

X-Ways Forensics

Filtern

Beispiel: Auflisten von *gelöschten JPEG-Dateien*

X-Ways Software Technology AG
Carl-Diem-Str. 32
32257 Bünde
Web: <http://www.x-ways.net>

X-Ways Software Technology AG
Agrippastr. 37-39
50676 Köln
E-Mail: mail@x-ways.com

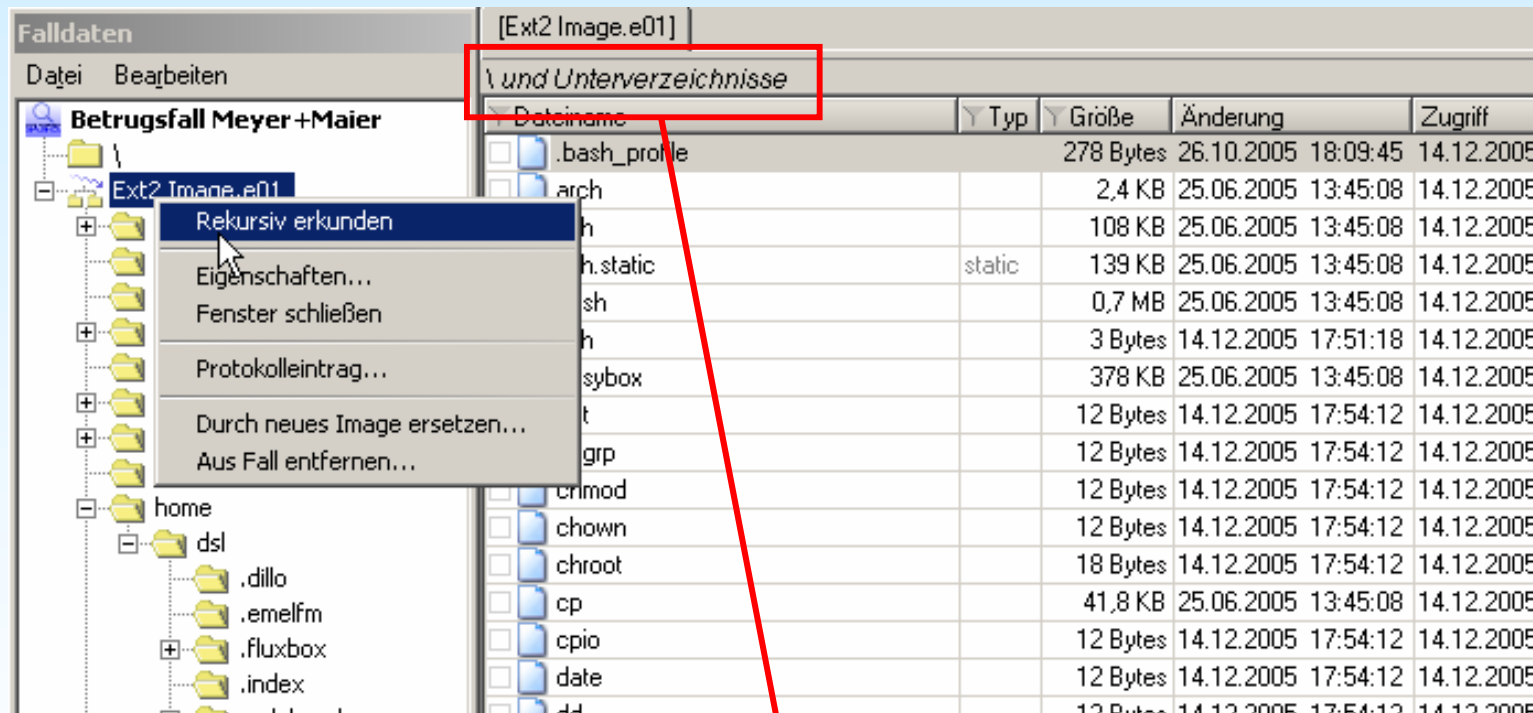
Tel.: 0221-420 486 5

Stand: v14.9. Bitte abonnieren Sie den Newsletter, um über Neuerungen in der Software informiert zu werden.

Alle Rechte, insbes. der Vervielfältigung, vorbehalten.

