



Digital Forensics

Module 2
CS 996

Polytechnic
UNIVERSITY



Review from Module #1

- Forensics: Investigation in support of litigation
- Proactive vs. Reactive
 - Paul Kedrosky article WSJ 1/30/2004
- Start with Internet research
 - www.namebase.org



Investigating E-Mail

- Increasing volume of fraudulent email
 - Spam costs 0.01 cents/message to send!
- Virus propagation
- Spam in the workplace
- Increased successful prosecution of spammers!
- Deleting email



Characteristics of Email

- Why are investigations tough??
 - “Noone knows you are a dog on the Internet”
 - Must tie spam to actual sender or his agent
- Why are investigations feasible?



Sending Spam

- **Profile of NYC mass mailer**
 - 1 million messages/hour/server
 - Gig-E Internet connection; SQL backend
 - Call center: 45 people in Costa Rica
 - Product: herbal viagra
 - Many sophisticated programmers on staff



Spam Tools

- “Keep your enemies close”
- Robomail mass mailer
- Lencom email harvester
- www.paulgraham.com



Types of Email Exploits

- Denial of Service (DOS)
- Fraudulent spam
- Phishing scams
- Viruses
- Annoyance, stalking
- “Joe Jobbing”
- 419 Scams: Nigerian Bank Accounts
 - Still being used!!
 - www.scamorama.com

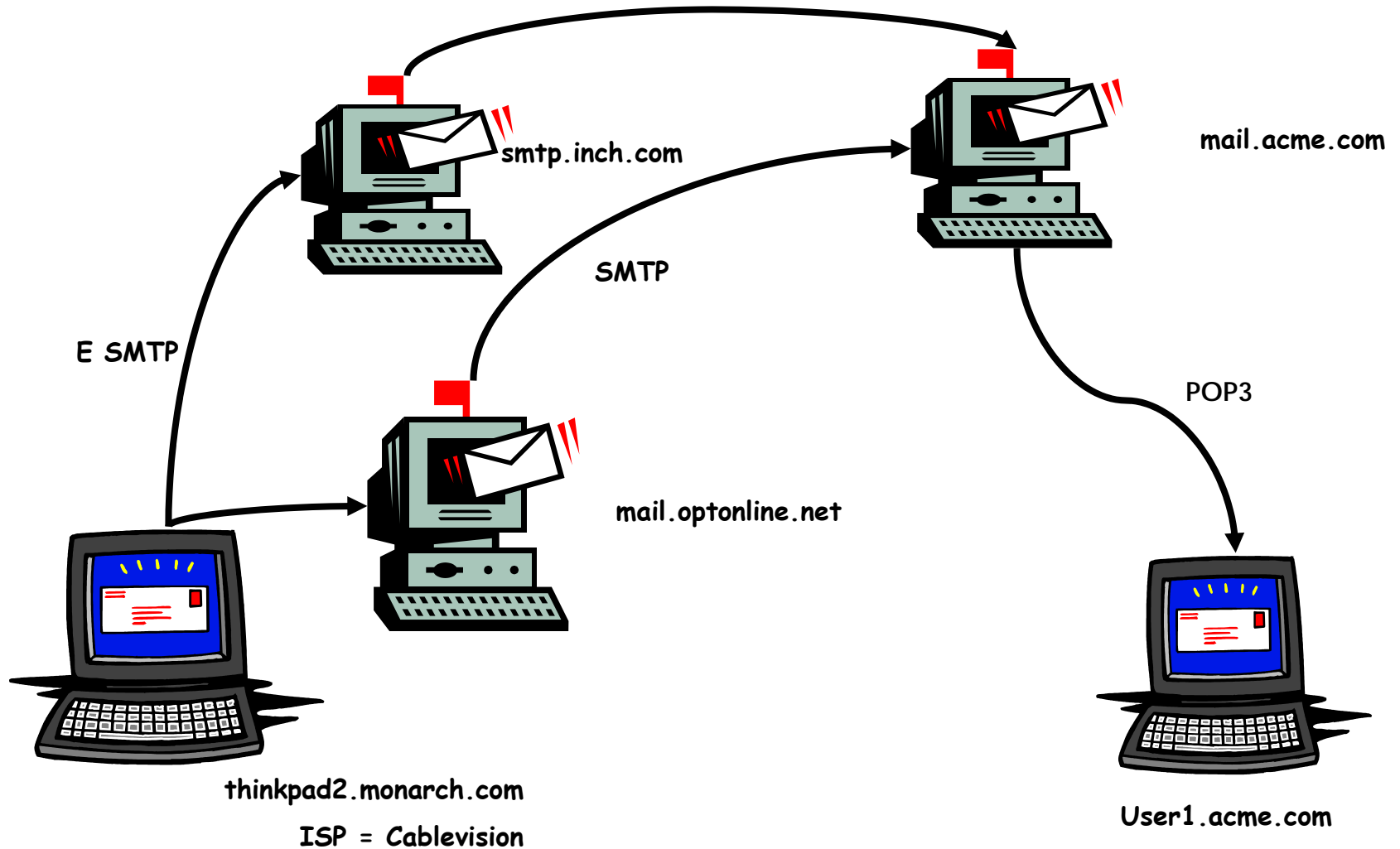


Email Phishing

- Serious threat of financial loss
- Newest, most damaging type of spam
- Rely on “social engineering”
- www.antiphishing.org



