STEP2 LAB: RESOURCES AND PROCEDURES NOTES

Resources

1. A Linux Forensic virtual machine (VM), NIXFOR01
2. A Forensic image file: LD2-Step1.dd
3. A flash drive image file "FlashDrive.img"

Virtual Machine Credentials

Username: **StudentFirst**

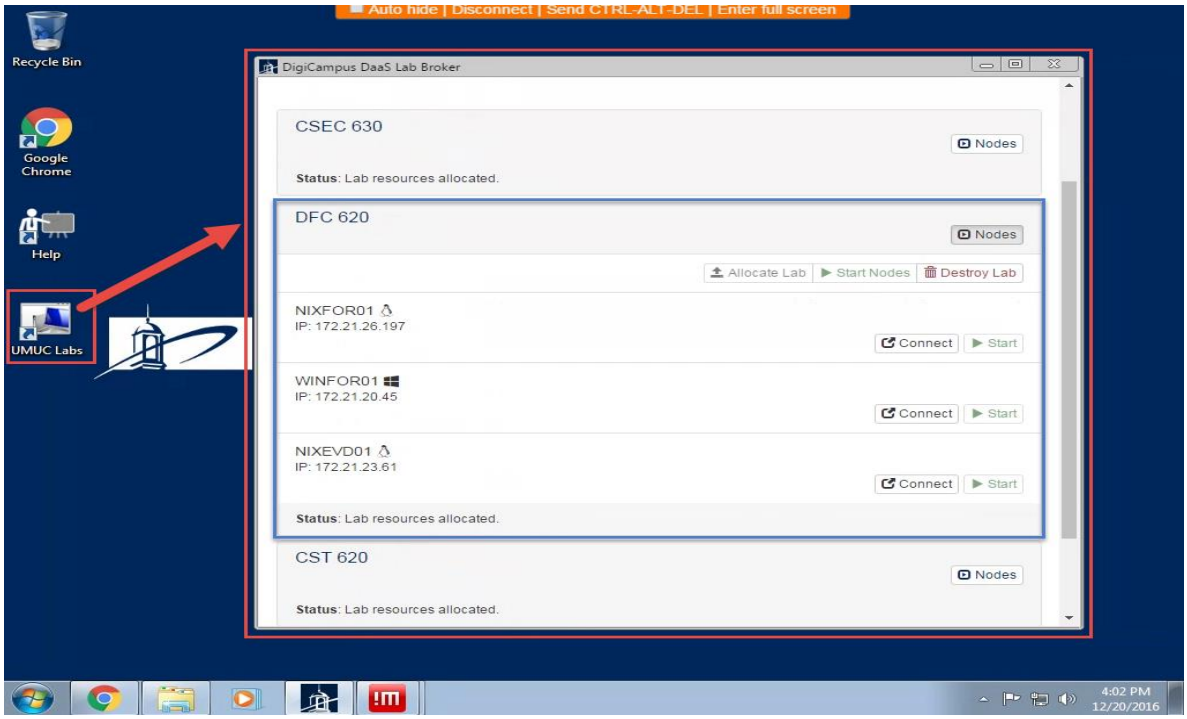
Password: **Cyb3rl@b**

Procedure Notes

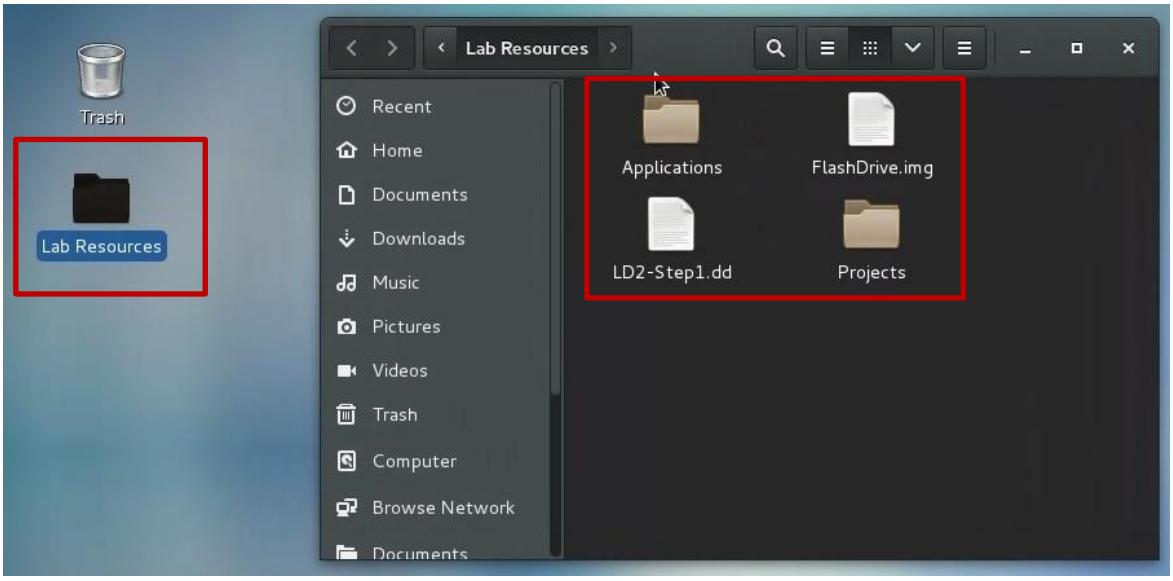
1. Placeholders are in [brackets].
2. Comments are in (parentheses and italics).
3. Command line instructions are indicated as follows:
   - $ command (Linux normal user)
   - # command (Linux root user)
   - Expected output highlighted in grey
