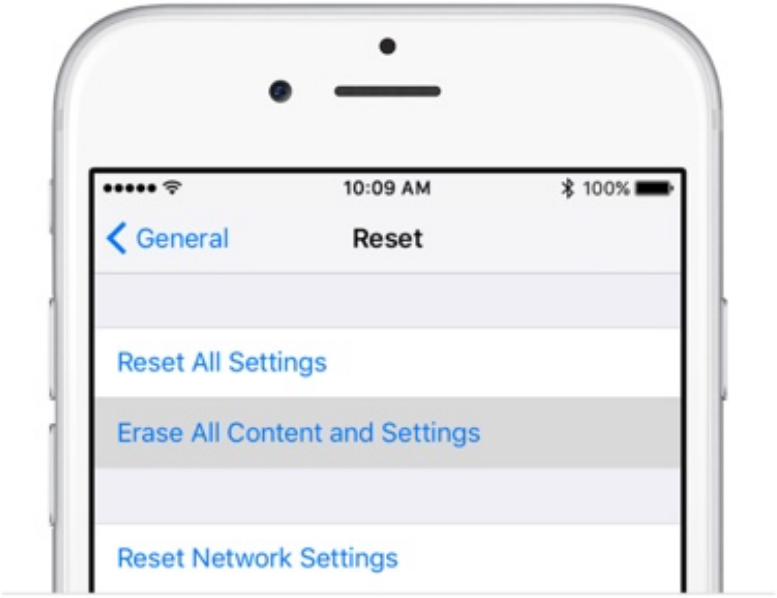
How to securely wipe the data off hard drives, SSDs, flash drives, iPhones and iPads, and Android devices

Published: August 4, 2018



We live in an age where a little bit of paranoia is healthy and making sure that out personal information is safely and securely erased off devices we've used is a good thing. Here's a quick guide to securely wiping hard drives (HDDs), solid state drives (SSDs), flash drives, and even iOS and Android devices.

Built-in way to erase iOS and Android devices

iOS and Android devices both have built-in tools to erase the devices.

- On iOS: **Settings** > **General** > **Reset** and then tap **Erase All Content and Settings**.
- On Android: **Settings** > **Backup & reset** > **Factory data reset** and then tap **Reset phone** or **Reset device**.

You can also securely wipe the devices remotely using Find My iPhone for iOS or the Google Account associated with the Android device.

Price: Free

The hands-on method

Not sure how to erase a device? I guarantee you that if you get a big enough hammer and spend enough time hammering, this will work on anything!

This method also works great if you just want to destroy drives before you take them to the recycling plant. It's also a great stress reducer!

You will need:

- A hammer (I use my trusty 32oz "fine adjustment" hammer)
- A thick nail (a 6-inch nail will do fine)
- Thick gloves - because you're going to be hammering that nail through the drive using the hammer, and hammers seem to be magnetically attracted to thumbs
- A block of wood -- so you don't nail the drive through your floor (it's preferable to do this outside if you can)
- Eye protection -- you've only got a maximum of two to start with, so it's silly to take chances!

Now you apply brute force. Ideally you want to put a nail through the platters of the drive, going all the way through (it's actually not as hard as it sounds). I aim for the spot marked by the red X on hard drives.

Alternatively you can use a power drill to make holes, but make sure that you have a way to securely hold the drive, for example, using a vice. Don't hold the drive in your hand because if the drill bit catches and the drive starts to spin -- or "helicopters" -- on the end of the drill then there's a real risk of injury.

Another thing to bear in mind is that the data in SSDs is held on small flash storage chips rather than large platters, and to securely erase the data you need to smash the chips. Usually, this means taking the cover off the drive before you start swinging.
If you're not sure which are the flash storage chips, just drive a nail through all the large chips to be on the safe side.
Price: Free

What about storage that's defective but under warranty?

The time that wiping storage devices gets complicated is when the device is broken or malfunctioning in some way.

For example, a hard drive that dies, or a storage card that can no longer be accessed.

What do you do if you have to return something under warranty but there's data stored on the device?
Well, things get complicated.

