Digital Forensics

Module 5
CS 996
More Investigating Windows

- Class action suits and forensics
- ADS and slack space
- Basic Windows investigations
- Hard drive properties
- Hard drive case study
- Disposal of hard drives
- HIPAA security legislation
Review of Module #4

- Strategy for digital evidence collection
  - Look at the whole sandbox
  - Multiple ways to prove case
  - KISS
- Sarbanes Oxley example
- Investigation Windows
  - Metadata
  - Registry
  - Logfiles
- Managing Windows graphics files
Sonus Networks Update

- Example of importance of data integrity!
- Lost $800M+ in market cap because of delay in filing Q4/2003 report
- Now: class action lawsuit filed against company 2/13/04
- Reference: www.bigclassaction.com
Petcurean Class Action

A class action lawsuit has been filed against Petcurean Pet Nutrition, Inc., and Pet Food Express, Ltd. on behalf of dog and cat owners throughout California whose pets died or suffered serious injuries after eating Go! Natural pet food. The suit alleges that the pet food, which was marketed as the 'healthiest pet foods in the world,' contained toxic substances. The suit further claims that the defendants were negligent in the manufacture, quality assurance, sale and distribution of Go! Natural pet food.
A class action lawsuit has been filed against Puppy Palace in Hollywood on behalf of customers who purchased their dogs from the store. The suit alleges that the dogs that came from the store had serious diseases, genetic disorders and other health problems. The suit is seeking reimbursement for the cost of the dogs, as well as any past or future veterinary bills, legal and investigation fees and an injunction to prevent the store from continuing to sell dogs.
Cablevision Class Action

Class action status is being sought in a lawsuit filed against Cablevision Systems Corp. on behalf of New York State consumers. The suit claims that the company conspired to defraud the plaintiffs by falsely accusing them of cable piracy. The suit alleges that the company tried to force some consumers to pay thousands of dollars to avoid litigation after claiming that they were using unauthorized cable-television decoder boxes. The suit claims that the company sent letters and phoned people who they suspected had purchased decoder boxes although they had no proof these people were stealing cable programming. The suit was filed on behalf of seven consumers who were accused of stealing cable, and although they denied the allegations, some agreed to pay the company between $2,000 and $6,000 to avoid mounting legal fees and the loss of cable service. Class action status is being sought in a lawsuit filed against Cablevision Systems Corp. on behalf of New York State consumers who claims that the company conspired to defraud them by falsely accusing cable piracy.
Overtime Lawsuits Are Increasing

- Class actions suits looking for back pay
- Based on Fair Labor Standards Act (1938)
- Exempt v. non-exempt
  - Exempt: manage two or more people; professionals; traveling salespeople
  - Non-exempt: hourly workforce
- Recent cases
  - Caribbean Cruises
  - Cost Plus
Connections With Forensics

- Examine business rules for pay calculation
- Examine database of employee time records and pay
- Could involve 100’s or 1000’s of employees going back in time!
- Remember: the other side will counterattack!
Issues from Module #3

- NTFS alternate data streams
- Swap space
NTFS Alternate Data Streams

- Method of hiding executables or proprietary content
- Uses NTFS file system multiple attributes
- Syntax---{file name}:{stream name}
- Create: type textfile > visible.txt:hidden.txt
- View: more < visible.txt:hidden.txt
- Reference: www.heysoft.de
  - LADS—List Alternate Data Streams
Create ADS

```
02/16/2004  04:00a   3,346 LADS_ReadMe.txt
02/28/2004  07:50p   2,579 research.txt
02/28/2004  08:14p    14 test.txt
       5 File(s)  67,379 bytes
       2 Dir(s)  33,728,952,320 bytes free

C:\TEMP\ads>type LADS_ReadMe.txt > test.txt: lads.txt

C:\TEMP\ads>dir
Volume in drive C is IBM_PRELOAD
Volume Serial Number is F831-00F1

Directory of C:\TEMP\ads
02/28/2004  08:27p    <DIR>
02/28/2004  08:27p    <DIR>
02/28/2004  06:33p    0 af ile.txt
02/16/2004  04:00a    61,440 lads.exe
02/16/2004  04:00a    3,346 LADS_ReadMe.txt
02/28/2004  07:50p    2,579 research.txt
02/28/2004  08:28p    14 test.txt
       5 File(s)  67,379 bytes
       2 Dir(s)  33,728,948,736 bytes free
```
Run LADS

```
02/28/2004 07:50p  2,579 research.txt
02/28/2004 08:28p  14 test.txt
  5 File(s)   67,379 bytes
  2 Dir(s)   33,728,948,736 bytes free

C:\TEMP\ads>lads

LADS - Freeware version 4.00
(C) Copyright 1998-2004 Frank Heyne Software (http://www.heysoft.de)
This program lists files with alternate data streams (ADS)
Use LADS on your own risk!

Scanning directory C:\TEMP\ads

size    ADS in file
----------
  14   C:\TEMP\ads\afile.txt:hidden.txt
    0   C:\TEMP\ads\test.txt:hidden
 3346   C:\TEMP\ads\test.txt:eads.txt
50960   C:\TEMP\ads\test.txt:np.exe
    0   C:\TEMP\ads\test.txt:stream

54320 bytes in 5 ADS listed
```
View Hidden Files

