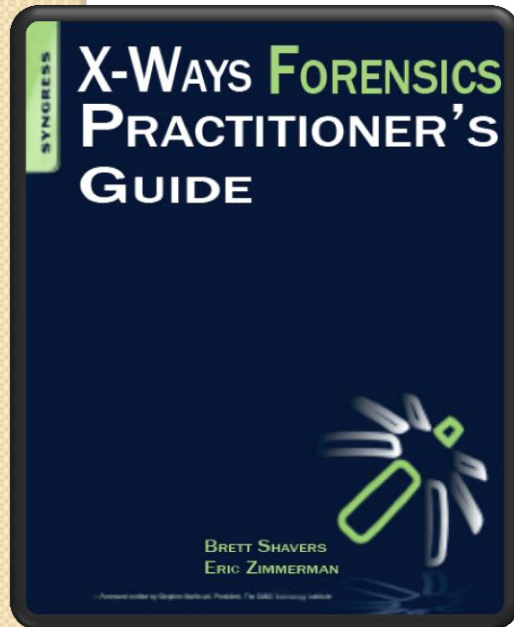


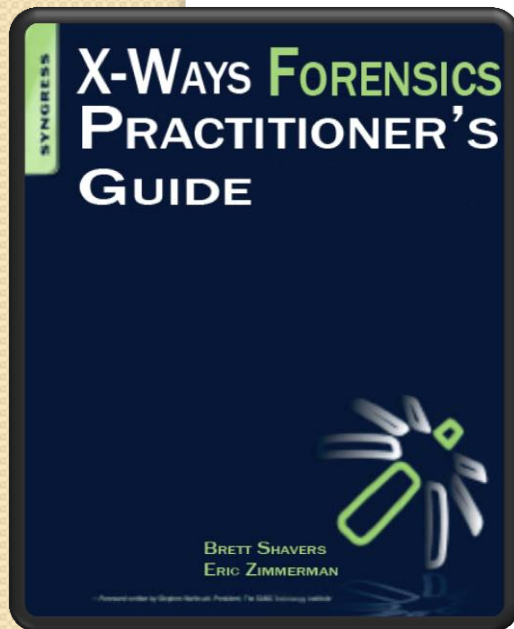
X-WAYS FORENSICS

Advanced Methods and Techniques



The XWF Book

- Not done yet...
- Eric Zimmerman (FBI) is the co-author
- Jimmy Weg is the tech editor
- Will be done in a few months
- This is a preview of some of the information in the book



Not a bash on any other program

- Accessdata's FTK works
- Guidance Software's Encase Forensics works
- TechPathWays' ProDiscover works too

This will be just talking about
X-Ways Forensics*.

*And if you don't already have XWF....you should really consider getting it...

Topics

- Tips on XWF
 - Make it run faster
 - Run it from a boot disc
 - Using XWF in eDiscovery work
- Features you may not have known before
- There are lots of, “*I didn’t know XWF could do that*” kind of features

The dongle

- Do you use XWF outside your office?
 - Insure it!
- Network dongle available!



Speeding up XWF

Keep the data on a different drive

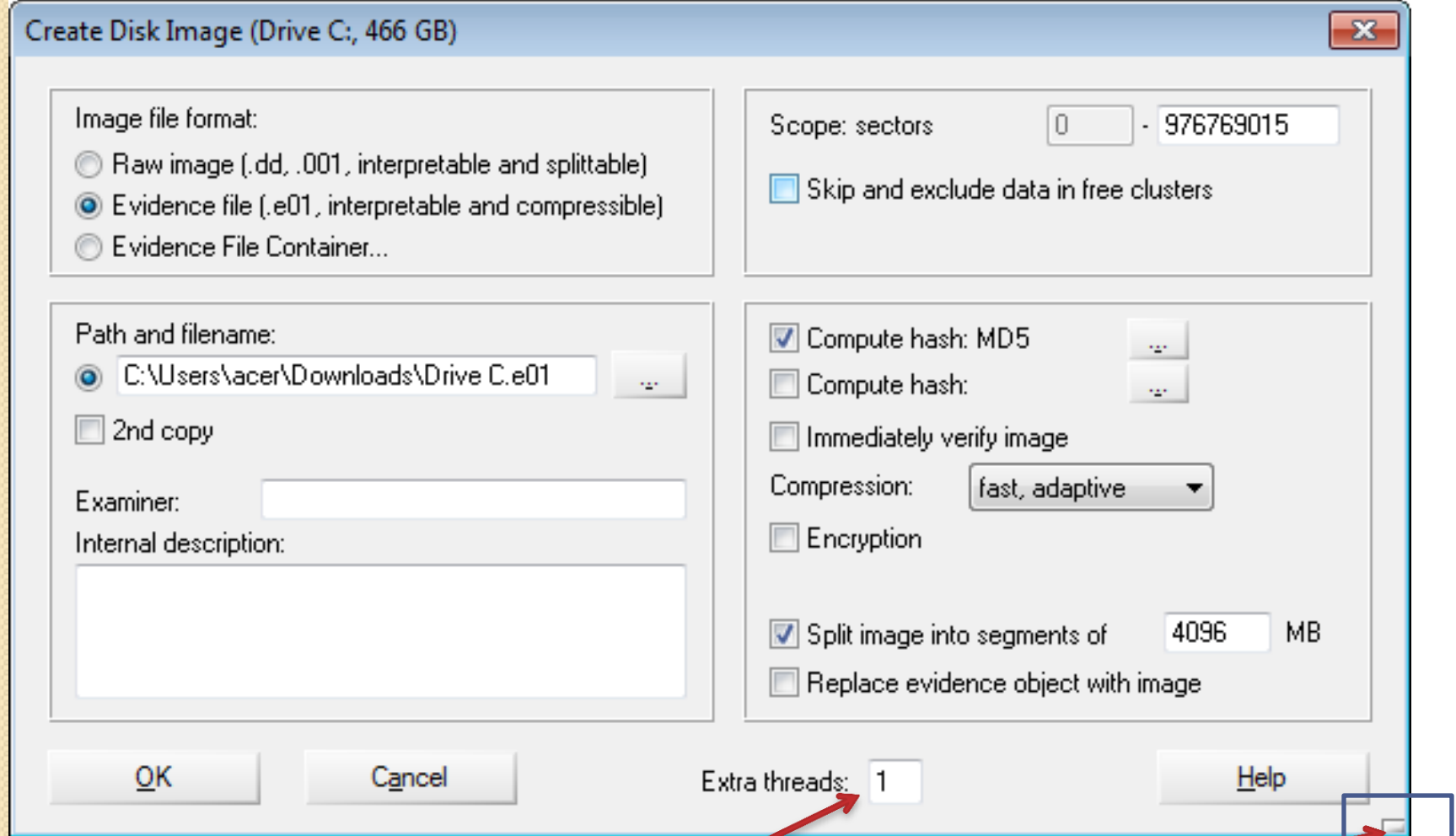
- Keep the hard drives separate
 - Don't run XWF from the same drive your image is on or being created onto.

Analysis Speed Increase

- Do you have extra examiners..?
- Shared analysis and distributed volume snapshot refinement capable.
- Multiple machines on the same network can access the same image/s.
- Case results are all saved to the same case file!

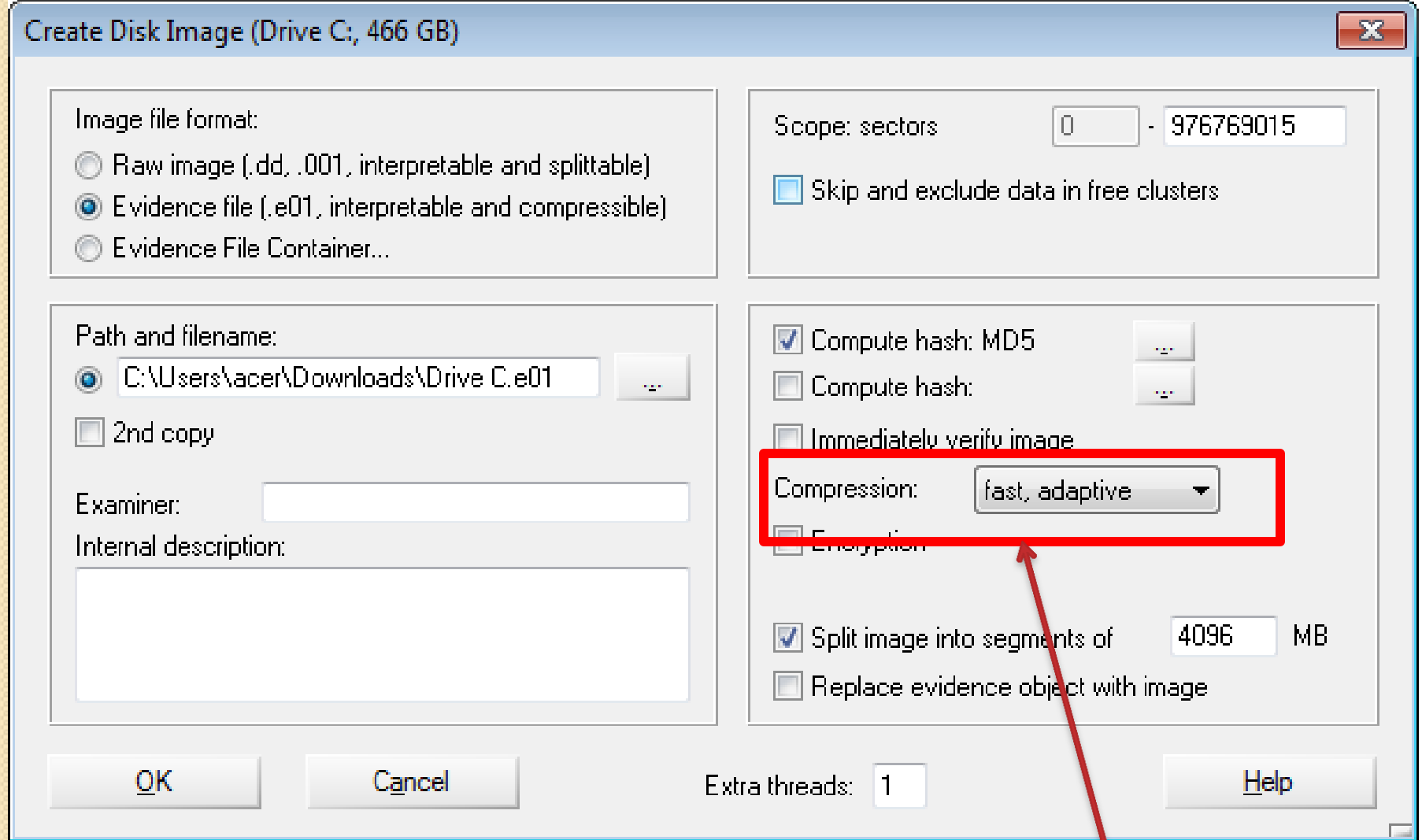
Imaging Speed

- Compress? Why?
- Image to the network or RAID
 - Store images on a RAID for higher transfer rate.
 - Avoid using USB connections with media
- When imaging, change the number of threads, based on your hardware, to increase imaging speed.



Speed tip!

By default, XWF uses four threads when creating E01 files. Adjust as fits your hardware.



Speed tip!

You can change the compression during imaging, just in case your needs change



Computer Set Up

Computer Set Up

- The **more processors** you have, the better (of course)
- 64-bit is faster than 32-bit (no kidding)
- **More RAM**, faster it runs (duh)
- **But** it can run on 256MB!!! Can other tools do that?

Computer Set Up

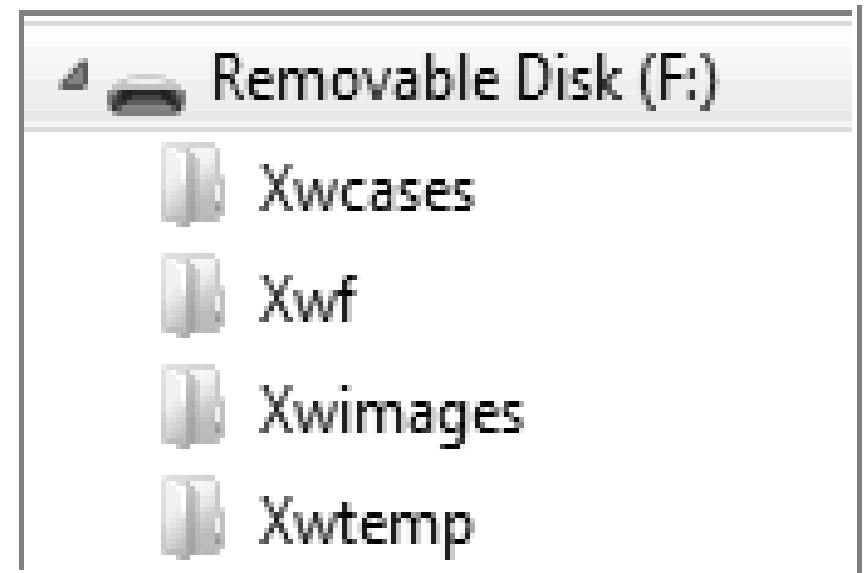
- Turn off the AV.
- Avoid using compressed images created with something other than XWF.
- Don't select everything for data carving, just what you need.



Portable Configuration

Portable Installation

- When creating a portable installation of XWF, you can use the “.” and “..” options to configure XWF to work, regardless of the drive letter assigned to the XWF medium.



General Options



☒ Restore last window arrangement³

16 recent documents in list

☐ Items in Windows context menu³

☒ Allow multiple program instances³

☐ Do not update file time

☒ Open data windows maximized

☒ WinHex context menu

☒ Show file icons³

☒ Save program settings in .cfg file

☒ Number partitions by disk location

☒ Auto-detect deleted partitions

☒ Sector reading cache

☐ Check for surplus sectors

☐ Alternative disk access method³

Substitute pattern for unreadable sectors:

UNREADABLESECTOR

Folder for temporary files:

..\temp

Folder for images and backup files:

..\images

☐ Default when adding images

Folder for cases and projects:

..\case

Folder for templates and scripts:

.

Folder for internal hash database:

..\HashDB

☐ GUI of X-Ways Investigator³

☐ Always run as administrator

☒ Gallery: Show pictures in archives

☒ Gallery: Allow auxiliary thumbnails

Preferred thumbnail size: 80

☐ Progress notification...

☐ Generate 0x 000A with Enter

☐ Generate Tabs with Tab key

☒ <0x20 substitute character:

☐ Display bytes as text one by one

☒ Hexadecimal offsets

☒ Virtual addresses in RAM editor

☒ Display page separators³

16 bytes per line

8 -byte groups

< > < > Dialog window style

☒ Search hit highlighting in File mode³

☒ Auto coloring for FILE records etc.³

Block background color:

Record background color:

Annotation color:

☒ Highl. modified bytes:

Font: Courier

OK

Cancel

Display time zone...

Notation...

Help

General Options



☒ Restore last window arrangement³

16 recent documents in list

☐ Items in Windows context menu³

☒ Allow multiple program instances³

☐ Do not update file time

☒ Open data windows maximized

☒ WinHex context menu

☒ Show file icons³

☒ Save program settings in .cfg file

☒ Number partitions by disk location

☒ Auto-detect deleted partitions

☒ Sector reading cache

☐ Check for surplus sectors

☐ Alternative disk access method³

Substitute pattern for unreadable sectors:

UNREADABLESECTOR

Folder for temporary files:

..\temp

Folder for images and backup files:

..\images

☐ Default when adding images

Folder for cases and projects:

..\case

Folder for templates and scripts:

.

Folder for internal hash database:

..\HashDB

☐ GUI of X-Ways Investigator³

☐ Always run as administrator

☒ Gallery: Show pictures in archives

☒ Gallery: Allow auxiliary thumbnails

Preferred thumbnail size: 80

☐ Progress notification...

☐ Generate 0x 000A with Enter

☐ Generate Tabs with Tab key

☒ <0x20 substitute character:

☐ Display bytes as text one by one

☒ Hexadecimal offsets

☒ Virtual addresses in RAM editor

☒ Display page separators³

16 bytes per line

8 -byte groups

< > < > Dialog window style

☒ Search hit highlighting in File mode³

☒ Auto coloring for FILE records etc.³

Block background color:

Record background color:

Annotation color:

☒ Highl. modified bytes:

Font: Courier

OK

Cancel

Display time zone...

Notation...

Help

General Options



☒ Restore last window arrangement³

16 recent documents in list

☐ Items in Windows context menu³

☒ Allow multiple program instances³

☐ Do not update file time

☒ Open data windows maximized

☒ WinHex context menu

☒ Show file icons³

☒ Save program settings in .cfg file

☒ Number partitions by disk location

☒ Auto-detect deleted partitions

☒ Sector reading cache

☐ Check for surplus sectors

☐ Alternative disk access method³

Substitute pattern for unreadable sectors:

UNREADABLESECTOR

Folder for temporary files:

..\temp

Folder for images and backup files:

..\images

☐ Default when adding images

Folder for cases and projects:

..\case

Folder for templates and scripts:

.

