

X-Ways Forensics

Searching

Example: Occurrences of “John” and “Doe”

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

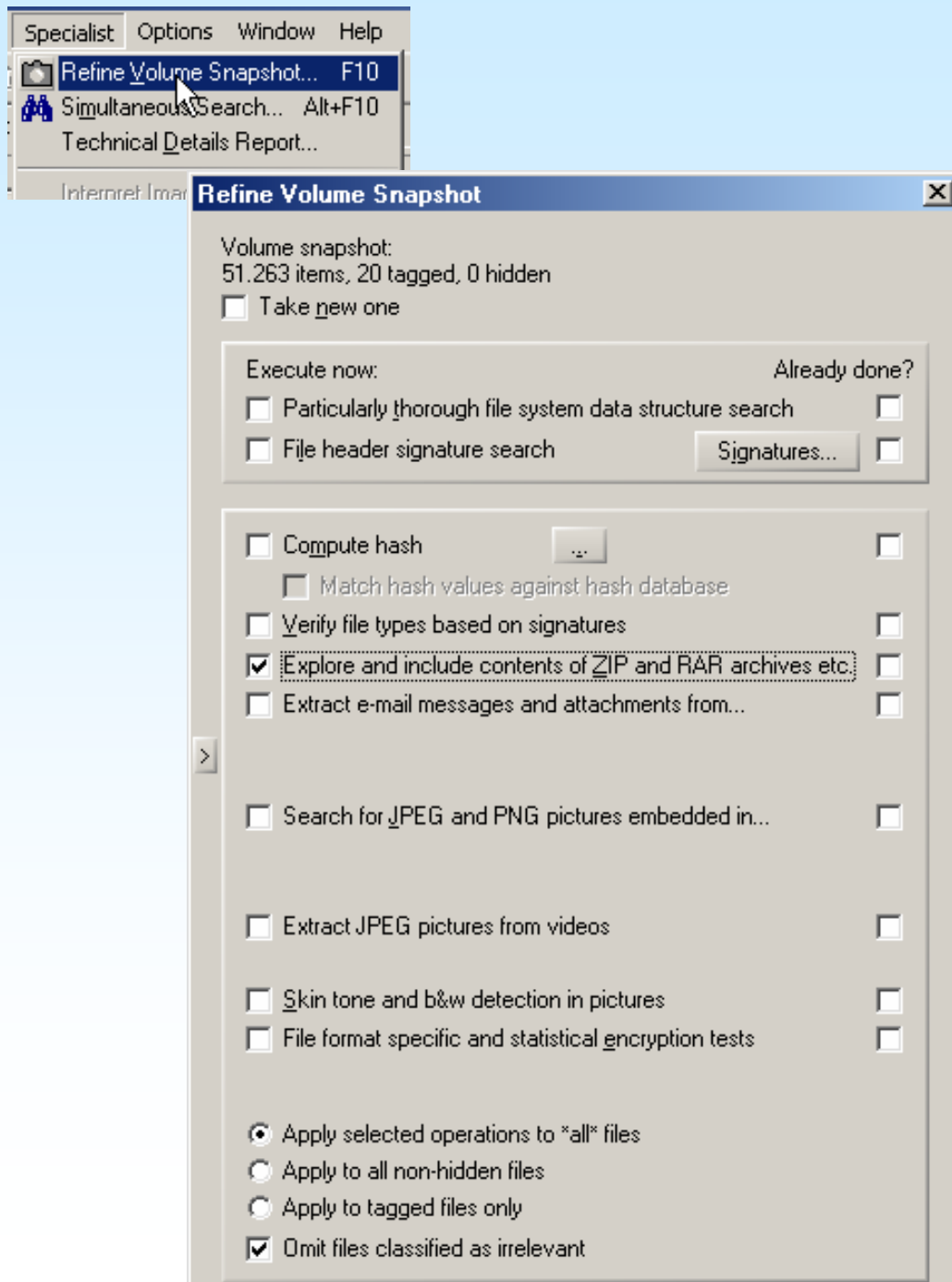
E-mail: mail@x-ways.com

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: Refine Volume Snapshot

