

X-Ways Forensics

Suchen

Beispiel: Vorkommnisse von „John“ und „Doe“

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

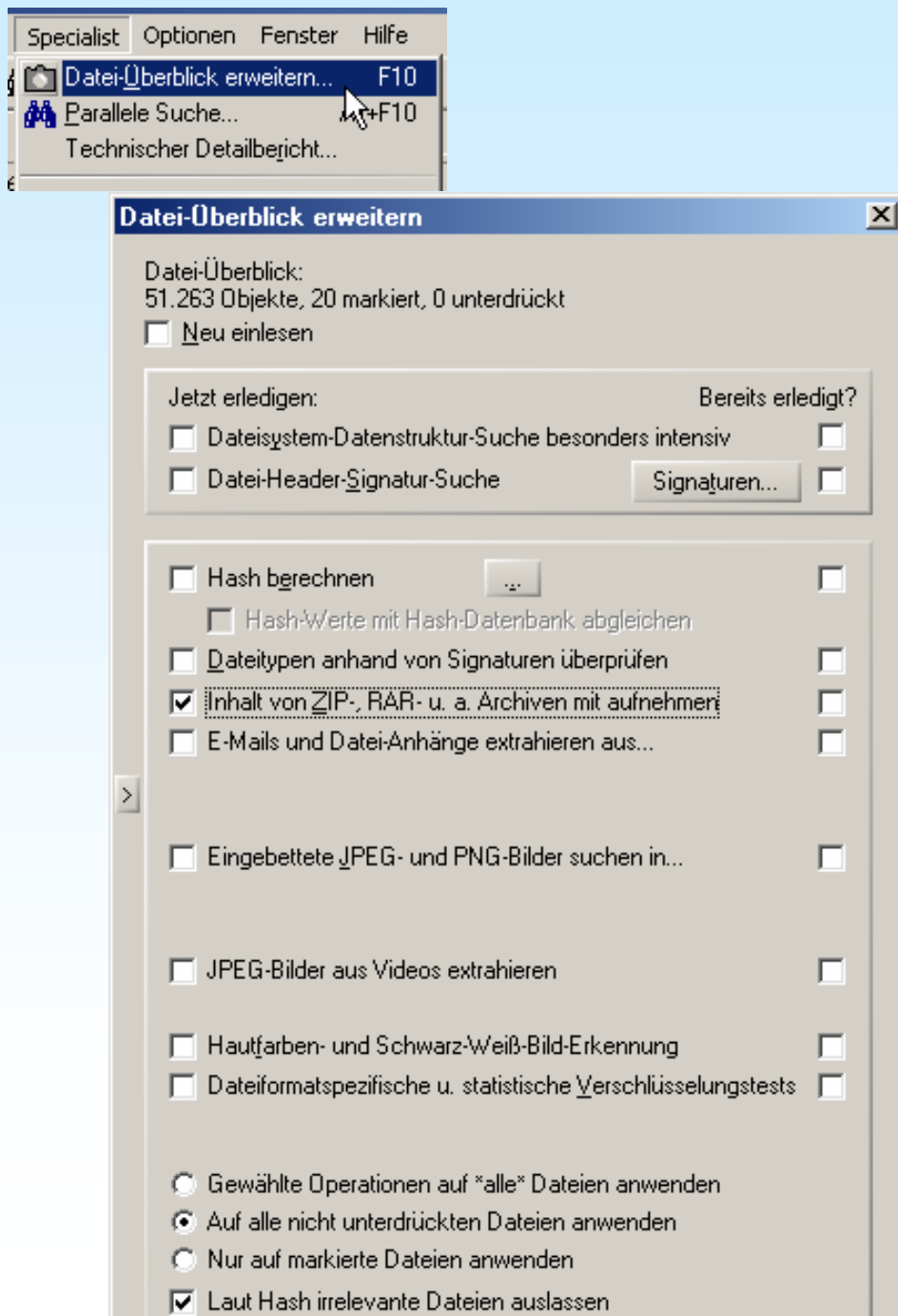
X-Ways Software Technology AG
Agrippastr. 37-39
50676 Köln
E-Mail: mail@x-ways.com

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: Datei-Überblick erweitern

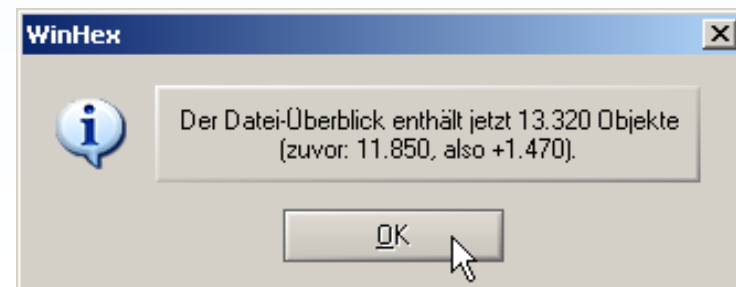


Das Erweitern des Datei-Überblicks erlaubt u. a. die Suche in komprimierten Dateien in Archiven.

