5. Introduction to Digital Forensics

Digital Forensics and Cybercrime course

Prof. Zanero

What does “Digital Forensics” mean?

- Forensics is the application of scientific analysis methods to reconstruct evidence.
- Digital (or Computer) Forensics is the application of scientific analysis methods to digital data, computer systems, and network data to reconstruct evidence.

The “Daubert” standard (US)

RULE 702. TESTIMONY BY EXPERT WITNESSES

A witness who is qualified as an expert by knowledge, skill, experience, training, or education may testify in the form of an opinion or otherwise if:

(a) The expert's scientific, technical, or other specialized knowledge will help the trier of fact to understand the evidence or to determine a fact in issue;

(b) The testimony is based on sufficient facts or data;

(c) The testimony is the product of reliable principles and methods; and

(d) The expert has reliably applied the principles and methods to the facts of the case.

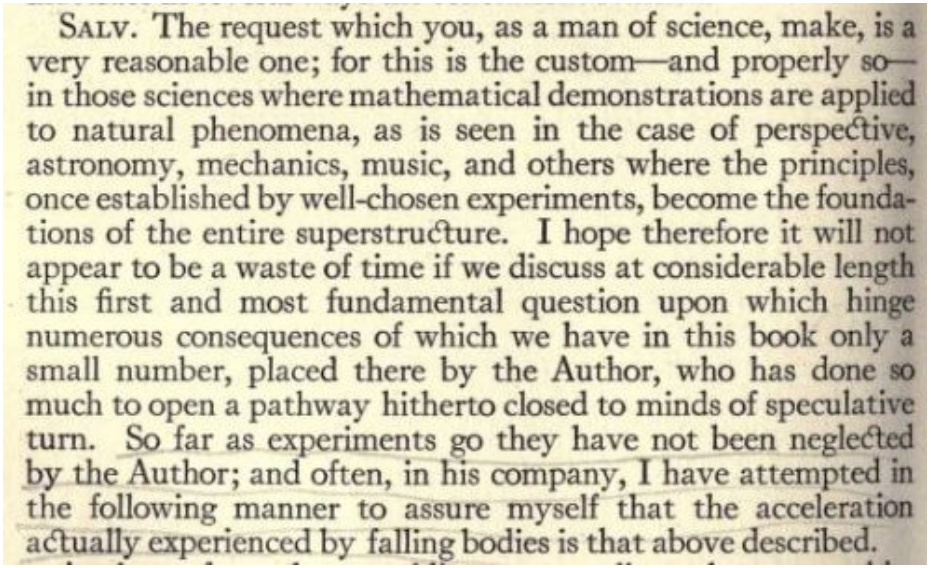
Elements of the Daubert standard

- Relevance and reliability: expert testimony "relevant to the task at hand" and rests "on a reliable foundation"
- Scientific knowledge = scientific method/methodology

What is the “scientific method”?

What does “scientific” mean?

- **Scientific = Repeatable** (Galileo, 1650)



SALV. The request which you, as a man of science, make, is a very reasonable one; for this is the custom—and properly so—in those sciences where mathematical demonstrations are applied to natural phenomena, as is seen in the case of perspective, astronomy, mechanics, music, and others where the principles, once established by well-chosen experiments, become the foundations of the entire superstructure. I hope therefore it will not appear to be a waste of time if we discuss at considerable length this first and most fundamental question upon which hinge numerous consequences of which we have in this book only a small number, placed there by the Author, who has done so much to open a pathway hitherto closed to minds of speculative turn. So far as experiments go they have not been neglected by the Author; and often, in his company, I have attempted in the following manner to assure myself that the acceleration actually experienced by falling bodies is that above described.

- **Scientific = Falsifiable** (Popper, 1934)

“In so far as a scientific statement speaks about reality, it must be falsifiable: and in so far as it is not falsifiable, it does not speak about reality.”

— Karl R. Popper, The Logic of Scientific Discovery

Daubert test for “scientific”

- Factors to consider:
  - Whether the theory or technique employed by the expert is generally accepted in the scientific community
  - Whether it has been subjected to peer review and publication
  - Whether it can be and has been tested
  - Whether the known or potential rate of error is acceptable; and
  - Whether the research was conducted independent of the particular litigation or dependent on an intention to provide the proposed testimony.

Example of forensic engagements

Situations and constraints

- Internal investigations (inside an organization)
- Criminal investigations (defense or prosecution)
- Post-mortem of a system to assess damage / define recovery strategy
- Research (honeypot, etc)

Crimes and events (examples)

- Child pornography
- Fraud
- Cyber extortion / threats
- Espionage
- Copyright infringements
- Policy violations

4 phases of an investigation

- Source acquisition
- Evidence identification
- Evaluation
- Presentation

M. M. Pollitt, (1995) “Computer Forensics: An Approach to Evidence in Cyberspace”, in Proceeding of the National Information Systems Security Conference, Baltimore, MD, Vol. II, pp. 487-491