Digital diplomatics and forensics
Going forward on a global basis

Digital Diplomatics 2013 – Paris, France
2013-11-14

Dr. Fred Cohen

CEO – Management Analytics
Acting Director – Cyberlab – Webster University

This work was supported by InterPARES Trust

Management Analytics

Webster UNIVERSITY

Outline

- Context
  - The lack of consensus in digital forensics
  - The history of diplomatics
  - A view of core concepts in classical diplomatics
    - Inconsistency based on physicality and content
- Questioned digital documents
  - A science-based approach: $C \rightarrow^{m} E$
  - Causality → attribution
    - Source → particularization, individualization
    - Method → fonds and the archival bond
- A future for global record-keeping

Context – my background

- As you will soon see, I am not a diplomaticist
  - I work substantially in digital forensics
  - I seek to use the results and concepts of diplomatics
- I believe that in the digital arena, diplomatics and forensics are – or should be – merging / uniting
  - The concepts from diplomatics appear to me to be closely aligned with those of modern digital forensics
- I believe that the legal notions formulated out of diplomatics are core to many of the concepts used in forensics
  - I believe that the common use of language would be most helpful in uniting these fields
  - I think we need to better understand each other

Management Analytics

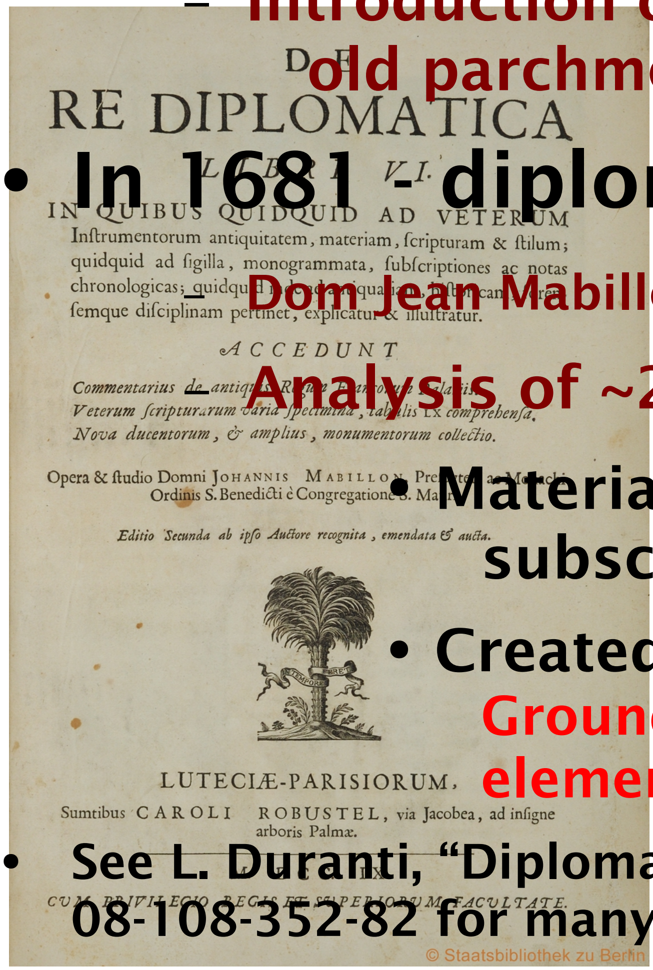
Webster UNIVERSITY

Context - forensics

- The lack of consensus in forensics
  - Recent studies have shown little or no consensus in even the basic definitions underlying digital forensics
  - Less consensus around the basics than the consensus for global climate change being caused by humans
  - The ability to copy without alteration doesn't exceed random levels of consensus
  - Other similar seemingly standard things are also sub-consensus levels (most random, none at 95%)
  - F. Cohen, "Update on the State of the Science of Digital Evidence Examination", Conference on Digital Forensics, Security, and Law, May 29-31, 2012.
  - F. Cohen, J. Lowrie, C. Preston, "The State of the Science of Digital Evidence Examination", IFIP Seventh annual IFIP WG 11.9 International Conference on Digital Forensics, 2011/01/30, also published as a chapter in in "Advances in Digital Forensics VII".