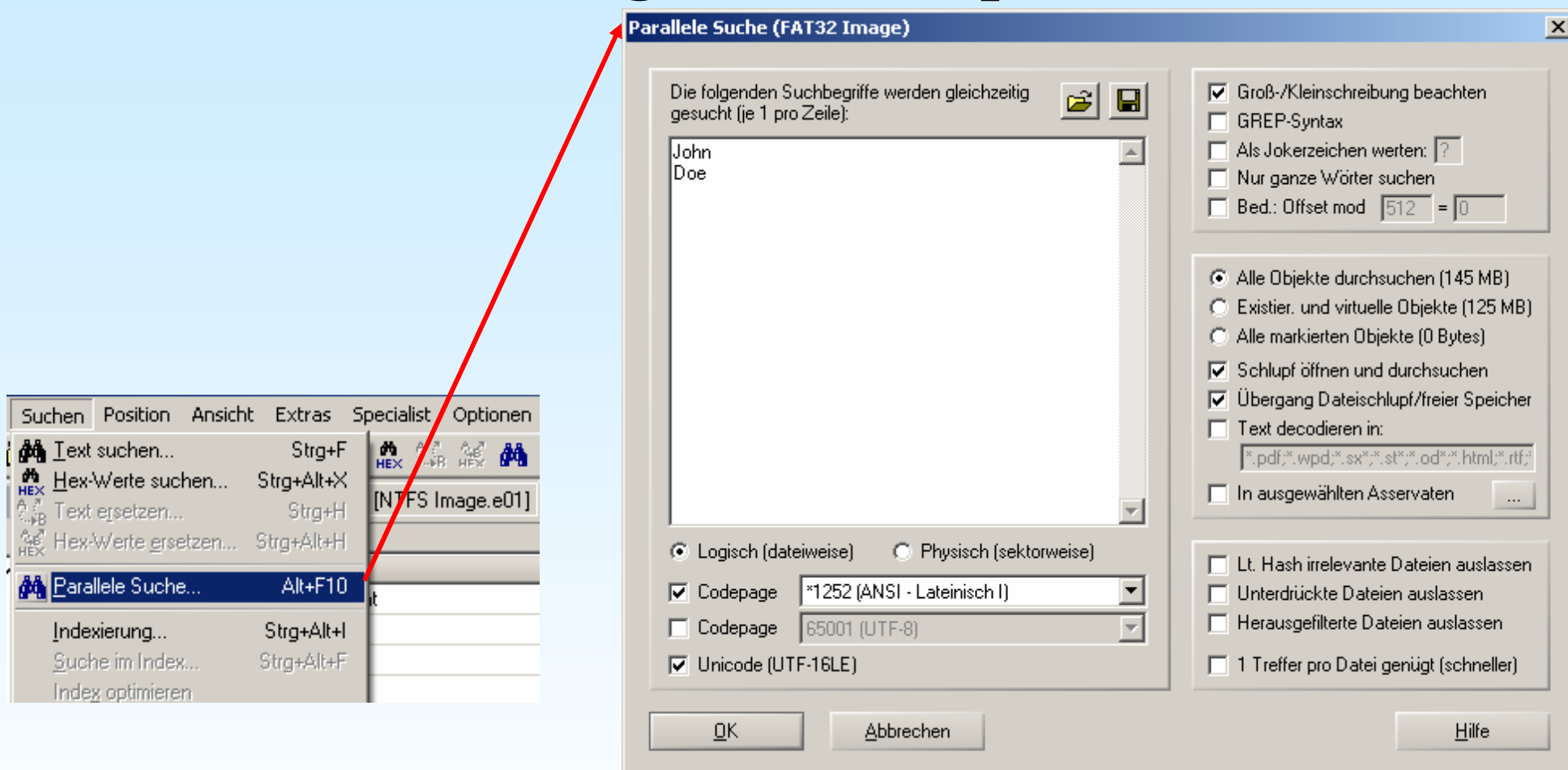
Drücken Sie hierzu auf F10 oder rufen Sie „Datei-Überblick erweitern“ aus dem Specialist-Menü auf.

Wählen Sie die Option „Inhalt von ZIP-, RAR- u.a. Archiven mit aufnehmen“ aus.

Klicken Sie auf OK, was schließlich zu einer Meldung ähnlich der untenstehenden führen wird. Bestätigen Sie mit OK.



Schritt 2: Suchbegriffe und -optionen auswählen



In diesem Fall seien wir nur interessiert an Vorkommnissen von John und Doe als ganze Wörter. Wenn alle Einstellungen gemacht sind, klicken Sie auf OK.

Die Suche wird jetzt anlaufen. Wenn Sie beendet ist, haben Sie die Möglichkeit, die Suchtreffer auszuwerten (Bildschirmfoto und Erläuterungen auf den beiden folgenden Seiten).

