

# *X-Ways Forensics*

## Kurzanleitung

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](mailto:mail@x-ways.com)

Tel.: 0221-420 486 5

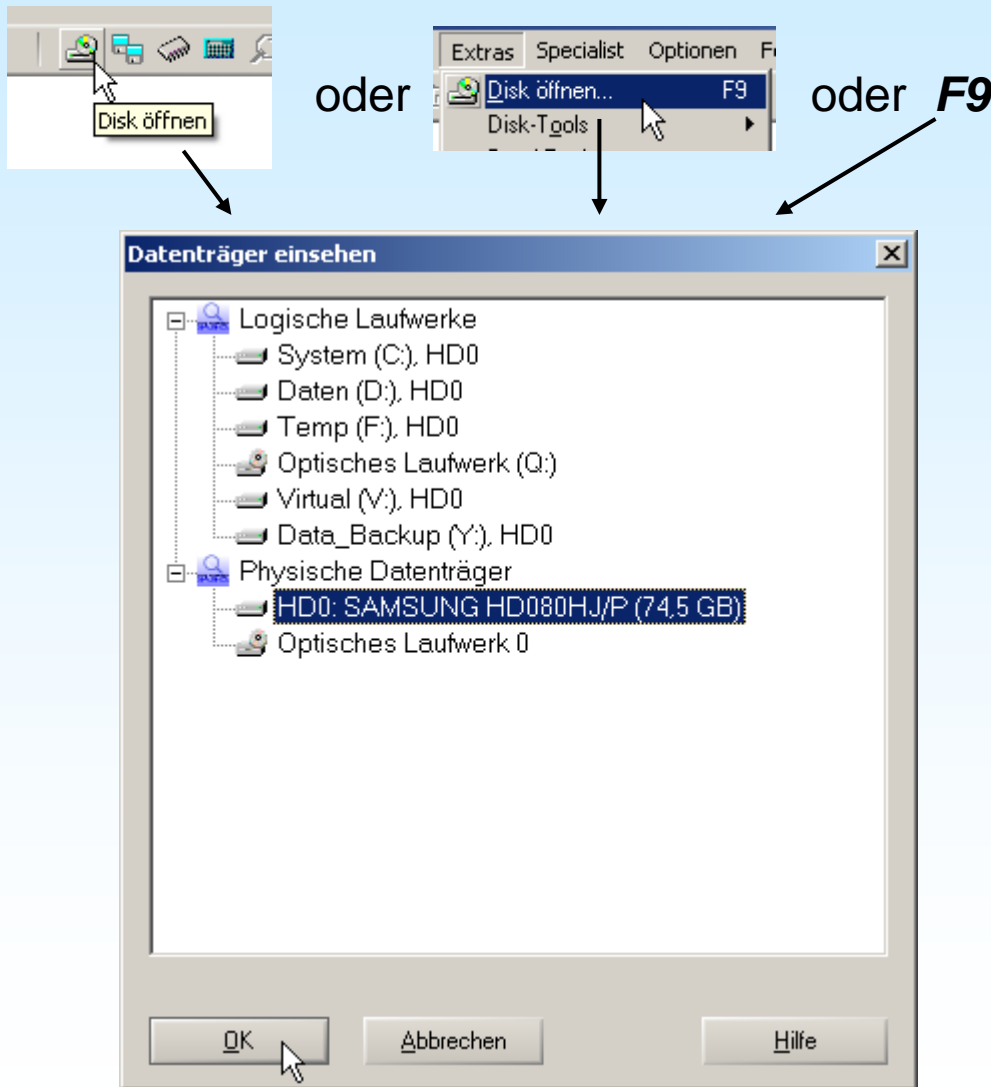
Stand: v16.7. Bitte abonnieren Sie den Newsletter, um über Neuerungen in der Software informiert zu werden.

**Alle Rechte, insbes. der Vervielfältigung, vorbehalten.**

# Inhaltsübersicht

|   |    |
|---|----|
| 1: Images erstellen.....                      | 3  |
| 2: Fall erzeugen, Images hinzufügen.....      | 6  |
| 3: Berichten wichtiger Dateien.....           | 11 |
| 4: Filtern (Bsp. gelöschte JPEG-Dateien)..... | 16 |
| 5: Datei-Überblick erweitern.....             | 21 |
| 6: Office-Metadaten.....                      | 23 |
| 7: Suchen (Bsp. "John" und "Smith").....      | 27 |
| 8: Dateien herauskopieren.....                | 31 |
| 9: Datei-Container.....                       | 33 |

# 1: Images erstellen



## **Schritt 1: Datenträger zum Sichern öffnen**

Mit „Disk öffnen“ in der Symbolleiste oder im Extras-Menü oder durch Drücken der F9-Taste rufen Sie den Dialog „Datenträger einsehen“ auf.

Sie können entweder einen kompletten physischen Datenträger oder einen logischen Laufwerksbuchstaben auswählen.

# 1: Images erstellen

## *(Optional) Schritt 1a: Gewünschte Partition öffnen*

The screenshot shows the Windows Disk Management interface for 'Festplatte 0' (Disk 0) with MBR partitioning. A table lists seven partitions. Partition 3, which is 19.5 GB in size, is selected. A context menu is open over it, with the 'Erkunden' (Explore) option circled in red. A red arrow points from this menu to a second screenshot below, which shows the contents of 'Festplatte 0, Partition 3'. This second screenshot shows a file explorer view with a table of files and folders.

| Name        | Typ | Größe   | Erzeugung | Änderung | Zugriff | Attr.      |
|-------------|-----|---------|-----------|----------|---------|------------|
| 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 |     | 1,5 GB  |           |          |         | 94317678   |
| Partition 6 |     | 9,1 GB  |           |          |         | 97402158   |
| Partition 7 |     | 19,0 GB |           |          |         | 1164552... |

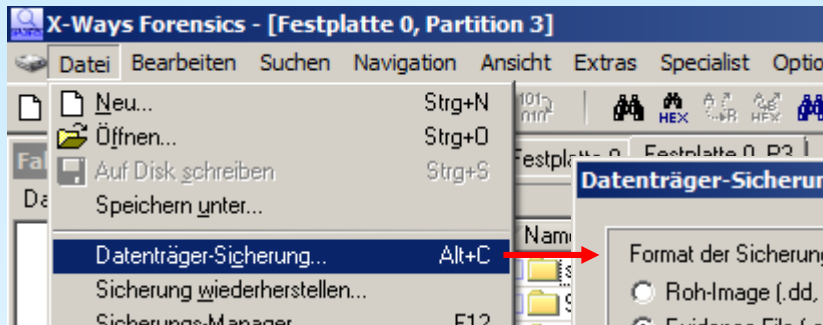
  

| Name               | Typ | Größe     | Erzeugung           | Änderung            | Zugriff             | Attr. |
|--------------------|-----|-----------|---------------------|---------------------|---------------------|-------|
| Pfad unbekannt     |     |           |                     |                     |                     |       |
| (Stammverzeichnis) |     | 8,2 KB    | 03.01.2006 10:03:38 | 30.05.2007 10:28:21 | 30.05.2007 10:28:21 | SH    |
| RECYCLER           |     | 328 Bytes | 03.01.2006 11:25:56 | 03.01.2006 11:25:56 | 30.05.2007 10:28:05 | SH    |
| temp               |     | 4,0 KB    | 26.09.2006 10:17:43 | 19.12.2006 11:13:13 | 30.05.2007 10:28:05 |       |
| Daten Jens         |     | 8,2 KB    | 03.01.2006 10:10:05 | 15.01.2007 13:53:45 | 30.05.2007 10:28:04 |       |
| Borland            |     | 464 Bytes | 03.01.2006 10:33:26 | 12.06.2006 12:53:41 | 30.05.2007 10:28:04 |       |

Wählen Sie eine bestimmte Partition aus.  
 Um ein Image des kompletten Datenträgers zu erstellen, lassen Sie diesen Schritt einfach aus.

# 1: Images erstellen

## Schritt 2: Den geöffneten Datenträger sichern



Bezieht sich immer auf das Fenster mit der aktiven Registerkarte.

Erzeugen Sie zwei Kopien simultan, falls benötigt!

Die Hash-Berechnung erlaubt eine spätere Überprüfung der Sicherung.

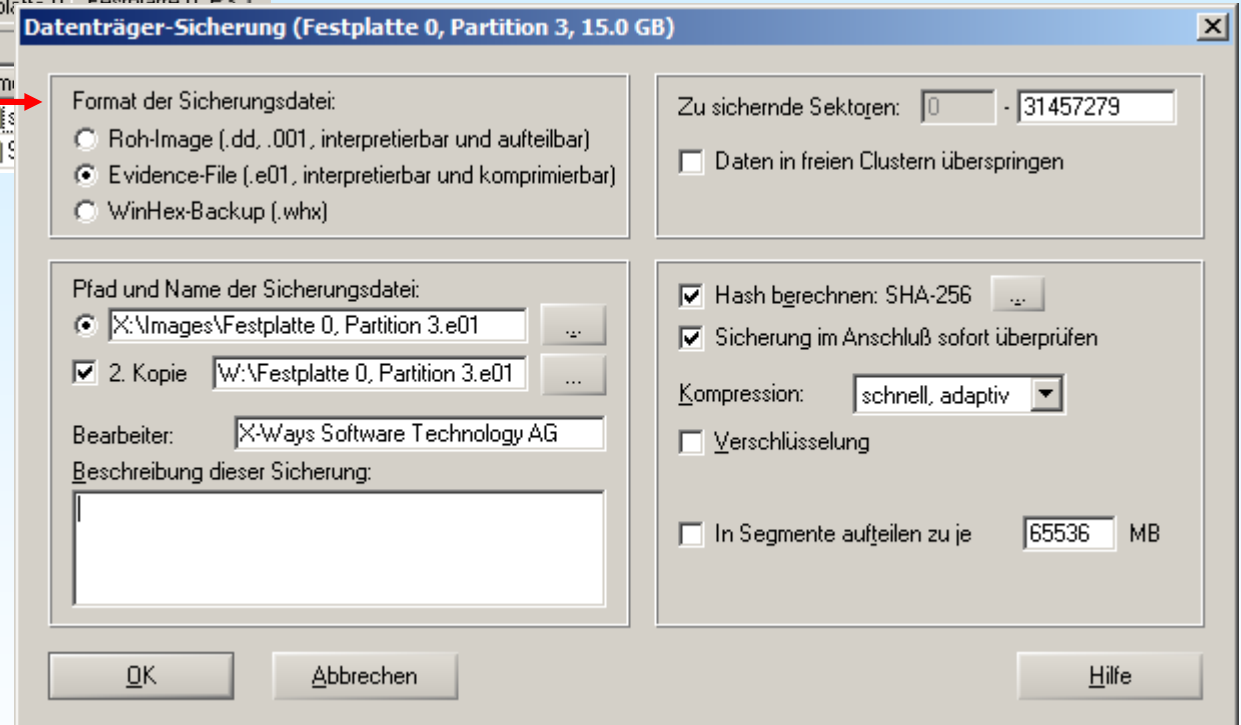
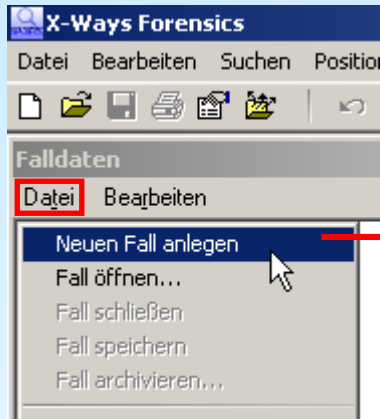


Image-Dateien zu splitten kann nützlich sein zum Speichern auf CD-Rs bzw. DVD+/-Rs oder auf FAT32-Dateisystemen.

## 2: Fall erzeugen, Images hinzufügen

### Schritt 1: Neuen Fall anlegen



Wählen Sie im Datei-Menü des Falldatenfensters den Menübefehl *Neuen Fall anlegen* und füllen Sie das folgende Dialogfenster aus:

**Eigenschaften**

Bez./Nr. des Falls: AZ 27-314-2012 Erzeugung: 16.10.2012 15:28:53

Verzeichnis: E:\cases

Beschreibung: System beschlagnahmt im Zusammenhang mit Untersuchung von Betrugsverdacht gegen Maier, Meyer, Mayer und Co.

