TECHNOLOGY

Computers have become so integrated into our lives that it seems the obvious starting place to look for evidence. Because of the expanding trend toward creating, using and transmitting electronic documents, most investigations should include the computer.

Computers have made prolific writers out of all of us, as nearly all documents and correspondence today is generated on computers, and statistics show 95% never gets printed. We are also prolific packrats. An 80-gigabyte hard drive can store enough information to fill a stack of paper 10,000 feet high, so there is no real incentive to delete files. On top of that, we have become less formal in our communications. Before email, who took the time to copy a joke or funny picture and mail it to all their friends? Email makes sharing of information very easy, and some of that information is inappropriate. The evidence is on the hard drive, and computer forensics is the discipline for recovering that evidence.

82% of E-Crimes are committed by company employees, with roughly 1/3 committed by senior management. -Ernst & Young

INSIDE THE FIREWALL

The greatest risks can be on the inside of the firewall, as it is usually a company's own employees who are using their access to the network to delete, steal, leak, or corrupt a company's critical data. Employees viewing or trading pornography can expose a company to embarrassing law enforcement intervention, sexual harassment suits and network inefficiency.

COMPUTER FORENSICS: The need for investigation
Reasons to initiate an investigation include:

- **Suspected theft or sharing of proprietary information (client data, proposals, confidential memos, accounting data, etc.)**

- **Inappropriate e-mail and other electronic communications**

Suspected access to questionable websites through the Internet (According to Websense, 70% of Internet porn traffic occurs during the 9 to 5 workday.)

- **Illegal activities by employees (According to the FBI/Computer Security Institute's 2001 survey, upwards of 70% of computer crime is committed by employees.)**

- **Inappropriate computer use**

INVESTIGATOR VS. THE IT GUY

Electronic evidence is becoming more common in the legal arena, so data discovery is a job that's best left to a computer forensics consultant rather than your IT guy. Computers don't violate company policy or commit crimes, people do; and that underscores the necessity for hiring a trained investigator to analyze the computer instead of a computer consultant. The methods used in a corporate setting provide the widest range of choices: termination, civil litigation, or referral to law enforcement.

Computer forensics is more than just technology, it is using only tools and methodologies that are forensically sound and acceptable in court as part of an investigation. Treat every case as if it were going to be used in litigation. It is critical that the computer forensics investigator understand the legalities surrounding the capture of electronic evidence.

COMPUTER FORENSICS USES:

- **Preserve the integrity of your evidence with secure chain of custody protocols and mirror imaging of storage media**
- **Retrieve email correspondence**
- **Access active and deleted data files or file fragments**
- **Discover graphic images**
- **Identify Internet usage**
- **Recover data appearing lost due to hardware or software malfunction or destruction**
- **Access password protected or encrypted files**
- **Present findings for litigation, etc.**

Recovered data is documented, catalogued, analyzed, and recorded in reports which are presented to the client or the courts in compliance with all rules of evidence.