Digital Forensics

Module 6
CS 996
Review from Module #5

- 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
Outline of Module #6

- Computer Fraud and Abuse Act (CFAA)
- Mock trial: McDanel vs. US
- More on Window search tools
- Network sniffing
- Review for midterm exam
CFAA

- Title 18 US Code § 1030
- 1984: protected only Federal computer installations
- 1996: amended to include all Internet computers (relatively late!!)
- Also have state laws against computer abuse
- (a)(2)(C) access computer *without authorization*; obtain *information* from protected computer; *interstate or foreign* communication
CFAA, continued

(a)(5)(A)
- Cause transmission of program, information, code or command; intentionally cause damage without authorization to protected computer
- Accessing protected computer without authorization; causing damage

(a)(5)(B)
- Loss during any 1-year period aggregating at least $5000 in value
CFAA Cases

- Shurgard Storage Centers v. Safeguard Self Storage
  - Employees emailed trade secrets to new employer
  - Employees said they were “authorized”
  - Court determined they were no longer authorized

- E.F. Cultural Travel v. Explorica
  - Student travel sites
  - Explorica scraped EF web site for fares
  - “Damage” = loss = lost business + goodwill
AA v. FareChase (2003)

- FareChase markets software to help browse travel web sites, including www.aa.com
- FareChase aggregates fare information
- AA sued to block access to its site
- Texas Penal Code § 33.02
  - “a person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner”.

"FareChase markets software to help browse travel web sites, including www.aa.com"
FareChase Proxy Architecture

FARECHASE

SERVER

INTERNET

TRAVEL AGENT

WWW.AA.COM

WWW.DELTA.COM

WWW.UNITED.COM
Analysis of Damage to Site

WEB SITE RESPONSE TIME

RESPONSE TIME (SEC.)

NUMBER OF DAILY USERS

0 200000 400000 600000 800000 1000000

0.00 2.00 4.00 6.00 8.00 10.00 12.00 14.00 16.00
McDanel v. United States

- Convicted under CFAA June 25, 2002
- Appealed to 9th Circuit Court of Appeals
dtsearch: Investigative Searching

- www.dtsearch.com
- Free evaluation
- Step #1: build document index of words
  - Index specific folders
  - Index entire harddrive!
- Step #2: run searches
Search Options

- Boolean
- Stemming: grammatical forms
- Phonic: sounds like
- Fuzzy: misspellings
- Synonyms
- Files filters: date, size, name, etc.
Monarch Information Networks was founded in 1991 to provide computer network testing services to Fortune 500 firms. Clients have included firms like JP Morgan Chase, United Technologies, McGraw-Hill, Dow Jones and many others. Services have expanded to encompass network testing and analysis for legal and business clients in support of litigation and business development.

Dr. Frederick Scholl founded Monarch after pioneering work at two fiber optic startups. He has authored or presented over 45 technical papers and holds 13 patents on network and fiber optic technology.
dtSearch: Email messages

<table>
<thead>
<tr>
<th>Name</th>
<th>Score</th>
<th>Hits</th>
<th>Location</th>
<th>Date</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW Very Sick Joke.rtf</td>
<td>44%</td>
<td>3</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>2,797</td>
</tr>
<tr>
<td>FW Humour.rtf</td>
<td>33%</td>
<td>2</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>2,160</td>
</tr>
<tr>
<td>FW Swedish Joke.rtf</td>
<td>33%</td>
<td>2</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>2,563</td>
</tr>
<tr>
<td>FW Fwd(3) White House internship Opportunities.rtf</td>
<td>33%</td>
<td>2</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>4,135</td>
</tr>
<tr>
<td>FW Dr. Seuss.rtf</td>
<td>33%</td>
<td>2</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>2,113</td>
</tr>
<tr>
<td>FW Funnies.rtf</td>
<td>44%</td>
<td>3</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>5,941</td>
</tr>
<tr>
<td>FW Candy Store.rtf</td>
<td>55%</td>
<td>4</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>248,035</td>
</tr>
<tr>
<td>FW Happy Valentines Day!.rtf</td>
<td>77%</td>
<td>6</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>616,033</td>
</tr>
<tr>
<td>FW Open Alone!!!.rtf</td>
<td>33%</td>
<td>2</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>70,986</td>
</tr>
<tr>
<td>FW 1.rtf</td>
<td>33%</td>
<td>2</td>
<td>D:\Grn</td>
<td>8/10/2001</td>
<td>2,160</td>
</tr>
</tbody>
</table>

dtSearch was not able to access the document 'D:\Grn\FW Very Sick Joke.rtf'.
dtsearch: Outlook .pst Files

