

# Scrub, Scrub, Scrub

by Paul French  
New Technologies, Inc.

Advancements in hard disk drive storage capacities, operating systems and software applications encourage law firms and corporations to buy or lease new computers every year. When the time comes to retire a laptop or desktop PC to make way for new machines, administrators generally reformat the hard disk drives on the old machines to eliminate sensitive data before discarding them or donating them to charity. Unfortunately, many people do not realize that the data that seems to have been removed from the hard drive is still there in a shadow sense, and is easily recoverable through computer forensic or simple data recovery processes. *The bottom line: the reformatting of a hard disk drive provides essentially no level of security.*

*Taking extra precautions with hard drives and portable data disks can safeguard sensitive information and ensure that attorney-client privilege is maintained.*

Today's computers and operating systems were designed primarily for speed and convenience. Security was not a significant concern. Because of security flaws, sensitive information can leak into *ambient computer data storage areas* such as *file slack*, the *Windows swap file* and *unallocated (erased) file space*, all without the knowledge of the computer user. (Definitions provided later in this article.) Such information can unknowingly be transferred to others. In the context of legal practice, this may inadvertently compromise attorney-client privilege through the exchange of word processing files and floppy diskettes to clients or other professionals -- or worse, opposing counsel. In the case of corporate executives, insider information and trade secrets may unintentionally be compromised through the transfer of notebook computers or through the disposition of corporate computers. Be assured that such data can easily be recovered.

Fortunately, these problems need not exist; software programs exist to securely eliminate or scrub all data from selected storage devices. There are two different types of scrubbing utilities. The first type writes over the entire drive, regardless of files or operating system. This more destructive method is useful if the drive being cleaned will be going to another user or leaving the organization entirely.

The second type of scrubbing utility is used to clean drives that are still in use. It leaves files intact so the computer stays operational, but it cleans the ambient computer data storage areas by repeatedly overwriting them in such a way that the original data they contained cannot be recovered using data recovery or computer foren-

sics software. Among other things, this allows you to be sure that the removable media you are using to transfer files contains only the information you want.

The most stringent scrubbing applications on the market, which conform to U.S. Department of Defense computer security standards, incorporate a data overwrite process that involves multiple passes where the program writes a single character across the entire drive, followed by a final pass that verifies that the previous writes were successful.

Here are some common scenarios where scrubbing can prevent the unintended dissemination of sensitive information:

It is used by lawyers and law enforcement agencies to eliminate the potential disclosure of sensitive information when data is exchanged in the legal discovery process.

It is used by lawyers, accountants and corporate executives to eliminate confidential client and trade secret data from portable notebook computers, which are easily stolen or compromised from a security standpoint.

It is used by law enforcement computer crime specialists to eliminate the potential of data bleeding from one case to another in the processing of computer evidence.

It is used to eliminate ambient data on floppy diskettes and Iomega Zip Disks that are exchanged with others. You can avoid sharing more information than you intend.

It is used to securely scrub computer hard disk drives when computers are transferred from one employee or division to another.

A good scrubbing application is affordable, and is easy to run. If your employees are regularly dealing with sensitive information, it's a piece of software you can't afford to be without.

## Key Computer Forensics Terms

### Ambient Data

Ambient data is a forensic term that describes data residing in non-traditional computer storage areas and formats. It generally describes data in file slack, the Windows swap file and unallocated file space.

### File Slack

Files are created in varying lengths depending on their contents. DOS, Windows and Windows NT-based computers store files in fixed-length blocks of data called clusters. Rarely do file sizes exactly match the size of one or multiple clusters perfectly. The data storage space left between the end of the file itself and the end of the last cluster assigned to the file is called file slack, and it will continue to contain whatever was in the cluster the last time the system used it for an earlier file. Deletion of the old file or defragmentation of the disk released the cluster in question for reuse, but did not eliminate its contents; only overwriting with new data or null characters will do that. Cluster sizes can vary in length depending on the operating system and the size of the logical partition involved. Larger cluster sizes mean more file slack. File slack is a significant source of evidence and leads for computer forensics investigators, because very few computer users understand or eliminate this computer security weakness.

### Windows Swap File

To make more efficient use of random access memory, Microsoft Windows operating systems use a "scratch pad" called a swap or page file. Swap files are potentially huge and most computer users are unaware of their existence. These files can contain remnants of word processing documents, e-mail messages, Internet browsing activity, database entries and almost any other work that may have occurred during past Windows work sessions. This situation creates a significant security problem because the potential exists for data to be transparently stored within the Windows swap file without the knowledge of the computer user. This can occur even if the work product was stored on a computer network server. The result is another significant computer security weakness that can provide computer forensics specialists with investigative leads that might not otherwise be discovered.

### Unallocated File Space

When files are erased or deleted in DOS, Windows, Windows 95, Windows 98 and Windows NT, the content of the file is not actually erased. Unless security-grade file deletion software is used, data from the theoretically erased file remains behind in an area called unallocated file space, where it is available for discovery through the use of data recovery or computer forensics software utilities.