STEP6 LAB: RESOURCES AND PROCEDURES NOTES

Resources

1. Two Linux virtual machines (*VMs*); one (the forensic workstation) with additional storage device large enough to store a full copy of the evidence hard drive.

Virtual Machine Credentials

Username: **StudentFirst**

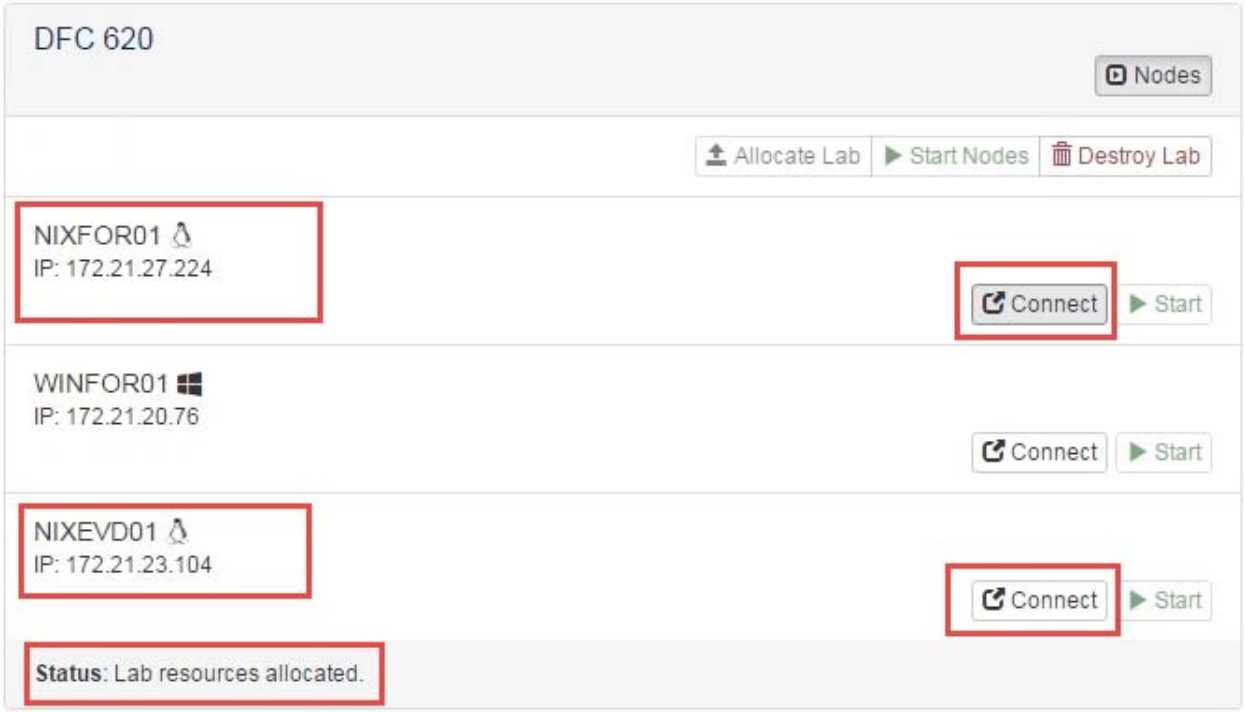
Password: **Cyb3rl@b**

Procedure Notes

1. All tasks should be performed on the forensic workstation unless otherwise specified as in steps 1, 6 and 9.
2. Placeholders are in [brackets].
3. Comments are in *(parentheses and italics).*
4. Command line instructions are indicated as follows:
    - $ command *(Linux normal user)*
    - # command *(Linux root user)*

Part E: Acquiring an Image over a Network

1. From the lab broker on your Workspace, allocate and connect to both of your Linux virtual machines (*VMs, NIXFOR01 and NIXEVD01*).



   a. One Linux VM is your forensic workstation (*NIXFOR01*) and one is your evidence system (*NIXEVD01*).

   b. Connect and logon to both.

   c. Open a terminal window on each.

   d. Check and take note of the Internet Protocol (IP) addresses.

      $ ifconfig (*optain IP for eth0*)

   e. Confirm connectivity with ping.

      $ ping [IP_NIXFOR01] [IP_NIXEVD01]

   f. Confirm that the additional storage device is attached to the forensic VM by running the following command:

      $ gnome-disks

      Note: We are looking for a 17GB Device connected to /dev/xvdb.