Update Index

Index to update
- email2

Actions
- Index new or modified documents
- Clear index before adding documents
- Remove deleted documents from index
- Compress index after adding documents

Index information
- Location: C:\Program Files\dtSearch\UserD.
- Word count: 122
- Document count: 0
- Index size: 21 kb
- Percent full: 0%
- Last updated: ---

What to index

Filename filters

Exclude filters
- *.pdb *.pch *.opt *.lib "*\Deleted Items"*
- *.cab *.mov *.mp3

Start Indexing

Add folder... Add Outlook... Add file... Remove Add web... Clear list

Apply View log Help
SOURCES OF INFORMATION

- HARD DRIVE
- REGISTRY & CONTENT
- ROUTER SYSLOG FILES
- SERVER LOG FILES
- FIREWALL LOG FILES
- LIVE SNIFFER DATA COLLECTION
- ISP RECORDS
- IP INVESTIGATIONS
- INTERNET ARCHIVES
Network Sniffers

- Wildpackets Etherpeek: network engineers
- Eeye IRIS: user friendly
- Ethereal: free!
- Kismet (Linux): wireless and free!
- CommView (www.tamosoft.com)
- CommView for WiFi
Eeye IRIS Features

- Easy to use
- Reconstructs TCP sessions
  - Renders HTML content
- Filters
  - Usual IP, MAC, port, etc.
  - Word filters
- Does packet logging
  - No content
  - Pen register/trap and trace
### Did you know...

You can double-click on the adapter icon from status bar to open the Select Adapter dialog.
<table>
<thead>
<tr>
<th>No.</th>
<th>Date/Time (M.D.Y/h.m.s.m:s)</th>
<th>Client</th>
<th>Server</th>
<th>Client port</th>
<th>Server port</th>
<th>MAC client</th>
<th>B</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3/7/2004/12:45:16:192</td>
<td>PAVILION466</td>
<td>ad.doublecli...</td>
<td>3586</td>
<td>80</td>
<td>00:ED:2...</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>3/7/2004/12:45:18:906</td>
<td>PAVILION466</td>
<td>pagead2.go...</td>
<td>3594</td>
<td>80</td>
<td>00:ED:2...</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>3/7/2004/12:45:19:546</td>
<td>PAVILION466</td>
<td><a href="http://www.nytime">www.nytime</a>...</td>
<td>3595</td>
<td>80</td>
<td>00:ED:2...</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3/7/2004/12:45:16:041</td>
<td>PAVILION466</td>
<td>graphics7.n...</td>
<td>3583</td>
<td>80</td>
<td>00:ED:2...</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3/7/2004/12:45:15:661</td>
<td>PAVILION466</td>
<td><a href="http://www.nytime">www.nytime</a>...</td>
<td>3580</td>
<td>80</td>
<td>00:ED:2...</td>
<td>2</td>
</tr>
<tr>
<td>2</td>
<td>3/7/2004/12:45:16:041</td>
<td>PAVILION466</td>
<td>graphics7.n...</td>
<td>3582</td>
<td>80</td>
<td>00:ED:2...</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>3/7/2004/12:45:14:700</td>
<td>PAVILION466</td>
<td><a href="http://www.nytime">www.nytime</a>...</td>
<td>3579</td>
<td>80</td>
<td>00:ED:2...</td>
<td>9</td>
</tr>
<tr>
<td>2</td>
<td>3/7/2004/12:45:23:783</td>
<td>PAVILION466</td>
<td>crl.verisign.c...</td>
<td>3596</td>
<td>80</td>
<td>00:ED:2...</td>
<td>4</td>
</tr>
</tbody>
</table>