Message Transfer





Analyzing Message Headers

- *Envelope header information*
 - *Added by sender*
 - *Often forged*
- *Message Headers*
 - *Added by receivers*
 - *Use these for analysis*
- *Reference:*
www.stopspam.org/email/headers.html
- *[Sample message header](#)*



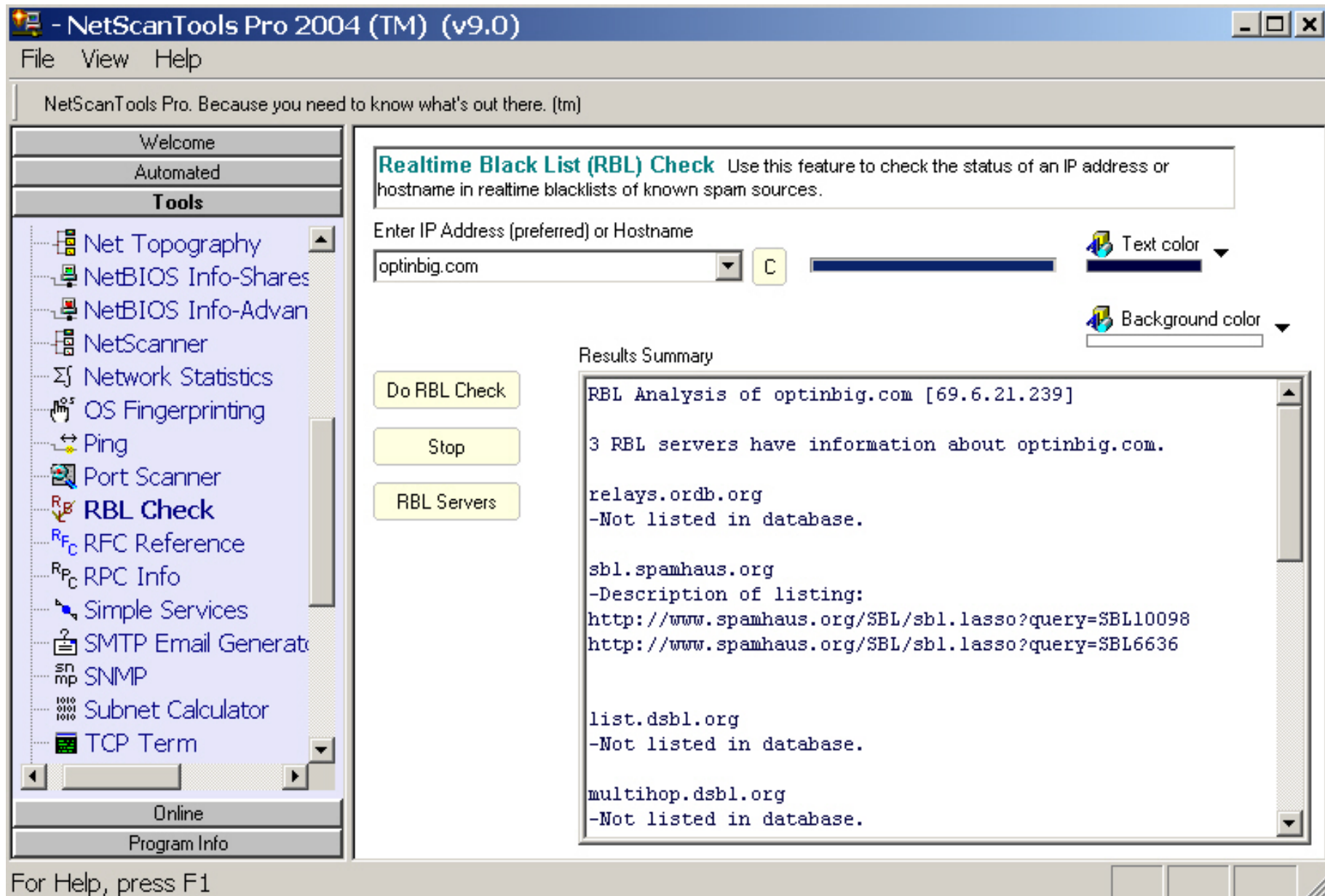
Sample SPAM Message Header

- Return-Path: <coleman@qwest.net>
- Received: from mx4.inch.com (mx4.inch.com [216.223.208.58])
 - by util.inch.com (8.12.10/8.12.10/UTIL-INCH-3.0.10) with ESMTP id i07AhNQs011147;
 - Wed, 7 Jan 2004 05:43:23 -0500 (EST)
 - (envelope-from coleman@qwest.net)
- Received: from pool-68-163-194-196.bos.east.verizon.net (pool-68-163-194-196.bos.east.verizon.net [68.163.194.196])
 - by mx4.inch.com (8.12.8p1/8.12.8/MXER-INCH-3.0.8) with SMTP id i07AhMF6071192;
 - Wed, 7 Jan 2004 05:43:22 -0500 (EST)
 - (envelope-from coleman@qwest.net)
- Received: from [80.11.104.75]
 - by pool-68-163-194-196.bos.east.verizon.net id vnXzM8nKRZZT;
 - Wed, 07 Jan 2004 15:35:11 +0500
- Message-ID: <10b\$9--9c\$hjd7o71p28-05@nm81.1j4aip1>
- From: "Tracey Porter" <coleman@qwest.net>
- Reply-To: "Tracey Porter" <coleman@qwest.net>
- To: freds@inch.com
- Subject: *****SPAM***** The tool Law



Internet Investigations: NetScan Tools

- www.nwpsw.com
- 34 tools grouped in one windows package
- For email
 - Traceroute (ICMP, TCP)
 - Relay testing
 - RBL (Real-time Block List) testing
 - Automated data collection across multiple tools



80.11.104.75

10

whois.ripe.net

.net
.12.1

167.206.3.218



Log



Log



Copy



Paste



Ping

.net
.12.1
DNS

Whois



IPBlock



Dig



Trace



Finger



SMTP



Time



whois 80.11.104.75@whois.ripe.net, finished

% See <http://www.ripe.net/ripenncc/pub-services/db/copyright.htm>

inetnum: 80.11.104.0 - 80.11.104.255

netname: IP2000-ADSL-BAS

descr: BSLYO110 Lyon Bloc1

country: FR

admin-c: WITR1-RIPE

tech-c: WITR1-RIPE

status: ASSIGNED PA

remarks: for hacking, spamming or security problems send mail to

remarks: postmaster@wanadoo.fr AND abuse@wanadoo.fr

mnt-by: FT-BRX

changed: gestionip.ft@francetelecom.com 20011011changed: gestionip.ft@francetelecom.com 20011128changed: gestionip.ft@francetelecom.com 20020605changed: gestionip.ft@francetelecom.com 20030318

source: RIPE

route: 80.11.0.0/17

descr: France Telecom

descr: Wanadoo France

remarks: -----

remarks: For Hacking, Spamming or Security problems

remarks: send mail to abuse@wanadoo.fr



Investigating Spammers on the Internet

- Spamhaus
 - IP lookup on suspect domain name
 - The Spamhaus Project
- Search on usenet
 - news.admin.net-abuse.*
 - Search for Scott Richter—2,040 entries



URL Obfuscation

- Mislead “victim” into clicking on attachment
- Reference: www.counterhack.net
- Some examples
 - <http://eer5673469d@www.monarch-info.com>
 - <http://www.microsoft.com@216.223.193.36>
 - [http://www.microsoft.com@
%77%77%77.monarch-info.com](http://www.microsoft.com@%77%77%77.monarch-info.com)

