Forensics Lab Hashing and hash comparisons in the course of an investigation.

*Useful Resources:*

* Md5deep man page (<http://linux.die.net/man/1/md5deep>)
* dd man page (<http://linux.die.net/man/1/dd>)
* General Reference (<http://www.cyberciti.biz/faq/linux-partition-naming-convention-and-ide-drive-mappings/>)

*Activity:*

1. Each Investigator should “seize” the 2 GB USB drive of evidence. (Reminder: chain of custody should be recorded on the back of this sheet – this is different than it is done in real investigations, but you can do it this way for this lab)
2. Connect the 2 GB USB drive and your Controlled Boot USB to your investigation workstation. Your investigation workstation should be shutdown before doing any other steps.
3. Boot from your Controlled Boot USB using “Forensics Mode.” This mode boots into an operating system called Kali/BackTrack 5R3 specifying that detected drives will not be automatically mounted.
4. Obtain a hash value of the 2 GB flash drive. List the command line command(s) you used to do this.
5. Record this hash value below for comparison:
6. Mount the 2GB USB drive (of course, this should NOT be done in a real investigation, but this will show the learner the basics of hashing algorithms), by mounting the drive to a sub-folder or the /mnt folder. If you need to investigate this, look at the resources linked above.

You will need to create a sub-directory in the /mnt folder call it something like /mnt/evidence, then use the mount command to mount the usb drive here.

1. Create a plain text file in the 2 GB flash drive without changing it in any other way than creating it. (Answer: use the touch command and address the file using /dev/sdb1/text)
2. Dismount the 2 GB flash drive.
3. Hash the file you just created. Record this hash value for comparison.
4. Hash the 2 GB flash drive. Record this hash value for comparison.
5. Put only “1” into the text file on the flash drive just created (echo “1” or append “1” to the file just created). (You’ve made minimal changes). List the command line command(s) you used to do this. What do you need to do before you can write to the 2 GB flash drive?
6. Dismount the 2 GB flash drive.
7. Hash the text file. Record this hash value for comparison. Hash the 2 GB flash drive. Record hash value. How much of each hash value has changed in each step of the above lab? What implications does this have for digital forensics investigations?

Review of what was learned.

1. Imagine that the 2 GB flash drive was the internal evidence HDD on a computer. How did you bypass the 2 GB HDD in the computer from loading and changing the evidence? How is this completed in the boot process?
2. What was changed between the first hash of the drive and the second?
3. How different were the 2 hash values?
4. Complete an investigation report with notes and a chain of custody.
5. Additional activity: boot into Windows. Open Windows Explorer. Put a USB into the USB drive, while windows is installing the driver, open the drive. Do you see the temp file being written to the disk? You may or may not be able to see it. If you can take a screen capture of it and place it here. If not, look online and try to find a story about this practice in Windows. If there is a screenshot of it, copy that here (with the correct citation), if not – put the link to the story here.