Folder for internal hash database:

..\HashDB

☐ GUI of X-Ways Investigator³

☐ Always run as administrator

☒ Gallery: Show pictures in archives

☒ Gallery: Allow auxiliary thumbnails

Preferred thumbnail size: 80

☐ Progress notification...

☐ Generate 0x 000A with Enter

☐ Generate Tabs with Tab key

☒ <0x20 substitute character:

☐ Display bytes as text one by one

☒ Hexadecimal offsets

☒ Virtual addresses in RAM editor

☒ Display page separators³

16 bytes per line

8 -byte groups

< > < > Dialog window style

☒ Search hit highlighting in File mode³

☒ Auto coloring for FILE records etc.³

Block background color:

Record background color:

Annotation color:

☒ Highl. modified bytes:

Font: Courier

OK

Cancel

Display time zone...

Notation...

Help

Portable Installation

- Can be run from a flash drive on a live system
- Can be run from a booted Windows Forensics Environment (WinFE)
 - <http://winfe.wordpress.com>



Encrypting your images

Real Encryption for Images

- XWF can fully encrypt the data in the e01 image using 128 or 256-bit encryption!
- This is different from simple password protection.

Create Disk Image (Drive C:, 466 GB)

Image file format:

- ☐ Raw image (.dd, .001, interpretable and splittable)
- ☒ Evidence file (.e01, interpretable and compressible)
- ☐ Evidence File Container...

Scope: sectors

0

- 976769015

☐ Skip and exclude data in free clusters

Path and filename:

☒ C:\Users\acer\Downloads\Drive C.e01

☐ 2nd copy

Examiner:

Internal description:

☒ Compute hash: MD5

☐ Compute hash:

☐ Immediately verify image

Compression:

fast, adaptive

☐ Encryption

☒ Split image into segments of

4096

MB

☐ Replace evidence object with image

OK

Cancel

Extra threads:

1

Help



**Need to image AND triage/preview?
At the same time? No problem!**


- 
- Begin the imaging process
 - Open another instance of XWF, create a new case, and add the same device that you are imaging to the case.
 - Since you are working with a case, XWF will remember anything that you do against the device.

Image at network speed!

- USB3 and eSATA ports are fast, but not very widespread.
- F-Response allows imaging over the network. By either setting up your own gigabit network with a small switch or using an existing high-speed network, speed is FAST!
- You should create the images on a device that can handle the faster speed, such as SSD drives or a RAID array, not to an external USB drive...



Bad evidence hard drive?

Reverse Imaging

- Reverse disk imaging is meant for hard disks with a severe physical defect that causes a computer to freeze or crash when reaching a certain area on the hard disk.



XWF container file

Container Files

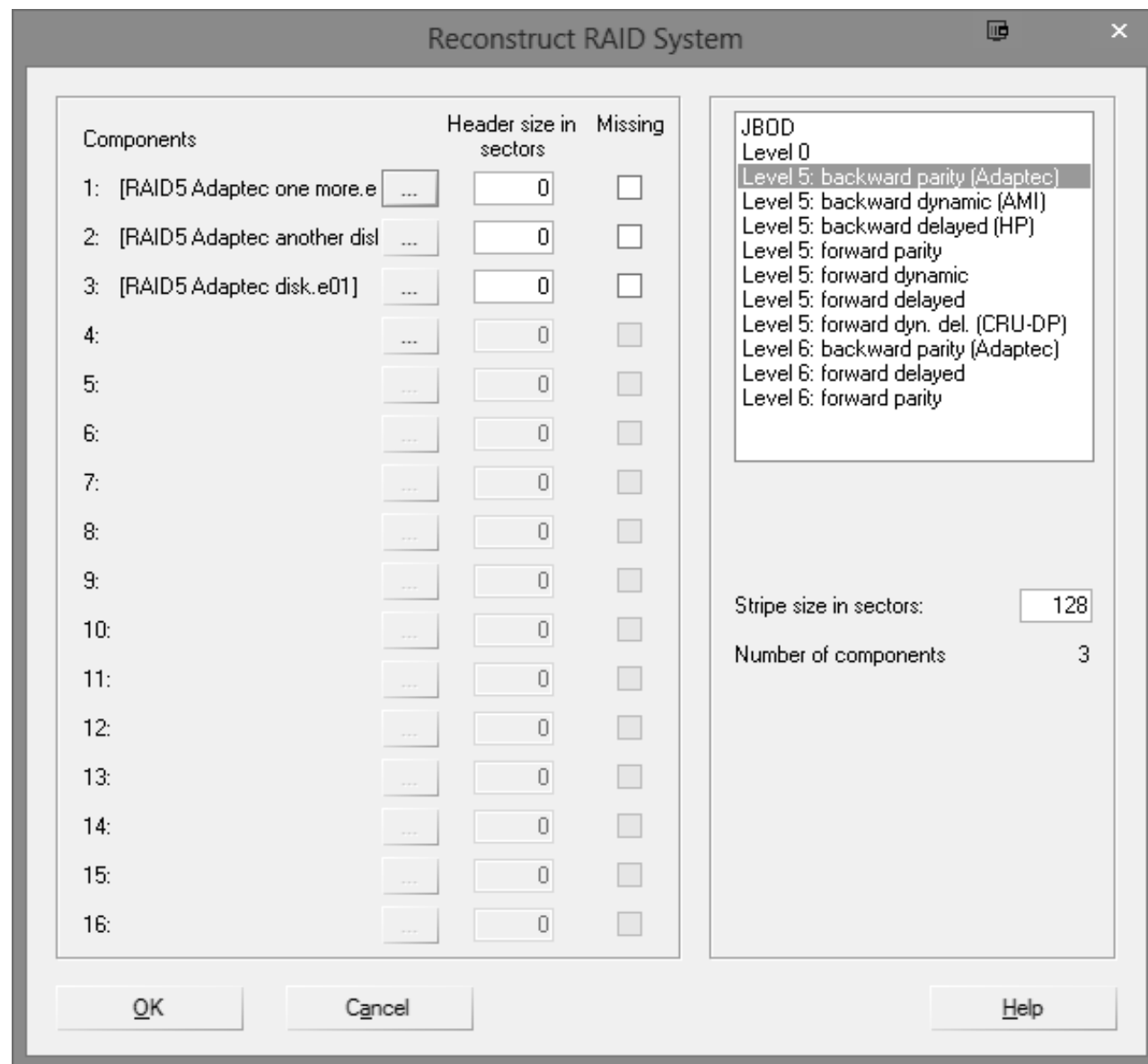
- XWF can create container files that are similar in function to container files used by other forensic suites.
- XWF container files can easily handle up to one billion objects.
- Encase 5/6/7, MountImagePro, and XWF can read the file container (basic metadata). XWF reads all metadata.



RAIDs

Don't image individual disks, image the array itself

- If possible, rather than image many hard drives in a RAID array, image the logical array itself.
- This can be done by imaging a computer in a live environment or via F-Response.
- But if you have to rebuild a RAID...

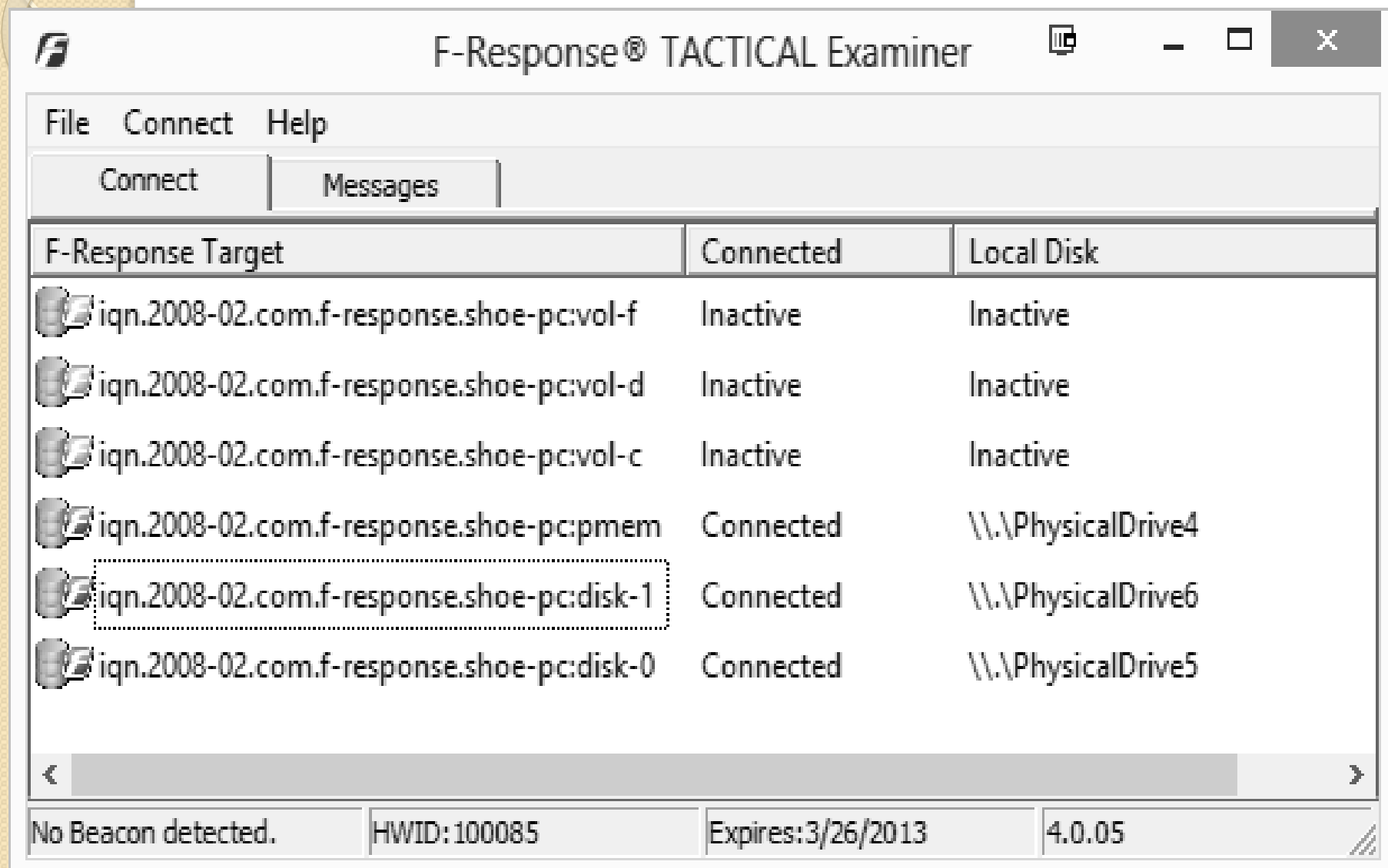


XWF does it's best, but trial and error helps to rearrange and find the right RAID config.



X-Ways Forensics Enterprise

Turn XWF into Enterprise XWF!





The Refine Volume Snapshot

Refine Volume Snapshot



Volume snapshot of Drive C: 828,375 items, 0 tagged, 0 hidden, 38,623 already viewed

☐ Take new one

Execute now:

Already done?

☐ Run X-Tensions



☐ Particularly thorough file system data structure search



☐ File header signature search

Signatures...



☒ Compute hash: MD5



☐ Match hash values against hash database



☒ Verify file types with signatures and algorithms



☐ Again

Signatures...

☒ Extract internal metadata, browser history and events



☒ Include contents of ZIP and RAR archives etc.

☐ JAR



☒ Extract e-mail messages and attachments from...



.pst;.ost;*.edb;*.dbx;*.pfc;*.mbox;*.mbx;*.eml;*.emlx;*.mht

☒ Uncover embedded data in miscellaneous file types



.pdf;.doc;*.ppt;*.pps;*.xls;*.ole2;*.jpg;thumb*.db;thumb*.dat

☒ Export JPEG pictures from videos



.3gp;.3gpp;*.asf;*.avi;*.divx;*.flv;*.m1v;*.m4v;*.mkv;*.mov

☒ Skin tone and b&w detection in pictures



☒ File format specific and statistical encryption tests



☒ Apply selected operations to *all* files

☐ Apply to tagged files only

☐ Omit files classified as irrelevant

☐ Omit hidden files

☐ Omit files that are filtered out

☐ In selected evidence objects



☐ Simultaneous Search

OK

Cancel

Help

The following search terms will be searched simultaneously (one per line):



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



- ☒ Match case
- ☐ GREP syntax³

- ☐ Whole words only³

Alphabet to define word boundaries: ...

☐ Cond.: offset mod 512 = 0

- ☐ Run X-Tensions ...

- ☒ All objects in volume snapshot (485 GB)
- ☐ Search all tagged objects (0 B)

- ☒ Open and search files incl. slack³

- ☒ Cover file slack/free space transition

- ☒ Decode text in files:

.pdf;.docx;*.pptx;*.xlsx;*.odt;*.odp;*.oc

- ☐ In selected evidence objects ...

- ☒ Omit files classified as irrelevant

- ☒ Omit hidden files

- ☐ Omit files that are filtered out

- ☒ Recommendable data reduction

- ☐ Omit directories

- ☐ 1 hit per file needed only (faster)

OK

Cancel

Logical (file-wise) ▼

Help











Speed tip!



File type(s):

Signatures...

More...

- ☒  Pictures
- ☒  Documents
- ☒  E-mail
- ☒  Internet
- ☐  Archives
- ☒  OS Artifacts
- ☐  Music/Video
- ☐  Programs
- ☐  Application Data
- ☐  Special Interest

Default file size: 1024 KB

☒ Respect individual default sizes in file type definitions

Max. file size: 100 times default size

Filename prefix:

☒ Intelligent naming, where possible

Look for file headers everywhere ▼

☐ Search in block only☒ Always ignore start sectors of known files

Respect individual cluster boundary flags ▼

☐ Compensate for NTFS compression

OK

Cancel

Help

Index words composed of these characters:

range:a-zA-Zäöüüß

☐ Include substrings (will find "wife" in "housewife")☐ Match case☒ Exceptions

...

☐ Character substitution

...

Word lengths: 4 - 7 (min. 2, max. 24)

☒ ANSI - Latin I (1252)

...

☒ Unicode UTF-16 Little Endian (1200)

...

☐ Unicode UTF-8 (65001)

...

...

...

☒ All objects in volume snapshot (485 GB)☐ Search all tagged objects (0 B)☒ Open and search files incl. slack³☒ Decode text in files:

.pdf;.docx;*.pptx;*.xlsx;*.odt;*.odp;*.ods;*.pa

☐ In selected evidence objects

...

☒ Omit files classified as irrelevant☒ Omit hidden files☐ Omit files that are filtered out☒ Recommendable data reduction☐ Omit directories☐ Distributed indexing

OK

Cancel

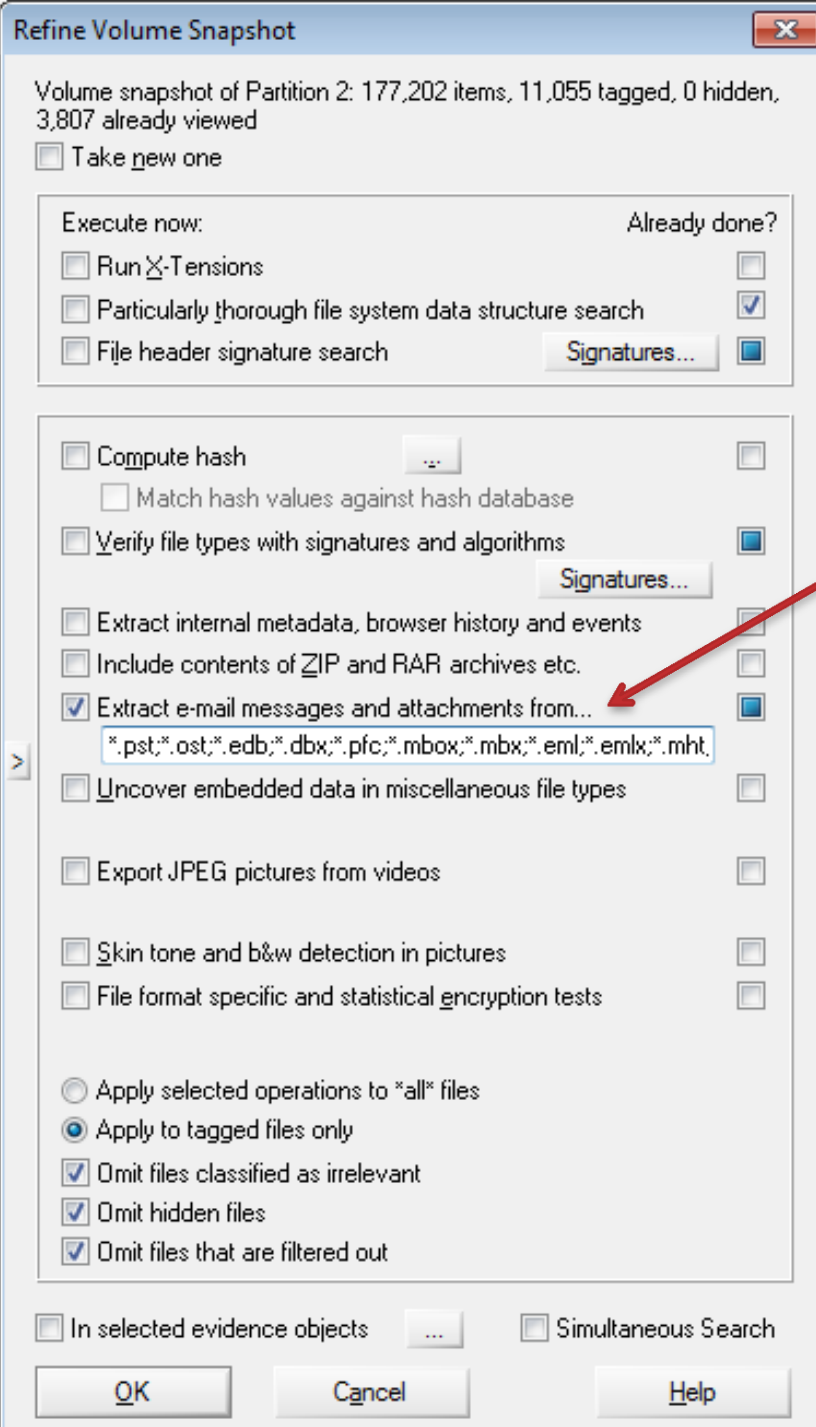
Help

Speed tip!

