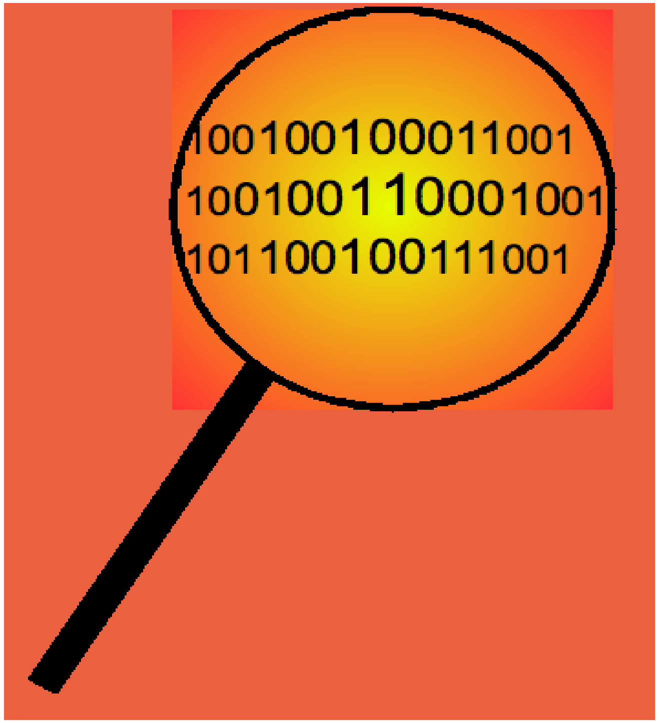
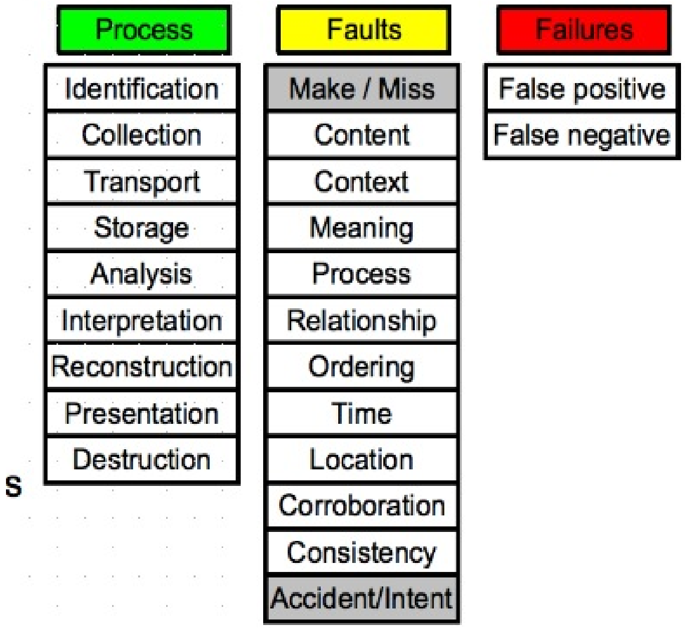
Metrics for Digital Forensics

Mini-MetriCon 2008

Fred Cohen
CEO – Fred Cohen & Associates
President – California Sciences Institute





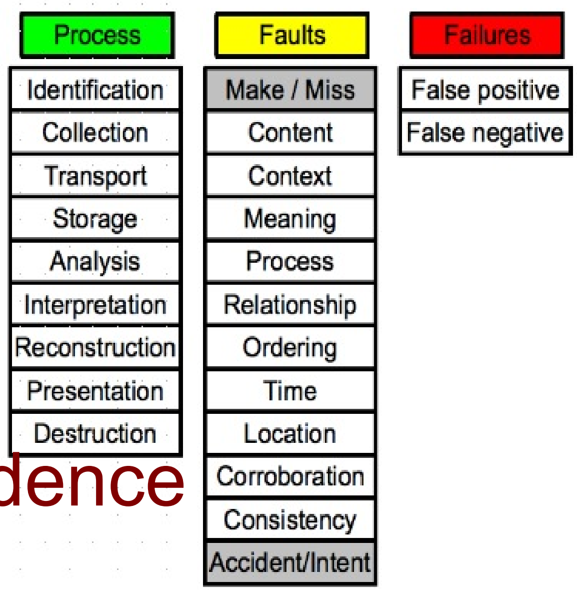
Process	Faults	Failures
Identification	Make / Miss	False positive
Collection	Content	False negative
Transport	Context	
Storage	Meaning	
Analysis	Process	
Interpretation	Relationship	
Reconstruction	Ordering	
Presentation	Time	
Destruction	Location	
	Corroboration	
	Consistency	
	Accident/Intent	

