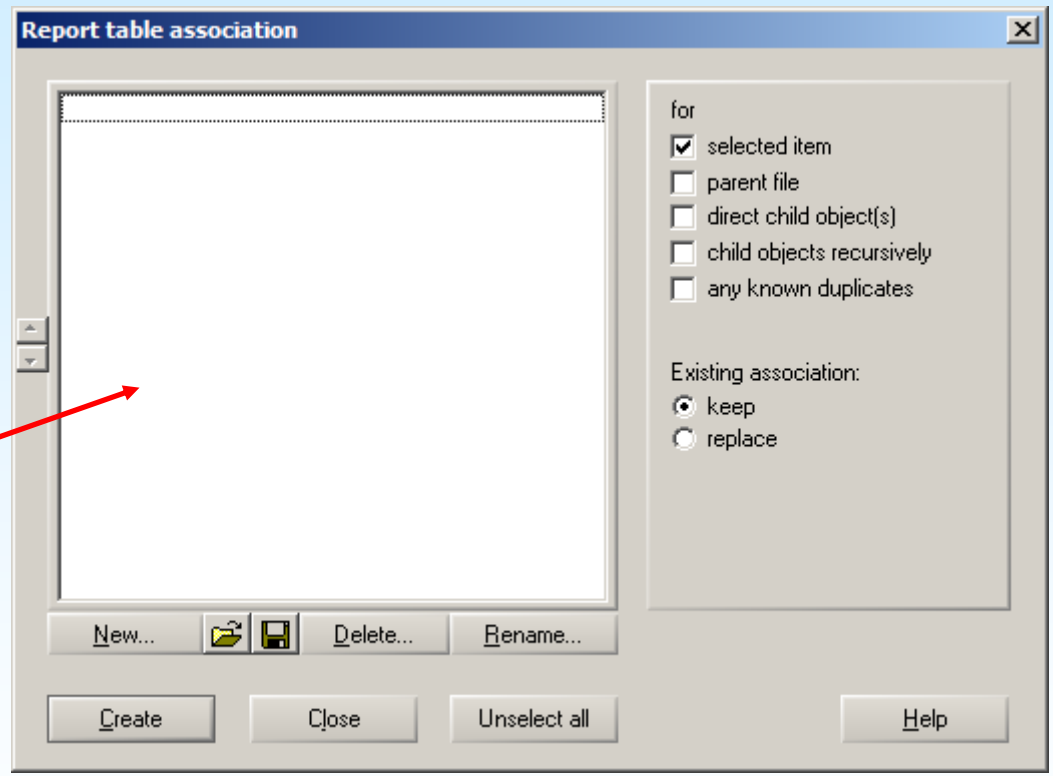


Properties of an image can be accessed via the context menu in the Case Data window.
There you can have X-Ways Forensics verify the image's hash value as well.

3: Report Noteworthy Files



Step 1: Report table association



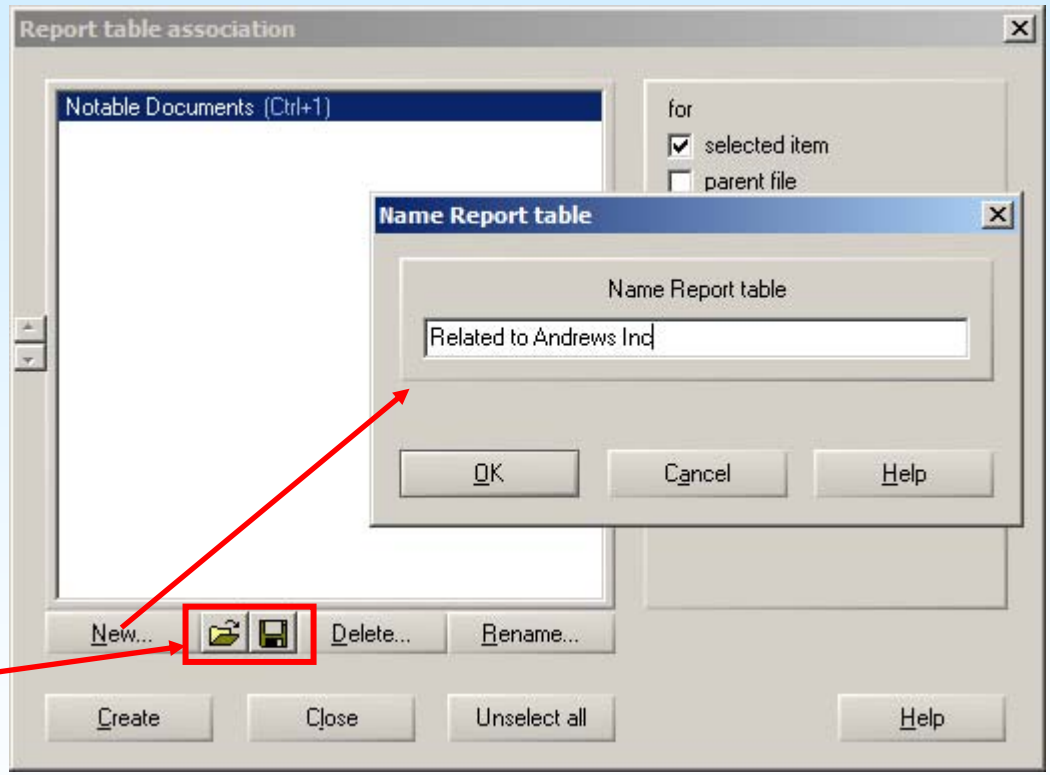
Select the files and directories in question and right-click the selection. In the context menu, use “Report table association…”, which will bring up the list of currently available report tables.

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)

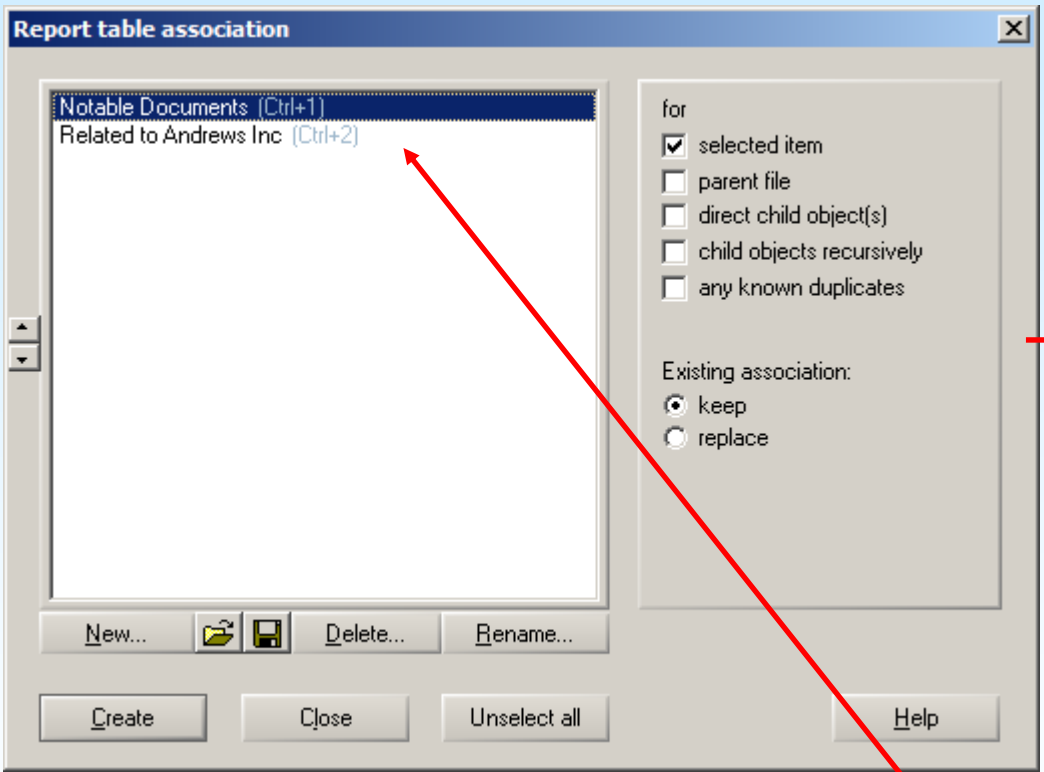


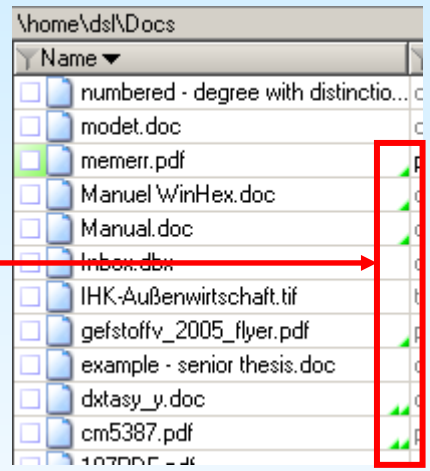
Create as many tables as you need – the list can be added to at any time.