4. Since we are operating in a virtual environment, we are not currently able to plug in a physical USB stick into our virtual machine somewhere in the cloud. As a result, we will be simulating the operations involved in plugging in, mounting and removing a virtual flash drive.

Part A: Setting Up Your Evidence Drive

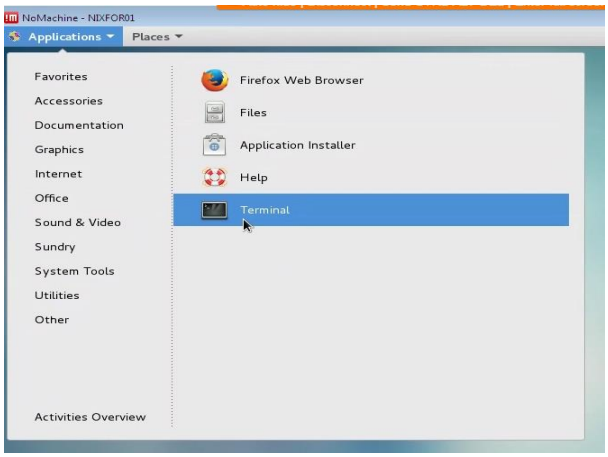
Access your "NIXFOR01", Linux Forensic VM, using the Lab Broker from your Workspace as depicted below. The steps that follow are all completed inside of the "NIXFOR01" Linux VM, unless otherwise indicated.

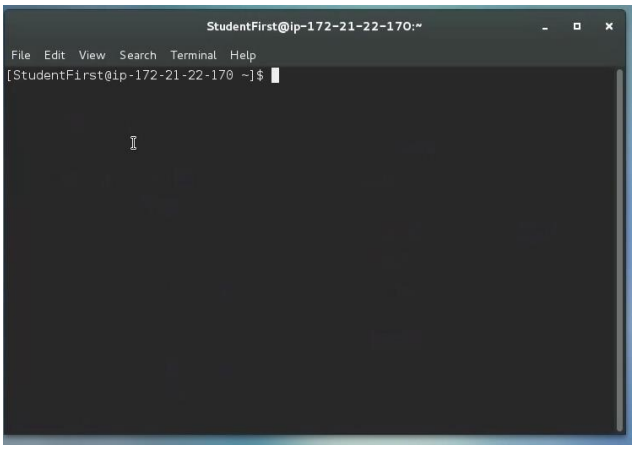


1. Locate the LD2-Step1.dd file in the Downloads folder of your "NIXFOR01" VM.
2. Locate and confirm the existence of the "FlashDrive.img" file in the Downloads folder of your "NIXFOR01" VM.



