FORENSIC FAILS
SHIFT + DELETE WON'T HELP YOU HERE
ERIC ROBI + MICHAEL PERKLIN
DEFCON 21
AUGUST 4, 2013
ABOUT THIS GUY

ERIC ROBI

Founder of Elluma Discovery - 11 years

Forensic Examiner

Thousands of exams

Expert Witness

Likes Cats
ABOUT THIS OTHER GUY

MICHAEL PERKLIN
Senior Investigator / Forensic Examiner
Security Professional
Thousands of exams
Likes to break things
... A Lot
AGENDA

7 Stories full of FAIL
Learn something about Forensic Techniques
Fails brought to you by both THE SUSPECT and THE EXAMINER
*Names have been changed to protect the idiots on both sides
  *Many of the case facts have been changed too.
  I don’t know why. We don’t need to. It just seemed like a nice thing to do.
This presentation required the creation of Teh Fail Matrix
User Retard Level
10
Punishment Level
5
$ Distress Caused
5
Bonus Points
15

Fail Matrix

Personal Fial

Lost the case
35

$$$$

GF left him

$$$$$
FAIL #1 - The “Wasn’t Me” Defense

Employee Bob worked in sales at Acme

He resigned his position and left to work for a competitor

Allegation was made that he took Acme’s company list with him
FAIL #1 - The “Wasn’t Me” Defense

Bob said “I’ve got nothing to hide”. “Come at me bros!”.

We began imaging the drive and started planning the examination

- Look for deleted files in unallocated space
- Look for ‘recent files’ used by common programs (Word, Excel)
- Look for USB device insertion

Finally the drive finished imaging…

DEFCON EXCLUSIVE… New finding!
FAIL #1 - The “Wasn’t Me” Defense

Bob had used a data destruction program to overwrite every byte of unallocated space on his drive.

He used a pattern that was not likely to appear through normal use of a Windows operating system.

The existence of this pattern MIGHT suggest POSSIBLE willful destruction of evidence.

...maybe
What have we learned...

#1

Data destruction software can almost ALWAYS be detected

Even if you don’t use a repeating pattern, it’s still detectable

We may not know what you destroyed

But we definitely know you destroyed SOMETHING

Also, mean phrases make people dislike you.
FAIL #2 - The Nickelback Guy

- Standard case: Allegation of stolen confidential documents
- Suspect John left NOCFED industries after 3 years to work for a competitor
- John worked on confidential projects
- NOCFED was worried John took data to competitor
FAIL #2 - The Nickelback Guy

- Opened HDD to begin analysis
- Lots of MP3s identified
- Found the confidential documents (as expected)
- Almost immediately, something jumped out at me as an examiner
  (We’ll get into why in a bit...)
FAIL #2 - The Nickelback Guy

It seems that John assumed that nobody would play his Nickelback MP3s!! (a sound assumption)

They are all .avi files with a renamed filename. Clever, kinda

What was he hiding???
FAIL #2 - The Nickelback Guy

PREGGER PORN!!!!

It seemed John did more at work than just work on his confidential project!!
What have we learned...

#2

Examiners see files in a long list; not a folder/tree structure.

A “File Signature Analysis” is run that analyzes every file on the HDD.

It compares the contents of files with the extensions of the filenames.

Any file with a discrepancy is identified for closer analysis.

John’s attempt at hiding something put it at the top of the list for analysis.
User Retard Level: 12
Punishment Level: 13
$Distress Caused: 0
Bonus Points: 5

Fail Matrix

Lost his job: 30
For owning Nickelback
ABC Firm outsourced key part of their business for many years

Received bills on an hourly basis. Amounted to several million $ per year on average.

Client started bill review project. Suspected some tasks were taking a weeeeee bit too long.

Asked us to help
FAIL #3 - JUST BILL ME LATER

- Thousands PDF format invoices not much help.
- Where to start? Not a lot of clues
- Ah ha! Located billing database on vendor's network
- Forensic copy of database, migrated DB to MSSQL
- No easy way to compare DB to PDFs.
FAIL #3 - JUST BILL ME LATER

Reverse engineered tables in DB
Noticed audit logs were turned on!
Ran many queries of time billed vs. audit logs
Noticed that audit logs showed changes to DB
Time inflation! Rate inflation!
What have we learned #3

Audit logs off by default. Turned ON by IT peeps!

Audit logs are the BEST evidence of theft in a DB case.