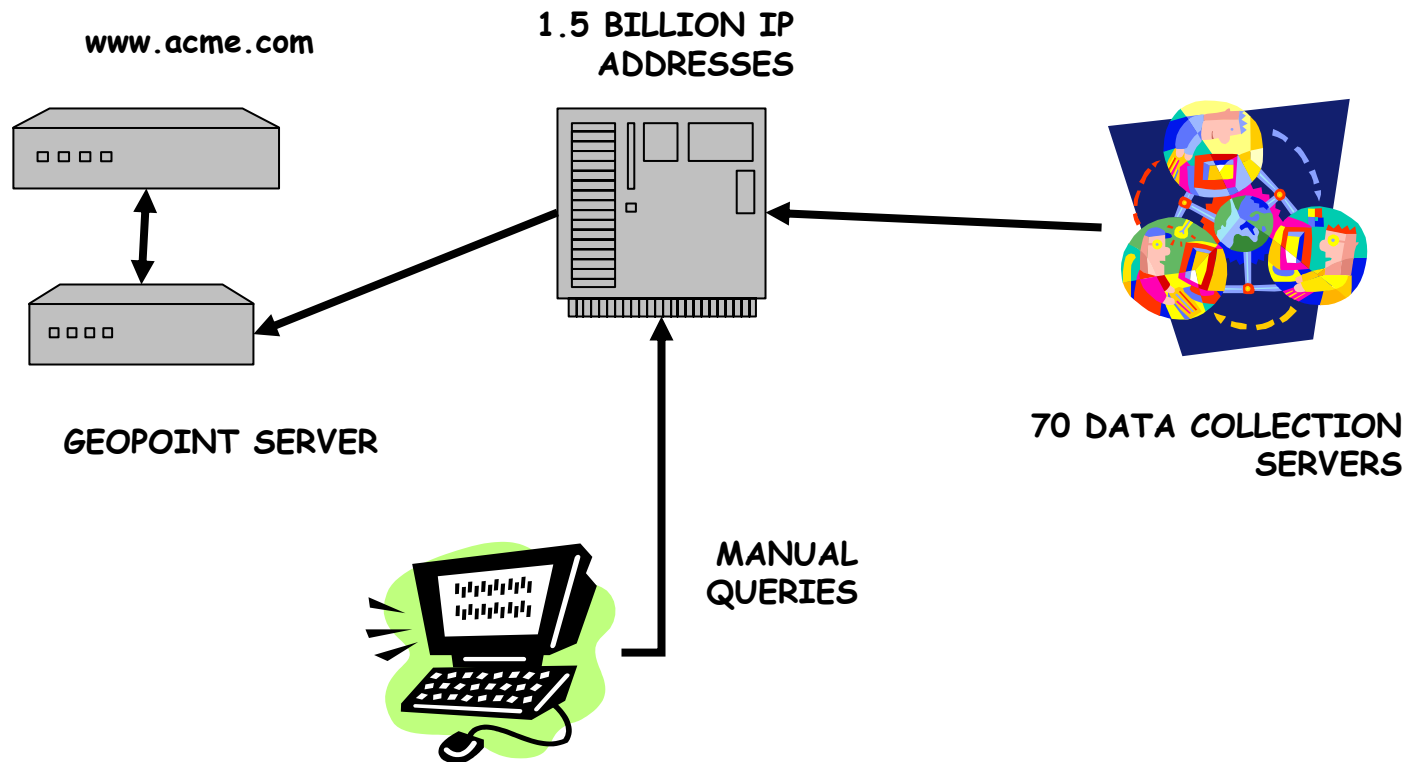


Geolocation

- Critical to forensic analysis on Internet
- Need to find a *person*!
- Commercial businesses
 - Use for high volume investigations
 - Infosplit (NYC)
 - Quova
- Fraud prevention in credit card applications



Quova Geopoint Architecture





Quova Geolocation Data

- **Location Data**
 - Continent, country, state, city, zip code
 - Latitude + longitude
- **Marketing Data**
 - DMA (Nielson Media Research)
 - MSA (Metropolitan Statistical Area)
- **Internet Connection**
 - ASN, carrier organization, domain
 - Connection type, speed, routing method



How Quova System Works

- US Patent # 6684250 (January 27, 2004)
- They use a *weighted average* to find best estimate of geographic location
 - Multiple traceroutes
 - DNS lookups
 - Whois information
 - Ping times
 - BGP tables
 - Regional Internet Registries (ARIN, RIPE, APNIC, LACNIC)



How Quova Works, cont.

- Local Internet Registries (KRNIC, JPNIC, etc.)
- You can learn from them and use their methods on individual addresses



Sample IP Addresses

- **66.8.129.0/24**
 - Registered in ARIN to Roadrunner, Herndon, VA
 - Hostname: a66b8n129client1.hawaii.rr.com
 - Traceroutes converge on:
 - Fas1-0-kauihi-kalaheo-ubr1.hawaii.rr.com
- **24.112.120.0/25**
 - Registered in ARIN to Rogers Cable, Toronto
 - Hostname: CPE002018d9dc11-CMO14340002240.cpe.net.cable.rogers.com
 - Traceroutes converge on
tlgw5.mtwx.phub.net.cable.rogers.com (mtwx = Scarborough, ON)



Sample IPs, cont.

- **209.198.199.0/25**
 - Registered to Interpacket, Santa Monica, CA
 - Traceroutes converge on Verestar router in Seattle (a satellite provider)
 - Research uncovers hostnames ending in carec.org= Caribbean Epidemiology Centre in Trinidad&Tobago
- **212.165.173.0/24**
 - Registered to New Skies Satellites in Netherlands
 - No hostname
 - Impossible to determine location: satellite connection could be anywhere