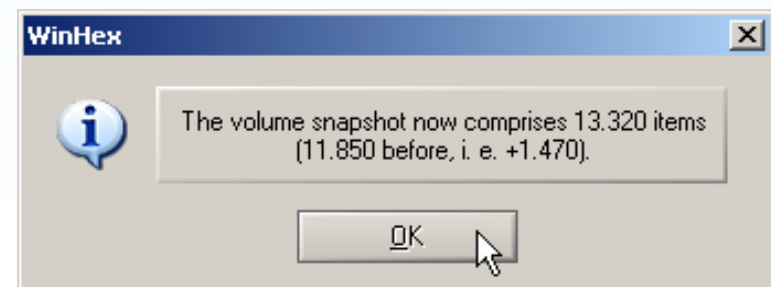


Refining the Volume Snapshot first will allow searching compressed files in archives (among others).

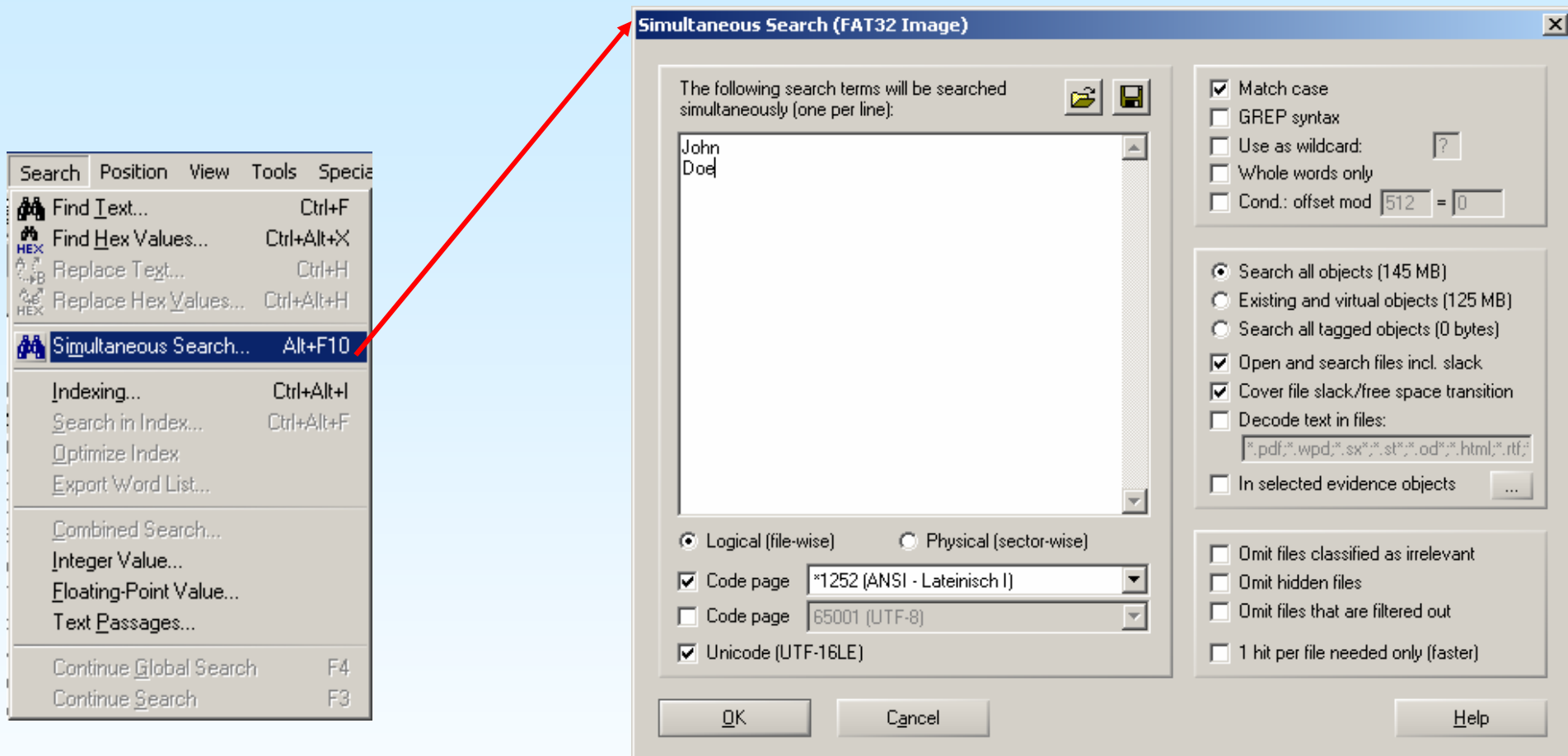
To that end, press F10 or invoke “Refine Volume Snapshot” from the Specialist menu.