Schritt 3: Suchtreffer auswerten

Falldaten

Datei Bearbeiten

Betrugsfall Meyer+Maier

- Ext2 Image.e01
 - Pfad unbekannt
 - .rr_moved
 - bin
 - boot
 - cdrom
 - dev
 - etc
 - floppy
 - home
 - dsl
 - .dillo
 - .emelfm
 - .fluxbox
 - .index
 - .sylpheed
 - .xmms
 - .xtdesktop
 - Docs
 - GNUstep
 - Pictures
 - lib
 - lost+found
 - mnt
 - none
 - opt
 - proc

[Markierte Treffer]

[Index-Suchtreffer]

John

Doe

[Ext2 Image.e01]

Suchtreffer in \ und Unterverzeichnisse

Offset	Rel. Offs.	Suchtreffer	Dateiname	Erw.	Größe
9579890	90	2004 #email questions to john@damnsmlinux.org	sqlitebook.pl	pl	6,6 KI
957C494	94	:box and jwm # Written by John Andrews DESKTOP=`cat	switcher.sh	sh	347 Byte
A293C1C	1C	/usr/bin/perl -w # Author John Andrews `killall -9 fluxter &	enhance		0,5 KI
A44C447	47	n Small Linux # Written by John Andrews # Makes Nirc w	irc.to.pl	pl	1,0 KI
A5B92BA	48EBA	; -- John F. Kennedy Vis	naim		355 KI
A6F7849	49	51 phil Exp \$ # Written by John Hasler <john@dhh.gt.org>	poff		2,1 KI
A6F7856	56	# Written by John Hasler <john@dhh.gt.org> and based c	poff		2,1 KI
A6F861F	21F	;; esac ## small add in by john to make it play nice with a	pon		1,0 KI
A7B395C	3115C	1 öiÄ 2 NT ÖYÜwÄ IIÉYDOe»Ý äIN É SHA`vöä3 vc`_.	smbclient		240 KI
A9D3A3B	ADE3B	id/d d d@d%d'd dçç d.dld doe'eÜetfCEf*ñk<fŠf"xf gf_	libX11.so.6.2	2	0,7 MI
AAE399B	E19B	id/d d d@d%d'd dçç d.dld doe'eÜetfCEf*ñk<fŠf"xf gf_	libXutf8.so.0	0	448 KI
AB17A1B	4221B	id/d d d@d%d'd dçç d.dld doe'eÜetfCEf*ñk<fŠf"xf gf_	libXutf8.so.0	0	448 KI
AE7BF22	FCF22	suwe Gian-Carlo Pascutto John Riddoch (Solaris plugin) J	xmms		1,0 MI
BOED01A	1A	!/bin/sh # Odns-down by John Hasler 1 Apr 1999. You n	Odns-down		412 Byte
BOEDC18	18	#!/bin/sh # Odns-up by John Hasler 1999-2002. You rr	Odns-up		1,2 KI
B280B90	B90	[" ÖAIOb äfö"è C@_NÄ:" dOE§ 4f½ { Ü>{ >@`è<Aw ff.	luBIS14.pcf.gz	gz	13,4 KI
B9342D7	76D7	id/d d d@d%d'd dçç d.dld doe'eÜetfCEf*ñk<fŠf"xf gf_	nls_cp950.o	o	103 KI
B9C040C	C	! Hacked by John Andrews for the DSL proje	BizCard		3,2 KI
B9ED4F9	78F9	evin (echo + stereo plugin) John Riddoch (Solaris plugin) J	xmms.mo	mo	62,4 KI

Sektoren Datei Vorschau Galerie Kalender Legende Sync

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
0A6F7820	39	2F	30	38	2F	32	38	20	31	36	3A	33	34	3A	35	31	9/08/2008 16:34:51
0A6F7830	20	70	68	69	6C	20	45	78	70	20	24	0A	23	20	57	72	phil Exp \$ # Wr
0A6F7840	69	74	74	65	6E	20	62	79	20	4A	6F	68	6E	20	48	61	itten by John Ha
0A6F7850	73	6C	65	72	20	3C	6A	6F	68	6E	40	64	68	68	2E	67	sler <john@dhh.g
0A6F7860	74	2E	6F	72	67	3E	20	61	6E	64	20	62	61	73	65	64	t.org> and based
0A6F7870	20	6F	6E	20	77	6F	72	6B	20	0A	23	20	62	79	20	50	on work # by P
0A6F7880	68	69	6C	20	48	61	6E	64	73	20	3C	70	68	69	6C	40	hil Hands <phil@
0A6F7890	68	61	6E	64	73	2E	63	6F	6D	3E	2E	20	20	44	69	73	hands.com>. Dis
0A6F78A0	74	72	69	62	75	74	65	64	20	75	6E	64	65	72	20	74	tributed under t
0A6F78B0	68	65	20	47	4E	55	20	47	50	4C	0A	0A	69	66	20	5B	he GNU GPL if [
0A6F78C0	20	2D	78	20	2F	75	73	72	2F	62	69	6E	2F	6B	69	6C	-x /usr/bin/kil

- 1** Ein Klick auf diesen Schalter ruft die Suchbegriffs- und Suchtrefferlisten auf.
- 2** Dies ist die Suchtrefferliste. Sie können die Suchtreffer eingrenzen, indem Sie entweder Unterverzeichnisse im Verzeichnisbaum **3** auswählen oder die Filtermethoden des Verzeichnis-Browsers **4** anwenden.
- 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.