(Approx. 837 wods)

Really, *really*, deleting files
by Chris Taylor, President

Ottawa PC Users' Group, Ontario, Canada

Published in Ottawa PC News (September 2023)
<https://opcug.ca>
Editor: brigittelord (at) opcug.ca

When you delete a file in Windows, the actual on-disk data is not removed. The file is usually moved to the Recycle Bin, where it can be easily recovered. Even if you empty the Recycle Bin or bypass the Recycle Bin by holding down the Shift key while deleting files, the data remains on disk. All that happens is the pointers to the file are removed, making the space available for new files.

**Recovering deleted files**

Utilities to recover deleted files date back to ***Unerase*** in the first version of the Norton Utilities in 1982. They continue to this day with dozens of free and commercial programs available for Windows, macOS, Linux, Android, and iOS.

If you are in a high-security situation, please ignore this article. It is intended for the average home or business user whose adversaries are not about to use [magnetic force microscope](https://en.wikipedia.org/wiki/Magnetic_force_microscope) techniques to recover data. If you are likely to have [CSIS](https://www.canada.ca/en/security-intelligence-service.html) looking for your deleted data, you need to go well beyond what I recommend here.

**Making data unrecoverable**

When you want to dispose of a storage device, you should ensure all sensitive data is deleted and ***unrecoverable***. This can be achieved by physical destruction of the storage device: hard disk drive (HDD), solid-state drive (SSD), flash drive, etc., or—if you want the storage device to be reusable—by over-writing the data areas of the disk with random data, obliterating the original data.



Some secure deletion programs boast of capabilities such as the [Gutmann algorithm](https://en.wikipedia.org/wiki/Gutmann_method), which overwrites all data with 35 passes. For the average computer user, I wouldn't worry beyond a single pass.

There are many programs available, both free and commercial, for secure data removal. The programs I list are not necessarily the best—they are simply programs that have been around quite a while (have stood the test of time), are free, and have been used successfully either by me or other members of OPCUG.

Be careful using secure deletion programs. By their very nature, there is no "undo" button! There are several levels of overwriting data: individual files, free space on the drive, and the entire disk.

**Individual files**

If you just want to make a few files unrecoverable, there are programs that can target individual files or folders of files. One example is the free and open-source program File Shredder (<https://www.fileshredder.org/>). It is very simple and straightforward to use.

**Free space**

Storage devices eventually end up with data in all locations on the device. The free space has data that was used for files that have since been deleted. You have no way of knowing what recoverable data might be there. Some programs can target free space and securely overwrite data there. File Shredder is one program that can wipe free space.

**Entire disks**

If you want to securely delete all data on an entire storage device, HDShredder (<https://www.miray-software.com/products/applications/hdshredder.html>) is available in free and commercial versions. The free version should be sufficient for the vast majority of users. The website details the additional capabilities in the commercial versions.

Another popular program for securely erasing all data on storage devices is the free and open-source DBAN (<https://sourceforge.net/projects/dban/>). DBAN was acquired by [Blancco](https://www.blancco.com/) in 2012 and is no longer in development but remains popular. I recently had occasion to use DBAN to help a friend dispose of an old laptop, and it was quite easy to use DBAN to ensure the entire hard drive was securely wiped.

DBAN comes as a disk image (.ISO file), so you will need a program to create a bootable flash drive, CD, or DVD using the DBAN ISO file. Free options are available, such as Rufus (<https://rufus.ie/en/>), NCH Software's Express Burn (<https://www.nch.com.au/burn/index.html>), and Ashampoo Burning Studio Free (<https://www.ashampoo.com/en-us/burning-studio-free>).

**Solid state drives**

Due to the architecture of the technology, SSDs cannot be securely wiped in the same manner as HDDs. If you want to securely delete data from SSDs, check that the software you are using specifies that it works on SSDs. EaseUS has a free version of Partition Manager (<https://www.easeus.com/partition-manager-software/securely-erase-ssd-hdd.html>) that can securely erase SSDs.

Some SSD manufacturers provide special utilities to securely wipe their devices, such as Samsung's Magician (<https://semiconductor.samsung.com/consumer-storage/magician/>) or Crucial's Storage Executive (<https://www.crucial.com/support/storage-executive>). Personally, if the manufacturer of your SSD has a special utility for securely erasing their branded SSDs, I would choose that option.

**Final words**

Rather than destroying or securely wiping old storage devices, you might want to repurpose them for your own use. Inexpensive drive enclosures are available: you can install your old storage device in one and then plug it into a USB port to use it as an external drive.

While this article details effective means of securely removing data, if you can't be sure you have completely removed all sensitive files from your device, you might be better off destroying the device rather than disposing of it.