Digital Forensics

Module 6
CS 996
Module #5 Covered

- B of A case; corporate responsibility for security
- New security standards: NIST 800-53 and ITIL
- Another new security standard: ISF “Standard of Good Practice” (January, 2005)
- Using EnCase
- Basic Linux forensics commands
Outline of Module #6

- SamSpade Presentation
- Discussion re Infragard meeting
- Recent host forensic case in the news

- Host forensics, continued
  - Linux
  - Windows

- Don’t forget vacation next week 😊
Infragard: Takeaways

- Cross-validation between tools
- Documentation!!
- Tools
  - www.networkview.com network discovery
  - www.firehand.com image analysis
- Business issues
  - Kruse: “main business is intellectual property related”
Intellectual Property Theft

- “Fakes!” BusinessWeek, 2/7/2005
- Counterfeit products = $500+B/year!!
- Forensic opportunities
  - Uncovering evidence of IP theft
  - Reverse engineering computer products to determine if they are real or not
  - Developing countermeasures
Today's Email

- Incredible replica watches in stock
- Get a first-class Rolex watch
- We only sell top-notch watches and handbags. There's no battery in these replicas just like the real ones since they charge themselves as you move. The second hand moves JUST like the real ones, too. These original watches sell in stores for thousands of dollars. We sell them for much less.

- Our Rolex are:
  - Replicated to the smallest detail
  - 98% Perfectly Accurate Markings
  - Signature Green Sticker w/ serial number on watch back
  - Magnified Quickset Date
  - Includes all Proper Markings

- Please copy and paste the following link into your browser to learn more.

- Link to website - ->> elitereplicasonline.com
Ohio v. Morris (2/16/2005)

- Morris, Jr. finds child porn on his computer after seeing Morris, Sr. using computer
- Computer sent to lab; imaged and analyzed using EnCase. Viewed images; ran keyword searches (“preteen lolita”, etc.)
- Hard drive overwritten at lab!
- Convicted of pandering child porn
- Morris appeals
Appeals Contentions

- Denied “Due Process” because original evidence was deleted
- Claims images were “virtual”
- Were images really “minors” or possibly his own children or wards?
Open Source Forensic Tools

- Sleuthkit (v2.0)
- Autopsy (Sleuthkit with browser interface)
- Knoppix (includes forensic tools)
- Helix-Knoppix + forensic utilities
Using Open Source Forensic Tools

- Great for learning and research
- Great for background investigations
- Will be subject to attack if used in court
  - Autopsy/Sleuthkit: not used in US courts (Carrier)
- Exception: SMART (www.asrdata.com), a commercial product--$2000
  - Used in many investigations, including Enron
What Drives Are on Host?

```
ide1: BM-DMA at 0xffa8-0xffaf, BIOS settings: hdc:DMA, hdd:pio
hda: HDS722580ULAT20, ATA DISK drive
hdb: WDC WD400BB-75JHAA, ATA DISK drive
hdc: HL-DT-ST RW/DVD GCC-4481B, ATAPI CD/DVD-ROM drive
hda: max request size: 1024Kib
hda: 156250000 sectors (80000 MB) w/1794Kib Cache, CHS=16383/255/63, UDMA(33)
hda: cache flushes supported
  hda: hda1 hda2 hda3
hdb: max request size: 128Kib
hdb: 78125000 sectors (4000 MB) w/2048Kib Cache, CHS=65535/16/63, UDMA(33)
hdb: cache flushes supported
  hdb: hdb1 < hdb5 hdb6 hdb7
swsusps: Resume From Partition: /dev/hda2
ReiserFS: hda3: found reiserfs format "3.6" with standard journal
ReiserFS: hda3: using ordered data mode
ReiserFS: hda3: journal params: device hda3, size 8192, journal first block 18,
  max trans len 1024, max batch 900, max commit age 30, max trans age 30
ReiserFS: hda3: checking transaction log (hda3)
ReiserFS: hda3: Using r5 hash to sort names
Adding 1036184k swap on /dev/hda2. Priority:42 extents:1
hdc: ATAPI 48X DVD-ROM CD-R/RW drive, 2048kB Cache
SCSI device sda: 512000 512-byte hdwr sectors (262 MB)
e100: eth0: e100_watchdog: link up, 100Mbps, half-duplex
dell3000:~ #
```
Add Image to Autopsy

1. **Location:** The full path (starting with /) to the raw file system image.
   
