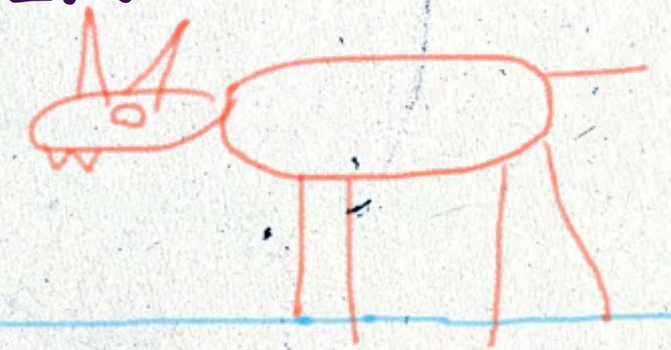
FORENSIC FAILS

SHIFT + DELETE WON'T HELP YOU HERE

ERIC ROBI + MICHAEL PERKLIN

DEFCON 21

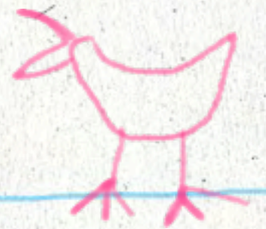
AUGUST 4, 2013



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

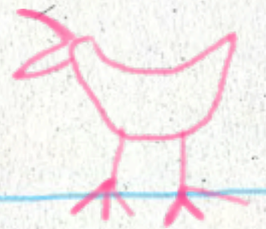
Senior Investigator / Forensic Examiner

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

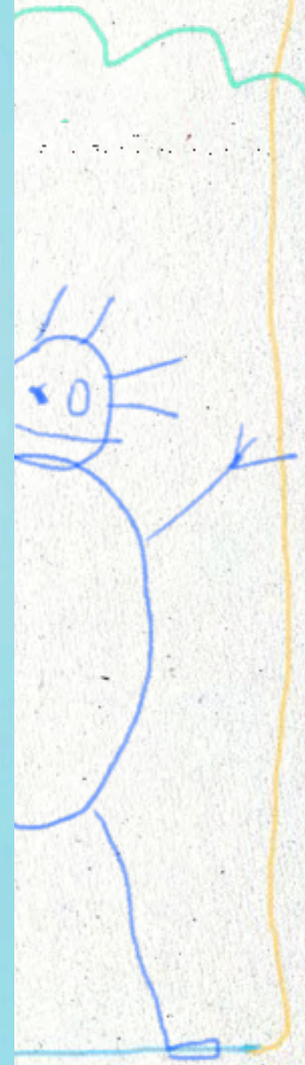
Personal Fial

Lost the case

35

$$$$

GF left him

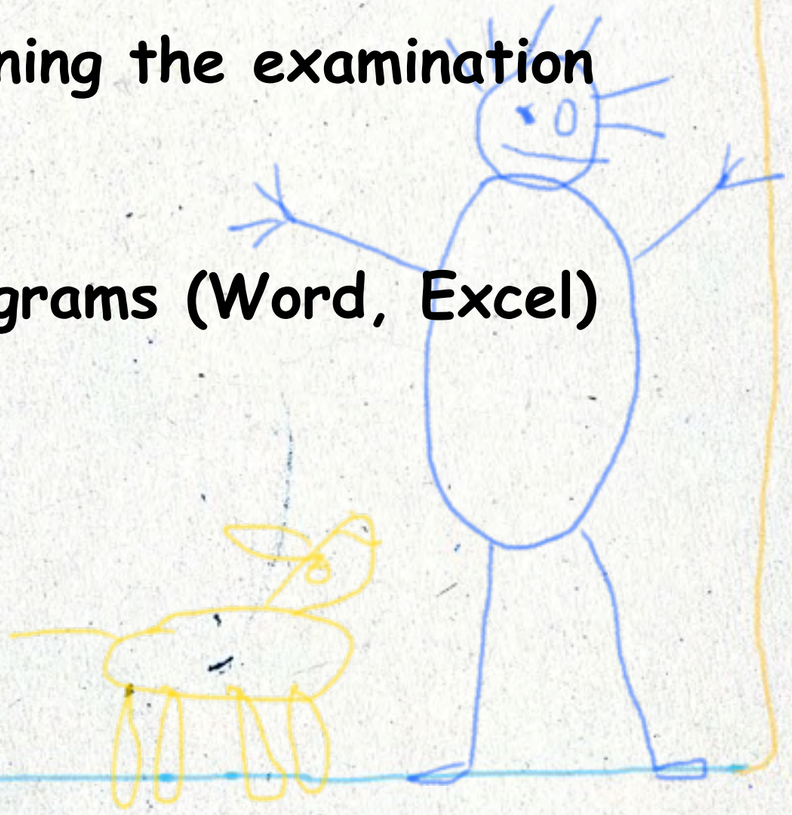


FAIL #1 – The "Wasn't Me" Defense

- 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!



*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***
*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you
* you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you ·
· f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f*** you · f***

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.

User Retard Level

12

Punishment Level

12

$ Distress Caused

3

Bonus Points

0

Fail Matrix

Lost the case

27

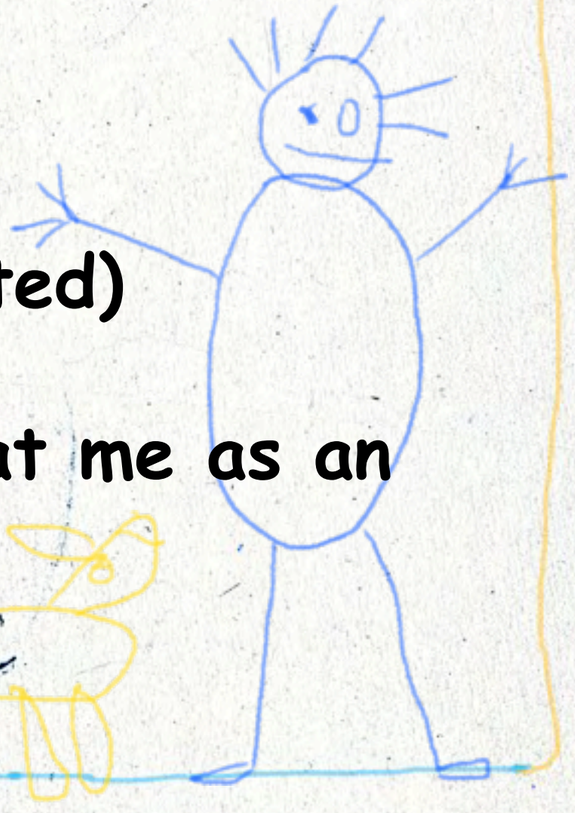
Under $100K

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

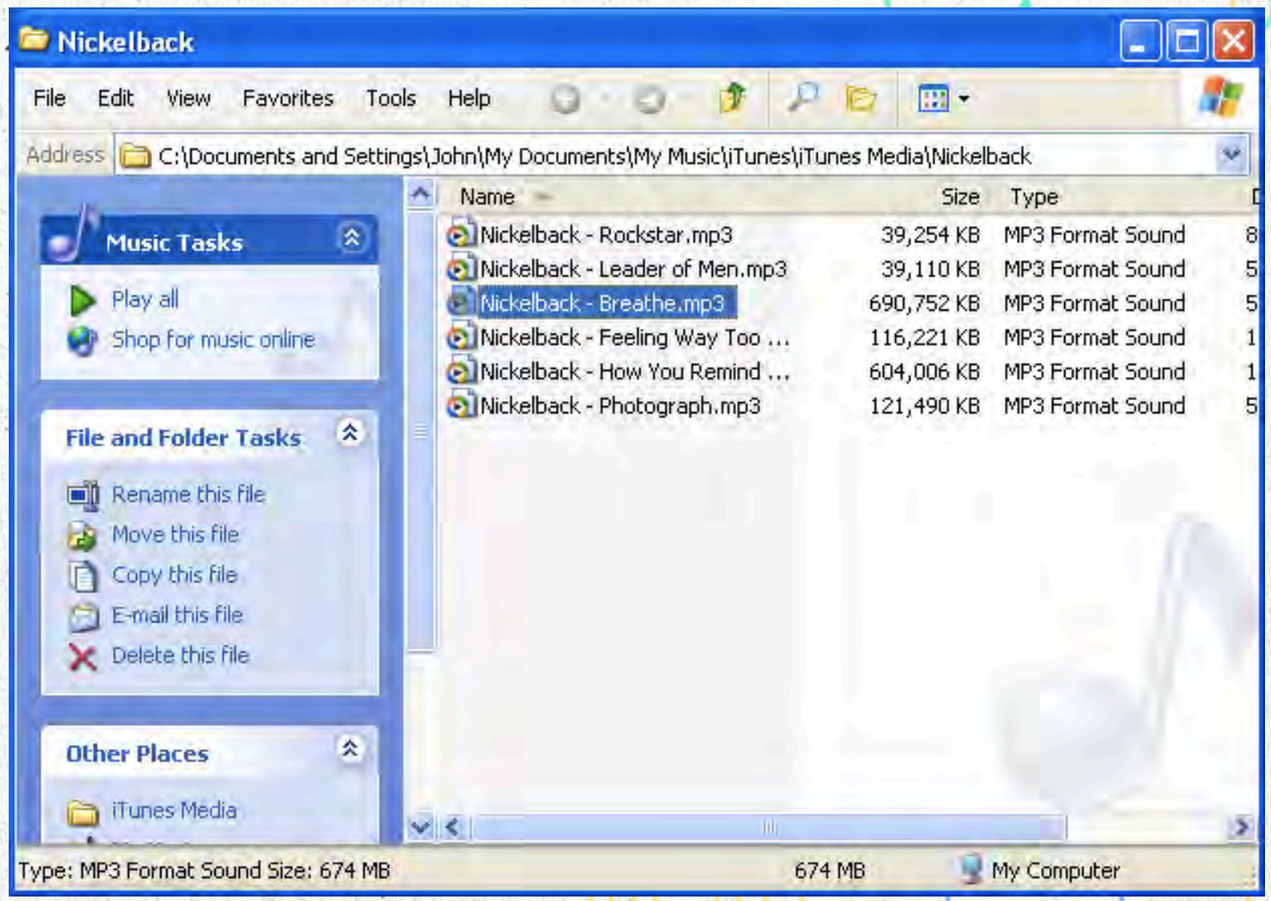
FAIL #2 - The Nickelback Guy

- 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???