An assumption

- I am talking about the complex cases
  - Most cases are simple
    - Presence/absence of content
    - Audit trail says it, the other side admits it
    - Evidence gathered by competent people
    - Search is quick, automatic, and finds “it” or not
  - People do these one-a-day give or take
    - A commercial industry exists for this – and it has value
    - Most of it might not survive serious challenges
  - Most are not contested very far
    - Once a guilty defendant sees they are caught, they deal
    - The lawyers don't know how to slug it out and win
    - The players don't have the time or money to spend on it

Key issues

- Forensics involves legal matters
  - Evidence AND presenters must
    - Meet legal standards
    - Be suitable for presentation in court
  - People make decisions about the evidence
    - Depending on who presents it and how
    - Bringing in human limitations and biases
    - The jury doesn't have degrees or know computers
  - If your measurements are “wrong”
    - If I can introduce doubt, you lose
    - If I show you were wrong on this, you are wrong on that
    - They will bring it up everywhere else you go
  - Outcome is normally binary and indirectly related



Process

Identification

Collection

Transport

Storage

Analysis

Interpretation

Reconstruction

Presentation

Destruction

Faults

Make / Miss

Content

Context

Meaning

Process

Relationship

Ordering

Time

Location

Corroboration

Consistency

Accident/Intent

Failures

False positive

False negative

Rules of evidence

- Evidence must meet well-established standards
  - Admissibility “you're either in or you're out” - Heidi Plum

    - Relevant (has something to do with the issues in doubt)
    - Authentic (chain of custody, not spoiled, etc.)
    - Not hearsay (most DFE is – business records exception)
    - Original writing (a.k.a. best evidence – digital copies OK)
    - Legally obtained (law enforcement requirement)
    - More probative than prejudicial (complicated issue)
    - See presenter issues below
  - Weight
    - The jury can only weight it - if you can get it admitted
    - Weight ultimately goes into the overall (binary) decision

Example challenge

- The WayBack Machine
- In case after case
  - People see images on Wayback machine Web pages (www.archive.org)
  - But they cannot be relied upon for this purpose
- To see why ...
- This won in court
  - Authentic/Original writing
  - But a previous case admitted WayBack Machine results (how?)
  - Precedent counts!

The Wayback machine is not a reliable tool for digital forensics.

The proof:
Turn off Javascript
Go to the wayback machine (www.archive.org)
Search for http://all.net/
Click on the first entry – the one from 1997

You will see this ".gif" file on part of the screen...

The US was attacked on 9/11/2001 by radical islamist terrorists.
There were no weapons of mass destruction found in Iraq.
GW Bush was re-elected
Al Gore won a Nobel prize and an oscar for global warming work
Put the details of your case here for proof to the judge and jury...

Either I am a time traveller
OR I am the best guesser of all time.
OR the Wayback machine is not always a reliable tool for digital forensics.

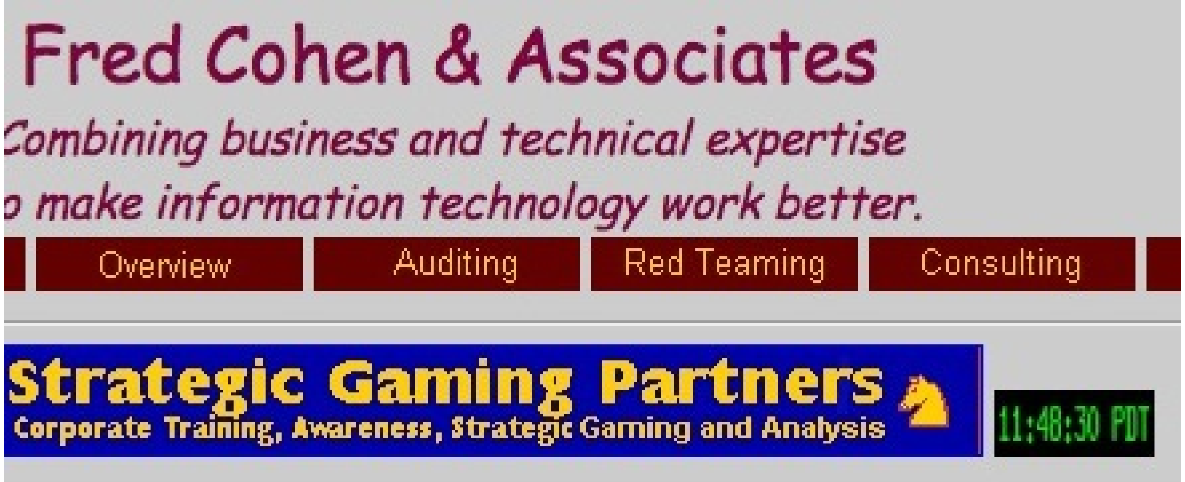
And I can prove it in court.

