Digital Forensics

Module 5
CS 996
Outline of Module #5

- Exam next week, 6-8 pm
  - No notes
  - Covers up through and including module #5
- Linux lab update
- Presentation on PDA forensics
- Presentation on Spam Lab (?)
- Forensics legal and business update
- EnCase review
- Linux forensics
Bank of America Case

- Lopez v. B of A filed 2/7/05
  - $90,000 stolen from his account and transferred to Latvia
  - Found a keystroke logger on his PC
- Lopez claims bank was negligent in not advising him about risks of Trojans
- First lawsuit where plaintiff alleges inadequate security practices!
- What do you think?
ITIL Service Management

- “IT Infrastructure Library”
- Just became ISO 20000 Standard (February)
- It is a set of best practices for infrastructure management
- Rapidly increasing adoption
  - Government
  - Private business
  - Vendors
- [http://www.get-best-practice.co.uk/itilProducts.aspx](http://www.get-best-practice.co.uk/itilProducts.aspx)
Why is ITIL Interesting?

- Potential global *standard* for infrastructure management
  - CEO’s and CIO’s pay attention to auditable standards
- Security management
  - Incident management
  - Availability management
  - Capacity management
“Security Controls for Federal Information Systems”


Describes minimum security requirements for (FIPS 199):
- Low impact
- Moderate impact
- High impact
## Incident Response (800-53)

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Training</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Testing</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Handling</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
## Incident Response, cont.

<table>
<thead>
<tr>
<th></th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Reporting</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Assistance</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>
EnCase Image File

- Contains more than raw dd sector image
- Case information header
- CRC for each 32KB of data
- MD5 checksum for entire image
- Image verification
  - Does CRC match for each 32KB block
- “Expert Witness Compression Format”
Low Level Sector Structure (more details)

- AM: Address marker for controller
- CHS: Cylinder/Head/Sector
- CRC: Address checksum
- SP: balancing
- ECC: Error correcting code
- CRC: Data checksum

DATA AREA: 512B
Navigating Case View

- Table
  - Signature analysis (in Search function)
  - Hash analysis
- Gallery
- Timeline
- Report
- Disk
<table>
<thead>
<tr>
<th>Entry</th>
<th>Last Written</th>
<th>Entry Modified</th>
<th>File Deleted</th>
<th>Logical Size</th>
<th>Physical Size</th>
<th>Starting Extent</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>07/28/00 10:14:46AM</td>
<td>07/28/00 10:14:46AM</td>
<td>266</td>
<td>8,192</td>
<td>0C-C43321</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>07/28/00 10:14:44AM</td>
<td>07/28/00 10:14:44AM</td>
<td>266</td>
<td>8,192</td>
<td>0C-C43322</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>07/28/00 10:14:44AM</td>
<td>07/28/00 10:14:44AM</td>
<td>181</td>
<td>8,192</td>
<td>0C-C43323</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>08/01/00 10:06:00AM</td>
<td>08/01/00 10:06:00AM</td>
<td>766</td>
<td>8,192</td>
<td>0C-C43324</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>08/01/00 10:06:00AM</td>
<td>08/01/00 10:06:00AM</td>
<td>775</td>
<td>8,192</td>
<td>0C-C43325</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>08/01/00 10:06:32AM</td>
<td>08/01/00 10:06:32AM</td>
<td>2,611,779</td>
<td>2,613,248</td>
<td>0C-C43325</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>08/01/00 10:06:32AM</td>
<td>08/01/00 10:06:32AM</td>
<td>24,266</td>
<td>24,576</td>
<td>0C-C43645</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>07/28/00 10:20:16AM</td>
<td>07/28/00 10:20:16AM</td>
<td>266</td>
<td>8,192</td>
<td>0C-C43648</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>07/28/00 10:20:16AM</td>
<td>07/28/00 10:20:16AM</td>
<td>25</td>
<td>8,192</td>
<td>0C-C43649</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>07/28/00 10:14:46AM</td>
<td>07/28/00 10:14:46AM</td>
<td>266</td>
<td>8,192</td>
<td>0C-C43650</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>07/28/00 10:14:46AM</td>
<td>07/28/00 10:14:46AM</td>
<td>25</td>
<td>8,192</td>
<td>0C-C43651</td>
<td>3</td>
</tr>
<tr>
<td>12</td>
<td>08/01/00 10:06:16AM</td>
<td>08/01/00 10:06:16AM</td>
<td>266</td>
<td>8,192</td>
<td>0C-C43652</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>08/01/00 10:06:16AM</td>
<td>08/01/00 10:06:16AM</td>
<td>1,358</td>
<td>8,192</td>
<td>0C-C43653</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>07/28/00 10:16:30AM</td>
<td>07/28/00 10:16:30AM</td>
<td>266</td>
<td>8,192</td>
<td>0C-C43654</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>07/28/00 10:16:30AM</td>
<td>07/28/00 10:16:30AM</td>
<td>25</td>
<td>8,192</td>
<td>0C-C43655</td>
<td>3</td>
</tr>
</tbody>
</table>
Finding Evidence

