Applies to all: Encryption!

The universal method for securely removing all data from a drive is to encrypt all the data in the first place!

Erasing encrypted drives with the "Dumb" method MAY NOT always be complete, however. Encrypted drives need a section of data holding the decryption keys, which are unlocked at boot with your password. This data block WILL be erased when an encrypted partition table is erased, but over time, the block/sector the data is stored on may fail. If this happens, the drive copies the data to a new location and abandons the bad block/sector, with the data intact. This block is not acessible from the OS, but could theoretically could still be acessed and read.

Utilizing encryption from the start ensures that, no matter what formatting method is used (even the "Dumb method"), any data remaining on dead secotrs/blocks is properly useless.

Self-Encrypting Drives

Some SSD's support self-encrypting, making secure erase as simple as scrambling the stored the keys saved on disk. More info here (Arch only).

Windows: BitLocker

On Windows, set up Bitlocker on the C: drive (requires Windows Pro). This is done AFTER installing WIndows, simply right click on C: and select "Turn on BitLocker". You will have to set up either a USB key or password/PIN to unlock the drive when booting.

To erase securely, follow the Windows directions in the other sections depending on drive type and secure formatting features.

Linux: LVM + LUKS

For non-encrypting SSD's and HDD's, Arch supports encrypted LUKS volumes, which can either act directly as a partition, or can be a container to house multiple partitions. a single LUKS volume with multiple partitions is the easiest to manage, as you can use the same key to encrypt root, /home, swap, etc.

Only the boot partition remains unencrypted. Same as self-encrypting drives, securely erasing a LUKS encrypted drive is as easy as erasing the LUKS header data from the volume (which stores the keys required to decrypt.)

More info here (Arch) on setting up an enecrypted volume.

More info (also Arch) on preparing/wiping an encrypted disk.

Revision #5
Created 2023-01-14 22:19:27 UTC by Dev
Updated 2023-01-15 00:48:12 UTC by Dev