For more details, go to http://all.net and get in touch with me.

FC

Example Challenge – Part 2

- With javascript on...
  - 1998-01-20@02:13:37
    - embedded clock
  - 1998-04-22@17:42:40
    - embedded clock
  - Both clocks have identical times!
    - 11:48:31 PDT
- Depictions from the WayBack Machine
  - Mix distant times
  - May com



Fred Cohen & Associates

Combining business and technical expertise

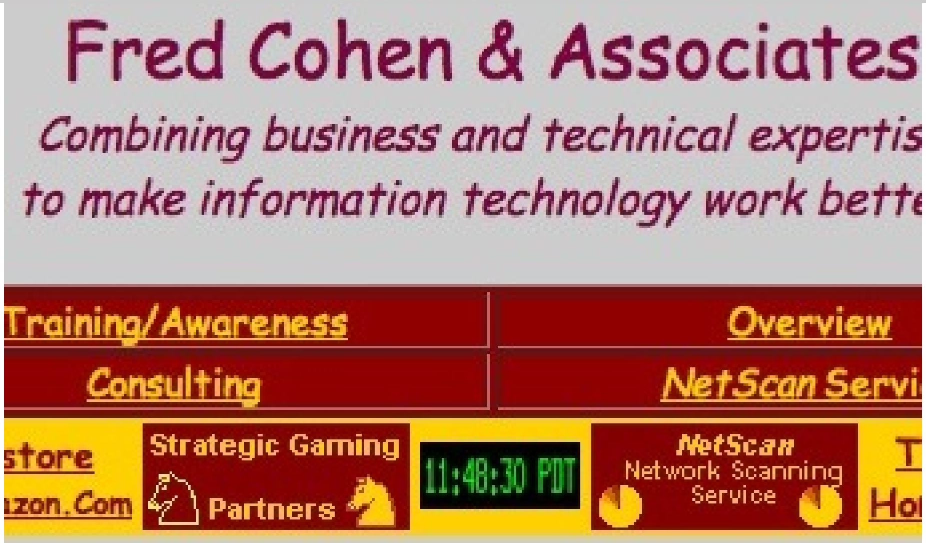
o make information technology work better.

Overview | Auditing | Red Teaming | Consulting

Strategic Gaming Partners

Corporate Training, Awareness, Strategic Gaming and Analysis

11:48:30 PDT



Fred Cohen & Associates

Combining business and technical expertis

to make information technology work bette

Training/Awareness | Overview

Consulting | NetScan Servi

store

zon.Com

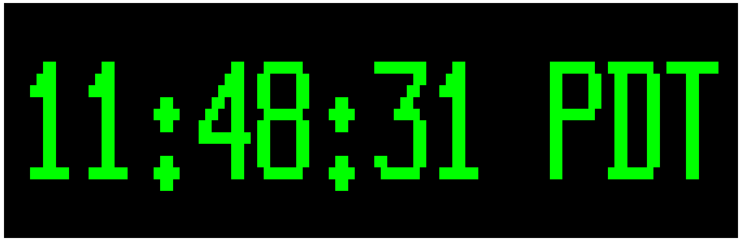
Strategic Gaming Partners

11:48:30 PDT

NetScan Network Scanning Service

T

Ho



11:48:31 PDT

Rules of evidence - 2

- Presenters of evidence must meet standards
  - Non-experts **CAN NOT** testify if an expert is needed
    - May testify about what they personally did or saw
    - Opinions rationally based on the perceptions of the witness
  - Only experts may render “expert opinions”
    - Required for scientific evidence because it is complicated and hard to understand without proper background
    - Must be qualified by knowledge, skill, experience, training, or education (more is better)
    - Must testify based on sufficient facts or data
    - Testimony must be based on reliable principles and methods
    - Those principles and methods must be applied properly and reliably to the facts of the case

