How to securely erase your hard drive

The siren has sung and you've finally succumbed to her call: You're the proud owner of a shiny new PC; a faster, better SSD; or a bigger, better hard drive. It's time to toss your old equipment in the trash and start playing with your new toys, right? Not so fast.

First you need to clean the data off your old drives so you don't become a victim of identify theft. Simply deleting the data off your hard drive doesn't actually delete it; it basically just hides it from immediate view. To truly hide the data on your storage device and protect yourself against identity theft, you need to take much more drastic (and time-consuming) measures that overwrite your drive space with ones and zeroes. That's where this guide comes in.

Different technology and scenarios call for different tools. We'll identify the best secure-erasing utility for every job, no matter what type of drive you're using—even USB flash drives. If you want to erase only specific files, we'll show you how to do that, too. Best of all, every solution discussed is free.

Before you begin

Back up your data! Once these programs get ahold of your drive, you can't go back for a forgotten file. And if you're going to erase a laptop's hard drive, be sure to plug the notebook in before you start. If the power goes out in the middle of a disk wipe, it could spell disaster for the drive.

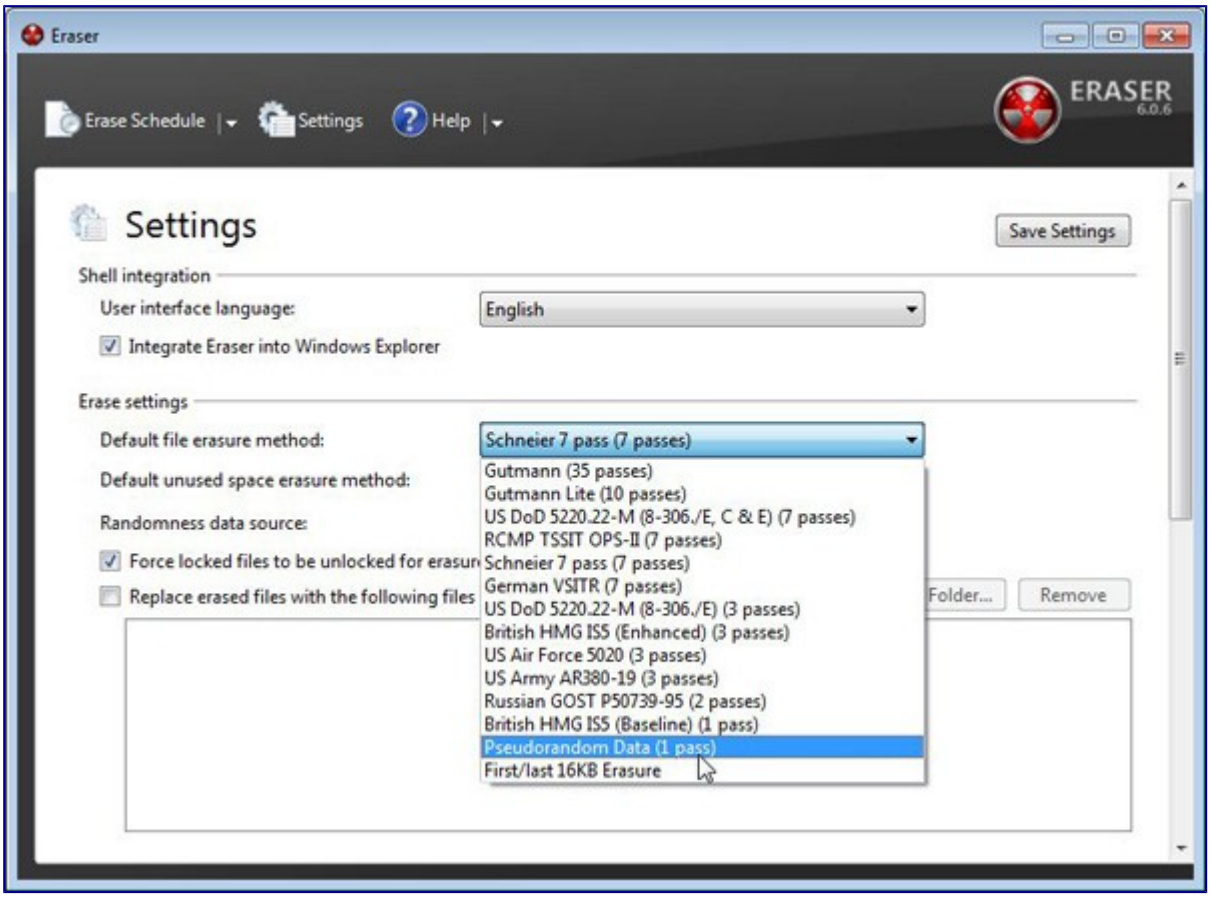
Let's talk terminology. Drive-wipe utilities specify how many "passes" the software makes. Each pass signifies a complete overwrite of the data, so a utility that makes three passes overwrites your data with ones and zeroes three separate times. The more times you overwrite your data, the less likely it is to be recovered. Some utilities support "Gutmann"-level protection with 35 passes, but three passes is enough for the U.S. Department of Defense's "Short" specification and for numerous militaries around the globe.

