X-WAYS FORENSICS
Advanced Methods and Techniques

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

<table>
<thead>
<tr>
<th>F-Response Target</th>
<th>Connected</th>
<th>Local Disk</th>
</tr>
</thead>
</table>
The Refine Volume Snapshot
The following search terms will be searched simultaneously (one per line):

- D:
- E:

Speed tip!
- 1 hit per file needed only (faster)
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)
Refine Volume Snapshot

Volume snapshot of Partition 2: 177,202 items, 11,055 tagged, 0 hidden, 3,807 already viewed

- Take new one

Execute now:
- Run X-Tensions
- Particularly thorough file system data structure search
- File header signature search

Already done?
- Signatures...

- Compute hash
- 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;*.olk;
  - 4MsgSource;*.msg;*.oft;*.mbs;store.fdb

- 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

- 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
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 05/19/2000 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

**********
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 <http://creativecommons.org/licenses/by/3.0/us/> . To provide attribution, please cite to "ZL Technologies, Inc. (http://www.zti.com)."
**********
Extracts to .msg to selected directory

Re HL&P 600.msg
Out on vacation

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 personally)
Sort by sender/receiver

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 personnel)
No items match your search.
Exported email from a PST file

- Exported as .eml, by file path or flattened
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

<table>
<thead>
<tr>
<th>Subject</th>
<th>2nd rev Dec. 1999 Josey Ranch nom</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sender</td>
<td>Susan D Trevino</td>
</tr>
<tr>
<td>Recipients</td>
<td>Daren J Farmer, Carlos J Rodriguez, Lauri A Allen, Stretch Brennan <a href="mailto:djb@KCESEnergy.com">djb@KCESEnergy.com</a>, Kevin McLarney <a href="mailto:kmm@KCESEnergy.com">kmm@KCESEnergy.com</a>,</td>
</tr>
</tbody>
</table>

------------------------------------------ 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

<table>
<thead>
<tr>
<th>Date/Subject</th>
<th>Sender</th>
<th>Recipients</th>
<th>Viewer Programs</th>
<th>Export list</th>
</tr>
</thead>
<tbody>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Susan D Trevino</td>
<td>Daren J Farmer, Daren J Farmer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Melissa K Ratnala</td>
<td>Brent A Price</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Daren J Farmer</td>
<td>Susan D Trevino</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Howard B Camp</td>
<td>Tima Lannou</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Aimee Lannou</td>
<td>Daren J Farmer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Carlos J Rodriguez</td>
<td>Alex Saldana</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Robert E Lloyd</td>
<td>Daren J Farmer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Kenya Perkins</td>
<td>Daren J Farmer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Gregg Lenart</td>
<td>Howard B Camp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Ricky Archer</td>
<td>Tima Lannou</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Robert E Lloyd</td>
<td>Daren J Farmer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2nd rev Dec. 1999...</td>
<td>Stella L Morris</td>
<td>Daren J Farmer</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Choose metadata for the list
Place into a spreadsheet and make it pretty

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Name</td>
<td>Description</td>
<td>Ext.</td>
<td>Sender</td>
<td>Recipients</td>
<td>Evidence object</td>
</tr>
<tr>
<td>3</td>
<td>Meter 1431 - Nov 1999.eml</td>
<td>extracted e-mail</td>
<td>eml</td>
<td>Howard B Camp</td>
<td>Aimee Lannou,Daren J Farmer, Stacey Neuweiler, Mary</td>
<td>ctin, Partition 2</td>
</tr>
<tr>
<td>4</td>
<td>Meter 1431 - Nov 1999.eml</td>
<td>extracted e-mail</td>
<td>eml</td>
<td>Aimee Lannou</td>
<td>Daren J Farmer,George Grant</td>
<td>ctin, Partition 2</td>
</tr>
<tr>
<td>5</td>
<td>Y2K - Texas Log.eml</td>
<td>extracted e-mail</td>
<td>eml</td>
<td>Carlos J Rodriguez</td>
<td>Alex Saldana, Robert Superty,Daren J Farmer</td>
<td>ctin, Partition 2</td>
</tr>
<tr>
<td>6</td>
<td>Calpine Daily Gas Nomination.eml</td>
<td>with attachment</td>
<td>eml</td>
<td>Ricky Archer &lt;RickyA@Robert E Lloyd,Daren J Farmer</td>
<td>ctin, Partition 2</td>
<td></td>
</tr>
</tbody>
</table>
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.
Summary of Attachments by File Type

**Metric**

- Total size of attachments: 366.90 MB
- Total count of attachments: 2,898
- Unable to determine file type: 0 (0.00%)

