Title:
Eliminate Unnecessary Files Forever - Use File Shredder

Word Count:
539

Summary:
The basic intent of a file shredder is to entirely obliterate the file. However, advanced software's does the dual task of not only destroying a file but also shreds the evidence that the file was deleted.

A file shredder works by overwriting the file, mostly once and if needed up to three times. The program then removes the file from the directory area by again overwriting it. Running a defragmentation after file shredding can render the file impossible to recover. Runni...

Keywords:
file shredder,file wiping,file security

Article Body:
The basic intent of a file shredder is to entirely obliterate the file. However, advanced software's does the dual task of not only destroying a file but also shreds the evidence that the file was deleted.

A file shredder works by overwriting the file, mostly once and if needed up to three times. The program then removes the file from the directory area by again overwriting it. Running a defragmentation after file shredding can render the file impossible to recover. Running a file shredder is imperative for anyone who is considering selling or donating their old comp. These are a potential treasure house of personal information that can be used to wreck havoc on pre users. Recent studies have shown a rise in the disturbing trend of misusing personal information and files on donated comps even after files were deleted.

People often assume that by deleting a file from their hard drive the file is forever lost. Actually the file is very much there on their hard drive. When a file is moved into the recycle bin, the file stays in its place. But the directory entry of the file, i.e., the complete path and filename of a file is moved into a hidden folder. The file is then renamed; the original name of the file is stored in a hidden index file called INFO2. If at any point the file is clicked to be restored, windows read the original path from the INFO file and rename the file into the directory. So what happens when you delete the file

from the recycle bin? Again the data is not deleted, instead windows simply marks the place occupied by the file as not needed and available fro use. The data will be there until the time the system needs the space for another file, when it will be overwritten. This dramatically increases your chance of recovering a deleted file if you haven't done any subsequent disk activity such as creating, copying and editing.

A techie who knows his job can easily recover deleted data from a hard drive within minutes. Even after it has been overwritten once, the information underneath the top layer can be scrapped up by using sophisticated equipments.

Trade espionages stalk the cyber world looking for tit bits of trade secrets that can knock you out of business within in days. File shredding forms one of the core entities in the complex labyrinth of security programs. There are basically three ways to decimate a sensitive file. One would be to use a file shredding software, next is using a powerful encryption and lastly a bit on the extreme side is incinerating media or pouring acid on it. Of the three the file shredder is the most practical for an average user and largely sufficient. The newer files shredding programs comes augmented with features such as wipe free space and wipe file names. Wipe file names allows you to overwrite the file names. After file wiping, simple recovery programs will not even show the file. The sophisticated ones show the name of the file, but it will be scrambled beyond recognition. Free disk space wiping is a powerful feature which renders it impossible to recover deleted files.