Content-Length: 1491
Accept-Ranges: bytes
Date: Sun, 07 Mar 2004 17:48:14 GMT
Connection: keep-alive

GET /images/article/bullet_blue.gif HTTP/1.1
Accept: */*

Did you know...
You can double-click on the adapter icon from status bar to open the Select Adapter dialog.
IRIS: Creating Filters

Edit filter settings

- Hardware filter
- Layer 2, 3
- Words
- MAC address
- IP address
- Ports
- Advanced

Keyword list
- nytimes

Insert keyword

- ALL
- ANY

Remove ->
Remove all

Mode
- Apply filter to packets
- Mark sessions containing keywords

Note: This filter is only Inclusive

OK Cancel Apply Help
<table>
<thead>
<tr>
<th>No</th>
<th>Timestamp</th>
<th>Type</th>
<th>Protocol</th>
<th>Source IP address</th>
<th>Dest IP address</th>
<th>Source port</th>
<th>Dest port</th>
<th>SEQ</th>
<th>ACK</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>17:22:13:546</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3645</td>
<td>1751904084</td>
<td>677907458</td>
<td>1427</td>
</tr>
<tr>
<td>2</td>
<td>17:22:13:546</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3639</td>
<td>1344281957</td>
<td>677908541</td>
<td>1514</td>
</tr>
<tr>
<td>3</td>
<td>17:22:13:546</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3639</td>
<td>1344283417</td>
<td>677908541</td>
<td>1514</td>
</tr>
<tr>
<td>4</td>
<td>17:22:13:546</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3639</td>
<td>1344284877</td>
<td>677908541</td>
<td>60</td>
</tr>
<tr>
<td>5</td>
<td>17:22:13:546</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3639</td>
<td>1344284877</td>
<td>677908541</td>
<td>1203</td>
</tr>
<tr>
<td>6</td>
<td>17:22:13:556</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3646</td>
<td>909283189</td>
<td>677907461</td>
<td>1514</td>
</tr>
<tr>
<td>7</td>
<td>17:22:13:556</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3646</td>
<td>909284649</td>
<td>677907461</td>
<td>1514</td>
</tr>
<tr>
<td>8</td>
<td>17:22:13:556</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3646</td>
<td>909286109</td>
<td>677907461</td>
<td>883</td>
</tr>
<tr>
<td>9</td>
<td>17:22:13:556</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3646</td>
<td>909286109</td>
<td>6779086109</td>
<td>60</td>
</tr>
<tr>
<td>10</td>
<td>17:22:13:727</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3639</td>
<td>1344286026</td>
<td>677907461</td>
<td>60</td>
</tr>
<tr>
<td>11</td>
<td>17:22:13:727</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3639</td>
<td>1344286026</td>
<td>677907461</td>
<td>60</td>
</tr>
<tr>
<td>12</td>
<td>17:22:13:727</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3639</td>
<td>1344286026</td>
<td>677907461</td>
<td>60</td>
</tr>
<tr>
<td>13</td>
<td>17:22:13:737</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3640</td>
<td>3591700843</td>
<td>677907461</td>
<td>718</td>
</tr>
<tr>
<td>14</td>
<td>17:22:13:737</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3640</td>
<td>3591700843</td>
<td>677907461</td>
<td>718</td>
</tr>
<tr>
<td>15</td>
<td>17:22:13:737</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3640</td>
<td>3591700843</td>
<td>677907461</td>
<td>717</td>
</tr>
<tr>
<td>16</td>
<td>17:22:13:737</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3640</td>
<td>3591700843</td>
<td>677907461</td>
<td>717</td>
</tr>
<tr>
<td>17</td>
<td>17:22:13:767</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3645</td>
<td>3591700843</td>
<td>677907461</td>
<td>1349</td>
</tr>
<tr>
<td>18</td>
<td>17:22:13:767</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3645</td>
<td>3591700843</td>
<td>677907461</td>
<td>1349</td>
</tr>
<tr>
<td>19</td>
<td>17:22:13:767</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3645</td>
<td>3591700843</td>
<td>677907461</td>
<td>1349</td>
</tr>
<tr>
<td>20</td>
<td>17:22:13:767</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3645</td>
<td>3591700843</td>
<td>677907461</td>
<td>1349</td>
</tr>
<tr>
<td>21</td>
<td>17:22:13:817</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3645</td>
<td>3591700843</td>
<td>677907461</td>
<td>1349</td>
</tr>
<tr>
<td>22</td>
<td>17:22:13:817</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3645</td>
<td>3591700843</td>
<td>677907461</td>
<td>1349</td>
</tr>
<tr>
<td>23</td>
<td>17:22:13:827</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3639</td>
<td>1344286026</td>
<td>677909206</td>
<td>885</td>
</tr>
<tr>
<td>24</td>
<td>17:22:13:847</td>
<td>IP TCP-&gt;</td>
<td>HTTP (A...</td>
<td>69.44.114.38</td>
<td>PAVILION466</td>
<td>80</td>
<td>3646</td>
<td>3646</td>
<td>867908124</td>
<td>909287662</td>
</tr>
</tbody>
</table>
Review of Course: Modules #1-6