   `/root/evidence/testfile2.dd`

2. **Import Method:** The image can be imported into the Autopsy Evidence Locker from its current location by making a symbolic link, by copying it, or by moving it. Note that if a system failure occurs during the move, then the image could become corrupt.
   
   - Symlink
   - Copy
   - Move

3. **File System Type:** Specify the type of file system.
   
   [linux-ext2]

4. **Mount Point:** The directory or drive where the file system was mounted in the original suspect system (i.e. C:\ for Windows or /usr/ for UNIX). Not needed for swap or raw file system types.
   
   - other
   - other: __________

5. **Data Integrity:** An MD5 hash can be used to verify the integrity of the file system image.
   
   - Calculate the hash value for this image.
   - Ignore the hash value for this image.
   - Add the following hash value for this image:
     
     `cbe0a562c33f3094f7f04a53ce6a5b`
   - Verify MD5 After Importing?
Autopsy Evidence Folder
CONTENT INFORMATION
Block Range: 0 - 26096
Block Size: 4096
Free Blocks: 25263

BLOCK GROUP INFORMATION
Number of Block Groups: 1
Inodes per group: 26112
Blocks per group: 32768
Group: 0:
Inode Range: 1 - 26112
Block Range: 0 - 26096
Layout:
Super Block: 0 - 0
Group Descriptor Table: 1 - 1
Data bitmap: 2 - 2
Inode bitmap: 3 - 3
Inode Table: 4 - 819
Data Blocks: 820 - 26096
Free Inodes: 26098 (99%)
Free Blocks: 25174 (76%)
Total Directories: 2
**File Analysis**

### Directory Seek

Enter the name of a directory that you want to view:

```
/show/evidence2/
```

### File Name Search

Enter a Perl regular expression for the file names you want to find:

### Current Directory: `/mnt/evidence2/`

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Modified</th>
<th>Accessed</th>
<th>Changed</th>
<th>Size</th>
<th>UID</th>
<th>GID</th>
<th>Meta</th>
</tr>
</thead>
<tbody>
<tr>
<td>dir</td>
<td><code>/</code></td>
<td>2005.03.14</td>
<td>2005.03.14</td>
<td>2005.03.14</td>
<td>4096</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>dir</td>
<td><code>/d</code></td>
<td>2005.03.14</td>
<td>2005.03.14</td>
<td>2005.03.14</td>
<td>4096</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0000.00.00</td>
<td>0000.00.00</td>
<td>0000.00.00</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>dir</td>
<td><code>/lost+found/</code></td>
<td>2005.02.26</td>
<td>2005.02.27</td>
<td>2005.02.26</td>
<td>49152</td>
<td>0</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14:54:10 (PST)</td>
<td>13:40:51 (PST)</td>
<td>14:54:10 (PST)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dir</td>
<td><code>/r</code></td>
<td>2005.02.21</td>
<td>2005.03.14</td>
<td>2005.03.14</td>
<td>195486</td>
<td>0</td>
<td>0</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td>18:33:27 (PST)</td>
<td>20:37:18 (PST)</td>
<td>20:36:57 (PST)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dir</td>
<td><code>/r</code></td>
<td>2005.02.20</td>
<td>2005.03.14</td>
<td>2005.03.14</td>
<td>159085</td>
<td>0</td>
<td>0</td>
<td>13</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14:07:20 (PST)</td>
<td>20:37:07 (PST)</td>
<td>20:36:40 (PST)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dir</td>
<td><code>/r</code></td>
<td>2005.02.27</td>
<td>2005.03.14</td>
<td>2005.02.27</td>
<td>14</td>
<td>0</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13:41:49 (PST)</td>
<td>20:38:56 (PST)</td>
<td>13:41:49 (PST)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ASCII (display - report) * ASCII Strings (display - report) * Export * Add Note

File Type: ASCII text, with no line terminators
Inode Contents

Inode Number: 13

Pointed to by file:
/mnt/evidence2/snapshot1.jpg

File Type:
JPEG image data, JFIF standard 1.01

MD5 of content:
40cbb3c52517a7fd68a9c874754a6425

SHA-1 of content:
87783804351aad2330f8e653f8c0f69983d2446e

Details:
inode: 13
Allocated
Group: 0
Generation Id: 4284695194
uid / gid: 0 / 0
mode: -rw-r--r--
size: 159085
num of links: 1