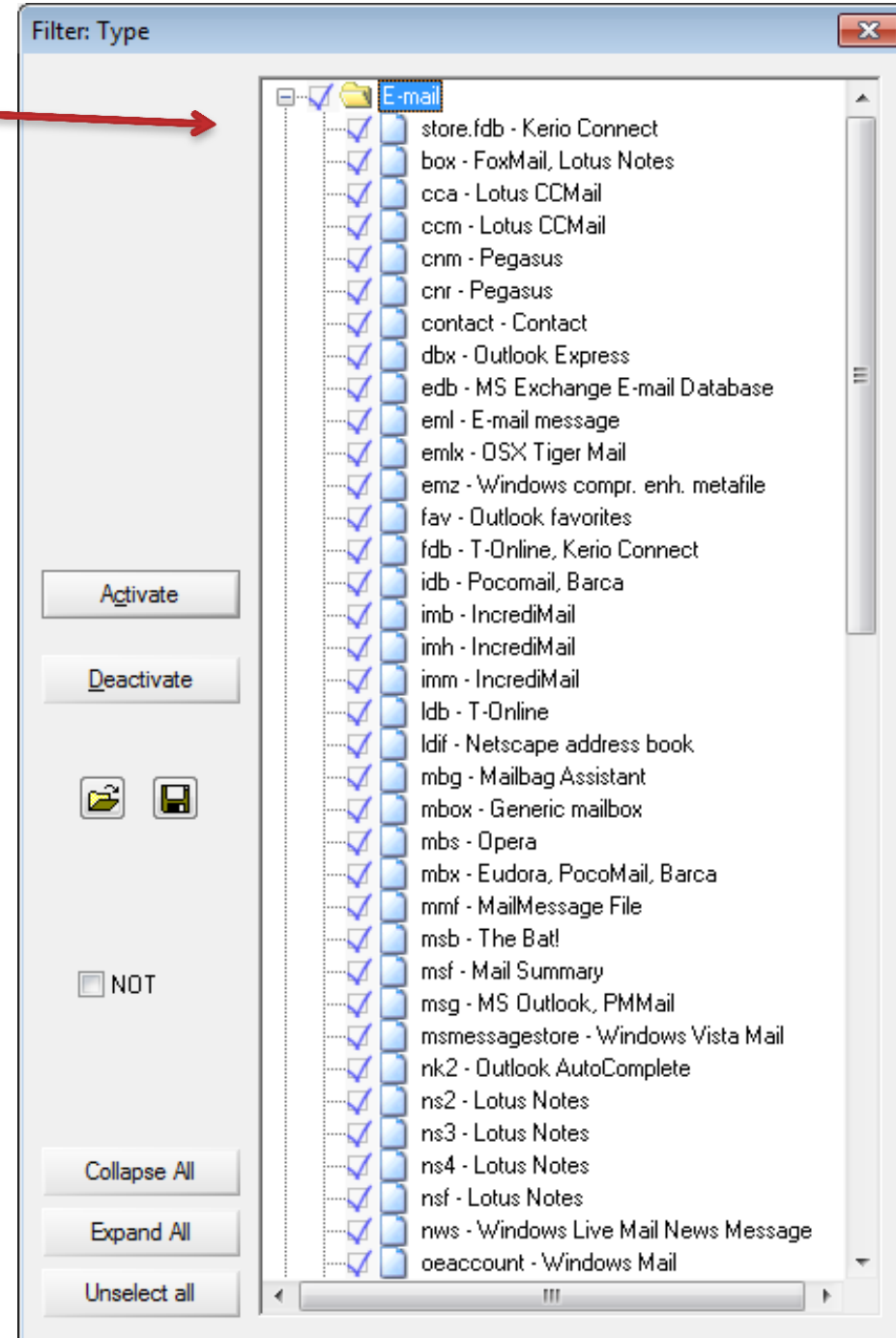
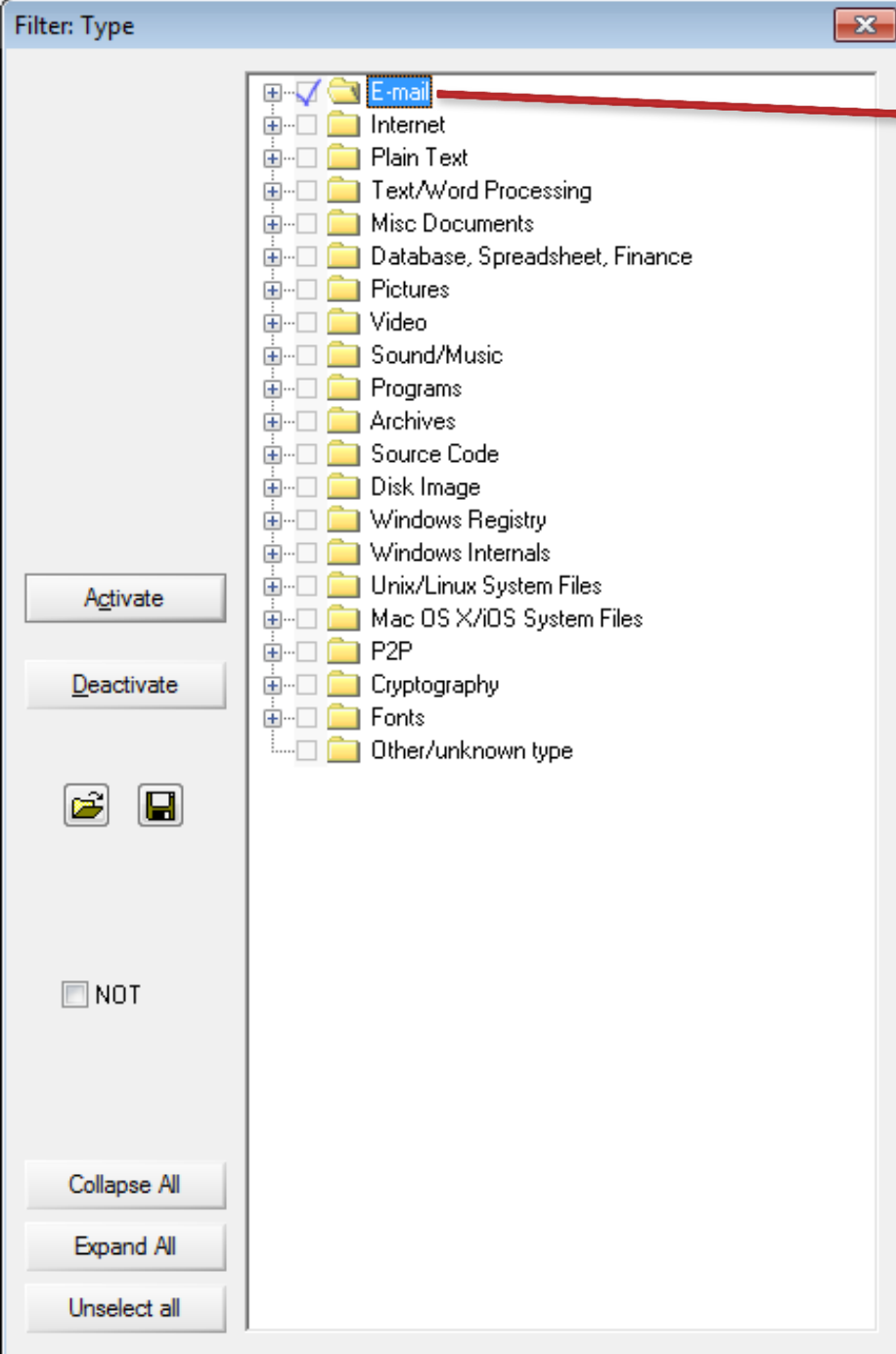
If you know the search terms, you can adjust indexing options to reduce the time to index a drive. (hint: index after hiding irrelevant files)

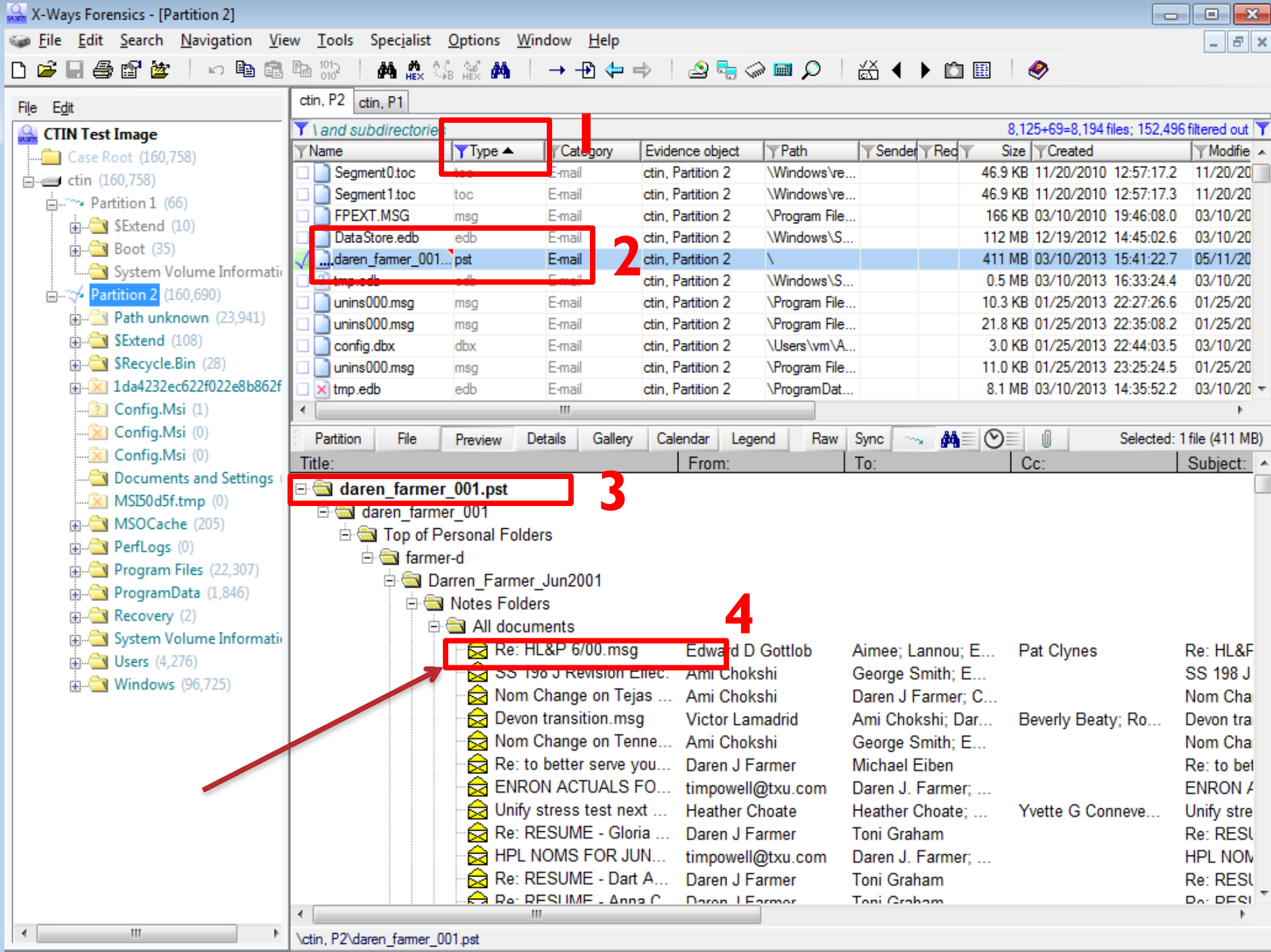


Email



.pst;.ost;*.edb;*.dbx;*.pfc;*.mbox;*.mbx;*.eml;*.emlx;*.mht;*.olk|4MsgSource;*.msg;*.oft;*.mbs;store.fdb





CTIN Test Image

- Case Root (160,758)
 - ctin (160,758)
 - Partition 1 (66)
 - \$Extend (10)
 - Boot (35)
 - System Volume Information
 - Partition 2 (160,690)
 - Path unknown (23,941)
 - \$Extend (108)
 - \$Recycle.Bin (28)
 - 1da4232ec622f022e8b862f
 - Config.Msi (1)
 - Config.Msi (0)
 - Config.Msi (0)
 - Documents and Settings
 - MSI50d5f.tmp (0)
 - MSOCache (205)
 - PerfLogs (0)
 - Program Files (22,307)
 - ProgramData (1,846)
 - Recovery (2)
 - System Volume Information
 - Users (4,276)
 - Windows (96,725)

ctin, P2 ctin, P1 Re: HLP 6/00.msg

From: Edward D Gottlob
To: Aimee[Aimee]; Lannou[Lannou]; Elsa Villarreal[Elsa.Villarreal@enron.com]; ...
Cc: Pat Clynes[Pat Clynes]
Date: Tue 6/20/2000 4:09:00 PM
Subject: Re: HL&P 6/00
Attachment: [jun00hl&p2.xls](#)

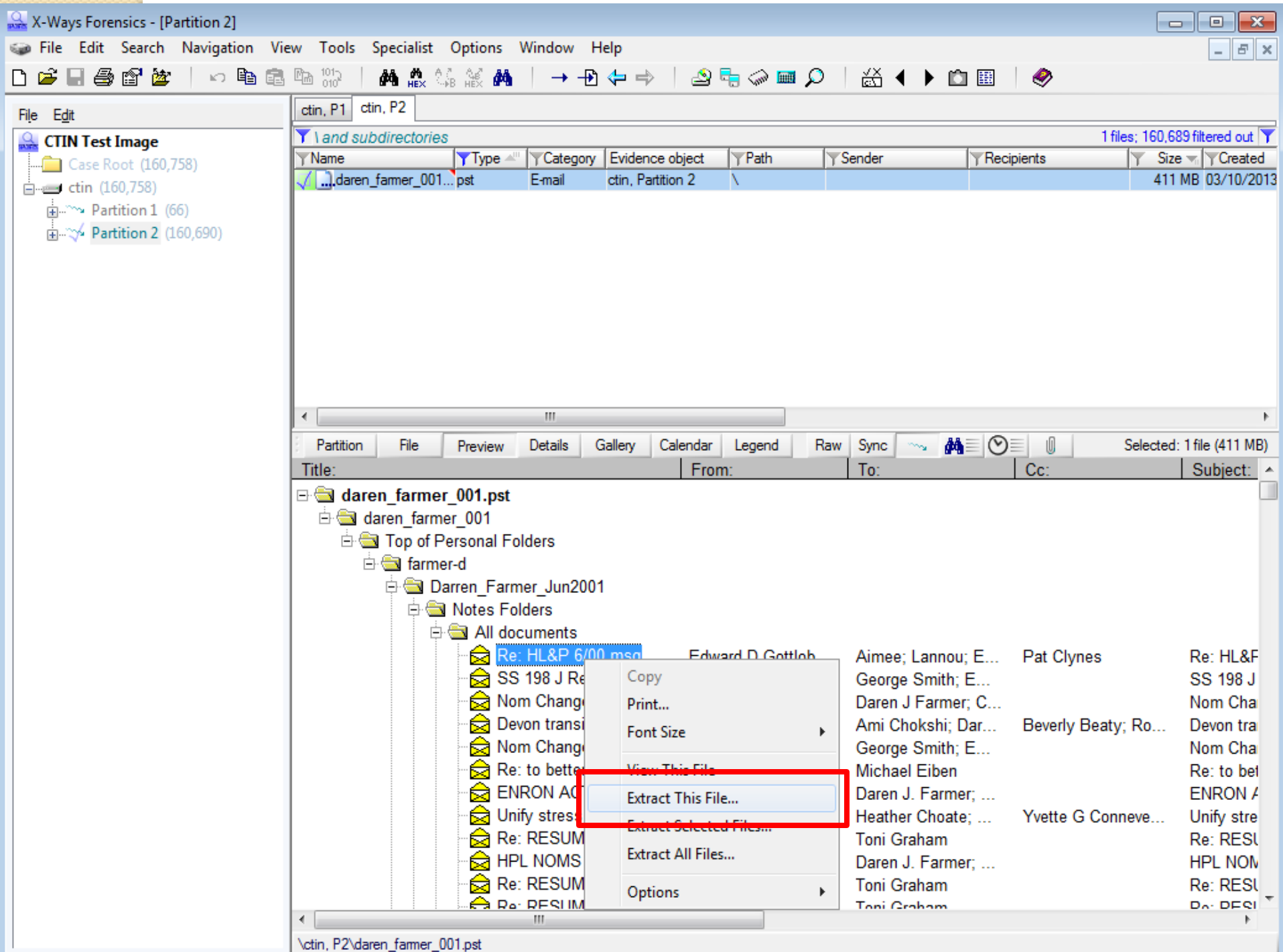
Aimee,
Are you confirming these volumes with HL&P? We have been doing some special deals at Green's Bayou and the HL&P dealmaker has been calling to find out what the volumes are. I do not think he communicates with his scheduler, is that the case? Anyway, we need to agree with HL&P on what volumes flowed on these special days and get them into the system so they can be billed correctly.