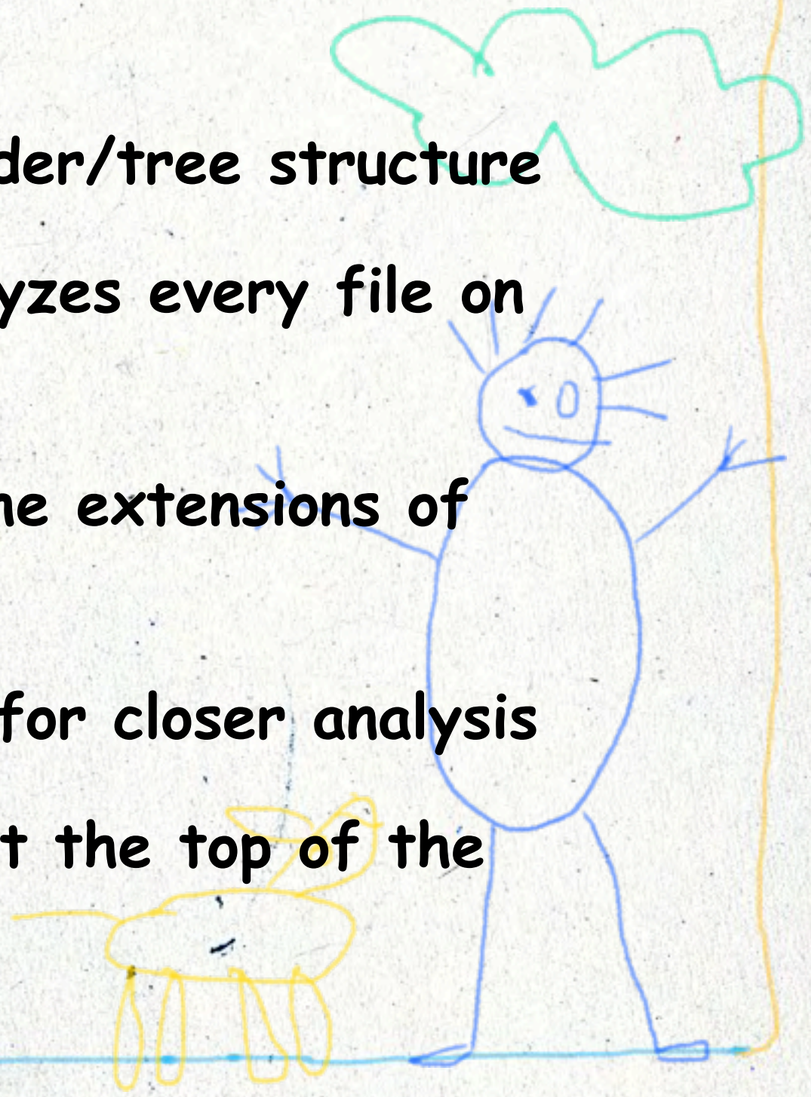


FAIL #2 - The Nickelback Guy

- 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

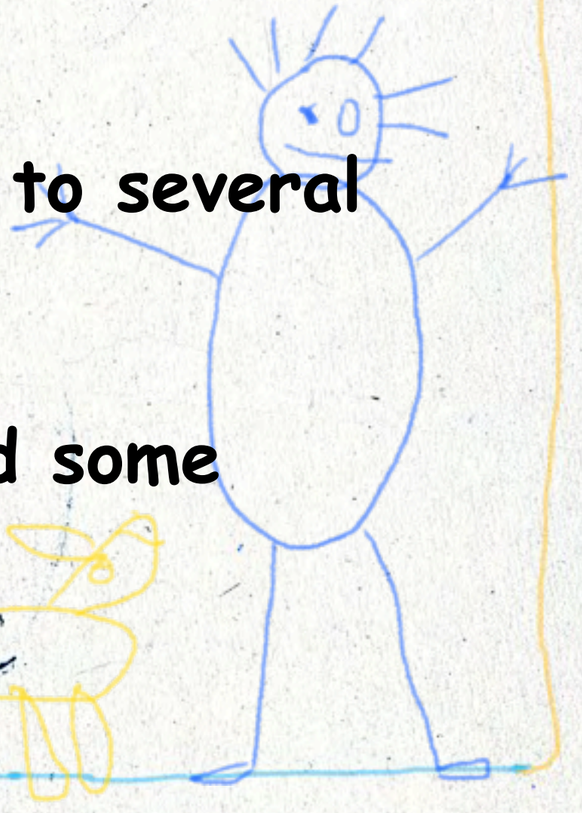
Lost his job

30

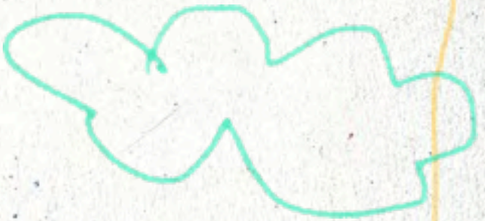
For owning Nickelback

FAIL #3 - JUST BILL ME LATER

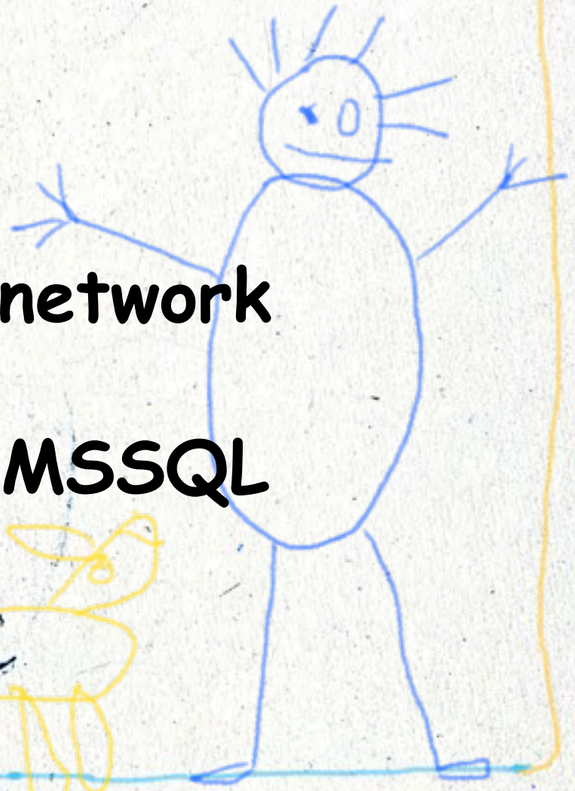
- ABC Firm outsourced key part of their business for many years
- Received bills on an hourly basis. Amounted to several million $ per year on average.
- Client started bill review project. Suspected some tasks were taking a weeeeeee bit too long.
- Asked us to help



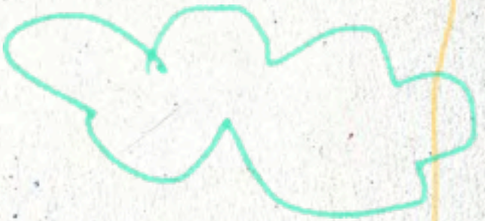
FAIL #3 - JUST BILL ME LATER



- 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.



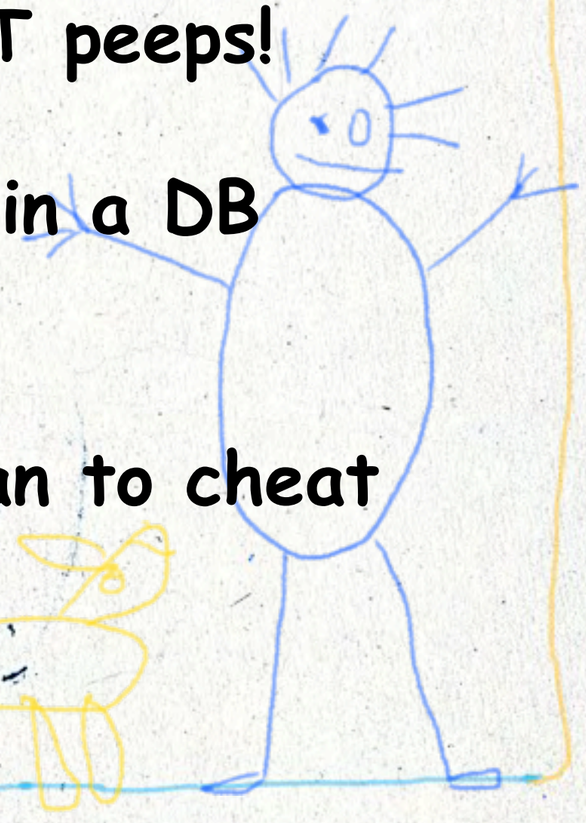
FAIL #3 - JUST BILL ME LATER



- 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!