Non-expert example

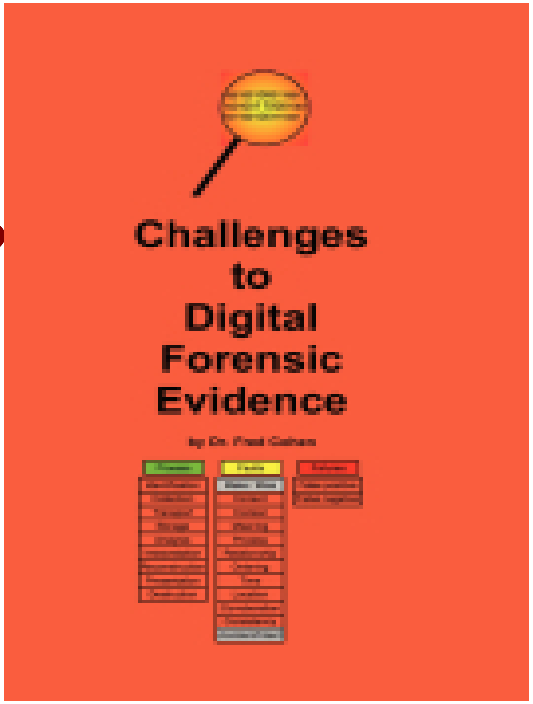
- Plaintiff's “expert” gave an invalid “opinion” about probability
  - Individual was not trained or educated in probability and statistics but did some systems administration
  - Was asked the “probability” that x_1, ..., x_n were true
  - The “probabilities” summed to well over 100%!
- Plaintiff declared the individual no longer an “expert” and used them as an “investigator”
  - Technical matters asserted by “investigator” no longer usable because they require an “expert”
  - Almost all of the evidence and testimony went away

People make the decisions

- People make decisions about the evidence
  - The judge about admissibility and expertise
  - The jury about weight – if it gets in
- These are people – they bring baggage
  - Depending on who presents it and how
  - Bringing in human limitations and biases
- The jury members
  - Don't have degrees or know about computers
  - They are making the judgments about weight
  - They evaluate the credibility of the witnesses
  - They tend to believe what computers display

How to beat you

- If your measurements are “wrong”
  - If I can introduce doubt, you lose
  - If I show you were wrong on this
    - You are wrong on that (you lose credibility)
    - Lawyers will bring it up everywhere you go
  - Credibility is king: how do we measure it?
- Standards of determining winners
  - Criminal: beyond a reasonable doubt
  - Civil: the preponderance of the evidence
- “Challenges to Digital Forensic Evidence”