Command Prompt - more

```
14 C:\TEMP\ads\afile.txt:hidden.txt
 0 C:\TEMP\ads\test.txt:hidden
 3346 C:\TEMP\ads\test.txt:ladstxt
50960 C:\TEMP\ads\test.txt:np.exe
 0 C:\TEMP\ads\test.txt:stream

54320 bytes in 5 ADS listed
C:\TEMP\ads>more <test.txt:ladstxt
LADS - Freeware version 4.00
(C) Copyright 1998-2004 Frank Heyne Software (http://www.heysoft.de)
LADS lists the name and size of every alternate data stream (ADS) it finds in the specified directory (with or without subdirectories).
This software is provided "as is", without warranty of any kind!
Use it on your own risk!
Directory: directory to scan, current if omitted
/S    include Subdirectories
/D    Debug LADS (I hope you never need to use this option ;-) 
/U    Verbose error reports
/A    give a summary of All bytes used in the scanned directories
       (All files and directories are considered as uncompressed)
```
Additional ADS References

- http://patriot.net/~carvdawg/docs/dark_side.html
Swap Files in Windows

- Win2000 & WinXP
  - Pagefile.sys
  - C:\

- Win98
  - Win386.swp
  - C:\

Module 5-More Investigating Windows
Configure Virtual Memory (Win2000)
Create Win98 Boot Disk

Format - 3½ Floppy (A:)

Capacity:
1.44 Mb (3.5'')

Format type
- Quick (erase)
- Full
- Copy system files only

Other options
- Label:
- No label
- Display summary when finished
- Copy system files
View win386.swp in Hex Editor
NTFS Swap Files

- Use NTFSDOS to boot system
  - www.sysinternals.com
- View file with hex editor
Windows Investigation (Before Looking for Deleted Files!)

- Check application logs
  - C:\winnt\system32\config\appevent.evt

- Recently used documents
  - C:\Documents and Settings\User\Recent
  - Contains shortcuts to recently used files

- Programs from start > run menu
  - HKEY_CURRENT_USER\software\microsoft\windows\current version\explorer\RunMRU
More Windows Investigation

- Windows Temp Files
  - C:\WINNT\Temp
  - C:\Documents and Settings\User\Local Settings\Temp

- Find {Files, Computers, Text} Dialog Box
  - HKEY_CURRENT_USER\software\microsoft\Internet explorer\explorer bars\ID\Files Names MRU
    ComputerNamedMRU
    ContainingTextMRU
Module 5 - More Investigating
Windows
Browser Files

- AOL (v8; v9)
- MSN Explorer
- Netscape Navigator
- Opera (6.x,7.x)
- IE
  - C:\documents and settings\user\local settings\
    - History
    - Temporary Internet Files
  - C:\documents and settings\user\cookies
What Other Apps Are Being Run?

- Yahoo Messenger
  - Logs: `c:\program files\Yahoo!\messenger\profiles\user\archive`
  - Message cache: `c:\program files\yahoo!\messenger\cache`
- Investigate history for all apps
Investigating .chk Files

Hex Workshop - [FILE0000.CHK]