**Visible**

- File type: *.xls: 1,306 (45.67%)
- File type: *.doc: 902 (31.12%)
- File type: *.pdf: 18 (0.62%)
- File type: *.rtf: 2 (0.07%)

**Hidden**

- File type: *.exe: 8 (0.28%)
- File type: *.xlsx: 42 (1.45%)
- File type: *.txt: 2 (0.07%)

**Message Summary**

- Total messages: 8,098
- Total size of all messages (including attachments): 398.69 MB

**Visible Attachment Summary**

- Total visible attachments (ex: Word document): 2,808
- Total size of visible attachments: 366.90 MB

**Hidden Attachment Summary**

- Total hidden attachments (ex: embedded images): 0
- Total size of hidden attachments: 0.00 bytes
<table>
<thead>
<tr>
<th>Analysis Summary</th>
<th>Analysis Summary</th>
<th>Analysis Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Started at</td>
<td>14:29:46 tt</td>
<td></td>
</tr>
<tr>
<td>Time elapsed</td>
<td>0:03:58 tt</td>
<td></td>
</tr>
<tr>
<td>Stopped at</td>
<td>14:33:44 tt</td>
<td></td>
</tr>
<tr>
<td>Mailbox and folder summary</td>
<td>Mailbox and folder summary</td>
<td>Mailbox and folder summary</td>
</tr>
<tr>
<td>Mailbox(es)</td>
<td>daren_farmer_001.pst</td>
<td>100.00%</td>
</tr>
<tr>
<td>Total folders</td>
<td>58 / 58</td>
<td>100.00%</td>
</tr>
<tr>
<td>Folders with messages and/or subfolders</td>
<td>54</td>
<td>93.10%</td>
</tr>
<tr>
<td>Empty folders</td>
<td>4</td>
<td>6.90%</td>
</tr>
<tr>
<td>Message summary</td>
<td>Message summary</td>
<td>Message summary</td>
</tr>
<tr>
<td>Total messages</td>
<td>8,098 / 8,098</td>
<td>100.00%</td>
</tr>
<tr>
<td>Total size of all messages (including attachments)</td>
<td>398.69 MB</td>
<td></td>
</tr>
<tr>
<td>Duplicate messages</td>
<td>3230</td>
<td>39.89%</td>
</tr>
<tr>
<td>Total size of all duplicate messages</td>
<td>146.84 MB</td>
<td></td>
</tr>
<tr>
<td>Total size of all attachments</td>
<td>366.9 MB</td>
<td></td>
</tr>
<tr>
<td>Average message size</td>
<td>50.41 KB</td>
<td></td>
</tr>
<tr>
<td>Size of largest message</td>
<td>14.11 MB</td>
<td></td>
</tr>
<tr>
<td>Total inbound messages</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>Total outbound messages</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>Total internal messages</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>Unable to determine flow direction</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>Messages with visible attachments</td>
<td>2184</td>
<td>26.97%</td>
</tr>
<tr>
<td>Messages with hidden attachments</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>Messages with BCC recipients</td>
<td>0</td>
<td>0.00%</td>
</tr>
<tr>
<td>Messages with no identifiable recipients (usually spam)</td>
<td>856</td>
<td>10.57%</td>
</tr>
<tr>
<td>Messages with no identifiable sender</td>
<td>5711</td>
<td>70.52%</td>
</tr>
</tbody>
</table>
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.
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.
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
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Category</th>
<th>Evidence object</th>
<th>Path</th>
<th>Y Sender</th>
<th>Y Recipients</th>
<th>Size</th>
<th>Created</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GreenBubbles.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\Windows...</td>
<td>Daren J Farmer</td>
<td><a href="mailto:tjfarmer@juno.com">tjfarmer@juno.com</a></td>
<td>6.3 KB</td>
<td>07/13/200</td>
<td></td>
</tr>
<tr>
<td>grandsn4.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\daren_fame...</td>
<td>Daren J Farmer</td>
<td><a href="mailto:tjfarmer@juno.com">tjfarmer@juno.com</a></td>
<td>36.2 KB</td>
<td>07/13/200</td>
<td></td>
</tr>
<tr>
<td>grandsn3.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\daren_fame...</td>
<td>Daren J Farmer</td>
<td><a href="mailto:tjfarmer@juno.com">tjfarmer@juno.com</a></td>
<td>34.4 KB</td>
<td>07/13/200</td>
<td></td>
</tr>
<tr>
<td>OrangeCircles.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\Program Files...</td>
<td>Daren J Farmer</td>