Fail Matrix

User Retard Level

8

Punishment Level

18

$ Distress Caused

15

Bonus Points

4

Had to refund the $

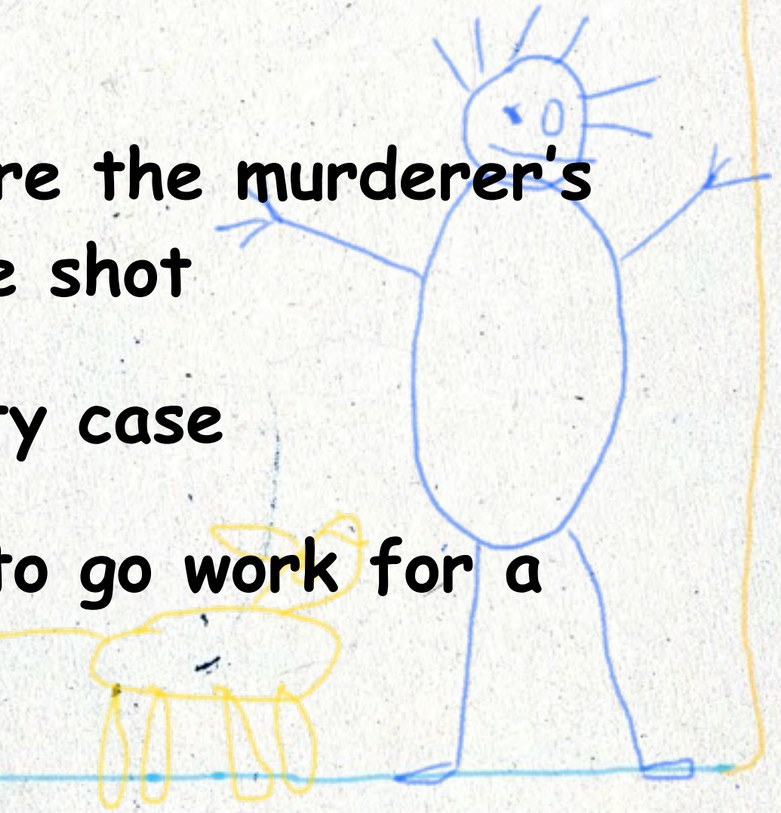
45

$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



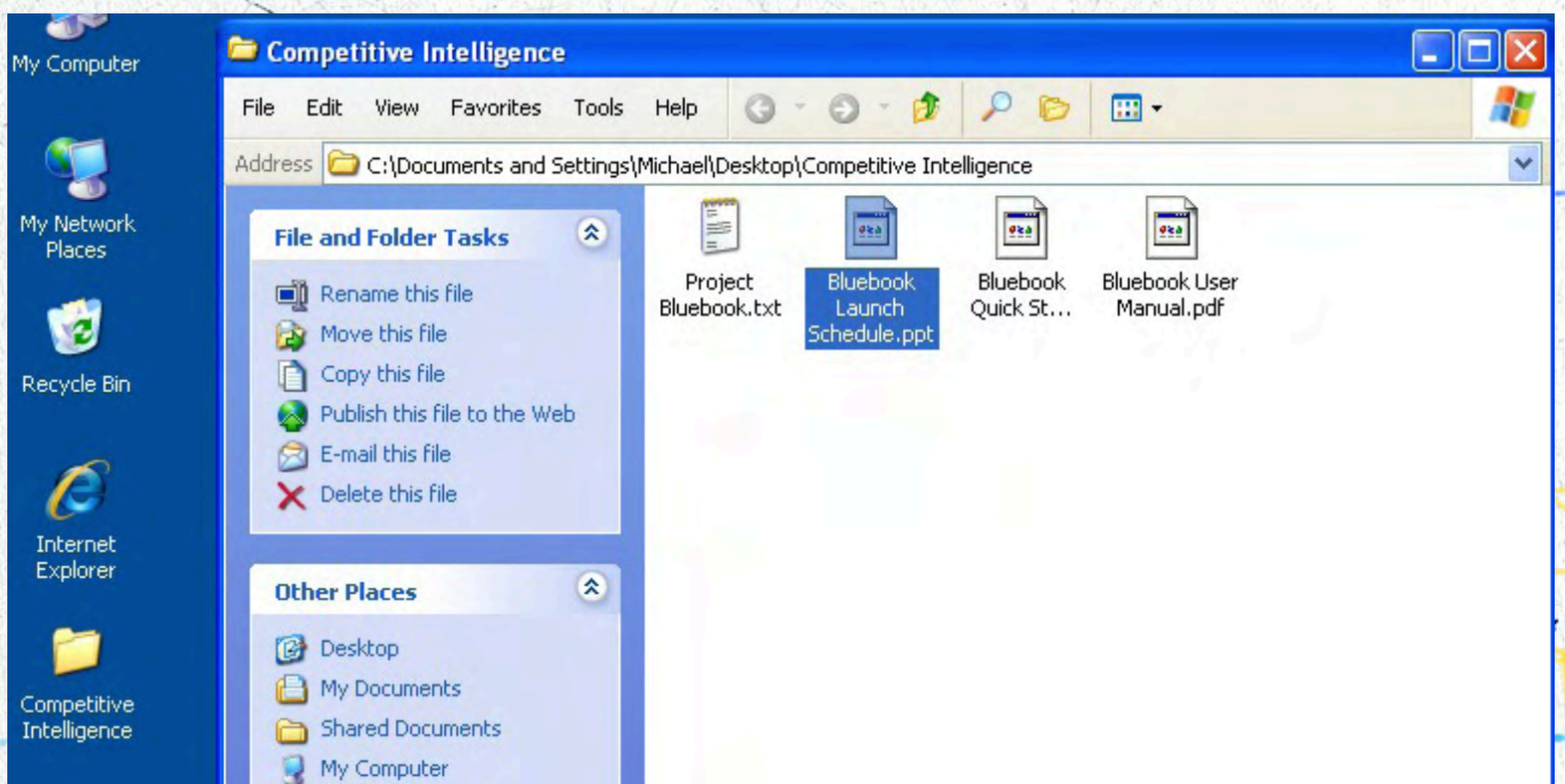
FAIL #4 - Smoking Gun.txt

- 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

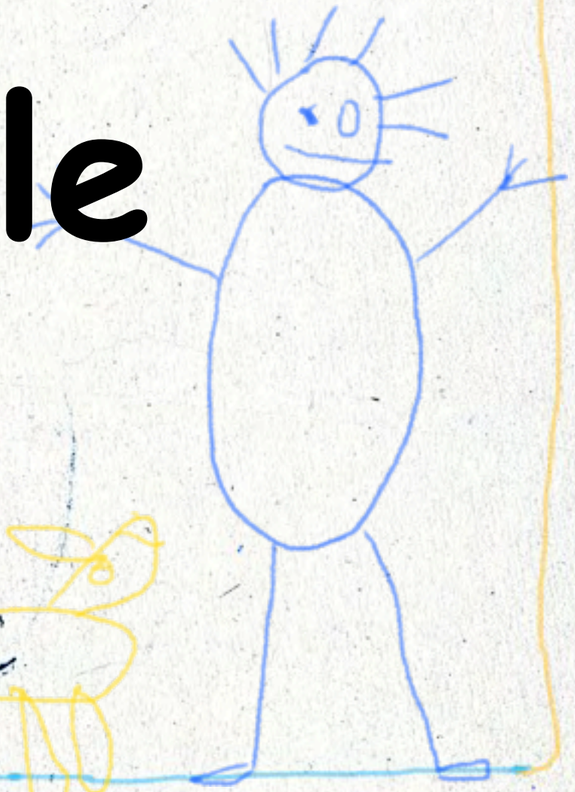
FAIL #4 - Smoking Gun.txt

- 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...
#4

Sometimes people don't even try.



Fail Matrix

User Retard Level

18

Punishment Level

10

$ Distress Caused

6

Bonus Points

12

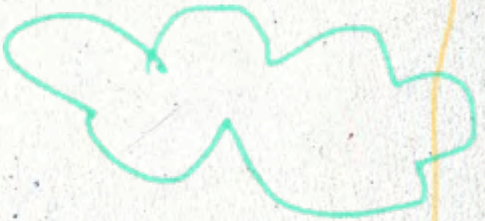
Had to settle for $

46

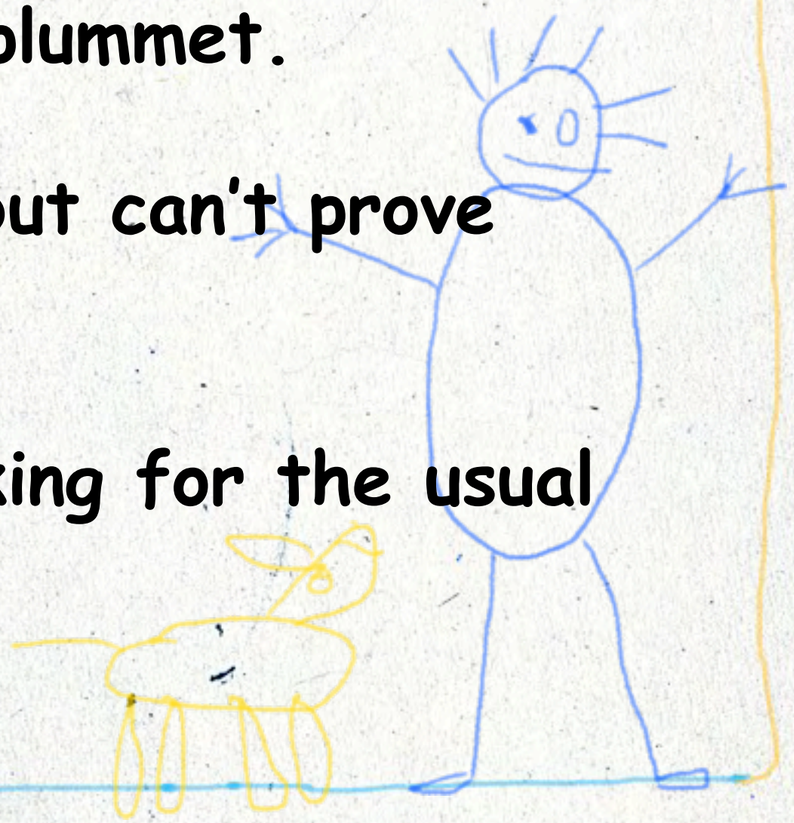
$1.5M in damages

Zero effort!