Aimee Lannou 06/19/2000 02:18 PM

To: Edward D Gottlob/HOU/ECT@ECT, Pat Clynes/Corp/Enron@ENRON
cc:
Subject: HL&P 6/00

Ed - when you have a chance, I would like to go over this with you.

Aimee



Extracts to .msg to selected directory



Re HL&P 600.msg

X-Ways Forensics - [Partition 2]

File Edit Search Navigation View Tools Specialist Options Window Help

CTIN Test Image

- Case Root (160,758)
- ctin (160,758)
- Partition 1 (66)
- \$Extend (10)
- Boot (35)
- System Volume Information
- Partition 2 (160,690)
- Path unknown (23,941)
- \$Extend (108)
- \$Recycle.Bin (28)
- 1da4232ec622f022e8b862f
- Config.Msi (1)
- Config.Msi (0)
- Config.Msi (0)
- Documents and Settings
- MSI50d5f.tmp (0)
- MSOCache (205)
- PerfLogs (0)
- Program Files (22,307)
- ProgramData (1,846)
- Recovery (2)
- System Volume Information
- Users (4,276)
- Windows (96,725)

ctin, P2 ctin, P1

8,125+69=8,194 files; 152,496 filtered out

Name	Type	Category	Evidence object	Path	Sender	Rec	Size	Created	Modified
Evergreen deals.eml	eml	E-mail	ctin, Partition 2	\daren_fame...	Daren ...	Julie...	1.0 KB		
Re: Evergreen de...	eml	E-mail	ctin, Partition 2	\daren_fame...	Julie M...	Dar...	1.6 KB		
Re: Pennzoil Avail...	eml	E-mail	ctin, Partition 2	\daren_fame...	Ami Ch...	Bren...	1.5 KB		
January Productio...	eml	E-mail	ctin, Partition 2	\daren_fame...	Susan ...	Dar...	2.1 KB		
January Productio...	eml	E-mail	ctin, Partition 2	\daren_fame...	Daren ...	Ken...	2.4 KB		
Calpine Daily Gas ...	eml	E-mail	ctin, Partition 2	\daren_fame...	Ricky ...	Rob...	1.1 KB		
Out on vacation.eml	eml	E-mail	ctin, Partition 2	\daren_fame...	Romeo...	Dav...	1.5 KB		
Re: Evergreen de...	eml	E-mail	ctin, Partition 2	\daren_fame...	Daren ...	Julie...	1.7 KB		
Re: Entex Transiti...	eml	E-mail	ctin, Partition 2	\daren_fame...	Pamela...	Rita ...	3.4 KB		
Re: Evergreen de...	eml	E-mail	ctin, Partition 2	\daren_fame...	Julie M...	Dar...	1.9 KB		
Kerr Mcgee: Tom...	eml	E-mail	ctin, Partition 2	\daren_fame...	Ami Ch...	Joe ...	1.8 KB		

Selected: 1 file (1.5 KB)

Subject	Out on vacation
Sender	Romeo D'Souza
Recipients	Dave Nommensen, Christine Pham, Shawn MacPhail, Debbie Keeton, Milind Patil,

FYI,
I will be out of the office (actually out of the country) starting from
22nd of Dec 1999 through the 20th of Jan 2000. I will be back in the
office on the 21st of Jan 2000.

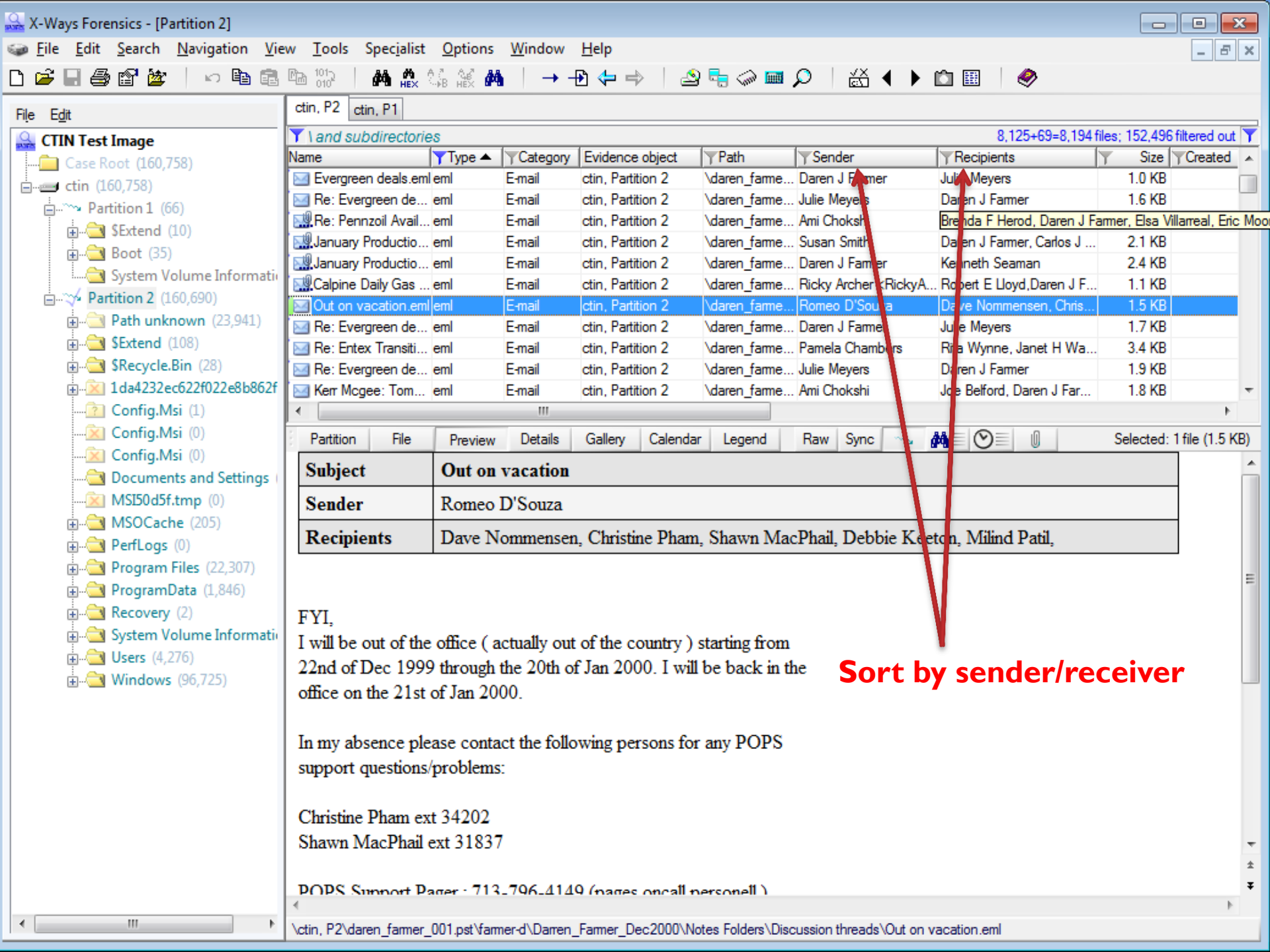
In my absence please contact the following persons for any POPS
support questions/problems:

Christine Pham ext 34202
Shawn MacPhail ext 31837

POPS Support Pager : 713-796-4149 (pages oncall personell)

Extracted from pst within XWF

\\ctin, P2\daren_famer_001.pst\famer-d\Darren_Famer_Dec2000\Notes Folders\Discussion threads\Out on vacation.eml



X-Ways Forensics - [Partition 2]

File Edit Search Navigation View Tools Specialist Options Window Help

CTIN Test Image

- Case Root (160,758)
- ctin (160,758)
- Partition 1 (66)
- \$Extend (10)
- Boot (35)
- System Volume Information
- Partition 2 (160,690)
- Path unknown (23,941)
- \$Extend (108)
- \$Recycle.Bin (28)
- 1da4232ec622f022e8b862f
- Config.Msi (1)
- Config.Msi (0)
- Config.Msi (0)
- Documents and Settings
- MSI50d5f.tmp (0)
- MSOCache (205)
- PerfLogs (0)
- Program Files (22,307)
- ProgramData (1,846)
- Recovery (2)
- System Volume Information
- Users (4,276)
- Windows (96,725)

ctin, P2 ctin, P1

8,125+69=8,194 files; 152,496 filtered out

Name	Type	Category	Evidence object	Path	Sender	Recipients	Size	Created
1st rev Dec. 1999...	eml	Email	ctin, Partition 2	\daren_fame...	Susan D Trevino	Daren J Farmer, Lauri A ...	1.8 KB	
Unify Close Sched...	eml	Email	ctin, Partition 2	\daren_fame...	Melissa K Ratnala	Brent A Price, Tommy J ...	1.9 KB	
2nd rev Dec. 199...	eml	Email	ctin, Partition 2	\daren_fame...	Susan D Trevino	Daren J Farmer, Carlos J ...	1.5 KB	
Meter 1431 - Nov ...	eml	Email	ctin, Partition 2	\daren_fame...	Howard B Camp	Aimee Lannou, Daren J F...	1.1 KB	
Meter 1431 - Nov ...	eml	Email			Aimee Lannou	Daren J Farmer, George ...	1.5 KB	
Y2K - Texas Log...	eml	Email			Carlos J Rodriguez	Alex Saldana, Robert Su...	1.2 KB	
Calpine Daily Gas ...	eml	Email			Ricky Archer <RickyA...	Robert E Lloyd, Daren J F...	1.1 KB	
Your approval is r...	eml	Email			Kenya Perkins	Daren J Farmer	0.7 KB	
HPL FUEL GAS B...	eml	Email			Gregg Lenart	Howard B Camp, Daren ...	1.6 KB	
Calpine Daily Gas ...	eml	Email			Ricky Archer <RickyA...	Robert E Lloyd, Daren J F...	1.1 KB	
UA4 - Meter 1441 ...	eml	Email			Stella L Morris	Daren J Farmer, Mary M ...	1.0 KB	

View
Viewer Programs
Open
Print...
Recover/Copy...
Export list...
Report table associations...
Edit comment...
Untag
Select
Hide
Navigation
Refine Volume Snapshot...
Simultaneous Search...
Run X-Tensions...
Create Hash Set...
Copy "E-mail"

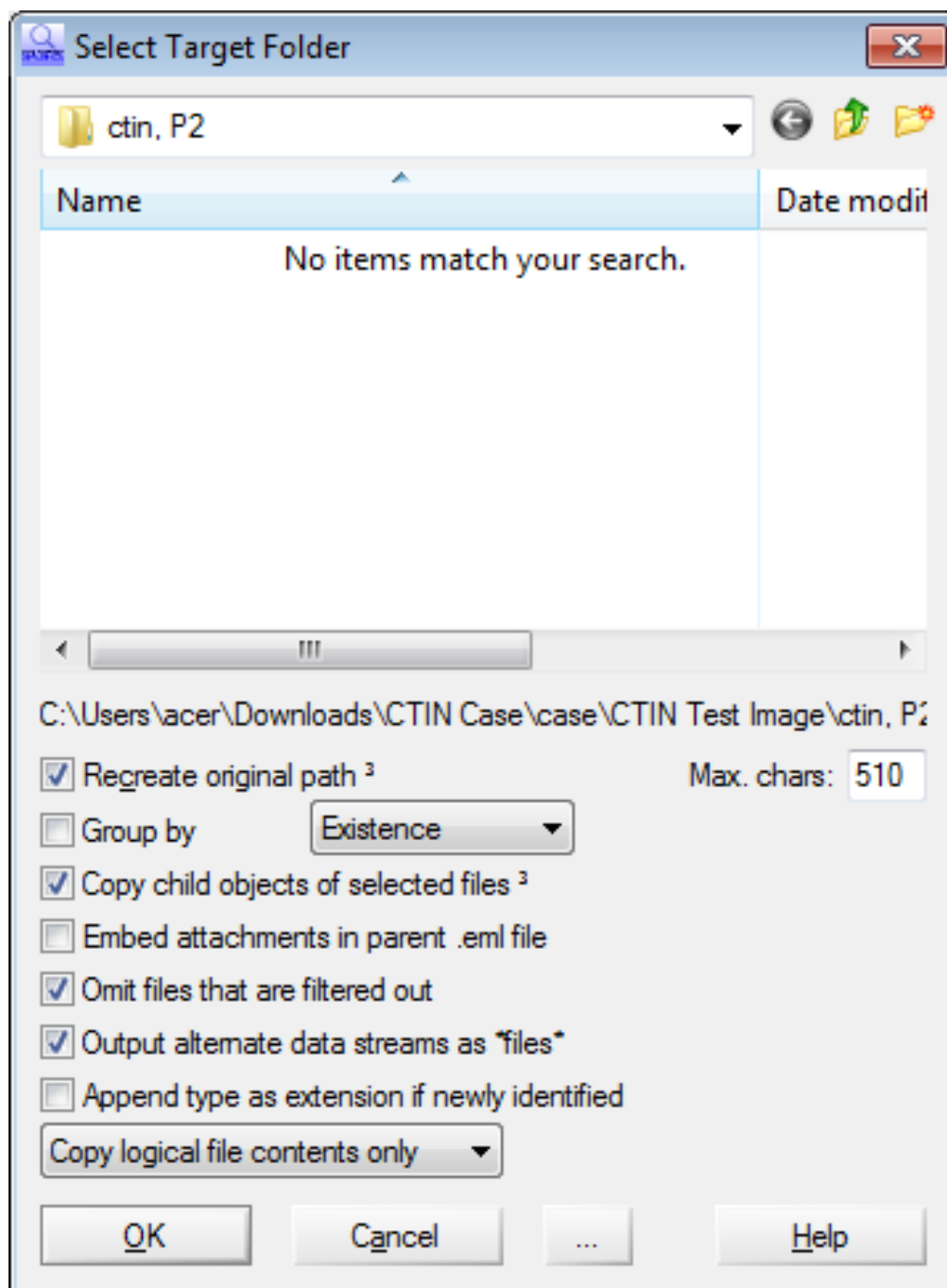
Partition	File	Preview	De
	Subject	Calpine Dai	
	Sender	Ricky Arche	
	Recipients	Robert E Llo	
	Attachment	CALPINE D	

- CALPINE DAILY GAS NOMINATION

EDRM Enron Email Data Set has been produced in EML, PST and NSF format by ZL Technologies, Inc. This Data Set is licensed under a Creative Commons Attribution 3.0 United States License . To provide attribution, please cite to "ZL Technologies, Inc. (<http://www.zlti.com>)."