- #1: Introduction to Forensics
- #2: Investigating Email
- #3: Email continued:
- #4: Investigating Windows systems
- #5: More investigating Windows
Introduction to Digital Forensics

- “Network and computer testing and analysis done in support of litigation”
  - Criminal litigation
  - Civil litigation
  - Homeland security

- Standards of Evidence
  - Criminal: “Beyond a reasonable doubt”
  - Civil: “Clear and convincing evidence” or “A preponderance of the evidence”
Laws and Regulations

- Sarbanes Oxley
  - Section 302: Certification of Financial Reports
  - Section 404: Financial controls
  - [www.guidancesoftware.com](http://www.guidancesoftware.com) white paper
  - Sonus Networks matter

- CFAA 18 USC 1030
Internet Investigations: Start Here

- www.superpages.com
- Google usenet listings
- www.archive.org
- www.samspade.org
- Geolocation services
  - www.networldmap.com
  - www.ip2location.com
- Teleport Pro (www.tencom.com)
  - Download website for future investigation, presentations
Email Exploits

- DOS
- Fradulent spam
- Phishing scams
  - www.antiphishing.org
- Joe Jobbing
Recent Email Case

- Shattuck v. Klotzbach
  - Superior Court, Mass., 12/11/2001
- Emails exchanged regarding real estate sale
  - Purchase price
  - 10% down payment
- Defendant argued that Statute of Frauds voided any sale: no written, signed contract
- Court ruled that sale could go through
  - Based on prior case law regarding telegrams
Spam Header Analysis

- Return-Path: <elva.newton_zv@vrflow.oulu.fi>
- Received: from euireland.ie ([218.50.116.179])
  by util.inch.com (8.12.10/8.12.10/UTIL-INCH-3.0.10) with SMTP id i06AvasC028574
  for <freds@inch.com>; Tue, 6 Jan 2004 05:57:42 -0500 (EST)
  (envelope-from elva.newton_zv@vrflow.oulu.fi)
- Message-ID: <0b8001c3d4c8$cb9e52ff$57e05367@euireland.ie>
- From: "Elva C. Newton" <elva.newton_zv@vrflow.oulu.fi>
- To: freds@inch.com
- Subject: *****SPAM***** 52,483 Bottles sold daily - SIZE MATTERS! 5 urdsusd
- Date: Wed, 07 Jan 2004 02:44:50 +0000
- MIME-Version: 1.0
More Spam