Context – history of diplomatics

- 1643 – Acta Sanctorum (Bollandist society)
  - Testimony about single saints evaluated to separate fact from legend
- 1675 – Volume 2 (Bollandist: intro by van Papenbroeck)
  - Introduction on general principals for establishing authenticity of old parchments. Declared diploma of Dagobert 1st a forgery!


DE RE DIPLOMATICA
LIBRI VI.
IN QUIBUS QUIDQUID AD VETERUM
Instrumentorum antiquitatem, materiam, scripturam & stilum; quidquid ad sigilla, monogrammata, subscriptiones ac notas chronologicas; quidqu... semque disciplinam pertinet, explicatur & illustratur.
ACCEDUNT
Commentarius de antiq...
Veterum scripturarum varia specimina, tabellis LX comprehensa.
Nova ducentorum, & amplius, monumentorum collectio.
Opera & studio Domni JOHANNIS MABILLON, Pre... Ordinis S. Benedicti è Congregatione S. Ma...
Editio Secunda ab ipso Auctore recognita, emendata & aucta.
LUTECIÆ-PARISIORUM,
Sumtibus CAROLI ROBUSTEL, via Jacobea, ad insigne arboris Palmæ.
CUM PRIVILEGIO REGIS ET SUPERIORUM FACULTATE.

- In 1681 - diplomatics had begun (read as rhyme)
  - Dom Jean Mabillon, “De Re Diplomatica”, 1681, Saint-Maur, France.
  - Analysis of ~200 documents divided into categories and examined:
    - Material, ink, language, script, punctuation, abbrev., formulas, subscripts, seals, special signs, chancery notes, …
    - Created descriptions to allow the detection of forgeries
      Ground truth based on recurrence of intrinsic and extrinsic elements in documents from same time and place (redundancy)
- See L. Duranti, “Diplomatics – New uses for an old science”, Scarecrow Press, 1998, ISBN 08-108-352-82 for many more and more definitive details.

History moved on

- Later works improved on this approach
  - A correlation approach – but correlation is not causality
    - Similar characteristics do not imply similar causes
      - Effect does not imply cause!
- Authenticity of records related to procedure of creation
  - Beitrage zur Diplomatik I-VIII, by Theodor von Sickel, in Sitzungsberichte der Raiserlichen Akademie der Wissenschaften, published in Vienna between 1861 and 1882
- Many historical documents now exist claiming to identify when which terms were used in which ways
  - A basis for refutation of a document claimed to be of a certain period based on content.
  - However, this is time consuming, relies on knowledge that may not be available, cannot be easily and quickly applied
- By now you understand how little I understand…

Core concepts

- Inconsistency based on physicality
  - The nature of the media
    - Age, makeup, manufacture, composition, materials, etc.
  - The way the media is imprinted
    - 'hand', ink type and makeup, carbon and other dating, materials, instruments used, tool marks, oils from hands, fibers from clothes, etc.
- Inconsistency based on form (structure, rules of record making, elements present / missing, etc.), not content
  - Known formats, fields, syntax, locations on forms, etc.
  - Spelling, language, usage, methods, font, etc.
  - Redundancy in the record, in the fonds, across fonds

Management Analytics

Webster UNIVERSITY

Outline

- Context
  - The lack of consensus in digital forensics
  - The history of diplomatics
  - A view of core concepts in classical diplomatics
    - Inconsistency based on physicality and content
- Questioned digital documents
  - A science-based approach: $C \rightarrow {}^{m}E$
  - Causality → attribution
    - Source → particularization, individualization
    - Method → fonds and the archival bond
- A future for global record-keeping

Why diplomatics matters in forensics

- Georges Tessier : « On peut donc avancer que la critique diplomatique est née dans le prétoire ou sur le forum à l'occasion de débats judiciaires ou de controverses politiques ou religieuses, quand le nœud du litige ou de la polémique était constitué par un document ou une série de documents contestés ». Cette citation est tirée de L'Histoire et ses méthodes (La Pléiade, 1961) dont Georges Tessier a signé le chapitre « Diplomatique ». - http://www.marieannechabin.fr/ - 2013-11-11 blog of Marie Ann Chabin
  - (English by Google: "It can be argued that the diplomatic criticism is born in court or forum on the occasion of judicial proceedings, or political or religious controversy when the crux of the dispute or controversy consisted of a document or series of documents in dispute . " This quote is from The History and Methods (The Pleiades, 1961) with Georges Tessier signed the chapter "Diplomacy".

