Metrics for Digital Forensics

MiniMetriCon Conference – Feb 14, 2011

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

Outline

- Background
- The need for metrics in forensics
- Specific metrics
- The level of disconnect
- Meeting the need
- Summary / Conclusions / Discussion

Your speaker

- Fred Cohen
  - B.S. EE (C-MU '77), M.S. Info Sci (Pitt '81), Ph.D. EE (USC '86)
  - CEO - Fred Cohen & Associates / President CalSci
- CalSci
  - 501(c)3 research and educational institution
  - M.S. Advanced Investigation / Ph.D. Digital Forensics
- FCA
  - Enterprise Information Protection
  - Digital Forensics
  - Research and Development

Abstract

- This talk will
  - Examine the need for and state of the art in metrics for digital forensics,
  - Provide an in-depth look at specific metrics, such as those for admissibility of evidence, qualifications of experts, reliability of methods and their application, and related issues mandated by the legal system.
  - Weighed against the state of the art in the physics of digital information to get a sense of the level of disconnect today between the needs and state of measurement in digital forensics
  - Notions about how to meet the emerging needs

Outline

- Background
- The need for metrics in forensics
- Specific metrics
- The level of disconnect
- Meeting the need
- Summary / Conclusions / Discussion

Metrics required by courts

- Metrics on witnesses
  - Non-expert
    - Must have probative content
    - Must only talk about what they experienced
  - Expert
    - Must be qualified as an expert in the matter
      - Training, Experience, Education, Skills, Knowledge
    - Must only talk about things beyond normal knowledge
    - Must provide the basis for their claims

Metrics required by courts

- Metrics on evidence
  - Must be more probative than prejudicial
    - Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 US 579, 125 L. Ed. 2d 469, 113 S. Ct. 2786 (1993).
      - allows **accepted methods** of analysis that properly reflect the data they rely on
    - Frye v. United States, 293 F 1013 D.C. Cir, 1923
      - The findings presented are **generally accepted within the relevant field**; and
      - **Beyond the general knowledge of the jurors.**
  - Must be relevant, reliable, authentic
  - Original writing – sort of

Recent research results

- Presented 2011-02-01 at IFIP TC11.9
  - The basics of digital forensics are not at a consensus level above random in the relevant communities
    - It is possible to observe digital information without altering it.
    - Digital evidence is trace evidence.
    - Digital evidence is finite in granularity in both space and time.
    - Computational complexity limits digital forensic analysis.
- It might seem we don't have generally accepted methods!!!

Other requirements

- Must be relevant
  - Determined by the judge
- Must be reliable
  - What is reliable?
- Must be authentic
  - What constitutes adequate authenticity?
- Original writing – sort of
  - We'll get to this as well...

Outline

- Background
- The need for metrics in forensics
- Specific metrics
- The level of disconnect
- Meeting the need
- Summary / Conclusions / Discussion

What is "reliable"?

- A reliable methodology properly applied
  - Some method that has been shown to be reliable to an identified level
    - We need reliability metrics to show this
    - Or we can simply claim it is "reliable" ...
  - A person who applies it reliably
    - The person who applied the method has to testify about it (or may)
    - The person in situ has to be shown reliable at applying the method
    - We need to measure performance of people in tasks
    - Or we can simply claim them "reliable" ...

Reliability example

- Fingerprints...
  - Used for 100 year or more to show a person was at a place or touched a thing (trace evidence of the transfer of the finger oils)
- Then the Madrid bombings
  - FBI analysts declared a “match” of a lawyer from Oregon against the print found on a device at the bombing
- But he wasn't there... really... and showed it.
  - So now evidence given regarding many finger-prints is now unreliable AND historic cases are subject to appeals (many are underway)

Name a "reliable" method

- What is a reliable method for examining a digital record?
  - How about a search for string?
  - Find "fingerprint" in the last slide…
- How reliable is it?
  - How do we measure reliability?
  - Even something as simple as a string search is potentially problematic
- How do you show the reliability?

What is authentic enough?