Remember, you also have the option to simply encrypt your entire drive and throw away the (encryption) keys rather than securely erasing everything from the drive. Disk encryption is pretty robust these days and this method should suffice in general circumstances—but why take chances? Encrypting drives and wiping drives each take a big chunk of time, so you might as well erase the data completely.

Note that if you do choose to erase your data with any of these methods, you do so at your own risk—which is why we advise making a backup before you begin. Nevertheless, we have used all of these methods successfully in the past.

Securely erase specific files with Eraser

If you need to delete only specific files and folders rather than entire drives, the open-source Eraser is the tool for you. Just boot up the program, click the arrow next to the 'Erase Schedule' option at the top of the screen, and select *New task*. From there, a window pops up with the task and time-scheduling options. Click *Add Data* to select the files to wipe and choose an erasure method. (I usually go with the DoD three-pass option.)



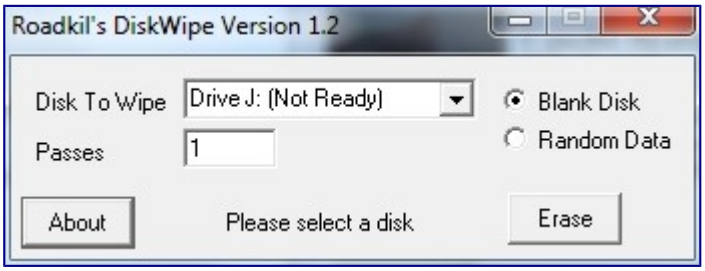
An Eraser option also appears when you right-click on a file in Windows Explorer, allowing you to permanently delete files quickly and easily.

Eraser has a ton of advanced scheduling and file options if you want to securely wipe specific files or sectors of your hard drive on a regular basis. Be careful while you tinker with the finer settings, though—you don't want to accidentally wipe something important. Also note that Eraser works only with mechanical hard drives, as the wear-leveling algorithms in solid-states drives (SSDs) negate the utility's ability to securely wipe information.

Securely erase your USB flash drive

Did you think using Erase was simple? Roadkil's Disk Wipe is even easier, and it works just fine on USB flash drives as well as traditional hard drives. Simply download, unzip, and boot the itty-bitty application, and then select a drive and type in the number of passes you'd like the program to make. (Again, we suggest at least three.) Choose to either wipe the disk or fill it with junk data, click Erase, and you're done. Roadkil's Disk Wipe hasn't been updated in

years, but it hasn't needed to be—it just works. Be sure to select your operating system when you downloading the utility.

