Outline of Module #9

- Report from Spain (Jason, Larisa, PJ)
- Review MidTerm exam
- Using EnCase
EnCase Resources

- **Academic CD**
  - Instructor Notes
  - User Manual excerpts on analysis
  - Training Manual
- [www.guidancesoftware.com](http://www.guidancesoftware.com)
  - Online videos
Hard Drive Forensics

- **Acquisition**
  - Bit for bit copy (may include some proprietary data)
  - Write protect the evidence media
  - EnCase for DOS
  - Safeback (NTI: www.forensics-intl.com)

- **Analysis**
  - EnCase
  - FTK (www.accessdata.com)
Acquisition Steps With EnCase

- Create EnCase boot disk
  - DOS boot disk
  - Network boot disk
- Start subject computer with boot disk
- Acquire data to storage computer
  - Network acquisition
  - Drive to drive acquisition
  - Parallel cable acquisition
  - Windows acquisition
EnCase Acquisition Geometry

- Network cable acquisition

![Diagram of network cable acquisition](image)
EnCase Acquisition Geometry, cont.

- Drive to Drive acquisition
EnCase Acquisition in Windows

- CD-ROMs, write-protected floppy, etc.
- Use hardware write protection for harddrive
Analysis With EnCase

- Initialize case
- Bookmarks: reporting
Initialize Case: EnCase Scripts

- Allow custom forensic analysis
- Program in C++ like API
- Pre-made scripts
  - Initialize Case
  - Download from www.guidancesoftware.com
  - Install in: c:\program files\encase\scripts\examples
- Running scripts:
  - View Scripts | Select Script | Run
  - View report => Bookmarks
Using Bookmarks

- Save important data for report
- View Bookmarks: Create New Folder
  - Text
  - Images
of altering consciousness; when you cultivate these plants, the state has been through a long con
secration of sorts while you tended to the plant bearing the particular "spirit." If you keep ev
everything in it's proper place, should you be afraid? Why did differnt altogether in conjunction with your plants to justify one could begin painting, wine making, or anything else co...
Navigating Case View

- Table
  - Signature analysis (in Search function)
  - Hash analysis
- Gallery
- Timeline
- Report
- Disk
### Table of Entries

<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></td>
<td>266</td>
<td>8,192</td>
<td>OC-C43321</td>
<td>3</td>
</tr>
<tr>
<td>2</td>
<td>07/28/00 10:14:44AM</td>
<td></td>
<td>266</td>
<td>8,192</td>
<td>OC-C43322</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>07/28/00 10:14:44AM</td>
<td></td>
<td>181</td>
<td>8,192</td>
<td>OC-C43323</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>08/01/00 10:06:00AM</td>
<td></td>
<td>766</td>
<td>8,192</td>
<td>OC-C43324</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>08/01/00 10:06:00AM</td>
<td></td>
<td>775</td>
<td>8,192</td>
<td>OC-C43325</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>08/01/00 10:06:32AM</td>
<td></td>
<td>2,611,779</td>
<td>2,613,248</td>
<td>OC-C43325</td>
<td>3</td>
</tr>
<tr>
<td>7</td>
<td>08/01/00 10:06:32AM</td>
<td></td>
<td>24,266</td>
<td>24,576</td>
<td>OC-C43645</td>
<td>3</td>
</tr>
<tr>
<td>8</td>
<td>07/28/00 10:20:16AM</td>
<td></td>
<td>266</td>
<td>8,192</td>
<td>OC-C43648</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>07/28/00 10:20:16AM</td>
<td></td>
<td>25</td>
<td>8,192</td>
<td>OC-C43649</td>
<td>3</td>
</tr>
<tr>
<td>10</td>
<td>07/28/00 10:14:46AM</td>
<td></td>
<td>266</td>
<td>8,192</td>
<td>OC-C43650</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>07/28/00 10:14:46AM</td>
<td></td>
<td>25</td>
<td>8,192</td>
<td>OC-C43651</td>
<td>3</td>
</tr>
<tr>
<td>12</td>
<td>08/01/00 10:06:16AM</td>
<td></td>
<td>266</td>
<td>8,192</td>
<td>OC-C43652</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>08/01/00 10:06:16AM</td>
<td></td>
<td>1,358</td>
<td>8,192</td>
<td>OC-C43653</td>
<td>3</td>
</tr>
<tr>
<td>14</td>
<td>07/28/00 10:16:30AM</td>
<td></td>
<td>266</td>
<td>8,192</td>
<td>OC-C43654</td>
<td>3</td>
</tr>
<tr>
<td>15</td>
<td>07/28/00 10:16:30AM</td>
<td></td>
<td>25</td>
<td>8,192</td>
<td>OC-C43655</td>
<td>3</td>
</tr>
</tbody>
</table>

