Review from Module #1

- Forensics:
  - Investigation in support of litigation
  - Investigation to avoid litigation

- Proactive vs. Reactive
  - Paul Kedrosky article WSJ 1/30/2004—"You’ve Got MyDoom"

- Hard Drive Analysis
Using Google Search for Investigations: Lab Assignment

- `inurl:viewerframe?mode=`
- Lists public “nannycams”
- Ref: Scott Bradner article, “Network World”
- Other resources
  - [http://johnny.ihackstuff.com](http://johnny.ihackstuff.com)
Hard Drive Data Hiding Places

- Low Level Format
  - Redundant sectors
  - Bad sectors

- Partition
  - Interpartition gaps
  - Unallocated space
  - “Hidden” partitions
  - Boot records and partition tables
  - Deleted partitions
Physical Disk Geometry (CHS)

- One head for each surface (H)
- All tracks at \( r = d_n \) form “cylinder” (C)
- Each sector has 512 bytes of user data (S)
- One disk surface devoted to positioning and synchronization
- Not all parts of the disk are addressable by the OS
- Disk capacity = \( C \times H \times S \times 512 \) bytes
- Applies to older drives!!
Example: IBM 2.5” 48GB Travelstar

- C = 16383, H = 15, 63 sectors/track, 512 B/sector (from drive label)
- Capacity = 8GB! Wrong!

- Logical Block Addressing (LBA)
  - Gets around 8GB BIOS limits
  - Numbers sectors sequentially 1…N
  - 48GB Travelstar: 93,759,120 LBA’s = 48GB
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

- 512 Bytes
- Sector Overhead
- Redundant Sector
Partitioning

- PARTITION #1
- PARTITION #2
- MASTER BOOT RECORD
- INTER-PARTITION GAP
- VOLUME BOOT RECORD
- VOLUME BOOT RECORD
Partitioning Windows 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
FAT File System

- **Types**
  - FAT12, 16, 32; cluster address size in bits
  - FAT1 and FAT2; first and second copy of File Allocation Table itself

- **Applications**
  - Floppy: FAT12
  - USB memory: FAT16
  - CF (Compact Flash): FAT12/16
FAT File System

- Four parts
  - Volume boot record
  - File allocation tables
  - Root directory
  - User data area
FAT12/16 Structure

- DOS BOOT SECTOR
- ROOT DIRECTORY
- FAT #1
- FAT #2
- USER DATA AREA
FAT32 Structure

- DOS BOOT RECORD (3)
- COPY OF DOS BOOT RECORD
- FAT #1
- FAT #2
- RESERVED SECTORS
- RESERVED SECTORS
- USER DATA
- 32 SECTORS
File Allocation Table

DIRECTORY ENTRY (32 BYTES)
- File Name
- First cluster address
- Length of data
- Other information

TEST
217

0

217
618

339
FFFF

618
339
WinHex: Forensic Hex Editor

- www.x-ways.net
- Disk cloning
  - DOS version
  - Windows version (use write blocker)
- Disk editor
- API for scripting tasks
2/02/2005 Module 2- Investigating Email
Navigating to FAT12 Directory

- Start at boot sector #1
- Add 2 x 9 sectors
- Directory at sector #20
- Offset is: $19 \times 512 = 9728$ bytes = $2600\text{H}$
Navigating to FAT32 Allocation Table

- Start at boot sector
- Go to sector #33, offset of 32 x 512 bytes
- $32 \times 512 = 16384 = 4000H$
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
  - Anonymizers hide spammers
- 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](http://www.paulgraham.com) (Bayesian filtering)
Recent Spam References

- www.spamconference.org (MIT, Jan 2005)
- http://spamkings.orielly.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
Dear freds@monarch-info.com

In response for your PayPal account security we have to report that your password may be is compromised. Your account is marked for too many successful logins last week (January, 18-25, 2005). It is more interesting that the hostnames are from different countries:

United States (c-67-160-224-80.client.comcast.net)
Canada (HSE-Toronto-ppp304429.sympatico.ca)
Sweden (c213-100-93-27.swipnet.se)
Russia (32.122-140-213.telenet.ru)

Your account is limited for security reasons.

