Digital Forensics

Module 1
CS 996
Instructors

- Dr. Frederick Scholl
  - Office Hours: 5-6 PM, Wednesdays (by appointment)
  - E-mail: freds@monarch-info.com
  - Phone 212-869-4458
  - I am a technologist, not a lawyer!
- Kulesh Shanmugasundaram
- Professor Nasir Memon
Course Calendar

- Classes Start: January 26
- Presidents Day: February 21
- Mid-term Exam: March 9 (in class)
- March 23: Spring Break
- April 27: Last Class
- May 9-16: Final Exams
Grading

- Eight Labs (45%)
- Mid-term Exam (20%)
- Final Exam (20%)
- Class participation (5%)
- Class presentation (10%)
Reference Books

- Digital Evidence and Computer Crime, Casey
- Counter Hack, Skoudis
- Computer Forensics, Kruse
- Know Your Enemy (2004), Honeynet Project
- GigLaw Internet Law Guide, Isenberg
- Guide to Forensic Testimony, Smith
- Searching and Seizing Computers, USDOJ
My Background: Civil Litigation

- Help businesses reduce risk through Internet forensics
  - Web site trespassing
  - Network abuse
  - SLA disputes
  - Outsourcing disputes
  - Web site break-in
  - Porn in the workplace
  - Spam investigation
  - Patent infringement
- Testified in state and Federal courts
Outline of Lectures (Draft)

- Module 1: Applications of Forensics; Hard drives
- Module 2: Hard Drive Analysis; Investigating Email
- Module 3-4: Collecting Evidence from Hosts
- Module 5-6: Evidence Collection from Network Traffic
- Module 7: Evidence Collection from PDAs
- Module 8-9: Hard Drive Data Recovery
- Module 10-11: Using Commercial Tools: EnCase, MFP
- Module 12: Guest lecturer, FBI/NYPD
Today’s Lecture: The Big Picture

- Applications of Forensics
- Business and law enforcement drivers
- How forensics reduces risk and saves $$$ for businesses
- Where are business opportunities?
- Finding evidence on the Internet
What is Digital Forensics?

- Comes from Latin meaning: public forum
- “Network and computer testing and analysis done in support of litigation”
- Civil litigation
- Criminal litigation
- Homeland security: military tribunals
- “Internet Forensics”: http://www.acm.org/~hlb/edit/digital_village/aug-03/dv_8-03.html
Why is forensics important today?

- Willie Sutton, born in Brooklyn 1901
  - Why do I rob banks?
  - That’s where the money is!

![Bar chart showing GDP and Ecommerce growth from 2001 to 2003]
Why is Forensics Difficult?

- More information v. better analysis
- Information generated in 2002
  - 5 Exabytes (500,000 Libraries of Congress)
  - 92% stored on magnetic media
- Information communicated
  - 18 Exabytes (telephone, radio, TV, Internet)
  - 400,000 Terabytes (email)
  - 274,000 Terabytes (IM)
- http://www.sims.berkeley.edu/research/projects
SOURCES OF INFORMATION

- Hard Drive
- Registry & Content
- Router Syslog Files
- Email, IM, ETC
- Server Log Files
- Firewall Log Files
- Live Sniffer Data Collection
- ISP Records
- Internet Archives
- IP Investigations
- PDA's
Standards of Evidence

- Criminal Case
  - “Beyond a Reasonable Doubt”

- Civil Case
  - “Clear and Convincing Evidence”
  - “A Preponderance of the Evidence”

- Legal standards go beyond engineering standards
  - Technical: primary, backups
  - Legal: as many ways as possible
Challenges

- Evidence collection done in adversarial environment
- Judge and jury are not technical
- Commercial testing tools may not work
- Integrate business, technical and legal
- Definition of terms in legal world
Example: Legal vs. Engineering Practice

- Evidence must be admissible and stand up to cross examination
  - Current example: fingerprint analysis

- Case: ISP vs. Internet backbone provider
  - SLA dispute involving $100M
  - Ran independent tests measuring performance
  - Commercial software #1 failed to provide consistent data
  - Removed software; installed new test system
Forensics Procedures/Best Practices

- Few available
- Common Body of Knowledge: “Law, Investigation and Ethics”
- ISO 17799: System Auditing and Monitoring; not forensics
- Hot off the presses: NIST “Computer Security Incident Handling Guide”