History - forensics

- 1929 – E. Locard publishes a treatise on forensics
  - Identifies causes (e.g., step in mud as you walk)
  - Identified effects (e.g., layers of mud on shoes)
  - Identified mechanism (i.e., “transfer”)
- Transfer of particles from contacting materials leaves traces on each material of the other.
  - Layers of transferred material accumulated over time
  - Remove last (outer) layer first and loop
  - Find sources of trace materials (i.e., fabric from factory)
  - This produces a history of where someone was

- E. Locard, "The Analysis of Dust Traces", Revue International de Criminalistique I. #s 4-5, 1929, pp 176-249, (translated into English and reprinted in 3 parts in A, J. Police Science, 1930 in V1#3, May-Jun 1930, pp276-298, V1#4 Jul-Aug 1930, pp 401-418, and V1#5 Sep-Oct 1930, pp 496-514.)

History - forensics

- Latent evidence
  - Fingers have natural oils
  - When fingers contact surfaces, they transfer those oils
  - What is left behind is a pattern of oils that are in the same shape as the swirls, ridges, etc. on fingers
    - "Finger prints"
  - Cause: Fingers touch things (e.g., guns, bullets, etc.)
  - Mechanism: Transfer (e.g., oils transfer to trigger)
  - Effect: Traces (i.e., finger prints)
- But you cannot see the finger prints directly
  - You need to use tools to make them visible and do analysis – thus they are "latent"

Fingerprints part 2

- Washington, we have a problem
  - Theory: Each set of ridges and swirls is unique
    - Application: Print → individual (attribution)
  - However…
    - Partial prints (essentially all real ones) are … partial
    - Analysis in real situations involves smears, etc.
    - A "Standard" of practice was used
      - Number of "features" found and relative position
      - No real experimental basis for level of certainty
    - March 2004: Madrid bombings → False Positive!!!
      - Identified an attorney in Oregon
      - Verified by several independent experts
      - The only problem: ground truth refuted it – ID was wrong!

- Statement of Glenn A. Fine, Inspector General, U.S. Department of Justice before the House Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security concerning "Section 1001 of the USA Patriot Act" May 10, 2005, at: http://www.usdoj.gov/oig/testimony/0505b.htm

Digital forensics

- Started (sort of) in the 1950s – but really the 1960s…
  - Computers are compositions of input mechanisms, finite state automata (machines), and output mechanisms.
  - In executing their operations, they produce traces (stored digital values).
    - Cause: input and state
    - Mechanism: the operation of the FSM
    - Effect: traces in the form of bits at locations
  - $C \rightarrow^{m} E$ – a causal model with a firm basis in fact
    - The mechanisms are "known" (or knowable)
    - The properties of digital systems are known
    - We should be able to do scientific document analysis!

Management Analytics

Webster UNIVERSITY

Digital forensics – part 2…

- However…
  - The physics of digital information is not the same…
    - Information loss as time moves forward
    - Traces not produced by transfer (no transfer)
    - Essentially all traces are latent (tools required)
    - An "exact copy" is possible (at the digital level)
    - Anybody can produce any sequence of bits easily
  - The assumptions underlying causality are thus different in the digital arena
    - Common practice:
      - Look at traces (e.g., a log file)
      - Attribute to cause (e.g., known program caused it)
  - But Effect does NOT imply Cause

- F. Cohen, "Digital Forensic Evidence Examination", 2009, ISBN # 1-878109-49-9, Chapter 3

Big problem – Possible solution

- Digital traces do not have unique causes
  - Many causes for the same effect →
    - How can we know which one cause the results?
  - You can only dig so deep
    - The "bottom" level is the bit – it is digitally indivisible
- I claim a resolution is from redundancy and consistency
  - Most digital systems produce many (redundant) traces
    - Example: Web browsing produces:
      - Local: cached pages, cached URLs, history, audit logs, file time and date stamps, inode usage sequences, disk allocations, delays in other processes, etc.
      - Distant: URL lookups in DNS, IP addresses and content characteristics in network flow logs, server logs, logs from interdependent systems of server, etc.