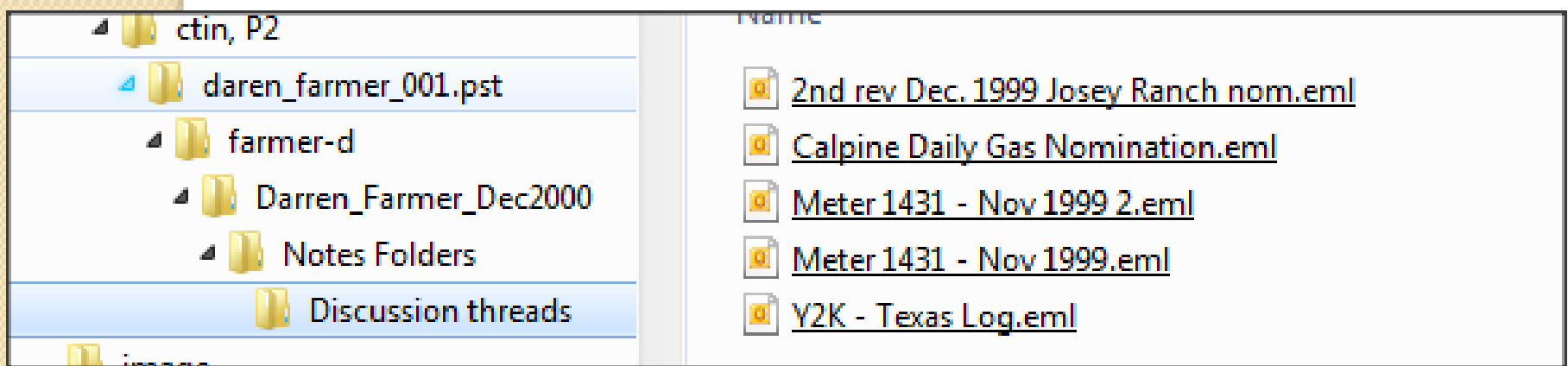
E-mail Header

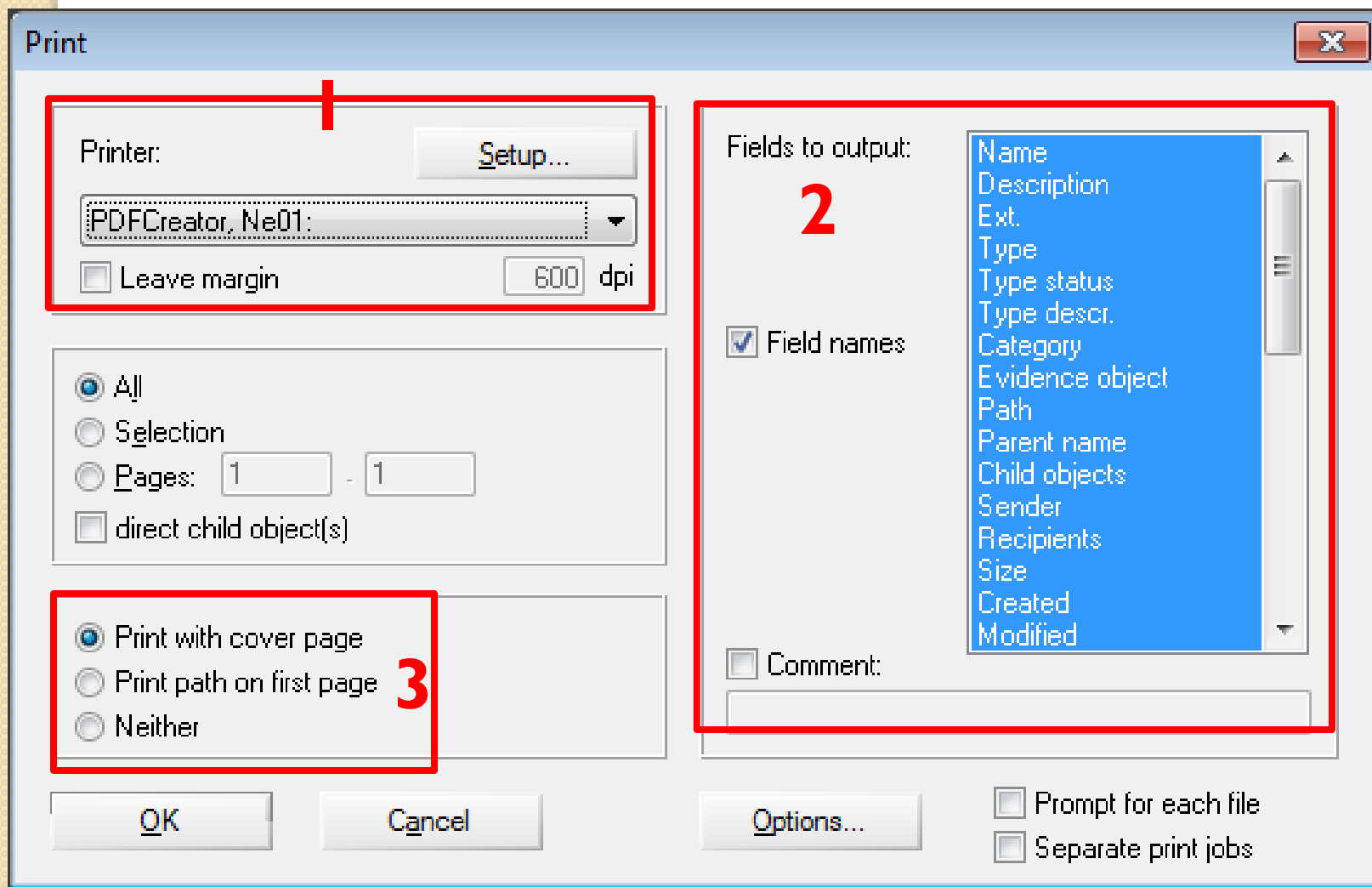
\\ctin, P2\daren_famer_001.pst\daren-d\Darren_Famer_Dec2000\Notes Folders\Discussion threads\Calpine Daily Gas Nomination.eml



Exported email from a PST file

- Exported as .eml, by file path or flattened





Printed email from a PST file (cover page)

Printed on 05/11/2015, 09:01:20 by ACET with X-Ways Forensics 17.01 Review 17.
CTIN Test Image

2nd rev Dec. 1999 Josey Ranch nom.eml

Description: extracted e-mail

Ext.: eml

Type: eml

Type status: confirmed

Type descr.: E-mail message

Category: E-mail

Evidence object: ctin, Partition 2

Path: \daren_farmer_001.pst\farmer-d\Darren_Farmer_Dec2000\Notes Folders\Discussion threads

Parent name: Discussion threads

Child objects:

Sender: Susan D Trevino

Recipients: Daren J Farmer, Carlos J Rodriguez, Lauri A Allen

Size: 1.5 KB

Created:

Printed email (pdf) from a PST file

Subject	2nd rev Dec. 1999 Josey Ranch nom
Sender	Susan D Trevino
Recipients	Daren J Farmer, Carlos J Rodriguez, Lauri A Allen, Stretch Brennan <djb@KCSEnergy.com>, Kevin McLarney <kmm@KCSEnergy.com>.

----- Forwarded by Susan D Trevino/HOU/ECT on 12/15/99 08:41 AM -----

Bob Withers on 12/15/99 08:28:08 AM
To: Susan D Trevino/HOU/ECT@ECT
cc: Stretch Brennan , Kevin McLarney ,
"Taylor Vance (E-mail)"
Subject: 2nd rev Dec. 1999 Josey Ranch nom

Here's REVISED December 1999 (effective 12/15/99) setup for
Josey: (using 1.081 Btu/Mcf)
* Gas deliveries into HPL
9,300 MMBtu/d for KRI (net reduction of
3,000 MMBtu/d)
9,300 MMBtu/d into HPL

Bob Withers <*)>><
KCS Energy, 5555 San Felipe, Suite 1200
Houston, TX 77056
voice mail/page 713-964-9434

Export list of selected emails

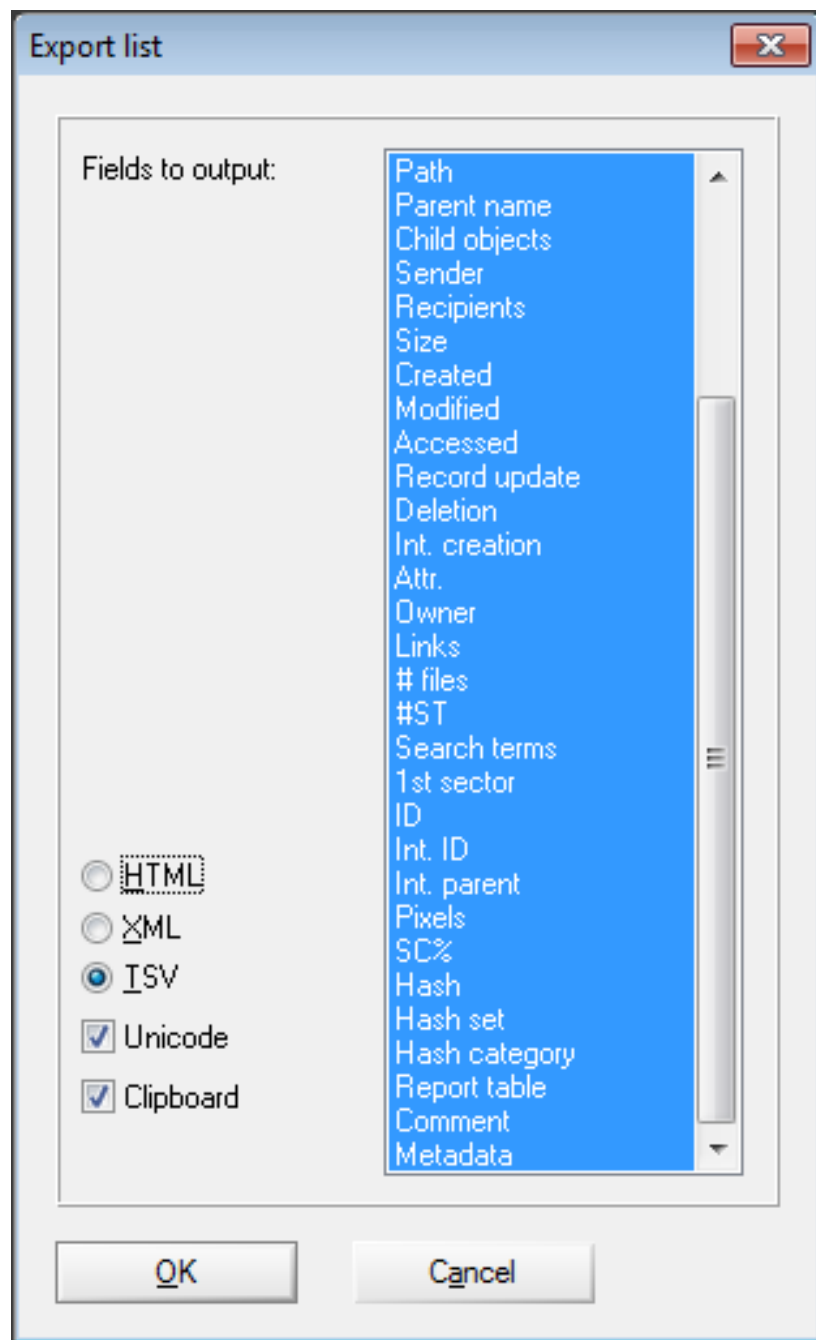
2nd rev Dec. 1999...	eml	E-mail	ctin, Partition 2	\daren_fame...	Susan D Trevino	Daren J Farr
ify Close Sched...	eml	E-mail	ctin, Partition 2	\daren_fame...	Melissa K Ratnala	Brent A Pric
2nd rev Dec. 199...	eml	E-mail	ctin, Partition 2	\daren_fame...	Susan D Trevino	Daren J Farr
eter 1431 - Nov ...	eml	E-mail	ctin, Partition 2	\daren_fame...	Howard B Camp	Aimee Lann
eter 1431 - Nov ...	eml	E-mail	ctin, Partition 2	\daren_fame...	Aimee Lannou	Daren J Farr
2K - Texas Log....	eml	E-mail			Carlos J Rodriguez	Alex Saldan
alpine Daily Gas ...	eml	E-mail			Ricky Archer <RickyA...	Robert E Llo
our approval is r...	eml	E-mail			Kenya Perkins	Daren J Farr
PL FUEL GAS B...	eml	E-mail			Gregg Lenart	Howard B C
alpine Daily Gas ...	eml	E-mail			Ricky Archer <RickyA...	Robert E Llo
A4 - Meter 1441 ...	eml	E-mail			Stella L Morris	Daren J Farr

Partition	File	Preview	Details
Subject	2nd rev Dec. 1		
Sender	Susan D Trevino		
Recipients	Daren J Farmer		

View	Viewer Programs ▶	
Open		
Print...		
Recover/Copy...		
Export list...		
Report table associations...		
Edit comment...		
Untag		
Select ▶		
Hide ▶		

Raw	Sync				
-----	------	--	--	--	--

Allen, Stretch Brennan <djb@K



Choose metadata
for the list

Place into a spreadsheet and make it pretty

Book1 - Microsoft Excel

	A	B	C	D	E	F
1	Name	Description	Ext.	Sender	Recipients	Evidence object
2	2nd rev Dec. 1999 Josey Ranch nom.eml	extracted e-mail	eml	Susan D Trevino	Daren J Farmer, Carlos J Rodriguez, Lauri A Allen	ctin, Partition 2
3	Meter 1431 - Nov 1999.eml	extracted e-mail	eml	Howard B Camp	Aimee Lannou,Daren J Farmer, Stacey Neuweiler, Mary M	ctin, Partition 2
4	Meter 1431 - Nov 1999.eml	extracted e-mail	eml	Aimee Lannou	Daren J Farmer,George Grant	ctin, Partition 2
5	Y2K - Texas Log.eml	extracted e-mail	eml	Carlos J Rodriguez	Alex Saldana, Robert Superty,Daren J Farmer	ctin, Partition 2
6	Calpine Daily Gas Nomination.eml	with attachment	eml	Ricky Archer <RickyA@	Robert E Lloyd,Daren J Farmer	ctin, Partition 2
7						
8						
9						
10						
11						