Inode Times:
File Modified: Sun Feb 14 07:20 2005
Inode Modified: Mon Mar 14 20:36:40 2005

Direct Blocks:
2048 2049 2050 2051 2052 2053 2054 2055
2056 2057 2058 2059 2061 2062 2063 2064
2065 2066 2067 2068 2069 2070 2071 2072
2073 2074 2075 2076 2077 2078 2079 2080
2081 2082 2083 2084 2085 2086 2087
Activity Timeline

File Activity Timelines

Here you can create a timeline of file activity.
This process requires two steps:

1. Create Data File from file system data
   -> 2. Create Timeline from the data file

Use the tabs above to start.
### Timeline Results

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Name</th>
<th>Permissions</th>
<th>Size</th>
<th>Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sun Feb 20</td>
<td>14:07:20</td>
<td>159085 m.</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td>/mnt/evidence2/snapshot1.jpg</td>
</tr>
<tr>
<td>Mon Feb 21</td>
<td>18:33:27</td>
<td>195486 m.</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td>/mnt/evidence2/nytimes.jpg</td>
</tr>
<tr>
<td>Sat Feb 26</td>
<td>14:54:10</td>
<td>49152 m.c</td>
<td>-drwxr-xr-x</td>
<td>0</td>
<td>/mnt/evidence2/lost+found</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 mac</td>
<td>------------</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sun Feb 27</td>
<td>13:40:51</td>
<td>49152 .a.</td>
<td>-drwxr-xr-x</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Sun Feb 27</td>
<td>13:41:49</td>
<td>14 m.c</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Mon Mar 14</td>
<td>20:36:40</td>
<td>159085 ..c</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Mon Mar 14</td>
<td>20:36:57</td>
<td>195486 ..c</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Mon Mar 14</td>
<td>20:37:07</td>
<td>159085 .a.</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Mon Mar 14</td>
<td>20:37:18</td>
<td>195486 .a.</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Mon Mar 14</td>
<td>20:38:49</td>
<td>33 m.</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td>&lt;testfile2.dd-Alive-1&gt;</td>
</tr>
<tr>
<td>Mon Mar 14</td>
<td>20:38:56</td>
<td>14 .a.</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td>&lt;testfile2.dd-Alive-1&gt;</td>
</tr>
<tr>
<td>Mon Mar 14</td>
<td>20:39:04</td>
<td>33 .a.</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td>&lt;testfile2.dd-Alive-1&gt;</td>
</tr>
<tr>
<td>Mon Mar 14</td>
<td>20:39:15</td>
<td>33 ..c</td>
<td>-r-w-r-r-</td>
<td>0</td>
<td>&lt;testfile2.dd-Alive-1&gt;</td>
</tr>
</tbody>
</table>
Linux MAC Times

- **Modify time (mtime)**
  - Last time file was written to or appended to
  - For directory: time when file was added, deleted or renamed

- **Access time (atime)**
  - Last time file/directory was read
  - Can turn off with “noatime” option

- **Change time (ctime)**
  - Alter file attributes (inode) or content
Win32 MAC Times

- Modify time
  - Time when file is last modified. Carried over when file is copied to new directory

- Access time
  - Time when file was last accessed by application program

- Create time
  - Time when file was created in the current directory. New value is set when file is copied
MAC Time Example

- IIS file: graphic.jpg
- Observations made on 3/15/2005
  - Created: 2/14/2005
  - Modified: 1/20/2005
  - Accessed: 3/15/2005
- What happened?
## Internet Temp File Time Stamps

### Temporary Internet Files

This folder contains all the Web sites you have visited recently. The addresses are copied to this folder, which is also known as a cache. If you visit the sites again, they load faster.

To increase disk space, in the Internet control panel, on the **General** tab, click **Delete Files** to empty the folder. To adjust the amount of space the Temporary Internet Files folder uses on your hard disk, click **Settings**.

Select an item to view its description.

