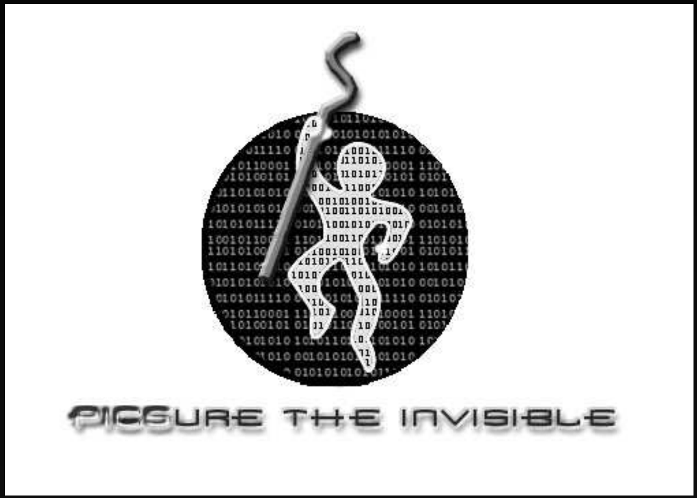
COMPUTER FORENSICS



Erin E. Kenneally
San Diego Supercomputer Center
University of California San Diego
erin @ sdsc.edu

ESSENCE OF ALL FORENSIC SCIENCES

- Principles applied to the
  - Detection,
  - Collection,
  - Preservation,
  - Analysis

  of evidence to ensure its admissibility in legal proceedings

Different Realms…. Same Principles

- http://host/cgi-bin/helloworld?
  type=AAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAA
  AAAAAAAAA
  AAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAA
  AAAAAAAA
  AAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAA
  AAAAAAAAAAAAAAAAAAAA
  AA

Computer Forensics: The 'New' Kid on the Block

- Compare to established Forensic Sciences

  - Fundamental assumptions the same
    …start with intense variability among large # variables/attributes

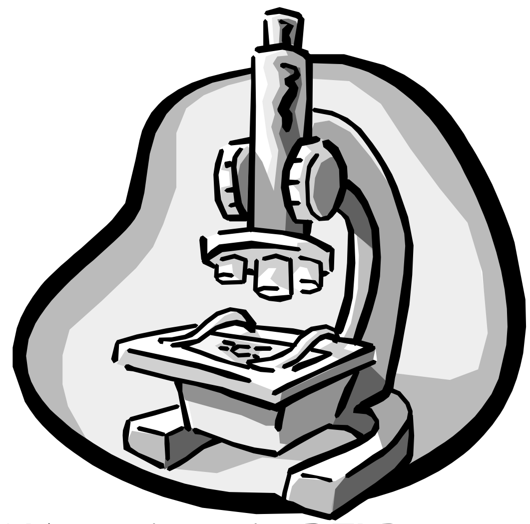
  - Advances aim to develop meaningful/probative value from variables

- identifying
- characterizing
- correlative

→ **Properties** of evidence sources

(…Compare to established Forensic Sciences)

- Techniques to enhance the I/C/C properties :
  - more precisely
  - more accurately
  - faster/less time
  - requiring less evidence



- /ex/ Digital Data v. Biological Data
  - A/B/O typing --> rH factors --> DNA typing via RFLP --> DNA typing via PCR
  - Hash libraries (to ID data); File signature (match name & file type); Mirror imaging software

(...Compare to established Forensic Sciences)

- "What we observe is not Science, but Science's answer to our questions"
  - Question : ~~existence of evidence~~

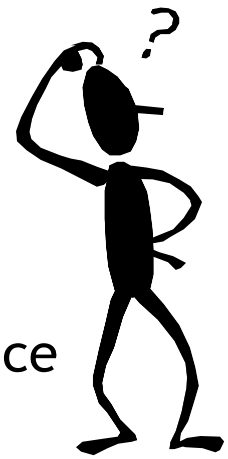
    ability to uncover & contextualize evidence
  - Challenge:
    - Where look ?
    - What technique to make apparent ?
    - Is it admissible ?

Analogize:

	DIGITAL EVIDENCE	DNA EVIDENCE
WHERE	Media (HD, floppy, CD, PDA, DVD) Location (server logs, IDS, firewall logs)	Clothing, cigarette butts, weapon Blood, saliva, hair shaft
WHAT TECHNIQUE	Software / Hardware to recover deleted data, file slack, unallocated space, swap files	PCR RFLP STR
ADMSSBLTY	Technology to recover deleted data ⟺ Accepted ⇕ SW recovery ⟺ Challenged (inclusiveness)	DNA technology ⟺ Accepted ⇕ STR technique ⟺ Challenged