Bearbeiter, Organisation, Adresse: KK Hans Klein  
Großstadtrevier

Allgem. Aktivitäten mitprotokollieren  Wiederherst./Kopieren protokollieren

Protokoll mit Bildschirmfotos  Asservat-Ordner als Standardausgabe

Protokoll: 0 B

Für die Bearbeitung geeignete Codepages:

Individuelle Zeitzonen je Asservat

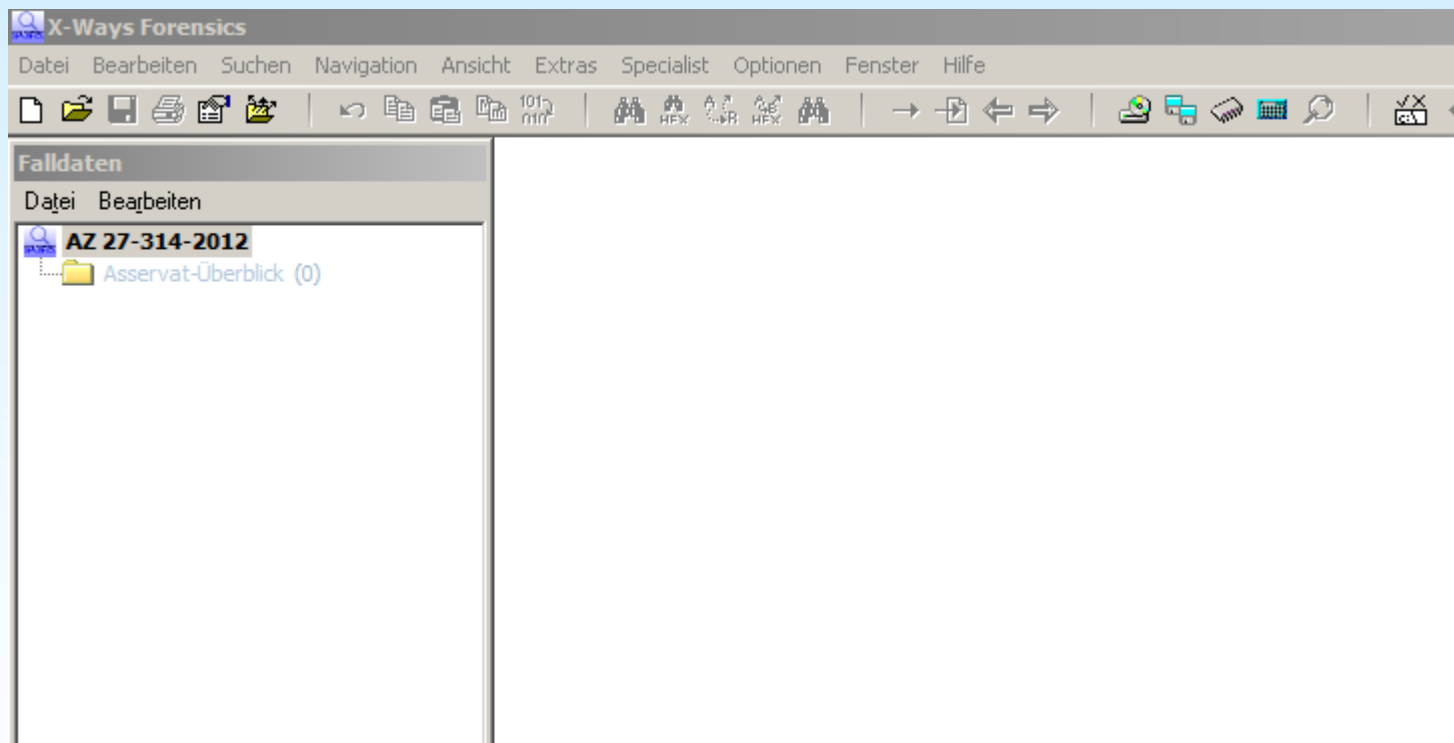
Autom. Speichern (in Min.)   Partitionen automatisch mit in Fall aufnehmen

Anzahl der Falldatei-Backups:   Falldatei mit Paßwort schützen<sup>3</sup>

DÜE: Schutz vor Duplikaten von Absturz-Dateien

## 2: Fall erzeugen, Images hinzufügen

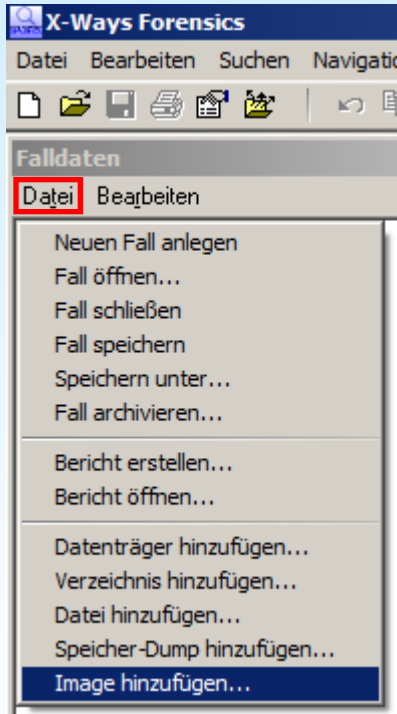
Nachdem Sie OK angeklickt haben, wird ein neuer Fall erzeugt und in X-Ways Forensics geöffnet:



Jetzt müssen Image-Dateien zur Untersuchung hinzugefügt werden.

## 2: Fall erzeugen, Images hinzufügen

### *Schritt 2: Image-Datei als Asservat hinzufügen*



Im Datei-Menü des Falldaten-Fensters gibt es Befehle zum Hinzufügen von Asservaten. Wählen Sie „Image hinzufügen...“.

Im darauf folgenden Dialog „Dateien öffnen“ können Sie Roh-Images (.dd/.001), Evidence-Files (.e01) oder virtuelle Festplatten (.vhd oder .vmdk) auswählen, die dann interpretiert werden.



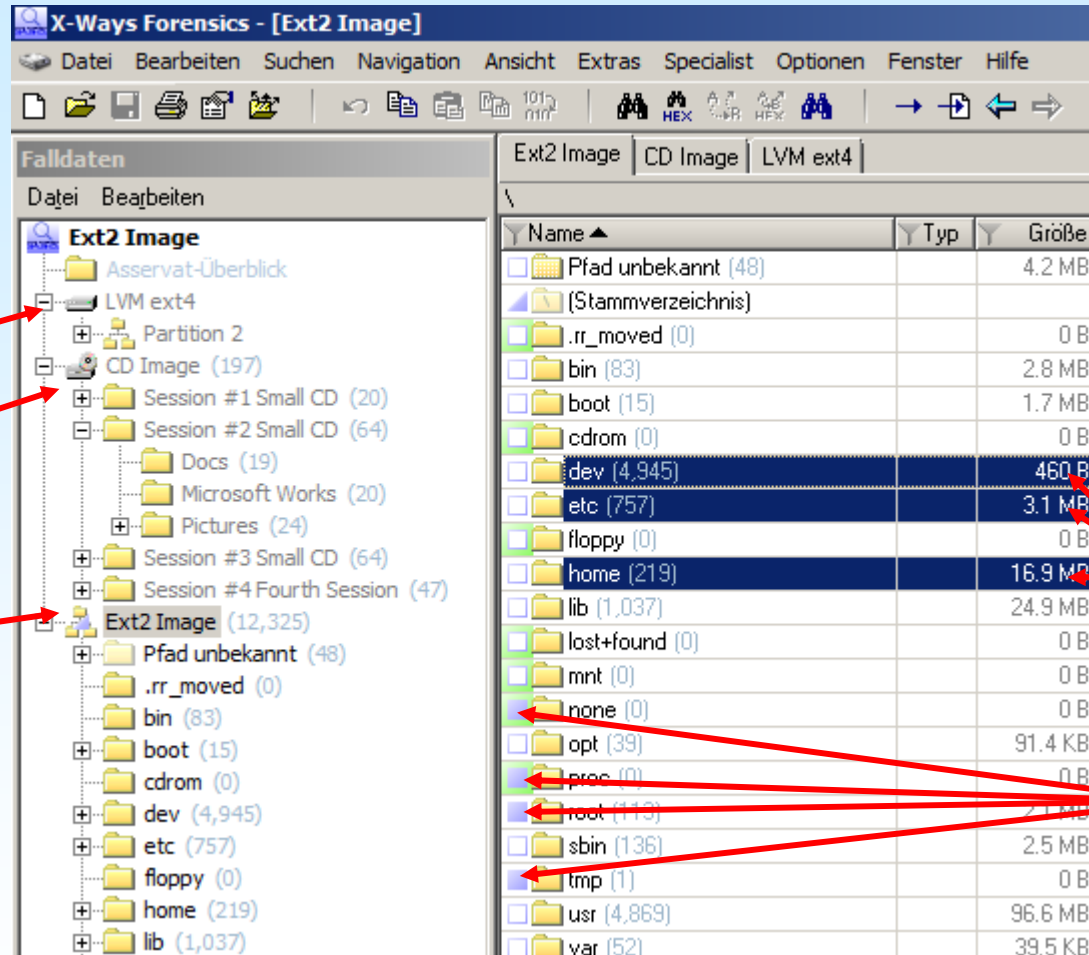
## 2: Fall erzeugen, Images hinzufügen

Images von:

Datenträgern

Optischen  
Medien

Partitionen/  
Volumes

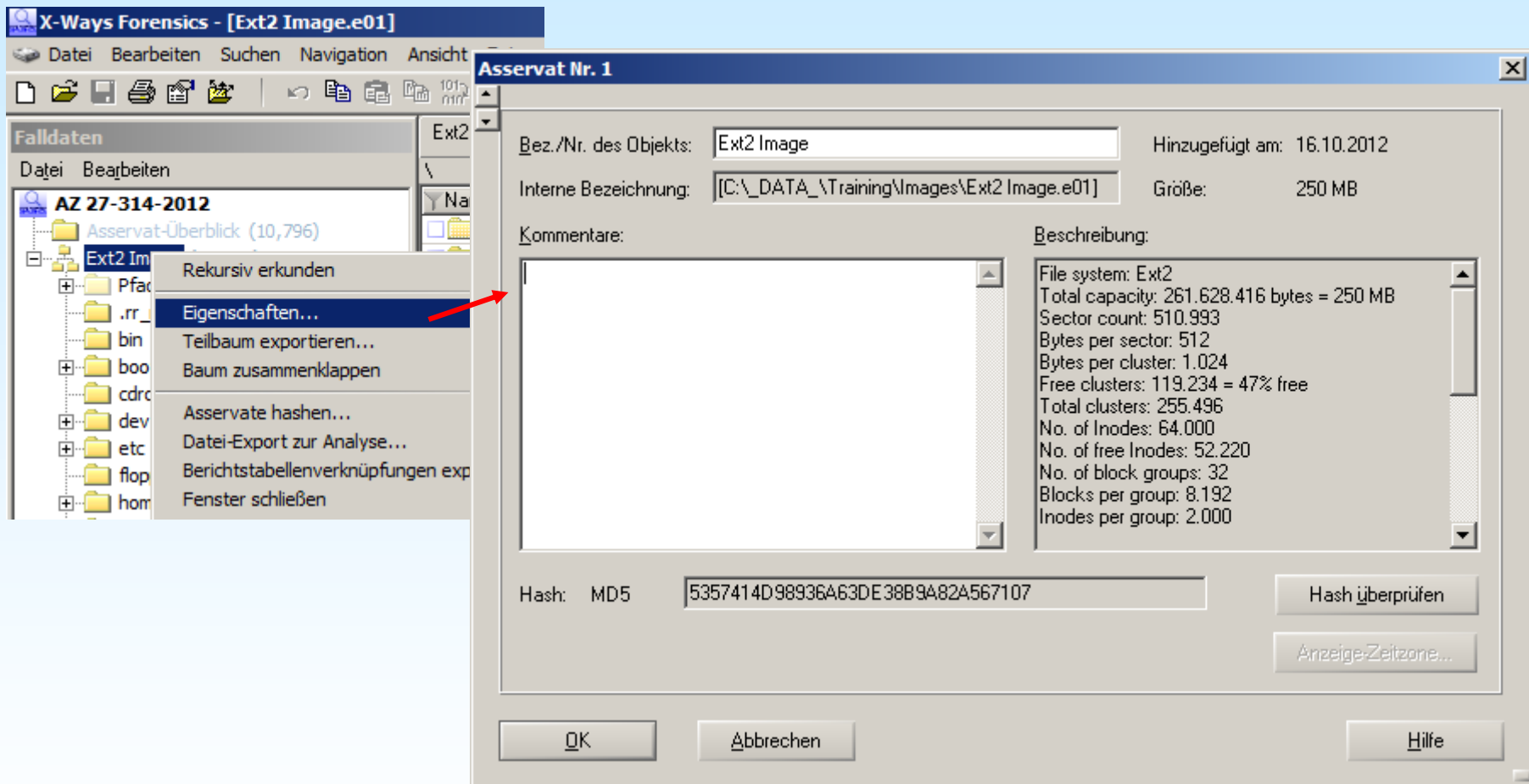


"Ausgewählt"

"Markiert"

Segmentierte Image-Dateien werden automatisch erkannt, wenn sie identische Namen tragen und ihre Datei-Erweiterungen durchnummeriert sind: .e01, .e02,... oder .dd, .002,... oder .001, .002,...

## 2: Fall erzeugen, Images hinzufügen

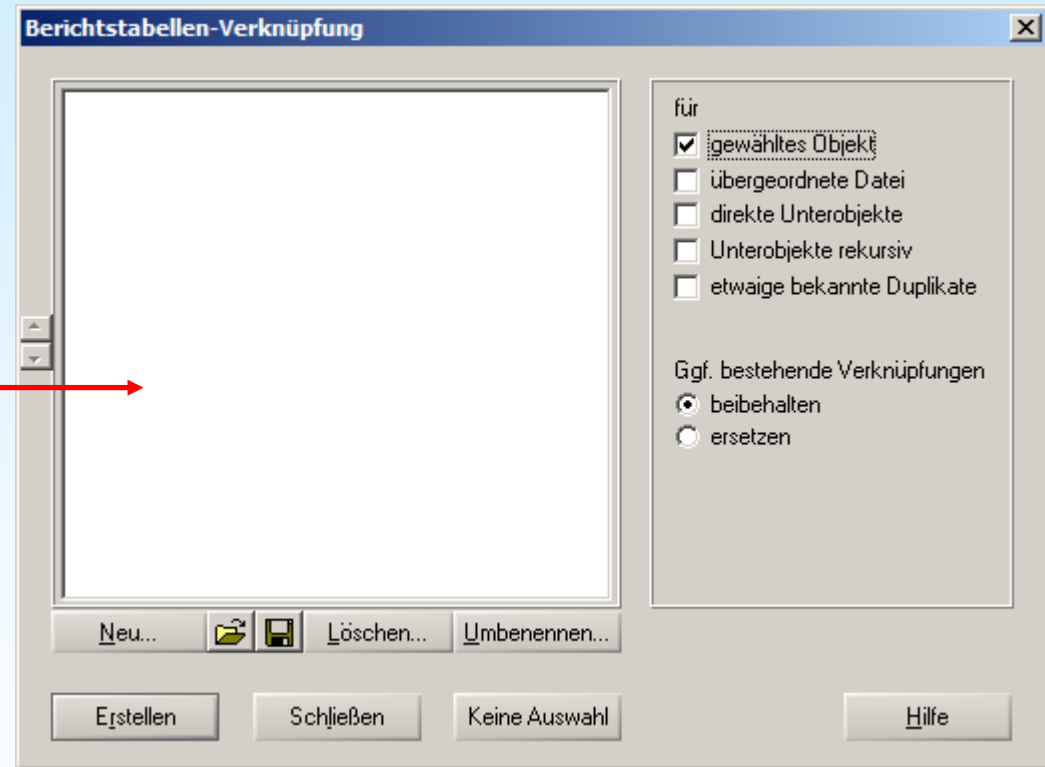
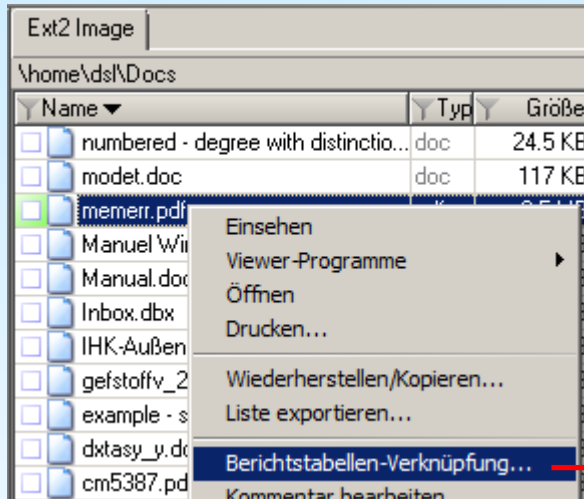


Eigenschaften eines Images lassen sich per Kontextmenü aus dem Falldatenfenster einsehen.