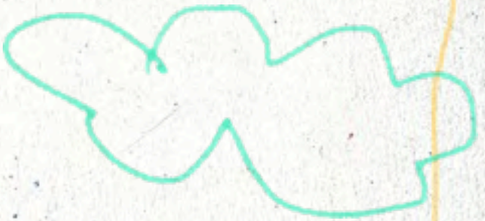
FAIL #5 - HIDING IN THE CLOUD



- 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

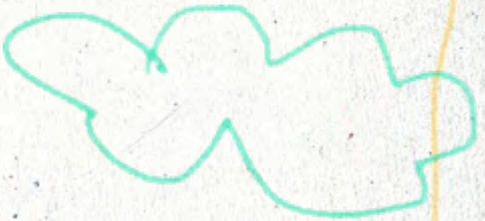


- Link files: Shows opened files
- BagMRU - Registry key shows user folder activity
- Jump lists - Shows opened files (Win 7+)
- IE history - Shows accessed files
- NO LOVE. SHOW ME THE LOVE.

FAIL #5 - HIDING IN THE CLOUD

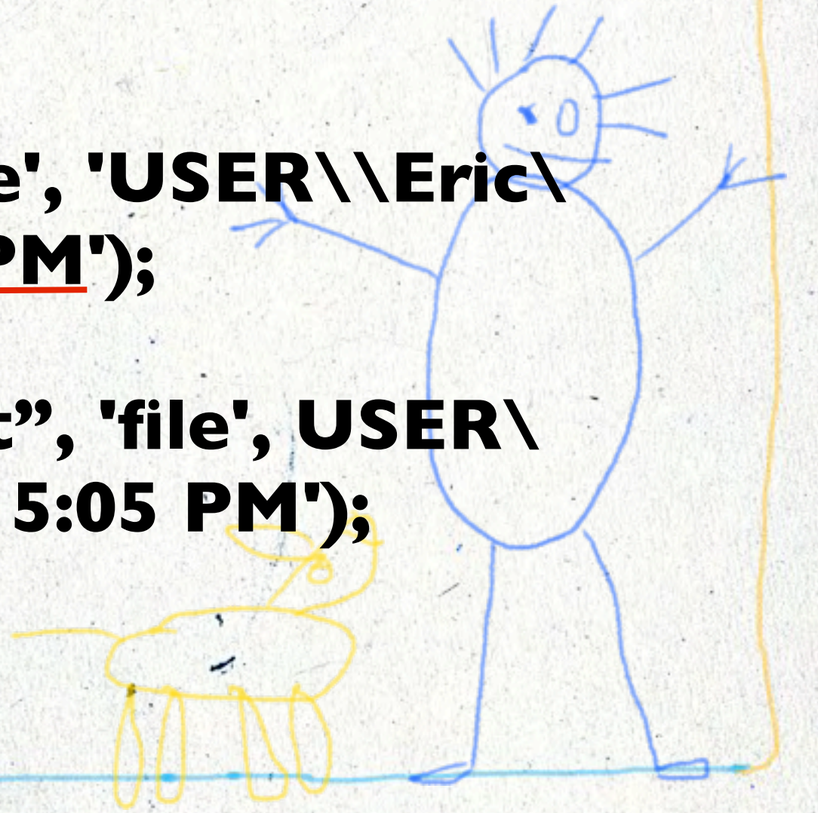
- Searched IE history
- Found a .htm file containing some javascript pointing to"filesanywhere.com"
- BINGO!
- Showed acct ID, upload times, file names
- FOUND SOME SWEET LOVIN'! (stolen files)

FAIL #5 - HIDING IN THE CLOUD



```
//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');
```