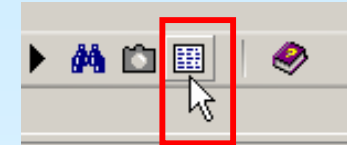
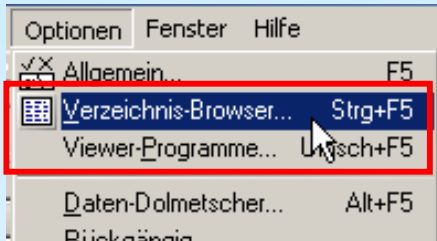
Schritt 1: Rekursiv erkunden

Klicken Sie das Asservat im Fallbaum mit der rechten Maustaste an und wählen Sie „Rekursiv erkunden“. Dies zeigt den Inhalt aller Unterverzeichnisse.

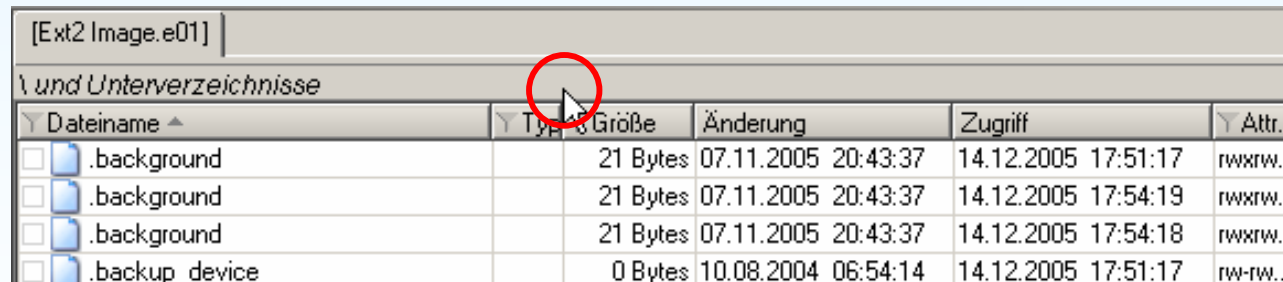


„und Unterverzeichnisse“ kennzeichnet rekursive Auflistungen!

Schritt 2: Aufruf der Verzeichnis-Browser-Optionen



Die Verzeichnis-Browser-Optionen können entweder über ihren Eintrag im Optionen-Menü, den entsprechenden Button in der Werkzeugleiste oder einfach durch Klicken auf die Titelzeile des Verzeichnis-Browsers aufgerufen werden.



A screenshot of a file explorer window titled '[Ext2 Image.e01]'. The window shows a table of files and subdirectories. The table has columns for 'Dateiname', 'Typ', 'Größe', 'Änderung', 'Zugriff', and 'Attr.'. A red circle highlights the 'Dateiname' column header. A mouse cursor is pointing at the first row of the table.

Dateiname	Typ	Größe	Änderung	Zugriff	Attr.
.background		21 Bytes	07.11.2005 20:43:37	14.12.2005 17:51:17	rwxrw..
.background		21 Bytes	07.11.2005 20:43:37	14.12.2005 17:54:19	rwxrw..
.background		21 Bytes	07.11.2005 20:43:37	14.12.2005 17:54:18	rwxrw..
.backup_device		0 Bytes	10.08.2004 06:54:14	14.12.2005 17:51:17	rw-rw..

Schritt 3: Verzeichnis-Browser-Optionen

Verzeichnis-Browser-Optionen, Filter

Verz. und Dateien gruppieren
 Existent und gelöscht gruppieren³
 Beim Kopieren mit Endung versehen
 ADS beim Kopieren beibehalten
 Schlupf öffnen und durchsuchen
 Mit Strg+A auch "x"-Dateien ausw.
 Rekursiv auch Verz. mit ausgeben
 Rekursive Auswahlstatistik³
 Filter in Spaltenüberschriften
 Dynamische E-Mail-Spalten
 Benutzernamen statt Besitzer-SIDs
 Dateien mit Unterobjekten erlauben
 Dateigrößen immer in Bytes zeigen
 Dezimalstellen hinter Sekunden:
 Abstand von UTC-Zeit anzeigen
 ISO9660 zusätzl. zu Joliet einlesen
 NTFS-LUS in Überblick aufnehmen³
 Eingesehene Dateien merken ...