3. Open a terminal window.





4. Simulate inserting a flash drive using the following commands in terminal.
    a. Attach the flash drive image, “FlashDrive.img”, to loopback device.

$ sudo losetup --find --show -P ~/Desktop/"Lab Resources"/FlashDrive.img

    b. List loopback devices allocated (*for verification purposes*).

$ losetup –l

    c. Show loopback and partition in /dev.

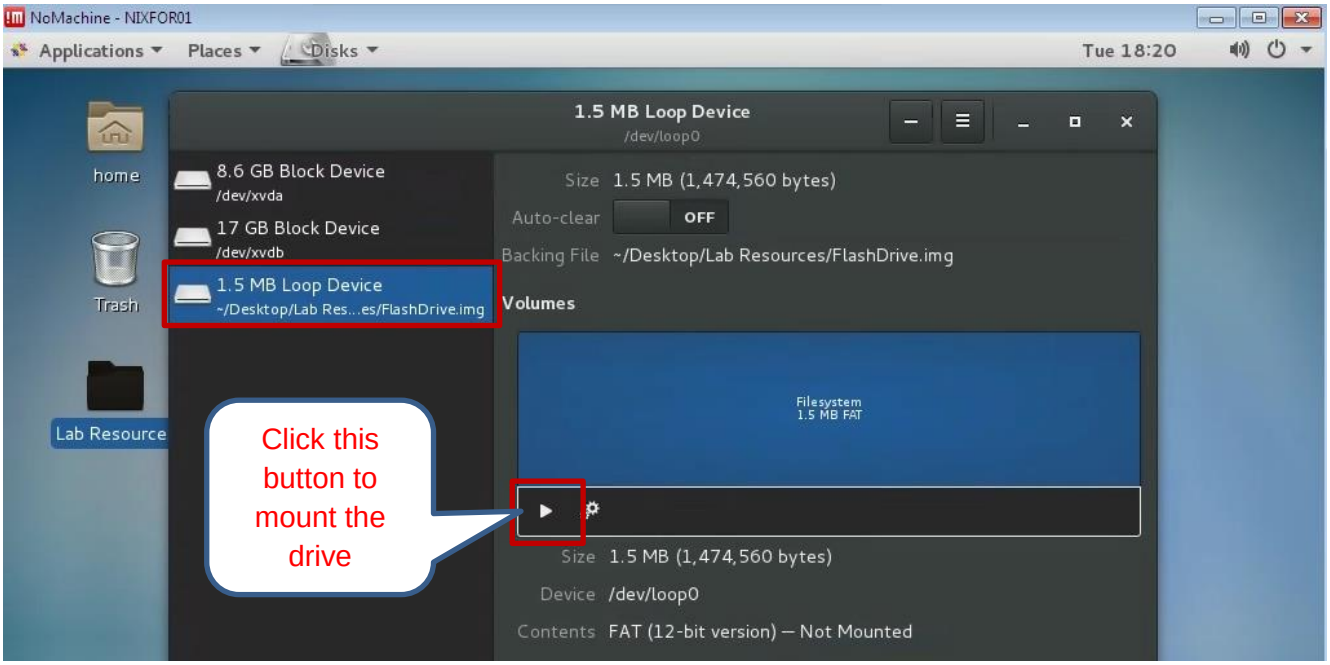
$ ls -l /dev/loop0

    d. Verify that no device is auto-mounted (*nothing should be listed as the result of the following command*).