<table>
<thead>
<tr>
<th>Offset</th>
<th>Value</th>
<th>Compare Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>00001A7C</td>
<td>6C75 7469 6F6E 732E 636F 6D61A 0600 0600 0600 B802</td>
<td>lutions.com............</td>
</tr>
<tr>
<td>00001A90</td>
<td>0000 0000 0000 003C E240 0000 060C 636F 6465</td>
<td>n.Data Base Access S</td>
</tr>
<tr>
<td>00001AA4</td>
<td>6E6F 6C6C 2E63 6F6D 0661 436F 6465 666F 666C 6520</td>
<td>s, Inc..PO Box 69.Dover, NJ 07802-0</td>
</tr>
<tr>
<td>00001AB8</td>
<td>6563 686E 6F6C 6F67 7920 436F 7270 6F72 6174 6966F</td>
<td>069.US...Palazzi, Mi</td>
</tr>
<tr>
<td>00001ACC</td>
<td>6E6A 4461 7461 2042 6173 6520 4163 6365 7373 2053</td>
<td>chael.mikep@MICROAN</td>
</tr>
<tr>
<td>00001AED</td>
<td>7973 7465 6D73 2020 496E 632E 0A50 4F20 462F 7820</td>
<td>LYTIC.COM.Data Base</td>
</tr>
<tr>
<td>00001AF4</td>
<td>3639 0A44 6F76 6572 2C20 4E4A 2030 3738 3032 2D30</td>
<td>Access Systems, Inc.</td>
</tr>
<tr>
<td>00001B08</td>
<td>3036 390A 5553 0A06 8650 616C 617A 7A69 2C20 4D69</td>
<td>.PO Box 961.Dover, N</td>
</tr>
<tr>
<td>00001B1C</td>
<td>6368 6165 6C6A 6D69 6B65 7040 4D49 4352 4F41 4E41</td>
<td>J 07802-0961.US.973</td>
</tr>
<tr>
<td>00001B30</td>
<td>4C59 5449 432E 434F 4D0A 4461 7461 2042 6173 6520</td>
<td>-335-0800 973-335-19</td>
</tr>
<tr>
<td>00001B44</td>
<td>4163 6365 7373 2035 7973 7465 6D73 2C20 496E 632E</td>
<td>56..fValueWeb.hostma</td>
</tr>
<tr>
<td>00001B58</td>
<td>0A50 4F20 426F 7820 3936 310A 446F 7665 722C 204E</td>
<td><a href="mailto:ster@VALUEWEB.NET.Va">ster@VALUEWEB.NET.Va</a></td>
</tr>
<tr>
<td>00001B6C</td>
<td>4A20 2030 3738 3032 2D30 3936 310A 5553 0A39 3733</td>
<td>lueWeb.3250 West Com</td>
</tr>
</tbody>
</table>
| 00001B80 | 2D33 3335 2D30 3830 3020 3937 323D 3333 352D 3139 | 3/1/04

Module 5-More Investigating Windows

Ready Offset: 00000000 Value: 275 65536 by!
Don’t Forget

- Recycle bin!
- Windows search functions!
Windows Search Functions: Type

Select an item to view its description.

<table>
<thead>
<tr>
<th>Name</th>
<th>In Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>forensics_module4</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
<tr>
<td>forensics_module5</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
<tr>
<td>Microsoft PowerPoint Present</td>
<td></td>
</tr>
</tbody>
</table>

Search Options:
- Date
- Type
- Advanced Options

Look in:
- Local Harddrive (C:)

Search Now
Stop Search
More Search: Date Range

Search Results

Select an item to view its description.

<table>
<thead>
<tr>
<th>Name</th>
<th>In Folder</th>
</tr>
</thead>
<tbody>
<tr>
<td>THINKPAD INF...</td>
<td>C:\Documents and Settings\fscholl\Desktop</td>
</tr>
<tr>
<td>briganti_2002...</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
<tr>
<td>keating2.doc</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
<tr>
<td>spf.doc</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
<tr>
<td>DALE KUTNICK.doc</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
<tr>
<td>~$report.doc</td>
<td>C:\Documents and Settings\fscholl\My Documents</td>
</tr>
</tbody>
</table>

Search Options

- Date
  - Files Modified
  - in the last
    - 1 months
  - in the last
    - 1 days
  - between
    - 1/31/2004 and
    - 3/1/2004
Physical Hard Drive Parameters

- Sectors (512B)
- Total disk capacity = C x H x T
  - C = #cylinders/surface
  - H = # heads
  - T = #sectors/track
- H is a fictitious number; not really that many surfaces!
Physical Parameters

Partition Information - C: IBM_PRELOAD (NTFS)

Partition type: 07 (Hex) NTFS
Serial Number: F831: F1

First physical sector: 63 (Cyl 0, Hd 1, Sect 1)
Last physical sector: 91,823,759 (Cyl 6,072, Hd 239, Sect 63)
Total physical sectors: 91,823,696 (44,835.8 MB)
Physical Geometry: 6,201 Cyls, 240 Hds, 63 Sects
Windows Logical File Information

