Formatting vs. Wiping a Hard Drive: Knowing The Differences.

By: David S. Capelli, MBA, CFC, ACE, CUC, CCE, DFCP  
Certified Forensic Examiner  
dcapelli@pvlforensics.com  
856.428.0878 (p)  
856.428.9401 (f)

You are upgrading to a new computer and giving your old computer to your friend. You have a new employee and are giving that employee a previously used computer. Or perhaps, you just want a fresh start on your existing computer. All of these instances certainly might lead you to decide that you want everything removed from the hard drive and the operating system re-installed – just as if it was a new computer coming out of the box. So, what method will be used in order to “clean” the disk and give it that fresh start?

The two methods that one can undertake in order to prepare a disk for a “fresh” installation of the operating system are formatting a disk and wiping a disk. What makes them different and what is the level of security for these methods? In others words – can any of the data be recovered after a format or wiping process has taken place? Depending on one's level of desire to prevent any possibility of data recovery, might determine which method is chosen. We look at both here and explain the differences.

Formatting the drive – The process of formatting a hard drive wipes its partition table clean and unlinks all the files in the files system, marking it entirety as writable space. It also sets up a new file tree to use with operating systems. However, data can still be forensically recovered from a formatted drive as it still exists on the drive. For process of formatting a drive can take place utilizing the operating system’s software and typically does not require any additional expense in terms of hardware or software

Wiping the drive (00 Hex) – The process of removing all data from the drive and making it unable to be recovered. This process places the “00 Hex” on the drive which is a series of zeros. Specialized hardware and/or software are needed to conduct this process. Typically, a user would need to purchase wiping software and execute the wiping process on the specific hard drive. The user can also purchase a hardware device that is entirely self-contained and capable of performing a wiping process on a hard drive or multiple hard drives at the same time. Such hardware is typically faster than the software method of wiping. However, these devices can be costly and are typically only purchased if an individual or an organization regularly wipes drives. The wiping process can involve either a (1) standard wipe which is a single pass & verify or (2) The Department of Defense (DoD) wipe which is seven passes & verify.