- Authentication is a
  - **Declaration** of authenticity
  - By a **competent** custodian or public official
- Either
  - A **sworn statement** or
  - **An element added** to the record after its completion.
- But authentication is not the same as authenticity.

Authentic

- Authenticity is a quality of the record
  - It is what it purports to be as long as it exists (e.g., this was the contract I signed)
- How do we show that a digital record is what it purports to be?
  - Determined by examining the context
  - Is it consistent with the claims about it?
  - It it in the proper place, order, format, etc.?
- How good is good enough?
  - The 50% rule – and the oppositional nature
  - How do I get to 50%??? I can only refute or not

Attribution as an example

- Notion: attribute authorship by “hand”
  - I tend to say things differently than you do.
  - We should be able to find a way to tell your writing from mine based on “stylometrics”
- What's the science behind it?
  - Theory: different people express themselves in different “styles” that we can measure and differentiate.
  - Test: Show a metric for “style” that allows such measurement to a level od quality adequate to show a jury.

Stylometrics today

- 2011 IFIP TC11.9 paper
  - comparative analysis with attribution methods: histogram distance, Manhattan distance, cosine distance, KS distance, cross-entropy, Kullback-Leibler distance, LDA, Gaussian SVM, and Naïve Bayes methods.
  - against sample set generated from words, 2-3 letter words, 3-4 letter words, word bi-grams, word tri-grams, word stems, parts of speech(POS), word lengths, syllables per word, characters, character bi-grams, character tri-grams, binned frequencies, binned reaction times, and Mosteller-Wallace function words
  - 15 authors with 5,000 words from each, 500 involving imitation and 500 involving obfuscation

Study results

- Under obfuscation
  - individuals sought to change their writing styles the best performance was correct in its classification only 42% of the time - the worst was never correct.
- For imitation
  - samples of other writing styles were provided and imitation was sought to deceive authorship, the best performance was 23% correct attribution, and the worst was never correct.
- No method performed significantly better than chance. **REFUTATION**

Show original writing?

- Original writing – sort of
  - We'll get to this as well...

Outline

- Background
- The need for metrics in forensics
- Specific metrics
- The level of disconnect
- Meeting the need
- Summary / Conclusions / Discussion

You in the metrics community

- Do you have any metrics that tell me whether the content I get from a system is what it purports to be?
  - Do your records systems keep such information?
  - How hard/easy is it to defeat the mechanisms?
    - If it's not “secure” how can it be “trustworthy” to produce records?
    - How can you tell if a record was altered?
    - Are you even measuring this?
    - What is the “reliability” measure for your records system?
    - How would you even go about it?

Diplomatics – codified in law

- Separate, different, independent, trustworthy...
  - 565 AD:
    - Deposit of the records in a public place
    - Unbroken legitimate custody
    - Authentication is based on form
  - 1681: archival science codified into laws
    - Focused on individual documents, their characteristics, genesis, and treatment
  - 1800s: every lawyer schooled in diplomatics
  - 1922: Naturalness, Interrelatedness, Authenticity, and Uniqueness (in context)
  - The same problems – Different technology

Diplomatics in digital archives

- When we moved to computers – we forgot it
  - The ownership of real estate is no longer kept in public records and properly certified
  - Rather it is kept in private records that are not kept to the same documentary standard
  - The courts believe the companies who attest to the authenticity of records that are wrong
  - Foreclosures of homes owned by the residents based on false records and inadequate process
- The loans and financial crisis
  - The records cannot be untangled as to who owns what – and massive frauds result

And we forgot...

- Separation of duties and financial systems
  - Most current financial systems enforce separation of duties for users
  - But not for systems administrators
  - Who can alter anything at will unnoticed
- Electronic medical records and malpractice
  - It used to be you had erasures on pieces of paper to review as evidence
  - Now you get a bag of bits that are easily altered at the lowest level of granularity
  -

Outline

- Background
- The need for metrics in forensics
- Specific metrics
- The level of disconnect
- Meeting the need
- Summary / Conclusions / Discussion

What I can do today

- You claim X
  - Is X consistent with the available
    - Traces (the bag of bits) – abbreviated 'T'
    - Events (the other stuff) – abbreviated 'Ev'
- If you did your job right, the answer is
  - Everything I found was consistent with X
  - I found nothing that was inconsistent with X
- So how do you do your job right?

