Challenges to DFE

Computer Forensics Show – Oct 6, 2009

Dr. Fred Cohen
President - California Sciences Institute
CEO – Fred Cohen & Associates

Outline

- Background of the speaker and subject
- The Big Picture
- Process elements, faults, and failures
- Detailing the faults
- Analysis of failures
- Presenting challenges
- Overcoming challenges
- Questions / Comments?

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	

Your speaker

- Education:
  - B.S. Electrical Engineering (C-MU '77)
  - M.S. Information Science (Pitt '81)
  - Ph.D. Electrical Engineering (USC '86)
- Experience:
  - >30 years of information protection R&D, design, engineering, testing, implementation, and operation
  - >20 years since first digital forensics case
- CEO - Fred Cohen & Associates
  - Enterprise information protection architecture
  - Digital forensics for high-valued legal cases

CalSci

- President – California Sciences Institute
  - Starting doctoral classes in 2009-2010
- M.S. And Ph.D. Program in National Security
  - Technical aspects of these fields
- M.S. In Advanced Investigation
- Ph.D. In Digital Forensics
  - The first Ph.D. program in Digital Forensics in the United States
- calsci.org

What does he know about the subject?

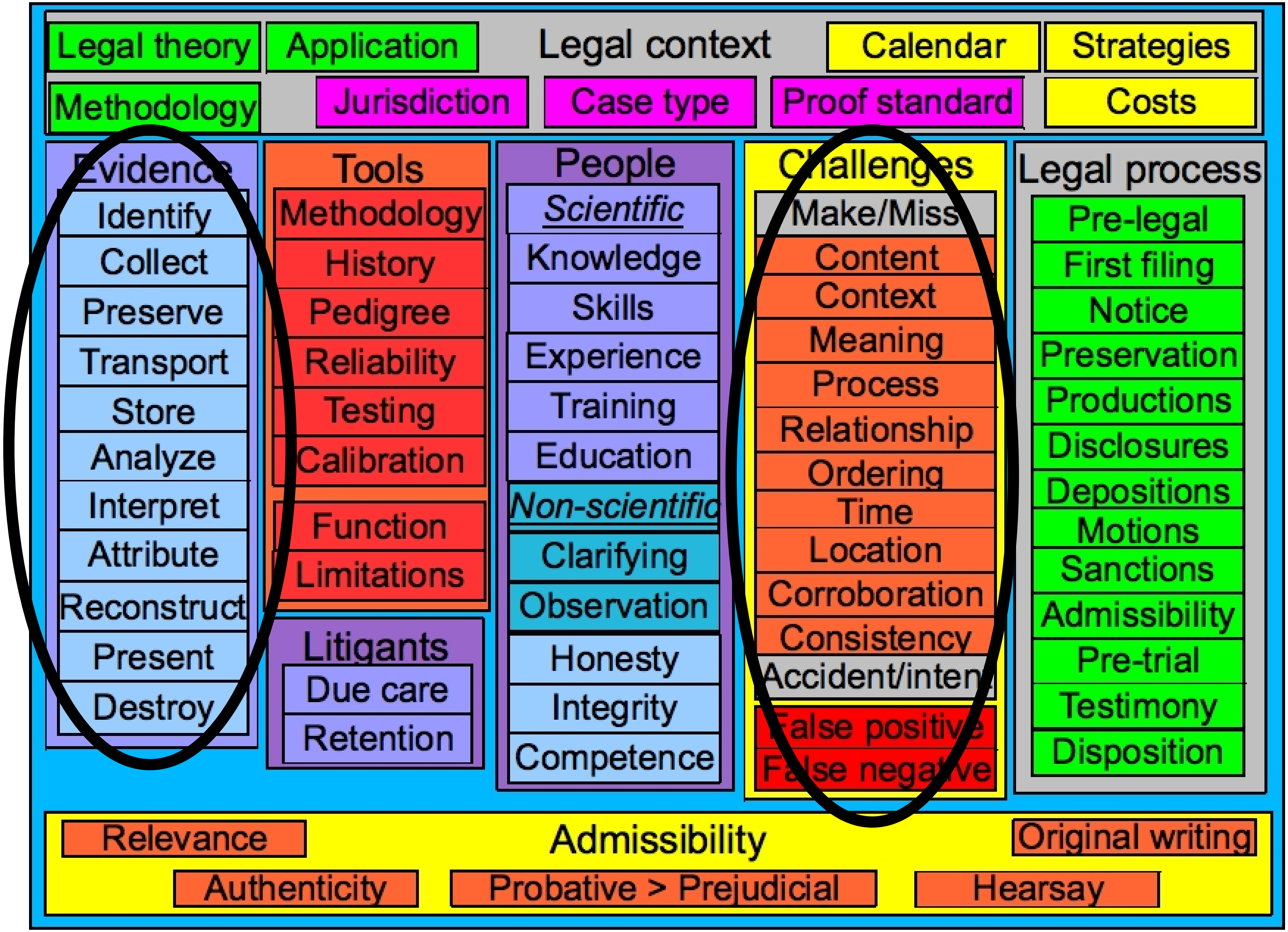
- Knowledge, skill, experience, training, or education
  - Federal Rules of Evidence 701-706
- Knowledge, Skills, and Experience:
  - POST certified trainer in these areas, admitted to testify as an expert in Federal, State, and Local Criminal and Civil digital forensics matters, published refereed and other articles on the subject, authored a book on the subject and another book closely related to it, taught at Federal Law Enforcement Training Center in this area, taught graduate classes at University of New Haven in this area, etc.
- Education:
  - B.S., M.S., and Ph.D. in relevant field

