Metrics for Digital Forensics

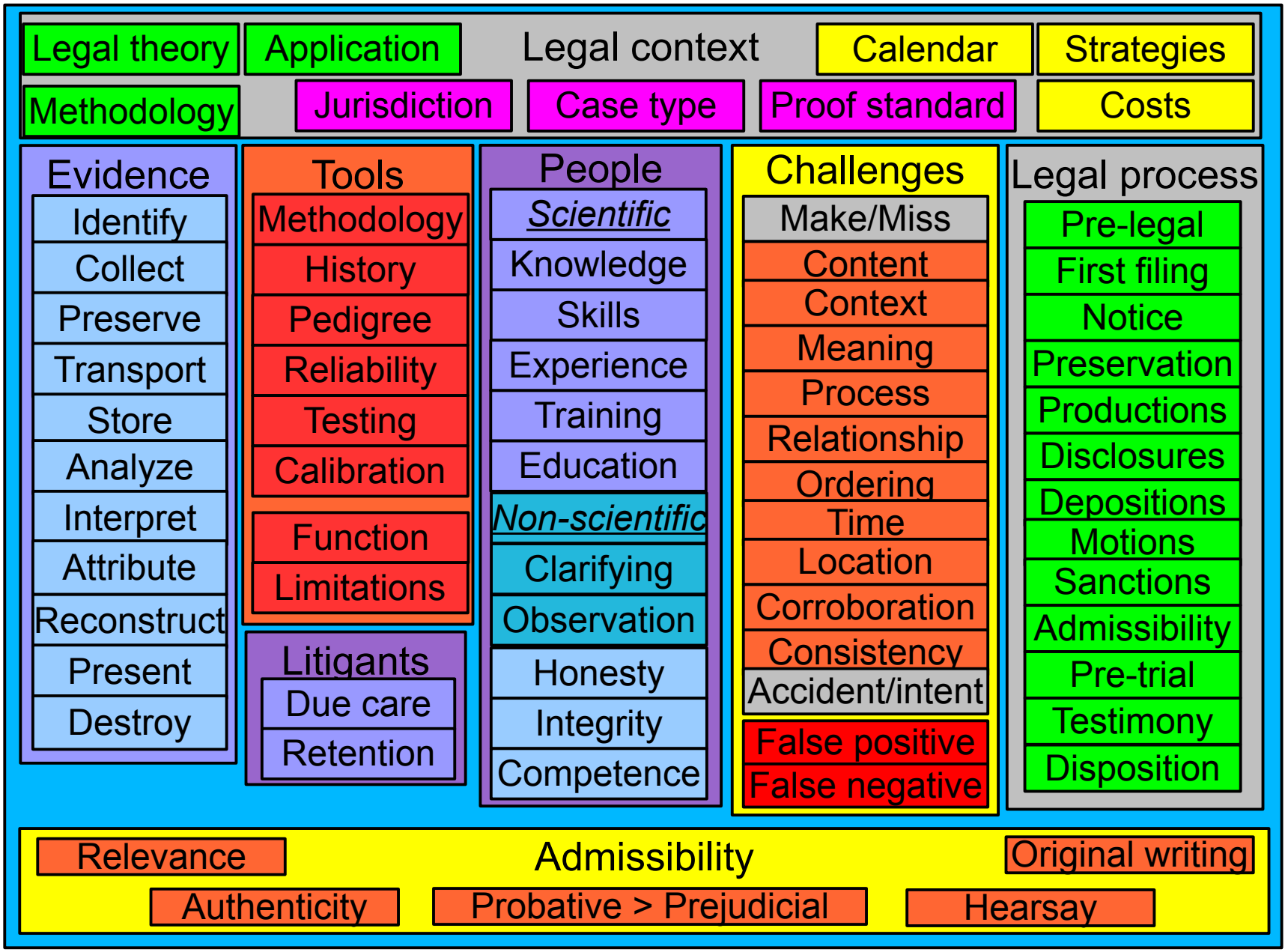
MiniMetriCon – April 13, 2009

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

Metrics for digital forensics

- A structure for considering digital forensics
  - The big picture for digital forensics
  - A mathematical structure to support it
- Why do we NEED metrics for digital forensics?
- Why don't we have decent metrics for it?
- How are we going to get them?
- Questions / comments / discussion