<table>
<thead>
<tr>
<th>Name</th>
<th>Expires</th>
<th>Last Modified</th>
<th>Last Accessed</th>
<th>Last Checked</th>
</tr>
</thead>
<tbody>
<tr>
<td>%3FLinkID%3D1043051</td>
<td>None</td>
<td>1/21/2005 2:46 PM</td>
<td>3/14/2005 6:10 PM</td>
<td>3/14/2005 6:11 PM</td>
</tr>
<tr>
<td>$brecs_per_page=20</td>
<td>None</td>
<td>None</td>
<td>3/14/2005 4:20 PM</td>
<td>3/14/2005 4:20 PM</td>
</tr>
<tr>
<td>$brecs_per_page=20</td>
<td>None</td>
<td>None</td>
<td>3/14/2005 4:20 PM</td>
<td>3/14/2005 4:20 PM</td>
</tr>
<tr>
<td>?inode=357</td>
<td>None</td>
<td>None</td>
<td>3/16/2005 7:05 AM</td>
<td>3/16/2005 7:05 AM</td>
</tr>
<tr>
<td>?r=mzorg1</td>
<td>None</td>
<td>None</td>
<td>3/14/2005 4:51 PM</td>
<td>3/14/2005 4:51 PM</td>
</tr>
<tr>
<td>?r=mzorg1</td>
<td>None</td>
<td>None</td>
<td>3/14/2005 4:51 PM</td>
<td>3/14/2005 4:51 PM</td>
</tr>
<tr>
<td>_planetelearn_88x31_1_12</td>
<td>None</td>
<td>1/26/2001 1:40 PM</td>
<td>3/15/2005 11:45 PM</td>
<td>3/15/2005 11:45 PM</td>
</tr>
</tbody>
</table>
Using Helix

- Knoppix plus many forensic tools!
  - Autopsy
  - Sleuthkit
  - Etc.
- Current version 1.6 (e-fense, inc)
- Applications
  - Tool kit installed on your hard drive
  - Preview machines in the field, before acquisition
  - Other?
Using Helix/Knoppix for Incident Response

- Preliminary on site investigation
- Run quick evaluation without altering evidence drives
- Boot from CD drive
- Install your USB memory key
- Change permissions to read/write for USB

File Search (JPEG on NTFS)
Image Gallery (save to USB)

Image Gallery for /mnt/hda1/Documents and Settings/fscholl/My Documents/My Pictures/

Number of images: 5
Created on: Tuesday 15 March 2005

File0001.JPG  firewall.jpg  newyorker_dog.jpg  peopleincar.jpg
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 Windows

- Registry
- Log files
  - Windows
  - IIS
- Application data search
- Graphics files in Windows
Windows Registry

- Great digital dumpster for investigations!
- Two primary “hives”
  - HKEY_LOCAL_MACHINE
  - HKEY_USERS
- Registry files
  - No extension: Full copy of hive data
  - .alt extension: Backup copy
  - .log extension: Changes to data
  - .sav extension
Location of Registry Files

- **Win2000 and XP**
  - C:\winnt\system32\config

- **Win98**
  - C:\windows
Discovering Deleted User Accounts

- Deleted accounts may not be visible in Windows Computer Manager (Win2000)
- Check registry
  - HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS NT\CURRENT VERSION\PROFILE LIST
- Shows deleted account names!
Searching Windows Registry

- Regedit has limited search ability
- Regedt32 has no search ability
- Resplendence Registrar: good search ability
  - www.resplendence.com
  - Freeware version: Resplendence Lite
- Searching under username
  - What has user done on machine?
- Looking for recent searches of current user using Windows Search function
Investigating the Registry

- Registrar Lite editor (free at www.resplendence.com)
- Investigate old user names
- Most recently used files
- Recent searches for files
What Files Has User Searched For?

- HKEY_USERS\SID\Software\Microsoft\Internet Explorer\Explorer Bars\ID\Files Named MRU\n  - List of recent Windows searches