You could rely on the face that the device is dead, and that your data is inaccessible, but that's probably not the case. Data can be recovered off most storage devices if you are willing to throw money at the problem. You might not be able to get access to it, but someone else could.

If this is something that you're worried about then the best thing to do is to ask your vendor in advance what their policy is and buy based on what the answer you get is. Some will point you to a privacy policy, others will allow you to physically destroy the device before returning it (common for smaller items like microSD cards and the like). Sometimes, as is the case with a PC or external storage system, you might be able to remove the drives before returning the device for repair (assuming it's not the storage that's died).

Another option open to for many devices is to encrypt all your data. If the data on your PC, external storage, or flash drive is encrypted (and the encryption is legit, and assuming you've chosen strong passphrases and the like), then the data is likely unrecoverable to third parties.

Use high-end storage with built-in data destruct features

High-end encryption devices -- such as the Apricorn Aegis Secure Key 3z -- will have a built-in data destruct feature where you enter a PIN code or run a program that will securely wipe the device.

PIN code data destruction is especially handy because after you enter the PIN the device destroys the encryption key and appears blank boots up, offering plausible deniability.

StarTech 4-bay drive eraser

If you have a lot of drives to erase, you need a professional piece of kit that can keep up with the demands that you're going to place on it.

This hard drive eraser provides standalone, simultaneous drive erasing for up to four 2.5-inch or 3.5-inch SATA hard drives or solid-state drives.

Unlike hard-drive docking stations or adapters that require a computer connection and software to erase drives, this hard drive sanitizer features standalone erasing that doesn't require a host computer. This avoids the hassle of connecting your drives to a host computer and protects your drives from external security threats like remote data access.

The four-bay design maximizes efficiency by batching multiple drives in single erase projects, saving you valuable time. The hard drive eraser supports USB 3.0, also known as USB 3.1 Gen 1, with file transfer rates of up to 5Gbps.
Price: $815 | More information

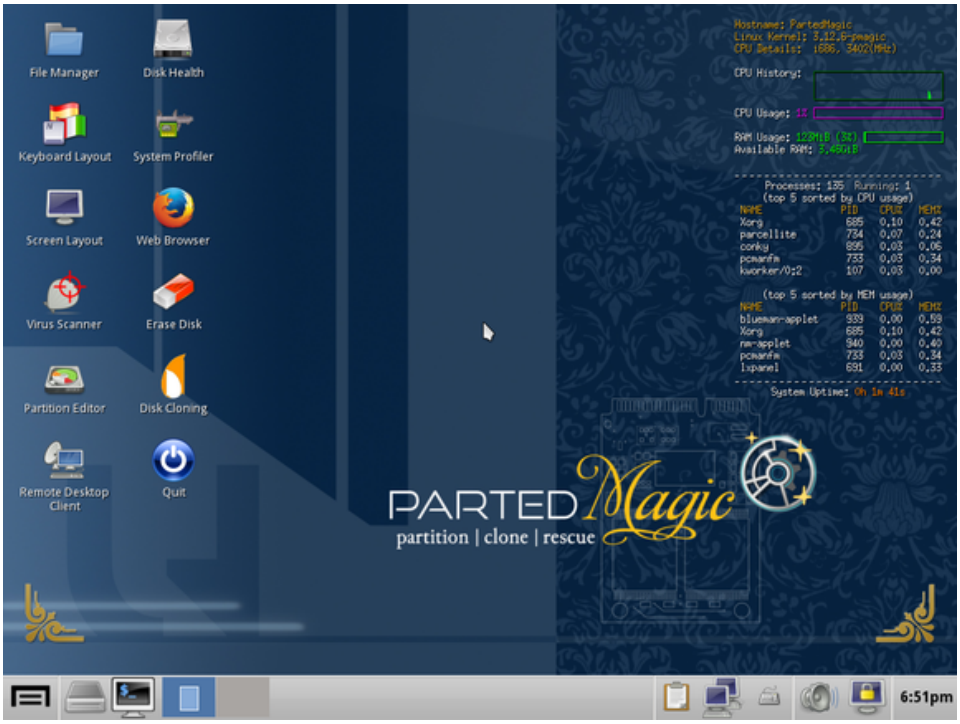
DBAN - Darik's Boot and Nuke

This is the default tool that most people who have the odd drive to erase turn to. I've used this tool to wipe thousands of drives and found it to be both thorough and very effective.

