What Your Client Wants From a Forensic Expert

Introduction to Digital Forensics

University of Houston

Prof. Chichester (guest of Prof. Mardis)

February 15, 2014

Never Forget...

- 1. ... why you have a job.
- 2. ... you have a job to make the case against the alleged perpetrator better than the case against ***you***.
- 3. ... that **you** can commit a crime very easily in the course of this employment.
- 4. ... that committing crimes doesn't make you look good in front of a judge or the jury.
- 5. ... the litigator is only concerned with what goes before the judge and the jury.

Never Forget....

- 6. ... the litigator (on either side) will happily destroy your reputation, your career and your livelihood if it helps his or her case.
- 7. ... **You're Expendable!**

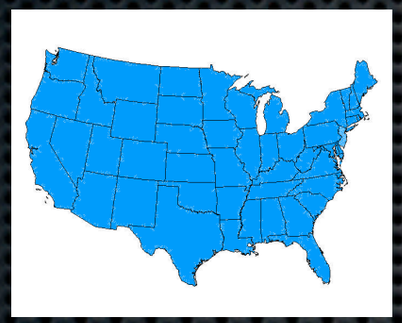
The Fundamentals

- Law is the regulation of activities between people.
- Activities between individuals using a computer can be recorded as data.
- That data is called *evidence*.
- Evidence is fundamental to a court case.
- If you don’t have evidence, you don’t have a case.
- If they can’t make a case, **they don’t need you**.

Data *can* be Evidence

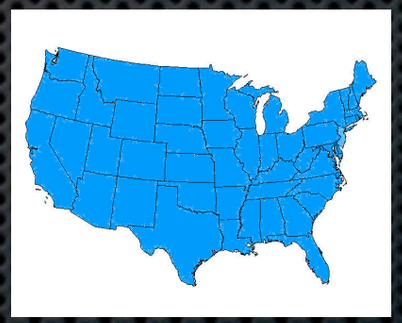
Civil cases

Criminal cases



Federal

Texas



Federal

Texas

- Civil Procedure
- Evidence

- Civil Procedure
- Evidence

- Crim. Procedure
- Crim. Evidence

- Crim. Procedure
- Crim. Evidence

The Rules That Apply to Physical Evidence Apply Equally to Electronically Stored Information (ESI) aka “Data”

Admissibility Rules

- Relevance (R 401)
- Expert Testimony (R 702)
- Authenticity (R 901(a))
- Hearsay (R 801)
- Original (Rs 1001-08)
- Prejudice (R 403)

Admissibility Rules

Relevance (R 401)

Expert Testimony (R 702)

Authenticity (R 901(a))

Hearsay (R 801)

Original (Rs 1001-08)

Prejudice (R 403)

Admissibility Rules

Relevance (R 401)

Expert Testimony (R 702)

Authenticity (R 901(a))

Hearsay (R 801)

Original (Rs 1001-08)

Prejudice (R 403)

But Rule 104 Comes First!

Rule 104 handles the relationship between the judge (the trier of law) and the jury (the trier of facts)

Rule 104(a)

- Questions of admissibility generally
  - Qualifications of a person to be a witness
  - Existence of Privilege
  - At this stage, the Judge is not bound by the other rules of evidence, subject to Rule 104(b)

Rule 104(b)

- When the relevancy of evidence depends upon the fulfillment of a condition of fact, the court shall admit it upon, or subject to, the introduction of evidence sufficient to support a finding of the fulfillment of the condition.
  - Translation: I'm skeptical, so I want to know more before I consider admitting it is evidence

Rule 104(a)

- Questions of admissibility generally
  - **Qualifications of a person to be a witness**
  - Existence of Privilege
  - At this stage, the Judge is not bound by the other rules of evidence, subject to Rule 104(b)

Rule 104(a)

- Qualifications of a person (generally) are different from those of an Expert
- Expert testimony and qualifications are governed by Rule 702.