Proactive and Reactive

- Proactive
  - “Detection is much more important than prevention. ...it is fundamentally impossible to prevent attacks. ...everything we know about complex systems tells us that we cannot find and fix every vulnerability. There will always be attackers; we just have to catch and punish them”. (Bruce Schneier, Secrets and Lies)

- Reactive
Proactive

- Prevent bad behavior like network abuse
- Sarbanes Oxley
  - Response to Enron
  - Companies must be able to acquire, search and preserve electronic data related to fraud
  - Effective July 20, 2002
  - Applies to public companies
Example: Consequences of Bad Behavior

- Eli Lilly disclosure of email addresses
- [www.prozac.com](http://www.prozac.com)
- Email went out with all addresses visible
- Consequence: FTC will monitor their security program for 20+ years+!!
Sarbanes Oxley

- Section 302: CEO’s, CFO’s certify financial reports. $5M fine; 20 years prison
- Section 404: ...”controls related to the prevention, identification and detection of fraud” (Technology Auditor position created)
- Risk: Inadequate control prevents financial auditor from signoff
Recent High Profile Cases

- Kobe Bryant: accuser’s SMS text messages recovered 4 months after sending
- Martha Stewart: changed message from “Peter Bacanovic thinks ImClone is going to start trading downward” to “Peter Bacanovic re: ImClone”
- Richard Scrushy: secret audio tapes will be admitted into evidence after defense challenges
High Profile Cases, cont.

- **www.sex.com**
  - 1994: Gary Kremen registers domain name with Network Solutions, Inc.
  - 1995: Stephen Cohen creates letter from Kremen authorizing domain name transfer to himself. Sends letter to NSI; they transfer name to him.
  - Cohen builds $250 million porn empire
  - Kremen sued; letter found to be forged; Cohen escapes to Mexico
  - 2004: Kremen settles suit with NSI
Recent Criminal Cases 18 U.S.C. § 1030—Federal Computer Fraud & Abuse Act

- **US v. Lamo**
  - Jan. 8, 2004
  - Entered NY Times web site; $300,000 damages
  - Hacker
- **US v. Baas**
  - Dec. 18, 2003
  - Stole customer data from Acxiom
  - Baas worked for outsourcer
Recent criminal cases, cont.

- **US v. Diaz**
  - Dec. 5, 2003
  - Remotely deleted critical programs; $80,000 damages to Hellman Logistics
  - Diaz was former IT employee

- **US v. Patterson**
  - Dec. 2, 2003
  - DOS attack against American Eagle Outfitters
  - Patterson was former employee

Homeland Security

- Need for more surveillance; Patriot Act
- Tension with privacy laws
  - HIPAA
  - GLB
  - Fourth Amendment covers government surveillance: “probable cause”
- Cyber-surveillance rules being redefined
  - Pen Register (outgoing calls)
  - Trap & Trace (incoming calls)
  - Wiretap (content)
Information Storage on Magnetic Media

- Hard drives
- Floppies
- USB memory devices
Erasing Magnetic Media

- **DOD 5220.22M**
- **Weak deletion:** OS level file removal
- **Block erasure:** overwrite *user accessible* blocks
- **Secure erase:** use ATA/SCSI drive commands
- **Physical destruction:** could recover using magnetic imaging
Lifecycle of Disk Drive

- Blank media
- Low level format
  - Performed at the factory
- Partition
- High level file system format
- Operating system install
- System operations
Low Level Format

- LLF done using factory software
- Low level formatting creates sectors
- Each sector holds 512 bytes + overhead bytes
- Overhead provides error correction and timing recovery
- Bad sectors remapped to redundant sectors by the HDD controller.
Low Level Format

- Sector Overhead
- 512 Bytes
- Redundant Sector
Partitioning Drive

- Master Boot Record = Master Boot Code + Master Partition Table (MPT)
  - Always at sector #1
- Volume Boot Record = Volume Boot Code + Disk Parameter Block
  - Each partition
Take Aways From This Module

- Many new career opportunities
  - Civil litigation
  - Corporate security + technology audit + risk management
  - Law enforcement
- Start to learn about legal issues
  - [http://cyberlaw.harvard.edu](http://cyberlaw.harvard.edu)
  - [www.gigalaw.com](http://www.gigalaw.com) (for non-lawyers)
References for Module 1

- http://mirror.href.com/thestarman
- http://cmrr.ucsd.edu
Understanding Cyberlaw Issues

- Sometimes I lie awake at night and ask: “Where have I gone wrong?”

- Then a voice out of the dark says to me, “This is going to take more than one night.”

Charlie Brown, Peanuts, Charles Schulz