Digital Evidence - Search & Seizure Issues

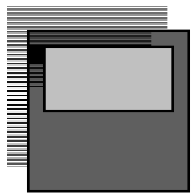
- Shifting Paradigms
  - Resource challenges
  - Defining "Reasonableness"
  - Modification/Destruction of Evidence

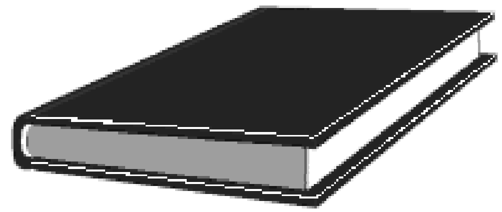


Search & Seizure - Resource Issues

- Traditional approach: seize everything
- Problem: collect ability >>>>> analysis ability
  - a lot of junk; case backlogs
  - economic infeasibility: storage capacity; human/time resources
    - /ex/ network search: image 100's of Gb's???
    - /ex/ C3D create "FMD-ROM" = 140 Gb
      - compare: cd= 650 Mb; DVD= 6Gb
    - /ex/ IBM- 73 Gb HD

Search & Seizure - Resource Issues





Search & Seizure - Defining Reasonableness

- What is unlawful S & S in Cyberspace?

  - 4th A violations judged by notions of "reasonableness"

    - Search Warrant Issuance standard = PC
      PC = Reasonableness
      Reasonable ≅ Narrow & Particular

  - Realize: Time & Scope variables with intangible, digital evidence

    - judges focus on disruption to business
    - assume narrow Scope by ↓ Time allotted
    - BUT, shorter Time = wider Scope
    - Result: Breadth of search is >>>>

Search & Seizure - Defining Reasonableness

- Search Warrant Parameters
  - Anywhere reasonably find evidence
    - s/w for gun precludes looking in a cell phone case
  - BUT, Digital Evidence - no physical limits
    - can hide/compress large amounts of data anywhere
    - file labels no reflect search subject matter

Search & Seizure - Evidence Modification Challenges

- Benign actions ……. Probative consequences
  - Truth:

    Turning on computer:
    Win95 system opened 417 files (8%) of files on hard drive just to boot (primarily .LNK and antivirus files)
  - Consequence: 417 access dates altered
  - So what?: Timestamps crucial

So what?: Timestamps crucial

- Charge: possession kiddie porn

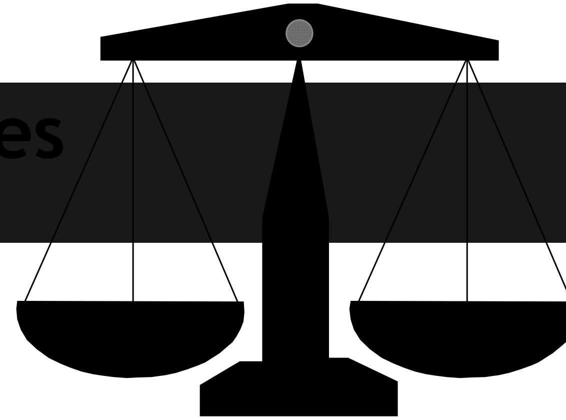
  Digital Evidence on Defendant's Computer: large collection of adult porn; couple dozen kid porn images.

  Defense: downloads adult porn via IRC; some of the kid porn was 'unintentionally' downloaded with adults.

  Computer Forensics: Timestamps show adult pics viewed (access date) after downloaded (creation date), but kid porn have same timestamps

  Destruction of exculpatory evidence: seizing officer boots machine and rifles through pics ……..

Jurisdictional Challenges



- Substantive Laws inconsistent
  - Hackers route through various countries, hoping lack of victim discourage investigation & prosecution coordination
    - /ex/ Love Bug Virus?
  - CFAA- $5K minimum -->reward corp's whose house is in disarray....easier to add up damages
  - ECPA- affords > protection for wire v. electronic communications
    - problems given convergence of voice (wire) & non-voice data in same data stream
    - USA-PATRIOT Act has changed this !!!!!!!

(jurisdictional challenges)

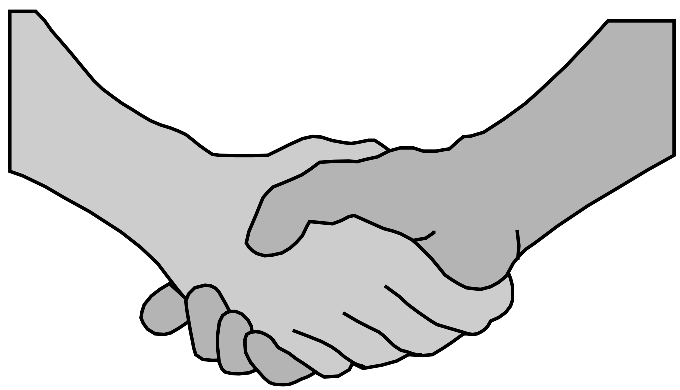
- Procedural Laws
  (The Law responds to technology……)
  - /ex/ Fraud case
    - victim: NV
    - perp: website owner in FL
    - NV prosecutors issue subpoena for records from FL co.