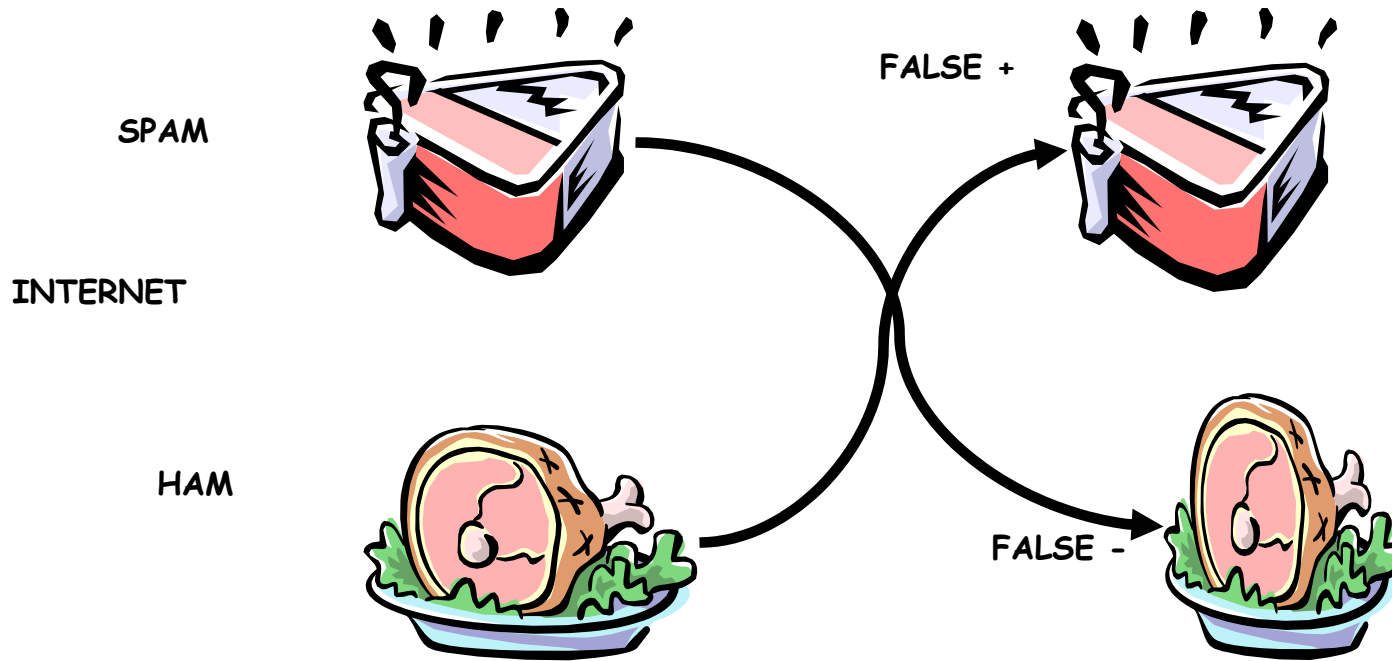


Fighting Spam

- www.spamconference.org
- Better filtering: Bayesian current hot approach
- Current systems: cocktail approach
- Stamps: cost in \$\$\$ or CPU time
- Tar pits
- RMX records (SPF=Sender Permitted From)