- Sorting columns in table view
- Filters, queries and scripts
- Recovering folders
- Keyword search
Filters, Queries and Scripts

- Filters
  - Use built-in capabilities
  - *Create queries when filter is run*

- Queries
  - Combine more than one filter in semi-custom query

- Scripts
  - Create your own search function using C++ like language
<table>
<thead>
<tr>
<th>Filter</th>
<th>Last Accessed</th>
<th>File Ext</th>
<th>File Type</th>
<th>File Category</th>
<th>Signature</th>
<th>Descriptive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link files</td>
<td>06/12/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/13/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Link files</td>
<td>04/13/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Link files</td>
<td>04/13/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Link files</td>
<td>04/04/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/11/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/13/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/13/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/13/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/13/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files</td>
<td>04/13/00</td>
<td>lnk</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
</tbody>
</table>

3/2/2005

Module 5
String Search

- Adding keywords
- Choose files/folders to be searched
- Configure search
**Hitachi**

**Search expression**

- **Name**: Hitachi
- **Search expression**: hitachi
- **Case Sensitive**: checked
- **Active Code-Page**: checked
- **UTF8**: unchecked
- **GREP**: unchecked
- **Unicode**: unchecked
- **RTL Reading**: unchecked
- **Unicode Big-Endian**: unchecked

**Hex View**

```
[48 68][49 69][54 74][41 61][43 63][48 68][49 69]
```

**GREP Symbols**

- `{wFFFF}`: Unicode character
- `{xFF}`: Hex character
- `{255}`: Decimal character
- `{.}`: Any character
- `{#}`: Any number [0-9]
- `{?}`: Repeat zero or one time
- `{+}`: Repeat at least once
- `{[A-Z]}`: A through Z
- `{[*]}`: Repeat zero+ times
- `{[XYZ]}`: Either X, Y or Z
- `{[^XYZ]}`: Neither X nor Y nor Z
- `{[l]}`: Literal character
- `{(ab)}`: Group ab together for ?, +, *, |
- `{(m,n)}`: Repeat m to n times
- `{a|b}`: Either a or b

**OK**  **Cancel**
File Signatures

- Stated extension on evidence file
- Header information in the file itself
- Matches or not?
- Example:
  - GIF file header: GIF89a (47 49 46 38 39 61)
  - GIF file trailer: .; (00 3B)
- Reference
  - www.garykessler.net/library/file_sigs.html
<table>
<thead>
<tr>
<th>Name</th>
<th>Filter</th>
<th>Search expression</th>
<th>GREP</th>
<th>Case Sensitive</th>
<th>Extensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multimedia</td>
<td>RIFF</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pictures</td>
<td>PDF</td>
<td></td>
<td></td>
<td></td>
<td>psd, pdd</td>
</tr>
<tr>
<td>Adobe Illustrator</td>
<td></td>
<td>\x25\x21\x50\x2D</td>
<td></td>
<td>a</td>
<td></td>
</tr>
<tr>
<td>Adobe PDF</td>
<td></td>
<td>\x21\x64\x68\x65</td>
<td></td>
<td></td>
<td>pdf</td>
</tr>
<tr>
<td>Adobe Photoshop</td>
<td></td>
<td>\x52\x49\x66</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compound Document</td>
<td></td>
<td>\x40\x2F</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corel PhotoPAINT</td>
<td></td>
<td>\x49\x45\x4E\x53</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corel Presentation</td>
<td></td>
<td>\x4D\x41\x44\x41</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CorelDRAW Graphic</td>
<td></td>
<td>\x41\x3C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced Metafile</td>
<td></td>
<td>\x41\x3C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GIF</td>
<td></td>
<td>\x46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interchange File Format</td>
<td></td>
<td>\x46</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>JPEG Image</td>
<td></td>
<td>\x2D\x2E</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kodak Camera DC2</td>
<td></td>
<td>\x4C\x4E\x4D\x4C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kodak PhotoCD</td>
<td></td>
<td>\x4D\x4E\x49\x49\x4D</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Micrografx Design</td>
<td></td>
<td>\x4D\x4E\x4D\x49</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Micrographic Graphic</td>
<td></td>
<td>\x4D\x4E\x4D\x49\x4E\x49\x4E</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PC Paintbrush Graphic</td>
<td></td>
<td>\x42\x45\x48\x4C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Portable Networks</td>
<td></td>
<td>\x4D\x4E\x4D\x49\x4E\x49\x4E</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Compound File Analysis