LESSON: Don’t turn on audit logs if you plan to cheat your client!
User Retard Level

8

Punishment Level

18

$ Distress Caused

15

Bonus Points

4

Fail Matrix

Had to refund the $

45

$12M + refunded

Systematic culture of overbilling
FAIL #4 - Smoking Gun.txt

Smoking Gun.txt is the gag name of “the file that proves the case”

Comes from cheesy western movies where the murderer’s gun is still smoking, proving he fired the shot

This case is another intellectual property case

Again, an employee left his company to go work for a competitor
FAIL #4 - Smoking Gun.txt

Imaged the drive

Kicked-off standard analysis scripts

Opened up his Desktop folder

You can tell a lot about a person by the way they organize their Desktop!

Immediately solved the case
FAIL #4 - Smoking Gun.txt
FAIL #4 - Smoking Gun.txt

The guy had created a folder filled with data from his previous employer

Bonus PowerPoint presentation to bring his new colleagues up-to-speed
What have we learned...

Sometimes people don't even try.
<table>
<thead>
<tr>
<th>User Retard Level</th>
<th>Fail Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Had to settle for $46</td>
</tr>
<tr>
<td>Punishment Level</td>
<td>$1.5M in damages</td>
</tr>
<tr>
<td>10</td>
<td>Zero effort!</td>
</tr>
<tr>
<td>$Distress Caused</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Bonus Points</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
</tr>
</tbody>
</table>
FAIL #5 - HIDING IN THE CLOUD

Top sales guy leaves company. Sales plummet.

They suspect he took customer list, but can't prove it.

We image his computer and start looking for the usual clues:
FAIL #5 - HIDING IN THE CLOUD

Link files: Shows opened files

BagMRU - Registry key shows user folder activity

Jump lists - Shows opened files (Win 7+)

IE history - Shows accessed files

NO LOVE. SHOW ME THE LOVE.
FAIL #5 - HIDING IN THE CLOUD

- Searched IE history
- Found a .htm file containing some javascript pointing to "filesanywhere.com"
- BINGO!
- Showed acct ID, upload times, file names
- FOUND SOME SWEET LOVIN'! (stolen files)
//Fill nodes data
oNodes[0] = new node("Stolen_File.txt", 'file', 'USER\Eric\Test\', 'F', '', 'false', '74', '10/19/2011 3:15:05 PM');

