

X-Ways Forensics

Filtering

Example: Focus on all *deleted* files of type *JPG*

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 v14.9. Please subscribe to the newsletter to stay informed of updates to the software.

All rights including but not limited to reproduction reserved.

Step 1: Exploring recursively

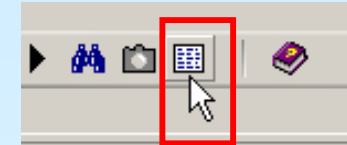
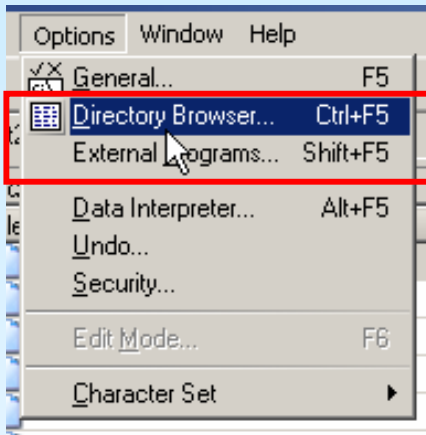
Right-click the volume in the directory tree and select “Explore recursively” from the context menu. This will generate a list of all files in all subdirectories.

The screenshot shows a forensic tool interface with a directory tree on the left and a file list on the right. The directory tree shows a volume named 'Ext2 Image.e01' selected. A context menu is open over this volume, with 'Explore recursively' selected. The file list on the right shows a list of files and directories. The header of the file list is highlighted with a red box, and the text '\and subdirectories' is highlighted within it. A red arrow points from this text to the explanatory text below.

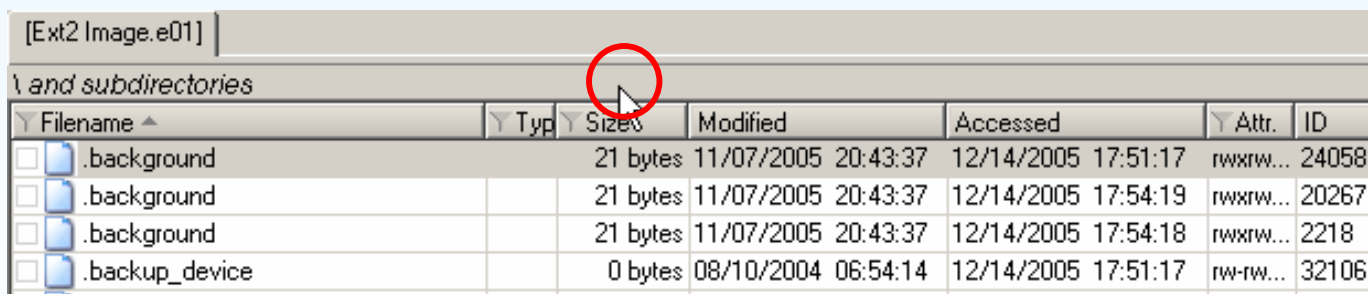
Filename	Type	Size	Modified	Accessed
.bash_profile		278 bytes	26.10.2005 18:09:45	14.12.2005
arch		2,4 KB	25.06.2005 13:45:08	14.12.2005
ash		108 KB	25.06.2005 13:45:08	14.12.2005
ash.static	static	139 KB	25.06.2005 13:45:08	14.12.2005
bash		0,7 MB	25.06.2005 13:45:08	14.12.2005
bsh		3 bytes	14.12.2005 17:51:18	14.12.2005
busybox		378 KB	25.06.2005 13:45:08	14.12.2005
cat		12 bytes	14.12.2005 17:54:12	14.12.2005
chgrp		12 bytes	14.12.2005 17:54:12	14.12.2005
chmod		12 bytes	14.12.2005 17:54:12	14.12.2005
chown		12 bytes	14.12.2005 17:54:12	14.12.2005
chroot		18 bytes	14.12.2005 17:54:12	14.12.2005
cp		41,8 KB	25.06.2005 13:45:08	14.12.2005
cpio		12 bytes	14.12.2005 17:54:12	14.12.2005
date		12 bytes	14.12.2005 17:54:12	14.12.2005
dd		12 bytes	14.12.2005 17:54:12	14.12.2005
df		12 bytes	14.12.2005 17:54:12	14.12.2005

“and subdirectories” denotes recursive listings!