Inconsistency as refutation

- I look for inconsistencies
  - Science explains and predicts
  - It assumes Cause → Effect exists (C→E)
    - No C→E means we cannot explain or predict
    - We think C→E because we have lots of history of successful prediction using it
- Science starts with a hypothesized C→E
  - We use experiments to try to refute C→E
  - Predictions are specific and a-priori
  - Results are specific and posteriori
  - Experiments are independently repeatable

Inconsistency → Redundancy

- I look for inconsistencies within and between T and Ev
  - The nature of digital space:
    - C→E non-unique with incomplete T
    - T is essentially never complete →
    - Non-unique C for the defined E
    - More (T, Ev)x(T, Ev) redundancy of the right sort → Fewer consistent C→E
- Without such redundancy, it is all assumption
  - You need redundancy to make your case
  - And I use it to break your case

Diplomatics revisited

- Separate, different, independent, trustworthy...
  - 565 AD:
    - Deposit of the records in a public place
    - Unbroken legitimate custody
    - Authentication is based on form
  - 1922:
    - Naturalness (C⟶E consistent with T and Ev)
    - Interrelatedness [(T, Ev) x (T, Ev) consistent]
    - Authenticity (uncorrupted) [evidence of such]
    - Uniqueness (in context) Fewer consistent C⟶E
  - The problems and solutions are the same
  - The technology is different

Outline

- Background
- The need for metrics in forensics
- Specific metrics
- The level of disconnect
- Meeting the need
- Summary / Conclusions / Discussion

One last example

- Legal matter involving claimed messages
  - Plaintiff offers hundreds of purported emails
  - Claims the source of the emails took control over his systems and caused damages
  - Basis is the emails themselves
- What is it to cause “damages”?
  - Defined in prior rulings:
    - damages as "money awarded to one party based on injury or loss caused by the other. ... different types or categories of damages [are]:
    - compensatory damages ... general damages … nominal damages ... punitive damages ... special damages ... statutory damages... treble damages

Assessing damages

- Computer break ins are trespass
  - Entitled at most to compensatory damages (a.k.a. actual damages)
    - Damages that cover actual injury or economic loss. Compensatory damages are intended to put the injured party in the position they were in prior to the injury.
    - Valid types: physical damage, conversion, **deprivation**, lost value, lost rights
  - Computing deprivation:
    - Must be: quantified, time framed, tangible, unmitigatable, uninvited, and causal
    - How do we show and compute this?

Metrics for damages

- Quantified: (how much deprivation)?
  - 10,000 bytes * 100,000 emails = 1 gigabyte.
    - If you didn't run out, you were not deprived.
    - If you did, the space must be prorated against overall cost ($0.10 at $100/Tbyte)
    - Didn't run out → no actual damages
  - Over 30 days, 38 bytes/second (<0.1% of BW)
    - If you didn't run out, you weren't deprived
    - Need records to show actual loss from deprivation
    - No such records → no evidence of actual damages
  - CPU usage not otherwise available... same issues
- No measurements → No quantified damages

More damages metrics

- Time framed
  - There was a 30-day period asserted
- Unmitigatable
  - Why didn't you delete the undesired records?
  - Why didn't you disable otherwise unused email addresses receiving the messages?
- Uninvited
  - Why did you configure your system to allow messages to addresses you don't use?
- Causal
  - How / how well can you attribute to defendant?

Digital Forensics Metrics

- For digital forensics we need real metrics that
  - Meet legal requirements for measurable reliability, authenticity, accuracy, precision, etc.
  - Are based on a sound scientific methodology properly applied
  - Have a basis provided for independent testing
- Those presenting evidence must be qualified by
  - knowledge, experience, skills, training, education
- Based on 1500 years of legal precedent not likely to disappear very soon
- Assume they call all bluffs ... snooze, you lose

Thank You

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