Outline

- Background of the speaker and subject
- The Big Picture
- Process elements, faults, and failures
- Detailing the faults
- Analysis of failures
- Presenting challenges
- Overcoming challenges
- Questions / Comments?

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	

The big picture



Legal context
- Legal theory
- Application
- Methodology
- Jurisdiction
- Case type
- Proof standard
- Calendar
- Strategies
- Costs

Evidence
- Identify
- Collect
- Preserve
- Transport
- Store
- Analyze
- Interpret
- Attribute
- Reconstruct
- Present
- Destroy

Tools
- Methodology
- History
- Pedigree
- Reliability
- Testing
- Calibration
- Function
- Limitations

Litigants
- Due care
- Retention

People
- *Scientific*
- Knowledge
- Skills
- Experience
- Training
- Education
- *Non-scientific*
- Clarifying
- Observation
- Honesty
- Integrity
- Competence

Challenges
- Make/Miss
- Content
- Context
- Meaning
- Process
- Relationship
- Ordering
- Time
- Location
- Corroboration
- Consistency
- Accident/intent
- False positive
- False negative

Legal process
- Pre-legal
- First filing
- Notice
- Preservation
- Productions
- Disclosures
- Depositions
- Motions
- Sanctions
- Admissibility
- Pre-trial
- Testimony
- Disposition

Admissibility
- Relevance
- Original writing
- Authenticity
- Probative > Prejudicial
- Hearsay

Outline

- Background of the speaker and subject
- The Big Picture
- Process elements, faults, and failures
- Detailing the faults
- Analysis of failures
- Presenting challenges
- Overcoming challenges
- Questions / Comments?

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	

The structure of challenges

- DFE processes takes place in every case
- This is an error model of the processes
- Each process element may
  - Make/miss
  - Fault types
  - By accident/intent
- Some faults lead to failures

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	

Process elements

- Basic processes
  - Identify
  - Collect
  - Preserve
  - Transport
  - Store
  - Destroy (aside)
- To do, see:
  - G. Carlton and R. Worthley, “An evaluation of agreement and conflict among computer forensics experts”, HICSS 2009

- Advanced processes
  - Analyze
  - Interpret
  - Attribute
  - Reconstruct
  - Present
- To do, see:
  - F. Cohen, “Digital Forensic Evidence Examination”, ASP Press, 2009