Dort kann man auch den Hash-Wert eines Images verifizieren lassen.

# 3: Berichten wichtiger Dateien

## Schritt 1: Berichtstabellen-Verknüpfung



Navigieren Sie zu den gewünschten Dateien und Verzeichnissen und klicken Sie diese rechts an. Im Kontextmenü gehen Sie zu „Berichtstabellen-Verknüpfung...“, was die Liste der derzeit verfügbaren Berichtstabellen zum Vorschein bringt.

Bei der ersten Verwendung der Funktion im aktuellen Fall liegen noch keine Berichtstabellen vor – diese müssen erst angelegt werden.

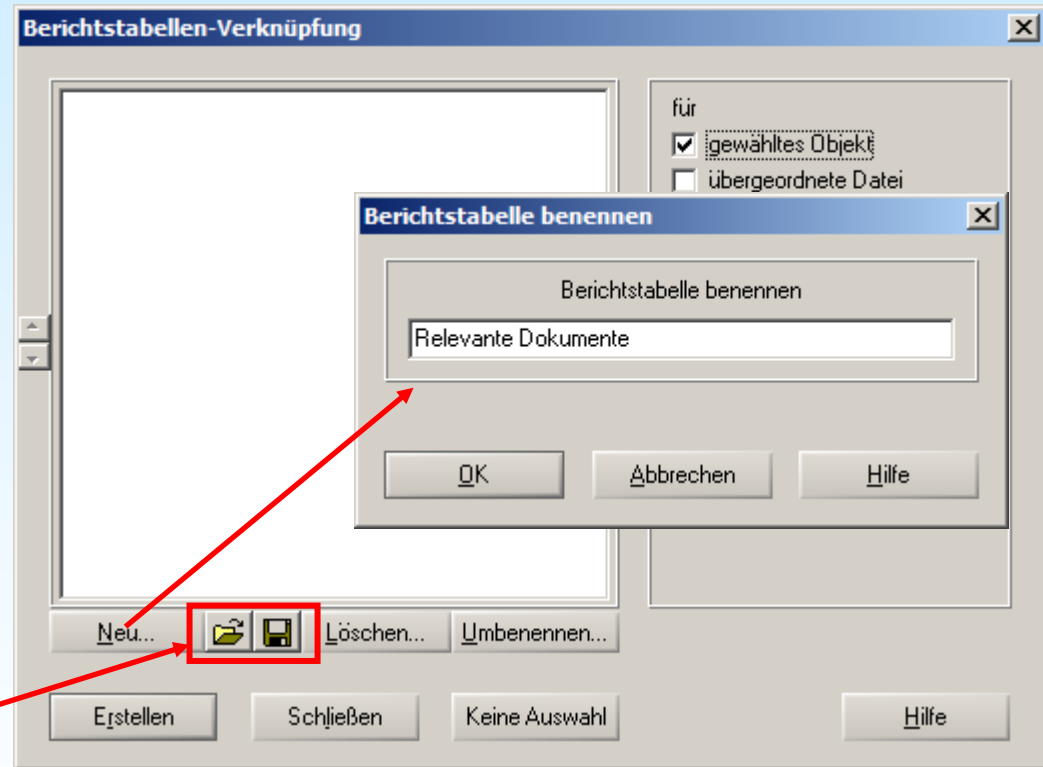
# 3: Berichten wichtiger Dateien

## Schritt 1a: Neue Berichtstabelle

(Schritt nur erforderlich, wenn gewünschte Tabelle noch nicht vorhanden)

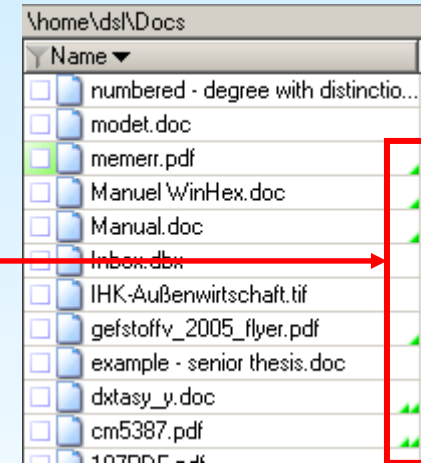
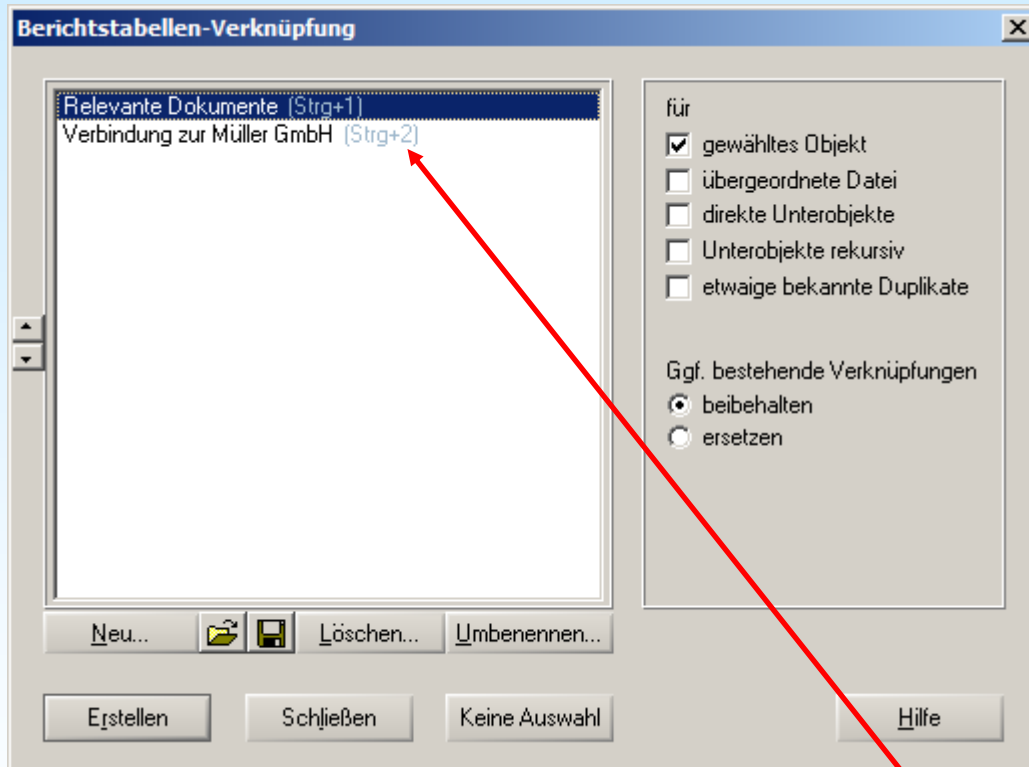
Legen Sie soviele Tabellen an, wie Sie benötigen – die Liste kann aber auch jederzeit später ergänzt werden.

Alternativ können Sie eine einmal erzeugte Liste von Berichtstabellen auch speichern und beim nächsten Fall direkt wieder laden.



# 3: Berichten wichtiger Dateien

## Schritt 1b: Berichtstabellen-Verknüpfung



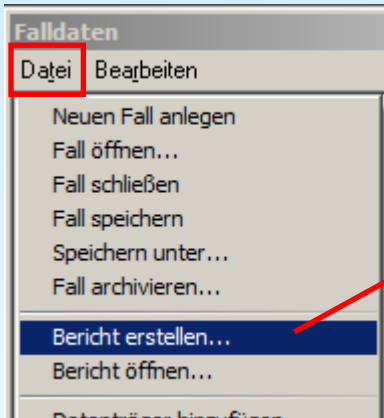
Das grüne Dreieck kennzeichnet Dateien, die einer Berichtstabelle zugewiesen sind.  
(zwei Dreiecke: zwei Tabellen)

Wählen Sie die gewünschte Tabelle aus und klicken Sie auf *Erstellen*, um die vorher ausgewählten Dateien und Verzeichnisse der Tabelle hinzuzufügen.

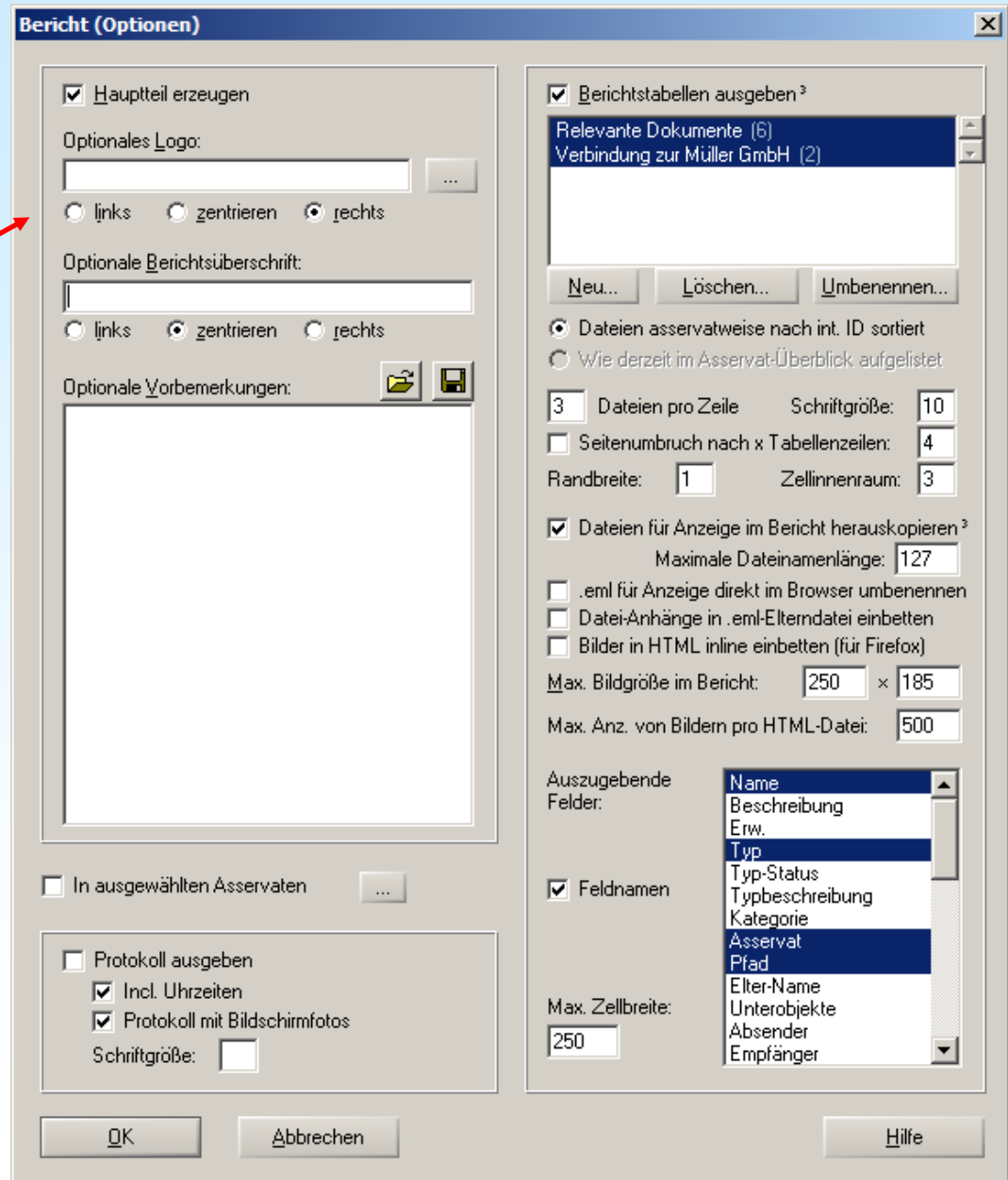
Beachten Sie die Tastenkürzel (z.B. Strg+1), die eine Zuweisung auch ohne Aufruf des Kontextmenüs ermöglichen.

## 3: Berichten wichtiger Dateien

### Schritt 2: Bericht erzeugen

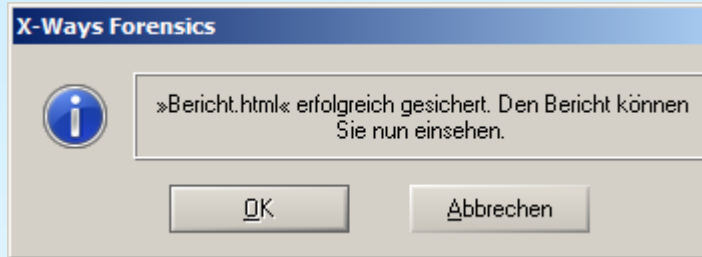


Setzen Sie, wenn gewünscht die Option „Dateien für Anzeige im Bericht herauskopieren“. Stellen Sie auch sicher, dass „Berichtstabellen aufnehmen“ angekreuzt ist. Wählen Sie außerdem die auszugebenden Felder nach Ihren Wünschen.



# 3: Berichten wichtiger Dateien

## Schritt 2a: Bericht einsehen



Wenn Sie auf OK klicken, wird die HTML-Viewer-Anwendung geladen, die in Optionen | Viewer-Programme festgelegt ist (keine Festlegung: Standard-Browser).