Follow the link to make sure you are on a secure PayPal page and login with currently password. Please reauthorize your account information on or before **January 31, 2005**.

https://www.paypal.com/cgi-bin/webscr?cmd=login-run

Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the header of any page.

PayPal Email ID PP23897
Message Transfer

thinkpad2.monarch.com
ISP = Cablevision

smtp.inch.com
SMTP
Port 25

mail.acme.com
POP3
Port 110

User1.acme.com

mail.optonline.net
Block port 25

thinkpad2.monarch.com

ISP = Cablevision
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$9--9c$hjd7071p28-05@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
Realtime Black List (RBL) Check

Use this feature to check the status of an IP address or hostname in realtime blacklists of known spam sources.

Enter IP Address (preferred) or Hostname

optinbig.com

Results Summary

RBL Analysis of optinbig.com [69.6.21.239]

3 RBL servers have information about optinbig.com.

relays.ordb.org
- Not listed in database.

sbl.spamhaus.org
- Description of listing:
  http://www.spamhaus.org/SBL/sbl.lasso?query=SBL10098
  http://www.spamhaus.org/SBL/sbl.lasso?query=SBL6636

list.dsbl.org
- Not listed in database.

multihop.dsbl.org
- Not listed in database.
inetnum: 80.11.104.0 - 80.11.104.255
netname: IP2000-ADSL-BAS
descr: BSlyO110 Lyon Block
country: FR
admin-c: WITR1-RIPE
tech-c: WITR1-RIPE
status: ASSIGNED PA
remarks: for hacking, spamming or security problems send to:
remarks: postmaster@wanadoo.fr AND abuse@wanadoo.fr
mnt-by: FT-BRX
changed: gestionip.ft@francetelecom.com 20011011
changed: gestionip.ft@francetelecom.com 20011128
changed: gestionip.ft@francetelecom.com 20020605
changed: gestionip.ft@francetelecom.com 20030318
source: RIPE
route: 80.11.0.0/17
descr: France Telecom
descr: Wanadoo France
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
Geolocation

- Critical to forensic analysis on Internet
- Need to find a *person*!
- Commercial businesses
  - Use for high volume investigations
  - Infosplit (NYC—merged with Quova)
  - Quova
- Fraud prevention in credit card applications
- Other methods: www.the41stparameter.com
Quova Geopoint Architecture

www.acme.com

1.5 BILLION IP ADDRESSES

GEOPOINT SERVER

70 DATA COLLECTION SERVERS

MANUAL QUERIES
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

- 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-o-kauhihi-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
- Tarpits
- RMX records (SPF=Sender Permitted From)
Filtering Spam

IMPLICATIONS FOR RETAILER... FOR HMO
Use of RMX Records

Email apparently from: spammer@foo.com

Received from 1.2.3.4

DNS query RMX record for foo.com

RMX records for foo.com
1.2.3.2
1.2.3.3
1.2.3.4

CONCLUSION: NOT SPAM!!!
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
CAN SPAM Convictions

- None, so far
- Buffalo spammer—Howard Carmack
- Jeremy Jaynes
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
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Filename</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive Folders</td>
<td>C:\Documents and Settings\ Archive Folders</td>
<td></td>
</tr>
<tr>
<td>Personal Folders</td>
<td>C:\Documents and Settings\ Personal Folders</td>
<td>Mail delivery...</td>
</tr>
</tbody>
</table>

**Personal Folders**

- **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
Erase for Good

Deleting a file using the Windows operating system does not remove the file contents from your hard drive. It simply prevents you from accessing the file. As a result, sensitive and private information can be easily recovered.

The Erase for Good feature ensures that previously deleted files are removed from your computer beyond forensic recovery.

Erase for Good

Erase the deleted information on the following drives:

- [ ] 3½ Floppy [A:]
- [x] IBM_PRELOAD [C:]
- [ ] Compact Disc [D:]

Wipe Options:

- [x] Wipe the free (unused) disk space
- [ ] Wipe the slack of existing files (slower)
- [ ] Scramble files and folders properties (name, date, size...)

By selecting the proper erase setting, you can prevent even the most advanced and sophisticated recovery methods from retrieving your data.

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 (RLL) (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
  - WhiteCanyon
  - Blancco
- Try to recover deleted email using EnCase