Rule 702

- Rules for expert testimony changed by S.Ct. in 1993.
  - *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579, 113 S.Ct. 2786, 125 L.Ed. 2d 469, (1993).
  - Three factors (called the "*Daubert* factors"):
    - (1) the testimony must be based upon sufficient facts or data,
    - (2) the testimony is the product of reliable principles and methods, **and**
    - (3) the witness has applied the principles and methods reliably to the facts of the case.

Rule 702

- Expert testimony is subject to a *Daubert* hurtle
  - Evidence can be admitted only after a showing that the evidence is reliable and scientifically sound
    - Four considerations:
      - a) Testing;
      - b) Peer Review;
      - c) Error Rates; and
      - d) Acceptability in the Relevant Scientific Community.

Rule 702

- Whether you are able to testify as an expert witness depends upon your *qualifications*
  - Education and training
  - Demeanor before the trier of fact [judge or jury]
  - Competence
    - ... with the tools chosen
    - ... and the interpretation of the results

Admissibility Rules

Relevance (R 401)

Expert Testimony (R 702)

Authenticity (R 901(a))

Hearsay (R 801)

Original (Rs 1001-08)

Prejudice (R 403)

ESI Authenticity (Rule 901)

- Determination of authenticity is a two step process
  - Before admission before the *jury*, the **court** must determine if the proponent has offered a satisfactory foundation for the evidence to be admitted
  - But the *finder of fact* determines the ultimate relevancy of the evidence

For ESI to be admissible...

... it must be authentic

Rule 901(a)

- You need to provide support that the evidence to be admitted *is* what its proponent claims it to be.
- A *prima facia* showing will do.

Rule 901(a)

- **Examples**:
  - Testimony of witness with knowledge
  - Comparison by expert witness with authenticated specimens
  - Public Records
  - Demonstrated process or system
  - Ancient data compilations
  - Methods provided by statute or rule
  - ... and more

Rule 901(b)(1)

- Testimony by one having knowledge
  - "Testimony that a matter is what it claims to be."
    - Usually by someone who witnessed the event.
    - But… it is not required that the authenticating witness have personal knowledge of the making of a particular exhibit if he or she has personal knowledge of *how* that type of exhibit is routinely made.

Rule 901(b)(3)

- "Comparison by the trier of fact or by expert witnesses with specimens which have been authenticated."
  - this rule allows either expert opinion testimony to authenticate a questioned document by comparing it to one *known to be authentic*, or by permitting the finder of fact to do so.

Translation: Show and Tell Time

Rule 901(b)(4)

- This rule permits exhibits to be authenticated or identified by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."
  - Usually used to authenticate e-mail, text messages and website content.
  - Hash values and metadata admitted under this rule.

Rule 901(b)(7)

- Records or Reports
  - Evidence that a writing authorized by law to be recorded or filed and in fact recorded or filed in a public office, or a purported public record, report, statement, or data compilation, in any form, is from the public office where items of this nature are kept.
- Example: Government database records

Rule 901(b)(9)

- This rule authorizes authentication by "[e]vidence describing a process or system used to produce a result and showing that the process or system produces an accurate result."
- Translation: *Did the computer and software work as it was supposed to?*

Rule 902

- Self Authentication
  - Official publications under 902(5)
  - Trade inscriptions “[i]nscriptions, signs, tags, or labels purporting to have been affixed in the course of business and indicating ownership, control, or origin.” under 902(7)
  - Certified domestic records of regularly conducted activity under 902(11)
- Example: Metadata in cell phone jpeg images

Don’t Forget...

- 1. You have to be able to gather the data competently;
- 2. You have to be able to analyze the data and interpret the results competently; **and**
- 3. You have to be able to support the admissibility of that data and interpretation so that a judge can admit it
- 4. If you can’t do 1), 2) **and** 3) above, **then your client doesn’t need you**

(Real Life) Horror Stories

O'Brien v. O'Brien, 899 S.2d 1133 (Dist. Crt. App., Fla., February 11, 2005)

Pop Quiz: Divorce -- Texas Style

Questions?