Die Berichtstabellen werden eingefügt mit Links für alle Nicht-Bild-Dateien, während Bilder direkt eingebettet werden (s. auch Skalierungsoptionen bei der Berichterstellung).

### AZ 27-314-2012

**Erzeugung:** 16.10.2012 15:28:53

**Falldatei:** E:\cases\AZ 27-314-2012.xfc

**Zeitzone** UTC +00:00 London, Lisbon, Dublin

**Bericht erzeugt von** X-Ways Forensics 16.7

**Beschreibung** System beschlagnahmt im Zusammenhang mit Untersuchung von Betrugsverda und Co.

**Bearbeiter, Organisation, Adresse:** KK Hans Klein  
Großstadtrevier

### Verbindung zur Müller GmbH (4 Einträge)

Name: **new-york-9400020.jpg**  
Typ: jpg  
Asservat: Ext2 Image  
Pfad: \home\dsl\Pictures\0003  
Größe: 18.6 KB



Name: **cm5387.pdf**  
Typ: pdf  
Asservat: Ext2 Image  
Pfad: \home\dsl\Docs  
Größe: 0.9 MB

[Link](#)

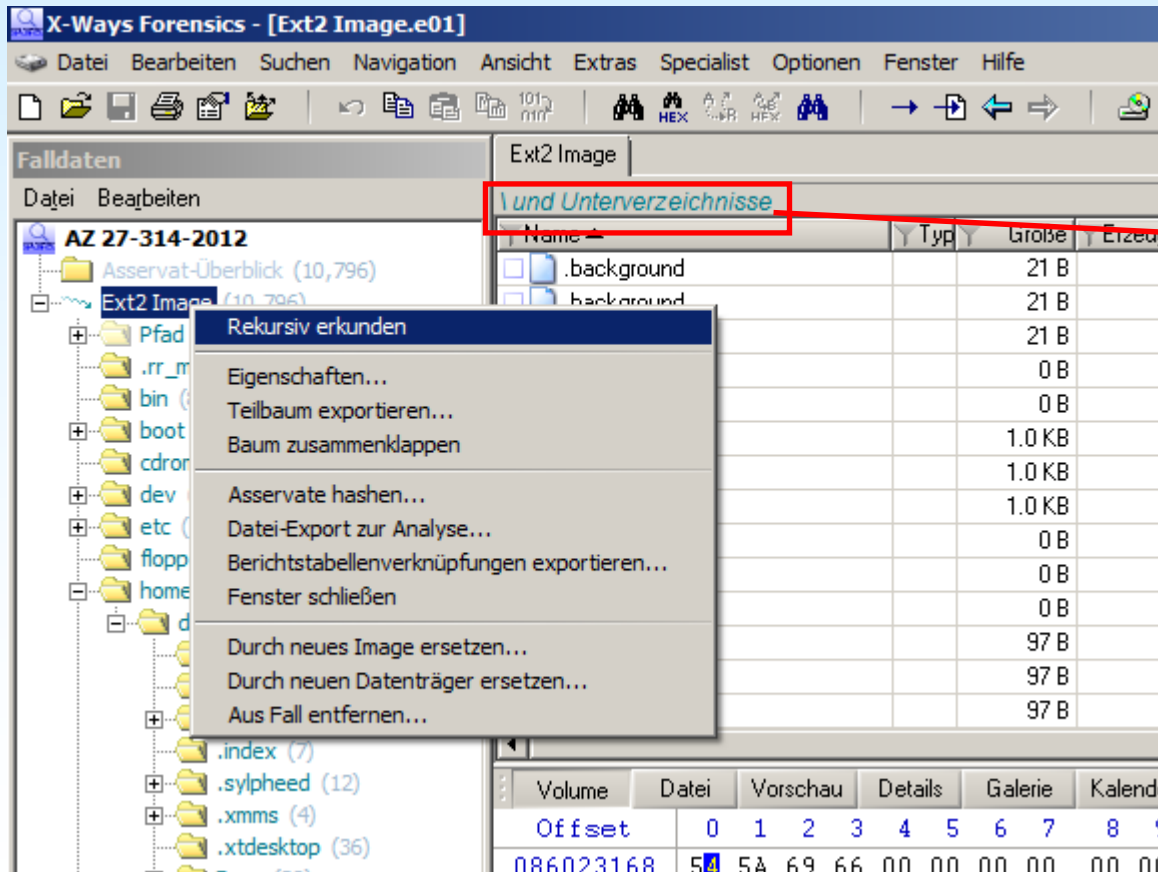
Name: **dxt**  
Typ: doc  
Asservat:  
Pfad: \hon  
Größe: 86.

[Link](#)

## 4: Filtern (Bsp. gelöschte JPEG-Dateien)

### 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.



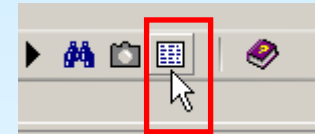
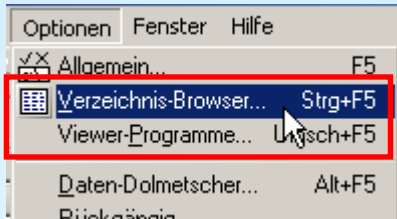
„\ und Unterverzeichnisse“  
kennzeichnet rekursive  
Auflistungen!

\ steht für das  
Stammverzeichnis einer  
Partition



## 4: Filtern (Bsp. gelöschte JPEG-Dateien)

### Schritt 2: Aufruf der Verzeichnis-Browser-Optionen



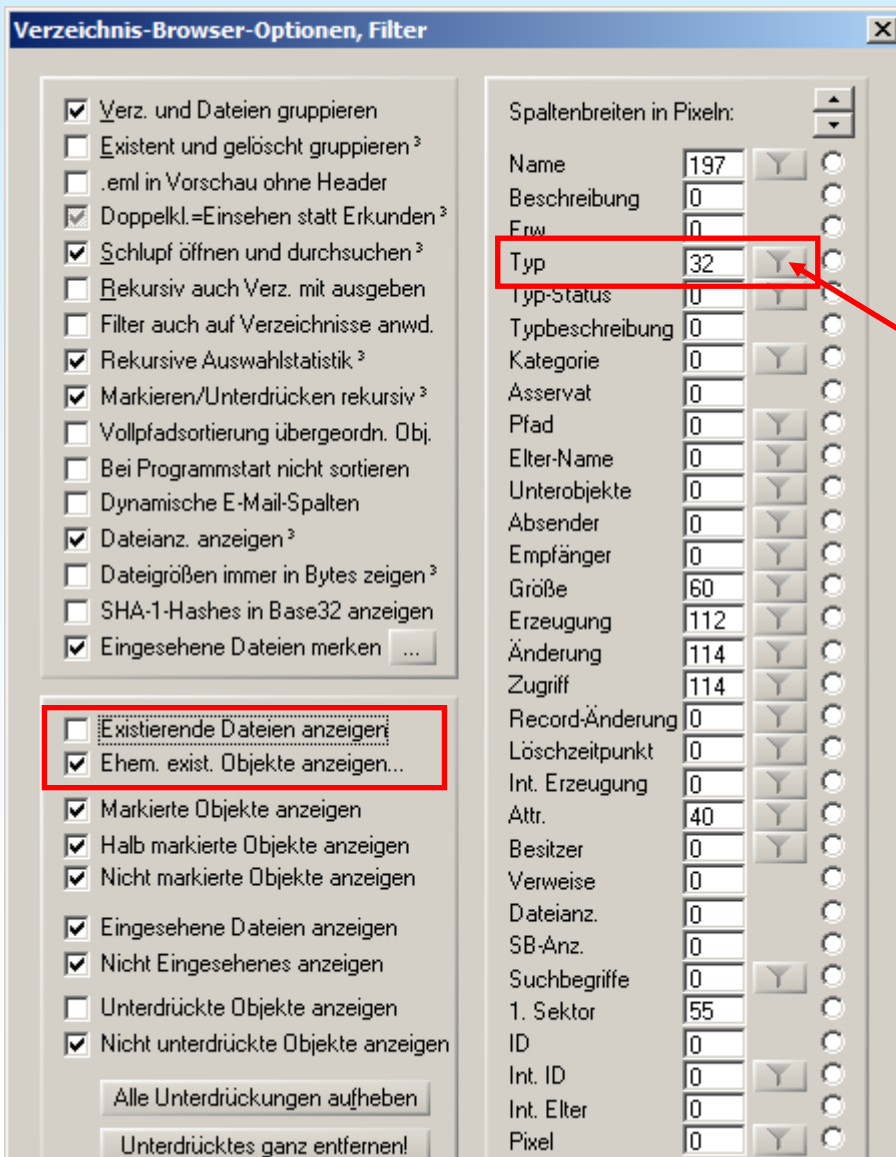
Die Verzeichnis-Browser-Optionen können entweder über ihren Eintrag im Optionen-Menü, den entsprechenden Button in der Werkzeugleiste oder einfach durch Klicken auf die Titelzeile des Verzeichnis-Browsers aufgerufen werden.

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

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

## 4: Filtern (Bsp. gelöschte JPEG-Dateien)

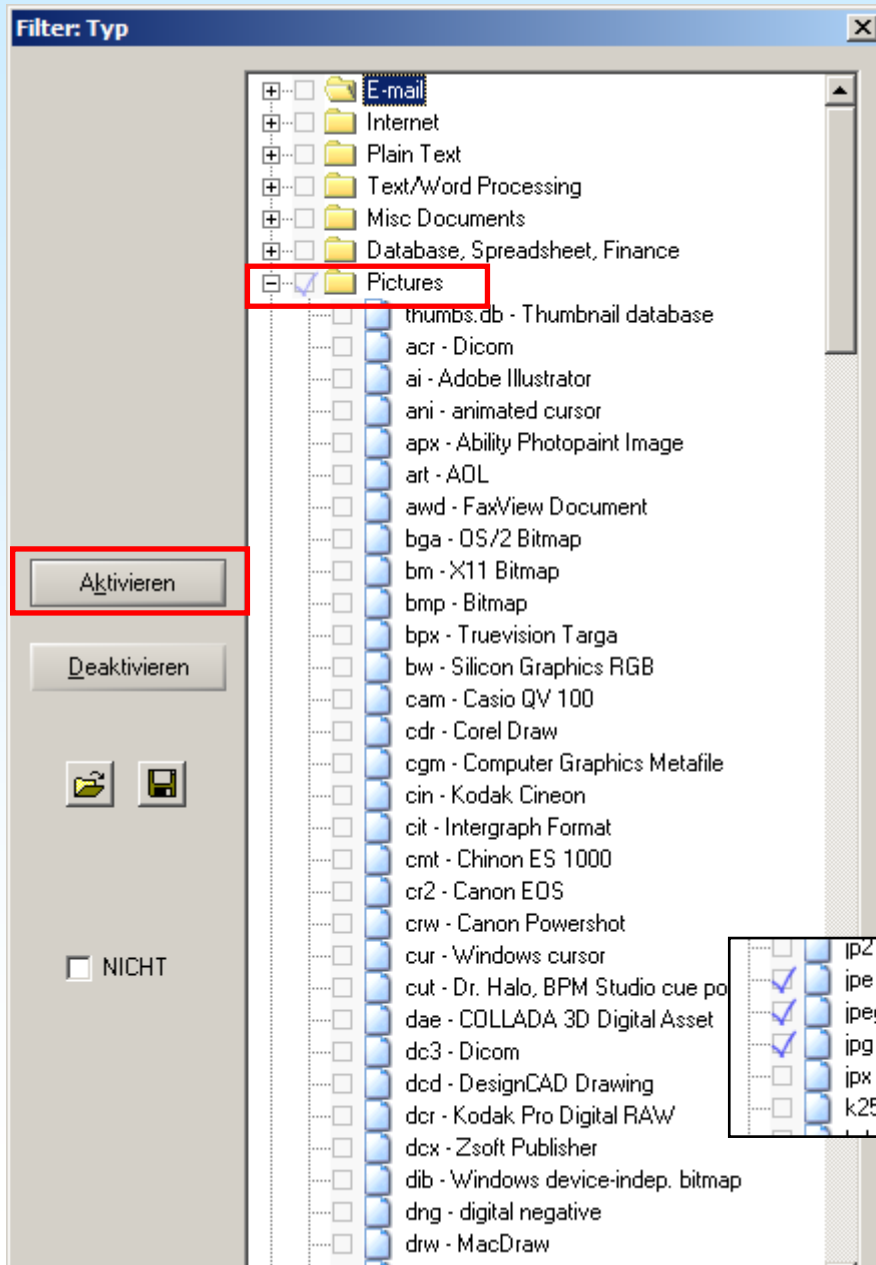
### Schritt 3: Verzeichnis-Browser-Optionen



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

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

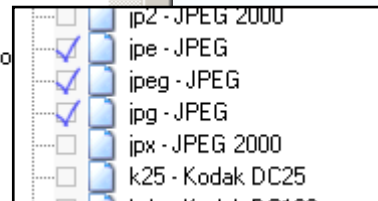
## 4: Filtern (Bsp. gelöschte JPEG-Dateien)



### Schritt 4: Auswahl des Typs

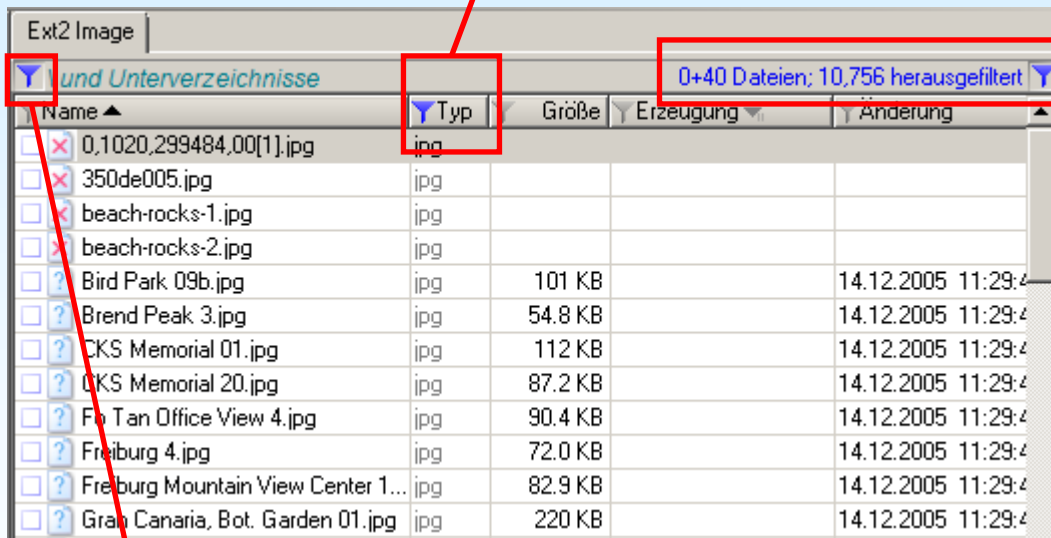
Öffnen Sie die Kategorie „Pictures“ und markieren Sie die JPEG-Typen. Nehmen Sie eventuell vorhandene sonstige Markierungen weg, falls erforderlich.