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





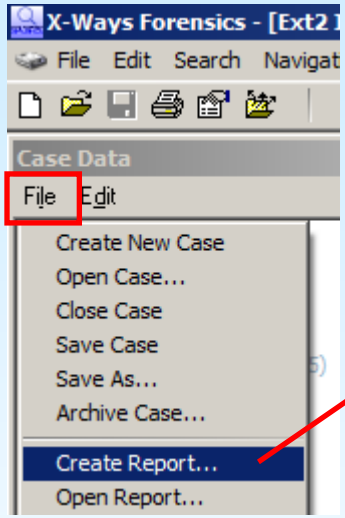
The green triangle identifies files presently in a report table (two triangles: two report tables)

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

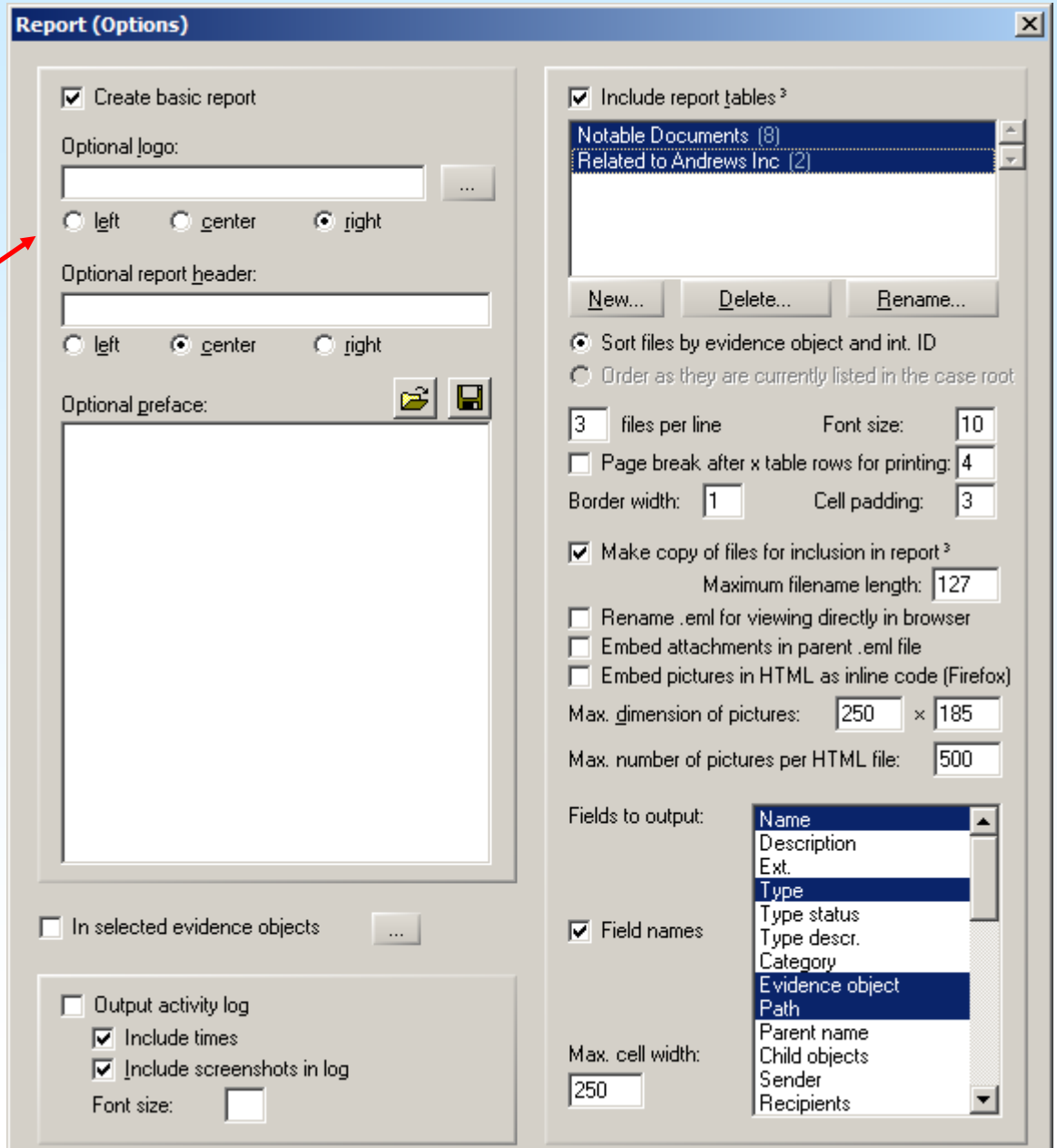
Note the keyboard shortcuts (e.g. Ctrl+1), which allow adding items to report tables without using the context menu.

3: Report Noteworthy Files

Step 2: Create Report

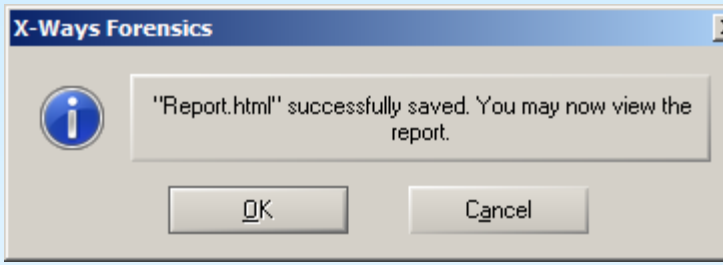


Select the option “Make copy of files for inclusion in report…”.
Ensure that “Include report tables” is checked.
Also select the fields to output according to your preferences.



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

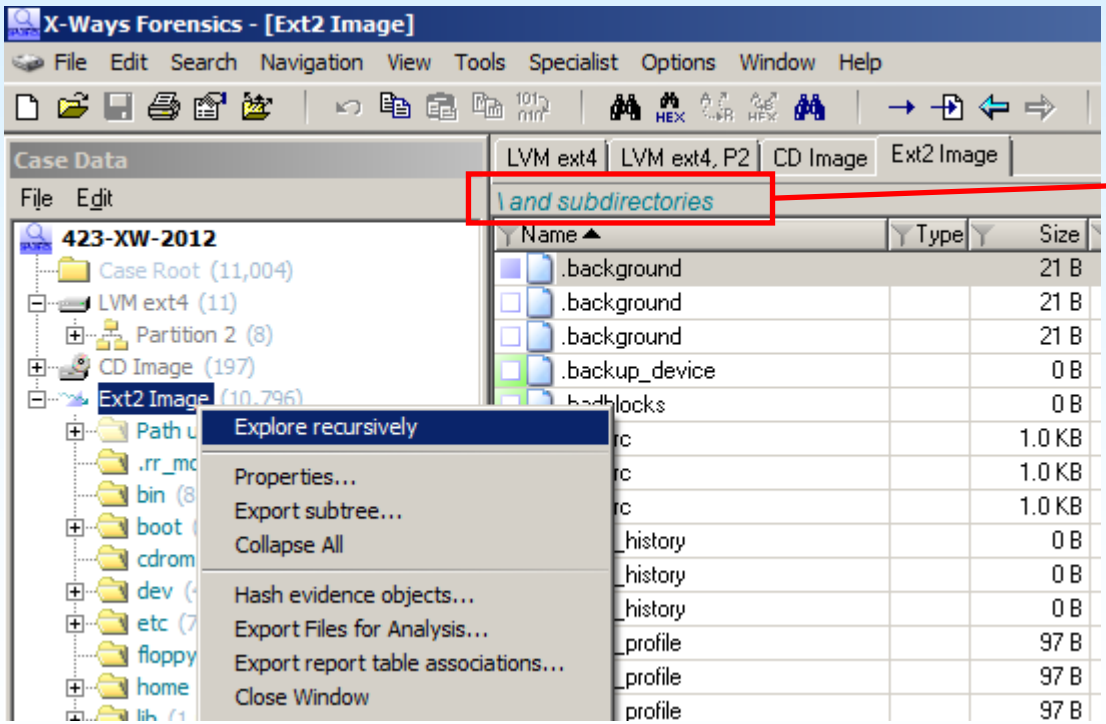
Notable Documents (8 items)

Name: **new-york-9400020.jpg** Type: jpg Evidence object: Ext2 Image Path: \home\dsl\Pictures\0003 Size: 18.6 KB	Name: **Manuel WinHex.doc** Type: doc Evidence object: Ext2 Image Path: \home\dsl\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.

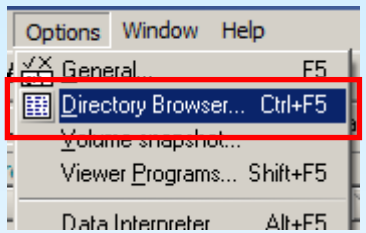


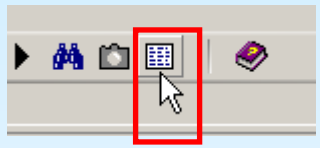
“and subdirectories” denotes recursive listings!

