**SY486J: Cyber Crime Investigation: Practice Lab**

**Static acquisition in Linux**

Deliverable for this lab: Please answer the embedded questions and the questions at the end of the lab exercise:

For this lab we will be using the Kali Linux bootable DVD. Kali is preferred for acquisition because it comes ready with the forensic tools like DFCLDD, hashlog and can be booted from Windows and Apple platforms.

We have several steps to perform today: Please concurrently do Step One and Two.

**Step One (USB1 –target disk)**: Preparing our media for acquisition. This will involve zeroing, partitioning and formatting our media. We would like to format the drive such that we are able to use it in Windows and Linux. We will therefore us FAT32.

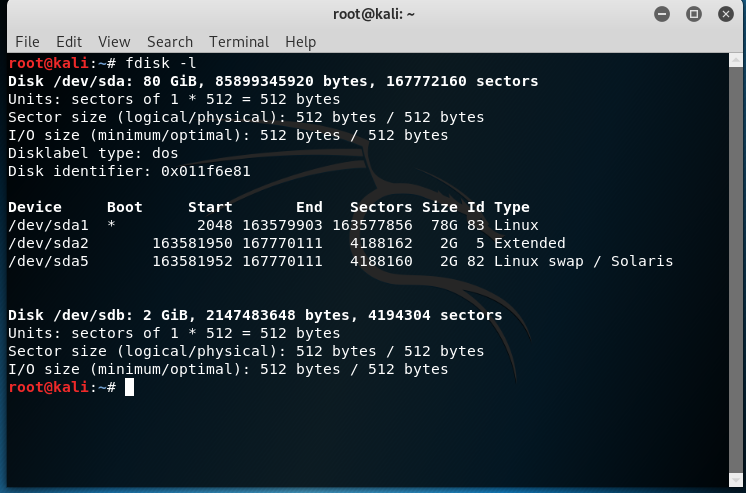
**Step Two (USB2- suspect disk)**: Preparing the suspect disk will involve creating a partition that is 0.5 GB using the parted command, formatting the partition and creating some evidence, Word documents, text files, pictures etc. Whatever you want to include.

**Step Three ( Acquisition Process)** – Creating a raw format file for the suspect disk.

**Step One(USB1 –target disk) – Preparing Media for acquisition**

This will display the hard drive configuration and details.

1. Access your Linux Virtual Machine (VM)
2. Connect the USB1(target) external drive to the VM
3. Confirm that the flash drive is mounted in the VM
4. Open a terminal
5. List the current disk devices connected to the computer by typing fdisk -l (lowercase L) and press Enter.



1. Record the labels for your main drive and its interface, and the label associated with the inserted drive below here (insert a screenshot here):
2. Type the below command to zero-out or wipe the USB drive - writing zeros over every single part of the drive. This is easy to do, but may take a little time:

sudo dd if=/dev/zero of=/dev/sdb bs=100000000

sync

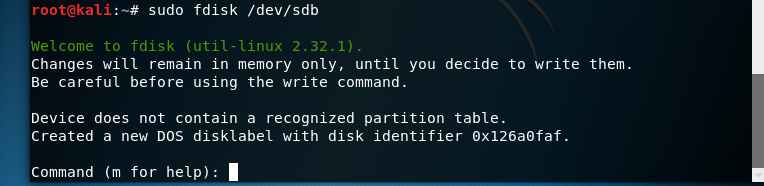
That looks complicated! It’s not:

* **dd** is a Linux command that reads bytes from a source (here /dev/zero) and writes bytes to a source (/dev/sdb, the second hard disk you just created). That’s it.
* **‘if=’** means use this input file. In this case, /dev/zero it is a device that provides the system with ‘zeros’. You ask for a zero, it gives you a zero.
* ‘**of=’** means write to this file. Note it’s pointing to /dev/sdb, which is our newly configured hard drive.
* **Finally, bs=**10000000 means read and write in BIG CHUNKS of zeros (10000000 to be precise). We could use the default, which is 512, but it takes longer, so we’ll use the bigger value.

The “No space left on device” error is normal. Also note that the number of records in and out multiplied by the block size (8192) will get you the number of bytes copied.

1. Partition the drive using the command below. We can’t do anything with a drive that isn’t partitioned and formatted, so let’s do that. We have to create a partition first.