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.



## 4: Filtern (Bsp. gelöschte JPEG-Dateien)

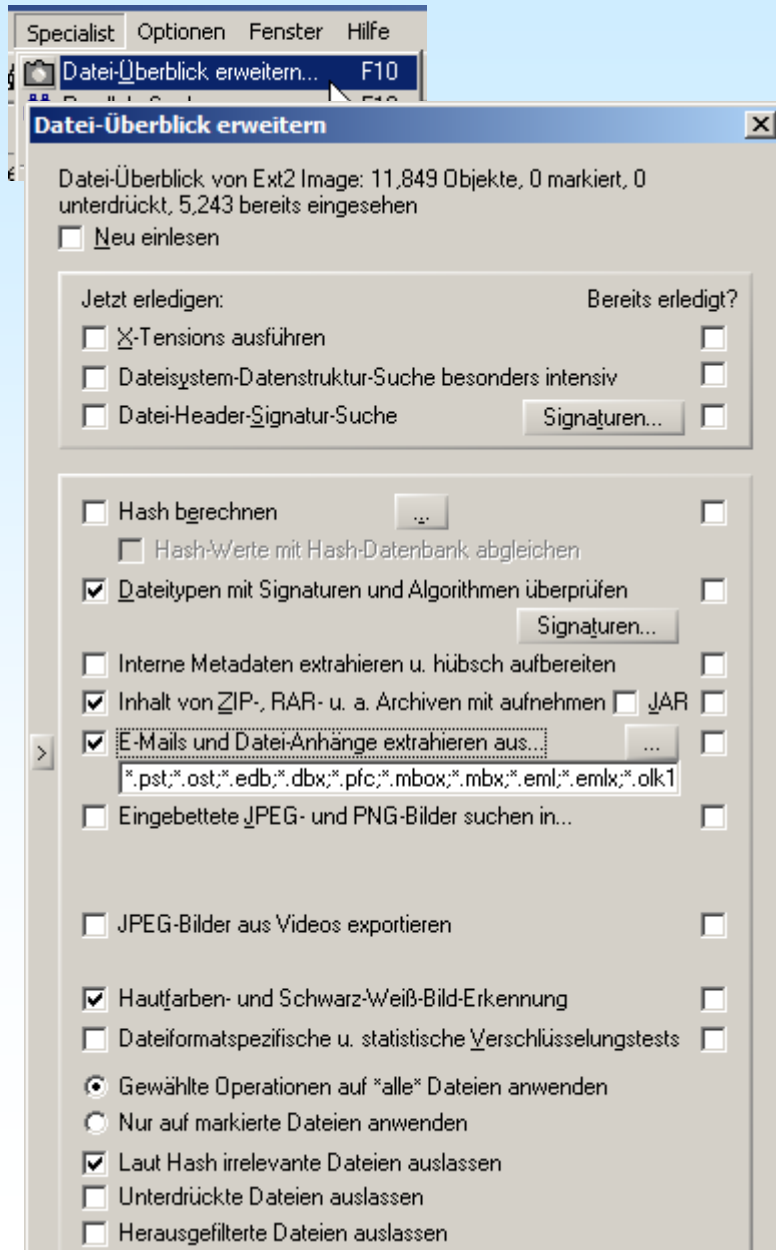
Schnellerer Zugriff auf die Spalten-basierenden Filter (z.B. um diese wieder zu deaktivieren)



Zeigt Details über die Effekte der Filter an: 40 ehemals existierende Dateien werden derzeit angezeigt (keine existierenden, keine virtuellen, keine Verzeichnisse). 10.756 zusätzliche Dateien wurden herausgefiltert (werden nicht aufgelistet)

Funktioniert auch als "alle Filter entfernen" Schaltfläche

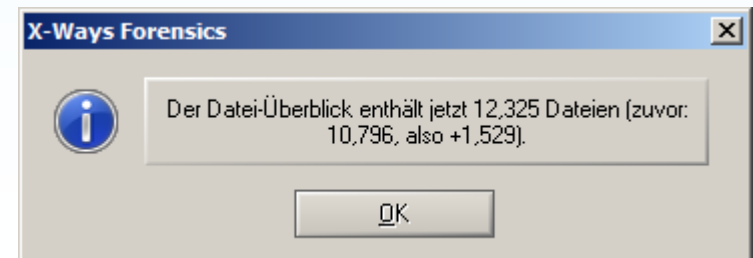
## 5: Datei-Überblick erweitern



Das Erweitern des Datei-Überblicks erlaubt u. a. die Suche in komprimierten Dateien in Archiven und E-Mails in E-Mail-Archiven, aber auch korrekte Erkennung von Dateitypen anhand ihres Inhalts, Extraktion von internen Metadaten, Erkennung von Hautfarben und Schwarz-Weiß-Bildern, etc.

Drücken Sie hierzu auf F10 oder rufen Sie „Datei-Überblick erweitern“ aus dem Specialist-Menü auf.


Wählen Sie die gewünschten Optionen aus und klicken Sie auf OK, was schließlich zu einer Meldung ähnlich der untenstehenden führen wird. Bestätigen Sie mit OK.



# 5: Datei-Überblick erweitern


## Beispiel-Effekte der Erweiterung

Vorher:

| Name ▲  | Typ |
|---|-----|
|  xyz.abc | abc |

Datei wird aufgelistet wie vom Dateisystem identifiziert – *Typ*-Spalte übernimmt ungeprüft die Dateierweiterung











Nachher:

| Name ▲   | Typ |
|--|-----|
|  ...xyz.abc (3) | zip |

Typ wird durch den anhand der Datei-Inhalte identifizierten Typ ersetzt.

Da es sich um ein Archiv handelt und die Option zur Auflistung deren Inhalte gewählt war, zeigen die .... im Icon die Existenz von Kind-Objekten an, die (3) hinter dem Namen gibt die Zahl der enthaltenen Dateien an.

Hautfarbanteil und Schwarz-Weiß-Erkennung:

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

Farbbilder erhalten einen Prozentwert für den Anteil des Bildes im Hautfarbbereich, Graustufen-Bilder werden stattdessen mit **s/w** gekennzeichnet.

## 6: Office-Metadaten

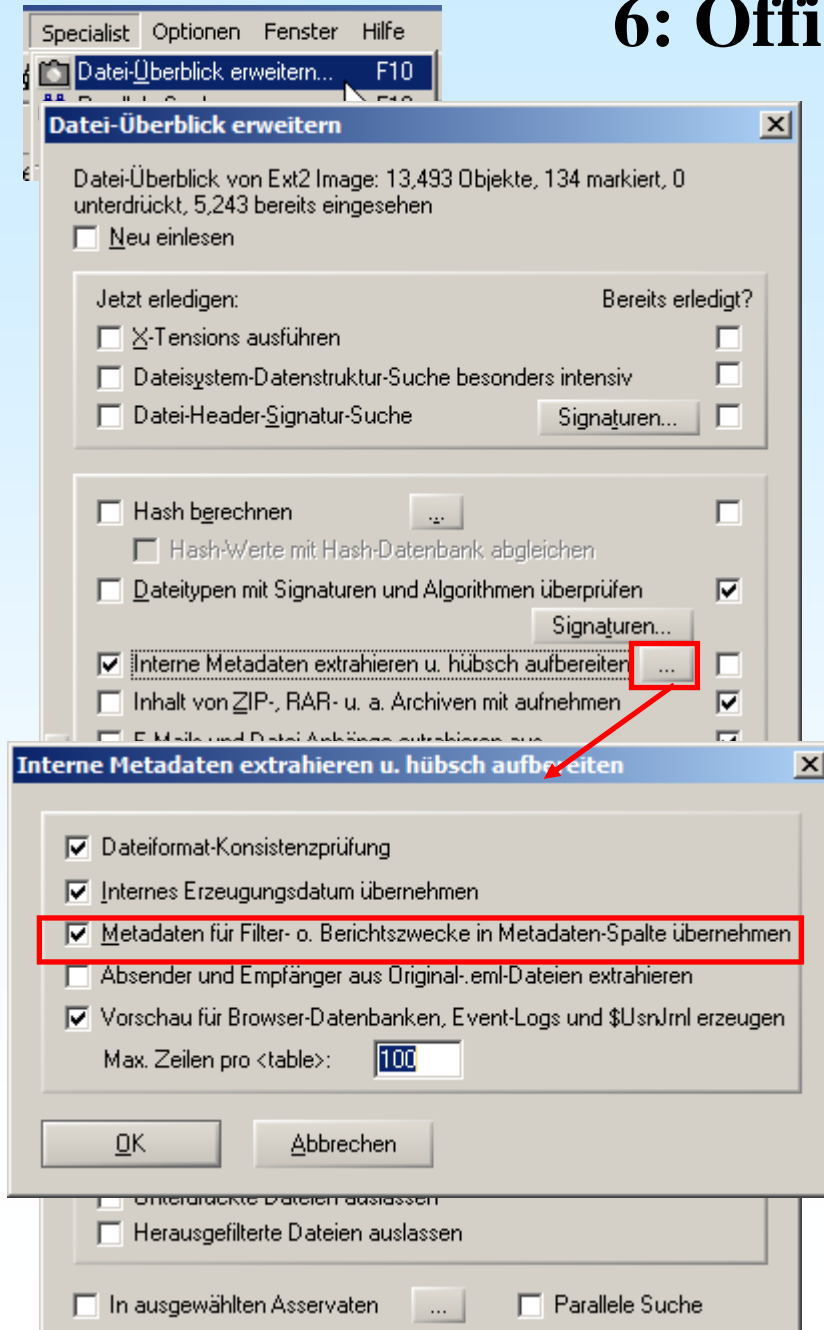
### Schritt 1: Datei-Überblick erweitern

Drücken Sie auf F10 oder rufen Sie „Datei-Überblick erweitern“ aus dem Specialist-Menü auf.

Wählen Sie die Option „Interne Metadaten extrahieren u. hübsch aufbereiten“. Klicken sie auf den ... Schalter, der rechts davon erscheint.

Wählen Sie „Metadaten für Filter.- o. Berichtszwecke in Metadaten-Spalte übernehmen“ aus. [An dieser Stelle kann auch das interne Erzeugungsdatum in die entsprechende Spalte aufgenommen und aus Browser-Datenbanken, etc. eine permanente Vorschau erzeugt werden.]

Klicken Sie in beiden Dialogen auf OK, um den Prozess laufen zu lassen.



## 6: Office-Metadaten

|  |                 |                 |     |   |
|--|-----------------|-----------------|-----|---|
| <input type="checkbox"/> .eml in Vorschau ohne Header                              | Beschreibung    | 0               |     |   |
| <input checked="" type="checkbox"/> Doppelkl.=Einsehen statt Erkunden <sup>3</sup> | Erw.            | 0               |     |   |
| <input checked="" type="checkbox"/> Schlupf öffnen und durchsuchen <sup>3</sup>    | Typ             | 43              | Y   |   |
| <input type="checkbox"/> Rekursiv auch Verz. mit ausgeben                          | Typ-Status      | 0               | Y   |   |
| <input type="checkbox"/> Filter auch auf Verzeichnisse anwd.                       | Typbeschreibung | 0               |     |   |
| <input checked="" type="checkbox"/> Rekursive Auswahlstatistik <sup>3</sup>        | Kategorie       | 0               | Y   |   |
| <input checked="" type="checkbox"/> Markieren/Unterdrücken rekursiv <sup>3</sup>   | Asservat        | 0               |     |   |
| <input type="checkbox"/> Vollpfadsortierung übergeordn. Obj.                       | Pfad            | 0               | Y   |   |
| <input type="checkbox"/> Bei Programmstart nicht sortieren                         | Elter-Name      | 0               | Y   |   |
| <input type="checkbox"/> Dynamische E-Mail-Spalten                                 | Unterojekte     | 0               | Y   |   |
| <input checked="" type="checkbox"/> Dateianz. anzeigen <sup>3</sup>                | Absender        | 0               | Y   |   |
| <input type="checkbox"/> Dateigrößen immer in Bytes zeigen <sup>3</sup>            | Empfänger       | 0               | Y   |   |
| <input type="checkbox"/> SHA-1-Hashes in Base32 anzeigen                           | Größe           | 60              | Y   |   |
| <input checked="" type="checkbox"/> Eingesehene Dateien merken ...                 | Erzeugung       | 0               | Y   |   |
|  | Änderung        | 114             | Y   |   |
|  | Zugriff         | 114             | Y   |   |
|  | Record-Änderung | 0               | Y   |   |
|  | Löschzeitpunkt  | 0               | Y   |   |
|  | Int. Erzeugung  | 0               | Y   |   |
|  | Attr.           | 40              | Y   |   |
| <input checked="" type="checkbox"/> Existierende Dateien anzeigen                  | Besitzer        | 0               | Y   |   |
| <input checked="" type="checkbox"/> Ehem. exist. Objekte anzeigen...               | Verweise        | 0               |     |   |
| <input checked="" type="checkbox"/> Markierte Objekte anzeigen                     | Dateianz.       | 0               |     |   |
| <input checked="" type="checkbox"/> Halb markierte Objekte anzeigen                | SB-Anz.         | 0               |     |   |
| <input checked="" type="checkbox"/> Nicht markierte Objekte anzeigen               | Suchbegriffe    | 0               | Y   |   |
| <input checked="" type="checkbox"/> Eingesehene Dateien anzeigen                   | 1. Sektor       | 55              |     |   |
| <input checked="" type="checkbox"/> Nicht Eingesehenes anzeigen                    | ID              | 0               |     |   |
| <input type="checkbox"/> Unterdrückte Objekte anzeigen                             | Int. ID         | 0               | Y   |   |
| <input checked="" type="checkbox"/> Nicht unterdrückte Objekte anzeigen            | Int. Elter      | 0               |     |   |
| Alle Unterdrückungen aufheben  |                 | Pixel           | 0   | Y |
| Unterdrücktes ganz entfernen!  |                 | HFA             | 50  | Y |
|  |                 | Hash            | 300 | Y |
| Erste rollbare Spalte: Beschreibung  |                 | Hash-Set        | 142 | Y |
|  |                 | Hash-Kategorie  | 176 | Y |
|  |                 | Berichtstabelle | 0   | Y |
|  |                 | Kommentar       | 200 | Y |
|  |                 | Metadaten       | 400 | Y |

OK      Abbrechen

### Schritt 2: Metadaten-Spalte sichtbar machen

Falls die Metadaten-Spalte im Verzeichnis-Browser bereits zu sehen ist, können Sie diesen Schritt überspringen.