$ mount | grep /dev/loop

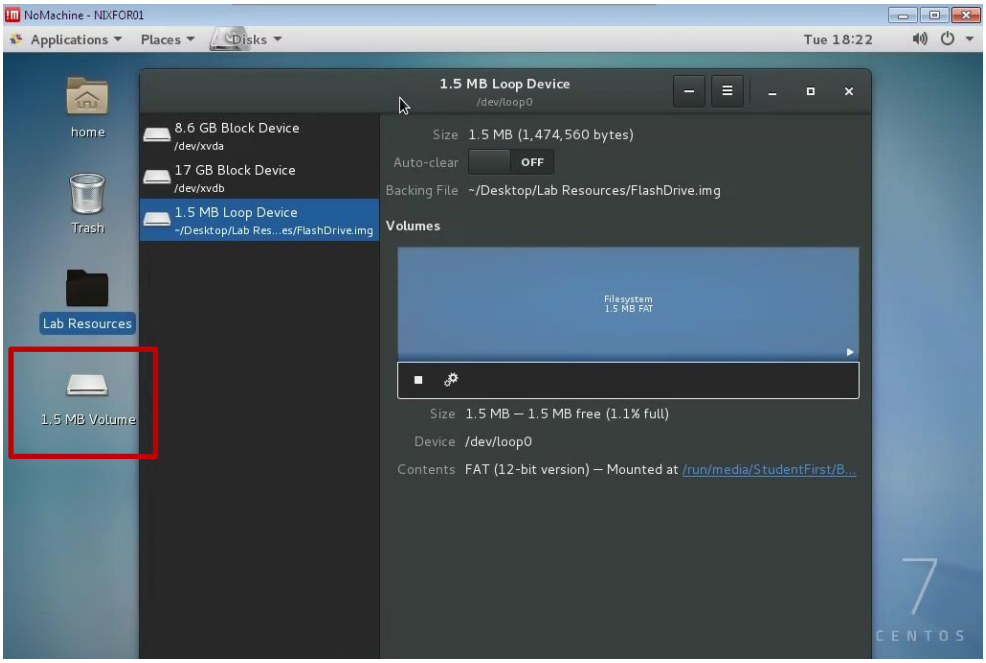
5. Mount the device
    a. Use the Graphical User Interface method to mount the device.
        i. Use the gnome-disks command to lunch the disk utility.

$ gnome-disks



b. Click on the play button to mount the "1.5 MB Loop Device".
   i. You will be prompted for a password. Please enter **Cyb3rl@b**

6. Confirm that the flash Drive is mounted in the VM by locating it's icon on the desktop.



7. Open a terminal window if one is not already open.

8. Determine the device location assigned to your flash drive.
    a. Type the following command:

$ sudo mount

    b. You are looking for the first part of the line containing the name of your flash drive. In our case, we are looking for the following line indicating that our device is assigned "/dev/loop0" :

(i.e., /dev/loop0 on /run/media/StudentFirst/BC61-C217 type vfat)

    c. You can also use the following command to filter through the multiple lines of text produced by the mount command:

$ mount | grep /dev/loop

9. Zero your flash drive
    a. This operation writes zeros to all locations on the flash drive. Be sure to use the correct location of your drive.

$ sudo dd if=/dev/zero of=/dev/loop0 bs=1024
$ sync (*This command makes sure the write process is complete*.)

Note: In practice or with a physical flash drive, we would not include the numerical suffix, "0", for the "of" part of the command (*of=/dev/loop0*). Since the flash drive is located at /dev/loop0, so the "of" part of the command would have been "/dev/loop" (*no trailing zero, "0").* However, in our example, since we are dealing with a virtual device, we address it as a partition by including the zero suffix in order to successfully Zero the out drive.

10. Copy the dd file to the flash drive.
    a. This is not a file copy, but rather a "raw" copy; follow the instructions below.
        i. Before executing the following commands, make sure that you are working in the directory that the dd file is located in. In our example, it is the Downloads directory.
        ii. Navigate to the Lab Resources Directory by typing the following:

$ cd Desktop/Lab\ Resources
(*make sure the folder contains the LD2-Step1.dd file by using the ls command*)

$ sudo dd if=./LD2-Step1.dd of=/dev/loop0 bs=1024
$ sync

11. Confirm that the image you wrote matches the image file by producing and comparing the hash value of the dd with that of our drive. If they do not match, repeat the above process starting with Step 6.

