

Computer Forensics

By Joan E. Feldman

Computer Forensics Inc.™
1749 Dexter Avenue North
Seattle, WA 98109
206-324-6232
jfeldman@forensics.com

Joan Feldman, known as one of the nation's premier "cybersleuths", is a pioneer in the science of forensic computing. Ms. Feldman is the founder and president of Computer Forensics Inc.™, specializing in the science of forensic computing, discovery, and risk management. Ms. Feldman's background combines over twenty years of computer forensics and litigation expertise. Ms. Feldman obtains and analyzes electronic data used as evidence in civil litigation and oversees the work of CFI's forensic teams. A recognized authority on electronic media discovery and related topics, Ms. Feldman is a busy national speaker, magazine contributor, and media resource for expert commentary.

© 2005 Computer Forensics Inc.™

The Expert's Role in Computer-Based Discovery

Joan E. Feldman, President
Computer Forensics Inc.™

Attorneys and judges can face extreme challenges to their technical knowledge when it comes to computer-based discovery. Locating, reviewing, and managing computer-based files requires an understanding of technology that often goes beyond that of the most experienced power user. In recent years, attorneys and the courts have turned to computer forensics experts for help in cutting through the technical issues that often cloud discovery objectives.

The computer forensics expert may fill one of two roles. The computer forensics expert may serve in the traditional role of the expert – helping to educate the court and all parties in their search for facts. In such cases the expert may review the computer evidence directly and prepare forensic reports and affidavits, or oversee the work of the other party's expert witnesses. In a secondary role, the expert may act as more of a “vendor” of services. For example, the expert may not prepare an expert report of findings, but may instead provide a range of services such as consulting or project management tasks.

Because computer-based discovery is still relatively new, the type of services provided by forensic experts in a “vendor” role is often misunderstood. The following list of activities and services explains some of the common tasks handled by forensic experts. The choice of the appropriate computer forensics expert is also driven by counsels' objectives. For many of the tasks listed below, consulting and project management skills are as important as technical expertise.

Identification of Data Types for Review

In a consulting role, the expert can work to ensure that the attorney understands the various types of data available for review. The main categories of data: active, residual, and backup will determine how the data is collected and reviewed. Various data types are described below:

Active data

In addition to program and operating system files, the two categories of active data most commonly reviewed are:

1. *User created data*, readily available and accessible to users. User created data includes email messages, word-processing documents, spreadsheets, databases, electronic calendars, etc. Active email messages can be read simply by opening a mailbox.

2. *System generated copies of user data*, not easily found or accessed by an average user. Such data includes copies of files created for the user by the application software or operating system. Common examples include temporary files created by Windows and stored in the “Temp” directory, and “near-copies” of files such as saved revised documents. Email client software e.g., Exchange Outlook, can automatically create entire archives of data. *See for example Microsoft Outlook’s description of its archive function:*

“During installation, several folders are set up with “AutoArchive” turned on. These folders and their default aging periods are Calendar (6 months), Tasks (6 months), Journal (6 months), Sent Items (2 months), and Deleted Items (2 months).”

Residual data

Includes “deleted” files that may still exist on a drive surface. When a file is deleted, the data in that file is not erased. Rather, the computer marks the file space as “free” and the file remains retrievable. Data in a deleted file is not erased until it is overwritten with data from a newly saved file or until it is “wiped” by specialized programs. Residual data can also include portions of files distributed on the drive surface or embedded within other files. These files are commonly referred to as “file fragments” and “unallocated” data.

Backup data

Information copied to portable media (usually tape) to provide users with access to their data in the event of a system failure. Networked systems are normally backed up on a routine schedule. Typical network backups capture only the data that are saved to the centralized storage systems (e.g., the file server) and do not capture data stored on individual users’ hard drives. PC users tend to selectively back up data onto floppy diskettes, tape, or removable hard drives.

Locating Responsive Data

In traditional discovery efforts, responsive documents can be found in locations throughout the business enterprise in many formats (file cabinets, desk drawers, file repositories, microfilm/microfiche collections, etc.). Identifying and locating *responsive computer-based* documents requires that parties understand where to look within the computing environment. The expert, in a consulting role, will help direct the parties in their review by first establishing what they are looking for (data types), then directing the parties to the appropriate data type location. Standard data locations include, but are not limited to, individual drives, shared drives, and backup tapes.

Individual Drives

Users may save their data on the drive of their desktop PC workstation or notebook computer. Floppy disk drives, Zip drives, or other drives may also be available, and data can be copied to floppy diskettes, Zip cartridges, or tapes at the desktop.

Note: Users generally store their files to the shared drive if they are on a networked system. Users can of course store files in more than one location, i.e., on their hard drive as well as on the server. Drives normally contain active, archival, and residual data.

Shared Drives

Shared drives, also referred to as network drives, file servers, etc., act as centralized data repositories for user data. A shared drive can be thought of as an electronic file room, with files indexed to facilitate access by individuals and groups. In most business environments, users save their work product (data) to a shared drive. Data created and saved may include:

- electronic mail
- word-processing documents
- databases
- general ledger and accounting documents

Shared drives are usually managed centrally by an information services department.

Note: Shared drives usually contain active data only. If residual data exists on shared drives, the volume is minimal.

Backup Tapes

Backup tapes contain copies of data stored on shared drives. Backup tapes rarely contain copies of data stored on individual drives.

Note: Backup tapes are often re-used or recycled. Recycling a backup tape is usually done on a rotation schedule. When a tape is re-used or recycled, data on the tape is overwritten by new data, effectively destroying the old data on the tape.