Rufen Sie die Verzeichnis-Browser-Optionen auf (s. Kapitel 4, Schritt 2).

Tragen Sie in die Textbox neben "Metadaten" einen Wert ein, z.B. 400.

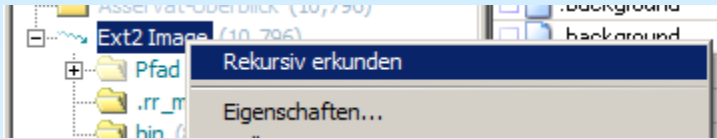
[Der eingegebene Wert wird die Spaltenbreite in Pixeln – die Breite kann mit der Maus später jederzeit reduziert oder erhöht werden.]

Bestätigen Sie mit OK. Die Spalte sollte im Verzeichnis-Browser erscheinen.

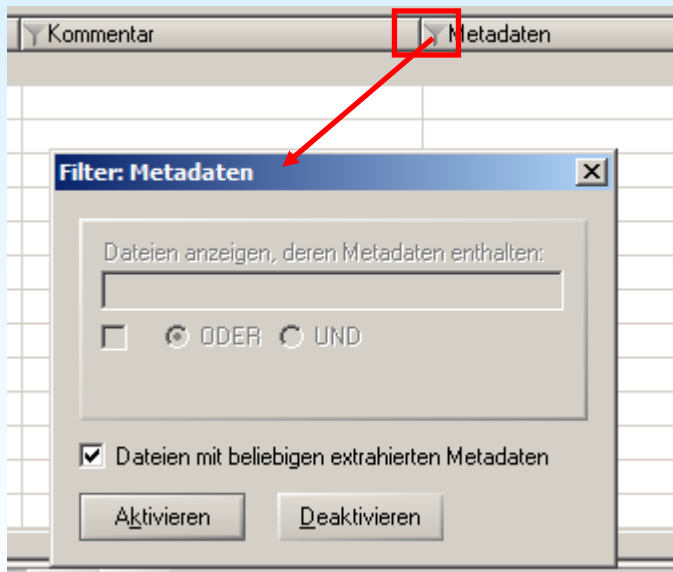


## 6: Office-Metadaten

### *Schritt 3: Metadaten filtern - beliebig*



Erkunden Sie die Partition rekursiv (s. Kapitel 4, Schritt 1).



Klicken Sie auf das Filter-Symbol in der Metadaten-Spalte. Der Filter: Metadaten sollte erscheinen.

[Wenn Sie das Symbol nicht treffen, sondern den Spaltenkopf selbst anklicken, wird stattdessen nach der Spalte sortiert.]

Lassen Sie "Dateien mit beliebigen extrahierten Metadaten" ausgewählt und klicken Sie "Aktivieren". Der Verzeichnis-Browser zeigt jetzt nur noch Dateien, deren Metadaten-Spalte nicht leer ist.

## 6: Office-Metadaten

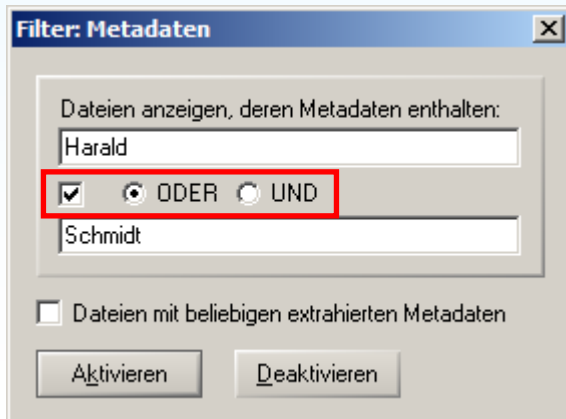
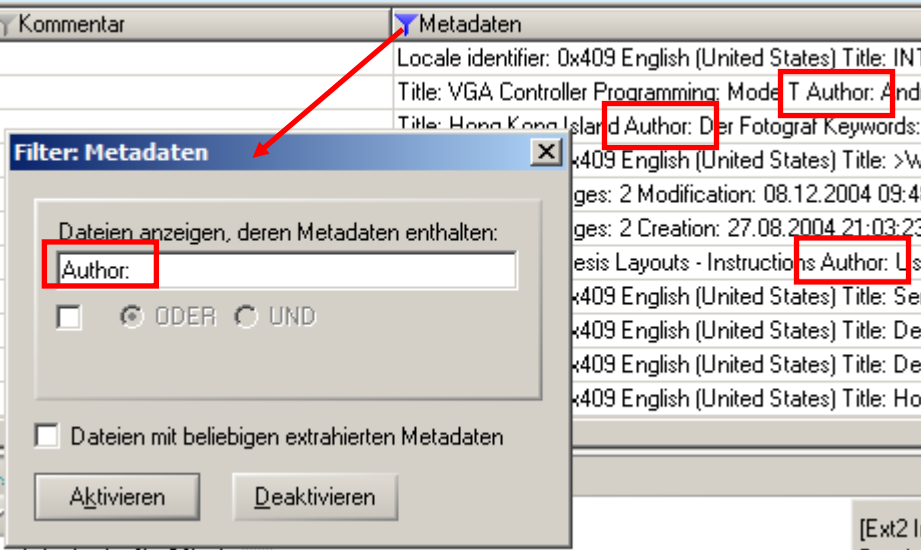
### Schritt 4: Metadaten filtern - spezifisch

Klicken Sie auf das Filter-Symbol in der Metadaten-Spalte. Der Filter: Metadaten sollte wieder erscheinen.

Entfernen Sie den Haken bei "Dateien mit beliebigen extrahierten Metadaten".

Geben Sie in das Textfeld beispielsweise "Author:" ein und klicken Sie "Aktivieren". Der Verzeichnis-Browser zeigt jetzt nur noch Dateien, deren Metadaten-Spalte "Author:" enthält.

Mittels Ankreuzfeld unter dem Suchbegriff können Sie ein zweites Textfeld hinzufügen, die dann mit ODER (alle Dateien, deren Metadaten-Feld einen der Begriffe enthält) bzw. UND (alle Dateien, deren Metadaten-Feld beide Begriffe enthält) verknüpft sein können.



# 7: Suchen (Bsp. "John" und "Smith")

## Schritt 1: Suchbegriffe und -optionen auswählen

Mittels Kontextmenü kann die Suche auf ausgewählte Objekte beschränkt, aber bei den Suchoptionen auch auf alle oder markierte Objekte geändert werden.

Die folgenden Suchbegriffe werden gleichzeitig gesucht (je 1 pro Zeile):

John  
Smith

Vorkommnisse von "John" und "Smith" nur als ganze Wörter

**OK** startet die Suche

Groß-/Kleinschreibung beachten  
 GREP-Syntax

**Nur ganze Wörter suchen**

Alphabet zur Wortgrenzenerkennung: ...

Bed.: Offset mod 512 = 0  
 X-Tensions ausführen

Alle Objekte im Datei-Überblick (267 MB)  
 Alle markierten Objekte (0 B)  
 Alle ausgewählten Objekte (10.4 MB)

Schlupf öffnen und durchsuchen<sup>?</sup>  
 Übergang Dateischlupf/freier Speicher  
 Text decodieren in:  
\*.pdf;\*.docx;\*.pptx;\*.xlsx;\*.odt;\*.odp;\*.oc

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

Laut Hash irrelevante Dateien auslassen  
 Unterdrückte Dateien auslassen  
 Herausgefilterte Dateien auslassen  
 Empfehlenswerte Datenreduktion  
 Verzeichnisse auslassen  
 1 Treffer pro Datei genügt (schneller)

OK Abbrechen  Logisch (dateiweise) Hilfe

Mehrere Textkodierungen simultan

# 7: Suchen (Bsp. "John" und "Smith")

## Schritt 2: Suchtreffer auswerten (Erläuterungen auf nächster Folie)

X-Ways Forensics - [Ext2 Image] 16.7 SR-3

Datei Bearbeiten Suchen Navigation Ansicht Extras Spezialist Optionen Fenster Hilfe

Falldaten

Ext2 Image

Suchtreffer in \ und Unterverzeichnisse **4** 18 Suchtreffer

| Offset    | Rel. Offs. | Anmerk. | Suchtreffer                                | Name               | Typ | Größe  | SB-Anz | S   |
|-----------|------------|---------|--|--------------------|-----|--------|--------|-----|
| 98162715  | 153627     | CP 1252 | file or disk. Find "John" [MatchCase Matc  | Manual.doc         | doc | 419 KB | 1      | Joh |
| 98162886  | 153798     | CP 1252 | indow for the name John or the hexadecima  | Manual.doc         | doc | 419 KB | 1      | Joh |
| 98585732  | 144516     | CP 1252 | disque actif. Find "John" [MatchCase Matc  | Manuel WinHex.doc  | doc | 438 KB | 2      | Joh |
| 98585900  | 144684     | CP 1252 | être active le nom John ou les valeurs hex | Manuel WinHex.doc  | doc | 438 KB | 2      | Joh |
| 98593231  | 152015     | CP 1252 | e.g.: Letter to Mr. Smith.doc Invoice*.pdf | Manuel WinHex.doc  | doc | 438 KB | 2      | Joh |
| 107947537 | 136721     | CP 1252 | file or disk. Find "John" [MatchCase Matc  | Spanish Manual.doc | doc | 394 KB | 2      | Joh |
| 107947708 | 136892     | CP 1252 | indow for the name John or the hexadecima  | Spanish Manual.doc | doc | 394 KB | 2      | Joh |
| 107954449 | 143633     | CP 1252 | e.g.: Letter to Mr. Smith.doc Invoice*.pdf | Spanish Manual.doc | doc | 394 KB | 2      | Joh |
| 107964172 | 153356     | CP 1252 | e words [Dear Mr. Smith] in a MS Word do   | Spanish Manual.doc | doc | 394 KB | 2      | Joh |
| 108575010 | 127266     | CP 1252 | file or disk. Find "John" [MatchCase Matc  | WinHex Manual.doc  | doc | 378 KB | 2      | Joh |
| 108575181 | 127437     | CP 1252 | indow for the name John or the hexadecima  | WinHex Manual.doc  | doc | 378 KB | 2      | Joh |

Volume Datei Vorschau Details Galerie Kalender Legende Sync **1** Gewählt: 1 Suchtreffer

| Volume | Datei | Vorschau | Details | Galerie | Kalender | Legende | Sync |    |    |    |    |    |    |    |    |                  |                             |
|--------|-------|----------|---------|---------|----------|---------|------|----|----|----|----|----|----|----|----|------------------|-----------------------------|
| 0      | 1     | 2        | 3       | 4       | 5        | 6       | 7    | 8  | 9  | 10 | 11 | 12 | 13 | 14 | 15 | CP 1252          | Spanish Manual.doc          |
| 2      | 69    | 74       | 68      | 6D      | 20       | 28      | 31   | 32 | 38 | 20 | 62 | 69 | 74 | 29 | 2E | rithm (128 bit). | \home\ds\NDocs              |
| D      | 0D    | 44       | 65      | 63      | 72       | 79      | 70   | 74 | 20 | 22 | 4D | 79 | 20 | 50 | 61 | Decrypt "My Pa   | Dateigröße: 394 KB          |
| 3      | 73    | 77       | 6F      | 72      | 64       | 22      | 0D   | 44 | 65 | 63 | 72 | 79 | 70 | 74 | 73 | ssword" Decrypts | 403,456 Bytes               |
| 0      | 74    | 68       | 65      | 20      | 61       | 63      | 74   | 69 | 76 | 65 | 20 | 66 | 69 | 6C | 65 | the active file  | Ohne Schlupf: 402,944 Bytes |
| 0      | 6F    | 72       | 20      | 64      | 69       | 73      | 6B   | 2E | 0D | 0D | 46 | 69 | 6E | 64 | 20 | or disk. Find    | [Schreibschutz-Modus]       |
| 2      | 4A    | 6F       | 68      | 6E      | 22       | 20      | 5B   | 4D | 61 | 74 | 63 | 68 | 43 | 61 | 63 | "John" [MatchCas | Letzte Änderung: 14.12.2005 |
| 5      | 20    | 4D       | 61      | 74      | 63       | 68      | 57   | 6F | 72 | 64 | 20 | 44 | 6F | 77 | 6F | e MatchWord Down | 11:29:58                    |
| 0      | 55    | 70       | 20      | 42      | 6C       | 6F      | 63   | 6B | 4F | 6E | 6C | 79 | 20 | 53 | 61 | Up BlockOnly Sa  | Letzter Zugriff: 14.12.2005 |
| 6      | 65    | 41       | 6C      | 6C      | 50       | 6F      | 73   | 20 | 55 | 6E | 69 | 63 | 6F | 64 | 65 | veAllPos Unicode | 11:29:58                    |
| 0      | 57    | 69       | 6C      | 64      | 63       | 61      | 72   | 64 | 73 | 5D | 0D | 46 | 69 | 6E | 64 | Wildcards] Find  |                             |
| 0      | 30    | 78       | 31      | 32      | 33       | 34      | 20   | 5B | 44 | 6F | 77 | 6F | 20 | 55 | 70 | 0x1234 [Down     |                             |