Existierende Dateien anzeigen
 Ehem. exist. Objekte anzeigen³
 Markierte Objekte anzeigen
 Nicht markierte Objekte anzeigen
 Unterdrückte Objekte anzeigen
 Nicht unterdrückte Objekte anzeigen

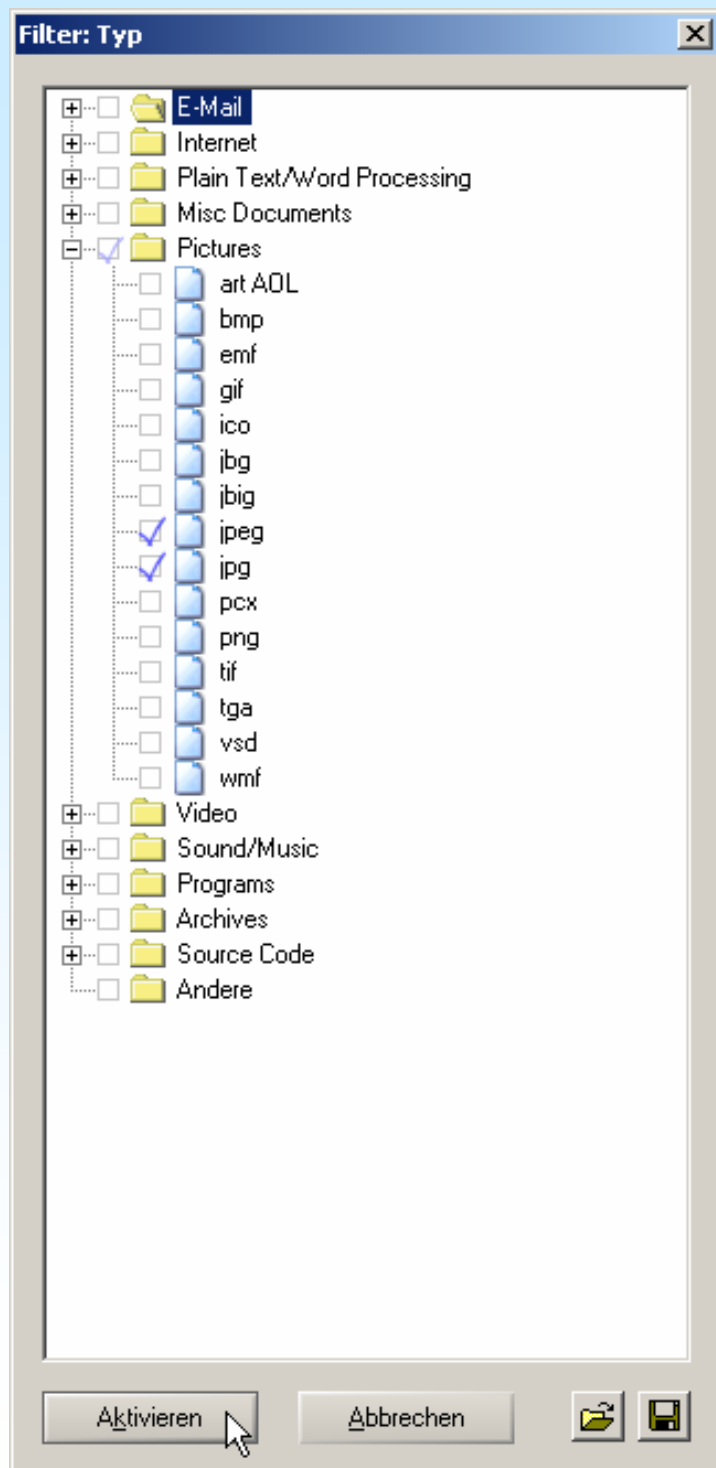
Erste rollbare Spalte:

Spaltenbreiten in Pixeln:

Name	<input type="text" value="226"/>	<input type="button" value="Y"/>	<input type="radio"/>
Beschreibung	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Erw	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Typ	<input type="text" value="48"/>	<input type="button" value="Y"/>	<input type="radio"/>
Status	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Typbeschreibung	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Kategorie	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Asservat	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Pfad	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Absender	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Empfänger	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Größe	<input type="text" value="65"/>	<input type="button" value="Y"/>	<input type="radio"/>
Erzeugung	<input type="text" value="76"/>	<input type="button" value="Y"/>	<input type="radio"/>
Änderung	<input type="text" value="67"/>	<input type="button" value="Y"/>	<input type="radio"/>
Zugriff	<input type="text" value="65"/>	<input type="button" value="Y"/>	<input type="radio"/>
Record-Änderung	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Löschzeitpunkt	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Int. Erzeugung	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Attr.	<input type="text" value="49"/>	<input type="button" value="Y"/>	<input type="radio"/>
Besitzer	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Verweise	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
1. Sektor	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
ID	<input type="text" value="55"/>	<input type="button" value="Y"/>	<input type="radio"/>
Int. ID	<input type="text" value="55"/>	<input type="button" value="Y"/>	<input type="radio"/>
Int. Elter	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Pixel	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
HFA	<input type="text" value="55"/>	<input type="button" value="Y"/>	<input type="radio"/>
(reserviert)	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Hash	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Hash-Set	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Hash-Kategorie	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Berichtstabelle	<input type="text" value="55"/>	<input type="button" value="Y"/>	<input type="radio"/>
Kommentar	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>
Metadaten	<input type="text" value="0"/>	<input type="button" value="Y"/>	<input type="radio"/>

Um nur gelöschte Dateien zu erhalten, entfernen Sie das Häkchen bei „Existierende Dateien anzeigen“.

Dann klicken Sie auf das Filter-symbol für „Typ“:  Das Dialogfenster für Schritt 4 wird geöffnet.

