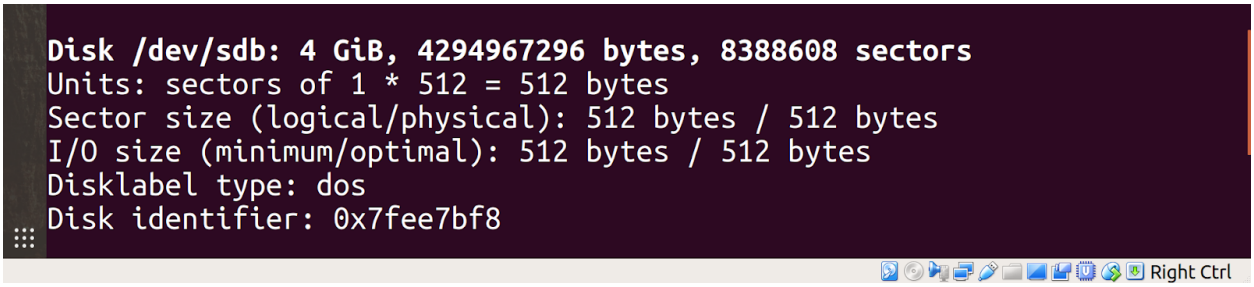
Installing the Forensics VM

Download the Forensics Virtual Machine.
In order to run it, you must import the image similarly to how you imported the student virtual machine. This is to emulate live analysis of a disk image you recover from a real device.

Connecting the Image to the Student VM (Dead Analysis)

These steps will allow you to access the forensics virtual disk image from your other virtual machine. This configuration is the equivalent to dead analysis of a hard drive that you attach to an already running computer. Be careful with this configuration because you will never want both virtual machines running at the same time.

1. Shut down both of the virtual machines if either is running. Note that this is different from “saving the machine state.” The VirtualBox manager should show that both are in the “Powered Off” state.
2. Click on the “infosec_vm_distribution” entry.
3. Click Settings.
4. Click Storage on the left-hand menu.
5. Click Controller: SATA. Two icons with green plus symbols should appear next to the controller entry.
6. Click on the rightmost of the two icons that appeared. It should look like a hard drive with a green plus in front of it. When you hover your cursor over it, the words “Adds hard disk” should appear as a tooltip.
7. Click “infosec_forensics_release-disk001.vdi” and click Choose.
8. Verify that the correct disk was added and click OK.
9. Start the “infosec_vm_distribution” virtual machine and open a terminal window.
10. Run `sudo fdisk -l` and verify the second disk is displayed (/dev/sdb with Disk identifier 0x7fee7bf8)



11. Take note of the /dev/ entry for the new disk partitions. Note that each different “Device” listed there is a partition of a hard disk. Using those entries, run the following commands to mount some of the partitions:
```
sudo mkdir /mnt1 && sudo mount /dev/sdb1 /mnt1
sudo mkdir /mnt2 && sudo mount /dev/sdb2 /mnt2
sudo mkdir /mnt3 && sudo mount /dev/sdb3 /mnt3
```
12. You can now browse the new directory (e.g., `cd /mnt1`) as you would any other file system directory. You may find that some of these partitions do not mount correctly, and that is something you need to investigate as a part of the assignment.
13. When you want to run the suspect machine for “live analysis,” be sure that you have shut down the “infosec_vm_distribution” virtual machine before trying to start the “infosec_forensics_release” virtual machine.

DO NOT RUN THE FORENSICS VM WHILE THE DISK IS MOUNTED IN THE STUDENT VM - THIS WILL CORRUPT BOTH MACHINES

Destroying the Virtual Machine

You might irreparably damage the state of the forensics virtual disk. This is why it is important to keep the source infosec_forensics_release.ova on hand to restart with a fresh instance. Follow these steps to completely destroy the virtual machine so you can reconfigure it by following the above steps again.

1. Shut down both virtual machines so you can safely manipulate the virtual disks.
2. Navigate to the storage settings menu of the “infosec_vm_distribution” as you did to connect the suspect image.
3. Under Storage Devices, right click on “infosec_forensics_release-disk001.vdi” and click Remove Attachment.
4. Click OK.
5. Right click on the “infosec_forensics_release” virtual machine and click Remove... in the context menu.
6. Click Delete All Files