Check the option to “Explore and include contents of ZIP and RAR archives etc.”.

Then click ok, which will eventually result in a message like the one below. Acknowledge with OK.



Step 2: Enter search terms and options



In this case, we are interested in John and Doe as whole words. Once set, click OK.

The search will run and eventually you will be able to review the search hits (s. next two pages for screenshot and explanations).

Step 3: Reviewing search hits

Case Data

File Edit

Investigation Doe, John

- Ext2 Image.e01
 - Path unknown
 - .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

[Notable hits]

[Index search hits]

John
Doe

[Ext2 Image.e01]

Search hits in \ and subdirectories

Offset	Rel. ofs.	Search hits	Filename	Ext.	Size
9579890	90	2004 #email questions to john@damnsmalllinux.org	sqlitebook.pl	pl	6,6 K
957C494	94	:box and jwm # Written by John Andrews DESKTOP=`cat	switcher.sh	sh	347 byte
A293C1C	1C	l/usr/bin/perl -w # Author John Andrews `killall -9 fluxter &	enhance		0,5 K
A44C447	47	n Small Linux # Written by John Andrews # Makes Nirc w	irccto.pl	pl	1,0 K
A5B92BA	48EBA	p; -- John F. Kennedy Vis	naim		355 K
A6F7849	49	51 phil Exp \$ # Written by John Hasler <john@dhh.gt.org:	poff		2,1 K
A6F7856	56	# Written by John Hasler <john@dhh.gt.org> and based c	poff		2,1 K
A6F861F	21F	: esac ## small add in by john to make it play nice with a	pon		1,0 K
A7B395C	3115C	1 0iÅ 2 NT 0Y0wÅ ÏEYD0e»Ý ãIN É SHA`v0ã3 vo`_	smbclient		240 K
A9D3A3B	ADE3B	id/d d d@d%d'd dçç d.dld doe'e0etfCEf*ñk<fŠF''fxf gfi	libX11.so.6.2	2	0,7 M
AAE399B	E19B	id/d d d@d%d'd dçç d.dld doe'e0etfCEf*ñk<fŠF''fxf gfi	libXutf8.so.0	0	448 K
AB17A1B	4221B	id/d d d@d%d'd dçç d.dld doe'e0etfCEf*ñk<fŠF''fxf gfi	libXutf8.so.0	0	448 K
AE7BF22	FCF22	suwe Gian-Carlo Pascutto John Riddoch (Solaris plugin) Ji	xmms		1,0 M
BOED01A	1A	! /bin/sh # 0dns-down by John Hasler 4 Apr 1999. You n	0dns-down		412 byte
BOEDC18	18	#!/bin/sh # 0dns-up by John Hasler 1999-2002. You r	0dns-up		1,2 K
B280B90	B90	(" 0A10b äfö`è C@,NÁ: *dOE\$ 4f½ { Ú>[>@`è<Aw fl.	luBIS14.pcf.gz	gz	13,4 K
B9342D7	76D7	id/d d d@d%d'd dçç d.dld doe'e0etfCEf*ñk<fŠF''fxf gfi	nls_cp950.o	o	103 K
B9C040C	C	! Hacked by John Andrews for the DSL proje	BizCard		3,2 K
B9ED4F9	78F9	win (echo + stereo plugin) John Riddoch (Solaris plugin) Ji	xmms.mo	mo	62,4 K

Sectors	File	Preview	Gallery	Calendar	Legend	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	9/08/28 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 Clicking this button calls the search term and search hit lists.
- 2 This is the search hit list. You can narrow search hits down by either selecting sub-directories in the directory tree **3** or by applying filtering methods available in the directory browser. **4**
- 5 This is the search term list. Selecting one or more search terms allows narrowing the search hits to just the currently desired terms. Double-click a single term or use multiple-selection and the Enter button or key.
- 6 Click a search hit so the lower half of the screen will bring the hit into view.