Outline

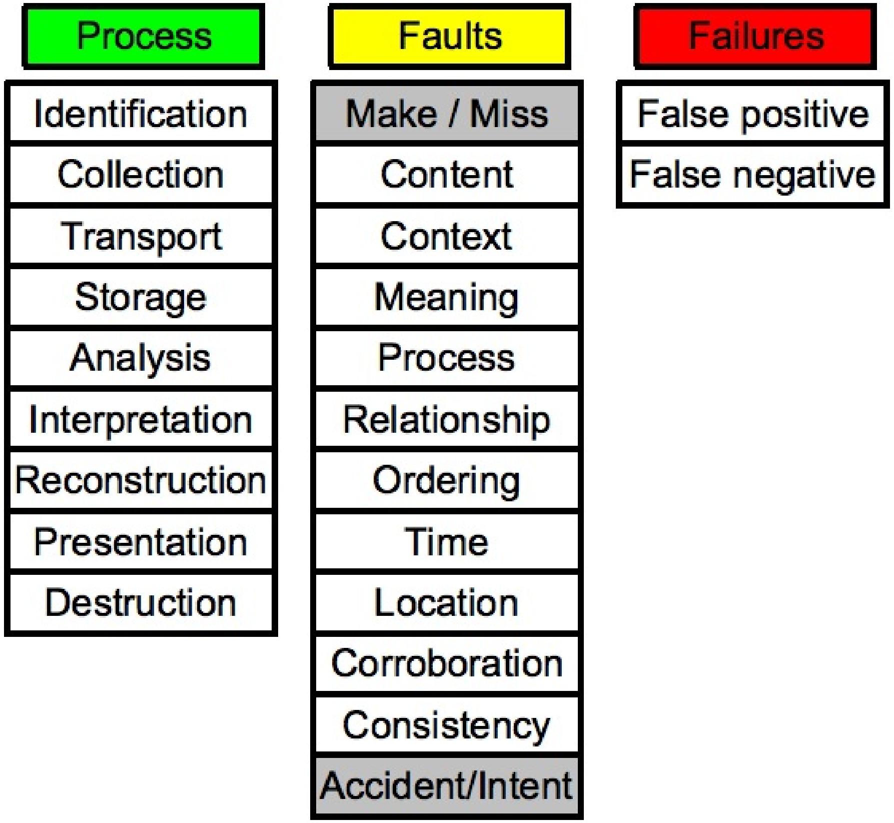
- Background of the speaker and subject
- The Big Picture
- Process elements, faults, and failures
- Detailing the faults
- Analysis of failures
- Presenting challenges
- Overcoming challenges
- Questions / Comments?

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	

Finding fault(s)

- Challenges to DFE is largely about finding faults
  - Miss/make Content (what is there)
  - Miss/make Context (its place in the digital world)
  - Miss/make Meaning (what it means for the case)
  - Miss/make Process (how it was done)
  - Miss/make Relationship (what it relates to)
  - Miss/make Ordering (causality and event seq)
  - Miss/make Time (when what happened)
  - Miss/make Location (where what happened)
  - Miss/make Corroboration (other supporting bits)
  - Miss/make Consistency (of traces and events)

Finding faults

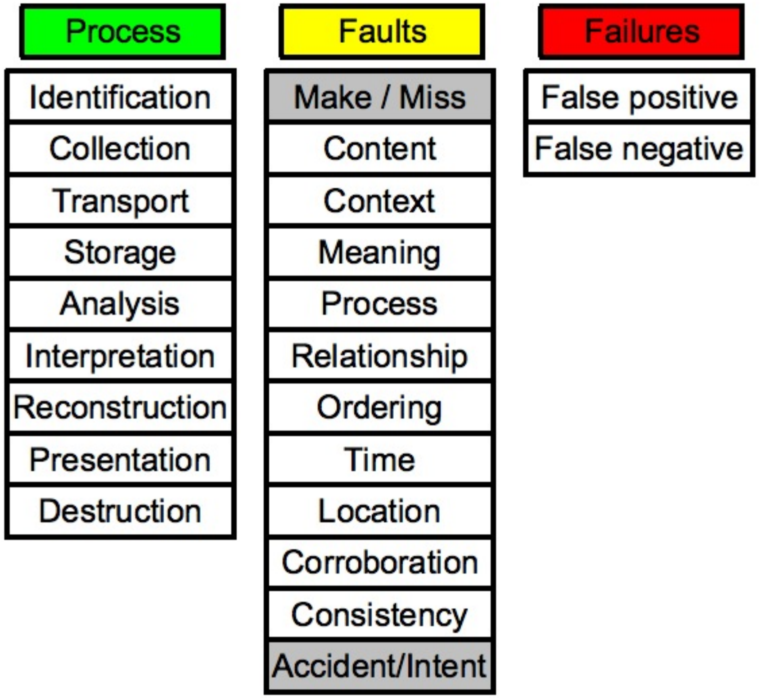


Process	Faults	Failures
Identification	Make / Miss	False positive
Collection	Content	False negative
Transport	Context	
Storage	Meaning	
Analysis	Process	
Interpretation	Relationship	
Reconstruction	Ordering	
Presentation	Time	
Destruction	Location	
	Corroboration	
	Consistency	
	Accident/Intent	