- FAT32 or NTFS
- Cluster: smallest logical unit on disk

<table>
<thead>
<tr>
<th>Drive Size</th>
<th>FAT32</th>
<th>NTFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>8-16GB</td>
<td>8KB</td>
<td>8KB</td>
</tr>
<tr>
<td>16-32GB</td>
<td>16KB</td>
<td>32KB</td>
</tr>
<tr>
<td>&gt;32GB</td>
<td>32KB</td>
<td>64KB</td>
</tr>
</tbody>
</table>
NTFS Information

Partition Information - C: IBM_PRELOAD (NTFS)

- NTFS Version: 3.0
- Bytes per NTFS sector: 512 (512 bytes per physical sector)
- Cluster size: 512 bytes (1 sectors per cluster)
- First MFT Cluster: 16
- File Record Size: 1 K bytes

---

- bytes in -- files (-- clusters)
- bytes unused in file clusters
- bytes in -- indexes (-- clusters)
- bytes reserved by system (-- clusters)
Where is the Data?

- Files
  - May contain stray data as well
- Slack space
  - In last cluster of file
  - File slack
  - RAM slack
- Unallocated blocks
  - Contain deleted data
- Unused partitions
- Boot track
Slack Space

- Sector Boundary
- Cluster Boundary
- End of File
- RAM Slack
- File Slack

512 B  |  512 B  |  512 B  |  512 B
Analyzing Slack Space

- Hex editors
- Forensic tools
  - Encase: FAT32 and NTFS
  - DriveSpy: only FAT32
  - NTI: only FAT32
Case Study

- Class v. AOL
- AOL v. St. Paul
- Problems with AOL 5.0
  - AOL 5.0 changed computer to prevent access to other ISPs
  - Installed its own dial up adapter (DUN)
  - Computers became unstable
  - Users had to reinstall Windows; lose data and applications
AOL v. St. Paul

- AOL sued to recover under its property damage insurance policy
- Issue: does damage caused by AOL software represent damage to tangible property
  - Computer is clearly tangible property
  - It is clearly damaged
  - Files on hard drive can be seen with hex editor or using microscopy
Federal Court System

- Trial courts: at least one per state
- New York has 4
  - Southern district
  - Northern district
  - Eastern district
  - Western district
- Appeals courts
  - 11 circuits
Federal Court of Appeals
Ruling by Fourth Circuit Court

- Damage not to tangible property
- Used example of combination lock with lost combination
  - What about electronic lock damaged by ESD?

What do you think?
Disposing of Hard Drives

- Garfinkel & Shelat Jan 2003
  (http://computer.org/security)
  - Tested 158 used hard drives
  - 9% sanitized
  - 64% mountable file systems
    - Found data entered at ATM machine
    - 3700 credit card numbers
    - Personal letters, email, etc.
# Recent Privacy Legislation Risks

<table>
<thead>
<tr>
<th>LEGISLATION</th>
<th>APPLIES TO</th>
<th>EFFECTIVE DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA SECURITY</td>
<td>HEALTH PLAN, CARE PROVIDER</td>
<td>APRIL 21, 2005</td>
</tr>
<tr>
<td>GRAMM LEACH BLILEY</td>
<td>BANKS, BROKER DEALERS, ETC.</td>
<td></td>
</tr>
<tr>
<td>NYS REG #173</td>
<td>INSURANCE FIRMS</td>
<td>JUNE 1, 2002</td>
</tr>
<tr>
<td>CAL SB 1386</td>
<td>DOING BUSINESS IN CALIFORNIA</td>
<td>JULY 1, 2003</td>
</tr>
</tbody>
</table>
HIPAA SECURITY STANDARDS

- Health Insurance Portability and Accountability Act (1996)
- Protects PII data
- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Safeguards
- Required/Addressable standards
HIPAA Forensic Requirements

- Security Incident Procedures
- Device and media disposal procedures
- Audit controls
Penalties for HIPAA Violations

- Fines against individuals and institutions
  - Non-compliance with standards: $100/occurrence up to $25,000
  - Willful disclosure of PII: up to $250,000
- Prison: 1-10 years
- Forfeiture of assets
- Biggest factor: loss of reputation!!
References for Module #5

- [www.brownstone.com](http://www.brownstone.com) (HIPAA)