THE COMPUTER CORNER

No. 225: File Shredders

Stan Kaplan, WB9RQR 715 N. Dries Street Saukville, WI 53080-1664
(262) 268-1949 wb9rqr@att.net

Note my current email address above. Please be sure your address book reflects this.

The ORC breakfast on Saturday mornings often provides interesting topics for this publication. Last month's article on constructing secure passwords was based on breakfast conversations with Brian Skrentny (N9LOO). This month's article was suggested by Ed Rate (AA9W) and consisted of a simple question. How does one securely erase files and folders so that the data is unrecoverable? The solution to Ed's question is quite simple. As is often the case, someone has thought of the problem and has written free software to solve it. The trouble is, lots of people have thought about it and they have written lots of solutions!

First, some background. When you erase a file in Windows (or DOS), you don't delete even a single byte. It is still all there. The only thing you do when you delete (erase) a file is to change the first letter of the filename to F6h (read F six hexadecimal, or decimal 246), which can be revealed by certain special editors as consisting of the Greek lower case letter sigma (σ). That sigma renders the file invisible (so you think it is gone, but it actually is not gone), and it signals to the operating system that the space occupied by the file on the hard drive platters may be used for other files from that point on. Thereafter, slowly or rapidly (depending upon many factors including how much you use your machine), the original file is overwritten. But, a forensic technician (or recovery software) can retrieve the file completely, if retrieval is tried soon after ordinary deletion. Later, partial retrieval could be successful.

So then, what is the job of file shredder software? Such software identifies a file that can be seen in Windows (you identify it by typing its name or highlighting its name on screen), and then the software overwrites each bit in the file with random bits at least once, sometimes up to eight times. This effectively destroys the file (including the filename) and makes it unrecoverable, even by file recovery software or a technician. You might think, "well why not just dump it into the Recycle Bin and then empty the Recycle Bin?" That ploy will simply create two copies of what you wanted to get rid of! One copy will be left behind in its original folder (though it won't be visible to you, owing to the σ). Another copy will be left in the Recycle Bin (though it won't be visible to you after the bin is emptied, again because of the σ). So you have just made the problem worse by making two copies of what you wanted to get rid of in the first place!

The answer to Ed's problem (and perhaps yours) is to go get a file shredder for yourself. I won't tell you to absolutely get a specific one, but I will give you some criteria to allow you to accept or reject one or another.

First and foremost, get it from majorgeeks.com. This is your only safe source for effective, virus free software. I recommend that you do **not** get one that costs money. There are just too many free ones out there that will do the job. So, go here: http://www.majorgeeks.com/. Look at the left panel labeled **FILES**, and in the list find **Drive Utilities**. Double click that and select **Shred, Format and Wipe**. You will be presented with at least four dozen possible programs.

Make your selection based on: 1. No cost (freeware, not shareware). 2. Date (don't select a program written in 2001 or earlier). Anything from about 2014 to the present should be OK. 3. Select based on use. If you want to securely wipe SD Flash, Compact Flash and USB drives as well as files on your hard drive, look for Koro File Shredder or the like, which advertises that capability. 4. Select one or two, try them and select one. Now you have a useful security tool.

One last thought. These utilities will render your files unrecoverable. There is no going back, once you shred a file. Double check that this is what you want to do, ***before*** you do it. Happy Computing!