Background on addressing devices from which you wish to- and to which you wish to dump.

* Linux detects everything as a file and or directory off of root, this is similar to a file directory in Windows (imagine viewing the contents of “C:\” drive).
* / is “root” of the drive, everything is an extension, or subdirectory of root
* Hard drives are usually assigned as hda, hdb, etc. off of /dev directory.
* USB drives are detected as “Serial Drives,” and as such are “sda,” “sdb,” etc.
* Partitions can exist on each drive and are addressed individually by specifying the partition number of the device: /dev/hda1, /dev/hda2, etc.

For the purposes of this lab, use if=[YOUR USB DRIVE] of=[SOME FILE NAME].raw. This will place the file in your /home directory so that you will be able to hash the file easily.

Command line utilities used in this lab:

In order to use these utilities, you will have to open the “terminal” in Kali/BackTrack

- black box with a white line in the taskbar (at the top of the screen)

Remember DOS or Windows command line? This is like that – but in Kali/BackTrack, terminal provides access to almost all utilities.

-md5deep for hashing

- md5deep [HASHING ALGORITHM – if you don’t specify anything the MD5 hashing algorithm will be used] [OUTPUT FILE].

.-This will output the hash value, we will use these for comparison

-dd for dumping evidence

-General syntax below:

dd if=[addressing the device you want to copy] of=[addressing the device and file path to which you want to copy the evidence]