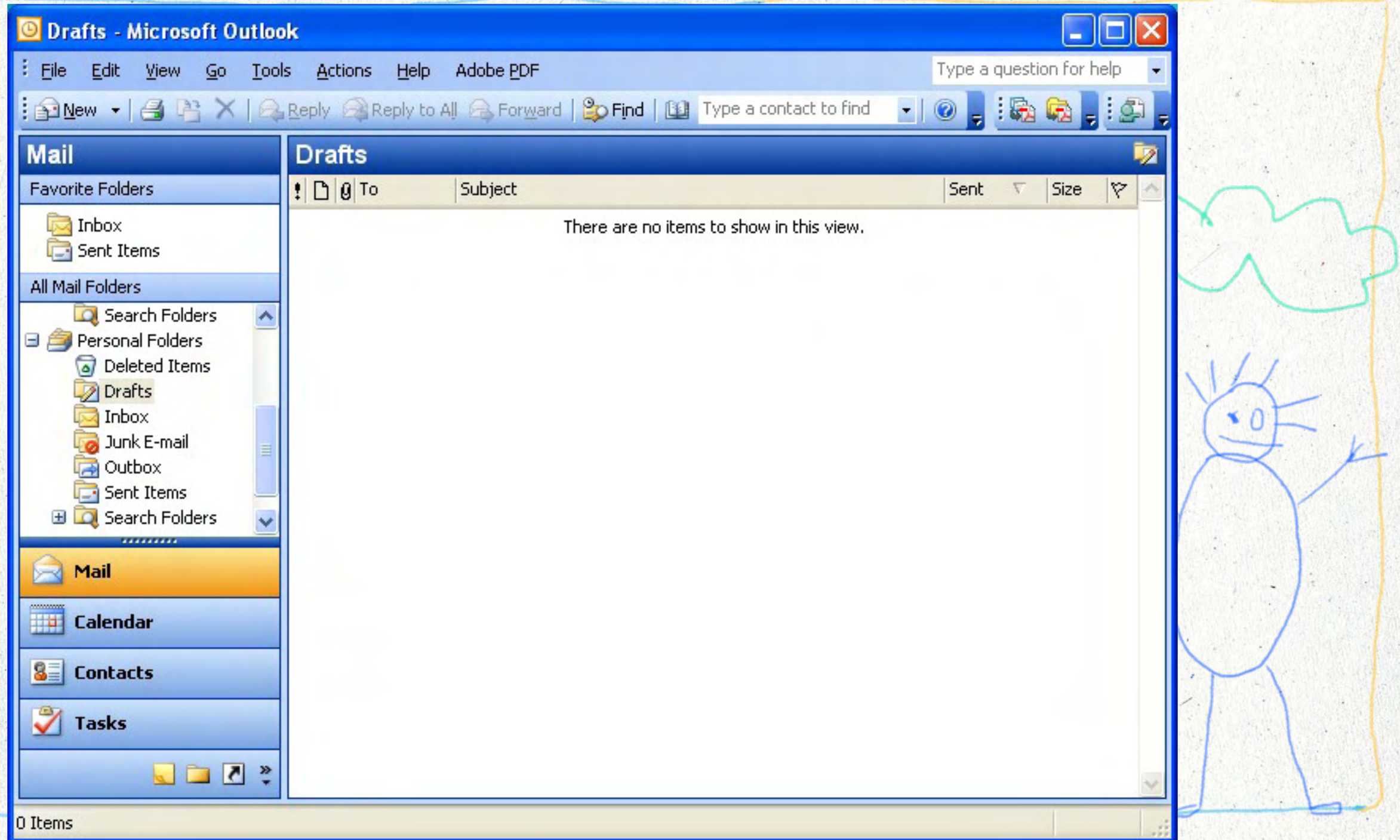


[redacted] - Recovered FilesAnywhere Information

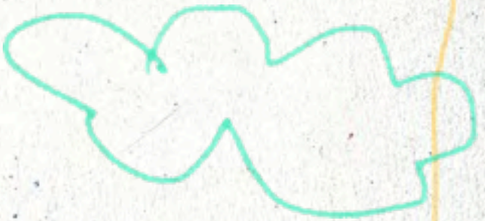
Timestamp (EDT)	Filename	Type	Destination Folder	Size
6/17/10 12:39:26 PM	Agents.xls	file	[redacted]\\	2,691,584
6/17/10 12:41:30 PM	0 - Generic flyer.doc	file	[redacted]\\New Reps\\	1,503,744
6/17/10 12:41:30 PM	ACCESSSORIAL CHARGE CHANGES.doc	file	[redacted]\\New Reps\\	58,880
6/17/10 12:41:30 PM	account review worksheet.xls	file	[redacted]\\New Reps\\	19,968
6/17/10 12:41:30 PM	ACI Codes Guide Training.doc	file	[redacted]\\New Reps\\	19,968
6/17/10 12:41:30 PM	ACI Codes.xls	file	[redacted]\\New Reps\\	15,872
6/17/10 12:41:30 PM	Adding venues.doc	file	[redacted]\\New Reps\\	78,848
6/17/10 12:41:30 PM	Adding venues.pdf	file	[redacted]\\New Reps\\	30,741
6/17/10 12:41:31 PM	Apples to apples.doc	file	[redacted]\\New Reps\\	25,600
6/17/10 12:41:36 PM	Carpet brochure.doc	file	[redacted]\\New Reps\\	2,338,816
6/17/10 12:41:36 PM	Carpet brochure.pdf	file	[redacted]\\New Reps\\	215,976
6/17/10 12:41:43 PM	Cases and Crates.doc	file	[redacted]\\New Reps\\	3,163,136
6/17/10 12:41:43 PM	Cases and Crates.pdf	file	[redacted]\\New Reps\\	241,206
6/17/10 12:41:44 PM	CC REQUEST FORM FORM 2010.doc	file	[redacted]\\New Reps\\	353,280
6/17/10 12:41:45 PM	CC REQUEST FORM FORM REVISED.doc	file	[redacted]\\New Reps\\	353,792
6/17/10 12:41:46 PM	Charges & Specials.doc	file	[redacted]\\New Reps\\	66,048
6/17/10 12:41:46 PM	Cold Call Tracker.pdf	file	[redacted]\\New Reps\\	5,219
6/17/10 12:41:46 PM	Cold Call Tracker.xls	file	[redacted]\\New Reps\\	15,872
6/17/10 12:41:46 PM	Cold calling inquisition.doc	file	[redacted]\\New Reps\\	25,600
6/17/10 12:41:46 PM	Cold calling tree.doc	file	[redacted]\\New Reps\\	32,768
6/17/10 12:41:46 PM	Cold calling tree.pdf	file	[redacted]\\New Reps\\	8,689
6/17/10 12:41:47 PM	Combo.doc	file	[redacted]\\New Reps\\	244,224
6/17/10 12:41:47 PM	Combo.pdf	file	[redacted]\\New Reps\\	49,134
6/17/10 12:41:47 PM	Conditions of Contract - rev 09-2007.pdf	file	[redacted]\\New Reps\\	25,611
6/17/10 12:41:47 PM	Conditions of Contract - rev 09-2007.pdf	file	[redacted]\\	25,611
6/17/10 12:41:47 PM	Conditions of Contract (rev 09-2007).doc	file	[redacted]\\	33,280
6/17/10 12:41:47 PM	Conditions of Contract (rev 09-2007).doc	file	[redacted]\\New Reps\\	33,280
6/17/10 12:41:47 PM	Convention Centers.xls	file	[redacted]\\	30,720
6/17/10 12:41:47 PM	Convention Centers.xls	file	[redacted]\\New Reps\\	30,720
6/17/10 12:41:48 PM	Credit Card Authorization, 03-29-10.doc	file	[redacted]\\	428,032
6/17/10 12:41:48 PM	Credit Card Authorization, 03-29-10.doc	file	[redacted]\\New Reps\\	428,032
6/17/10 12:41:48 PM	Customer service questionnaire.doc	file	[redacted]\\	29,184
6/17/10 12:41:48 PM	Customer service questionnaire.doc	file	[redacted]\\New Reps\\	29,184
6/17/10 12:41:54 PM	Display Pages Catalog.pdf	file	[redacted]\\	2,934,406
6/17/10 12:41:54 PM	Display Pages Catalog.pdf	file	[redacted]E\\New Reps\\	2,934,406
6/17/10 12:41:55 PM	Domestic Carriers rebuttals.xls	file	[redacted]\\	31,744
6/17/10 12:41:55 PM	Domestic Carriers rebuttals.xls	file	[redacted]\\New Reps\\	31,744
6/17/10 12:41:55 PM	Domestic Carriers.xls	file	[redacted]\\	54,272
6/17/10 12:41:55 PM	Domestic Carriers.xls	file	[redacted]\\New Reps\\	54,272
6/17/10 12:41:55 PM	Fax cover sheet.doc	file	[redacted]\\	165,888
6/17/10 12:41:55 PM	Fax cover sheet.doc	file	[redacted]\\New Reps\\	165,888
6/17/10 12:41:56 PM	Flyer template in header.doc	file	[redacted]\\	417,280

FAIL #5 - HIDING IN THE CLOUD

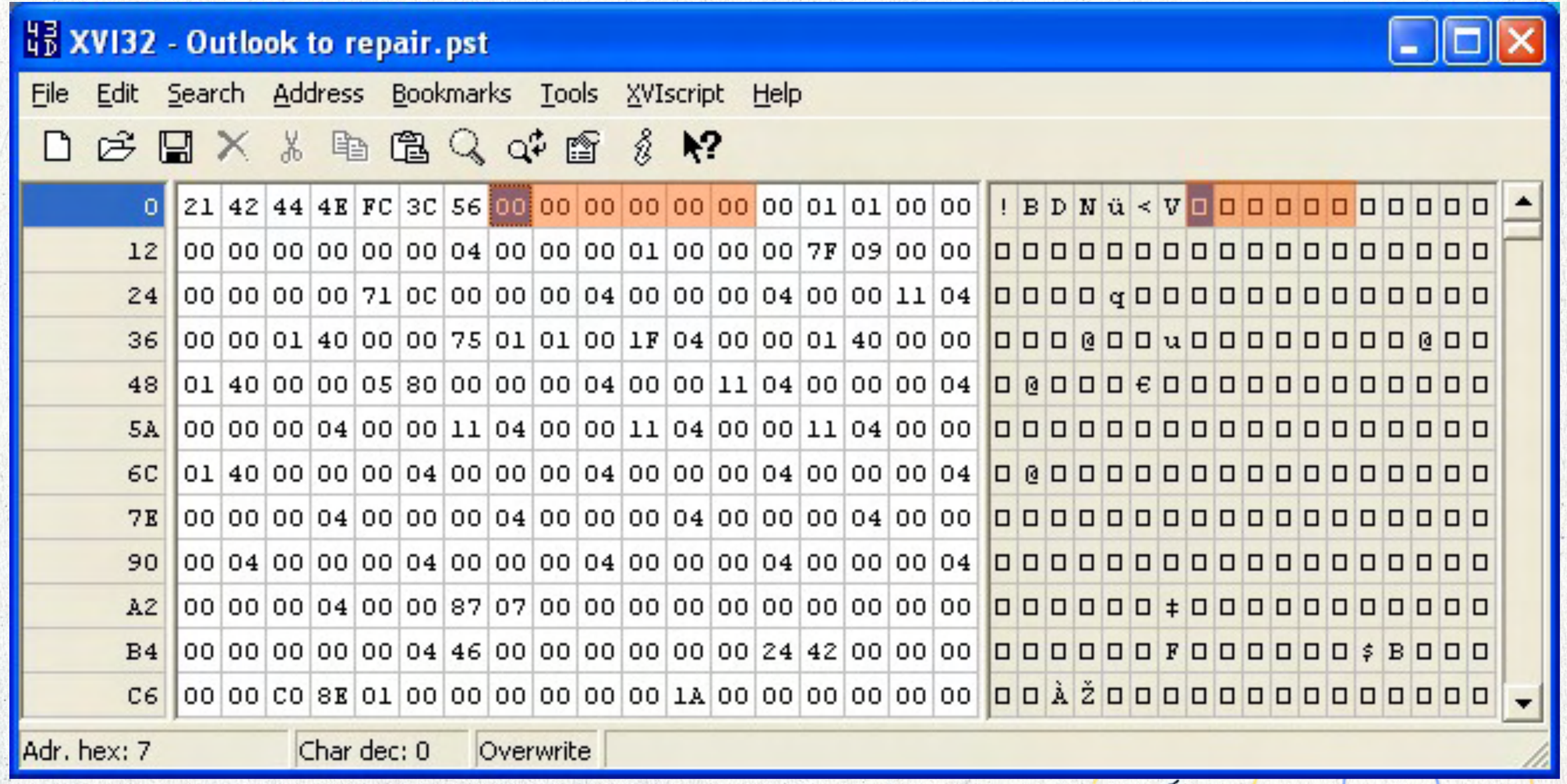
Opposing attorney handed us CD with an Outlook.PST

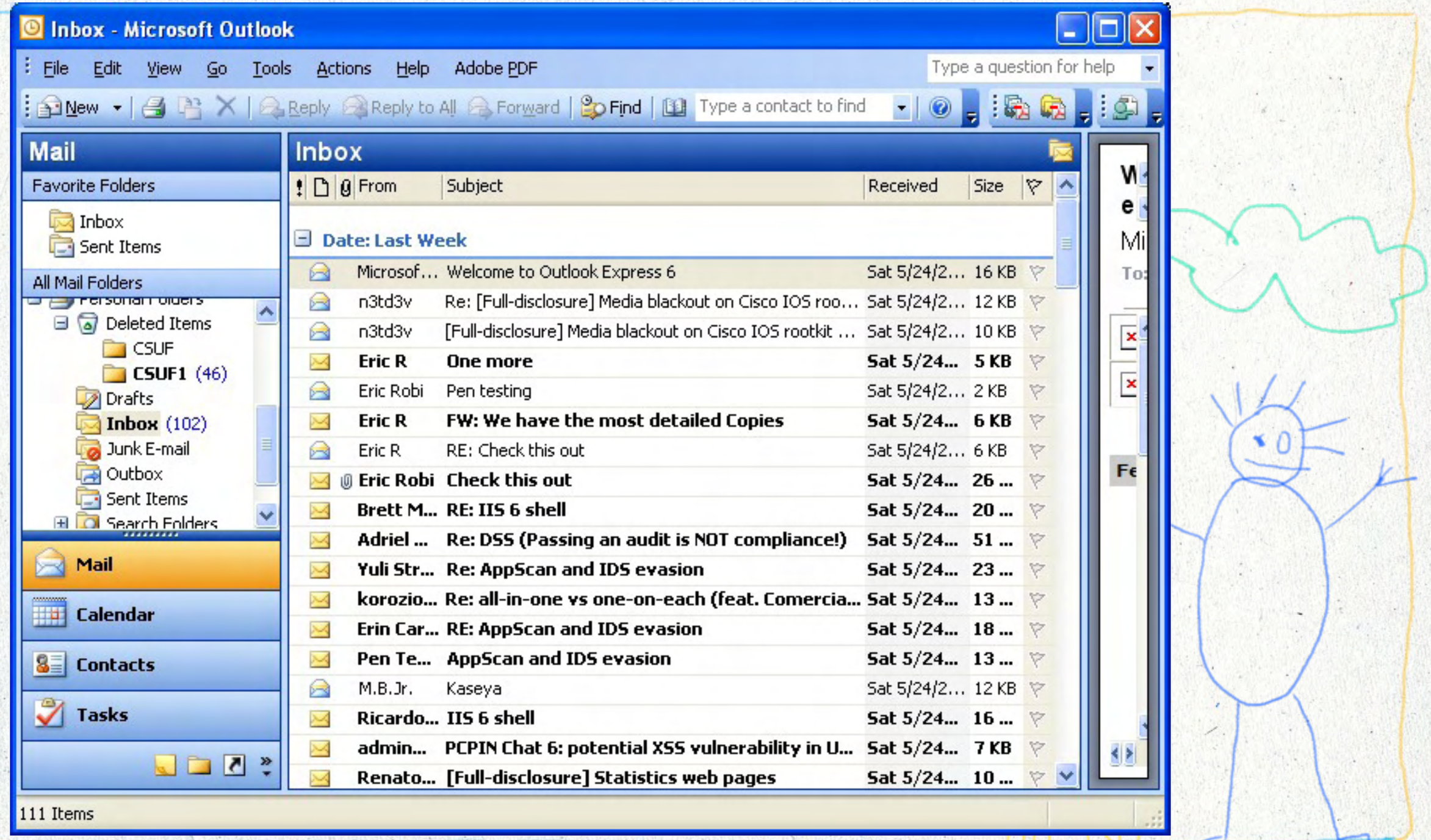

Drafts - Microsoft Outlook
File Edit View Go Tools Actions Help Adobe PDF
Type a question for help
New Reply Reply to All Forward Find Type a contact to find
Mail
Favorite Folders
Inbox
Sent Items
All Mail Folders
Search Folders
Personal Folders
Deleted Items
Drafts
Inbox
Junk E-mail
Outbox
Sent Items
Search Folders
Mail
Calendar
Contacts
Tasks
Drafts
To Subject Sent Size
There are no items to show in this view.
0 Items