\ represents a partition's root directory

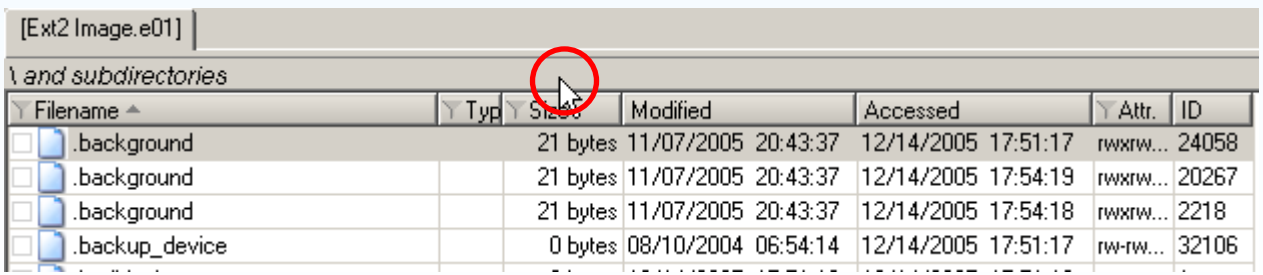
4: Filtering (Ex. Deleted JPEG Files)

Step 2: Open the directory browser options



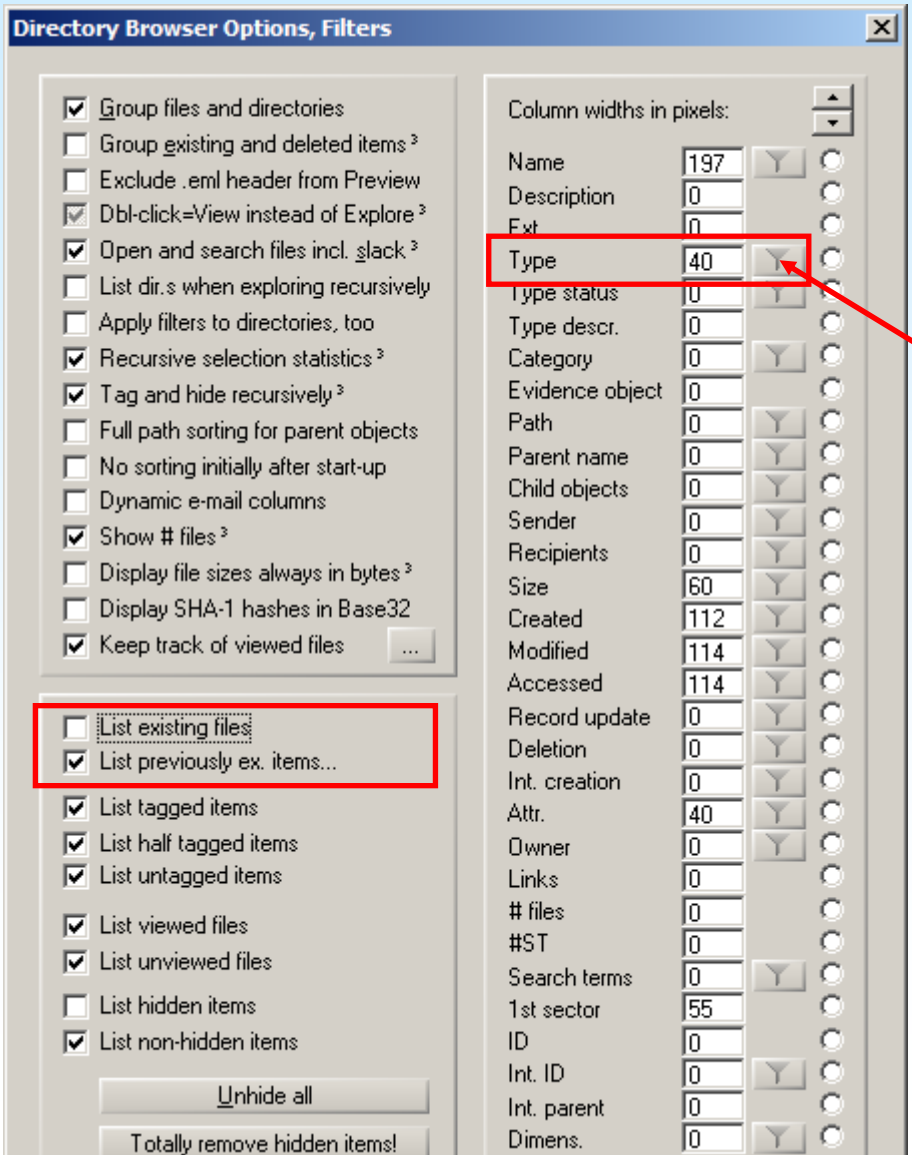


The directory browser options can be called either via their entry in the “Options” menu, the corresponding button in the toolbar or simply by clicking the directory browser’s title bar.



4: Filtering (Ex. Deleted JPEG Files)

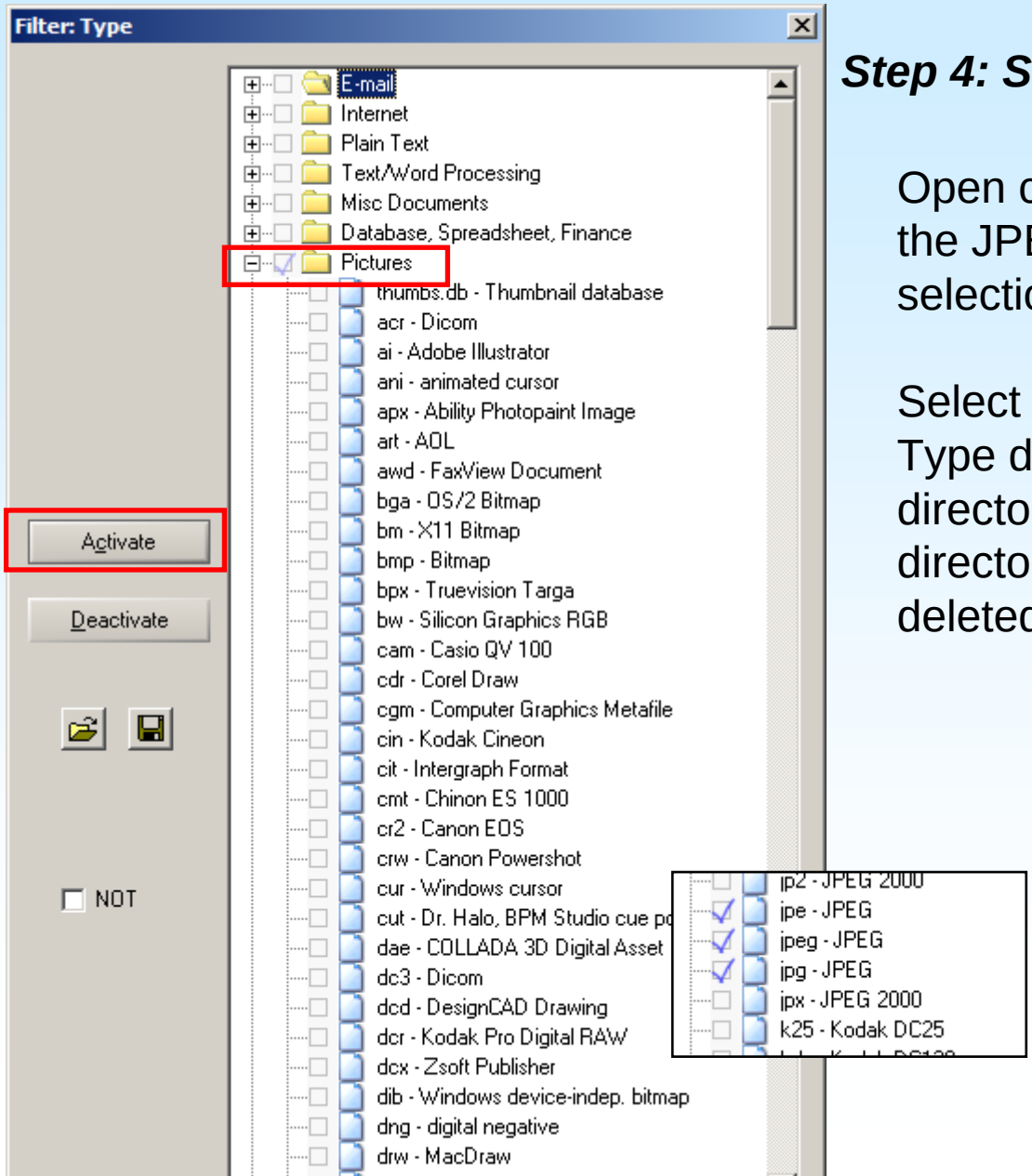
Step 3: Directory browser options



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)



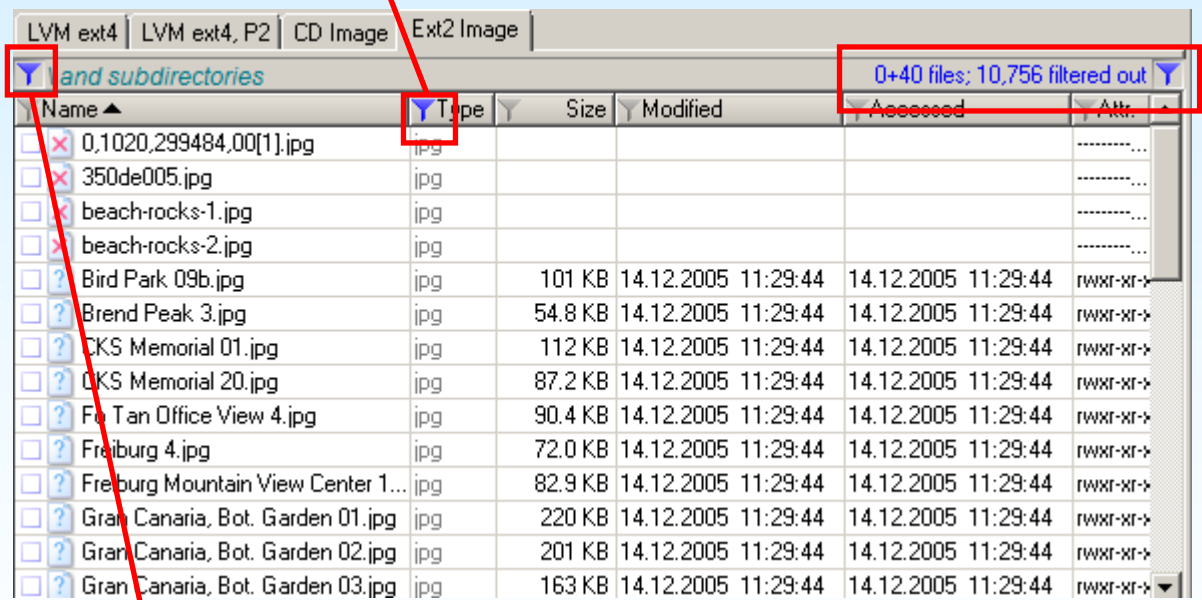
Step 4: Selecting the type

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)

