THE COMPUTER CORNER

# No. 169: What I Do To Wipe a Drive

Stan Kaplan, WB9RQR
715 N. Dries Street
Saukville, WI 53080-1664
(262) 268-1949
skaplan@mcw.edu

I rebuild and distribute computers (free) to ARES/RACES units around Wisconsin. When a donated desktop or laptop comes in, how can I insure that I am not distributing viruses or other malware, or even distributing confidential data left over from the person or institution that donated the machine? Let me give you some background to illustrate why the answer to this question is so vitally important.

When you delete a file in a modern Windows installation (or even ancient DOS), the contents of the file are not removed from the hard disk (the same is true for a floppy). On deletion, all that happens is that a reference to the file is removed from a hidden table that lists all the files on your hard drive. That means that the OS (Operating System: Windows or DOS or whatever you are using) is free to write new data in the space occupied by that file, overwriting the original data. But until that happens, all of the data contained in that file is still there (and accessible by those who know how)! So, files that you believe are gone forever are really not. Proper application of a file-undelete or recovery program can get them back. Even if they have been partially overwritten, the remaining snippets of information can be read using certain tools. So, deleting files in this conventional way is not a secure option.

What about reformatting a hard drive? In the old days, a process called “low-level formatting” could be applied which would truly wipe the data. But, since the late 1980’s, true low level formatting became impractical for the end user to accomplish without destroying the drive. Indeed, in most cases, it is not even possible anymore once the drive leaves the hard drive factory. So, when you format a hard drive today, it is really a “high level format”, a format at the file system level. A file system level format works exactly like deleting a file (with regard to the data). The contents of all the files are still there, though the space becomes available to be overwritten with new data. So, formatting a hard drive is also not a secure option. Give me a freshly formatted hard drive and I promise you I can still read the files!

What about malware (viruses, spyware, etc.)? Erasing malware files, even if you can identify and locate them, just removes the reference to them in a table, as we saw above. Formatting the hard drive does essentially the same thing. Furthermore, malware writers often put in a “back door”, wherein an erased malware file may be un-erased. Malware may also be planted in areas on the hard drive that are not accessible to the OS and therefore cannot be “seen” by it (or you). Or, malware may cloak itself by telling lies to the OS about what is contained in a particular spot on the hard drive. That is why virus scanners sometimes fail to clean infections. They rely on the OS’ file system to find out where files are. A cloaked malware file may not be visible at all to a scanner.

So, to be truly secure, the only way to go is to completely wipe the entire hard drive. This destroys the files, the formatting, the partitions (C: , D: , E:, etc.) and leaves the hard drive in a state virtually exactly the same as the day it left the hard drive factory (except for subsequent wear and tear). That is what I do to all ARES/RACES rebuilds.

I use Webroot System Eraser, a utility that came free with product I bought from Webroot years ago. Put a bootable CD in a machine with System Eraser on it, and one is presented with a number of possible wiping schemes. I use the Department of Defense approved method, which consists of changing the first bit on the hard drive to a 1, then a 0. Then it does the next bit.

When it has finished the entire drive (all 800 gigabits on a small 100 gigabyte drive), it goes back and does it again, from front to back. After the second pass, it does it a third time. This means that a small 100 gigabyte drive has 4,800 gigabits changed after the three passes are done. It takes several hours to completely wipe a drive in this way. But, when done, even a government forensic laboratory would not be able to recover data from the drive, notwithstanding their very sophisticated methods. The drive is really clean!

There are a bunch of free drive wipers out there. Here are just a couple, and all of them are available on the Utimate Boot CD (UBCD; Google any of these titles for more info):

1. Darik's Boot and Nuke
2. Active KillDisk Free Edition
3. CopyWipe
4. HDDErase
5. HDShredder

You can also consult majorgeeks.com to find these or other wiping programs. They will even give you recommendations.

Be careful if you play with any of these! They do exactly what they were designed to do – they completely wipe your hard drive! Be sure that is what you want to happen, because everything will be gone, *permanently*.

When done wiping, the hard drive is blank. It will not boot. You cannot put files on it.

I then partition the drive, typically into a C:, D:, and E: partition. C: is for Windows, D: is for programs and E: is for user creations (documents, pictures, etc.). My partitioning software also high-level formats each partition, making it able to receive files. Then I add an Operating System. Now it will boot, and user files and programs can be added. And, it is squeaky clean of old data and malware! Happy Computing!