While DBAN is an awesome tool, it's important to understand its limitations. Here is what the new owners of DBAN, Blancco Technology, have to say:

"While DBAN is free to use, there's no guarantee of data removal. It cannot detect or erase SSDs and does not provide a certificate of data removal for auditing purposes or regulatory compliance. Hardware support (e.g. no RAID dismantling), customer support and software updates are not available using DBAN. Should you need to erase data from a SSD or require a certificate of data removal, request a free trial of Blancco Drive Eraser."

Price: Free | More info/download



PARTED Magic

Another way to do this is to use a software tool called PARTED Magic.

While PARTED Magic is not free (price starts at a reasonable $11), it is a very effective tool, and one of the best I've used for wiping SSDs, as well as the depth of information it offers.
This tool also does a lot more than data erasure:

- Data cloning
- Benchmarking
- Disk partitioning
- Data rescue
- System stability tester

Price: $11

Blancco Drive Eraser

This is the go-to tool for professional, certified, drive erasure. Guarantee your data has been erased from any drives, including complex SSDs in desktop/laptop computers, servers and storage environments with the most certified and patented data erasure solution.

Includes advanced features such as:

- Patented solid state drive (SSD) erasure (Patent No. 9286231).
- Erases data permanently from multiple HDDs/SSDs simultaneously
- Automates the hard drive wiping process to remove system BIOS free locks
- Local and remote deployment
- RAID dismantling and pass through
- Identifies false positives during internal data erasure processes
- Provides digitally signed certificate of proof of secure erasure for auditing
- Compliant with state, federal and international data privacy regulations and guidelines, including ISO 27001 and ISO 27040

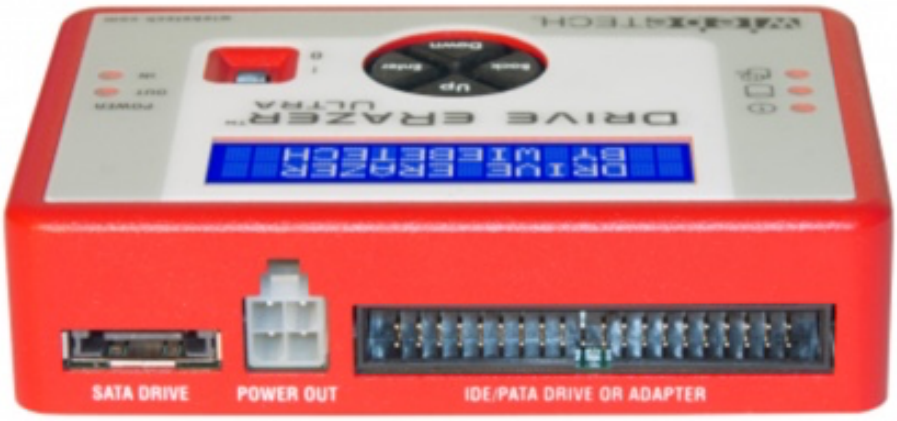
Price: $18.46 per erasure I More info/download

Blancco Mobile Device Eraser

Blancco mobile and phone wiping software allows organizations, mobile service providers and resellers to permanently erase all data from smartphones and tablets running on iOS, Android, Windows Phone and BlackBerry operating systems.

- Securely wipes iOS, Android, Windows Phone and BlackBerry operating systems
- Quickly erases data on up to 50 mobile devices simultaneously
- Automatically selects the fastest and most effective data erasure method
- Provides digitally signed certificate of proof of data erasure for audit trail purposes
- Compliant with state, federal and international data privacy regulations and guidelines, including ISO 27001 and ISO 27040

Price: $13.52 per erasure | More info/download



Wiebetech's Drive eRazer Ultra

The WiebeTech Drive eRazer Ultra is a stand-alone device that completely and quickly cleans hard drives. Simply connect a drive to the Drive eRazer Ultra and it will sanitize the drive faster than using software, and without tying up your computer.

The Drive eRazer Ultra leaves the drive ready for safe re-use, and comes with a dozen different preset erase procedures, including US Department of Defense graded methods for data wiping.