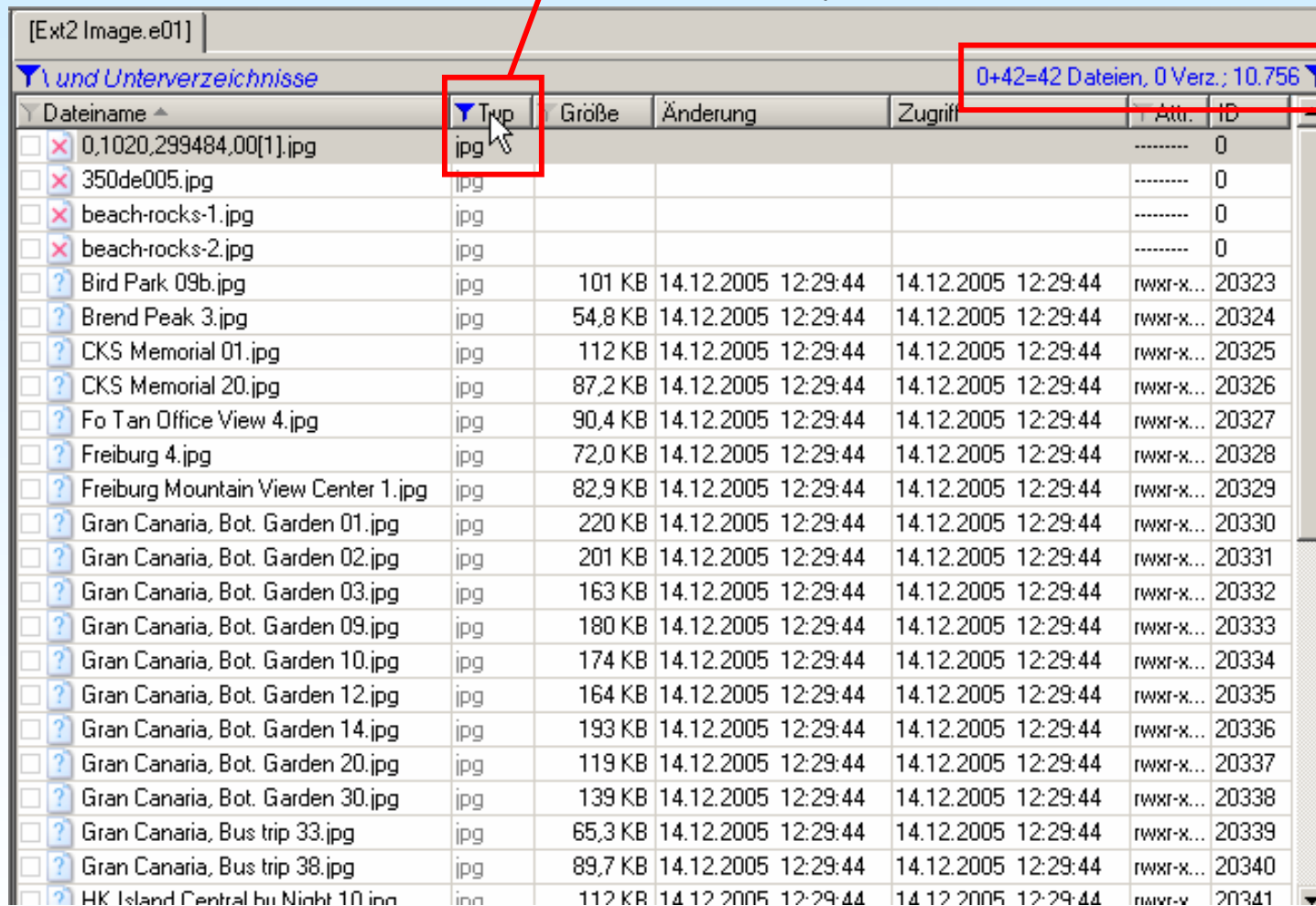


Schritt 4: Auswahl des Typs

Öffnen Sie die Kategorie „Pictures“ und markieren Sie „jpeg“ und „jpg“. Nehmen Sie alle übrigen Markierungen weg, falls erforderlich.

Klicken Sie auf „Aktivieren“ um den Dialog „Filter: Typ“ zu schließen und dann OK um die Verzeichnis-Browser-Optionen zu schließen. Der Verzeichnis-Browser wird jetzt nur noch gelöschte Dateien vom Typ JPG/JPEG zeigen.

Schnellerer Zugriff auf die Spalten-basierenden Filter (z.B. um diese wieder zu deaktivieren)



Dateiname	Typ	Größe	Änderung	Zugriff	Attr.	ID
<input checked="" type="checkbox"/> 0,1020,299484,00[1].jpg	jpg				-----	0
<input checked="" type="checkbox"/> 350de005.jpg	jpg				-----	0
<input checked="" type="checkbox"/> beach-rocks-1.jpg	jpg				-----	0
<input checked="" type="checkbox"/> beach-rocks-2.jpg	jpg				-----	0
<input type="checkbox"/> ? Bird Park 09b.jpg	jpg	101 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20323
<input type="checkbox"/> ? Brend Peak 3.jpg	jpg	54,8 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20324
<input type="checkbox"/> ? CKS Memorial 01.jpg	jpg	112 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20325
<input type="checkbox"/> ? CKS Memorial 20.jpg	jpg	87,2 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20326
<input type="checkbox"/> ? Fo Tan Office View 4.jpg	jpg	90,4 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20327
<input type="checkbox"/> ? Freiburg 4.jpg	jpg	72,0 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20328
<input type="checkbox"/> ? Freiburg Mountain View Center 1.jpg	jpg	82,9 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20329
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 01.jpg	jpg	220 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20330
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 02.jpg	jpg	201 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20331
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 03.jpg	jpg	163 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20332
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 09.jpg	jpg	180 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20333
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 10.jpg	jpg	174 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20334
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 12.jpg	jpg	164 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20335
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 14.jpg	jpg	193 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20336
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 20.jpg	jpg	119 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20337
<input type="checkbox"/> ? Gran Canaria, Bot. Garden 30.jpg	jpg	139 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20338
<input type="checkbox"/> ? Gran Canaria, Bus trip 33.jpg	jpg	65,3 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20339
<input type="checkbox"/> ? Gran Canaria, Bus trip 38.jpg	jpg	89,7 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20340
<input type="checkbox"/> ? HK Island Central bu Nicht 10 inn	inn	112 KB	14.12.2005 12:29:44	14.12.2005 12:29:44	rwxr-x...	20341

Zeigt Details über die Effekte der Filter an: 42 ehemals existierende Dateien werden derzeit angezeigt (keine existierenden, keine Verzeichnisse).

10.756 zusätzliche Dateien wurden herausgefiltert (werden nicht aufgelistet)