FAIL #5 - HIDING IN THE CLOUD



First thing we do is search for deleted emails


XVI32 - Outlook to repair.pst
File Edit Search Address Bookmarks Tools XVIscript Help
0 21 42 44 4E FC 3C 56 00 00 00 00 00 00 00 01 01 00 00
12 00 00 00 00 00 00 04 00 00 00 01 00 00 00 7F 09 00 00
24 00 00 00 00 71 0C 00 00 00 04 00 00 00 04 00 00 11 04
36 00 00 01 40 00 00 75 01 01 00 1F 04 00 00 01 40 00 00
48 01 40 00 00 05 80 00 00 00 04 00 00 11 04 00 00 00 04
5A 00 00 00 04 00 00 11 04 00 00 11 04 00 00 11 04 00 00
6C 01 40 00 00 00 04 00 00 00 04 00 00 00 04 00 00 00 04
7E 00 00 00 04 00 00 00 04 00 00 00 04 00 00 00 04 00 00
90 00 04 00 00 00 04 00 00 00 04 00 00 00 04 00 00 00 04
A2 00 00 00 04 00 00 87 07 00 00 00 00 00 00 00 00 00 00
B4 00 00 00 00 00 04 46 00 00 00 00 00 00 24 42 00 00 00
C6 00 00 C0 8E 01 00 00 00 00 00 00 1A 00 00 00 00 00 00
Adr. hex: 7
Char dec: 0
Overwrite


Inbox - Microsoft Outlook
File Edit View Go Tools Actions Help Adobe PDF
Type a question for help
New Reply Reply to All Forward Find Type a contact to find
Mail
Favorite Folders
Inbox
Sent Items
All Mail Folders
Deleted Items
CSUF
CSUF1 (46)
Drafts
Inbox (102)
Junk E-mail
Outbox
Sent Items
Search Folders
Mail
Calendar
Contacts
Tasks
Inbox
From Subject Received Size
Date: Last Week
Microsof... Welcome to Outlook Express 6 Sat 5/24/2... 16 KB
n3td3v Re: [Full-disclosure] Media blackout on Cisco IOS roo... Sat 5/24/2... 12 KB
n3td3v [Full-disclosure] Media blackout on Cisco IOS rootkit ... Sat 5/24/2... 10 KB
Eric R One more Sat 5/24... 5 KB
Eric Robi Pen testing Sat 5/24/2... 2 KB
Eric R FW: We have the most detailed Copies Sat 5/24... 6 KB
Eric R RE: Check this out Sat 5/24/2... 6 KB
Eric Robi Check this out Sat 5/24... 26 ...
Brett M... RE: IIS 6 shell Sat 5/24... 20 ...
Adriel ... Re: DSS (Passing an audit is NOT compliance!) Sat 5/24... 51 ...
Yuli Str... Re: AppScan and IDS evasion Sat 5/24... 23 ...
korozio... Re: all-in-one vs one-on-each (feat. Comercia... Sat 5/24... 13 ...
Erin Car... RE: AppScan and IDS evasion Sat 5/24... 18 ...
Pen Te... AppScan and IDS evasion Sat 5/24... 13 ...
M.B.Jr. Kaseya Sat 5/24/2... 12 KB
Ricardo... IIS 6 shell Sat 5/24... 16 ...
admin... PCPIN Chat 6: potential XSS vulnerability in U... Sat 5/24... 7 KB
Renato... [Full-disclosure] Statistics web pages Sat 5/24... 10 ...
111 Items

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

User Retard Level

18

Punishment Level

10

$ Distress Caused

8

Bonus Points

15

51

Huge lawsuit

$3.5M in fees and damages

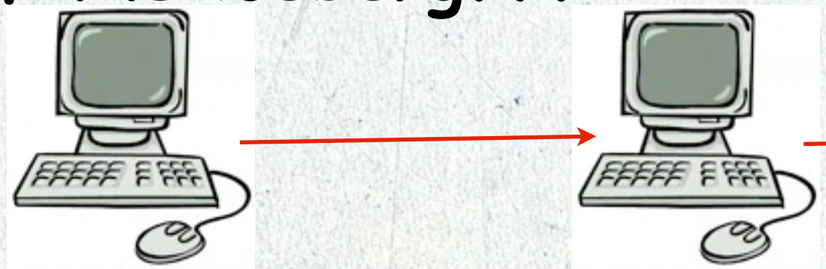
Attorney may lose his license

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

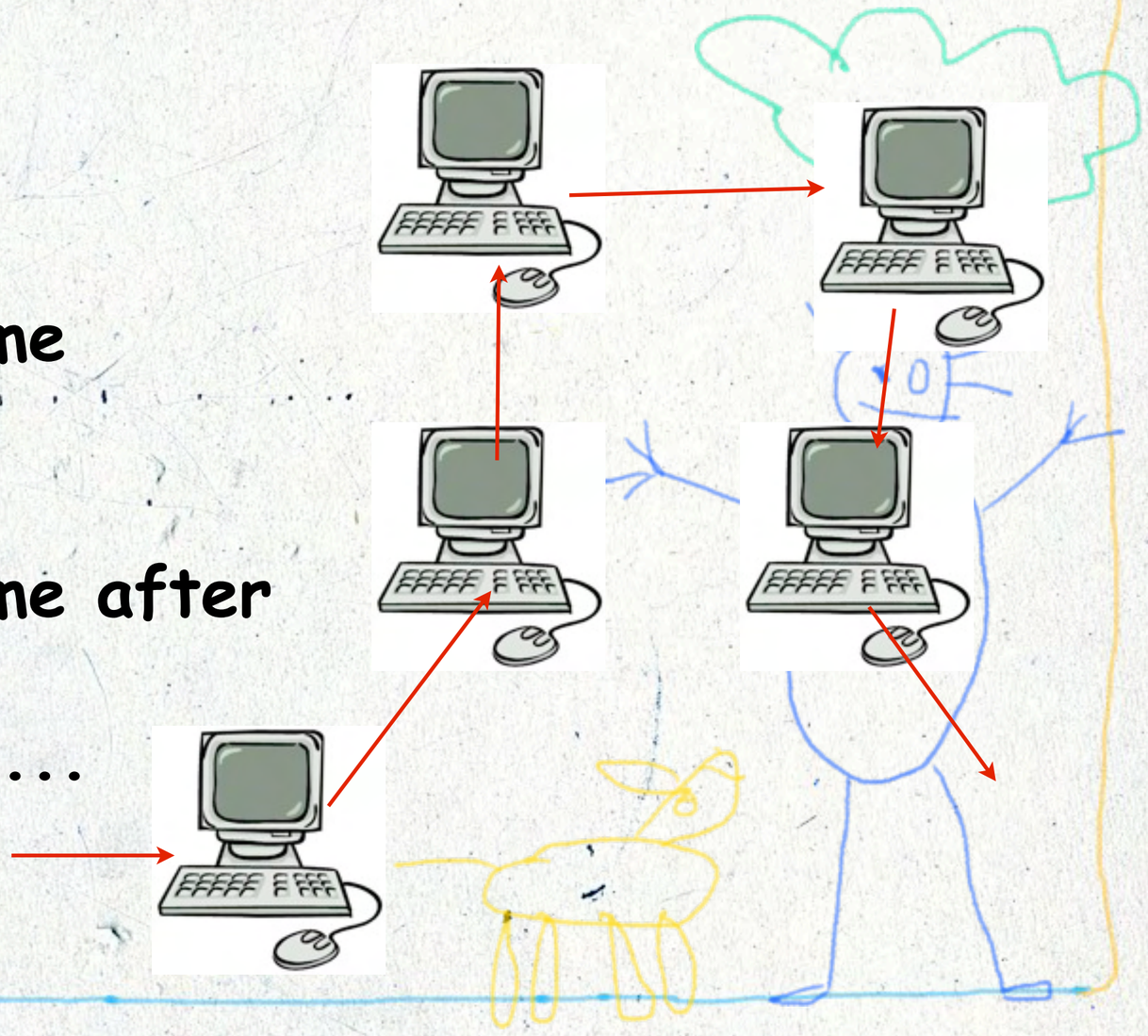
FAIL #6 - The RDP Bounce

- 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...