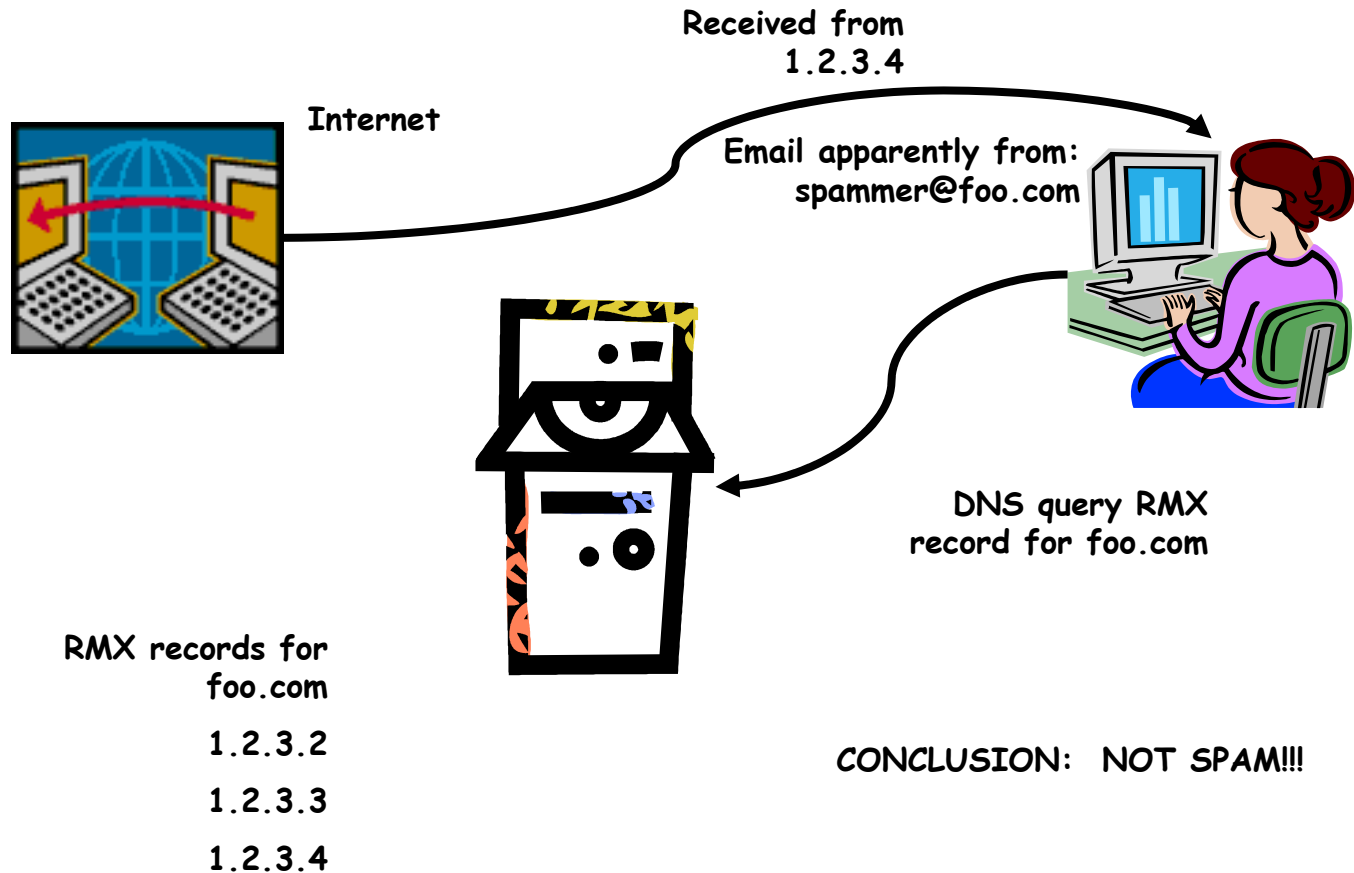
Filtering Spam



IMPLICATIONS FOR RETAILER....FOR HMO



Use of RMX Records





CAN-SPAM Bill: New Weapon for Investigators

- In effect Jan. 1, 2004
- www.spamhaus.org/legal/CAN-SPAM.html
- Preempts state anti-spam laws
- Applies only to commercial email
- Does not require opt-in



CAN-SPAM Do's

- **Accurate Headers**
 - From: line
 - Subject: line
 - Origin, routing, destination
- **Include opt-out address**
- **Include your real business address**
- **Clearly note that email is advertisement**
- **Mark sexually explicit material**