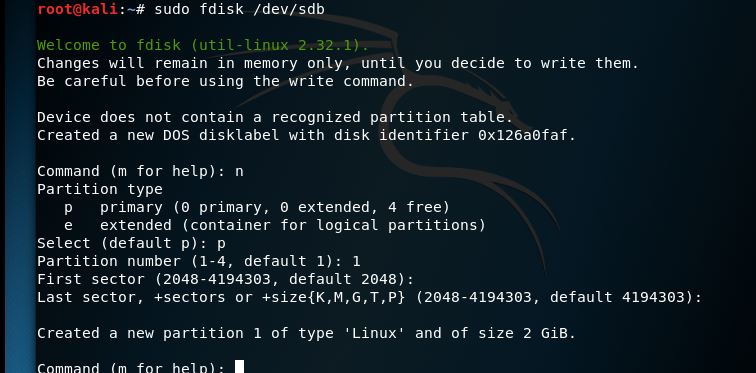
sudo fdisk /dev/sdb



You’ll see the screen above. Let’s walk through the steps of creating a new partition, type:

1. ‘n’ then Enter.
2. ‘p’ then Enter.
3. ‘1’ then Enter.

Your screen should now look like this:



Now we can just go with the defaults:

1. Hit Enter
2. Hit Enter

Now we need to tell the program to write out those changes to disk. Remember, all we are doing is creating a single primary partition.

Type ‘w’ and Enter to write out the changes.

And we have our drive partitioned!

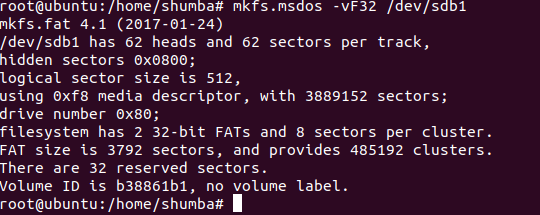
1. Now use the command below to format the drive this will write a file system to our evidence drive. A file system is like a table of contents for a device, it tells the operating system what’s on the disk, and where to find the files. We’ll need another command for this. There are many different options for file systems, but we’ll go with a FAT system for this example. Type the following then hit Enter:

sudo mkfs.msdos –vF32 /dev/sdb1

If you get an error that the device is busy, please check if it’s mounted. If it is, then un mount it following the below commands.

df –h //to check if the device is mounted

umount /dev/sdb // to umount if mounted



If your screen looks like that above, congratulations! You have a new partitioned and formatted hard drive! Insert your screenshot here

This drive can now be mounted and used to receive an image of a suspect drive.

***In a few statements, summarize what you have done and why it is important for the acquisition process.***

**Step Two (USB2- suspect disk) - Preparing the suspect drive**

1. Follow steps 7 to 9 from Step One still in Ubuntu
2. However for the partition size, please input +600M (Megabytes)- leave the start sector as default.
3. Take this to Windows and populate it with evidence.
4. Shut down the host computer
5. Record the evidence that you created here and the amount of space you had for the operations.

**Step Three (Acquisition Process)**

1. Insert KALI Linux Bootable DVD to ‘the workstation.
2. As soon as the boot screen starts keep in hitting the F12 key until booting switches to the DVD
3. Select ‘Live (forensic mode)’ from the KALI Linux startup (Refer to Picture 01).



1. Open terminal command page in the left pane of KALI desktop
2. Type command “fdisk -l” to view the connected drives. Record the physical label for the main drive here (insert a screenshot here)
3. Insert the target and suspect USB into the respective drives.
4. Type command “fdisk -l” to view the connected drives. Record the physical label for the two other devices connected here (insert a screenshot here)
5. Make virtual directory folder named evidence by typing the below command :

mkdir /mnt/evidence

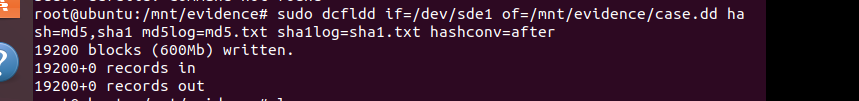
1. Mount the virtual directory evidence folder to the destination drive -target (which we sanitized).

mount <target drive> /mnt/evidence

1. Type the below command to enter evidence directory folder -the folder which will hold the image

cd /mnt/evidence

1. Type command as it appears in the screen to create the raw image named (dd image) insert a screenshot here)



### Questions for research

1. There are many hashing algorithms to use. Which one did you use in this case? Which one would you use if you were working on a case for a law enforcement agency? Why?
2. What are the possible issues/causes if the hash of your original does not match your forensic copy?
3. What are possible issues if your OS automatically mounts your flash drive prior to creating your forensic duplicate?
4. How do you know that your OS did not automatically mount your flash drive, and subsequently change the contents of the flash drive prior to you creating the forensic copy?