<td><a href="mailto:tjfarmer@juno.com">tjfarmer@juno.com</a></td>
<td>6.2 KB</td>
<td>07/13/200</td>
<td></td>
</tr>
<tr>
<td>OrangeCircles.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\Windows...</td>
<td>Daren J Farmer</td>
<td><a href="mailto:tjfarmer@juno.com">tjfarmer@juno.com</a></td>
<td>6.2 KB</td>
<td>07/13/200</td>
<td></td>
</tr>
<tr>
<td>grandsn2.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\daren_fame...</td>
<td>Daren J Farmer</td>
<td><a href="mailto:tjfarmer@juno.com">tjfarmer@juno.com</a></td>
<td>15.2 KB</td>
<td>07/13/200</td>
<td></td>
</tr>
<tr>
<td>pic17578.pcx</td>
<td>pccx</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\daren_fame...</td>
<td>Charlie Stone</td>
<td><a href="mailto:cUSTOMerlist@enron.com">cUSTOMerlist@enron.com</a></td>
<td>164 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bush-limo.jpg</td>
<td>pccx</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\daren_fame...</td>
<td>Charlie Stone</td>
<td><a href="mailto:cUSTOMerlist@enron.com">cUSTOMerlist@enron.com</a></td>
<td>98.3 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audiovox Slimline.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\daren_fame...</td>
<td>Daren J Farmer</td>
<td>Heath Chota</td>
<td>8.3 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>algore.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\daren_fame...</td>
<td>Daren J Farmer</td>
<td><a href="mailto:dheineke@tsteel.com">dheineke@tsteel.com</a></td>
<td>177 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Floriabebops.jpg</td>
<td>jpg</td>
<td>Pictures</td>
<td>ctin, Partition 2</td>
<td>\daren_fame...</td>
<td>Daren J Farmer</td>
<td><a href="mailto:dheineke@tsteel.com">dheineke@tsteel.com</a></td>
<td>121 KB</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Modified</td>
<td>Accessed</td>
<td>Recal</td>
<td>Deleting</td>
<td>Attr.</td>
<td>Search</td>
<td>1st sector</td>
<td>Int. LBA</td>
<td>Report</td>
</tr>
<tr>
<td>-------</td>
<td>----------</td>
<td>----------</td>
<td>-------</td>
<td>----------</td>
<td>-------</td>
<td>--------</td>
<td>------------</td>
<td>---------</td>
<td>--------</td>
</tr>
<tr>
<td></td>
<td>06/10/2009 14:29...</td>
<td>07/13/2009 15:28...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6,228,328</td>
<td>9735</td>
<td>0.0%</td>
</tr>
<tr>
<td></td>
<td>06/10/2009 14:29...</td>
<td>07/13/2009 15:28...</td>
<td></td>
<td></td>
<td>A</td>
<td></td>
<td>6,228,392</td>
<td>9747</td>
<td>21%</td>
</tr>
<tr>
<td>atta...</td>
<td>06/10/2009...</td>
<td>07/13/2009...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28,738,172</td>
<td>176684</td>
<td></td>
</tr>
<tr>
<td>atta...</td>
<td>06/10/2009...</td>
<td>07/13/2009...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28,738,173</td>
<td>176683</td>
<td></td>
</tr>
<tr>
<td>atta...</td>
<td>06/10/2009...</td>
<td>07/13/2009...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28,738,173</td>
<td>176682</td>
<td></td>
</tr>
<tr>
<td>atta...</td>
<td>06/10/2009...</td>
<td>07/13/2009...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28,738,174</td>
<td>176154</td>
<td></td>
</tr>
<tr>
<td>atta...</td>
<td>06/10/2009...</td>
<td>07/13/2009...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28,738,174</td>
<td>175833</td>
<td></td>
</tr>
<tr>
<td>atta...</td>
<td>06/10/2009...</td>
<td>07/13/2009...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28,738,175</td>
<td>175375</td>
<td></td>
</tr>
<tr>
<td>atta...</td>
<td>06/10/2009...</td>
<td>07/13/2009...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28,738,176</td>
<td>175092</td>
<td></td>
</tr>
<tr>
<td>atta...</td>
<td>06/10/2009...</td>
<td>07/13/2009...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>28,738,176</td>
<td>175044</td>
<td></td>
</tr>
</tbody>
</table>

Filter: SC%

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

Activate
Deactivate
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.
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