Possible solution

- I claim a resolution is from redundancy and consistency
  - Most digital systems produce many (redundant) traces
    - …
  - Normal operation produces consistency between traces
    - Attempts to subvert operation produce inconsistencies
      - Examine enough traces properly → can detect subversion
- However…
  - This too is a theory
    - Tested in many cases – detects many subversions
    - Requires a lot more data than is typically used
    - Requires consistency checking algorithms
    - Depends on difficulty of forging ALL related records
    - Inconsistency refutes hypothesis, doesn't tell history

Applying this in digital diplomatics

- In digital archives (or other record-keeping systems)
  - Records in context of fonds
    - The methods of operation of the archives define (at some level of detail) the finite state machines
  - The fonds exist in digital mechanisms
    - The mechanisms have specific FSMs and operations
    - To test the record, we examine the redundant traces
    - If inconsistent, the record cannot be trusted
  - Note this is a refutation method only!
    - Failure to refute does not imply truth
      - "The absence of evidence is not evidence of absence"*
- "What is inconsistent cannot be true"+

- *Unknown actual origin, widely used in US Law Enforcement +F. Cohen, Digital Forensic Evidence Examination ibid.

Management Analytics

Webster UNIVERSITY

[In]Consistency

- Internal (Type C) [In]Consistency
  - Internal elements of the same object (record / document / etc.) are [not] consistent with the hypothesized method of their construction
    - Example: The record is missing a required field
    - Example: The date and time stamp is the wrong format
- External (Type D) [In]Consistency
  - Elements of different objects (records / documents / testimony / etc.) are [not] consistent with the hypothesized method of overall construction
    - Example: No log record of access at claimed access
    - Example: Font used did not exist at the creation time

- F. Cohen, "Two models of digital forensic examination", IEEE SADFE (in conjunction with the IEEE Oakland Conference), 2009-05-21, Oakland, CA