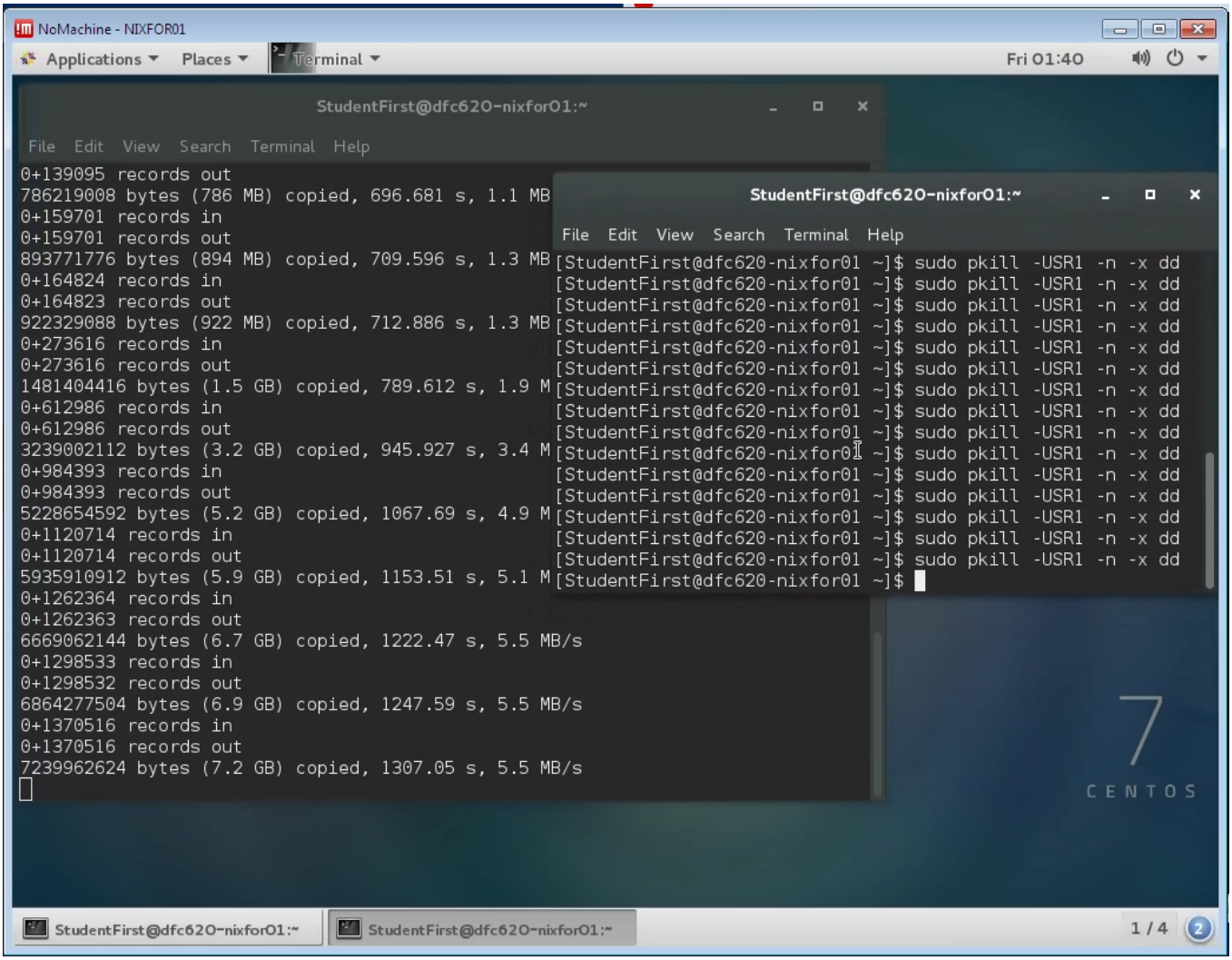
2. Zero the attached storage on the forensic workstation additional storage:

   $ sudo dd if=/dev/zero of=/dev/xvdb bs=8196
   $ sync

3. Confirm that data is flowing by opening a **second terminal window** and typing the following command:

   $ sudo pkill -USR1 -n -x dd

   which will provide a status of the transfer (*Repeat this command to see the progress as depicted below*).



4. Change the ownership of the additional storage (*/dev/xvdb*) to StudentFirst.

   $ sudo chown StudentFirst /dev/xvdb

Note: In order to perform the next task, the StudentFirst account needs a certain level of access to /dev/xvdb. For simplicity, we are making the StudentFirst account the owner of /dev/xvdb instead of root.

5. Create a netcat listener on your **forensic workstation, NIXFOR01**.

   $ sudo nc -l [port_number]|bzip2 -d|dd bs=16M of=/dev/xvdb

   where "port_number" is a number of your choosing, preferably greater than 10000 and must be less than 65535, and /dev/xvdb is where you will write your image file. You will not see any output after hitting Enter.

6. Create the forensic image by running the following command on the **evidence system, NIXEVD01**:

   $ sudo dd bs=16M if=/dev/xvda|bzip2 -c|nc [IP_NIXFOR01] 19000

   You will not see any output after hitting Enter.

7. Confirm that data is flowing (*as in step three*) by opening a **second terminal window** and typing the following command:

   $ sudo pkill -USR1 -n -x dd

   which will provide a status of the transfer.

8. Compute and record the md5 and sha1 checksums for the acquired image. On the forensic workstation, type:

   $ md5sum /dev/xvdb

   and

   $ sha1sum /dev/xvdb

   Note: Because the evidence system is running, the image checksum will not match a checksum taken of the drive itself (*from the evidence system*).

9. Collect evidence workstation and forensic workstation system information for your report and notes:

   $ uname -a
   $ lsb_release -a
   $ lsblk
   $ df -k *(for evidence workstation only)*