CAN-SPAM Don'ts

- Don't use harvested addresses
 - No dictionary attacks
 - No automated account signups
 - Don't use mail relays
-
- How much spam today is following these 9 rules??
 - Up to 5 years in jail



Deleting your Own E-Mail

- Your machine could be subpoenaed!
- Don't want to leave damaging evidence
- Keep personal email personal
- This process can be very tricky
 - Client storage
 - Exchange Server
 - Notes Server
- Many products don't work
 - Evidence Eliminator: no email delete!

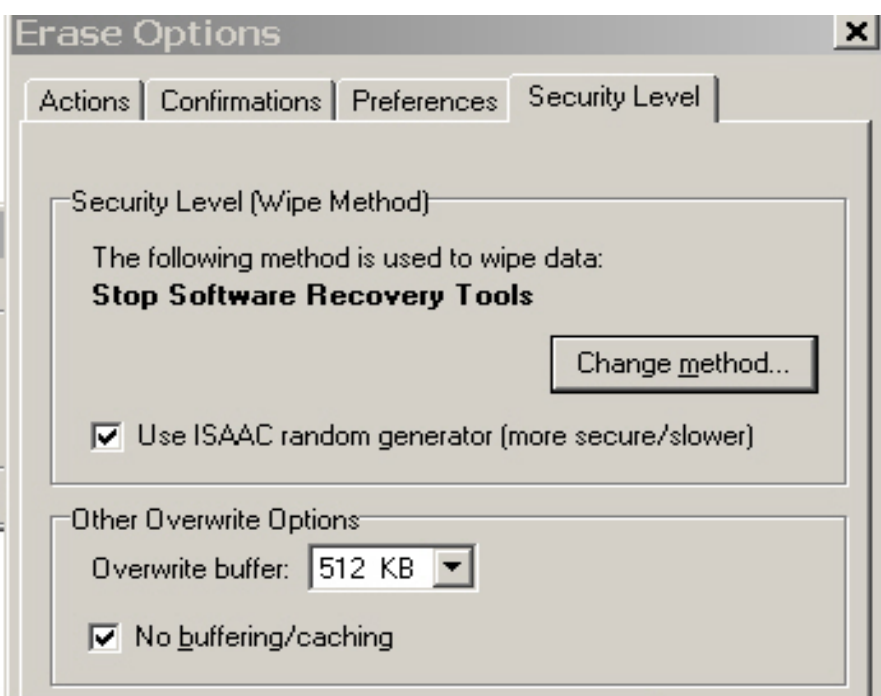
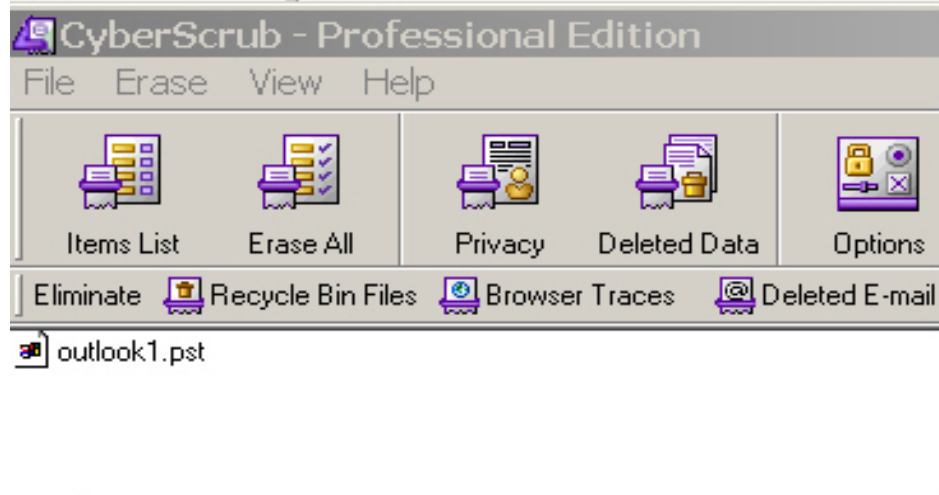


