Use of Seized Materials & Results in Evidence

CJ341 – Cyberlaw & Cybercrime
Lecture #21

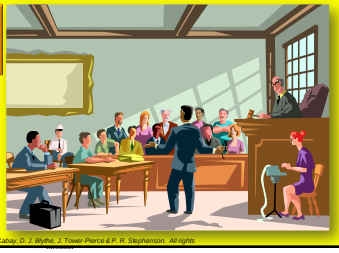
M. E. Kabay, PhD, CISSP-ISSMP
D. J. Blythe, JD
School of Business & Management

1

Topics

- Admissibility of Digital Evidence
- The Courts & Digital Evidence
- Admission of Digital Evidence at Trial

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (US DoJ) (SSCOEECI) §V (PDF pp 119-128).



2

Admissibility of Digital Evidence

- US v. Liebert (1975)
  - Could computer records for alleged federal tax-evader be admitted as evidence?
  - Yes, provided
    - ✓Prosecution could prove digital data were *accurate* and *authentic*
    - ✓Defense was given opportunity to check
- Resistance to admitting digital evidence continued
  - Based on Federal Rules of Evidence
  - http://www.law.cornell.edu/rules/fre/
  - Includes hearsay, authentication, nature of writings & copies

3

Hearsay

- Rule 801: "…statement, other than one made by the declarant…."
- Rule 801(d)(1) permits digital evidence such as e-mail or Web postings if
  - Statement contradicts sworn testimony
  - Statement rebuts accusation of lying
  - Statement helps identify person

4

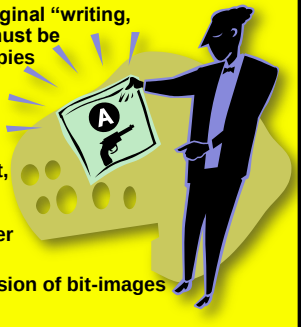
Authentication (1)

- Authentication validates evidence
- Rule 901(a) requires authentication
  - One method uses self-authentication mostly involving public records and certification (rarely works for digital evidence)
  - Other approach involves authentication by a qualified professional
- Prof Moore argues that only 2 of the Rule 901 subclauses apply to digital evidence: both involve testimony of expert witnesses

5

Nature of Writings

- Rule 1002: specifies that original "writing, recording or photograph" must be available to authenticate copies presented in evidence
- Rule 1001(1) stipulates that *writings and recordings* include "letters, words, or numbers, or their equivalent, set down by…magnetic impulse, mechanical or electronic recording, or other form of data compilation."
- Rule 1004: allows for admission of bit-images of forensic data



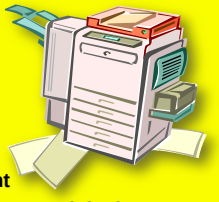
6

CJ341 Class Notes

Copies

Rule 1004 allows submission of copies when

- Originals are lost or destroyed
  - But verifiable copies make it easy to present in court given hash functions, proper bit-image
- Original is not obtainable
  - Usually have to return equipment to suspect
  - But data may be destroyed by suspect
- Original is in possession of opponent
  - Suspect may refuse to grant access to original data



7

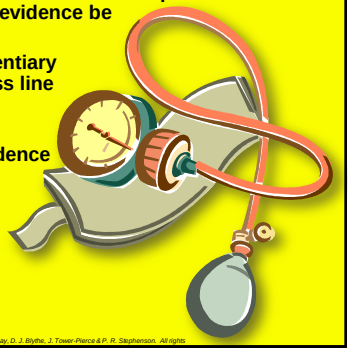
The Courts & Digital Evidence

- Frye v. US (1923)
- Daubert v. Merrell Dow Pharmaceuticals (1993)
- State v. Hayden (1998)
- People v. Lugashi (1988)
- US v. Scott-Emuakpor (2000)
- Williford v. State (2004)

8

Frye v. US (1923)

- Could *scientific evidence* about blood pressure and effects on polygraph evidence be introduced at trial?
- Court ruled that evidentiary collection had to cross line from *experimental* to *demonstrative*
- Set standard that evidence must be "*generally accepted in scientific community*"