Seite 777 von 2293 Offset: 136721 = 74 Block: 136721 - 136724 Größe: 4

**3** AZ 27-314-2012

- Asservat-Überblick (12,325)
- Ext2 Image (12,325)
  - Pfad unbekannt (8)
  - .rr\_moved (0)
  - bin (83)
  - boot (15)
  - cdrom (0)
  - dev (4,945)
  - etc (757)
  - floppy (0)
  - home (219)
  - lib (1,037)
  - lost+found (0)
  - mnt (0)
  - none (0)
  - opt (39)
  - proc (0)
  - root (113)

**5** [Wichtige Treffer]  
[Index-Suchtreffer]

- John (11)
- Smith (7)

**6** 0x1234 [Down]

**7** Treffer pro Datei auflisten  
Min. 1 Enter

## 7: Suchen (Bsp. "John" und "Smith")

### Schritt 2: Suchtreffer auswerten (Erläuterungen zu voriger Folie)

- 1 Ein Klick auf diesen Schalter ruft die Suchbegriffs- und Suchtrefferlisten auf.
- 2 Dies ist die Suchtrefferliste. Sie können Suchtreffer eingrenzen, indem Sie
  - Unterverzeichnisse im Verzeichnisbaum auswählen **3**
  - die Filtermethoden des Verzeichnis-Browsers anwenden. **4**
- 5 Dies ist die Suchbegriffsliste. Wählen Sie einen oder mehrere Suchbegriffe aus, um die Ergebnisliste auf die derzeit gewünschten Suchbegriffe einzugrenzen. Doppelklicken Sie einen einzelnen Suchbegriff oder benutzen Sie Mehrfachauswahl und die Enter-Taste bzw. den Schalter.
- 6 Klicken Sie auf einen Suchtreffer und die untere Hälfte des Bildschirms bringt den Treffer zur Ansicht.
- 7 Erhöhung der erwarteten Suchbegriffe (d.h. unterschiedliche Suchbegriffe, nicht Mehrfachtreffer eines einzelnen Suchbegriffs!) pro Datei reduziert Suchtrefferliste auf Dateien, die die Bedingung erfüllen.



# 7: Suchen (Bsp. "John" und "Smith" mit GREP)

## *GREP-Alternative zu Schritt 1: Suchbegriffe und -optionen auswählen*

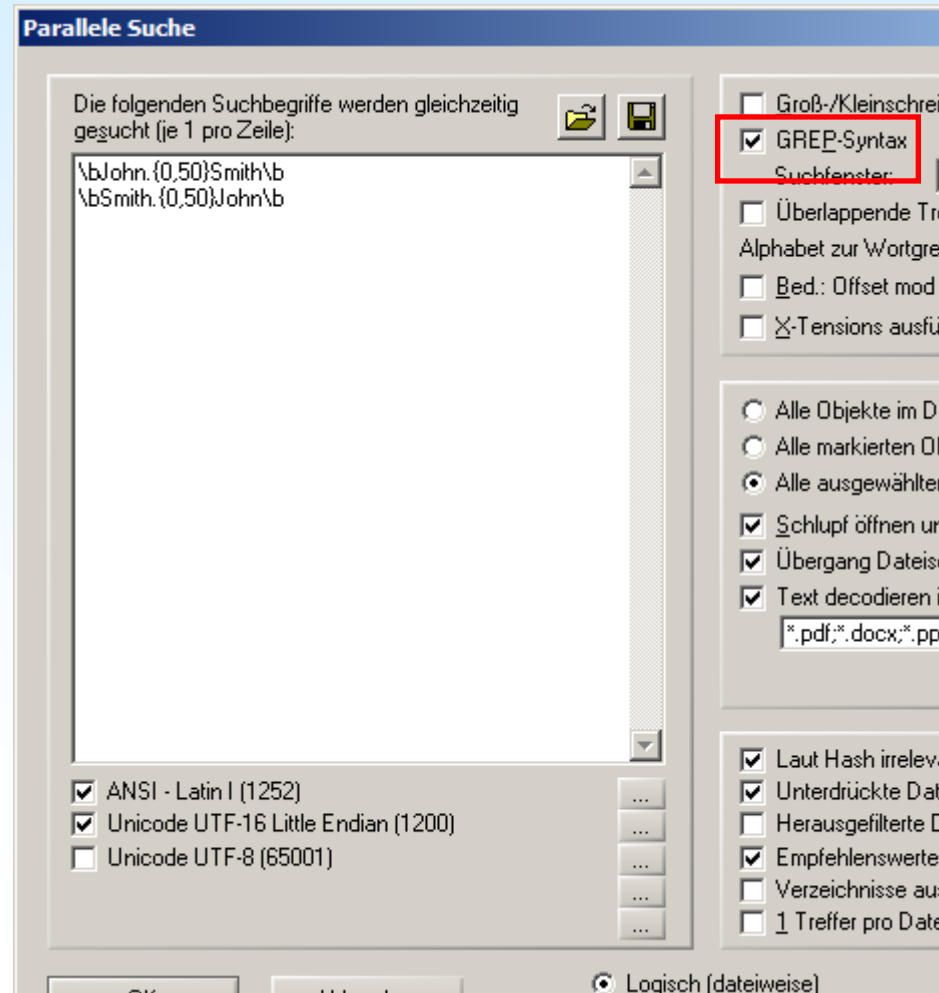
Statt "John" und "Smith" unabhängig voneinander zu suchen, erlaubt die Verwendung von GREP die beiden als "nahe beieinander liegend" zu suchen.

**\bJohn.{0,50}Smith\b**

\b verlangt eine Wortgrenze (also Wortanfang oder -ende, je nach Position) ersetzt somit also "Ganze Wörter"

.{0,50} erwartet zwischen 0 und 50 beliebige Zeichen (ausgedrückt durch den Punkt), erlaubt "John" und "Smith" also entweder zusammengeschieden oder durch maximal 50 beliebige Zeichen voneinander getrennt zu sein.

Die zweite Zeile erlaubt den beiden Begriffen, in umgekehrter Reihenfolge zu erscheinen.



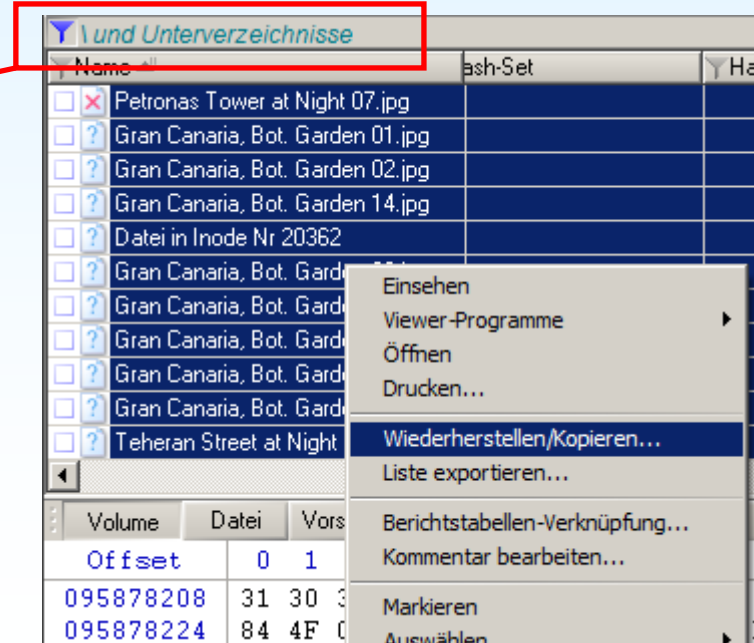
## 8: Dateien herauskopieren

### *Schritt 1: Wählen Sie die gewünschten Dateien und/oder Verzeichnisse aus*

- einzeln oder als Gruppe, mit Strg+A auch die gesamte derzeit angezeigte Liste
- rekursiv oder Standard-Anzeige
- mit frei gewählten Filtern oder ungefiltert

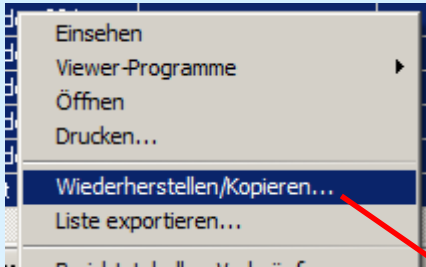
Als Beispiel hier wird nach gelöschten JPEGs gefiltert (wie in Kapitel 4 gezeigt) und mit Strg+A alle Dateien, die die Filterbedingungen erfüllen ausgewählt. Klicken Sie die Auswahl rechts an, um das Kontextmenü zu erhalten:

Filter aktiv (im Beispiel: Typ-Filter für JPEGs, existierende Dateien nicht angezeigt) und rekursive Auflistung ab Stammverzeichnis ("\\")

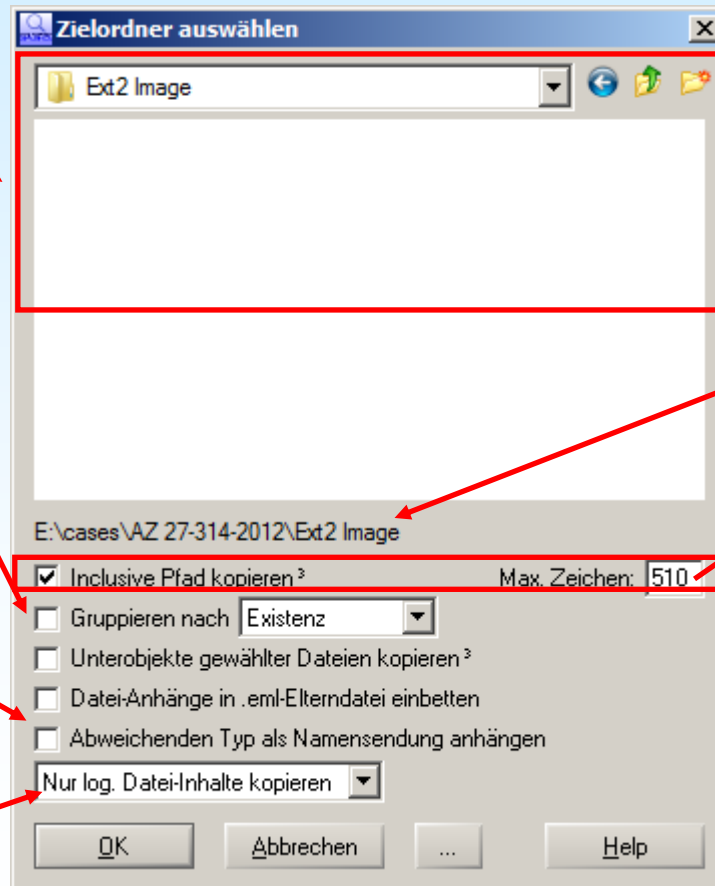


# 8: Dateien herauskopieren

## Schritt 2: Wiederherstellen/Kopieren



Im Kontextmenü das Kommando *Wiederherstellen/Kopieren* auswählen.



Erzeugt separate Ausgabeverzeichnisse, je nach Gruppierung

Benennt Dateien ohne aussagekräftige Dateierweiterung geeignet um – ermöglicht Windows, die Datei korrekt zu öffnen

Datei-Inhalte mit und ohne Schlupf – oder auch nur den Schlupfbereich, falls die Datei selbst gar nicht relevant ist.

Ausgabepfad für die zu kopierenden Daten festlegen

Reproduziert im Ausgabeverzeichnis die Pfade, wie sie am Ursprungsort vorliegen (sofern sie die maximale Pfadlänge nicht überschreiten).