Deleting E-Mail: Outlook Client

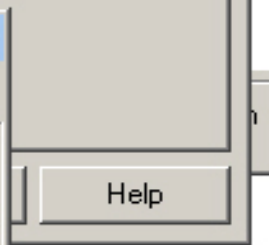
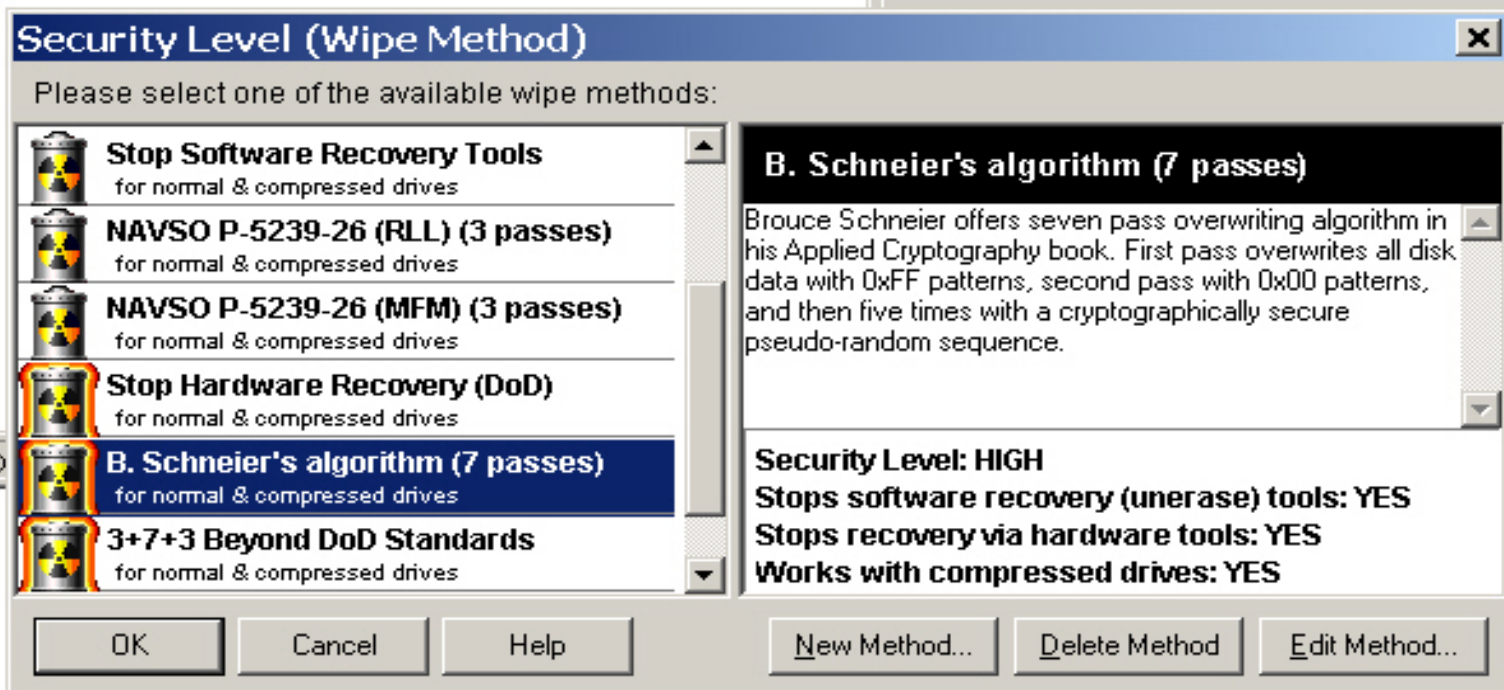
- **Method #1: Delete and scrub outlook.pst**
 - C:\documents and settings\user\localsettings\application data\microsoft\outlook\outlook.pst

- **Method #2:**
 - Empty delete bin
 - Compact outlook.pst file
 - Wipe remainder of disk

33)



1 ob



Data Files

Outlook stores your information on servers and in files on your computer. The list below shows the locations of your Outlook data. Click settings to see more information about a data store. Click Open Folder to display the file folder for your Outlook data. You must shutdown Outlook to move or copy these files.