- Registry
- Email
Access Registry
Win98: user.dat

<table>
<thead>
<tr>
<th>Name</th>
<th>Filter</th>
<th>File Ext</th>
<th>File  Type</th>
<th>File Category</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DEFAULT</td>
<td></td>
<td>DEFAULT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lost Keys</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unallocated Clusters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
View Email Folder

- Compound file
- Locate .dbx or .pst files
- View file structure
Slack Space in EnCase
Basic Unix Forensic Commands

- mount
- dd
- fdisk
- stat
- grep
- loop device
- md5sum
- ls
## Linux Drive Naming Conventions

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hda</td>
<td>Primary IDE controller</td>
<td>Master</td>
</tr>
<tr>
<td>/dev/hdb</td>
<td>Primary IDE controller</td>
<td>Slave</td>
</tr>
<tr>
<td>/dev/hdc</td>
<td>Secondary IDE controller</td>
<td>Master</td>
</tr>
<tr>
<td>/dev/hdd</td>
<td>Secondary IDE controller</td>
<td>Slave</td>
</tr>
<tr>
<td>/dev/fdo</td>
<td>Floppy drive</td>
<td></td>
</tr>
<tr>
<td>/dev/sda</td>
<td>USB drive</td>
<td></td>
</tr>
</tbody>
</table>
## More Drive Naming Conventions

<table>
<thead>
<tr>
<th>Device</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/hda</td>
<td>Primary controller, master</td>
</tr>
<tr>
<td>/dev/hda1</td>
<td>First primary partition</td>
</tr>
<tr>
<td>/dev/hda5</td>
<td>First logical drive on extended partition</td>
</tr>
<tr>
<td>/dev/hda6</td>
<td>Second logical drive</td>
</tr>
</tbody>
</table>
mount command

dell3000:~ # mount
/dev/hda3 on / type reiserfs (rw,acl,user_xattr)
proc on /proc type proc (rw)
tmpfs on /dev/shm type tmpfs (rw)
devpts on /dev/pts type devpts (rw,nodev,mode=0620,gid=5)
/dev/hda1 on /windows/C type ntfs (ro,noexec,nosuid,nodev,gid=100,umask=0002,nls=utf8)
/dev/hdc on /media/cdrecorder type subfs (ro,nosuid,nodev,fs=cdfss,procuid,iocacherset=utf8)
/dev/fd0 on /mnt/floppy type ufat (rw)
/dev/sda on /mnt/usbdrive type ufat (rw)
dell3000:~ #
mount syntax

- mount –t <filesystem> -o <options> <device> <mountpoint>
  - vfat, ext2, iso9660, etc.
  - read only: ro

- umount <mountpoint>
  - unmount file system
dd command

- Sector by sector imaging; no overhead bytes!
- Can image whole disk, partition or section of partition!
- Reference: www.crazytrain.com/dd.html
- Also “dd for windows”
  - http://users.erols.com/gmgarner/forensics
  - Need hardware write blocker!
dd syntax

- `dd if=*source* of=*destination*`
  - `if` = source of evidence (file, device, partition, etc.)
  - `of` = where you want to put the copy

- `dd if=/dev/hdb of=/evidence/hdb3205.img`
  - would use default block size

- Capabilities include carving and imaging arbitrary data “chunk”
fdisk syntax

- fdisk –l /dev/hdx
- Displays partitions for device
fdisk command

```
# fdisk -l /dev/hdb

de13000:~ # fdisk -l /dev/hdb

Disk /dev/hdb: 40.0 GB, 40000000000 bytes
255 heads, 63 sectors/track, 4063 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes

Device Boot Start  End   Blocks Id  System
/dev/hdb1   2   4863  39054015  f  W95 Ext’d (LBA)
/dev/hdb5   2  4718  37089271  83  Linux
/dev/hdb6  4719  4750  257008+  b  W95 FAT32
/dev/hdb7  4751  4763  104391  83  Linux

de13000:~ #
```
stat command

