Boot from System rescue CD (<https://www.f-secure.com/en/web/labs_global/rescue-cd>)

Continue until when you are in a shell

Prepare disk for cleaning. Delete existing partitions and create a single partition.

Source: <http://tldp.org/HOWTO/Partition/fdisk_partitioning.html>

* list current partitions  
  > **fdisk –l**  
    
  You may see  
  /dev/sda1  
  /dev/sda2  
  Note that number at end is the partition number; /dev/sda is the device.
* start fdisk to delete partitions on a device (here /dev/sda)  
  > **fdisk /dev/sda**  
    
  You are now in fdisk shell. Use m to list options.  
  Use d to select partition(s)  
  use w to write updates to disk
* start fdisk to create a single partition  
  > **fdisk /dev/sda**  
    
  You are now in fdisk shell. Use m to list options.  
    
  Use p to print current partition table  
    
  Use n to create one partition that contains the full disk  
  Use 1 as partition number.  
  For remainder of the questions, accept defaults;  
  Use w to write updates to disk
* list current partitions

Check harddisk for bad sectors  
Source: <http://www.linuxtechi.com/check-hard-drive-for-bad-sector-linux/>   
> **badblocks -v /dev/sdb**

Write random data to disk  
Source: <https://wiki.archlinux.org/index.php/Securely_wipe_disk>

> **shred –v /dev/sda**  
Execution can take a long time (hours-day) and depends on disk size and cpu speed.

Note: it is unclear if shred handles bad sectors

Clearing partitions after shredding  
> **dd if=/dev/zero of=/dev/had**

Alternative: Linux hdparm  
Source: <https://ata.wiki.kernel.org/index.php/ATA_Secure_Erase>

Cleaning SSD is even “complex”. See section: Secure Deletion in  
Read <http://www.linux-magazine.com/Online/Features/Tune-Your-Hard-Disk-with-hdparm>

Interesting article that mentioned “hidden areas” and to see if they exists  
[**http://superuser.com/questions/642637/harddrive-wipe-out-hidden-areas-like-hpa-and-dco-also-after-malware-infectio**](http://superuser.com/questions/642637/harddrive-wipe-out-hidden-areas-like-hpa-and-dco-also-after-malware-infectio)