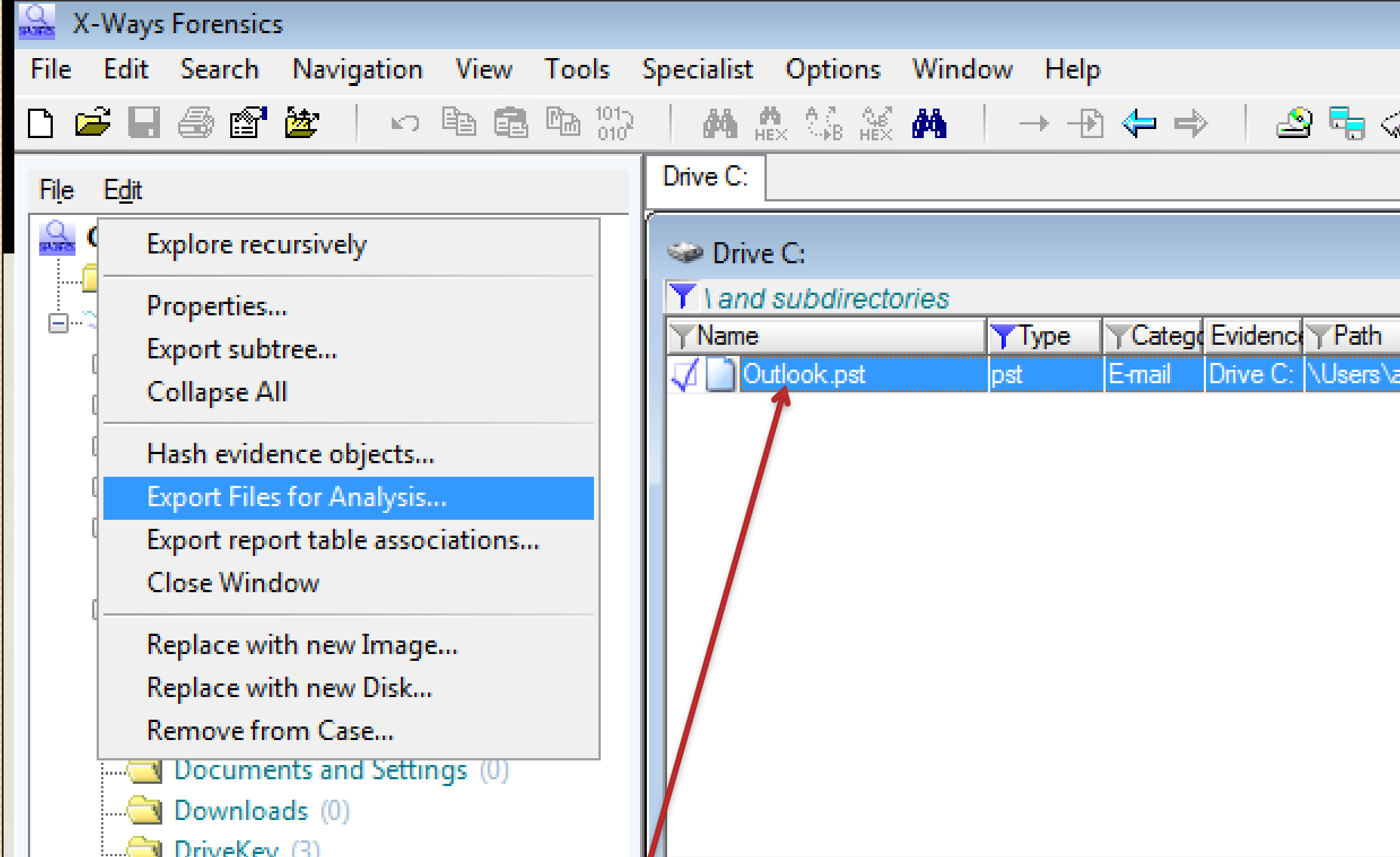
Sheet1 Sheet2 Sheet3



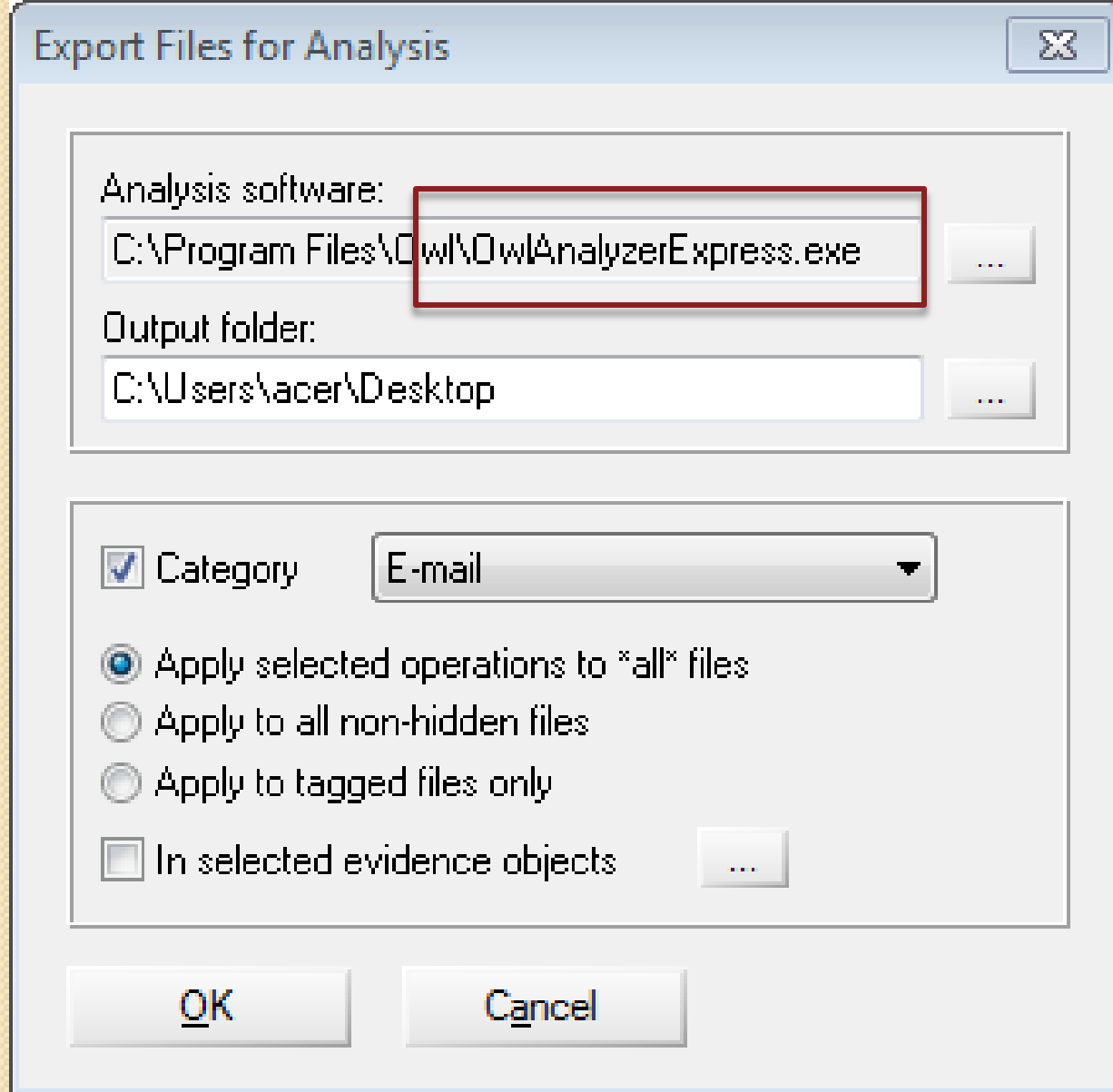
Export Files for Analysis

Export Files for Analysis

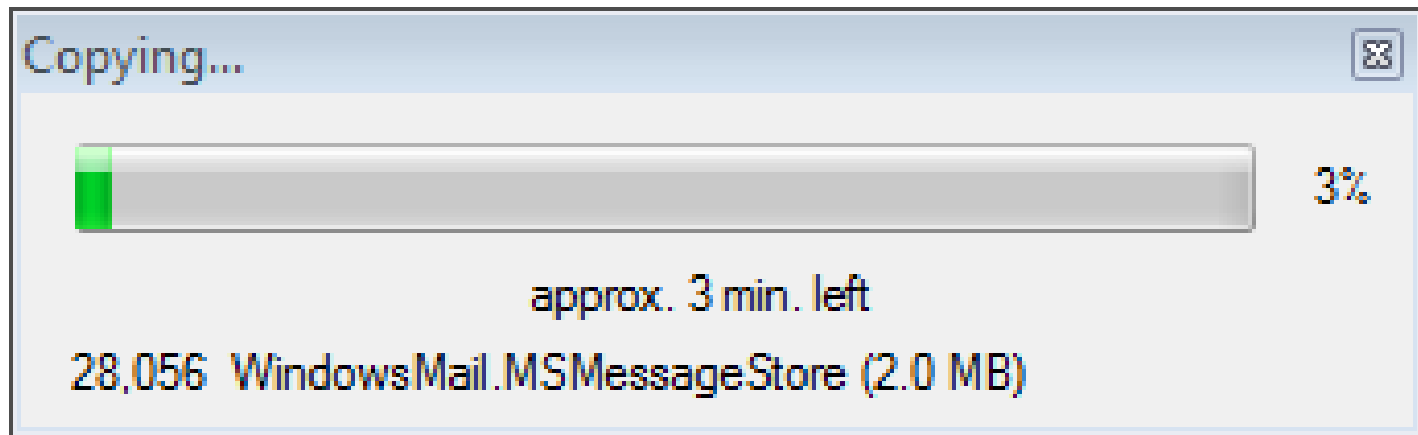
- The **Export Files for Analysis** menu allows XWF to export files so they can be processed by an external program.



- Choose your file/s
- Export for analysis



- Choose your analysis program and options
- (Owl Analyzer - <http://www.arcpst.com>)



- Files are copied out...

Owl Analyzer is used here as an example to examine a pst file. It opens after the extraction is finished.

Owl Analyzer Express

File Options Help

Mailbox(es) to scan: C:\Users\\Desktop\6AA90166\931213339167189.pst Browse

Start Exit

Progress: Idle.

Analysis Summary		
Started at	2013-03-09 14:23:32	
Time elapsed	-----	
Stopped at	2013-03-09 14:23:33	

Mailbox and folder summary		
Mailbox(es)	0	0.00%
Total folders	0	0.00%
Folders with messages and/or subfolders	0	0.00%
Empty folders	0	0.00%


Message summary		
Total messages	0	0.00%
Total size of all messages (including attachments)	0.00 bytes	
Duplicate messages	0	0.00%
Total size of all duplicate messages	0.00 bytes	
Total size of all attachments	0.00 bytes	
Average message size	0.00 bytes	
Size of largest message	0.00 bytes	
Total inbound messages	0	0.00%
Total outbound messages	0	0.00%
Total internal messages	0	0.00%
Unable to determine flow direction	0	
Messages with visible attachments	0	0.00%
Messages with hidden attachments	0	0.00%
Messages with BCC recipients	0	0.00%
Messages with no identifiable recipients (usually spam)	0	0.00%
Messages with no identifiable sender	0	0.00%
Messages with malformed dates	0	

Visible Attachment Summary		
Total visible attachments (ex: Word document)	0	
Duplicate visible attachments	0	0.00%
Total size of visible attachments	0.00 bytes	
Average visible attachment size	0.00 bytes	
Size of largest visible attachment	0.00 bytes	

Hidden Attachment Summary		
Total hidden attachments (ex: embedded images)	0	
Duplicate hidden attachments	0	0.00%
Total Size of hidden attachments	0.00 bytes	
Average hidden attachment size	0.00 bytes	
Size of largest hidden attachment	0.00 bytes	

Statistics updated every 500ms

View Attachment Summary by File Type



Mailbox(es) to scan: C:\Users\acer\Desktop\daren_farmer_001.pst

Browse

Start

Exit

Progress: Idle.

Analysis Summary

Started at	2013-03-09 14:38:46
Time elapsed	00:03:58
Stopped at	2013-03-09 14:33:44

Mailbox and folder summary

Mailbox(es)	daren_farmer_001.pst	100.00%
Total folders	58 / 58	100.00%
Folders with messages and/or subfolders	54	93.10%
Empty folders	4	6.90%

Message summary

Total messages	8,098 / 8,098	100.00%
Total size of all messages (including attachments)	398.69 MB	
Duplicate messages	3,230	39.89%
Total size of all duplicate messages	146.84 MB	
Total size of all attachments	366.90 MB	
Average message size	50.41 KB	
Size of largest message	14.11 MB	
Total inbound messages	0	0.00%
Total outbound messages	0	0.00%
Total internal messages	0	0.00%
Unable to determine flow direction	0	
Messages with visible attachments	2,184	26.97%
Messages with hidden attachments	0	0.00%
Messages with BCC recipients	0	0.00%
Messages with no identifiable recipients (usually spam)	856	10.57%
Messages with no identifiable sender	5,711	70.52%
Messages with malformed dates	0	

Visible Attachment Summary

Total visible attachments (ex: Word document)	2,898	
Duplicate visible attachments	1,227	42.34%
Total size of visible attachments	366.90 MB	
Average visible attachment size	129.64 KB	
Size of largest visible attachment	14.11 MB	

Hidden Attachment Summary

Total hidden attachments (ex: embedded images)	0	
Duplicate hidden attachments	0	0.00%
Total size of hidden attachments	0.00 bytes	
Average hidden attachment size	0.00 bytes	
Size of largest hidden attachment	0.00 bytes	

Statistics updated every 500ms

View Attachment Summary by File Type

Metric	Visible	Hidden
Total size of attachments	366.90 MB	0.00 bytes
Total count of attachments	2,898	0
Failed to determine file type	0 (0.00%)	0 (0.00%)
File type: *.xls	1,306 (45.07%)	0 (0.00%)
File type: *.htm	42 (1.45%)	0 (0.00%)
File type: *.doc	902 (31.12%)	0 (0.00%)
File type: *.ppt	37 (1.28%)	0 (0.00%)
File type: *.dat	88 (3.04%)	0 (0.00%)
File type: *.pcx	20 (0.69%)	0 (0.00%)
File type: *.jpg	54 (1.86%)	0 (0.00%)
File type: *.vcf	8 (0.28%)	0 (0.00%)
File type: *.pps	5 (0.17%)	0 (0.00%)
File type: *.pdf	18 (0.62%)	0 (0.00%)
File type: *.rtf	2 (0.07%)	0 (0.00%)
File type: *.exe	8 (0.28%)	0 (0.00%)
File type: *.txt	2 (0.07%)	0 (0.00%)
File type: *.gif	6 (0.21%)	0 (0.00%)
File type: *.xlw	2 (0.07%)	0 (0.00%)
File type: *.wk4	1 (0.03%)	0 (0.00%)
File type: *.url	385 (13.29%)	0 (0.00%)
File type: *.mpeg	2 (0.07%)	0 (0.00%)
File type: *.wps	1 (0.03%)	0 (0.00%)
File type: *.mpe	1 (0.03%)	0 (0.00%)
File type: *.avi	6 (0.21%)	0 (0.00%)
File type: *.mpg	2 (0.07%)	0 (0.00%)

Statistics updated every 500ms

File Home Insert Page Layout Formulas Data Review View

Paste Cut Copy Format Painter Clipboard

Tahoma 9 A A B I U Font

Wrap Text Merge & Center Alignment

General \$ % , .00 .00 Number

	A	B	C
D31			
1	Analysis Summary	Analysis Summary	Analysis Summary
2	Started at	14:29:46 tt	
3	Time elapsed	0:03:58 tt	
4	Stopped at	14:33:44 tt	
5	Mailbox and folder summary	Mailbox and folder summary	Mailbox and folder summary
6	Mailbox(es)	daren_farmer_001.pst	100.00%
7	Total folders	58 / 58	100.00%
8	Folders with messages and/or subfolders	54	93.10%
9	Empty folders	4	6.90%
10	Message summary	Message summary	Message summary
11	Total messages	8,098 / 8,098	100.00%
12	Total size of all messages (including attachments)	398.69	MB
13	Duplicate messages	3230	39.89%
14	Total size of all duplicate messages	146.84	MB
15	Total size of all attachments	366.9	MB
16	Average message size	50.41	KB
17	Size of largest message	14.11	MB
18	Total inbound messages	0	0.00%
19	Total outbound messages	0	0.00%
20	Total internal messages	0	0.00%
21	Unable to determine flow direction	0	
22	Messages with visible attachments	2184	26.97%
23	Messages with hidden attachments	0	0.00%
24	Messages with BCC recipients	0	0.00%
25	Messages with no identifiable recipients (usually spam)	856	10.57%
26	Messages with no identifiable sender	5711	70.52%

Export files for analysis

- Email specific tools
- Registry tools
- And others that may do better than XWF
- Or used as a validation to what XWF finds.

Shortcuts

- There are plenty.
- If you find something you do all the time, start using the shortcut to save time.

on View **Tools** Specialist Options Window Help

Open Disk... F9

Disk Tools ▶

File Tools ▶

Open RAM... Alt+F9

View Shift+F9

External Programs ▶

Calculator Alt+F8

Hex Converter... F8

 Analyze Disk F2

Compute Hash... Ctrl+F2


Hash Database ▶

Run X-Tensions...

Start Center... Enter

 Clone Disk... Ctrl+D

Explore recursively

 File Recovery by Type...

Take New Volume Snapshot

Scan For Lost Partitions...

Interpret As Partition Start

Set Disk Parameters...

☐  \$UpCase

☐  \$Extend (15)

☐  ntldr

Other/... Drive C: \

Drive C:

Other/... Drive C: \

Other/... Drive C: \

Other/... Drive C: \

Other/... Drive C: \

Other/... Drive C: \

Other/... Drive C: \

Other/... Drive C: \

Use your mouse!

- Rather than move the mouse to the forward or backward button and clicking on them, you can use the forward and backward buttons.

Refine Volume Snapshot



Volume snapshot of Drive C: 828,429 items, 0 tagged, 0 hidden, 38,570 already viewed

☐ Take new one

Execute now:

Already done?

☐ Run X-Tensions



☒ Particularly thorough file system data structure search



☒ File header signature search

Signatures...



☐ Compute hash: MD5



☐ Match hash values against hash database

☐ Verify file types with signatures and algorithms

Signatures...



☐ Extract internal metadata, browser history and events



☐ Include contents of ZIP and RAR archives etc.



☐ Extract e-mail messages and attachments from...



☐ Uncover embedded data in miscellaneous file types



☐ Export JPEG pictures from videos



☐ Skin tone and b&w detection in pictures



☐ File format specific and statistical encryption tests



☐ In selected evidence objects



☐ Simultaneous Search

OK

Cancel

Help

Refine Volume Snapshot



Volume snapshot of Drive C: 828,429 items, 0 tagged, 0 hidden, 38,570 already viewed

☐ Take new one

Execute now:

Already done?

☐ Run X-Tensions



☒ Particularly thorough file system data structure search



☒ File header signature search

Signatures...



☒ Compute hash: MD5



☐ Match hash values against hash database

☒ Verify file types with signatures and algorithms

Signatures...



☒ Extract internal metadata, browser history and events



☒ Include contents of ZIP and RAR archives etc.



☒ Extract e-mail messages and attachments from...