Example drill-down

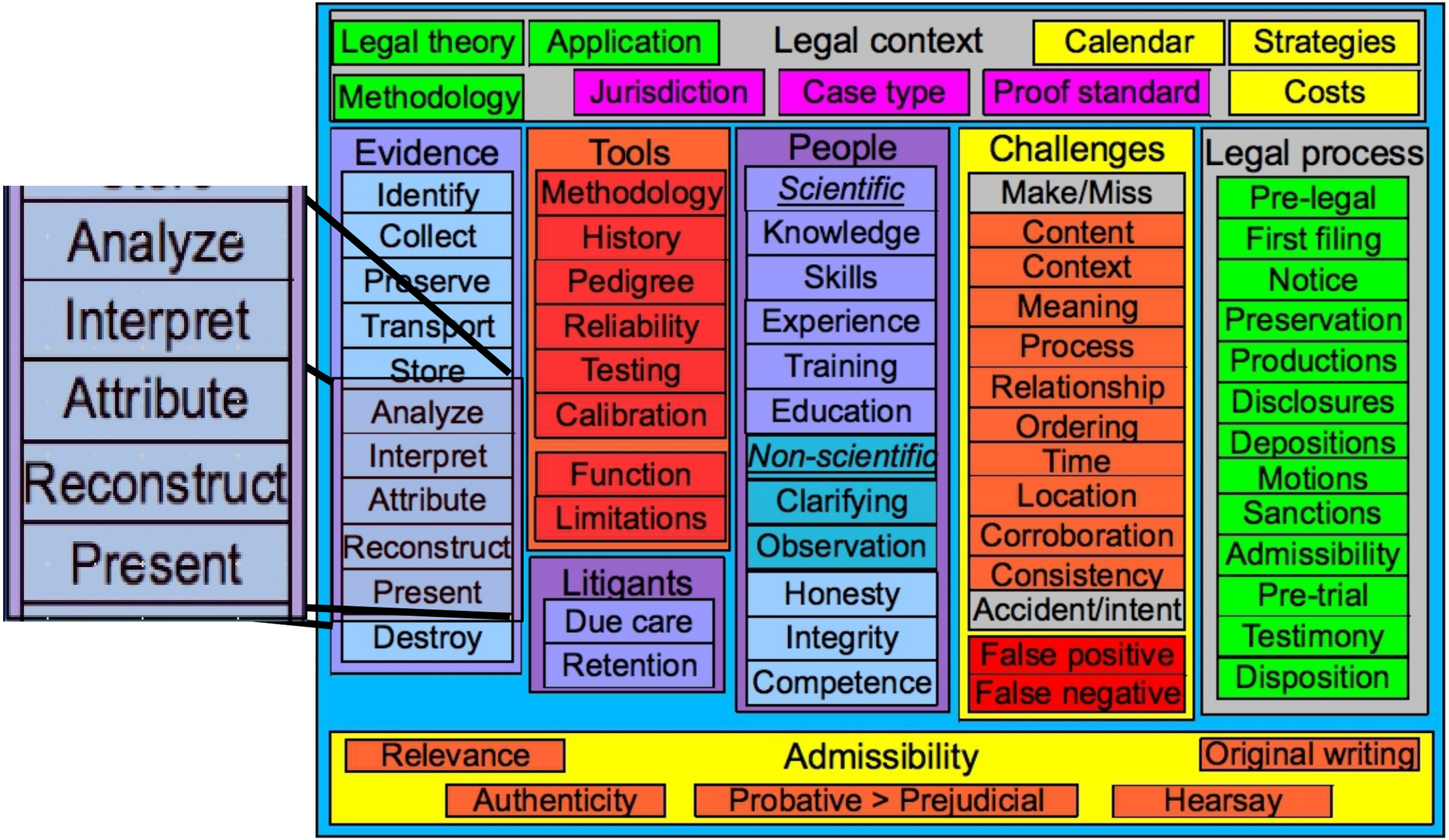
- File written with date and time stamp
  - Is directory entry in proper sequence?
    - Is inode used in proper sequence?
      - Is location on media in proper location for sequence?
        - Is overlay pattern of other files consistent with storage algorithms
        - …
      - Is location / fragmentation reflective of other processes?
      - …
    - Is overlaid previous content still present and right?
    - …
  - Is file metadata consistent with method of writing?
  - …
- Programs needed to write file are present? …

A lot of possible questions may be asked. Which ones should we ask? Why? When?

Management Analytics

Webster University

Digital Forensic Evidence Examination



Elements of Examination

- **Analyze:**
  - The set of methods applied to traces and events
- **Interpret:**
  - The examiner's interpretation of the traces and events as consistent or inconsistent with hypotheses
- **Attribute:**
  - Particularization of methods consistent with the productivity of the traces and individualization of potential sources of those traces
- **Reconstruct:**
  - The experimental methods used to test hypotheses
- **Present:**
  - The methods revealing latent evidence in human examinable form

Very recent example

- Plaintiff in a legal matter has expert claiming **Method**
  - **Method** based on indicators in traces (effects) claimed to allow reliable differentiation of cause:
    - e.g., How a message was sent and processed
  - Test of **Method** used reconstruction:
    - Circumstances differentiating causal conditions of interest reconstructed and executed in sequence
    - Traces produced captured for analysis
    - The claimed **Method** applied to produce results
    - Results found **inconsistent** with claims of **Method**
  - **Method** refuted by experiment (reconstruction)
- Actual case outcome is not yet known
  - We hope that the **Method** is **not** accepted by the courts