- Each challenge for each process element
  - Identify relevant faults and test for presence
  - Describe faults found
- For all found faults
  - Interpret fault
  - Attribute to cause
  - Present faults

Outline

- Background of the speaker and subject
- The Big Picture
- Process elements, faults, and failures
- Detailing the faults
- Analysis of failures
- Presenting challenges
- Overcoming challenges
- Questions / Comments?



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	

All faults are not failures

- The presence of evidence is evidence of presence?
  - Nobody is perfect – there will always be faults
  - Not all faults will be found – but some may be
  - For found faults, what do they imply?
    - What is probative to the matter at hand?
    - Can the fault be leveraged into a set of possible failures?
    - Are those failures probative with respect to the matter at hand?
  - As the number of faults grow, it speaks to the qualifications of the "expert"

Example implications

- Fault (missed content identification):
  - Missed identifying a disk later disposed of
- Failures:
  - False positives
    - No claimed records proving innocence
  - False negatives
    - The exculpatory evidence was on that disk!
- Probative?
  - Can the missed disk be leveraged into something probative to the matter at hand?
  - What can be said about the spoliated evidence?

Example implications

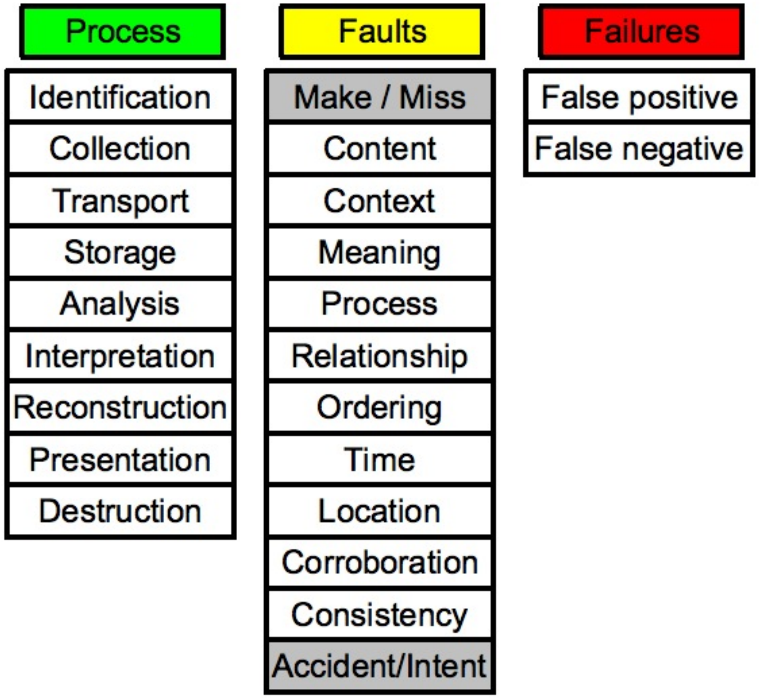
- Fault (made relationship attribution):
  - Configuration file related to wrong program
- Failures:
  - False positives
    - Claimed proof of use on date refutable
  - False negatives
    - Proof of linkage to a different program?
- Probative?
  - Can the made relationship be leveraged into refutation of claims?
  - What does it say about the “expert”?

Example implications

- Fault (made ordering analysis):
  - Date and time stamp sequence ignores time Δ
- Failures:
  - False positives
    - Claimed causality refutable
  - False negatives
    - Claimed non-causality refutable
- Probative?
  - Can the made ordering be leveraged into refutation/assertion of causality?
  - What is the proper Δ?

Outline

- Background of the speaker and subject
- The Big Picture
- Process elements, faults, and failures
- Detailing the faults
- Analysis of failures
- Presenting challenges
- Overcoming challenges
- Questions / Comments?