Why do we need this?
- Might not have access to disk image
- Court may give you a smaller sandbox!
- Minimize collateral damage in investigations!
<table>
<thead>
<tr>
<th>Name</th>
<th>Data</th>
<th>Type</th>
<th>Size</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(default)</td>
<td>(value not set)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>000</td>
<td>xyz</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>001</td>
<td>cat</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>002</td>
<td>userprofile</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>003</td>
<td>ntuser.dat</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>004</td>
<td>usi</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>005</td>
<td>*.dat</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>006</td>
<td>rye_jail.jpg</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>007</td>
<td>bana^1.jpg</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>008</td>
<td>svewg</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>009</td>
<td>*.pst</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>010</td>
<td>*.jpg</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>011</td>
<td>mta</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>012</td>
<td>cmd.exe</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>013</td>
<td>pagefile.sys</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>014</td>
<td>monarch3</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>015</td>
<td>imagehlp.dll</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>016</td>
<td>ping.exe</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>017</td>
<td>dlstupdater.exe</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>018</td>
<td>t33510.inf</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>019</td>
<td>*.dbf</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>020</td>
<td>XLSStart</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>021</td>
<td>*.xla</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
<tr>
<td>022</td>
<td>MONARCH.DBF</td>
<td>REG_SZ</td>
<td>2084</td>
<td></td>
</tr>
</tbody>
</table>
Windows Log Files (Win2000)

- Configure for proactive forensics
- Review for potential evidence
- Location: c:\winnt\system32\config\n  - appevent.evt
  - secevent.evt
  - sysevent.evt
- Basic configuration: administrative tools | computer management | event viewer
Setting Audit Policy

- Administrative Tools | Local Security Policy | Local Policies | Audit Policy
- Default: nothing logged!
<table>
<thead>
<tr>
<th>Policy</th>
<th>Local Setting</th>
<th>Effective Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit account management events</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit directory service access events</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit object access</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit policy change</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
<tr>
<td>Audit system events</td>
<td>No auditing</td>
<td>No auditing</td>
</tr>
</tbody>
</table>
Security Events of Interest

- Account logon
  - Logs local access
- Account management
  - Logs administrator activities
- Logon events
  - Where account is used
- System events
Auditing IIS Log Files

- Default location: `c:\winnt\system32\logfiles`
- Configure through: Administrative Tools | Internet Services Manager
- Three possible log file formats:
  - W3C Extended: configurable
  - Microsoft IIS: not configurable
  - NCSA Common Format
IIS Log File Format

192.168.1.7, 0, 12/20/2003, 23:20:07, W3SVC1, THINKPAD2, 192.168.1.3, 0, 702, 4817, 401, 5, GET, /,-,
192.168.1.7, 0, 12/20/2003, 23:20:26, W3SVC1, THINKPAD2, 192.168.1.3, 0, 1026, 4419, 401, 5, GET, /,-,
192.168.1.7, 0, 12/20/2003, 23:20:39, W3SVC1, THINKPAD2, 192.168.1.3, 0, 1042, 4419, 401, 5, GET, /,-,
192.168.1.7, 0, 12/20/2003, 23:20:49, W3SVC1, THINKPAD2, 192.168.1.3, 0, 1002, 4419, 401, 5, GET, /,-,
192.168.1.7, 0, 12/20/2003, 23:22:54, W3SVC1, THINKPAD2, 192.168.1.3, 0, 702, 4817, 401, 5, GET, /,-,
192.168.1.7, 0, 12/20/2003, 23:23:08, W3SVC1, THINKPAD2, 192.168.1.3, 10, 1026, 4419, 401, 5, GET, /,-,
192.168.1.7, 0, 12/20/2003, 23:23:15, W3SVC1, THINKPAD2, 192.168.1.3, 0, 1026, 4419, 401, 5, GET, /,-,
192.168.1.7, 0, 12/20/2003, 23:23:25, W3SVC1, THINKPAD2, 192.168.1.3, 0, 1042, 4419, 401, 5, GET, /,-,
127.0.0.1, 0, 12/20/2003, 23:36:10, W3SVC1, THINKPAD2, 127.0.0.1, 0, 882, 4813, 401, 5, GET, /,-,
127.0.0.1, THINKPAD2\Administrator, 12/20/2003, 23:36:10, W3SVC1, THINKPAD2, 127.0.0.1, 0, 551, 224, 304, 0, GET, /Default.htm,-,
Investigative Searching

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

- Boolean
- Stemming: grammatical forms
- Phonic: sounds like
- Fuzzy: misspellings
- Synonyms
- Files filters: date, size, name, etc.
Managing Graphics Files in Windows

- www.acdsystems.com
- www.cerious.com
  - Thumbsplus
  - Finds and creates thumbnail view of all graphic files
  - Creates database of images
  - Finds images “like” selected image
  - Free trial download
- www.firehand.com
References for Module #6

- www.sleuthkit.org
- Knoppix tutorial: http://www.eleli.de/knoppix/docs/tutorial/english/