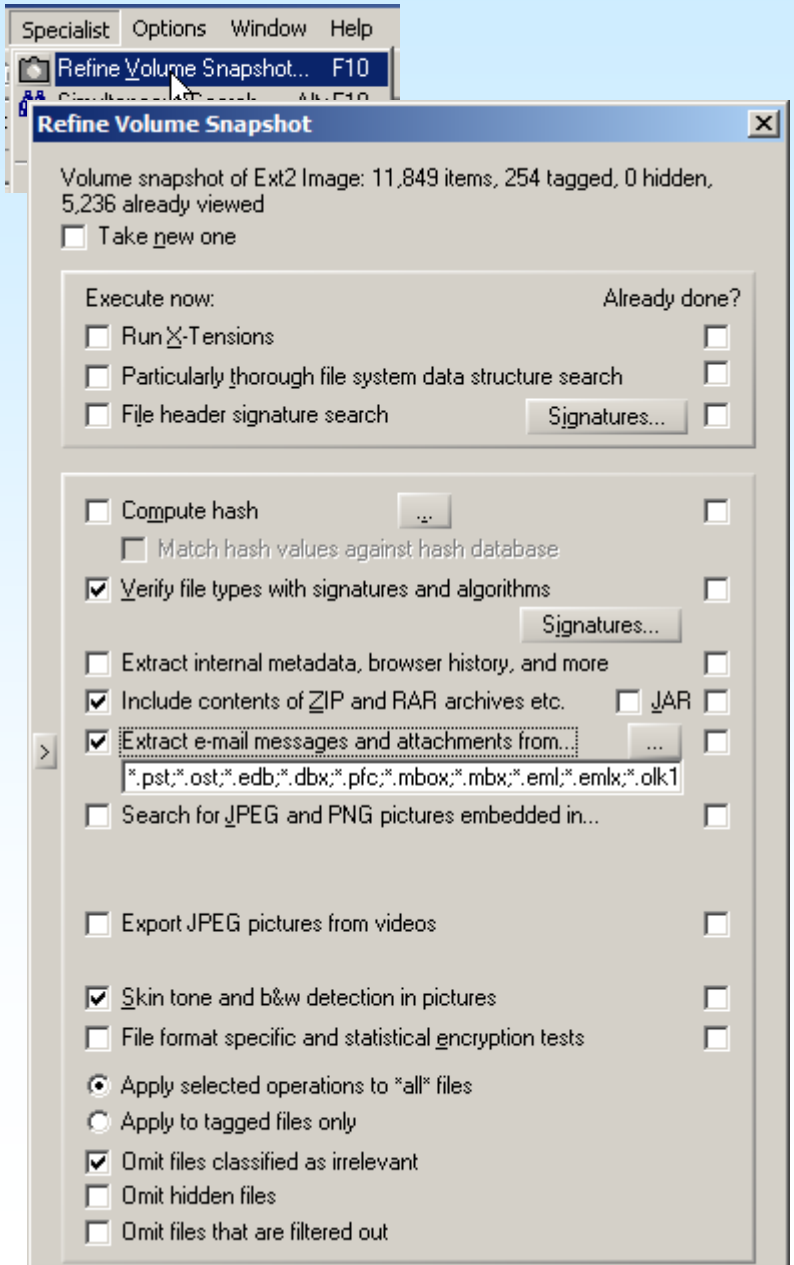
Quicker access to the column-based filters (e.g. to deactivate again)



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.

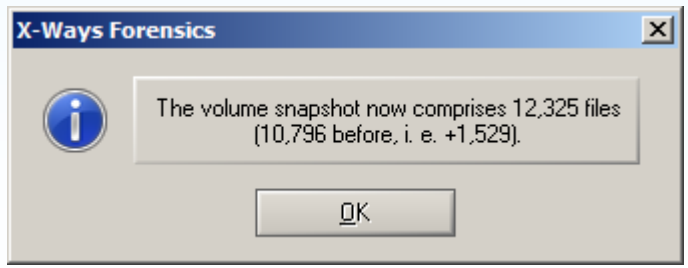
5: Refine Volume Snapshot



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.

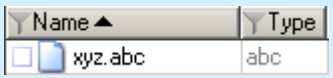
Check the desired options and click ok, which will eventually result in a message like the one below. Acknowledge with OK.



5: Refine Volume Snapshot

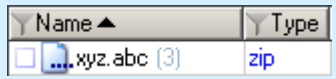
Sample Effects of the Refinement

Before:



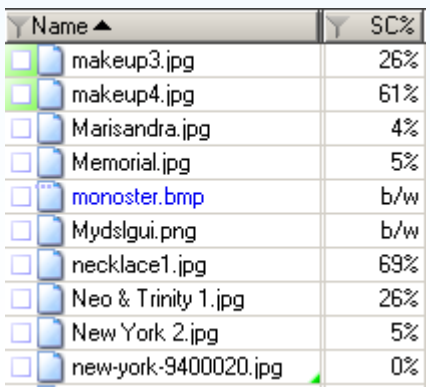
File is listed as specified by the file system – *Type* column simply assumes the extension

After:



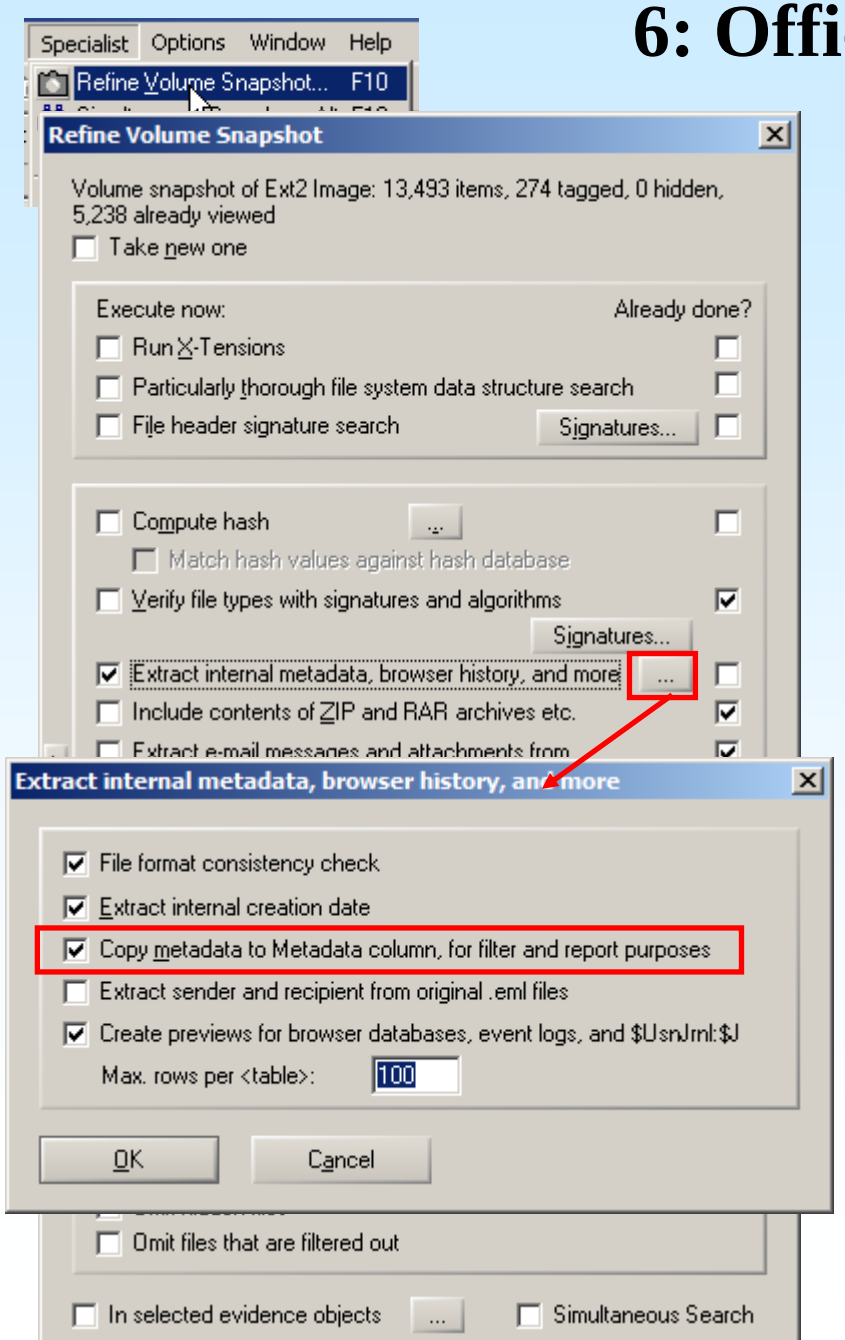
Type has been replaced by type identified from the file contents.
Since the file is an archive and listing their contents was amongst the options chosen, the …. in the icon shows there are now child objects present, the (3) after the name specifies the number of files inside.