Additional features:

- Simple setup and operation with LCD and menu buttons
- USB port for drive previewing and deletion confirmation
- Serial label printer connector
- Rugged aluminum construction
- 3-year warranty
- Free US-based customer support

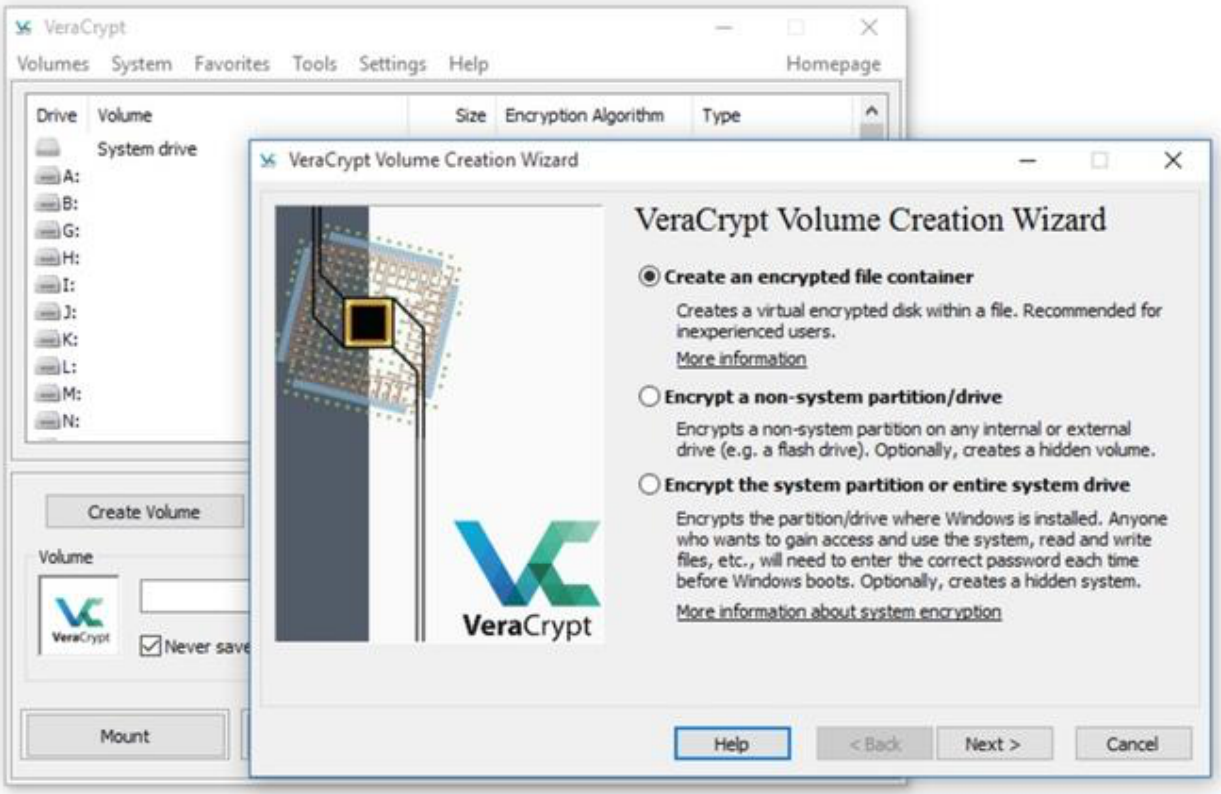
Price: $249 | More info/download

ProtectStar Data Shredder

I like ProtectStar Data Shredder software because it works across the board -- Windows, Mac, iOS, Android, even Apple TV.

This tool meets and exceeds government, military and industry standards for the permanent erasure of digital information and erases all existing data up to top-secret security level data.