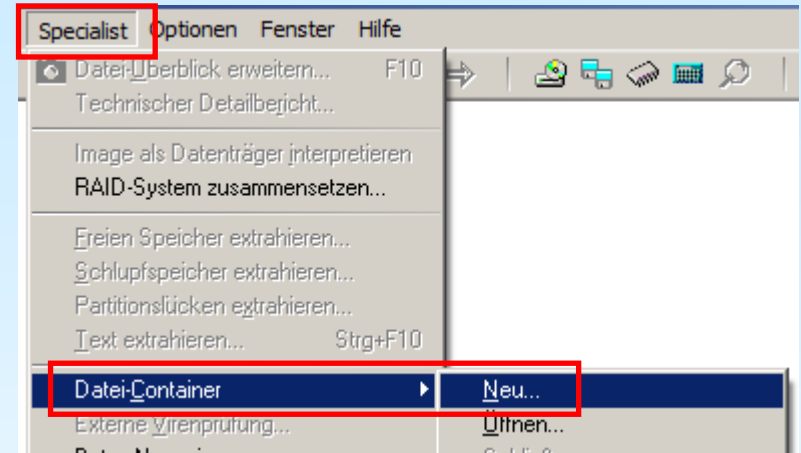


# 9: Datei-Container

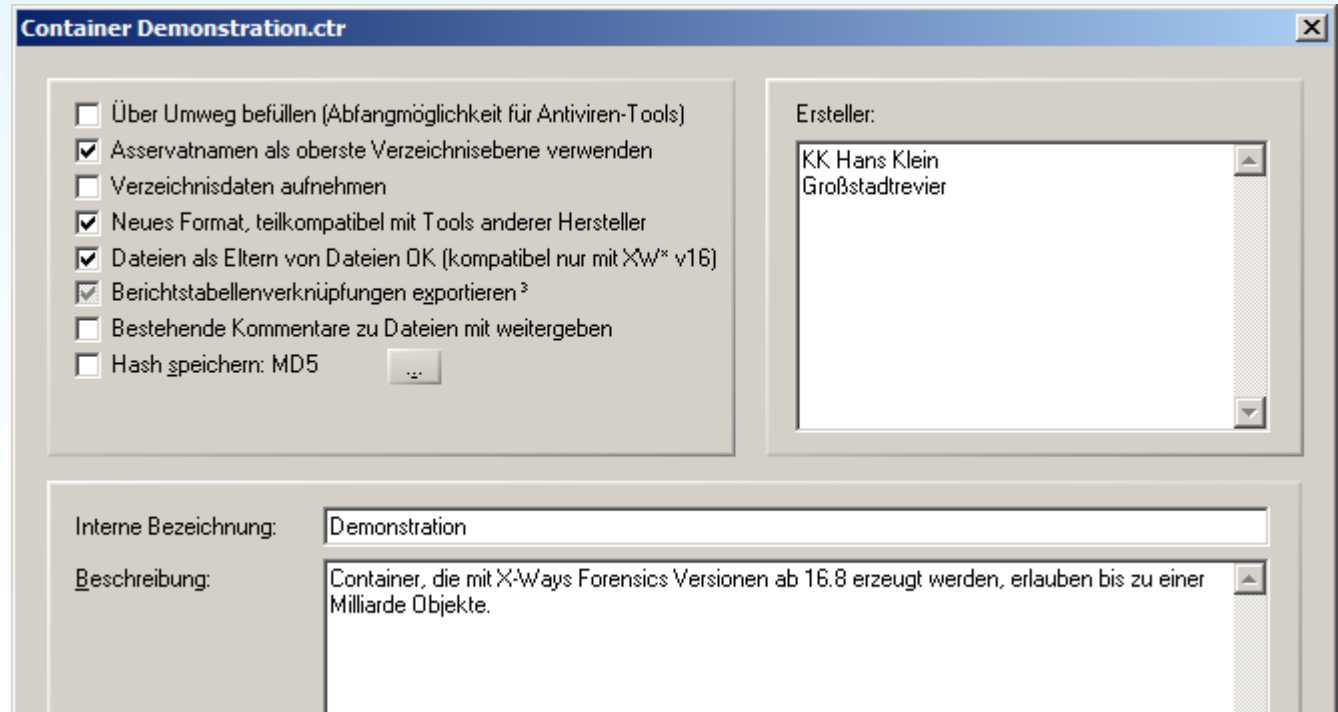
## Schritt 1: Datei-Container erstellen

Gehen Sie im Menu *Specialist* zu *Datei-Container* → *Neu...*

Wählen Sie im darauffolgenden Datei-Dialog den gewünschten Pfad und Dateinamen für den Container aus – X-Ways Forensics wird die Erweiterung *.ctr* hinzufügen.

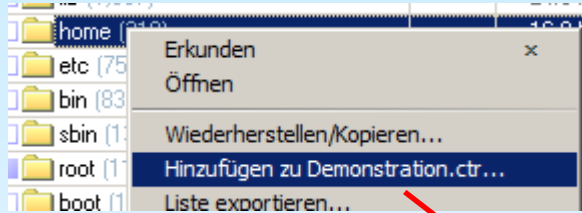


Nach Bestätigung des Dateidialogs fordert X-Ways Forensics Sie dazu auf, Einstellungen vorzunehmen. Behalten Sie die Einstellungen bei und geben Sie eine Beschreibung ein. Klicken Sie OK.

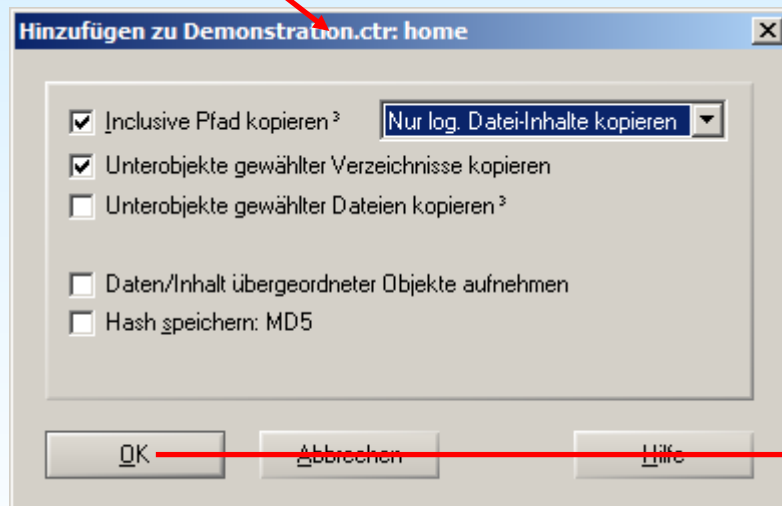


# 9: Datei-Container

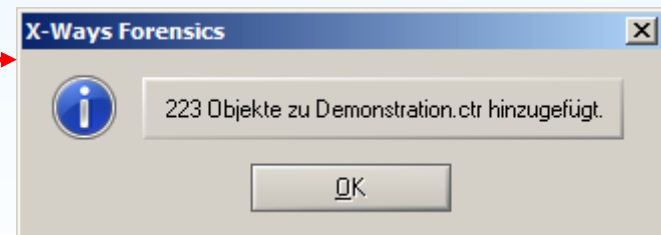
## Schritt 2: Dateien in den Container kopieren



Verfahren Sie genau wie beim Dateien herauskopieren (Kapitel 8, Schritt 1) um die gewünschten Dateien auszuwählen. Aber im Kontextmenü wählen Sie stattdessen *Hinzufügen zu [Name Ihres Containers]...*



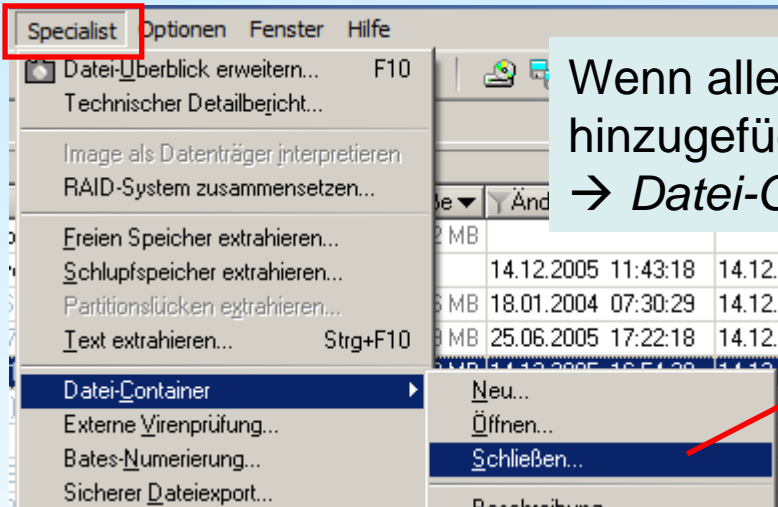
Auch die Optionen sind denen von *Wiederherstellen/Kopieren* nicht unähnlich, wobei natürlich kein Ausgabeverzeichnis benötigt wird – und alle Dateien im Container vor dem Zugriff des Betriebssystems geschützt sind.



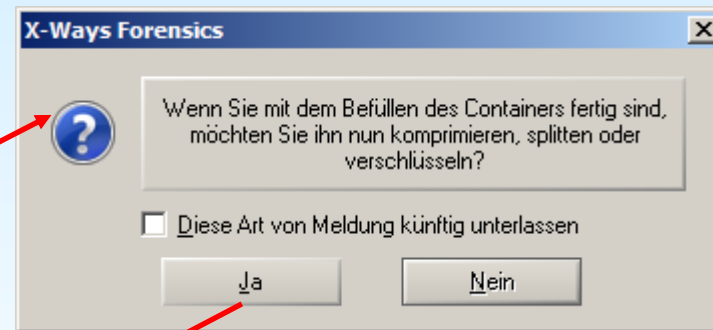
Sie können Dateien von beliebigen Quelldatenträgern in den selben Container kopieren. Hierbei ist es irrelevant, ob es sich bei der Quelle um Datenträger oder Images handelt, und auch ob diese in einen Fall eingebunden oder einfach so geöffnet wurden.

# 9: Datei-Container

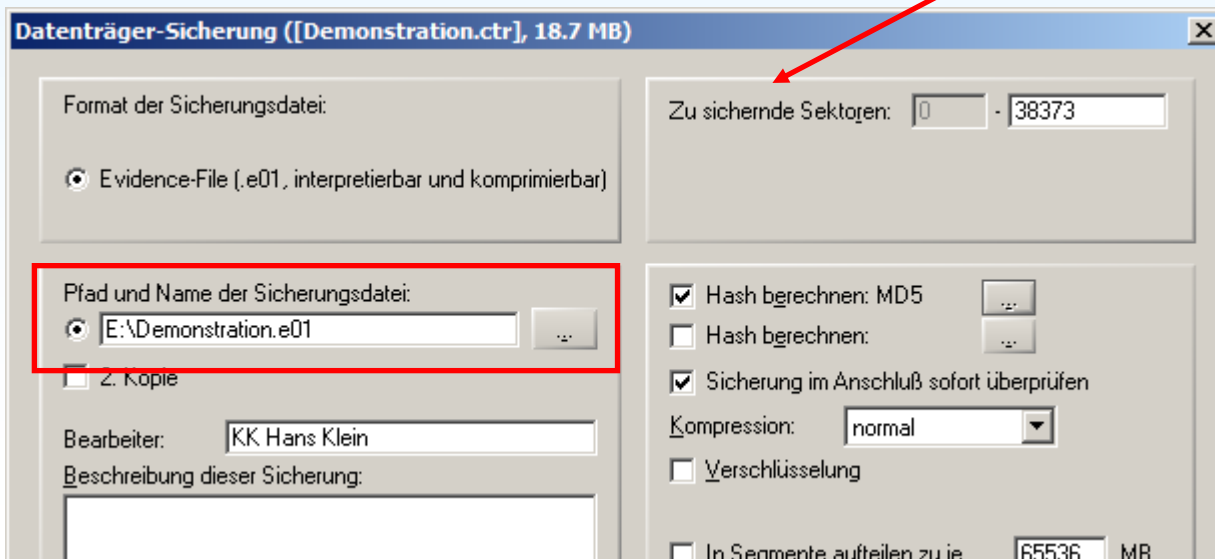
## Schritt 3: Container schließen



Wenn alle gewünschten Objekte zum Container hinzugefügt worden sind, gehen Sie wieder zu *Specialist* → *Datei-Container* und wählen Sie *Schließen*.



Klicken Sie auf *Ja*.



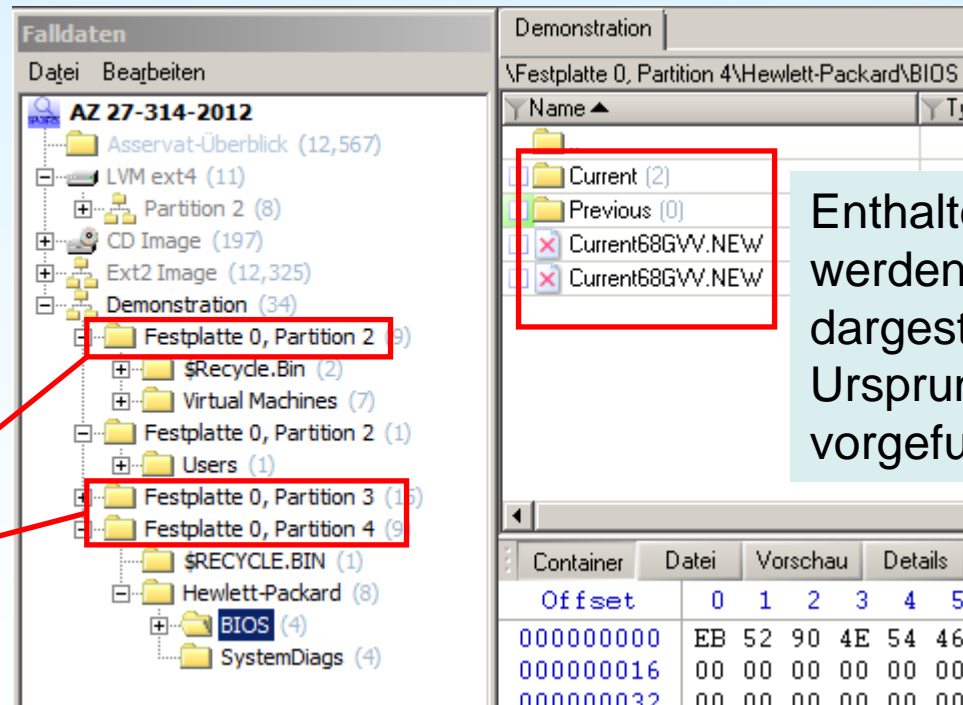
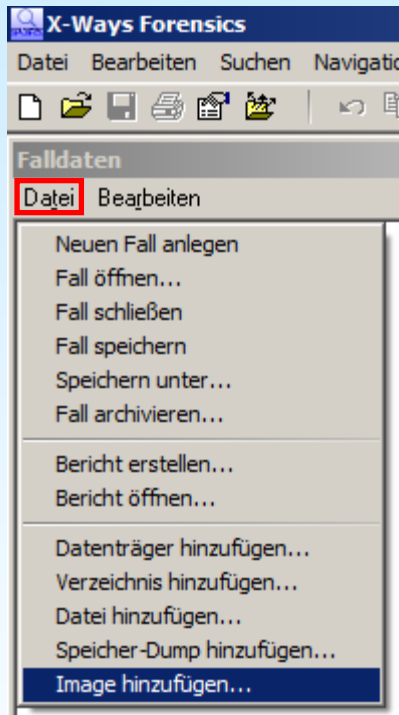
Dieser Dialog ist aus Kapitel 1, Schritt 2 bereits bekannt – nur jetzt auf *Evidence-File* fest voreingestellt.

Geben Sie einen geeigneten Zielort an und klicken Sie OK.

# 9: Datei-Container

## Schritt 4: Container in Fall einbinden

Container werden von X-Ways Forensics wie ganz normale Images behandelt – fügen Sie Ihren soeben erzeugten Container Ihrem Fall hinzu (wie in Kapitel 2, Schritt 2).



Ursprungssasservate  
werden zum obersten  
Verzeichnisnamen

Enthaltene Objekte  
werden im Container  
dargestellt wie im  
Ursprungssasservat  
vorgefunden.