Skin color and black-and-white detection:



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

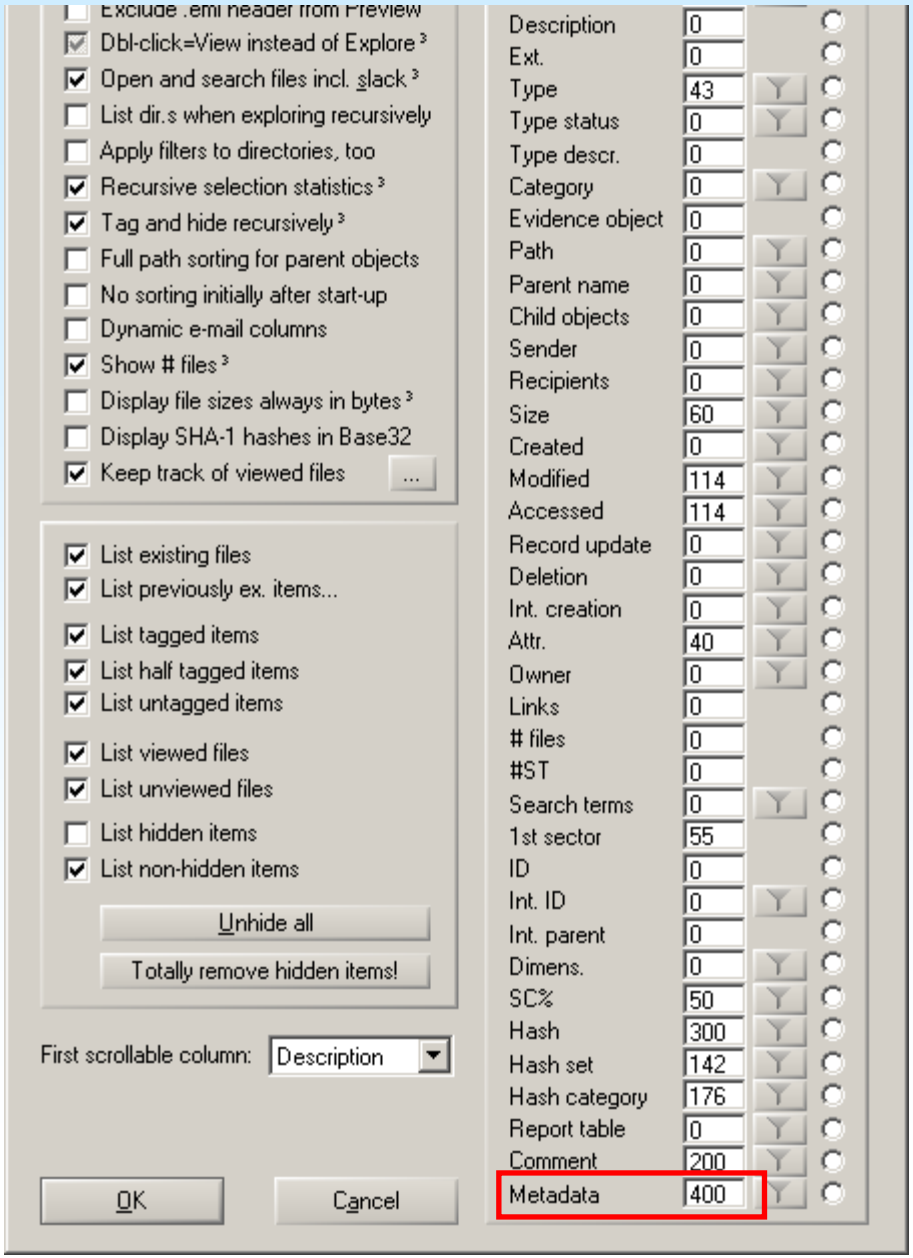
Press F10 or invoke “Refine Volume Snapshot” from the Specialist menu.

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



Step 2: Make Metadata column visible

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

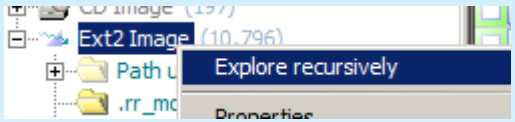
Open the directory browser options (cf. chapter 4, step 2).

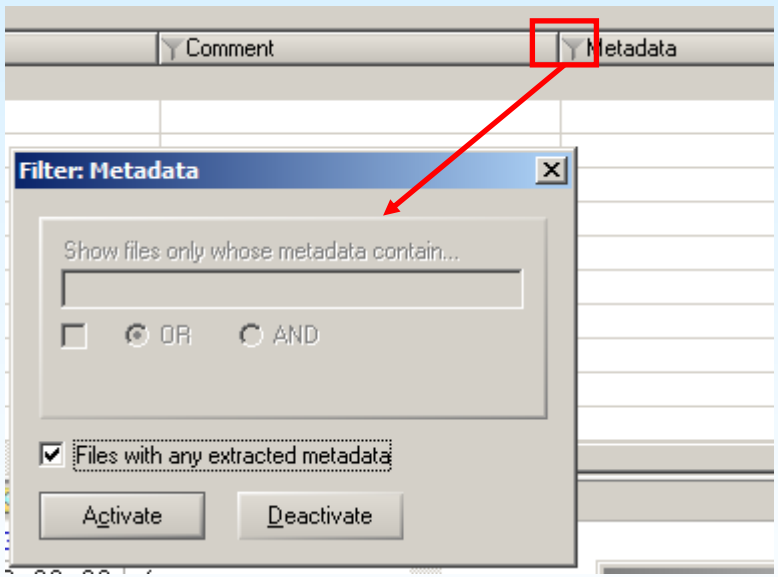
Enter a value in the box for "Metadata", e.g. 400.

[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

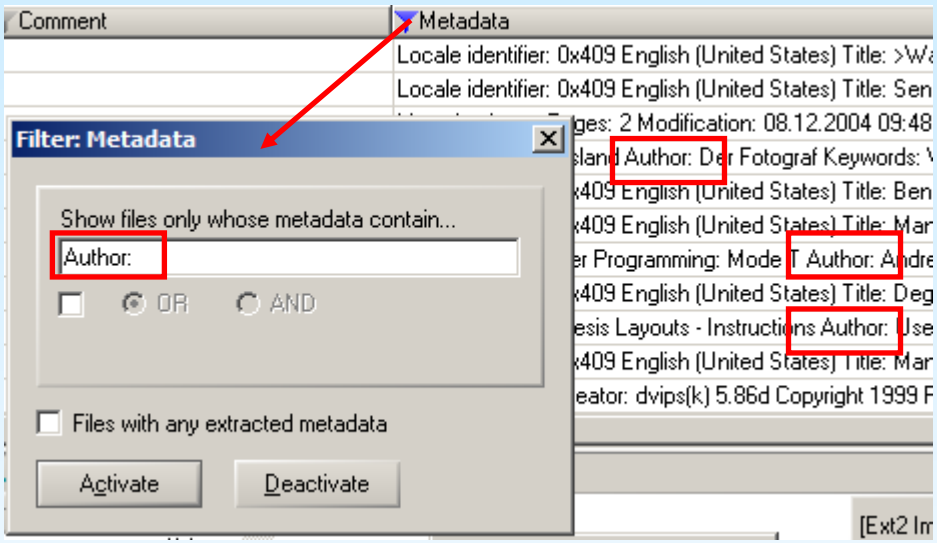
Explore the partition recursively (cf. chapter 4, step 1).

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.

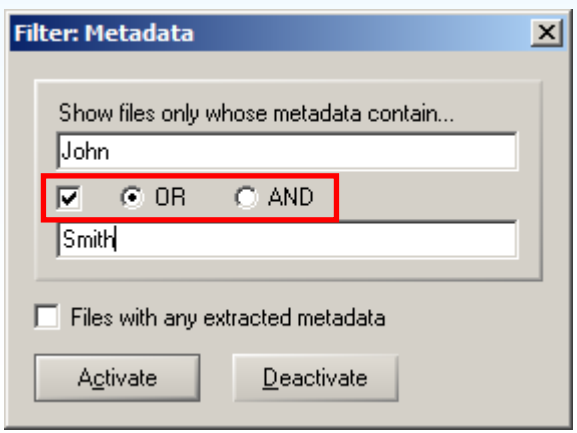
6: Office Metadata



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:".

