What the book says:
“Computer forensics involves the preservation, identification, extraction, documentation and interpretation of computer data. It is often more of an art than a science, but as in any discipline, computer forensic specialists follow clear, well-defined methodologies and procedures, and flexibility is expected and encouraged when encountering the unusual.”
From: "Computer Forensics: Incident Response Essentials"

- Computer forensics is closely associated to law enforcement for retrieving evidence, but it could AND should be used to retrieve data for other reasons as well.
Topics

- Intro to Computer Forensics
- What may be available

Software Recommendations

- Guidancesoftware’s Encase: www.encase.com
- Acessdata’s Forensic Toolkit: www.accessdata.com
- AccessData Password Recovery Toolkit
- AccessData's Distributed Network Attack
- Prodiscover (DFT or IR), www.techpathways.com
- Safeback, www.forensics-intl.com
- Quick View Plus, http://www.jasc.com/
- Thumbs Plus (Shareware), www.cerious.com
- Irfanview (freeware for non commercial use)
  - www.irfanview.com
What Computer Forensics is used for:

- High Tech Investigations
- Incident Response
- E-mail recovery and analysis
- Document & File Discovery
  - Locating and recovering previously inaccessible files.
- Data Collection
  - Collecting data while preserving vital date and time stamps, temporary files and other volatile information.

- Preservation of Evidence
  - Adherence to carefully developed set of procedures that address security, authenticity, and chain-of-custody.

- Analysis of User Activity
  - Reporting of all user activity on computer and company network including, but not limited to, e-mail, Internet and Intranet files accessed, files created and deleted, and user access times.

- Password Recovery
  - Accessing and recovering data from password protected files.
Investigative Methods

- Common sense
- Physical surveillance
- Victim\witness interview
- Undercover approach
- Electronic surveillance (network sniffer, NIDs, etc.)
- Informants
- Sting operation
- IMAGE!

Does this sound any different then other types of investigations?

Keys to Success

- Documentation of all action
- Preservation of evidence
- Swift action to collect electronic audit trails
- Resources
- Time – hard drives are getting HUGE!
Tools of our trade

Terminology

- **Image**: exact copy of a hard drive including deleted files and areas of the hard drive that a normal backup would not copy
- **Slack, Swap and Unallocated space**
Slack Space

Security Leakage

25% of Hard Drive
Space Is File Slack

Copyright © 2000 by Nam Technologies, Inc.

Slack Space Analogy

Collection Of Half Hour Video Tapes
How Can I Find Deleted Information?

- Episode One of The Simpsons
- News Item
- Yankees Highlights (GAMES 4 and 5)
- Yankees Highlights Continued
- Episode of Sopranos

How Can I Find Overwritten Information?

- Episode Two of Simpsons
- ISSA Video
- News Clip
- Cybercrime
- Episode Three of The Simpsons
How Can I Find Deleted Information?

- NYPD Blue
- News Item
- Another show
- Interesting Ad
- News

ISSA Remains
Yankees Remains
Continued Yankees tape
Simpsons Remains
Sopranos Remains

“Deleted” files?

Security Leakage

Data From
Erased Files
Remain

Copyright © 2000 by New Technologies, Inc.

Copyright Computer Forensic Services, LLC
Show Me Something!

- Password Protected files
- Deleted Files Demo's

Defeating Passwords

Security Leakage

Copyright Computer Forensic Services, LLC
Password Protection

Show Me Something Else!

- Once Upon a Time There Was a File Named PatentSubmission.Doc
A File Is Born

The File Dies...or Does It?
Encase Doesn’t Think So

How About Now?
Let's See Shall We?

It's ALLLLLLLIVE!
How About Now?

Let’s See
It’s STILL ALLLLLLLIVE!

The Resurrection
(“Deleted” File Before and After Format and Defrag)
### Carving Heads

**Image of Carving Heads**

- Software interface for forensic analysis
- Trees and data structures
- Panels for preview and selection
- Sector offset and bytes

### Word Doc Headers

**Image of Word Doc Headers**

- Image of document headers
- Table showing document properties
- Path and file locations
- Copyright notice
Carving Heads

Whoop There It Is!

Copyright Computer Forensic Services, LLC
Trace Information May Exist From:

- Email
- PDA/Blackberry
- Temp Files
- Recycle Bin
- Info File Fragments
- Recent Link Files
- Spool (printed) files
- Internet History (index.dat)
- Registry
- Unallocated Space
- File Slack

The File Lives On...

- This was made possible only through the forensic practice of treating the entire physical disk as evidence (rather than just files) and handling it as evidence.
- Demos anyone?
Where to go from here

- www.virtuallibrarian.com/legal/
- www.htcia.org
- **Shameless Plug Warning:**
  - Computer Forensics: Incident Response Essentials
    - **Paperback:** 416 pages
    - **Publisher:** Addison-Wesley Pub Co
    - **ISBN:** 0201707195

Questions?