- Return-Path: <karina_dcl@hotmail.com>
- Received: from dyn-83-152-160-99.ppp.tiscali.fr (dyn-83-152-160-99.ppp.tiscali.fr [83.152.160.99])
  by util.inch.com (8.12.10/8.12.10/UTIL-INCH-3.0.10) with SMTP id i27MWrn0000518
  for <freds@inch.com>; Sun, 7 Mar 2004 17:32:55 -0500 (EST)
  (envelope-from karina_dcl@hotmail.com)
- Received: from hotmail.com (mx1.hotmail.com [65.54.166.99])
  by dyn-83-152-160-99.ppp.tiscali.fr (Postfix) with ESMTP id 72DB5E006D
  for <freds@inch.com>; Sun, 07 Mar 2004 15:36:45 -0800
- Reply-To: karlocal@hotmail.com
- From: "Headache P. Cypriots" <karina_dcl@hotmail.com>
- To: Freds <freds@inch.com>
- Subject: RE:cheergirl6969 would like to meet you online draft
- Date: Sun, 07 Mar 2004 15:36:45 -0800
Recent Spam is More Subtle

- Return-Path: <jr@greatlyimpacted.com>
- Received: from mail.greatlyimpacted.com (mail.greatlyimpacted.com [66.64.111.175])
  by util.inch.com (8.12.10/8.12.10/UTIL-INCH-3.0.10) with ESMTP id i27Lrf92082655
  for <fred@monarch-info.com>; Sun, 7 Mar 2004 16:53:41 -0500 (EST)
  (envelope-from jr@greatlyimpacted.com)
- Message-ID: <9A82F7D670384E15d092265e065e2617@greatlyimpacted.com>
- From: "HANK VANDERHULST JR" <hvanderhulst.jr@greatlyimpacted.com>
- To: "Frederick Scholl" <fred@monarch-info.com>
- Subject: Frederick, isn't your property supposed to be your strongest asset?
- Date: Sun Mar 07 16:54:04 2004 EST
SmartWhois (www.tamosoft.com)
Other Anti-Spam Techniques

- Search [www.spamhaus.org](http://www.spamhaus.org)
- newsgroups: news.admin.net-abuse.*

- CAN-SPAM bill
- Outlook metadata
  - view | currentview | customize | fields
  - Timeline and other information
Mail Retention? (Cyberscrub)

**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 Settings...**
- **Help**
- **Cancel**
- **Start**

**Erase for Good**

- Destroy all files from the Recycle Bin beyond recovery
- Eliminate the deleted information on the following drives:
  - 3½ Floppy (A:)
  - IBM_PRELOAD (C:)
  - Compact Disc (D:)

**Wipe Options**

- 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.
MetaData in Office Documents

- Revision history
- Document authors
- Document changes
- Custom fields that you may have added!

- Use in investigations
- MetaData Assistant: www.payneconsulting.com
Content Search Products

- DolphinSearch (www.dolphinsearch.com)
- Platformedia (www.platformedia.com)
- WizSoft (www.wizsoft.com)
- Dtsearch (www.dtsearch.com)
  - Great product!
Guidelines for Collecting Evidence

- Dig up the entire sandbox
- Find multiple ways to prove your point
- KISS: Keep It Simple Stupid
Investigating Windows Systems

- Basic
  - Application log files
  - Temp files
  - Recently used documents
  - Recycle bin
  - History + temporary Internet files

- Registry

- Hidden Files
  - ADS
  - .chk files
  - Swap space
Investigating the Registry

- Registrar Lite editor (free at www.resplendence.com)
- Investigate old user names
- Most recently used files
- Recent searches for files
NTFS Alternate Data Streams

- Method of hiding exec files or content
- W2k.stream “proof of concept” virus
- Uses NTFS Master File Table (MFT) Structure

File #1          Time Security..  ADS Pointer #1
File #2          Time Security..  ADS Pointer #2

. .

File #N          Time Security ...............
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 <DIR>   0 afiile.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

Command Prompt

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:kids.txt
 50960 C:\TEMP\ads\test.txt:np.exe
    0  C:\TEMP\ads\test.txt:stream

54320 bytes in 5 ADS listed

C:\TEMP\ads>
**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:ldas.txt
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:ldas.txt
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 ;-) 
/V 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](http://patriot.net/~carvdawg/docs/dark_side.html)
Where Else 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

Polytechnic University

3/8/04  Module 6
Analyzing Slack Space

- Hex editors
- Forensic tools
  - Encase: FAT32 and NTFS
  - DriveSpy: only FAT32
  - NTI: only FAT32
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
References for Module #6

- www.brownstone.com (HIPAA)