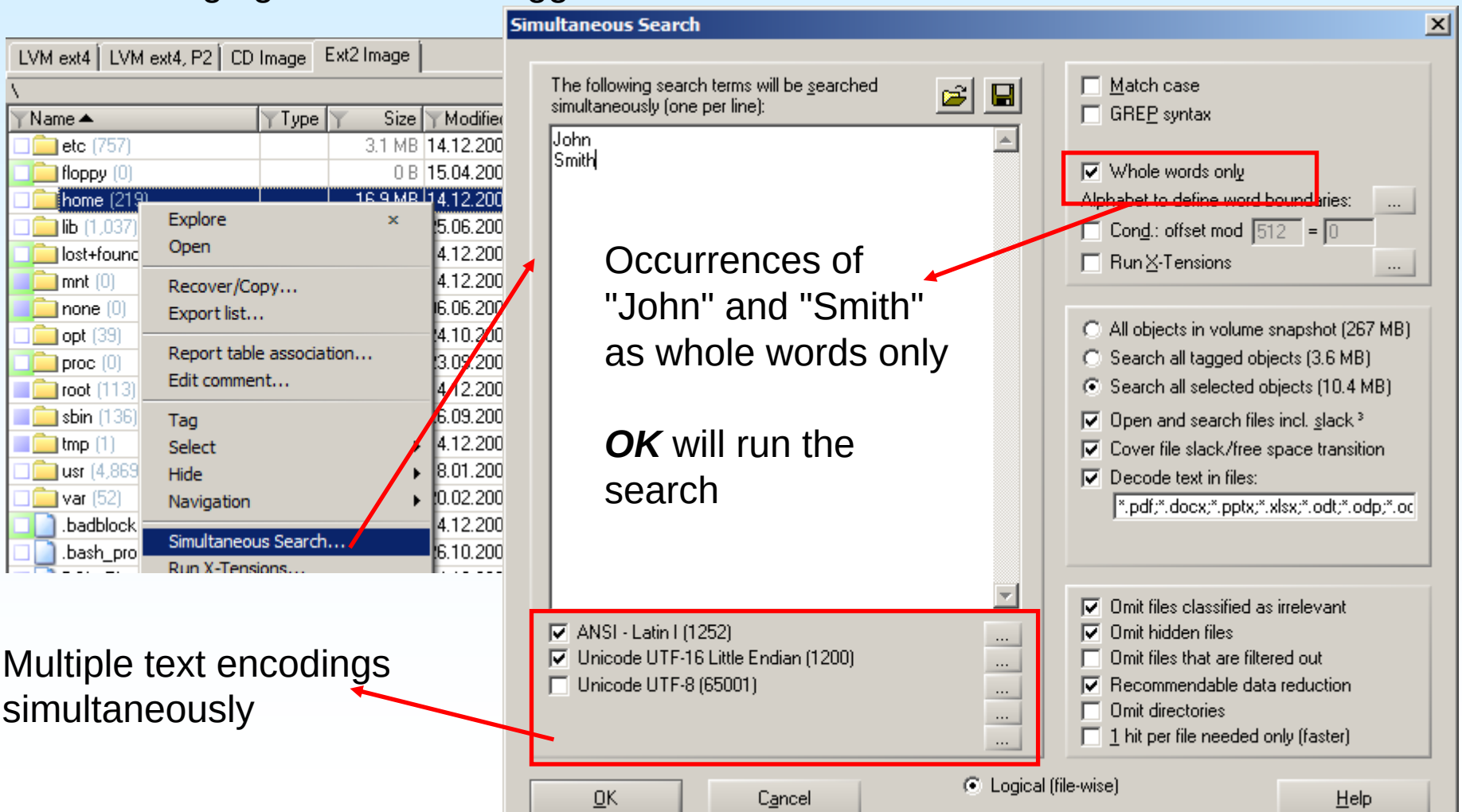


With the check box below the search term you can add a second text box. The two can then be combined with OR (all files whose Metadata field has at least one of the search terms) or AND (all files whose Metadata field contains both search terms) as required.

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

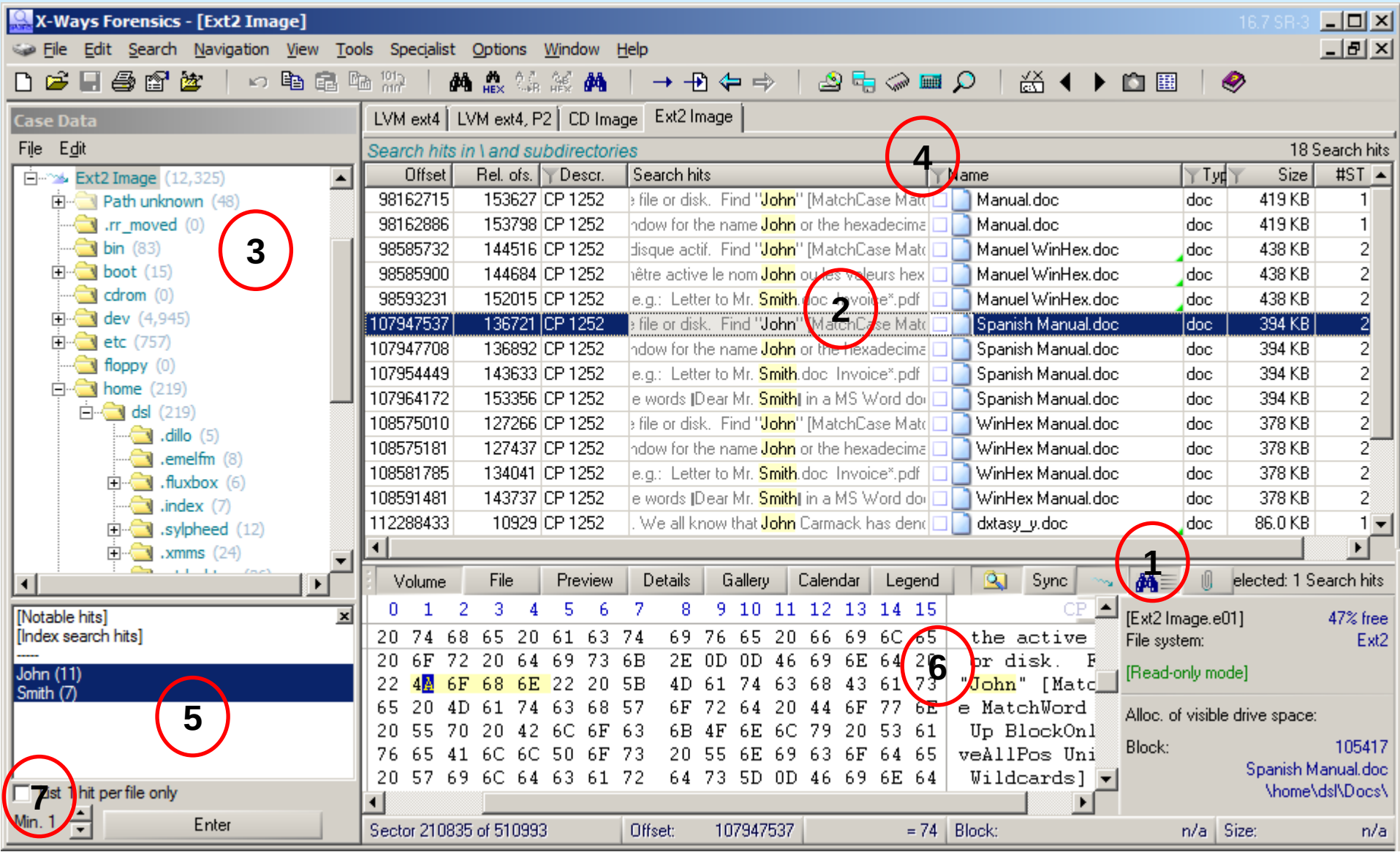
Step 1: Enter search terms and options

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



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

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



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

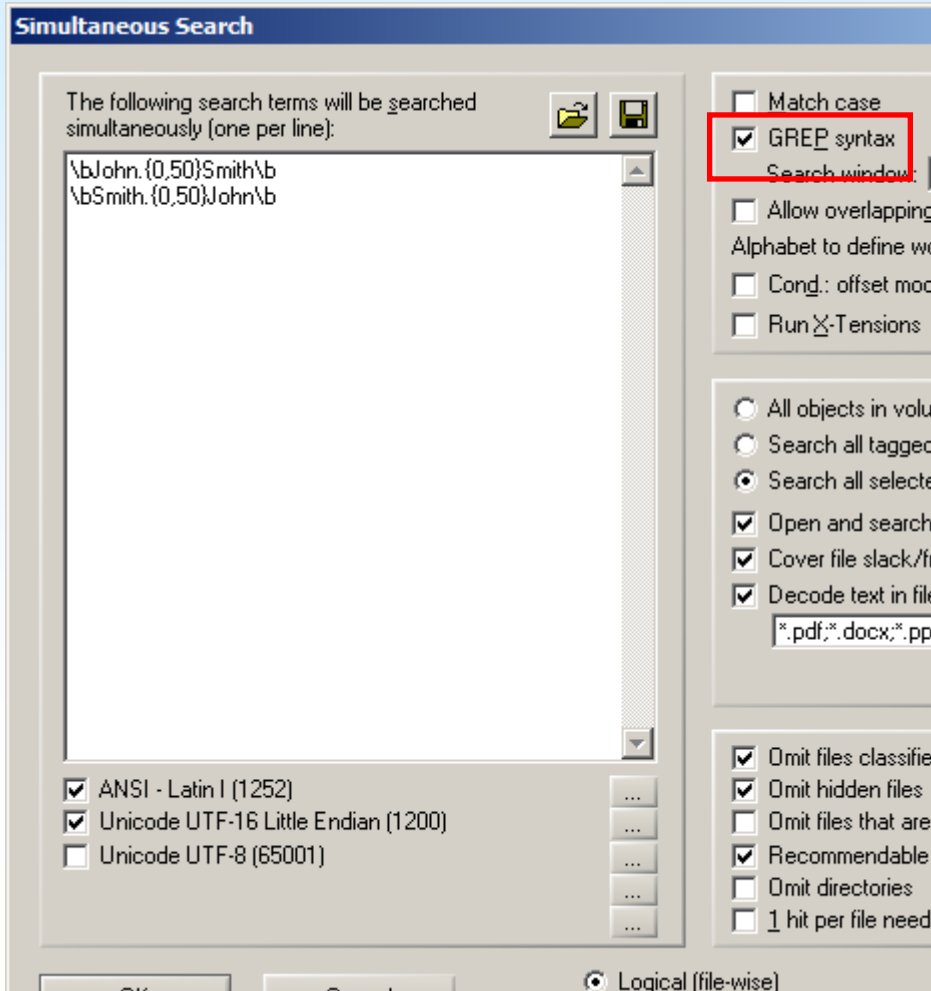
Instead of search for "John" and "Smith" as independent key words, GREP allows running a proximity search, i.e. requiring them to be found close together:

\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.