Notionally then – a scientific endeavor

- Hypothesize a causal mechanism ($C \rightarrow^{m} E$)
  - Hypothesize a method (P) for refuting claimed $C \rightarrow^{m} E$
  - Test the method in differentiating test cases
  - Refutation →
    - Either $C \rightarrow^{m} E$ is not correct
    - Or P does not properly differentiate cases
  - No refutation →
    - P properly differentiated cases in the identified tests
    - Apply P to actual instances of E in question
      - Refutation:
        - According to P, E is inconsistent with $C \rightarrow^{m} E$
      - No refutation:
        - According to P, E is consistent with $C \rightarrow^{m} E$

Redundant testing for higher certainty

- A set of tested procedures P=(p_1 … p_n) are applied
  - Test each p against the hypothesis H
  - IF ANY p∈P produces inconsistency →
    - The claimed hypothesis (H) is refuted
  - Otherwise
    - All procedures (P) tested were consistent with H
    - No procedures tested were inconsistent with H
- Note these are not "statistical" procedures…
  - Results must be consistent/inconsistent/indeterminate
    - Some (state) procedures were indeterminate
  - But they cannot be combined statistically
- Note that resources may limit P for any given matter

Management Analytics

Webster UNIVERSITY

A note on the use of language

- In digital forensics, many examiners go a bridge too far
  - Log A shows that Joe did Activity X
- Language usage should be strictly controlled:
  - I performed procedures P on traces T as follows:
    - Details… for each
      - Using tool T, I did this, I saw that
      - According to p_1 log A is consistent with Joe doing X
    - In summary, in all of the procedures I performed, I found log A consistent with Joe doing X and I found nothing inconsistent with Joe doing X
  - Use of personal pronouns (I did this, I saw that)
    - Sworn testimony reflecting what you did and saw

Criticality of tools

- The traces are latent
  - They can only be observed through tools
    - How do we validate and verify the tools?
    - How do we calibrate the tools and processes?
    - How do we know what we see reflects what is there?
    - How do we see “old” formats and content as original?
  - Digital tools are far more complex and brittle
    - Millions of lines of unverified code not unusual
    - Dependency on other tools for your tools
    - Inputs are often non-repeatable (e.g., try a rescan)
    - Analysis often produces wrong results for rare cases
    - Output often depends on media and settings
    - Tools often give different results for 'identical' input

Criticality of presentation

- Presentation can be, and often is, misleading
  - Presentation isn't just language usage in reports
  - Tool output appears (largely) as dots on a screen/sheet
    - Interpretation of those dots (e.g., 0 or O) is non-trivial
  - Presented information is used to make decisions
    - Further actions depend on previous output
    - Errors may propagate as presented results analyzed
  - Output reflects what the tool actually did
    - Not what you thought it did – and they often differ
  - How do you interpret what you see?
    - By looking at the output of another tool?
    - Much output isn't precise in what is depicted or where it came from

Management Analytics

Webster UNIVERSITY

Outline

- Context
  - The lack of consensus in digital forensics
  - The history of diplomatics
  - A view of core concepts in classical diplomatics
    - Inconsistency based on physicality and content
- Questioned digital documents
  - A science-based approach: $C \rightarrow {}^{m}E$
  - Causality → attribution
    - Source → particularization, individualization
    - Method → fonds and the archival bond
- A future for global record-keeping

Management Analytics

Webster UNIVERSITY

How can we improve record-keeping?

- I didn't mention some motivations…
  - Records of property ownership are now largely digital
  - Many contracts are digitally executed
  - Financial transaction records are almost entirely digital
  - The list goes on and on…
- The need for questioned document science seems high
  - A large part of the challenges come from the inability to systematically apply science to the issues
  - Science is slower than current technology change
  - Perhaps we should consider adding things to the record keeping systems to support diplomatics / forensics

What should we add?

- Redundancy seems to me to be a key answer
  - Both systematic and non-systematic should be added
    - Systematic redundancy may be easier to forge
    - Non-systematic may be less reliable to verify and harder to analyze – a benefit and detriment
- More analytical methods with reconstruction
  - There are many potential analytical methods
    - Not all of them are likely to be useful
    - We should seek to produce large numbers of methods
  - We should evaluate methods in situ via reconstruction
    - From a large set of systematically applicable methods
    - Automate testing in situ for different archives
    - Publish known good methods for each archive

Thank You

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