Instructors

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

- Classes Start: January 16
- Presidents Day: February 16
- Mid-term Exam: March 15 (in class)
- April 5: Spring Break
- May 3: Last Class
- May 6-14: Final Exams
Grading

- Eight Labs (50%)
- Mid-term Exam (25%)
- Final Exam (25%)
Textbooks


- References
  - *Counter Hack*, Ed Skoudis Prentice Hall, 2002
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
- Module 2: Tracking Spam
- Module 3: Creating Forensic Ready Infrastructure
- Module 4: Evidence Collection from Network Traffic
- Module 5: Evidence Collection from Hosts
- Module 6: Host Investigation Using Encase
- Module 7: Evidence Handling, Reporting and Presentation in Court
Outline of Lectures, cont.

- Module 8: Evidence Collection from SIM Tools
- Module 9: Using Network Intelligence Private I
- Module 10: Investigating Cybercriminals—Guest lecturer NYPD or FBI
- Module 11:
- Module 12:
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
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 E-commerce growth from 2001 to 2003.](chart.png)
SOURCES OF INFORMATION

- HARD DRIVE
  - Registry & Content

- ROUTER SYSLOG FILES

- SERVER LOG FILES

- FIREWALL LOG FILES

- LICE SNIFFER DATA COLLECTION

- INTERNET ARCHIVES
  - ISP RECORDS

- IP INVESTIGATIONS
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
- 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
- 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 Criminal Cases 18 U.S.C. § 1030

- **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
Evidence on the Internet

- Web search
  - www.superpages.com
  - Google usenet listings
  - Archival sites

- Whois search
- Nslookup
- www.samspade.org
INTERNET ARCHIVE (WWW.ARCHIVE.ORG)

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Pages</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Date</td>
<td>Jan 25, 1999</td>
<td>*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

* denotes when site was updated.
JOHNSONS
FLOWER & GARDEN CENTERS

“Our Business Is Blooming” Since 1933

FAX your orders to us.
Our FAX number is 301-946-7633

1-800-BLOOMUSA

www.800bloomusa.com
www.johnsons.com

NORTHWEST DC:
4200 Wisconsin Ave, NW
(entrance on Van Ness St.)

202-244-6100

KENSINGTON:
10313 Kensington Parkway
Next to the Post Office

301-946-6700

GAITHERSBURG:
12201 Dumontown Road Route 28
& Quince Orchard Rd

301-948-5650

Fresh Cut Flowers  Blooming House Plants  Beautiful Floral Arrangements  Dried and Silk Flowers
Seeds  Bulbs  Fertilizers  Annuals  Perennials  Trees  Shrubs  Pottery  Herbs  Soils  Mulches

Copyright 1999  TomatoPages, LLC  All rights reserved
IDENTIFYING INTERNET RESOURCES

SmartWhois

IP, host, or domain: monarch-info.com

monarch-info.com

216.223.193.36

Monarch Information Networks, Inc.
28 West 44th Street
NY, NY 10036
US

Scholl, Frederick
fred@MONARCH-INFO.COM
Monarch Information Networks, Inc.
17 E. 45th Street, Suite 1009
NY, NY 10017-2415
US

Internet Channel
hostmaster@INCH.COM
180 Varick Street, 4th Floor
NY, NY 10014
US
OrgName: The Internet Channel
OrgID: INCH
Address: 180 Varick Street 10th Floor
City: New York
StateProv: NY
PostalCode: 10014
Country: US

NetRange: 216.223.192.0 - 216.223.223.255
CIDR: 216.223.192.0/19
NetName: INCH-BLK-1
NetHandle: NET-216-223-192-0-1
Parent: NET-216-0-0-0-0
NetType: Direct Allocation
NameServer: NS.INCH.COM
NameServer: NS2.INCH.COM
NameServer: AUTH-2.INCH.COM
Comment: ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate: 1999-04-30
Updated: 2001-09-06

TechHandle: ZI81-ARIN
TechName: Internet Channel
TechPhone: +1-212-243-5200
TechEmail: noc@inch.com

# ARIN WHOIS database, last updated 2004-01-25 19:15
# Enter ? for additional hints on searching ARIN's WHOIS database.