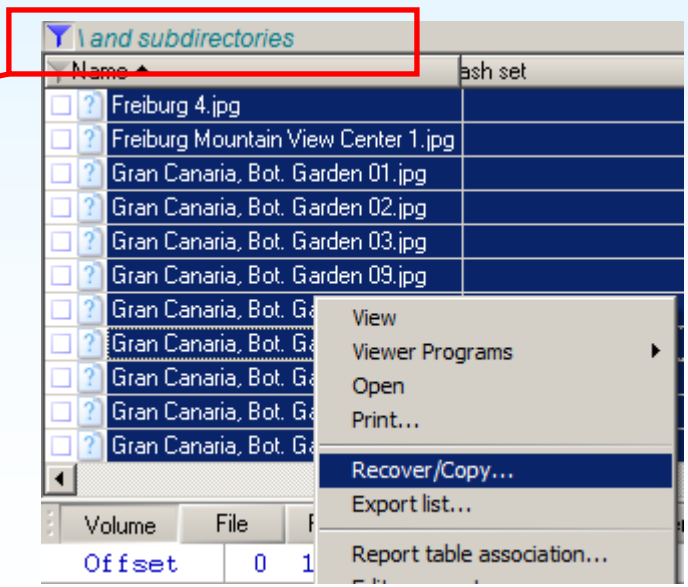
8: Copying Files

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

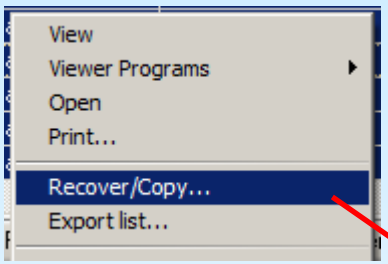
As an example, deleted JPEGs are filtered for (as shown in chapter 4) and using Ctrl+A all files are selected that meet the filter criteria. Right-click the selection to see the context menu:

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



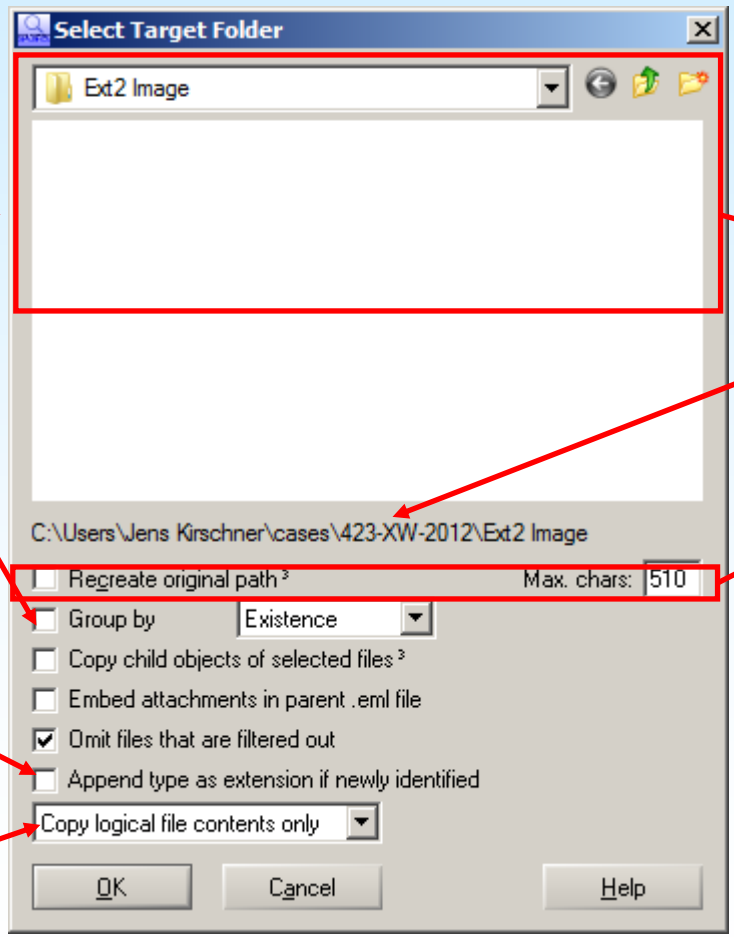
8: Copying Files

Step 2: Recover/Copy



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

Produces separate output directories, as per the grouping.



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

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

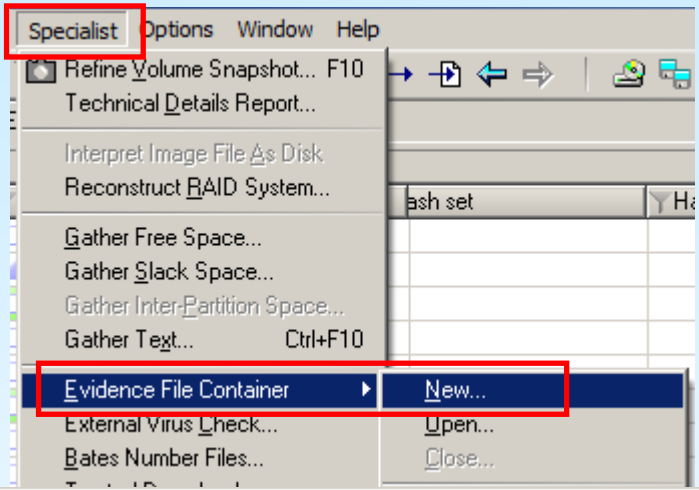
Reproduces within the output directory the paths as found at the origin (provided the maximum length is not exceeded).

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

9: Evidence File Container

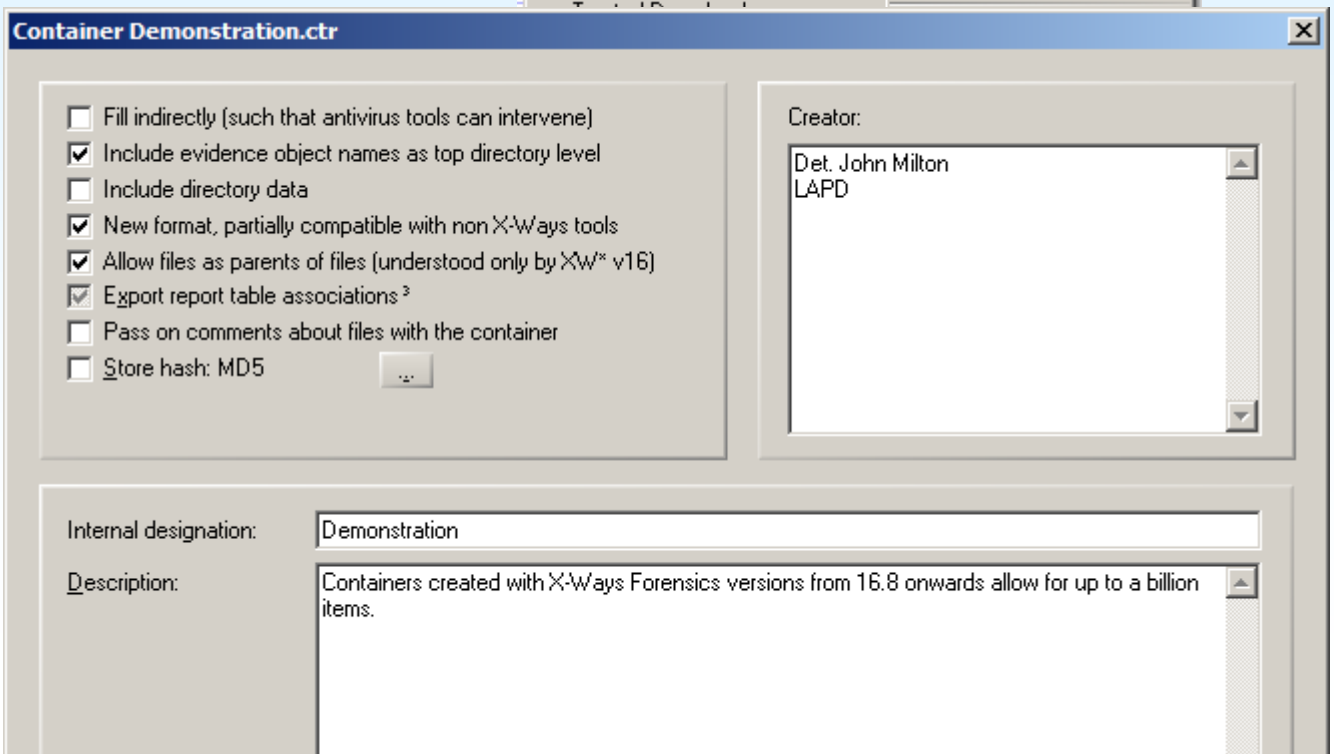
Step 1: Create the Evidence File Container

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



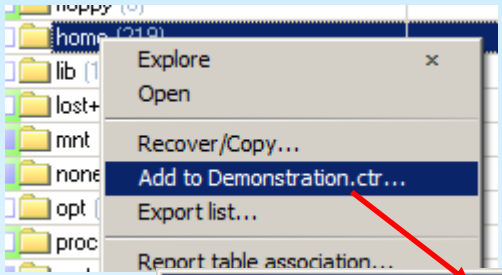
In the following file dialogue, choose the desired path and file name for the container. X-Ways Forensics will add the extension .ctr.