oNodes[1] = new node("Recipe_for_Coke.txt", 'file', 'USER\Eric\Test\', 'F', '', 'false', '23', '10/19/2011 3:15:05 PM');
<table>
<thead>
<tr>
<th>Timestamp (EDT)</th>
<th>Filename</th>
<th>Type</th>
<th>Destination Folder</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/17/10 12:39:26 PM</td>
<td>Agents.xls</td>
<td>file</td>
<td></td>
<td>2,691,584</td>
</tr>
<tr>
<td>6/17/10 12:41:30 PM</td>
<td>D - Generic flyer.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>1,503,744</td>
</tr>
<tr>
<td>6/17/10 12:41:30 PM</td>
<td>ACCESSORIAL CHARGE CHANGES.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>58,880</td>
</tr>
<tr>
<td>6/17/10 12:41:30 PM</td>
<td>account review worksheet.xls</td>
<td>file</td>
<td>\New Reps\</td>
<td>19,968</td>
</tr>
<tr>
<td>6/17/10 12:41:30 PM</td>
<td>ACI Codes Guide Training.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>19,968</td>
</tr>
<tr>
<td>6/17/10 12:41:30 PM</td>
<td>0 - Generic flyer.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>15,872</td>
</tr>
<tr>
<td>6/17/10 12:41:30 PM</td>
<td>Adding venues.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>78,848</td>
</tr>
<tr>
<td>6/17/10 12:41:30 PM</td>
<td>Adding venues.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>30,741</td>
</tr>
<tr>
<td>6/17/10 12:41:31 PM</td>
<td>Apples to apples.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>25,600</td>
</tr>
<tr>
<td>6/17/10 12:41:36 PM</td>
<td>Carpet brochure.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>2,338,816</td>
</tr>
<tr>
<td>6/17/10 12:41:36 PM</td>
<td>Carpet brochure.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>215,976</td>
</tr>
<tr>
<td>6/17/10 12:41:43 PM</td>
<td>Cases and Crates.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>3,163,136</td>
</tr>
<tr>
<td>6/17/10 12:41:43 PM</td>
<td>Cases and Crates.xls</td>
<td>file</td>
<td>\New Reps\</td>
<td>241,206</td>
</tr>
<tr>
<td>6/17/10 12:41:43 PM</td>
<td>CC REQUEST FORM FORM 2010.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>353,280</td>
</tr>
<tr>
<td>6/17/10 12:41:43 PM</td>
<td>CC REQUEST FORM FORM REVISED.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>353,792</td>
</tr>
<tr>
<td>6/17/10 12:41:46 PM</td>
<td>Charges &amp; Specials.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>66,048</td>
</tr>
<tr>
<td>6/17/10 12:41:46 PM</td>
<td>Cold Call Tracker.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>5,219</td>
</tr>
<tr>
<td>6/17/10 12:41:46 PM</td>
<td>Cold Call Tracker.xls</td>
<td>file</td>
<td>\New Reps\</td>
<td>15,872</td>
</tr>
<tr>
<td>6/17/10 12:41:46 PM</td>
<td>Cold calling inquisition.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>25,600</td>
</tr>
<tr>
<td>6/17/10 12:41:46 PM</td>
<td>Cold calling tree.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>32,768</td>
</tr>
<tr>
<td>6/17/10 12:41:46 PM</td>
<td>Cold calling tree.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>8,689</td>
</tr>
<tr>
<td>6/17/10 12:41:47 PM</td>
<td>Combo.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>244,224</td>
</tr>
<tr>
<td>6/17/10 12:41:47 PM</td>
<td>Combo.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>49,134</td>
</tr>
<tr>
<td>6/17/10 12:41:47 PM</td>
<td>Convention Centers.xls</td>
<td>file</td>
<td>\New Reps\</td>
<td>30,720</td>
</tr>
<tr>
<td>6/17/10 12:41:47 PM</td>
<td>Convention Centers.xlsx</td>
<td>file</td>
<td>\New Reps\</td>
<td>30,720</td>
</tr>
<tr>
<td>6/17/10 12:41:48 PM</td>
<td>Credit Card Authorization, 03-29-10.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>428,032</td>
</tr>
<tr>
<td>6/17/10 12:41:48 PM</td>
<td>Credit Card Authorization, 03-29-10.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>428,032</td>
</tr>
<tr>
<td>6/17/10 12:41:48 PM</td>
<td>Customer service questionnaire.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>33,280</td>
</tr>
<tr>
<td>6/17/10 12:41:48 PM</td>
<td>Customer service questionnaire.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>29,184</td>
</tr>
<tr>
<td>6/17/10 12:41:54 PM</td>
<td>Display Pages Catalog.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>2,934,406</td>
</tr>
<tr>
<td>6/17/10 12:41:54 PM</td>
<td>Display Pages Catalog.xls</td>
<td>file</td>
<td>\New Reps\</td>
<td>317,744</td>
</tr>
<tr>
<td>6/17/10 12:41:55 PM</td>
<td>Domestic Carriers rebuttals.xls</td>
<td>file</td>
<td>\New Reps\</td>
<td>31,744</td>
</tr>
<tr>
<td>6/17/10 12:41:55 PM</td>
<td>Domestic Carriers rebuttals.xlsx</td>
<td>file</td>
<td>\New Reps\</td>
<td>31,744</td>
</tr>
<tr>
<td>6/17/10 12:41:55 PM</td>
<td>Domestic Carriers.xls</td>
<td>file</td>
<td>\New Reps\</td>
<td>54,272</td>
</tr>
<tr>
<td>6/17/10 12:41:55 PM</td>
<td>Domestic Carriers.xlsx</td>
<td>file</td>
<td>\New Reps\</td>
<td>54,272</td>
</tr>
<tr>
<td>6/17/10 12:41:55 PM</td>
<td>Fax cover sheet.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>165,888</td>
</tr>
<tr>
<td>6/17/10 12:41:55 PM</td>
<td>Fax cover sheet.pdf</td>
<td>file</td>
<td>\New Reps\</td>
<td>165,888</td>
</tr>
<tr>
<td>6/17/10 12:41:56 PM</td>
<td>Flyer template in header.doc</td>
<td>file</td>
<td>\New Reps\</td>
<td>417,280</td>
</tr>
</tbody>
</table>
FAIL #5 - HIDING IN THE CLOUD

Opposing attorney handed us CD with an Outlook.PST
There are no items to show in this view.
FAIL #5 - HIDING IN THE CLOUD

First thing we do is search for deleted emails
FAIL #5 – HIDING IN THE CLOUD

10s of thousands of deleted emails
Changes the direction of the case 180 degrees
#WINNING
Who deleted the emails…????
What have we learned #5

IE history is hard to wipe

Found a new artifact (filesanywhere)

.js files are capable of love too!