.pst;.ost;*.edb;*.dbx;*.pfc;*.mbox;*.mbx;*.eml;*.emlx;*.mht

☒ Uncover embedded data in miscellaneous file types



.pdf;.doc;*.ppt;*.pps;*.xls;*.ole2;*.jpg;*.thumb;*.db;*.thumbdb

☒ Export JPEG pictures from videos



.3gp;.3gpp;*.asf;*.avi;*.divx;*.flv;*.m1v;*.m4v;*.mkv;*.mov

☒ Skin tone and b&w detection in pictures



☒ File format specific and statistical encryption tests



☒ Apply selected operations to "all" files

☐ Apply to tagged files only

☐ Omit files classified as irrelevant

☐ Omit hidden files

☐ Omit files that are filtered out

☐ In selected evidence objects



☐ Simultaneous Search

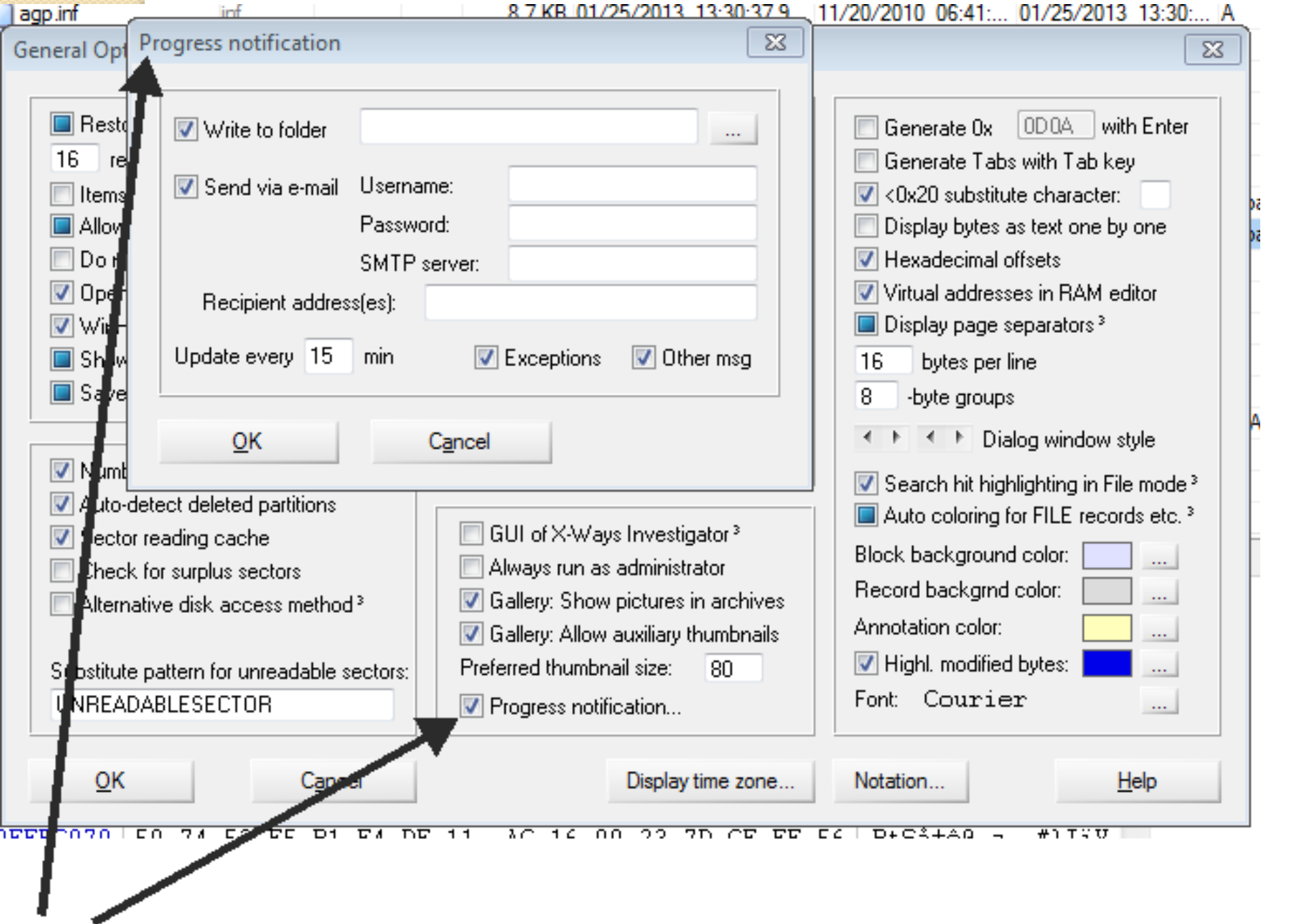
OK

Cancel

Help

Email notifications? Cool 😊

- How would you like XWF to contact you via email if an error occurs during processing or when it is finished?



Triage

- Or preview or whatever you want to call it....

Triage






















- On a live system, you have a complete forensic suite to use for a triage/preview and image if needed.
- On a WinFE booted system, you can do a quick and simple preview/triage all the way to a full forensic examination.

Pictures

- Consent searches
- Parole/supervision
- Quick PC

Filter: Type



- ☒  E-mail
- ☐  Internet
- ☐  Plain Text
- ☐  Text/Word Processing
- ☐  Misc Documents
- ☐  Database, Spreadsheet, Finance
- ☒  Pictures
- ☐  Video
- ☐  Sound/Music
- ☐  Programs
- ☐  Archives
- ☐  Source Code
- ☐  Disk Image
- ☐  Windows Registry
- ☐  Windows Internals
- ☐  Unix/Linux System Files
- ☐  Mac OS X/iOS System Files
- ☐  P2P
- ☐  Cryptography
- ☐  Fonts
- ☐  Other/unknown type

Activate

Deactivate



☐ NOT

Collapse All

Expand All

Unselect all

X-Ways Forensics - [Partition 2]

File Edit Search Navigation View Tools Specialist Options Window Help

CTIN Test Image

- Case Root (160,758)
- ctin (160,758)
 - Partition 1 (66)
 - \$Extend (10)
 - Boot (35)
 - System Volume Information
 - Partition 2 (160,690)
 - Path unknown (23,941)
 - \$Extend (108)
 - \$Recycle.Bin (28)
 - 1da4232ec622f022e8b862f1
 - Config.Msi (1)
 - Config.Msi (0)
 - Config.Msi (0)
 - Documents and Settings (0)
 - MSI50d5f.tmp (0)
 - MSOCache (205)
 - PerfLogs (0)
 - Program Files (22,307)
 - ProgramData (1,846)
 - Recovery (2)
 - System Volume Information
 - Users (4,276)
 - Windows (96,725)

ctin, P2 ctin, P1

and subdirectories 8,535+1,391=9,926 files; 150,764 filtered out

Name	Type	Category	Evidence object	Path	Sender	Recipients	Size	Created
GreenBubbles.jpg	jpg	Pictures	ctin, Partition 2	\Windows\wi...			6.3 KB	07/13/200
grandsn4.jpg	jpg	Pictures	ctin, Partition 2	\daren_fame...	Daren J Famer	tjfamer@juno.com	36.2 KB	
grandsn3.jpg	jpg	Pictures	ctin, Partition 2	\daren_fame...	Daren J Famer	tjfamer@juno.com	34.4 KB	
OrangeCircles.jpg	jpg	Pictures	ctin, Partition 2	\Program File...			6.2 KB	07/13/200
OrangeCircles.jpg	jpg	Pictures	ctin, Partition 2	\Windows\wi...			6.2 KB	07/13/200
grandsn2.jpg	jpg	Pictures	ctin, Partition 2	\daren_fame...	Daren J Famer	tjfamer@juno.com	15.2 KB	
pic17578.pcx	pcx	Pictures	ctin, Partition 2	\daren_fame...	Charlie Stone <cstone...	lbellamy@enron.com,"D...	164 KB	
Bush-limo.jpg	jpg	Pictures	ctin, Partition 2	\daren_fame...	Charlie Stone <cstone...	Janet_H_Wallis@enron...	98.3 KB	
Audiovox Slimline ...	jpg	Pictures	ctin, Partition 2	\daren_fame...	Daren J Famer	Heather Choate	8.3 KB	
algore.jpg	jpg	Pictures	ctin, Partition 2	\daren_fame...	Daren J Famer	dheineke@tsteel.com	177 KB	
Floridaballot.jpg	jpg	Pictures	ctin, Partition 2	\daren_fame...	Daren J Famer	dheineke@tsteel.com, D...	121 KB	

Partition File Preview Details Gallery Calendar Legend Sync

111

and subdirectories

8,535+1,391=9,926 file

	Modified	Accessed	Recon	Deletio	Attr.	Search	1st sector	Int. l	SC%	Report
15:28:34.3	06/10/2009 14:29:...	07/13/2009 15:28:...	12/19...		A		6,228,328	9735	0%	
					(attac...		28,738,1...	176684		
					(attac...		28,738,1...	176683		
15:28:34.3	06/10/2009 14:29:...	07/13/2009 15:28:...	12/19...		A		6,228,392	9746	21%	
15:28:34.3	06/10/2009 14:29:...	07/13/2009 15:28:...	12/19...		A		6,228,392	9747	21%	
					(attac...		28,738,1...	176682		
					(attac...		28,738,1...	176154		
					(attac...		28,738,1...	175833		
					(attac...		28,738,1...	175375		
					(attac...		28,738,1...	175092		
					(attac...		28,738,1...	175044		

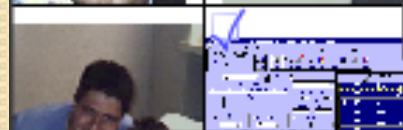
Filter: SC%

- ☒ >= 33 %
☐ <=
☐ irrelevant
☐ ?
☐ b/w

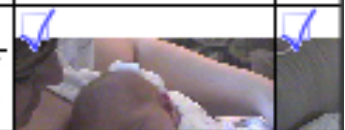
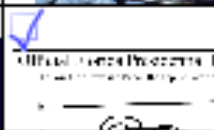
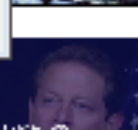
Activate

Deactivate

Partition File Preview



Sync





Electronic Discovery

eDiscovery Tips

- Many times, you are limited to;
 - Time periods of searches
 - Specific file types
 - Specific users
 - Active files only or deleted files only
 - File names only
 - Or a combination of many restrictions!
- XWF does this easily with filtering.

eDiscovery Tips

- Boot to WinFE.
 - Windows Forensics Environment
 - Modified WinPE (write protects hard drive)
 - Boots from CD/DVD/USB
 - Runs your Windows forensics applications on the custodian/suspect's computer, without modifying the drive.
 - That means you can boot the custodian computer and run Encase/XWF/etc... directly, including imaging the drive.

eDiscovery Tips

- Filter by allowed/requested file type
- Copy to XWF container
- The absolute best forensically sound electronic discovery collection, ever.
- (you can even data carve prior if you wanted, specific to the file types in question, and have those files in your forensic container!)

eDiscovery Tips

- You can de-dupe, de-NIST, and/or selectively de-select files that are not relevant before exporting to a container.
- You can PDF documents directly from within XWF, with or without a cover page of metadata from each document.
- This can be one pdf or individual PDFs.

Print



Printer:

Setup...

PDFCreator, Ne01: ▾

☐ Leave margin

600 dpi

☒ All

☐ Selection

☐ Pages: 1 - 1

☐ direct child object(s)

☒ Print with cover page

☐ Print path on first page

☐ Neither

Fields to output:

☒ Field names

☐ Comment:

Name
Description
Ext.
Type
Type status
Type descr.
Category
Evidence object
Path
Parent name
Child objects
Sender
Recipients
Size
Created
Modified

OK

Cancel

Options...

☐ Prompt for each file

☐ Separate print jobs

eDiscovery Tips

- You can export native files
 - By file path
 - Flatten the files to a folder
 - As a file listing (csv)

XWF benefits eDiscovery by...

- Solid logfile of your work created
- Forensically sound collection, all metadata preserved in a container file
- Fast
- Can data carve if needed
- Can filter by file type prior to collection
- Can filter after collection, pre-production
- Can keyword search and collect hits, onsite
- Can bates number files
- Can do real forensics with the same program as ediscovery

Filter Example

- Let's say you were looking for files that..
 - Were a specific file type
 - Not deleted
 - Modified after a certain date
 - Containing a specific search term
 - Sent from a specific person
 - Of a certain file size
- And you wanted to export these files to a container.

Filtering

nsics - [Drive C:]

Search Navigation View Tools Specialist Options Window Help



Drive C:

Find subdirectories

14 min. ago

Root (679,540)

C: (679,540)

th unknown (313,958)

extend (15)

ecycle.Bin (94,098)


Name	Type	Category	Evidence	Path	Sender	Rec	Size	Created	Modified
ddC5D7.tmp	tmp	Other/...	Drive C: \Users...				0 B	03/05/2013 20:29:32.0	03/05/2013 2
CVR5519.tmp.cvr	cvr	Other/...	Drive C: \Users...				0 B	03/05/2013 20:29:03.2	03/05/2013 2
CVR1A3B.tmp.cvr	cvr	Other/...	Drive C: \Users...				0 B	03/05/2013 20:10:14.0	03/05/2013 2
dd30CC.tmp	tmp	Other/...	Drive C: \Users...				0 B	03/05/2013 17:43:57.9	03/05/2013 1
dd1FF9.tmo	tmo	Other/...	Drive C: \Users...				0 B	03/05/2013 17:43:53.6	03/05/2013 1

10⁶ MP4 HEX B HEX MP4

Drive C:

\ and subdirectories

	Name	Type	Sender	Recd	Size
<input type="checkbox"/>	software				13.8
<input type="checkbox"/>	software				8.8
<input type="checkbox"/>	SOFTWARE				70.7
<input type="checkbox"/>	software				7.8
<input type="checkbox"/>	SOFTWARE				70.8





Filter: Type

- ☐ E-mail
- ☐ Internet
- ☐ Plain Text
- ☐ Text/Word Processing
- ☐ Misc Documents
- ☐ Database, Spreadsheet, Finance
- ☐ Pictures
- ☐ Video
- ☐ Sound/Music
- ☐ Programs
- ☐ Archives
- ☐ Source Code
- ☐ Disk Image
- ☐ Windows Registry
- ☐ Windows Internals
- ☐ Unix/Linux System Files
- ☐ Mac OS X/iOS System Files
- ☐ P2P
- ☐ Cryptography
- ☐ Fonts
- ☐ Other/unknown type