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.

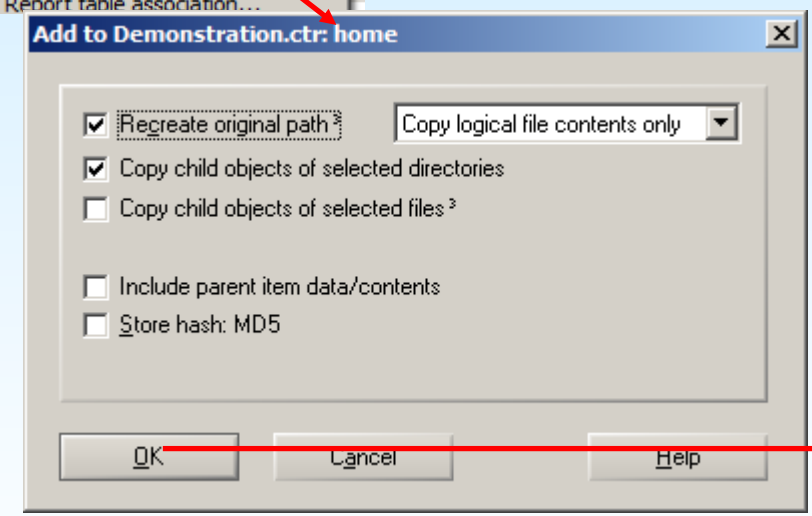


9: Evidence File Container

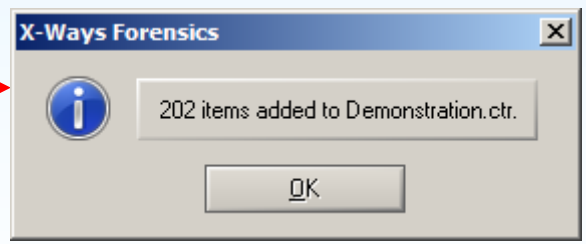
Step 2: Adding files to the container



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.



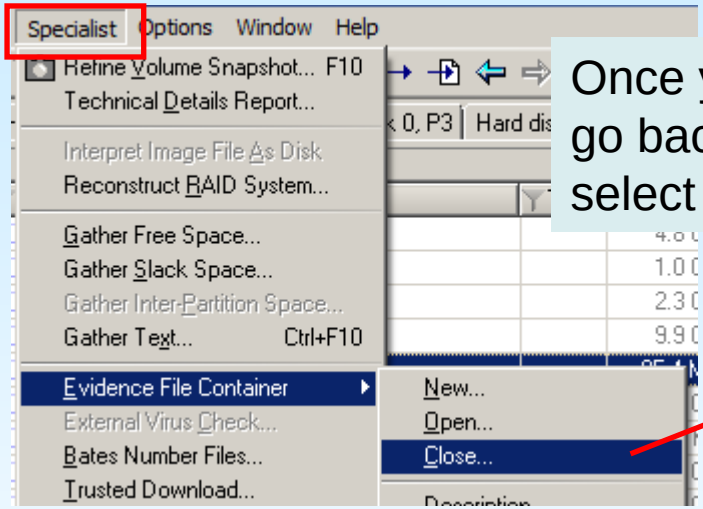
The options are similar to those of *Recover/Copy* as well, but no output directory is required, of course – and all files in the container are protected from interference by the operating system.



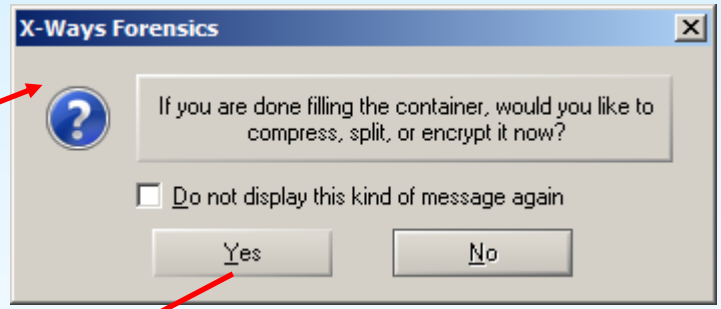
You can copy files from various sources into the same container. It does not matter whether the sources are media or images, or whether they are part of a case or have simply been opened standalone.

9: Evidence File Container

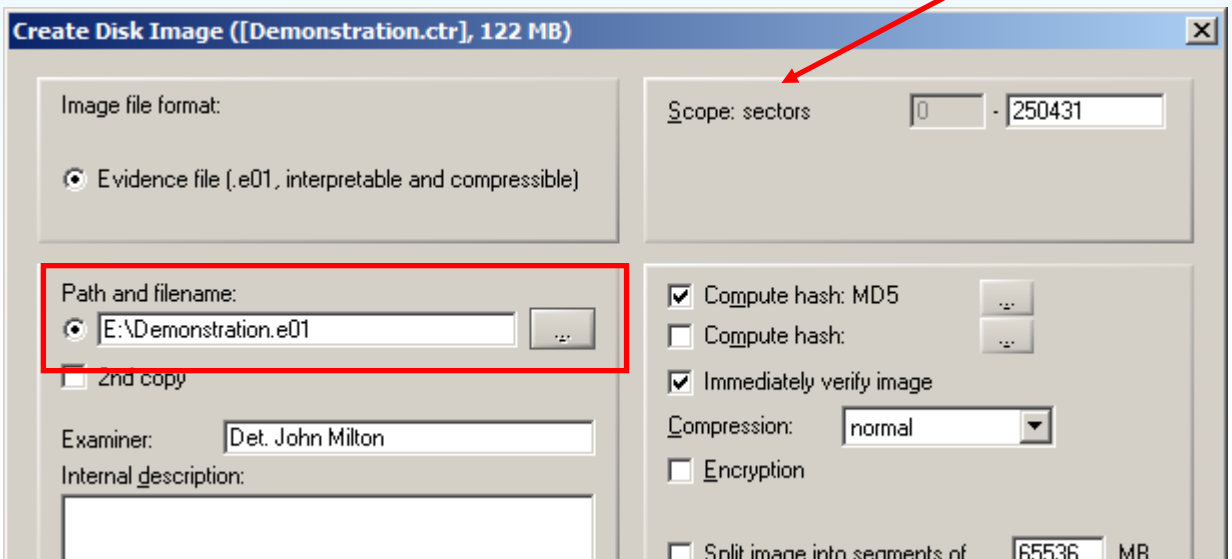
Step 3: Close the container



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



Click *Yes*.

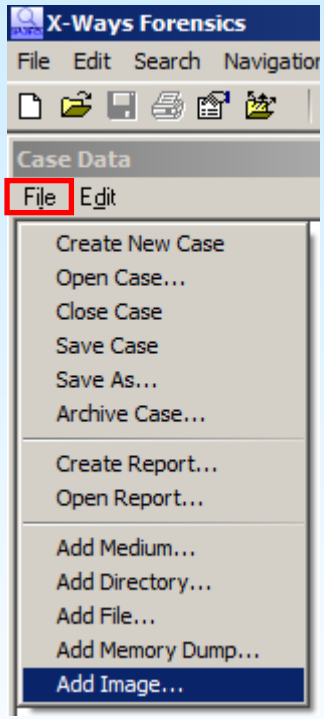


This dialogue is already known from chapter 1, step 2 – except here it is fixed to *Evidence file*.

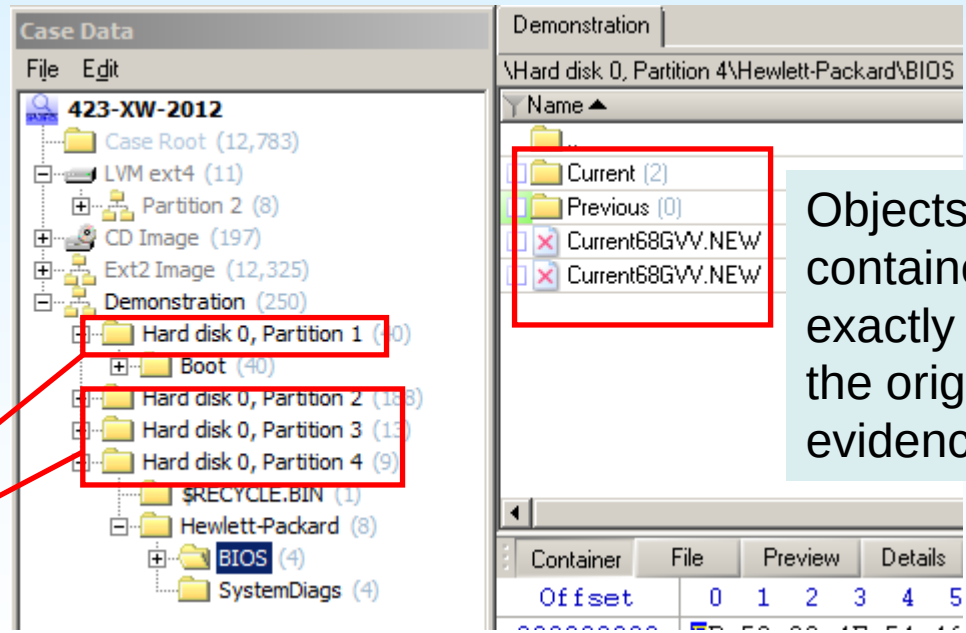
Specify an appropriate output destination and click OK.

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).



Objects in the container are shown exactly as found at the original source evidence item.

Original evidence sources are shown as the top-level directories