Step 2: Calling the directory browser options



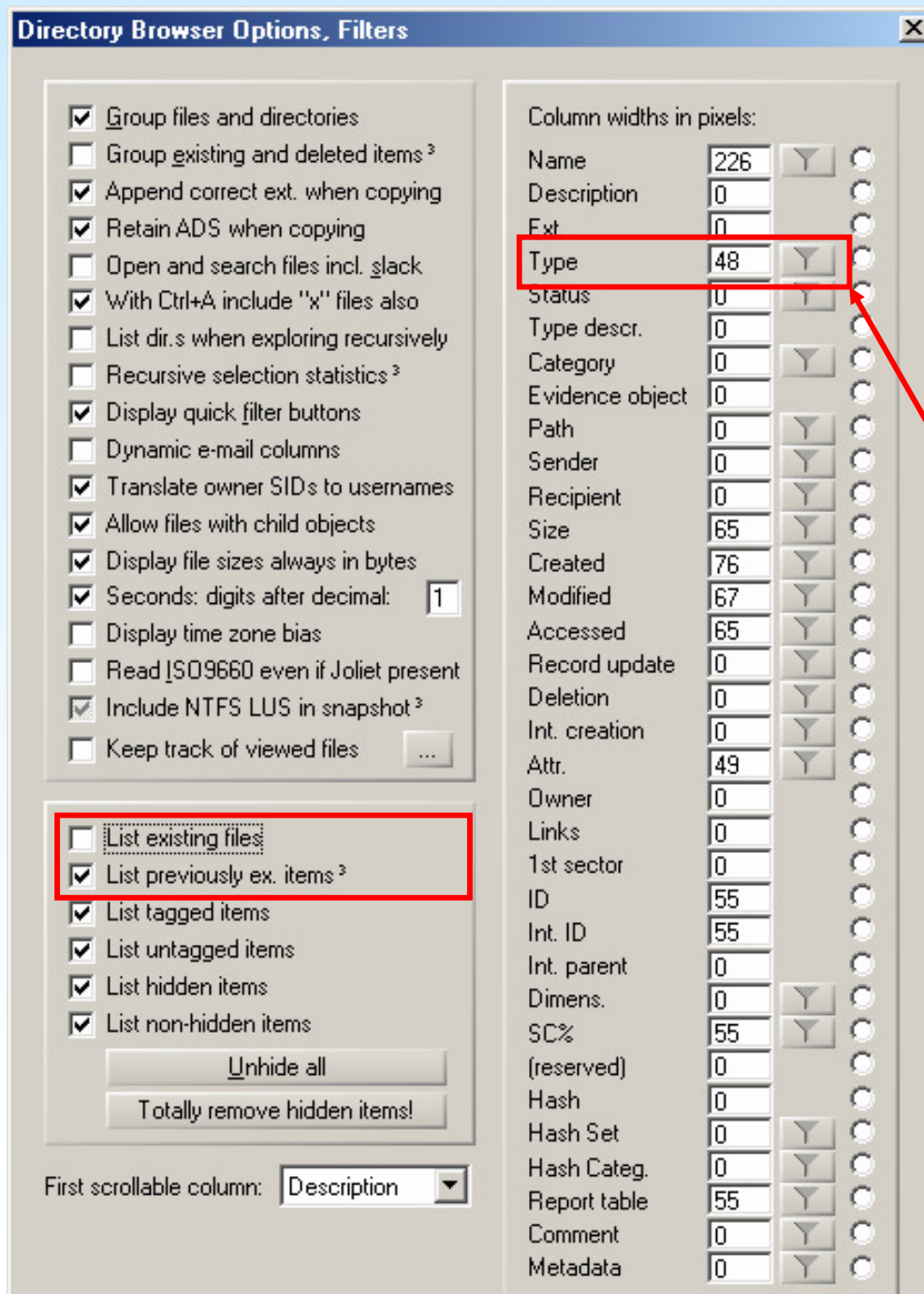
The directory browser options can be called either via their entry in the “Options” menu, the corresponding button in the toolbar or simply by clicking the directory browser’s title bar.




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 title bar of the table. The table has columns for 'Filename', 'Type', 'Size', 'Modified', 'Accessed', 'Attr.', and 'ID'. The files listed are '.background' (21 bytes) and '.backup_device' (0 bytes).