Uploading files still leaves traces

Attorneys shouldn’t mess with evidence! (Especially if they don’t understand how PSTs work)
Fail Matrix

Huge lawsuit
$3.5M in fees and damages
Attorney may lose his license

User Retard Level
18

Punishment Level
10

$ Distress Caused
8

Bonus Points
15
FAIL #6 - The RDP Bounce

Was called in to investigate a network breach

Some symptoms existed that indicated unauthorized access

Large company

Windows environment

Thousands of PCs in multiple sites around the world
FAIL #6 - The RDP Bounce

Analyzed one computer known to have been breached

Logs showed RDP was used to connect in (Local Admin password)

Logs showed RDP was used to connect out

Tip of the iceberg???
FAIL #6 - The RDP Bounce

Analyzed machine that came before

Analyzed machine that came after

Started noticing a pattern...
FAIL #6 - The RDP Bounce

We still wanted to know WHY. What was the target?

Followed the chain forward

Reached a high-profile machine

Target identified. Steal highly-confidential documents
FAIL #6 - The RDP Bounce

Focused analysis on target machine

What did they do?

What did they take?

Within minutes the attacker was identified

How?
Xerox 9700 [1977]

FAIL #6 - The RDP Bounce

By default, RDP maps your printer when connecting to a remote machine.

This allows you to “print” from their machine to your printer.

Attacker forgot to turn this off.
What have we learned... #6

Log entries generated from innocuous system events can give insight into user actions
User Retard Level: 20
Punishment Level: 15
$Distress Caused: 8
Bonus Points: 20

Fail Matrix

63

Lost job
Loss of income, no reference
Do some research!
Edgar charged with possession of contraband on his computer

Claims innocence (as usual)

Examined the computer and looked at examiner’s report and the allegations:
FAIL #7 - EPIC PORNO

FAIL

Allegations:

#1 Edgar downloaded porn

#2 Edgar's user accounts had passwords

#3 Edgar utilized newsgroups to download porn (for realz???)
FAIL #7 - EPIC PORNO

Allegation #1

Edgar downloaded illegal porn

Notable thing: Edgar left his house in April 2012
IE History


P2P Software - Download folder

Name: t-287878478-naughty file (sound - english)(2).mpg
Full Path: E\Users\Joe\AppData\Local\Ares\My Shared Folder\t-287878478-naughty file (sound - english)(2).mpg

File Created 12/17/12 10:32:56 AM
Last Accessed 12/17/12 10:32:56 AM
Last Written 12/17/12 12:57:35 PM
FAIL #7 - EPIC PORNO

Allegation #2

Edgar used Outlook Express to download porn
FAIL #7 - EPIC PORNO FAIL

In reality:

Outlook Express set up with account “PornoLuvr”...

AFTER Edgar moved out of his house

Only headers downloaded in Outlook Express. No content. No photos! (Just file names).
FAIL #7 - EPIC PORNO

FAIL

Allegation #3

Edgar’s user account had a password

Inference is that only Edgar had access
<table>
<thead>
<tr>
<th>User Name</th>
<th>LM Password</th>
<th>NT Password</th>
<th>&lt;8</th>
<th>&gt;14</th>
<th>LM Hash</th>
<th>NT Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>NO PASSWORD</td>
<td>NO PASSWORD</td>
<td>x</td>
<td></td>
<td>NO PASSWORD</td>
<td>NO PASSWORD</td>
</tr>
<tr>
<td>Guest</td>
<td>NO PASSWORD</td>
<td>NO PASSWORD</td>
<td>x</td>
<td></td>
<td>NO PASSWORD</td>
<td>NO PASSWORD</td>
</tr>
<tr>
<td>Edgar</td>
<td>NO PASSWORD</td>
<td>NO PASSWORD</td>
<td>x</td>
<td></td>
<td>NO PASSWORD</td>
<td>NO PASSWORD</td>
</tr>
</tbody>
</table>

Ready for passwords recovering
3 of 3 passwords were found (100.000%)
FAIL #7 - EPIC PORNO

More facts (undiscovered by examiner)

P2P client used to download porn...

Into a new user account

AFTER Edgar moved out of the house
FAIL #7 - EPIC PORNO FAIL

Our report submitted to prosecutor

Government DROPS the charges... YEARS later

and after $$$$ legal costs

Super Timeline Analysis - SANS & Rob Lee - THANK YOU!
FAIL #7 - EPIC PORNO FAIL

Government interviews Edgar’s friend

Friend confesses

Friend tried to frame Edgar to get jiggy with Edgar’s wife!!

Court clears Edgar’s name
What have we learned... #7

Base conclusions upon ACTUAL EVIDENCE

Find multiple artifacts backing up allegations

Tie it to a person, not just a machine
FORENSIC FAILS

SHIFT + DELETE WON'T HELP YOU HERE

ERIC ROBI + MICHAEL PERKLIN
DEFCON 21
AUGUST 4, 2013