Activate

Deactivate

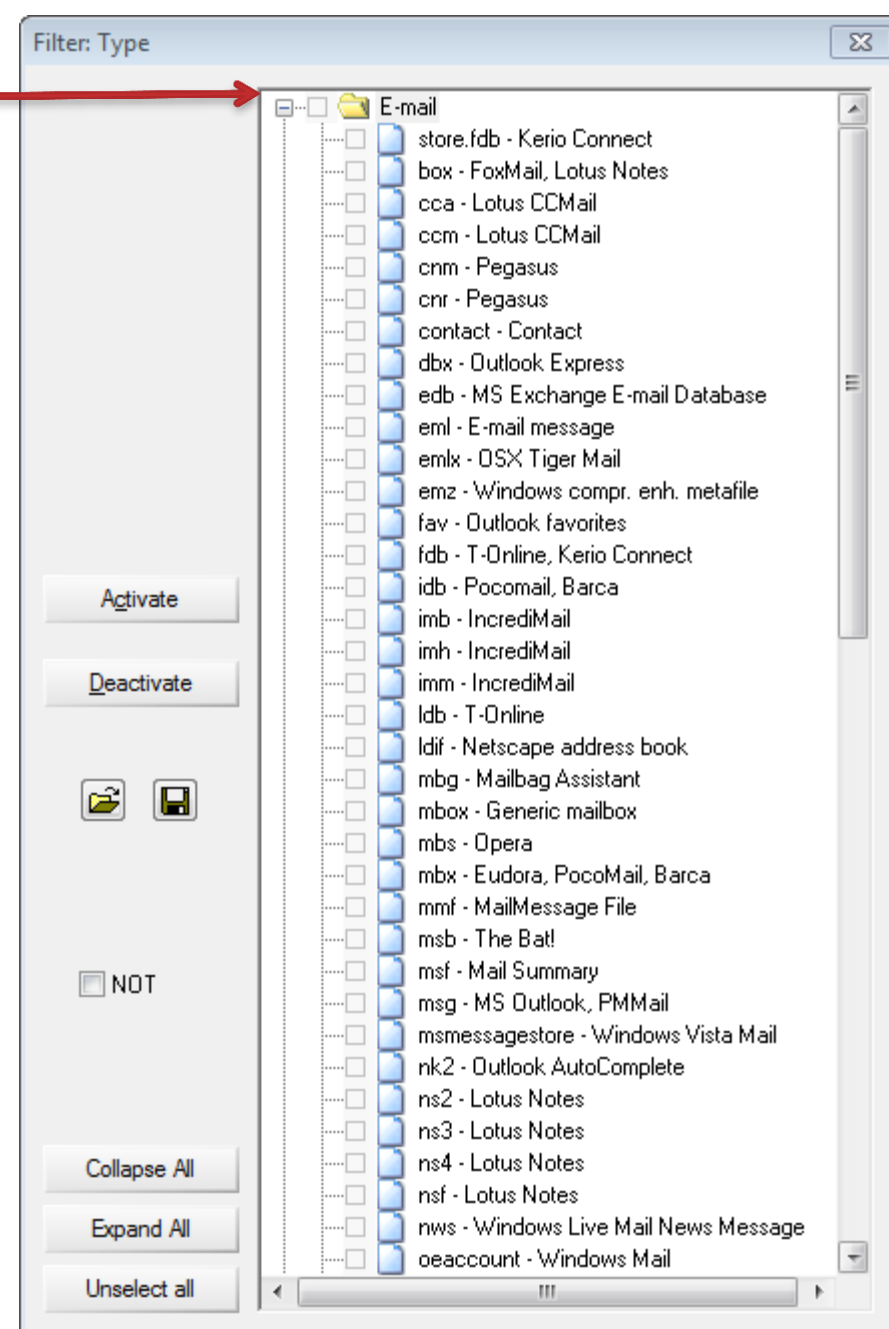
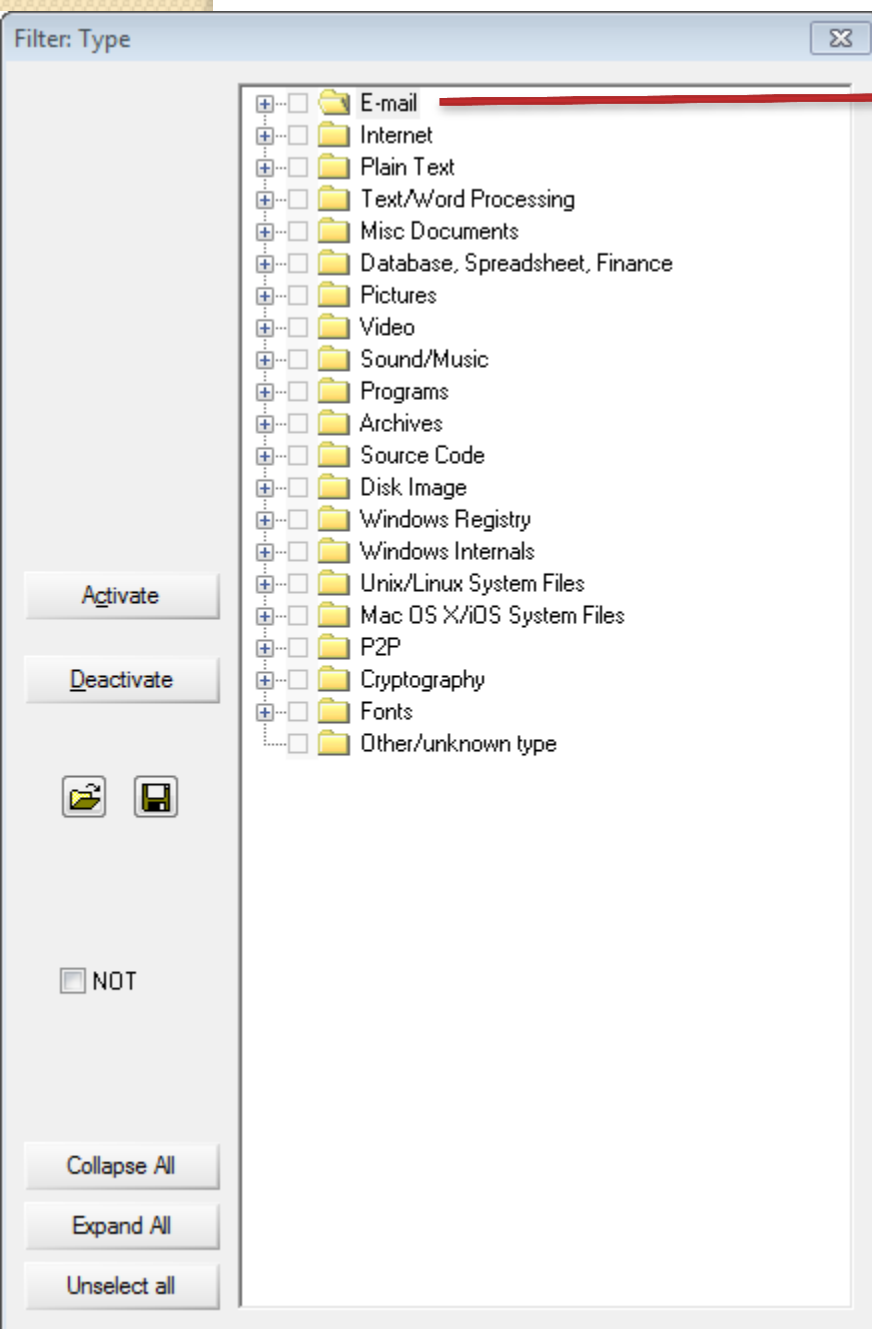
 

☐ NOT

Collapse All

Expand All

Unselect all



Directory Browser Options, Filters



- ☒ Group files and directories
- ☐ Group existing and deleted items³
- ☒ Dbl-click=View instead of Explore³
- ☒ Open and search files incl. slack³
- ☐ List dir.s when exploring recursively
- ☐ Apply filters to directories, too
- ☒ Recursive selection statistics³
- ☒ Tag and hide recursively³
- ☒ Use checkmarks for tagging
- ☐ Full path sorting for parent objects
- ☐ No sorting initially after start-up
- ☒ Store filter and sort settings in cases
- ☐ Dynamic e-mail columns
- ☒ Show # files³
- ☐ Display SHA-1 hashes in Base32
- ☒ Keep track of viewed files ...

- ☒ List existing files
- ☒ List previously ex. items...

- ☒ List tagged items
- ☒ List half tagged items
- ☒ List untagged items
- ☒ List viewed files
- ☒ List unviewed files
- ☐ List hidden items
- ☒ List non-hidden items

Unhide all

Totally remove hidden items!

First scrollable column: Name ▼

OK

Cancel

Column widths in pixels:

Name	141	Y	○
Description	0		○
Ext.	0		○
Type	51	Y	○
Type status	0	Y	○
Type descr.	0		○
Category	0	Y	○
Evidence object	0		○
Path	0	Y	○
Parent name	0	Y	○
Child objects	0	Y	○
Sender	47	Y	○
Recipients	33	Y	○
Size	60	Y	○
Created	130	Y	○
Modified	109	Y	○
Accessed	109	Y	○
Record update	0	Y	○
Deletion	0	Y	○
Int. creation	0	Y	○
Attr.	40	Y	○
Owner	0	Y	○
Links	0		○
# files	0		○
#ST	0		○
Search terms	0	Y	○
1st sector	55		○
ID	0		○
Int. ID	0	Y	○
Int. parent	0		○
Pixels	0	Y	○
SC%	30	Y	○
Hash	0	Y	○
Hash set	0	Y	○
Hash category	0	Y	○
Report table	60	Y	○
Comment	60	Y	○
Metadata	0	Y	○

Filter

Created

Modified

Accessed

Record update

Deletion

Int. creation

(OR)

☐ Before

☐ After

☒ Between

01/31/2003 20:05:06

&

01/31/2003 20:05:06

UTC -08:00 Pacific Time US & Canada

Activate

Deactivate

Filter: SC%



- ☒ \geq %
- ☐ \leq
- ☐ irrelevant
- ☐ ?
- ☐ b/w

Activate

Deactivate

Filter: Search terms



☐ NOT

Activate

Deactivate

Help

Filter: Search terms



Empty search results area

☐ NOT

Activate

Deactivate

Help

Filter: Sender (enter as substring)



@badapple.com

Activate

Deactivate

Help

Filter: Size

☐

<=

1

MB

☐

>=

3

KB

Activate

Deactivate

tmp	Other/...	Drive C: \Users...	0 B	02/05/2013 13:01:03.0	02/05/2013 13:01:...	02/05/2013
F2ED-E...	html	Intern...	10.0 KB	08/03/2012 14:08:14.0	08/03/2012 14:08:...	12/23/201
tmp	Other/...		0 B	01/24/2013 10:12:51.9	01/24/2013 10:12:...	01/24/201

File
Preview
Details

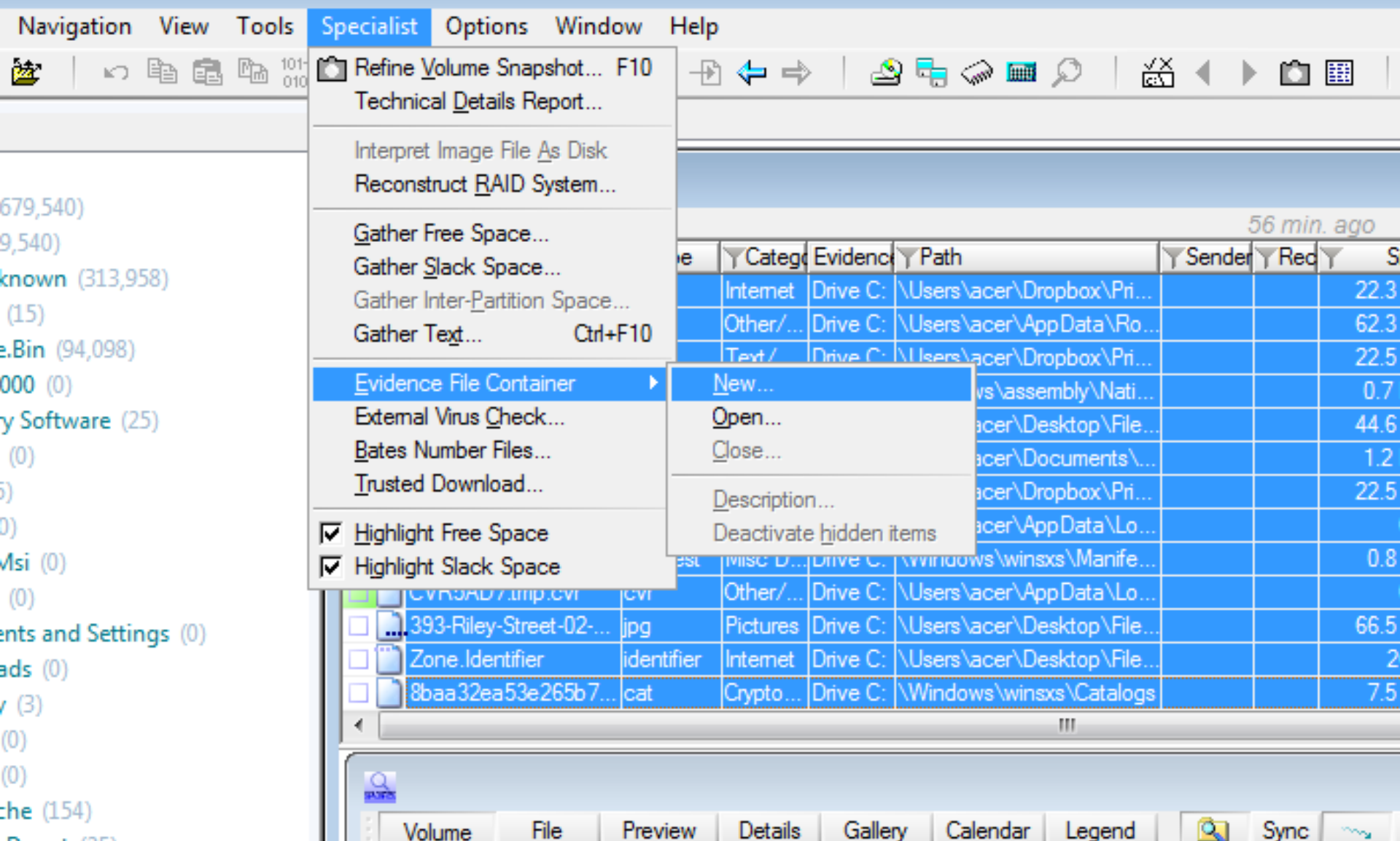
e Volume Snapshot

	GUID-D4C5F2ED-E23D-4ADD-9DBF-55B9EAF90B1
	existing file
	html
	html
	not verified
	HTML
	Internet
object	Drive C:

View
Viewer Programs
Open
Print...
Recover/Copy...
Export list...
Report table associations...
Edit comment...
Tag
Select
Hide
Navigation
Refine Volume Snapshot...
Simultaneous Search...
Run X-Tensions...
Create Hash Set...

Sync
GUID-D4C5F2ED-E23D-4ADD-9DBF-55B9EAF90B1.html
Duplicates in dir. browser based on hash...
All tagged items on volume
All UNtagged items on volume

- Duplicate files can be hidden.



Evidence file container creation



Make Backup/Create Image File



Save in:



Smith's Files



Open as read-only



Recent Places



Desktop



Libraries



Computer



Network

Name

Date modified

Type

Size

No items match your search.

File name:

Custodian_Smith



Save as type:

Raw Image/Container (.001, .dd, .img, .ctr)



Save

Cancel

- ☐ Fill indirectly (such that antivirus tools can intervene)
- ☒ Include evidence object names as top directory level
- ☐ Include directory data structures of the file system
- ☒ New format, partially compatible with non X-Ways tools
- ☒ Allow files as parents of files (understood only by X-W* v16)
- ☒ Export report table associations³
- ☐ Pass on comments about files with the container
- ☒ Store hash: MD5

Creator:

Brett Shavers

Internal designation:

Custodian_Smith

Description:

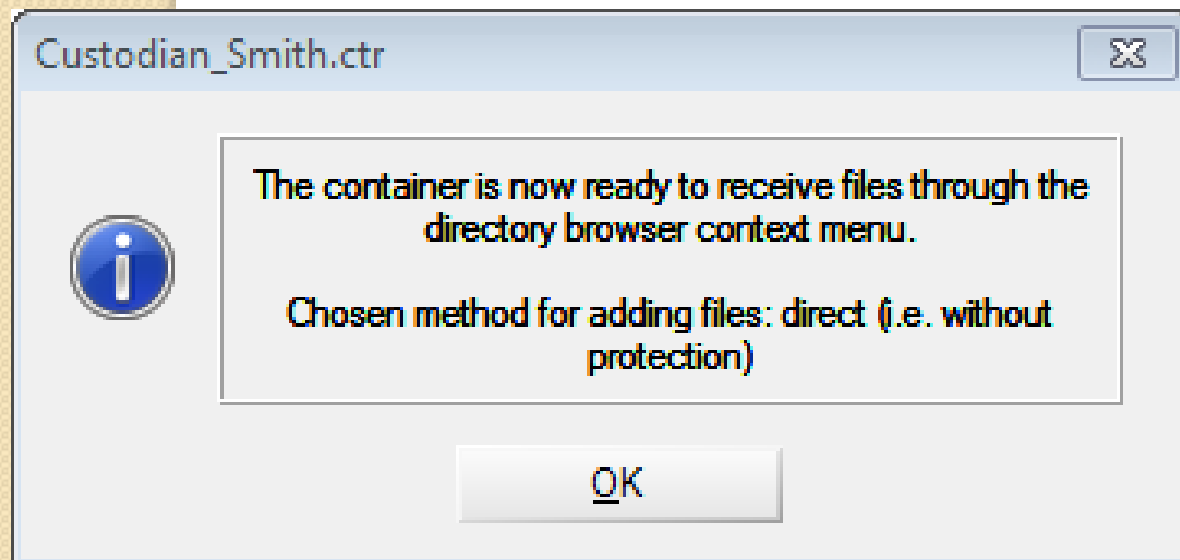
John Smith's work laptop.
Word documents collected between dates of 10/01/2005 and 02/04/2012
Active files only

Dell Inspiron Laptop, SN 123467890

OK

Cancel

Help





File Edit

CTIN

- Case Root (679,540)
- Drive C: (679,540)

Drive C:

Drive C:

Add Image

Selected: 0

Smith's Files

☐ Refine Volume Snapshot
Recent Places

Desktop



Libraries



Computer



Network

Name	Date modified	Type	Size
<u>Custodian Smith.ctr</u>	<u>3/9/2013 2:49 PM</u>	<u>CTR File</u>	<u>132 KB</u>

File name:

Files of type:

All Types of Images (.001, .dd, .img, .ctr, .e01, .vhd, .vmdk)

Open

Cancel

Too much on your screen?

- Then use more than one monitor.
- Drag a pane from XWF to another monitor and you have more usable screen real estate.

Questions?



bshavers@Gmail.com
by Google™