[Tell me more...](#)

Name	Filename	Comment
Archive Folders	C:\Documents and Settin...	
Personal Folders	C:\Documents and Settin...	Mail delivery l...

[Settings...](#)[Open Folder...](#)

Personal Folders



General

Name:

Personal Folders

Filename:

C:\Documents and Settings\fscholl\Local Settings\Ap

Encryption:

Compressible Encryption

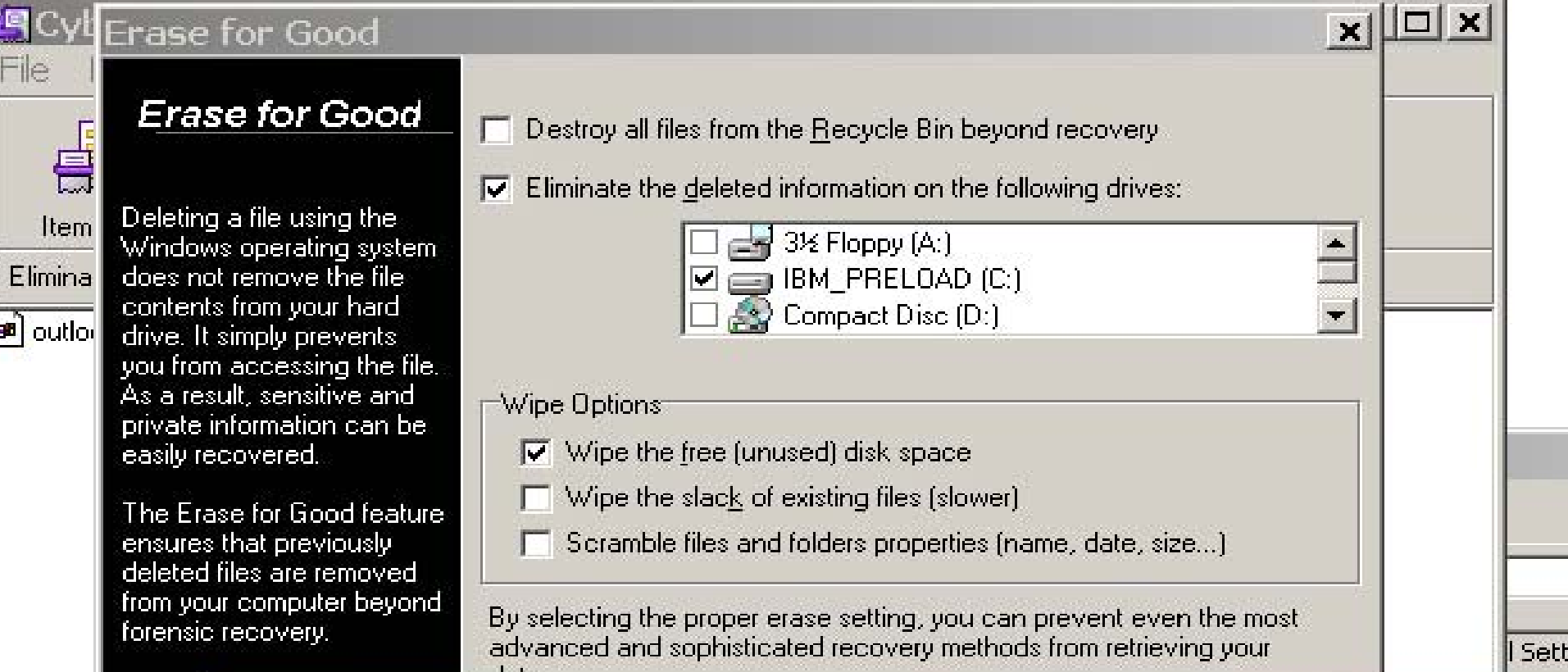
[Change Password...](#)

Changes the password used to access the personal folder file

[Compact Now](#)

Reduces the size of your personal folder file

Comment



Security Level (Wipe Method)

Please select one of the available wipe methods:

 **Quick Wiping (One Pass/No Check)**
for normal drives

 **Quick Wiping (One Pass/Check)**
for normal drives

 **Quick Wiping (Random Pass)**
for normal & compressed drives

 **Stop Software Recovery Tools**
for normal & compressed drives

 **NAVSO P-5239-26 (RLI) (3 passes)**
for normal & compressed drives

Stop Software Recovery Tools

Two pass wiping (one pass with random numbers and one pass with zeroes). Both passes are checked. Recommended if you only want to stop software recovery tools. Works with files on compressed drives.

Security Level: NORMAL

Stops software recovery (unerase) tools: YES



Interesting Lab Project

- Validate email delete process
 - Client side
 - Server side
- Use commercial delete programs: develop procedure
- Try to recover deleted email using EnCase