$ sudo sha1sum LD2-Step1.dd /dev/loop0

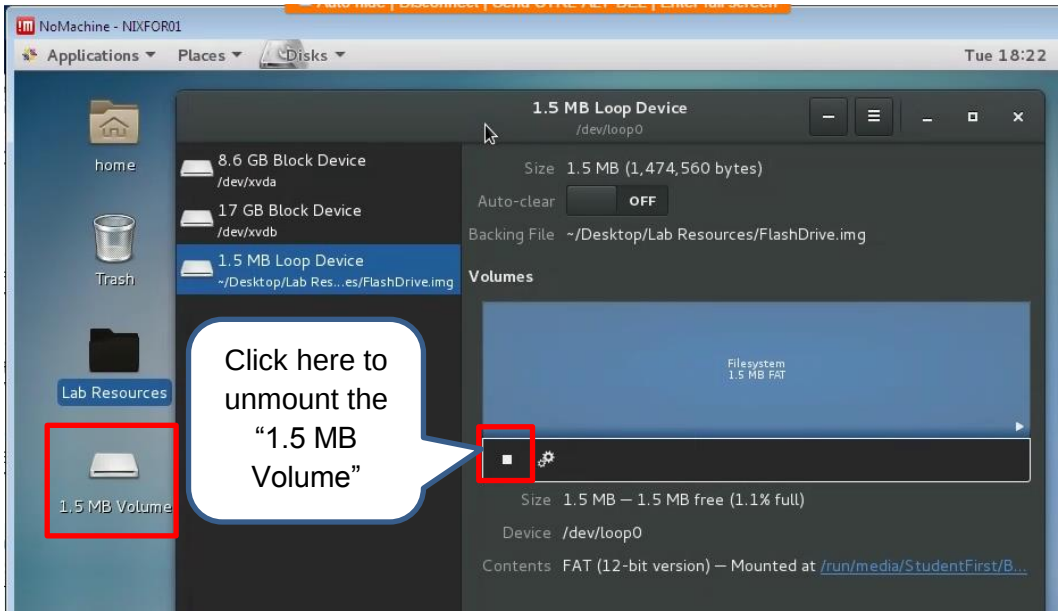
32b9fcb741aab43a4f80393d3df67c32c726924f LD2-Step1.dd
32b9fcb741aab43a4f80393d3df67c32c726924f /dev/loop0

12. **Note about disabling auto mounting:** at this point of the process, before moving to the static imaging and verification step, we would normally disable auto-mounting by doing the following:
    a. Adding the following line to the file "/etc/fstab"
        /dev/loop0 auto noauto 0 0

13. Let's now simulate removing the flash drive from the VM
    a. Unmount the "1.5 MB Volume"
        i. Use the gnome-disks command in terminal to open the Disk Utility

$ gnome-disks

    b. Click on the stop button highlighted in the picture below to unmount the volume (*notice the icon disappearing from the desktop after successful unmounting. We can also simply right mouse click on the Desktop icon and chose unmount from the menu*).



    c. Destroy loop devices to simulate unplugging a flash drive.
        i. Type the following command:

$ sudo losetup –D

    d. Verify that no loop devices are connect before continuing to Part B using the following command: **$ sudo losetup –l**

Part B: Static Imaging and Verification (Linux)

1. Using the same method illustrated in steps 5 Part A, let's simulate plugging in a flash drive without mounting any volume.
2. Verify that the loopback device is allocated, but the flash drive image file is not mounted.
3. Create a forensic copy of the flash drive with the following command:

   $ sudo dd if=/dev/loop0 of=forensic_copy2_LD2-Step1.dd bs=4096

   Note that we are creating a forensic image of a logical partition (*/dev/loop0*) of the flash drive, in this case, the partition that contains the dd file from above. In practice, we often will image the entire physical device (*/dev/loop in this case*).

4. Check the hash value of the forensic copy and compare to the image file hash from Part A; if they don't match, then repeat these steps, or optionally repeat the steps in Part A as well.

   $ sudo sha1sum forensic_copy_LD2-Step1.dd /dev/loop0

   32b9fcb741aab43a4f80393d3df67c32c726924f forensic_copy_LD2-Step1.dd

5. Complete your lab notes as well as your report for this Part B only. Complete the lab report and lab notes using the templates provided. Your lab notes must include dates and times as well as specific descriptions of what you did and the results.