WHY SSD SHOULD BE WIPED BEFORE DISPOSAL

According to the US Department of Commerce data security breaches cost over $250 billion to US companies per year. This means providing confidentiality implies not only information to be stored properly, but also be destroyed according to certain rules. The following article is going to illustrate the main peculiarities of irreversible data destruction in order to allow a secure storage disposal.

The approach to perform this kind of operation will differ from the type of storage device: HDD (Hard Disk Drive) or SSD (Solid State Drive). The internal architecture of an SSD is very different from that of a hard disk, and the way SSDs store data is very different as well. This means that existing disk sanitization techniques originally used for HDDs won't work on SSDs.

Let's clear up how the data is basically managed on each type of the mentioned storage devices.

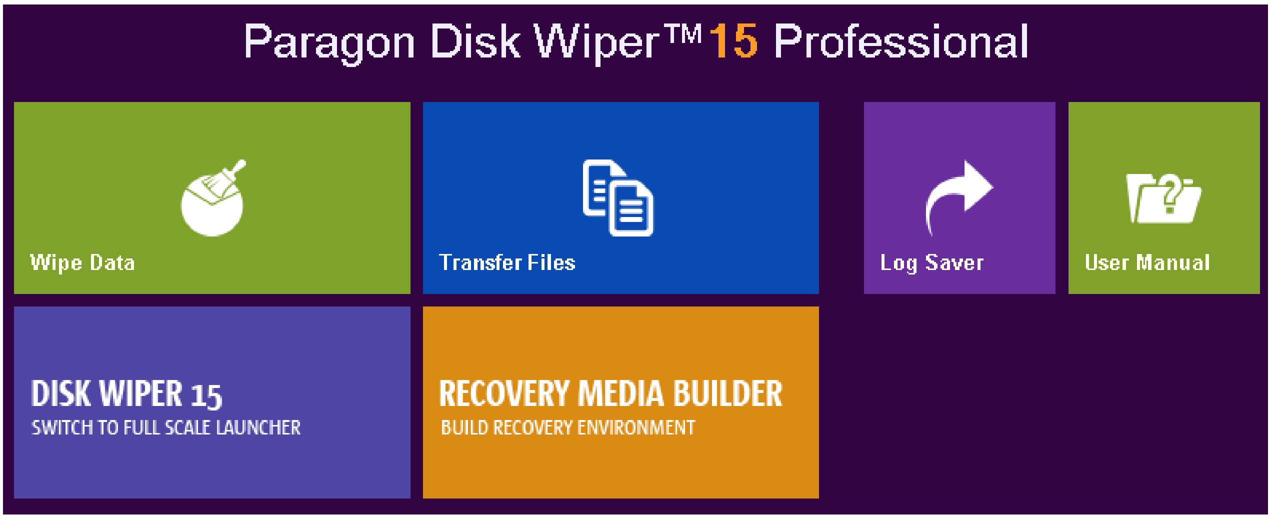
As you may know data is stored magnetically on traditional hard disks. As the heads pass over the magnetic substrate, bits of data are magnetically aligned and oriented in such a way that they can be interpreted as zeros and ones. Collection of these bits are put together to form bytes which are grouped in turn to form sectors. When you delete files on a HDD, an operating system actually marks corresponding sectors as 'unused' thus making them available for future write operations. As you can guess, these unused sectors can be easily recovered until they are overwritten by some other data. This is done to cut on system resources as writing over, instead of marking as unused would take much longer.

On solid state drives data is stored electronically, in special pages that vary in size from device to device. These pages are then grouped into erasure blocks which are then zoned together based on the physical address in the flash chip. The crucial is that data is not written to the pages sequentially but striped across the erasure blocks and is managed by a special controller. When the data is modified, the controller moves the entire block to a new location and schedules the original block for erasure. Deletion of files on an SSD is triggered by a special 'trim' command sent by an operating system directly to the drive.