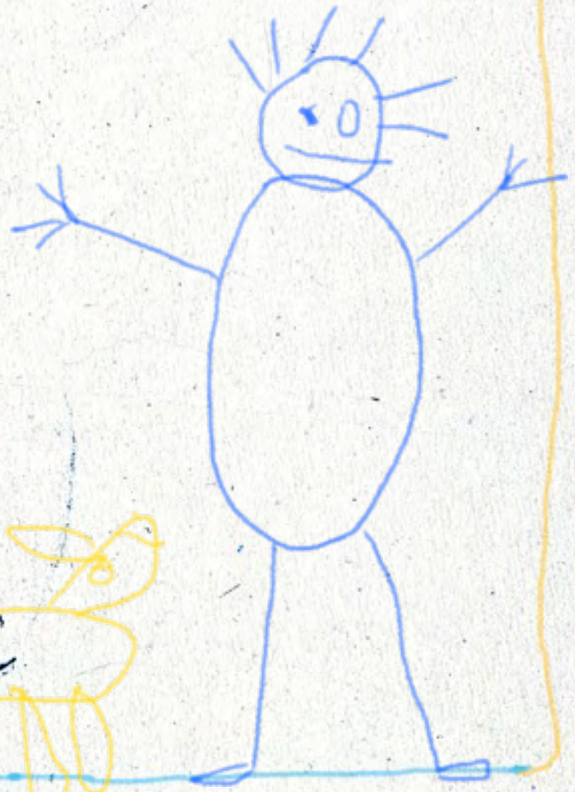


FAIL #6 - The RDP Bounce

- 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]

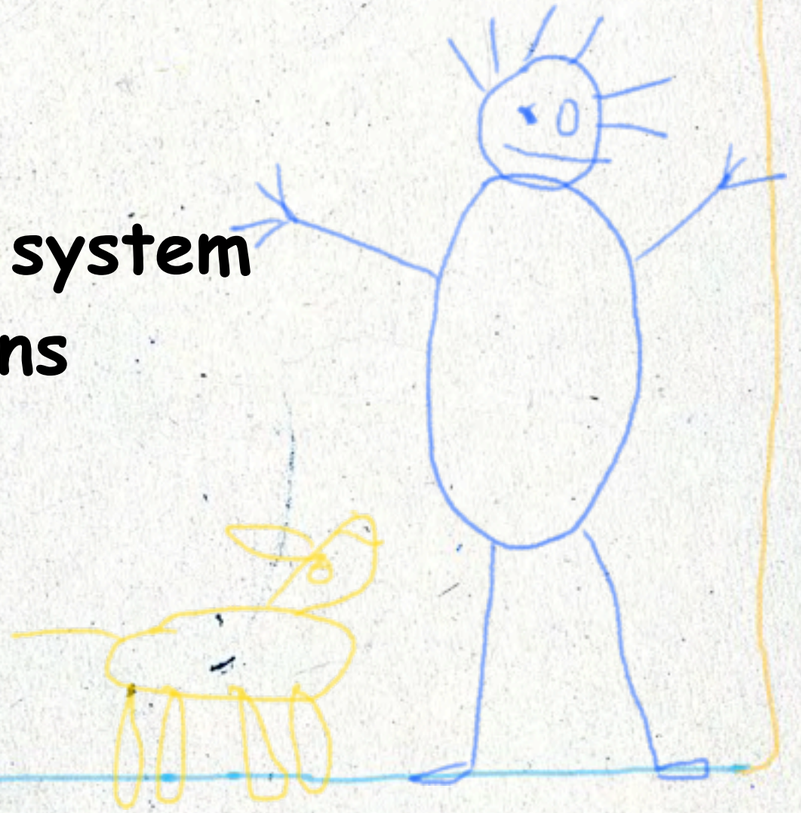
Credit: http://www.neatorama.com/2009/04/09/massive-old-school-printers/

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



Fail Matrix

User Retard Level

20

Punishment Level

15

$ Distress Caused

8

Bonus Points

20

Lost job

63

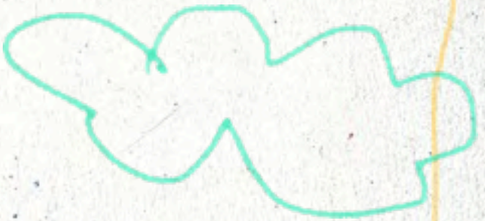
Loss of income, no reference

Do some research!

FAIL #7 - EPIC PORNO FAIL

- 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 FAIL

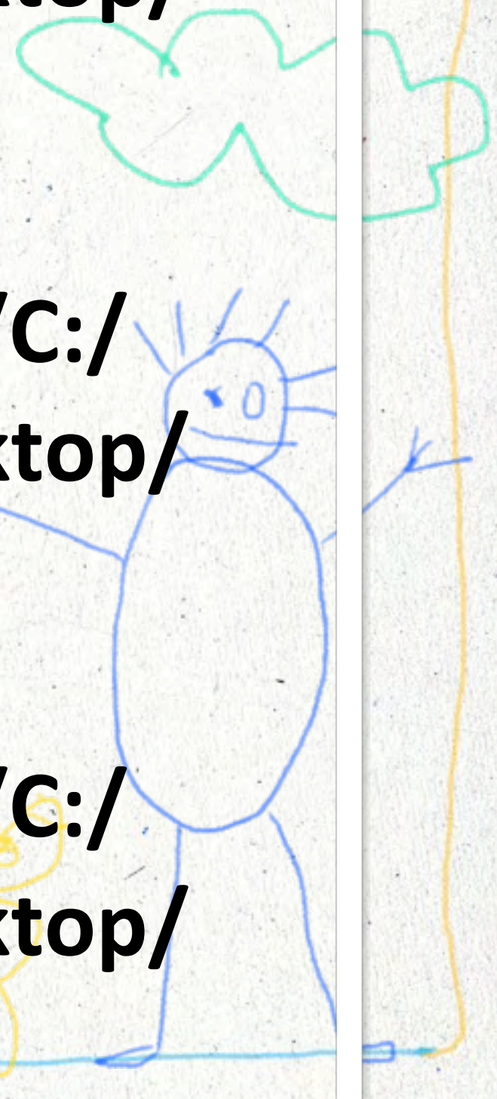
- Allegation #1
- Edgar downloaded illegal porn
- Notable thing: Edgar left his house in April 2012

IE History

File 06/29/2012 11:29:06 Fri SUSPECT file:///C:/Documents%20and%20Settings/SUSPECT/Desktop/DUDE%20profile%20-%20Naughty%20File1.jpg

File 07/25/2012 16:41:24 Wed SUSPECT file:///C:/Documents%20and%20Settings/SUSPECT/Desktop/DUDE%20profile%20-%20Naughty%20File2.jpg

File 07/25/2012 16:42:17 Wed SUSPECT file:///C:/Documents%20and%20Settings/SUSPECT/Desktop/DUDE%20profile%20-%20Naughty%20File3.jpg