9

Daubert v. Merrell Dow Pharmaceuticals (1993)

- Woman claimed drug company caused birth defects
- Offered scientific studies showing relationship
- Court required method to conform to general acceptance in scientific community using *Frye*
- SCOTUS *overturned* verdict
  - Scientific evidence need only be *reliable and scientifically valid*
  - Now known as the *Daubert Test* (see next slide)

10

The Daubert Test

- *Has the scientific theory or technique been empirically tested? According to K. Popper (1989) in The Growth of Scientific Knowledge, "the criterion on the scientific status of a theory is its falsifiability, refutability, and testability."*
- *Has the scientific theory or technique been subjected to peer review and publication? This ensures that flaws in the methodology would have been detected and that the technique is finding its way into use via the literature.*
- *What is the known or potential error rate? Every scientific idea has Type I and Type II error rates, and these can be estimated with a fair amount of precision. There are known threats to validity and reliability in any tests (experimental and quasi-experimental) of a theory.*
- *What is the expert's qualifications and stature in the scientific community? And does the technique rely upon the special skills and equipment of one expert, or can it be replicated by other experts elsewhere?*
- *Can the technique and its results be explained with sufficient clarity and simplicity so that the court and the jury can understand its plain meaning? This is just the Marx standard, which is assumed to be incorporated in Daubert as it was with Frye.*

Quoted from http://faculty.ncwc.edu/toconnor/425/425lect02.htm

11

State v. Hayden (1998)

- Hayden charged with rape and murder
- Difficulty obtaining fingerprints from bloody sheet
- Forensic specialist used digital photography and computer enhancement to develop fingerprint
- Challenged in court – not approved technique
- Prosecutors argued that all steps were scientifically sound
- Court *rejected argument*, suppressed evidence

12

CJ341 Class Notes

People v. Lugashi (1988)

- Case involved theft of credit-card data from backup tapes
- Forensic investigator could not explain details of how forensic software worked
- Defense argued for suppression of evidence
- Court ruled that expert had *sufficient experience* with software to warrant confidence
  - Relying solely on experts who understood *all details* of all hardware & software would limit testimony & impede justice

13

US v. Scott-Emuakpor (2000)

- Nigerian *advance-fee fraud*
- Secret Service investigators searched defendant's computer
  - Found evidence of crime
- Defense argued that SS officials were not computer experts and evidence should be suppressed
- Court ruled that SS agents were sufficiently expert in *use of forensic tools* to qualify as witnesses

14

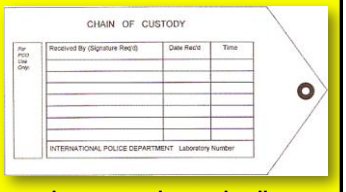
Williford v. State (2004)

- Computer repair tech found child porn on computer
- Police investigator made bit-image of suspect's HD using EnCase
- Investigator challenged at trial over lack of computer-science education
- Prosecution argued that *extensive training* in use of EnCase + *reliability of software itself* warranted admission of evidence
- Court ruled in favor of prosecution (2003)
  - Officer did qualify as expert for purposes of presenting digital forensic evidence
  - EnCase satisfied requirements for admission as scientific evidence
- Appeals Court of Texas supported decision (2004)

15

Admission of Digital Evidence at Trial

- Additional criteria for admissibility
  - Authentication
  - Chain of custody
- Authentication based largely on digital signatures or hashes



- Chain of custody requires minute attention to detail
  - Every person in contact w/ evidence is opportunity for challenge
  - Must have valid reason for access
  - Detailed records of involvement

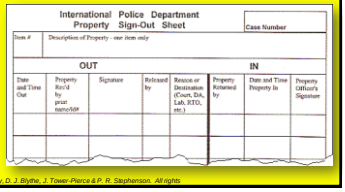
16

Supporting the Chain of Custody

Chain-of-custody log should include critical elements

- Evidence inventory number
- Date and Time
- Who Removed the Evidence
- Location Removed and Taken To
- Reason Evidence Being Removed
- Date of return

Also "Chain of Custody"
By R. L. Trench of the
Intl Assoc Property & Evidence
http://tinyurl.com/6febwf



17

Now go and study

18