

# *X-Ways Forensics*

## Anlegen eines Falls und Hinzufügen von Image-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](mailto:mail@x-ways.com)

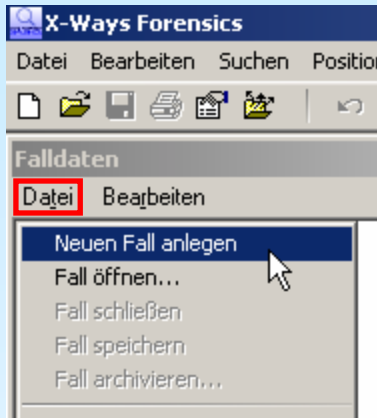
Tel.: 0221-420 486 5

Stand: v14.1. Bitte abonnieren Sie den Newsletter, um über Neuerungen in der Software informiert zu werden.

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

# Schritt 1: Fall anlegen

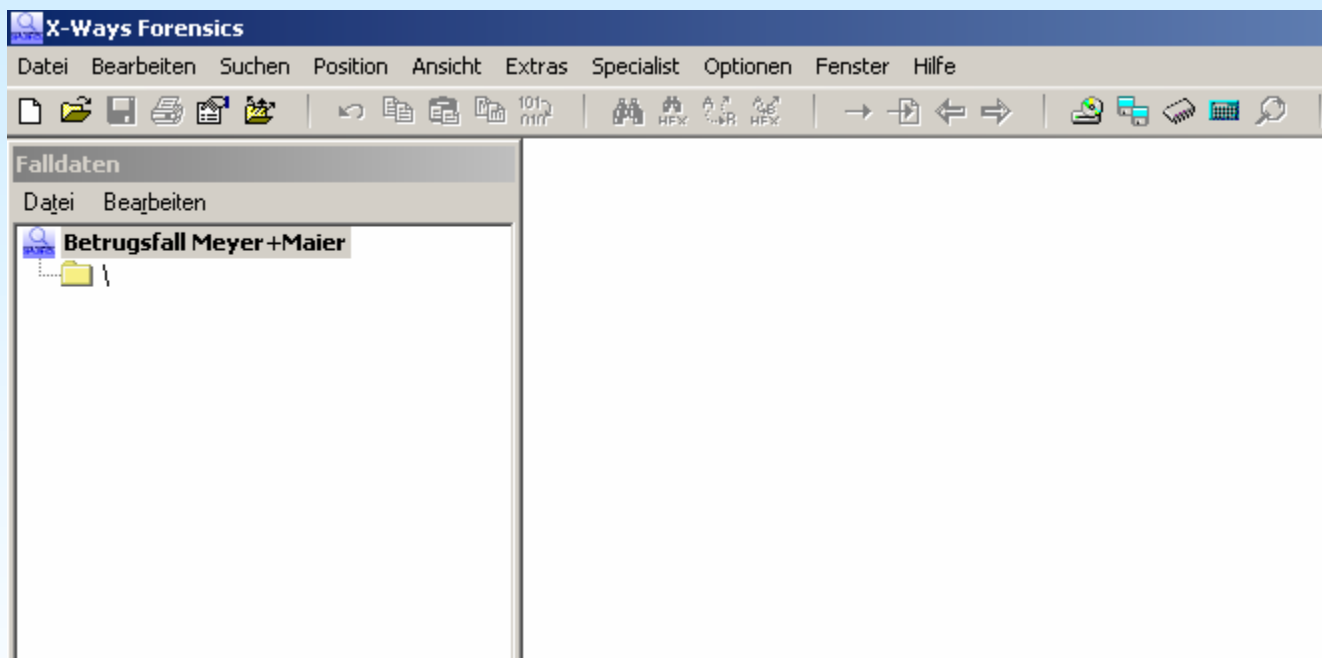
Wählen Sie im Datei-Menü des Falldatenfensters den Menübefehl „Neuen Fall anlegen“ und füllen Sie das folgende Dialogfenster aus:



The image shows the 'Falldaten' dialog box in X-Ways Forensics. The dialog is titled 'Falldaten' and contains the following fields and options:

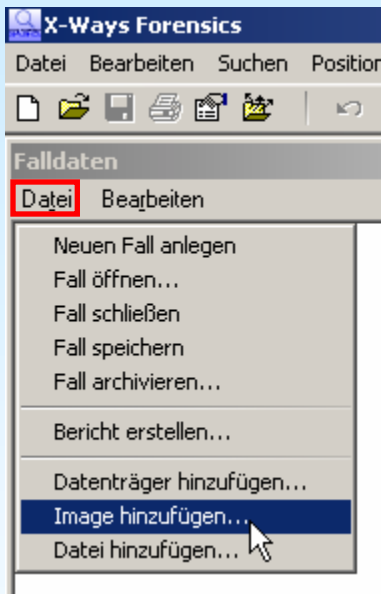
- Bez./Nr. des Falls:** Betrugfall Meyer+Maier
- Eröffnet am:** 05.06.2007 16:03:29
- Falldatei:** (empty)
- Beschreibung:** Untersuchung eines im Büro von Meyer+Maier beschlagnahmten Systems auf der Suche nach Belegen für einen vermuteten großangelegten Betrugsversuch.
- Bearbeiter, Organisation, Adresse:** Hans Müller, Kriminalpolizei, Berlin
- Allgem. Aktivitäten mitprotokollieren
- Wiederherst./Kopieren protokollieren
- Protokoll mit Bildschirmfotos
- Asservat-Ordner als Standardausgabe
- Protokoll: 0 Bytes
- Löschen... messages.txt... copylog.html...
- Bericht (Optionen)... Anzeige-Zeitzone...
- Individuelle Zeitzonen je Asservat
- Autom. Speichern (in Min.) 10
- Falldatei mit Paßwort schützen<sup>3</sup>
- Anzahl der Falldatei-Backups: 3
- Partitionen automatisch mit in Fall aufnehmen
- Buttons: OK, Abbrechen, SIDs..., Hilfe

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



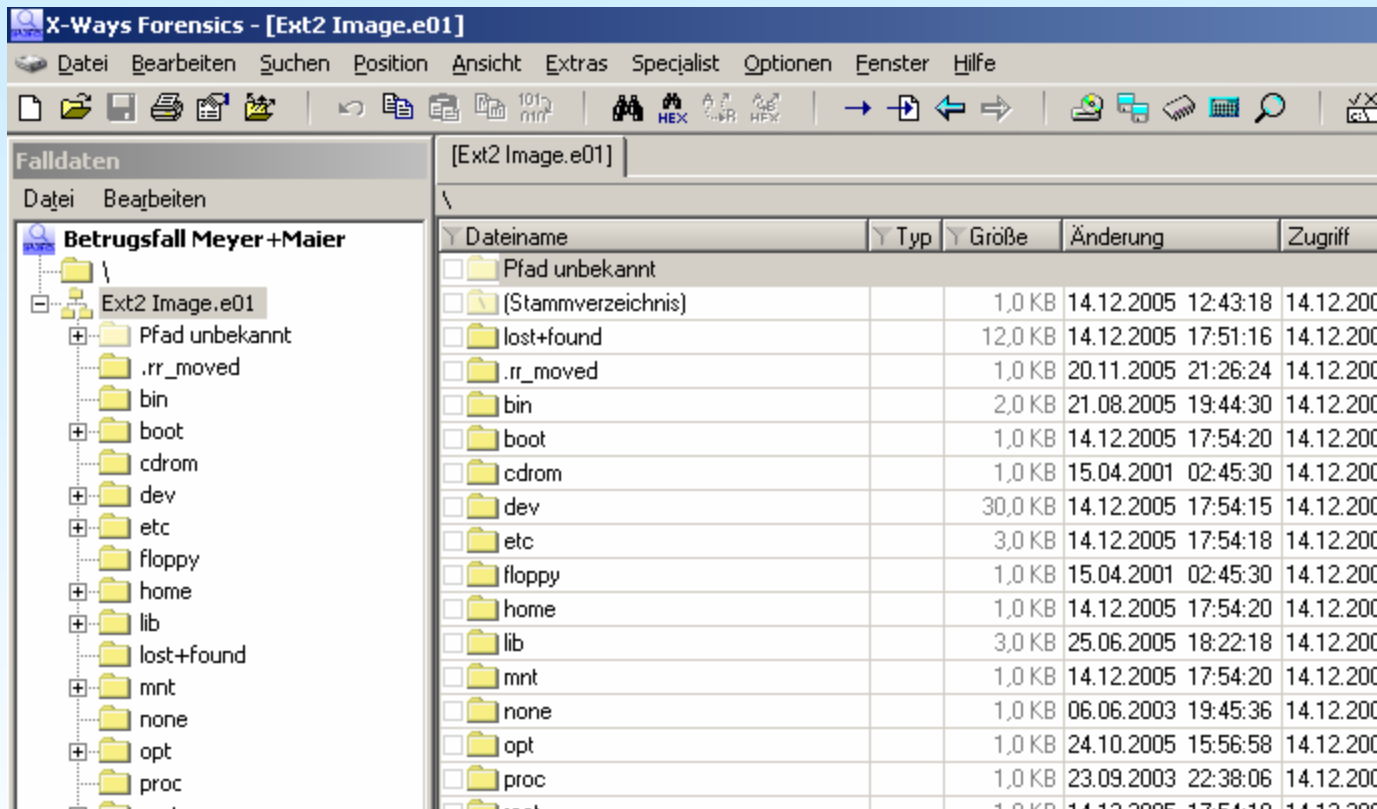
Jetzt müssen Image-Dateien zur Untersuchung hinzugefügt werden.

## 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) oder Evidence-Files (.e01) auswählen, die dann interpretiert werden.



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,...