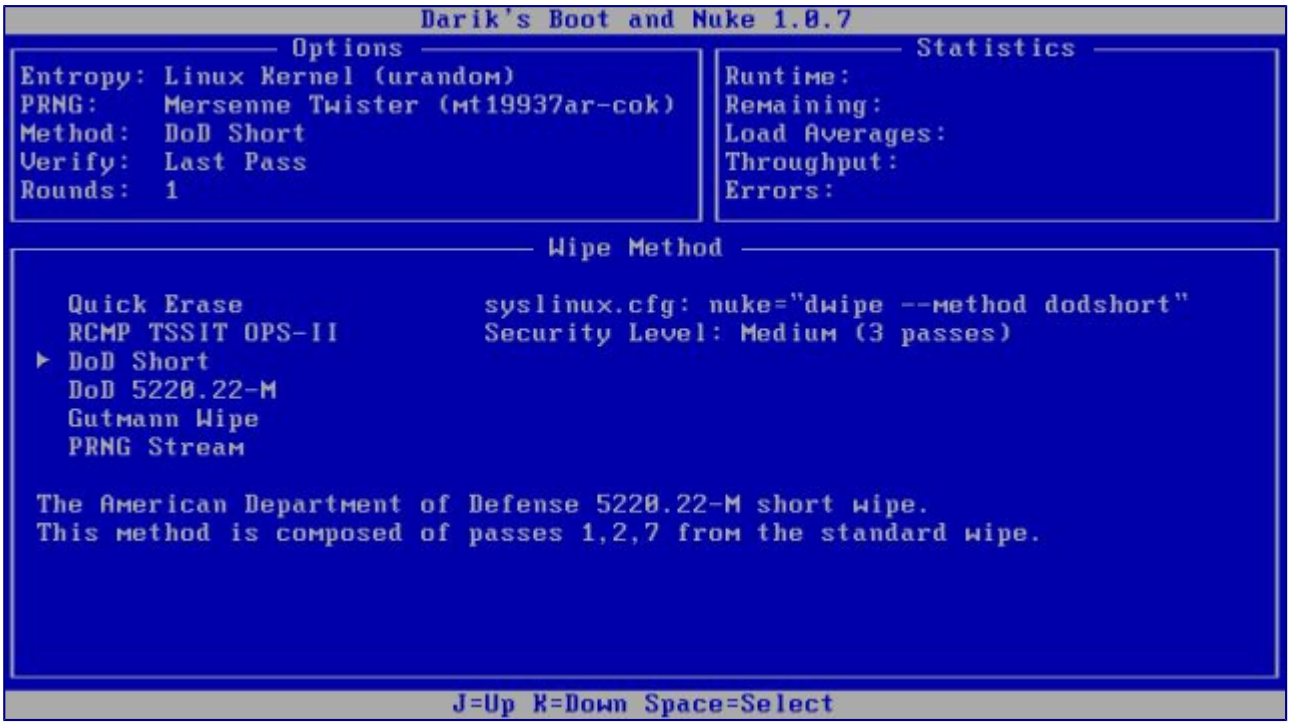


A note on whole-disk wiping software: Wiping entire drives requires slightly more complicated solutions than the easy-to-use apps mentioned previously. Since you'll be deleting the data from the drive that likely holds your PC's operating system, most tools that wipe whole drives require you to move the program to a flash drive or create a bootable disc from an .iso file.

To ensure that things run smoothly, you should also dive into your BIOS settings and make sure that your drives are set to IDE mode.

Securely erase a mechanical hard drive with DBAN

Download DBAN—a time-tested option for erasing HDDs that's loved by geeks around the world despite the fact that it hasn't been updated in years. Once you've downloaded it and burned the .iso to a disc, insert the disc into your PC and tell your computer to boot to the optical drive rather than your hard drive. If you're hoping to erase a RAID-enabled hard drive, you'll need to disassemble the RAID volume and set each disk to JBOD mode before you start, as well.



Once DBAN is up and running in all its blue-and-white glory, you simply select which disk to wipe and press the **M** key on your keyboard to select an erasure method. The three-pass "DoD Short" is (still) my preferred method, though more-robust options are available. Press **F10** to start the wipe once everything looks good. Depending on the method you choose and the size of the disk, erasing the data can take hours or even days. Bring a sandwich and a copy of *PCWorld* magazine, or better yet, walk away and do something else while DBAN does its magic.