    - No formal mechanism for service
    - Accomplish via pro courtesy……no guarantee serve or enforce
    - NV could refer case to FL counterparts
      – but, if no FL victim……..will it go forward?

    - USA-PATRIOT to the rescue

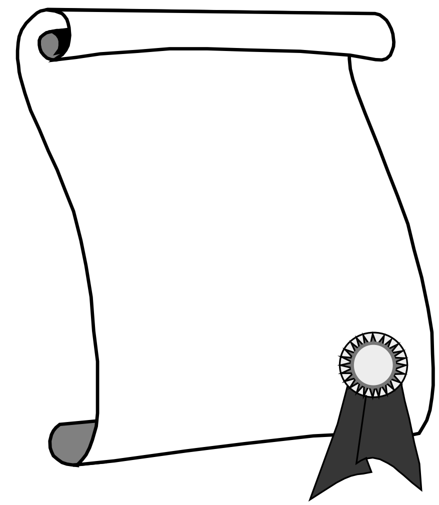
Coordination Challenges

- /ex/ Cyberstalker sends threatening email to pty in OH
  - ◆routes through 4 countries
  - ◆LE in OH would have to go through Office of Intntl Affairs, LE in various cntrys, just to trace back to perp in OH
  - ◆Timing is crucial……..crook long gone by time these procedures exhausted



Contrast: Computer Forensics v. Traditional Forensic Sciences

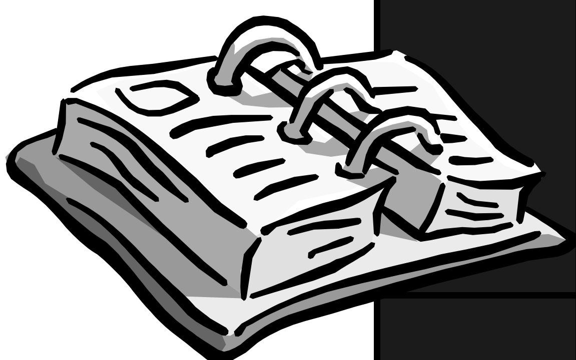
- **Qualifying Cyber Experts under Daubert/Kumho**



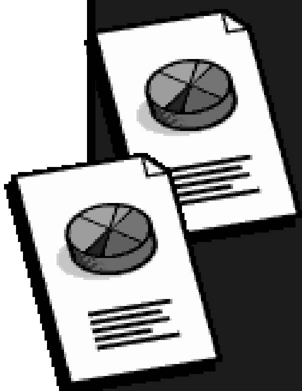
  - Shifting paradigm
    - What is ‘general acceptance’
    - academic credentials
      - CS curricula short academic tradition
      - high academic credentials << commercial/industrial value
    - quantifying experience
      - no certification standards
      - diverse knowledge-base

CONTRAST DIGITAL EVIDENCE

	PAPER-BASED EVIDENCE	DIGITAL EVIDENCE
STORAGE	→ Document storage can be cumbersome	→ Computers can store large amounts /i.e./ 1 Gb = 14 floors text pages
	→ organized	→ unorganized (by human standards) /why/- sequence or location of data irrelevant if takes seconds to find any
	→ search clarity *context relatively apparent	→ search hurdles * document may be stored in pieces …individually no context



	PAPER-BASED EVIDENCE	DIGITAL EVIDENCE
PROCESSING	→ 'back-ups' not routine	→ back-ups common
***COPYING**	→ copies maintained	→ copies scattered
	→ copies usually mimic original	→ copies show various 'stages' of document creation
	→ deliberate	→ often inadvertent /i.e./ file slack, swap
	→ 'perfect'	→ 'imperfect'



	PAPER-BASED EVIDENCE	DIGITAL EVIDENCE
***Transmission**	→ traditional methods: *snail mail *physical delivery *fax → 1-to-1 messaging → defined boundaries → limited distribution -transceiver doesn't retain copies → controlled	→ Internet; Email; Telnet; FTP; etc. → mutable (alteration proof?) → multifaceted - directed broadcast → complex - data on single host accessed & commingled with any number of users on the network → distributed -single transmission handled by many carriers, spanning multiple countries → automated

	PAPER-BASED EVIDENCE	DIGITAL EVIDENCE
SECURITY	Boundaries: - time, distance, physical locale - separate people and forged social identities - define perimeters for securing people and paper-based info	→ Boundaries: - time, space, location no longer define perimeter - between you & I; or, between my proprietary business database and your private email - integration of data & communications *Inet phone calls - applications & services * ASP’s