The big picture



People use Tools to Process Evidence w/in the legal framework. Legal process drives what can be done when Methodology is properly applied to evidence to show a legal theory

A mathematical model

- Laws L:{l_1, ..., l_n}, R:{r_1, ..., r_m}, LxR→V:[F|T]
- Events V: ∀E_x∈*E*, E_x:(e_{x1}∈E*, ..., e_{xp}∈E*)
- Traces T:(t_1, ...,t_q), ∃t:t∉T (Power set of bits available)
- Trace Consistency C:TxT→[-1...1], ∀c∈C, c→[-1...1]
- Demonstration Consistency D:TxE*→[-1..1]
- Procedures P:{p1, ..., pn}, (All "Available" procedures)
  - ∀p∈P, p→ {**c**⊂C, p→**d**⊂D, p→ℂ⊄C, p→𝕕⊄D}
- Resources $\mathcal{R}$:($\mathcal{T}$,$,$\mathcal{C}$,$\mathcal{E}$) (time, $s, capability, expertise)
- Schedule S:(s_1, s_2, ...),∀s∈S, s:(**l**⊂L, **r**⊂R, **h**⊂H, **e**⊂E, **t**⊂T, **c**⊂C, **d**⊂D, **p**⊂P, τ⊂$\mathcal{R}$, *t*, *t'*) (a constraint sequence)

Outline

- A structure for considering digital forensics
- Why do we NEED metrics for digital forensics?
  - Frye, Daubert, and Admissibility
  - Expert witnesses and their qualifications
  - The National Research Council Report of 2009
  - Federal Judicial Center report of 2000
- Why don't we have decent metrics for it?
- How are we going to get them?
- Questions / comments / discussion

Frye, Daubert, and Admissibility

- Frye v. United States, 293 F 1013 D.C. Cir, 1923
  - The Frye standard is basically: (1) whether or not the findings presented are generally accepted within the relevant field; and (2) whether they are beyond the general knowledge of the jurors.
- Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 125 L. Ed. 2d 469, 113 S. Ct. 2786 (1993).
  - Allows accepted methods of analysis that properly reflect the data they rely on.

Admissibility of DFE

- As any evidence, must meet specific criteria – to wit
- In order to be admitted, digital forensic evidence must survive challenges to:
  - Relevance (How do we measure this?)
  - Authenticity (How do we measure this?)
  - Hearsay nature (and business records exception)
  - Original writing (How do we measure this?)
  - More probative than prejudicial (How do we measure this?)
- Must be
  - Introduced and analyzed by people who meet standards

Non-expert testimony

- Non-expert testimony is only admitted if it is
  - (a) rationally based on the perception of the witness,
  - (b) helpful to a clear understanding of the witness' testimony or the determination of a fact in issue, and
  - (c) not based on scientific, technical, or other specialized knowledge within the scope of expert testimony
- Unless you are qualified as an expert, you cannot testify except about what you saw, did, or know from personal experience to be the case (with some sloppiness at the edges)

Experts and their qualifications

- Expert testimony requires:
  - A witness qualified as an expert by knowledge, skill, experience, training, or education. (How do we measure this?)
- May testify in the form of an opinion, if
  - (1) the testimony is based on sufficient facts or data, (How do we measure this?)
  - (2) the testimony is the product of reliable principles and methods, and (How do we measure this?)
  - (3) the witness has applied the principles and methods reliably to the facts of the case. (How do we measure this?)

