SATA SSD's: ATA Secure Erase

MOST SATA-based SSD's support some type of secure-erase. This is a much faster and more effective method of erasing data than the one as described in Dumb but Effective.

Instead of overwriting with pseudorandom data at the OS level, which may leave some bad blocks in tact, an SSD that supports ATA Secure Erase will use various methods of erasure on ALL BLOCKS on the drive, including the damaged/unavailable ones. This has the same effect as overwriting the drive with data, but with the added benifit of also overwriting the bad blocks.

Note that supported drives may be "frozen" by the BIOS, usually because of Secure Boot. Disable Secure Boot if SSD's refuse to "unfreeze"

Linux:

Best: Sanitize on tinyapps.org

1. install `hdparm`
2. check drive supports sanitize with `hdparm --sanitize-status /dev/sdx`. Supported sanitize features will be displayed for supported drives, options are block erase, crypto scramble, and overwrite.
3. run a supported sanatize command:
   a) `hdparm --yes-i-know-what-i-am-doing --sanitize-block-erase /dev/sdx`
   b) `hdparm --yes-i-know-what-i-am-doing --sanitize-crypto-scramble /dev/sdx`
   c) `hdparm --yes-i-know-what-i-am-doing --sanitize-overwrite-passes 1 --sanitize-overwrite hex:11111111 /dev/sdx`

Alternate, less secure: Secure Erase on tinyapps.org

1. install `hdparm`
2. check drive supports erase with `hdparm -I /dev/sdx`. it may be frozen, sleep and wake the PC to fix.
3. Set password (arbitraily set to "p") to enable secure erase: `hdparm --user-master u --security-set-pass p /dev/sdx`
4. erase drive with: `hdparm --user-master u --security-erase p /dev/sdx` (use `--security-erase-enhanced` if supported by the drive).

Windows:

Use the secure erase software from each manufacturer, ie Kingston, Samsung, Crucial, etc:

Ex:

- Samsung Magician Software (May ask to make a bootable USB to secure erase)
- Kingston SSD Manager (all partitions must be deleted first, see instructions.)