### Disk Image Analysis

```
0698649
0698700
0698751
0698802
0698853
0698904
0698955
0699006
```

### File Path

```
StudentDemo\Quantum\C\America Online 4.0\jdt\spool.lst
```
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 1</td>
<td>04/12/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Link files 2</td>
<td>04/13/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Link files 3</td>
<td>04/13/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Link files 4</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 5</td>
<td>04/13/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>Match</td>
<td>File, Archive</td>
</tr>
<tr>
<td>Link files 6</td>
<td>04/13/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 7</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 8</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 9</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 10</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 11</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 12</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 13</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 14</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 15</td>
<td>04/11/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 16</td>
<td>04/13/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Read Only</td>
<td></td>
</tr>
<tr>
<td>Link files 17</td>
<td>04/13/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 18</td>
<td>04/13/00</td>
<td>In</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
<tr>
<td>Link files 19</td>
<td>04/13/00</td>
<td>LNK</td>
<td>Link</td>
<td>Windows</td>
<td>File, Archive</td>
<td></td>
</tr>
</tbody>
</table>

```java
Class MainClass {
    Main (EntryClass entry) {
        return entry.Extension().Compare("link", false) == 0;
    }
}
```

Module 9
String Search

- Adding keywords
- Choose files/folders to be searched
- Configure search
EnCase Search Method

- First does logical search
- Next does sector by sector
- Compound files like .pst and .dat need to be mounted separately

```
| CLUSTER N | CHILD | PORNOGRAPHY | CLUSTER N+1 |
```
<table>
<thead>
<tr>
<th>Name</th>
<th>Filter</th>
<th>Preview</th>
<th>Hit Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>TECHFONE.BBS</td>
<td>Time</td>
<td>HITACHI</td>
<td>HITACHI</td>
</tr>
<tr>
<td>HANDSETX.BBS</td>
<td></td>
<td>HITACHI</td>
<td>HITACHI</td>
</tr>
<tr>
<td>HANDSETX.BBS</td>
<td></td>
<td>HITACHI</td>
<td>HITACHI</td>
</tr>
<tr>
<td>HANDSETX.BBS</td>
<td></td>
<td>HITACHI</td>
<td>HITACHI</td>
</tr>
<tr>
<td>HANDSETX.BBS</td>
<td></td>
<td>HITACHI</td>
<td>HITACHI</td>
</tr>
<tr>
<td>FONEFIND.BBS</td>
<td>30AL</td>
<td>HITACHI</td>
<td>HITACHI</td>
</tr>
<tr>
<td>FONEFIND.BBS</td>
<td></td>
<td>UOAH</td>
<td>HITACHI</td>
</tr>
<tr>
<td>FONEFIND.BBS</td>
<td></td>
<td>UOAH</td>
<td>HITACHI</td>
</tr>
<tr>
<td>FONEFIND.BBS</td>
<td></td>
<td>UOAH</td>
<td>HITACHI</td>
</tr>
<tr>
<td>13.BBS</td>
<td>13</td>
<td>Hitachi</td>
<td>Hitachi</td>
</tr>
<tr>
<td>13.BBS</td>
<td></td>
<td>0 HITACHI 2 Pro</td>
<td>HITACHI</td>
</tr>
<tr>
<td>13.BBS</td>
<td></td>
<td>0 HITACHI 2 Pro</td>
<td>HITACHI</td>
</tr>
<tr>
<td>13.BBS</td>
<td></td>
<td>0 HITACHI 2 Pro</td>
<td>HITACHI</td>
</tr>
<tr>
<td>13.BBS</td>
<td></td>
<td>12 HITACHI Distri</td>
<td>HITACHI</td>
</tr>
<tr>
<td>13.BBS</td>
<td></td>
<td>13 HITACHI 2 Pro</td>
<td>HITACHI</td>
</tr>
<tr>
<td>13.BBS</td>
<td></td>
<td>12 HITACHI Distri</td>
<td>HITACHI</td>
</tr>
</tbody>
</table>

4/12/04 Module 9 30
File Signatures

- Stated extension on evidence file
- Header information in the file itself
- Matches?
Compound File Analysis

- Registry
- Email
Access Registry
Win98: user.dat
View Email Folder

- Compound file
- Locate .dbx or .pst files
- View file structure
File Viewers

- Look at file outside Encase
- Add: View => File Viewers
- Create association: View => File Types
- Double click on file: copies and opens with viewer
- QuickView Plus
  - [www.avantstar.com](http://www.avantstar.com)
  - 200+ different file formats
  - Eliminates problems with trojans, viruses, etc.
Add File Viewer
Create Association (View Filetypes)
References for Module #9

- EnCase Legal Journal (course web site)