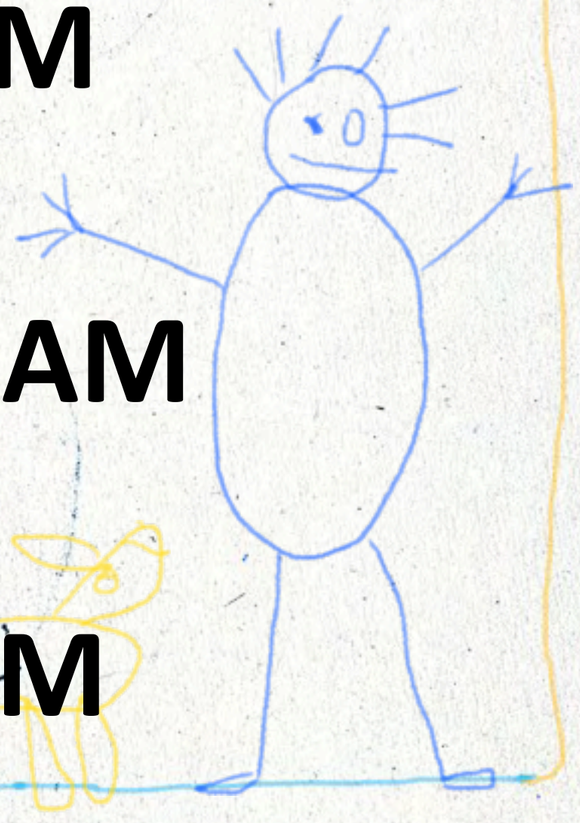
P2P Software - Download folder

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



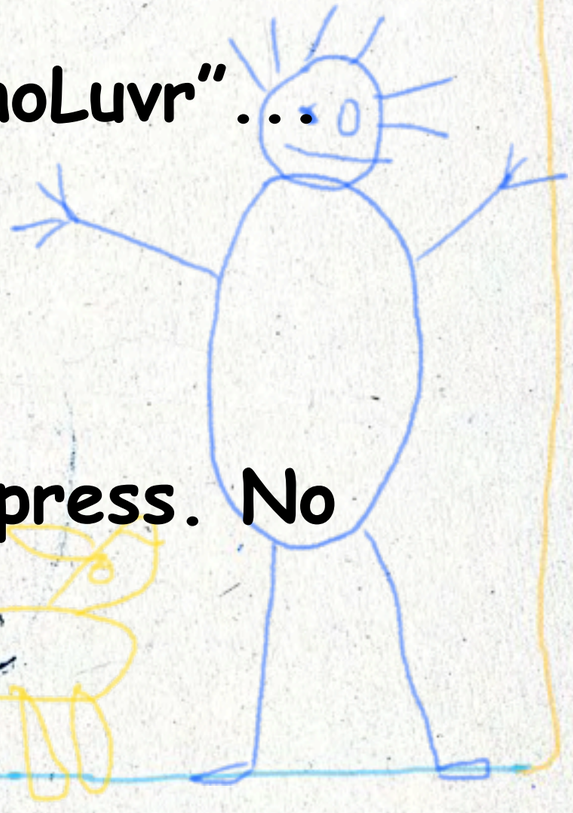
FAIL #7 - EPIC PORNO FAIL

Allegation #2

Edgar used Outlook Express to download porn

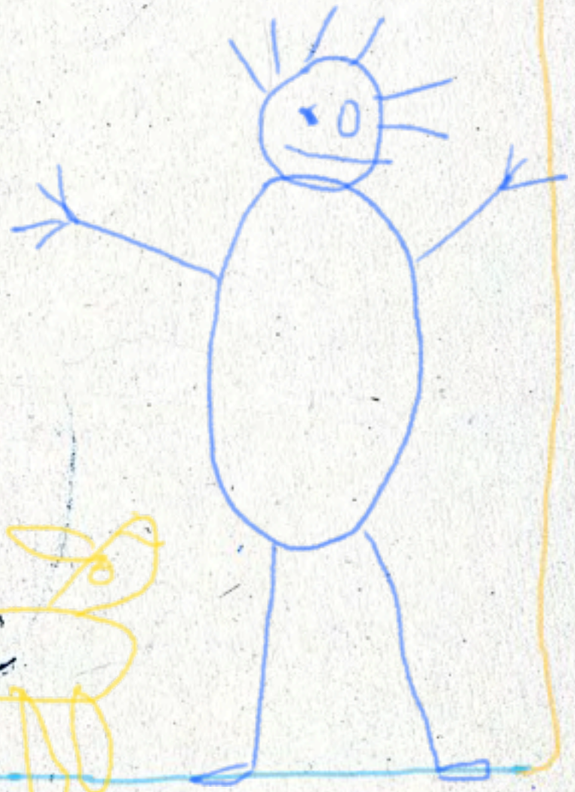
FAIL #7 - EPIC PORNO FAIL

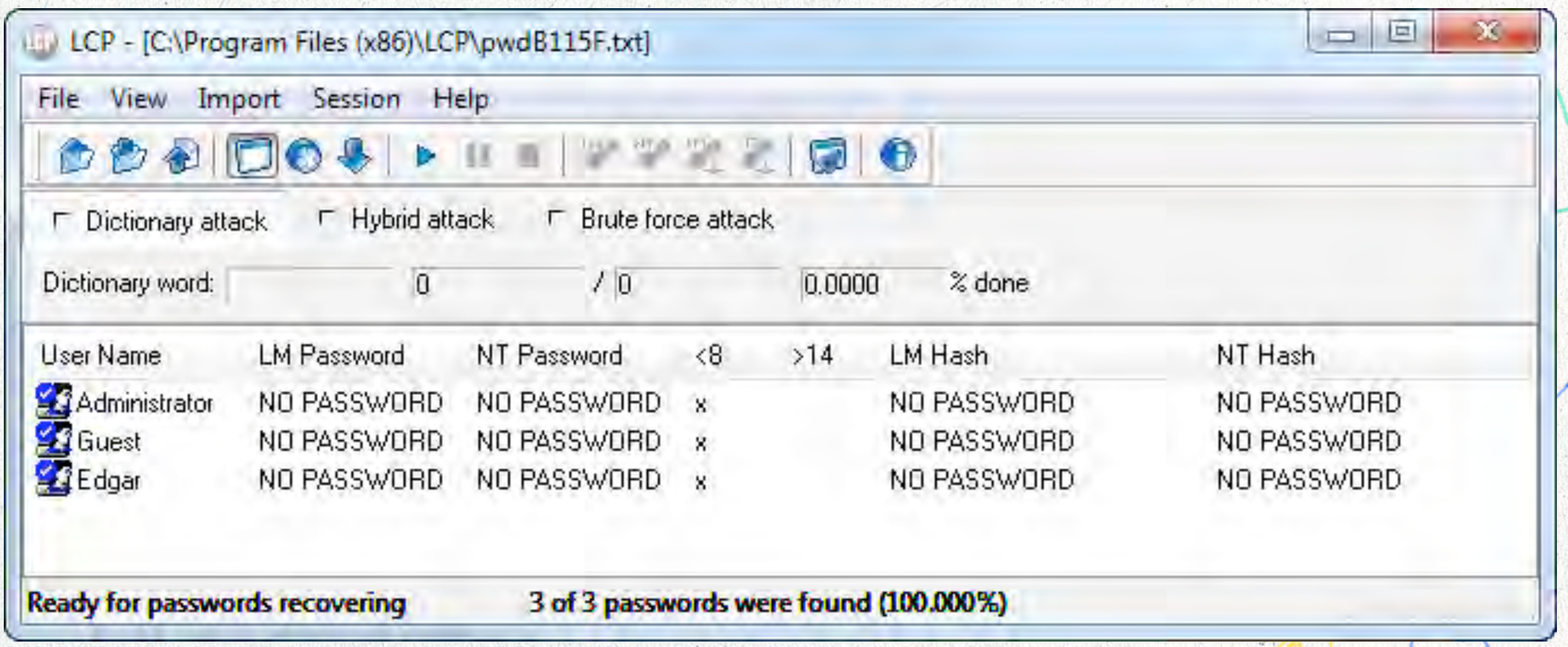
- In reality:
  - Outlook Express set up with account "PornoLuvr"...
  - **AFTER** Edgar moved out of his house
  - Only **headers** downloaded in Outlook Express. No content. No photos! (Just file names).



FAIL #7 - EPIC PORNO FAIL

- Allegation #3
  - Edgar's user account had a password
  - Inference is that only Edgar had access



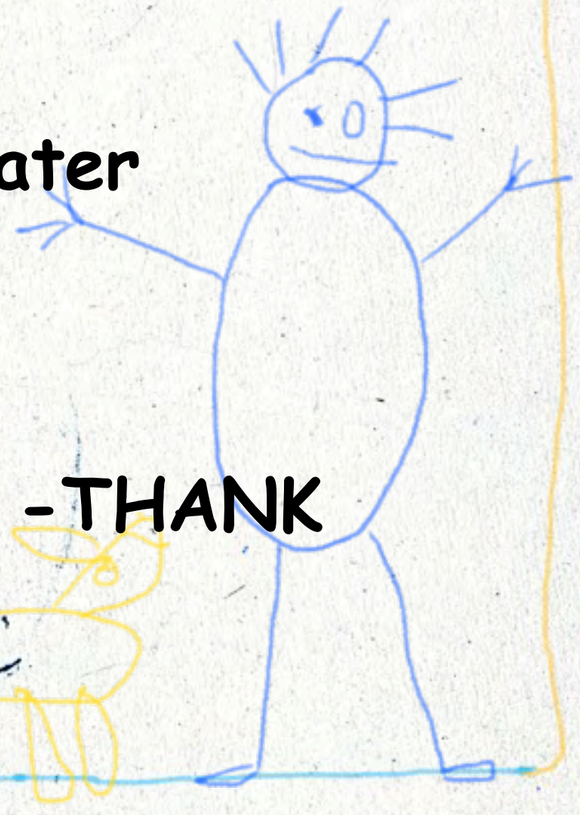

LCP - [C:\Program Files (x86)\LCP\pwdB115F.txt]
File View Import Session Help
Dictionary attack
Hybrid attack
Brute force attack
Dictionary word:
0
/ 0
0.0000
% done
User Name
LM Password
NT Password
<8
>14
LM Hash
NT Hash
Administrator
NO PASSWORD
NO PASSWORD
x
NO PASSWORD
NO PASSWORD
Guest
NO PASSWORD
NO PASSWORD
x
NO PASSWORD
NO PASSWORD
Edgar
NO PASSWORD
NO PASSWORD
x
NO PASSWORD
NO PASSWORD
Ready for passwords recovering
3 of 3 passwords were found (100.000%)

FAIL #7 - EPIC PORNO FAIL

- More facts (undiscovered by examiner)
- P2P client used to download porn...
- Into a new user account
- AFTER Edgar moved out of the house

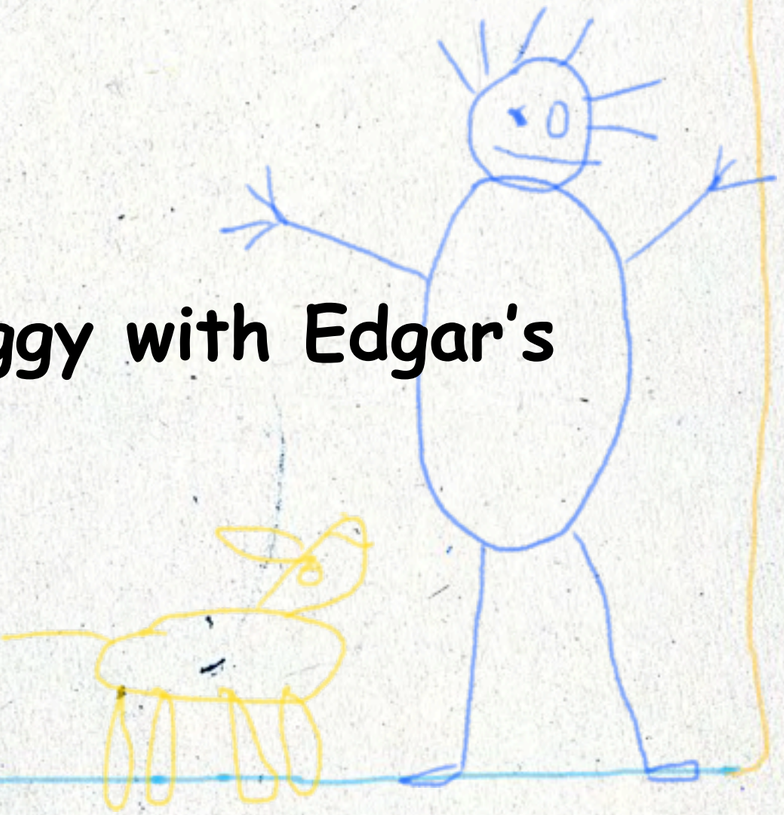
FAIL #7 - EPIC PORNO FAIL

- 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