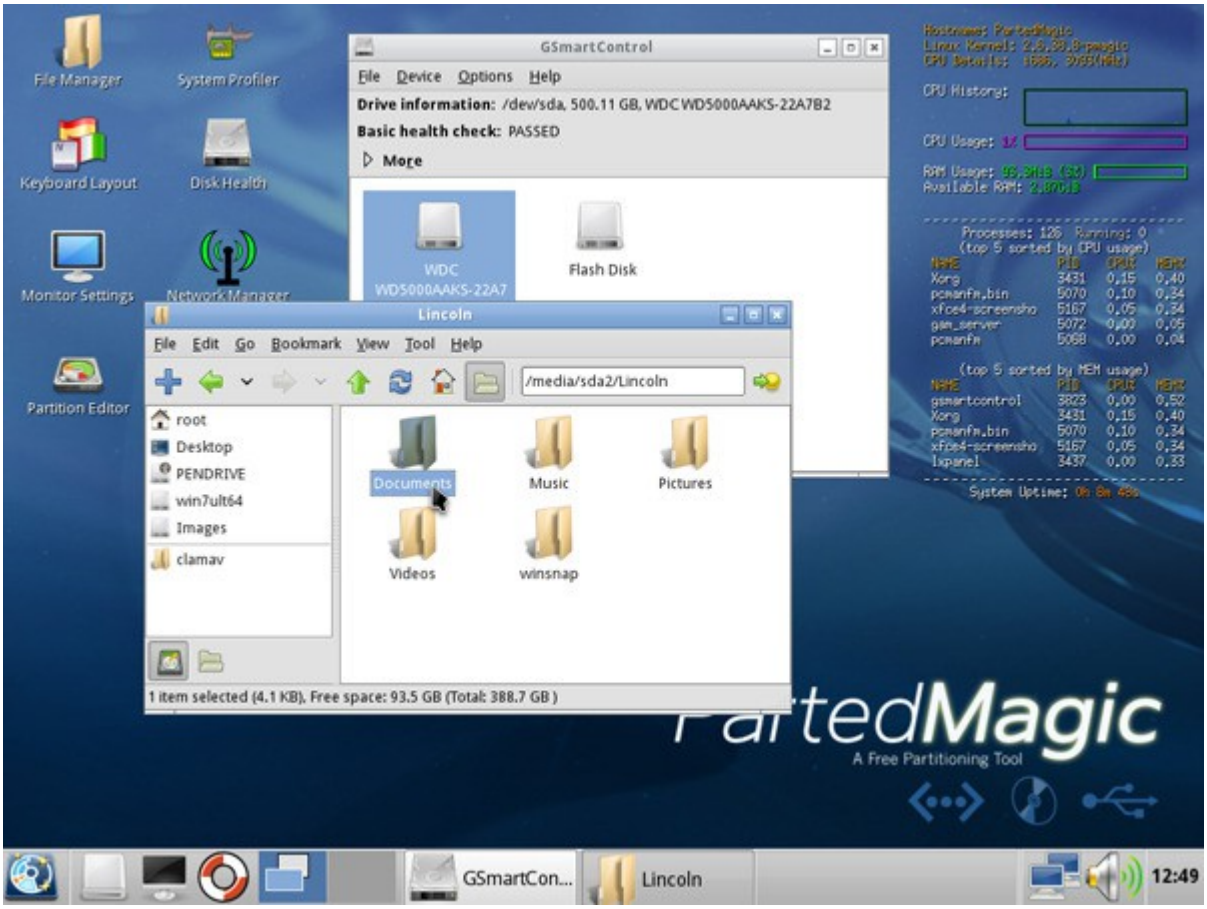
Securely erase a hybrid drive or SSD with Secure Erase or Parted Magic

Wiping data off of an SSD is a little different than erasing data from a HDD thanks to the wear-leveling algorithms used to write data evenly to an SSD. To securely erase all the data on an SSD, you use a command—called Secure Erase, appropriately enough—that's built into the firmware of all modern SATA drives and older PATA/IDE drives. Some SSDs ship with the ability to initiate secure erase, but if your drive doesn't, two top third-party programs that can activate the command and wipe SSDs are the Center for Magnetic Recording Research's Secure Erase tool and Parted Magic.

To run the CMRR's Secure Erase tool, you'll need to download the utility and then transfer the file to a flash drive or CD and boot to it directly. Type **hdderase** in the DOS prompt and press **Enter** to start the wipe. The utility works on SSDs and mechanical hard disks alike, which makes it perfect for use with hybrid drives.

While CMRR's Secure Erase is a battle-tested performer, it hasn't been actively developed in several years. If you run into compatibility issues using it, run Parted Magic instead. Ostensibly a tool for managing partitions, Parted Magic also includes a method for activating the Secure Erase command, though it's a little hidden.

Boot into Parted Magic and erase your disks from there.



Before you get to that part, though, you'll have to download the Parted Magic .iso (click the previous link to go to the download page) and use it to create a bootable disc. Boot the disc, and click on the Start-type button at the lower left. Hover over the System Tools option and select *Erase Disk* in the menu that appears. A window of various erasure options will pop up; the external commands work well with traditional hard drives, but you should select *Internal: Secure Erase command writes zeroes to entire data area* to wipe your SSD. Click *Continue,* and then pick a doomed drive and click *OK* to send its data into the abyss.

If Parted Magic warns you that your drive is frozen, put your computer to sleep as suggested and turn it back on and rerun the utility. If you're asked whether you want to run an Enhanced Secure Erase, click *No*; you'll want to stick to the tried-and-true standard version.

(source: http://www.pcworld.com/article/261702/how_to_securely_erase_your_hard_drive.html)