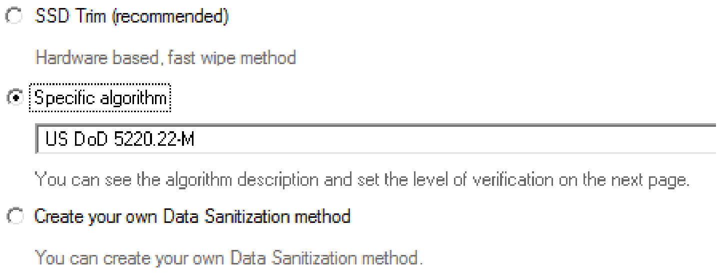
With this basic understanding of the way how data is managed, we can now look at existing data erasure methods. The most well known is a software based data wiping. Developed for hard disks, the essence of this method lies in writing a pattern of data to each sector of the disk in a sequential manner, thus overwriting the original data and making it unrecoverable while still leaving the storage device functional. But this method doesn't work great for solid state drives. First, an SSD has limited write cycles, and data wiping eat them up. Second, the erasure software is not able to control the specific region the data is written on as this is controlled by an SSD controller which doesn't guarantee complete destruction of on-disk data.

You might have however come across some articles on the Internet stating that you don't need to wipe your SSD, as the 'trim' command does the job by completely removing all traces of your personal data. Actually that is not quite true. Some researches has shown that this method is not successful when you delete an entire drive or individual volumes. The problem is that normally trimming is triggered by a file or folder delete operation and accomplished by relatively large blocks, which may lead to situations when remnants and entire small files remain intact. Besides, MFT (Master File Table) and other service areas are not trimmed at all, but they often contain user's data.

How to prevent moving your confidential data to the wrong hands together with your old SSD? Of course, you can physically shred your SSD into pieces that are small enough that a single chip cannot escape damage – an ultimate data destruction method, but not productive, as you won't be able to benefit from it. The best method is to use a specialized data erasure utility that supports solid state drives. For instance you can try out the latest Paragon Disk Wiper 15 which accomplishes secure data wiping on hard disks and SSDs without affecting their operating life.


Paragon Disk Wiper™ 15 Professional
Wipe Data
Transfer Files
Log Saver
User Manual
DISK WIPER 15
SWITCH TO FULL SCALE LAUNCHER
RECOVERY MEDIA BUILDER
BUILD RECOVERY ENVIRONMENT

Well known among IT professionals, the latest product version helps to not only irreversibly destroy an entire HDD, individual volumes, or remnants of deleted files through 10 different wiping algorithms, including major military and government disk sanitizing standards, but it now offers effective and safe data wiping for SSD, which employs the 'trim' command for individual volumes or an entire drive.



○ SSD Trim (recommended)

Hardware based, fast wipe method

● Specific algorithm

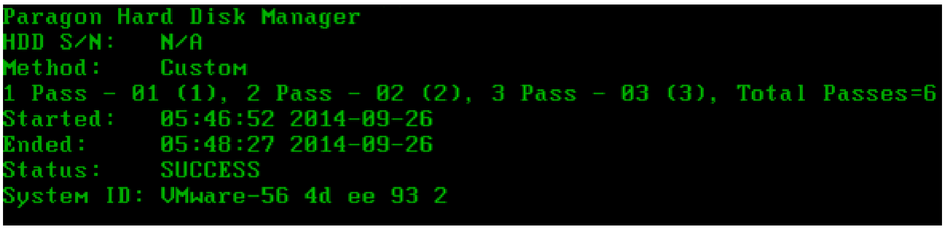
US DoD 5220.22-M

You can see the algorithm description and set the level of verification on the next page.

○ Create your own Data Sanitization method

You can create your own Data Sanitization method.

Among other new features to mention is a new streamlined, tile-oriented interface, support of the latest Windows 8.1 and bitlocked volumes, and the so-called 'wipe stamp option', which enables to add to the MBR (Master Boot Record) of the wiped storage device information on the used wipe program, algorithm, device serial number, wipe status, system ID (obtained through WMI), etc. Thus when attempting to boot from this storage, you'll be notified how and when this storage has been wiped.



```
Paragon Hard Disk Manager
HDD S/N:   N/A
Method:    Custom
1 Pass - 01 (1), 2 Pass - 02 (2), 3 Pass - 03 (3), Total Passes=6
Started:   05:46:52 2014-09-26
Ended:     05:48:27 2014-09-26
Status:    SUCCESS
System ID: VMware-56 4d ee 93 2
```

Another novelty of Paragon's Disk Wiper is a unique offering on the market at the moment! Besides a Windows installer, the product has been including the option to build WinPE or Linux based bootable media to wipe storages without installing the product. Now you can also start up a Mac computer with the prepared Linux based media and erase data it contains in such a way that even advanced forensic tools should not ever be able to recover it. Well, this could be a great news for our Mac community that can safely dispose of hard disks and solid state drives at last!