National Research Council

- "Strengthening Forensic Science in the United States: A Path Forward", 2009 recommends:
  - "As a general matter, laboratory reports generated as the result of a scientific analysis should be complete and thorough. They should contain, at minimum, “methods and materials,” “procedures,” “results,” “conclusions,” and, as appropriate, sources and magnitudes of uncertainty in the procedures and conclusions (e.g., levels of confidence)... Forensic reports, and any courtroom testimony stemming from them, must include clear characterizations of the limitations of the analyses, including measures of uncertainty in reported results and associated estimated probabilities where possible."
  - How do we measure this?

Federal Judicial Center

- The Reference Manual on Scientific Evidence:
  - "the theory's testability, whether it was the subject of peer review or publication, its known or potential rate of error, and its general acceptance within the relevant scientific community" - Reference Manual on Scientific Evidence - Second Edition - Federal Judicial Center, 2000
- (How do we measure this?)

Outline

- A structure for considering digital forensics
- Why do we NEED metrics for digital forensics?
- Why don't we have decent metrics for it?
- How are we going to get them?
- Questions / comments / discussion

Why aren't metrics very good?

- Relevance
  - Determined by a judge based on “merits”
- Authenticity
  - Currently - substantially altered from original
  - Rulings are non-uniform – because no metrics!!!
- Hearsay nature (business records exception)
  - Unless relied upon in the normal course of business
  - But many exceptions for DFE have been allowed
- What science does not measure, the judge decides, by human thought processes

Why aren't metrics very good?

- Original writing
  - Copies of DFE are accepted – unless they are not reliable in terms of substantive differences
  - Thus the burden is first on the party introducing the evidence, then on the party challenging, and back and forth
- More probative than prejudicial
  - All evidence prejudices the trier of fact – that is its purpose – to help them make a judgment
  - It is probative to the extent that it brings light to the issues at hand in the matter.
- How do we measure probe and prejudice?

Measuring experts?

- Knowledge and skill
  - Could be measured by testing procedures
  - But current “testing” is almost ridiculous
  - Certification processes are limited but improving
- Experience (required)
  - Resume, history of testimony and reports - checked out by the other side – brutally at times
- Training and education
  - Records of training (usually no tests)
  - Educational records from accredited institutions
  - Ph.D. best – in DF the first Ph.D.s are just starting

Measuring experts?

- Testimony is based on sufficient facts or data
  - We don't have a sound theory of what is enough
- Testimony is the product of reliable principles and methods
  - We don't have a way to measure reliability with regard to these issues
- Witness has applied the principles and methods reliably to the facts of the case
  - Most people testifying are not aware of many of the principles underlying their methods, there are not widely used reliability measures involved, and thing regarded as facts often are not really...

A sample problem

- The facts
  - The traces that are consistent with events
  - Events assert that...
  - Party A sent a set of items,
  - Party B received all of those items,
  - There is a contiguous path showing that each item went from party to party starting at party A and arriving at party B, and
  - Party B stated "Party A sent the items to me."
- Do you conclude that "party A sent the items to party B"? With what level of certainty?

Some new facts added

- Party A asserts that
  - They did not send those items to party B,
  - Except for the statement by party B that "Party A sent the items to me.", everything else is true
- Now what do you think? With what certainty?
-
- How do we measure the reliability of the conclusions drawn given that one added fact can change everything?

Problem 2

- The following command was used to search for the number of occurrences of lines containing "TeSt" within a file named "J.txt":
  - grep "TeSt" J.txt | wc
- Is the result reliable?
- How reliable is it?
- Under what circumstances?
- Identify ALL of the problems with this approach
- If we cannot answer these questions, how can we hope for reliable digital forensics?

Outline

- A structure for considering digital forensics
- Why do we NEED metrics for digital forensics?
- Why don't we have decent metrics for it?
- How are we going to get them?
- Questions / comments / discussion

How are going to get them?

- The only way I know is to
  - Fund substantial amounts of theoretical and experimental research over a long time frame
  - Produce large numbers of people with actual expertise as demonstrated by advanced university degrees from accredited universities and ongoing professional education and testing processes
  - Build up the science base by supporting ongoing research and development of new tools and techniques along with the surety required to have true understanding of what they do and how well under what circumstances

Thank You

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

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