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Category</th>
<th>Evidence</th>
<th>Path</th>
<th>Sender</th>
<th>Recvd</th>
<th>Size</th>
<th>Created</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>ddC5D7.tmp</td>
<td>tmp</td>
<td>Other</td>
<td>Drive C:</td>
<td>Users</td>
<td>0 B</td>
<td></td>
<td>0</td>
<td>03/05/2013</td>
<td>03/05/2013</td>
</tr>
<tr>
<td>CVR5519.tmp.cvr</td>
<td>cvr</td>
<td>Other</td>
<td>Drive C:</td>
<td>Users</td>
<td>0 B</td>
<td></td>
<td>0</td>
<td>03/05/2013</td>
<td>03/05/2013</td>
</tr>
<tr>
<td>CVR1A3B.tmp.cvr</td>
<td>cvr</td>
<td>Other</td>
<td>Drive C:</td>
<td>Users</td>
<td>0 B</td>
<td></td>
<td>0</td>
<td>03/05/2013</td>
<td>03/05/2013</td>
</tr>
<tr>
<td>dd30CC.tmp</td>
<td>tmp</td>
<td>Other</td>
<td>Drive C:</td>
<td>Users</td>
<td>0 B</td>
<td></td>
<td>0</td>
<td>03/05/2013</td>
<td>03/05/2013</td>
</tr>
<tr>
<td>dd1FF9.tmp</td>
<td>tmp</td>
<td>Other</td>
<td>Drive C:</td>
<td>Users</td>
<td>0 B</td>
<td></td>
<td>0</td>
<td>03/05/2013</td>
<td>03/05/2013</td>
</tr>
</tbody>
</table>
## Directory Browser Options, Filters

### List Items
- **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
- **Unhide all**
- **Totally remove hidden items**

### Column widths in pixels:

<table>
<thead>
<tr>
<th>Column</th>
<th>Width</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>141</td>
</tr>
<tr>
<td>Description</td>
<td>0</td>
</tr>
<tr>
<td>Ext.</td>
<td>0</td>
</tr>
<tr>
<td>Type</td>
<td>51</td>
</tr>
<tr>
<td>Status</td>
<td>0</td>
</tr>
<tr>
<td>Type descr.</td>
<td>0</td>
</tr>
<tr>
<td>Category</td>
<td>0</td>
</tr>
<tr>
<td>Evidence</td>
<td>0</td>
</tr>
<tr>
<td>Object</td>
<td>0</td>
</tr>
<tr>
<td>Path</td>
<td>0</td>
</tr>
<tr>
<td>Parent name</td>
<td>0</td>
</tr>
<tr>
<td>Child objects</td>
<td>0</td>
</tr>
<tr>
<td>Sender</td>
<td>47</td>
</tr>
<tr>
<td>Recipients</td>
<td>33</td>
</tr>
<tr>
<td>Size</td>
<td>60</td>
</tr>
<tr>
<td>Created</td>
<td>130</td>
</tr>
<tr>
<td>Modified</td>
<td>109</td>
</tr>
<tr>
<td>Accessed</td>
<td>109</td>
</tr>
<tr>
<td>Record update</td>
<td>0</td>
</tr>
<tr>
<td>Deletion</td>
<td>0</td>
</tr>
<tr>
<td>Int. creation</td>
<td>0</td>
</tr>
<tr>
<td>Attr.</td>
<td>40</td>
</tr>
<tr>
<td>Owner</td>
<td>0</td>
</tr>
<tr>
<td>Links</td>
<td>0</td>
</tr>
<tr>
<td># files</td>
<td>0</td>
</tr>
<tr>
<td>#ST</td>
<td>0</td>
</tr>
<tr>
<td>Search terms</td>
<td>0</td>
</tr>
<tr>
<td>1st sector</td>
<td>55</td>
</tr>
<tr>
<td>ID</td>
<td>0</td>
</tr>
<tr>
<td>Int. ID</td>
<td>0</td>
</tr>
<tr>
<td>Int. parent</td>
<td>0</td>
</tr>
<tr>
<td>Pixels</td>
<td>0</td>
</tr>
<tr>
<td>SC%</td>
<td>30</td>
</tr>
<tr>
<td>Hash</td>
<td>0</td>
</tr>
<tr>
<td>Hash set</td>
<td>0</td>
</tr>
<tr>
<td>Hash category</td>
<td>0</td>
</tr>
<tr>
<td>Report table</td>
<td>60</td>
</tr>
<tr>
<td>Comment</td>
<td>60</td>
</tr>
<tr>
<td>Metadata</td>
<td>0</td>
</tr>
</tbody>
</table>
Filter: SC%
Filter: Sender (enter as substring)

@badapple.com

Activate  Deactivate  Help
Filter: Size

- Less than or equal to: 1 MB
- Greater than or equal to: 3 KB

[Activate] [Deactivate]
• Duplicate files can be hidden.
Evidence file container creation
Include evidence object names as top directory level
New format, partially compatible with non X-Ways tools
Allow files as parents of files (understood only by XWx v16)
Export report table associations
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
The container is now ready to receive files through the directory browser context menu.

Chosen method for adding files: direct (i.e. without protection)
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