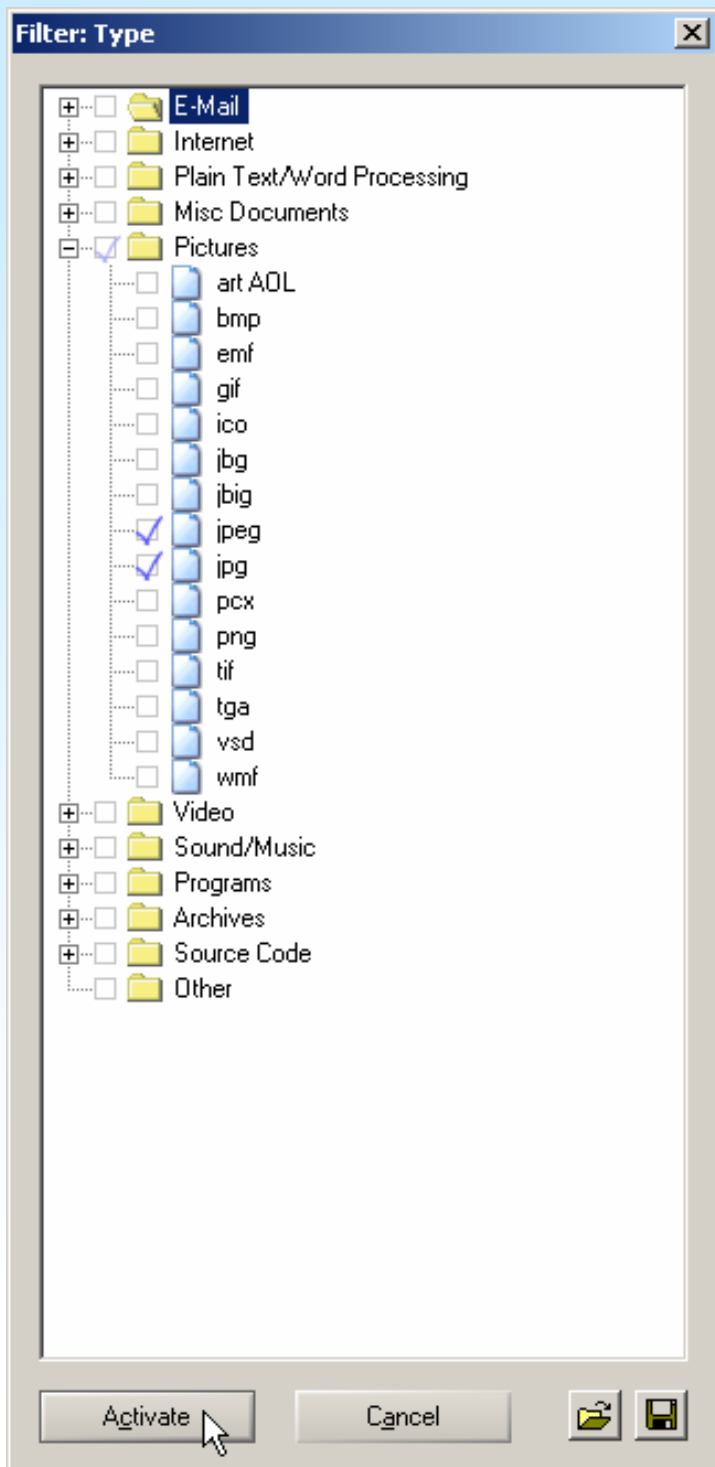
Filename	Type	Size	Modified	Accessed	Attr.	ID
.background		21 bytes	11/07/2005 20:43:37	12/14/2005 17:51:17	rw-rw...	24058
.background		21 bytes	11/07/2005 20:43:37	12/14/2005 17:54:19	rw-rw...	20267
.background		21 bytes	11/07/2005 20:43:37	12/14/2005 17:54:18	rw-rw...	2218
.backup_device		0 bytes	08/10/2004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

Step 3: Directory browser options



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

Then click the filter symbol for "Type":  The dialog for step 4 will come up.



Step 4: Selecting the type

Open category “Pictures” and check “jpeg” and “jpg”. Uncheck all the others, 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.

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

[Ext2 Image.e01]

Y \ and subdirectories

0+42=42 files, 0 dir.; 10,756

Filename	Type	Size	Modified	Accessed	Attr.	ID
0,1020,299484,00[1].jpg	jpg				-----	0
350de005.jpg	jpg				-----	0
beach-rocks-1.jpg	jpg				-----	0
beach-rocks-2.jpg	jpg				-----	0
Bird Park 09b.jpg	jpg	101 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20323
Brend Peak 3.jpg	jpg	54.8 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20324
CKS Memorial 01.jpg	jpg	112 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20325
CKS Memorial 20.jpg	jpg	87.2 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20326
Fo Tan Office View 4.jpg	jpg	90.4 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20327
Freiburg 4.jpg	jpg	72.0 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20328
Freiburg Mountain View Center 1.jpg	jpg	82.9 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20329
Gran Canaria, Bot. Garden 01.jpg	jpg	220 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20330
Gran Canaria, Bot. Garden 02.jpg	jpg	201 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20331
Gran Canaria, Bot. Garden 03.jpg	jpg	163 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20332
Gran Canaria, Bot. Garden 09.jpg	jpg	180 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20333
Gran Canaria, Bot. Garden 10.jpg	jpg	174 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20334
Gran Canaria, Bot. Garden 12.jpg	jpg	164 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20335
Gran Canaria, Bot. Garden 14.jpg	jpg	193 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20336
Gran Canaria, Bot. Garden 20.jpg	jpg	119 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20337
Gran Canaria, Bot. Garden 30.jpg	jpg	139 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20338
Gran Canaria, Rus trin 33 inn	inn	65.3 KB	12/14/2005 12:29:44	12/14/2005 12:29:44	rwxr-x...	20339

Gives details about the filters' effects: 42 previously existing files are currently displayed (no existing files, no directories).

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