Price: Depends on version and platform



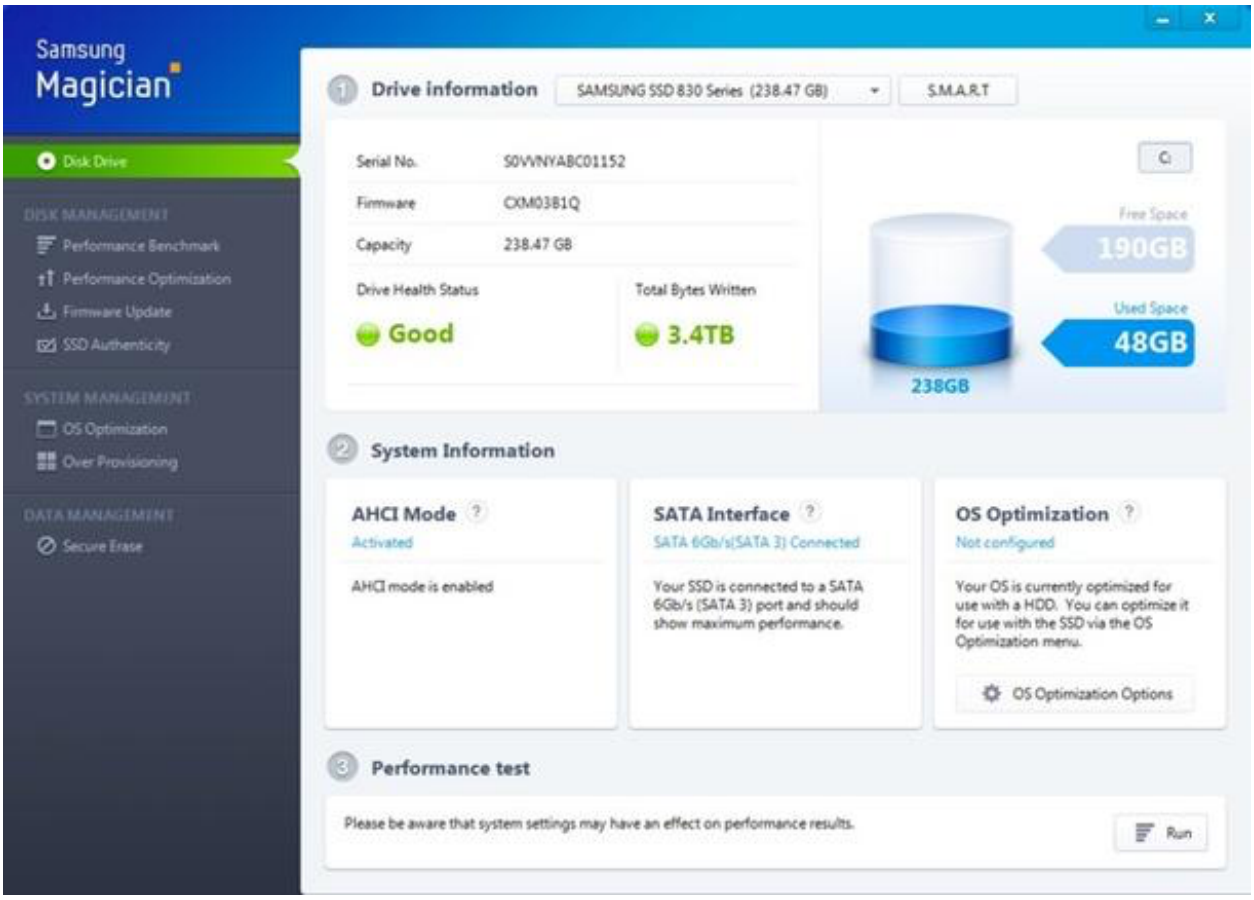
Encrypt the whole drive

One of the easiest -- and certainly the cheapest -- ways to erase data on a device is to encrypt the entire drive with a complex passphrase. You can use built-in tools such as BitLocker on Windows or FileVault on macOS, or a third-party tool such as or third-party VeraCrypt. Encrypt the drive with a strong throw-away passphrase and you're done.

No passphrase, no data.

You can then format the drive, from which point it should be sterile and ready to accept a reload of the data.

Price: Free



Erase using manufacturer utilities

Another way to erase SSDs is to use the manufacturer utilities. Here are some links to get you started.

- Intel Solid State Toolbox
- Corsair SSD Toolbox
- SanDisk SSD Toolbox
- Samsung Magician Software
- OCZ Toolbox

Price: Free