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	

Presenting example 1

- Fault (missed content identification):
  - Missed identifying a disk later disposed of
- Claim: False - exculpatory evidence was lost!
- Probative - The spoliated evidence!!!
- After demonstrating the relevant facts (if true):
  - The claim that the missing disk contained exculpatory evidence is consistent with CLIENT claims.
  - The exculpatory evidence would only be available on the missing disk and no other potential sources have been identified.
  - They destroyed any and all such evidence.

Presenting example 2

- Fault (made relationship attribution):
  - Configuration file related to wrong program
- Claimed Failures:
  - False +: Claimed proof of use on date refutable
  - False -: Proof of linkage to a different program
- After demonstrating the relevant facts (if true):
  - U failed to properly associate the configuration file with the actual program it reflects.
  - Ur claim of use is inconsistent with the traces.
  - My claim of use is consistent with the traces.
  - Ur expert failed to properly apply *** methodology

Presenting example 3

- Fault (made ordering analysis):
  - Date and time stamp sequence ignores time ∆
- Fail: False + Claimed causality refutable
- Probative: Close only counts in horse shoes
- After demonstrating the relevant facts (if true):
  - After adjusting for the time ∆ I identified as relevant for the matter at hand, the claim of causality can be clearly seen to be untrue.
  - In fact, the claimed effect happened before the claimed cause.
  - Ur claim is inconsistent with current scientific theory and methodology.

It's usually not that simple

- Challenges don't usually come in such simple forms
  - Combinations of many facts may be required
  - Individual evidence items may combine together to form inconsistencies
  - Multiple faults may have interactions
  - Other things may be consistent with all of the facts and alternative explanations may work
- Challenges dealing with consistency are particularly complex in nature

Outline

- Background of the speaker and subject
- The Big Picture
- Process elements, faults, and failures
- Detailing the faults
- Analysis of failures
- Presenting challenges
- Overcoming challenges
- Questions / Comments?

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	

Overcoming challenges

- Way 1: Don't have many of these faults!!!
  - Faults come largely from:
    - Errors and omissions
    - Lack of adequate knowledge, diligence, or care
    - Guessing and going a “bridge too far”
    - Inadequate preparation and thought
  - To avoid the faults, don't do these things!!!
    - Learn to be more careful
    - Study your field very thoroughly
    - Don't say things you aren't really sure of
    - When you are sure, check it out anyway!
    - Learn to say “I don't know”

Overcoming challenges

- Way 2: Rehabilitation
  - The claiming party has to push it over the threshold of the standard of proof
    - The preponderance of the evidence
    - Beyond a reasonable doubt
  - Then the burden shifts to the other party to push it back under the threshold of the standard
    - Assume that their challenge has pushed it back over the threshold and that you have to get it back to the standard of proof...
- Two approaches:
  - Find more/better evidence (usually too late)
  - Use what you have better

Find more or better evidence

- Problematic in most legal matters
  - By the time you know about the challenges that are actually brought, you usually cannot “find more evidence” or “find better evidence”
  - If you had this, you would have to have provided it in time for the other side to change all of its views and theories of the case
  - It may destroy all of the arguments and claims made (the whole strategy and tactics of the case may be affected).
  - It assume that the lawyers will let you go that way – which they rarely will.

Use what you have better

- In other words, be more thorough
  - But there are limits to time, effort, skills, tools, techniques, knowledge, education, training, and experience that can be brought to bear.
  - And it is infeasible in essentially all cases to be completely thorough [Cohen, “Digital Forensic Evidence Examination”]
  - How thorough can you be?
- Digital forensic evidence examination is:
  - A high stakes, high skills contest between opposing parties in a structured context
  - But we still have to seek and speak the truth

One hour of CPE

- This class provides about 1 contact hour
- To put it in context:
  - An MS degree from CalSci focussed on digital forensics involves about 160 contact hours and a total of about 500 total hours of effort over a minimum of 1 year.
  - A Ph.D. degree from CalSci focussed on digital forensics involves about 500 contact hours and a total of almost 2,000 hours of total effort over a minimum of 3 years.
- To meet the challenges of DFE
  - You need to be a student of the science forever

Outline

- Background of the speaker and subject
- The Big Picture
- Process elements, faults, and failures
- Detailing the faults
- Analysis of failures
- Presenting challenges
- Overcoming challenges
- Questions / Comments?

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	

Thank You

http://calsci.org/ - calsci at calsci.org

http://all.net/ - fc at all.net