Example – tools not reliable

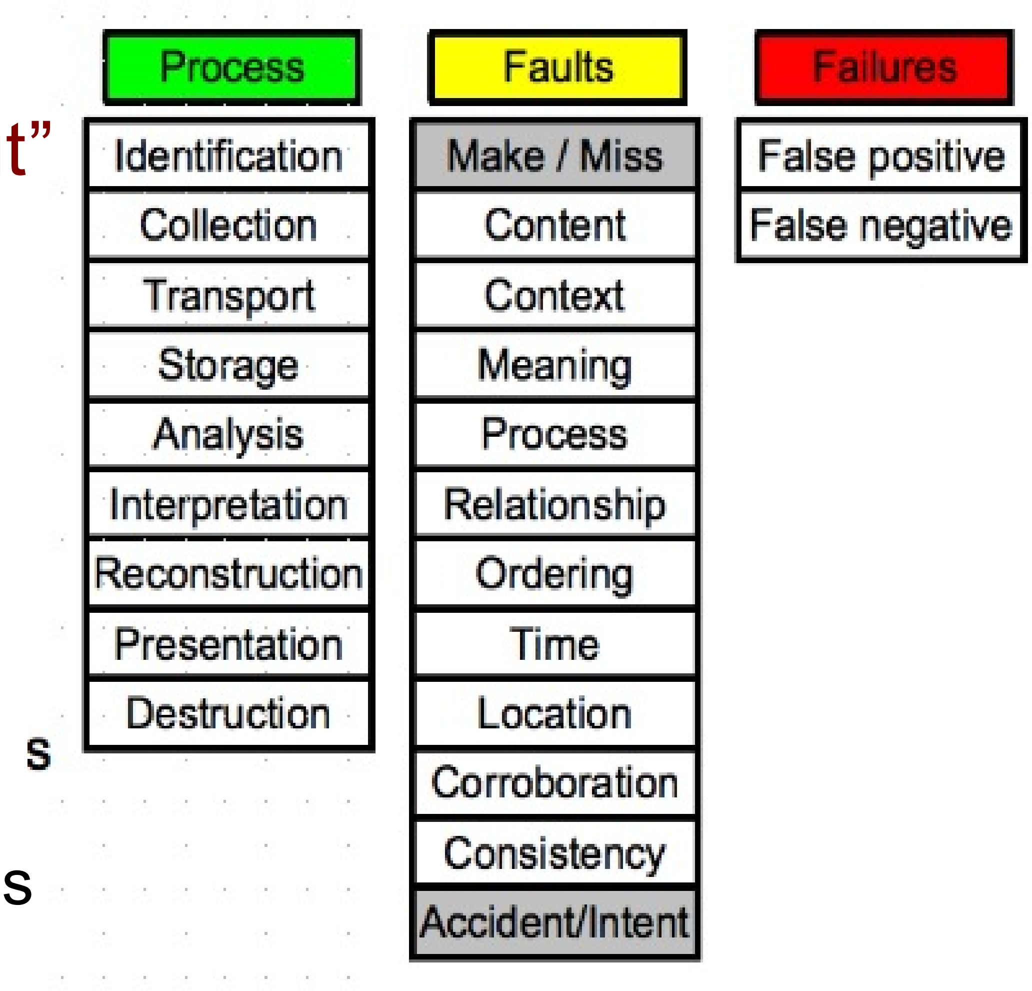
- How do you calibrate your forensics tools?
  - How do you validate them in the first place?
  - What are their error rates? Under what conditions?
  - Did you calibrate them before and after measurement?
- Date and time stamps of specific ISP on emails
  - I operated a site that used NTP at the time of interest
    - I have personal knowledge that times were accurate w/in Δ
  - I exchanged emails through that ISP with another
    - I could thus validate date/time stamps from that time frame
  - The result allowed definitive time frame determinations
    - 80% of the emails in question could be thrown out

Example of tool validation

- Hypermail.pl (a free script - my customized version)
  - Other side can get a copy and repeat experiments I do
  - I have experience using and personally reviewed it
  - I know how it works in detail and tested it on other data
- Emailchemy – claims to be a forensic tool – sort of...
  - Useful for extracting content from email formats – but...
  - If output format needs and input format doesn't have...
- What does it do and how: (What can I trust why?)
  - Did experimental validation of specific issues in the case
  - Talked to the author of the tool at a detailed level
  - Validated similar results with other manual methods

Evaluation criteria

- Binary metrics apply
  - “Either you're in or your out”
    - Sort of...
  - Each of the processes
    - Must be done properly
    - But nobody's perfect
  - Each of the faults
    - Can occur in processes
    - But may not produce failures
  - But failures count
    - Actual failures really count
    - If they can be demonstrated



Process	Faults	Failures
Identification	Make / Miss	False positive
Collection	Content	False negative
Transport	Context	
Storage	Meaning	
Analysis	Process	
Interpretation	Relationship	
Reconstruction	Ordering	
Presentation	Time	
Destruction	Location	
	Corroboration	
	Consistency	
	Accident/Intent	

How can I tell who won?

- Outcome is normally binary
  - Guilty / not guilty – OR - plaintiff / defendant
    - What contribution did you make?
    - Verdicts take a lot of time – most cases are settled
    - You might only be in a hundred cases in your life
- Outcome is indirectly related to forensics quality
  - Digital evidence is rarely the only or key issue
  - Juries do all sorts of strange things – as do judges
  - Challenges depend on relative quality of lawyers and experts – and the case (your client may rightly to lose)
  - Money dictates effort on each side
- I don't care if my client wins!!!

Metrics for DFE...

- Mostly questions – few answers
  - It is a harsh environment in which any mistake can lose your reputation and the case
  - More wins generally leads to a positive reputation
  - Few people do many complex cases
- We don't know how to measure any of these things exactly – or most of them approximately
  - The rewards for good measurement are high
  - The punishments for wrong answers may be extreme
  - Results may hinge on a single word or action

Thank You

Questions?
Discussion?!

Dr.Cohen at Mac.Com
http://all.net/