- Provides inode information
- stat /path/filename
stat command

```
dell3000:~ # stat /etc/fstab
    File: '/etc/fstab'
        Size: 823      Blocks: 8      IO Block: 4096   regular file
    Device: 303h/771d  Inode: 37165  Links: 1
    Access: (0644/-rw-r--r--)  Uid: (   0/ root)  Gid: (   0/ root)
    Modify: 2005-02-28 09:47:29.000000000 -0800

dell3000:~ #
```
**md5sum hash**

- *Always* use before and after creating image of evidence
- Creates 128 bit unique “fingerprint”
- Syntax
  - `md5sum /dev/fdo > md5.disk`
ls command

- View file or directory properties
- ls –l <filename>
### ls command

<table>
<thead>
<tr>
<th>Permission</th>
<th>Owner</th>
<th>Group</th>
<th>Size</th>
<th>Date/Time</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwxr-xr-x</td>
<td>2 root root</td>
<td>48 Oct 4 08:24</td>
<td>cron.weekly</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>511 Oct 1 18:09</td>
<td>crontab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>6261 Mar 30 2004</td>
<td>csh.cshrc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>2273 Sep 17 2003</td>
<td>csh.login</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>6 lp lp</td>
<td>552 Feb 25 10:32</td>
<td>cups</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>2 root root</td>
<td>120 Dec 27 18:36</td>
<td>default</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>0 Oct 1 17:54</td>
<td>defaultdomain</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>28968 Feb 28 09:24</td>
<td>defkeymap.map</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>6 root root</td>
<td>144 Dec 27 18:36</td>
<td>dev.d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>5982 Oct 1 18:10</td>
<td>enscript.cfg</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>152 Oct 2 06:10</td>
<td>esd.conf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>605 Oct 1 17:54</td>
<td>ethers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>5239 Oct 4 13:25</td>
<td>evms.conf</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>322 Oct 1 17:54</td>
<td>exports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>25028 Oct 1 17:54</td>
<td>fbs.modes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>1246 Oct 1 18:50</td>
<td>fdprm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>26 Oct 1 18:50</td>
<td>filesystems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>2 root root</td>
<td>264 Dec 27 18:32</td>
<td>fonts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>2 root root</td>
<td>120 Dec 27 18:37</td>
<td>fsomatic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>823 Feb 28 09:47</td>
<td>fstab</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>565 Oct 1 17:54</td>
<td>ftpusers</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>3 root root</td>
<td>72 Dec 27 18:54</td>
<td>gimp</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-rw-r--r--</td>
<td>1 root root</td>
<td>4675 Oct 4 11:59</td>
<td>gnokiirc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>drwxr-xr-x</td>
<td>2 root root</td>
<td>168 Dec 27 18:35</td>
<td>gpm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
File Properties

- File types
  - - = regular file
  - d = directory
  - b = block device
  - c = character device
  - l = link

- File permissions read, write, execute
  - Owner/Group/Others
Linux MAC Times

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

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

- **Change time**
  - Alter file attributes (inode) or content
loopback device

- Enables mounting of disk image directly without a physical drive
- Option in “mount” command
- Syntax
  - mount –t vfat –o ro,loop disk.img /mnt/analysis
grep command syntax

- grep –options <pattern> <search_range>
- grep –a –B20 –A20 "bomb" /dev/hda1 > search.results
  - -a process as binary file
  - -B20 output 20 lines before “bomb”
  - -A20 output 20 lines after “bomb”
  - /dev/hda1 search first partition of had
  - > redirect results to search.results file
Keywords and beyond

- Special characters (examples)
  - ^ start of line
  - $ end of line
  - . any character

- Regular Expressions
  - http://gnosis.cx/publish/programming/regular_expressions.html
  - http://sitescooper.org/tao_regexps.html
Sleuth Kit

- Current version: 1.73
- Command line tools
  - File system analysis
  - MACtime: “modified, add, changed”
- Supported file systems
  - EXT2
  - FAT
  - NTFS
- Analyze partitions; not whole disk
Sleuth Kit v. 2.0

- Under construction
- New features:
  - Analyze disk images
  - Analyze other tool formats (EnCase?)
  - Autodetect file system type
- My comment: use tool for research and basic investigation (not necessarily for court room presentation)
References for Module #5

- Barry Grundy, “The Law Enforcement and Forensic Examiner Introduction to Linux” (class handout).