CONESTOGA

Connect Life and Learning

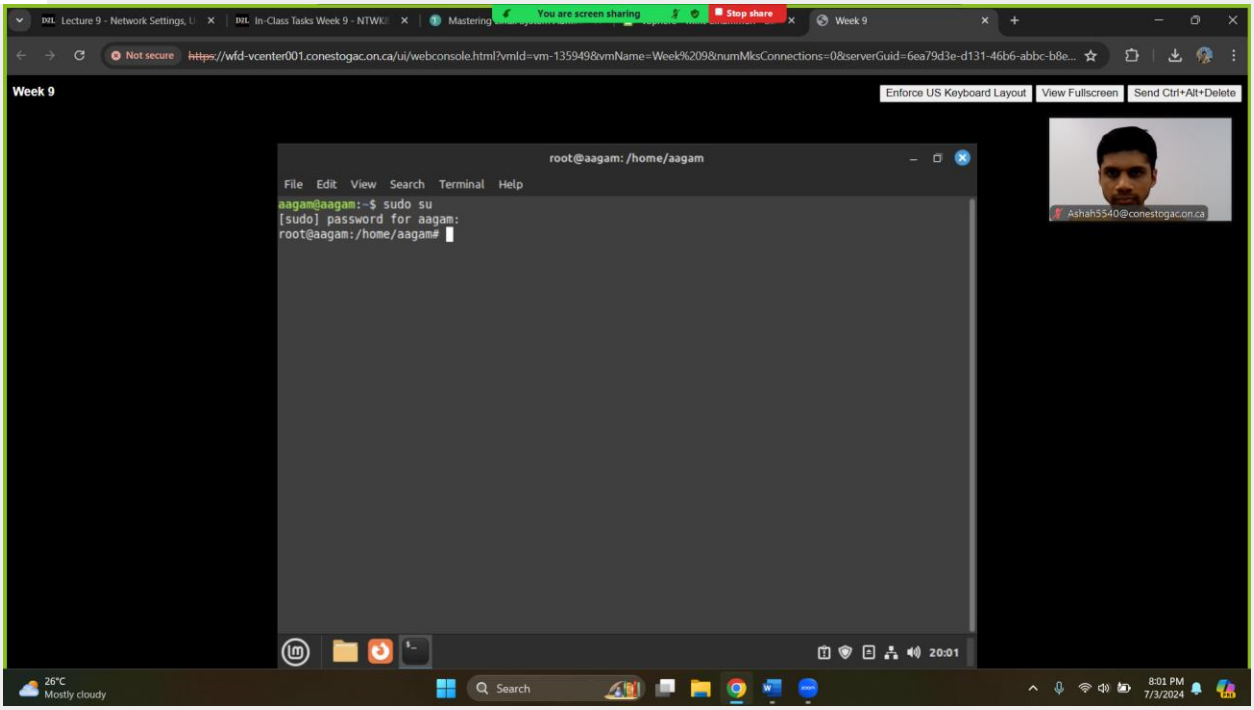
Student Name:	Aagam Sanjay Shah
Deliverable:	In-Class Tasks Week 9 Assignment
Course Name:	NTWK8141-24S-Sec3-Linux Server

Date Assigned:	03/07/2024
Date Due:	04/07/2024
Rules:	• Individual. • Cheating is not allowed. • Plagiarism counts as cheating! • That FAILURE to submit work in the course can result in a grade of ‘F’ or ‘I’ for failure to complete the course!

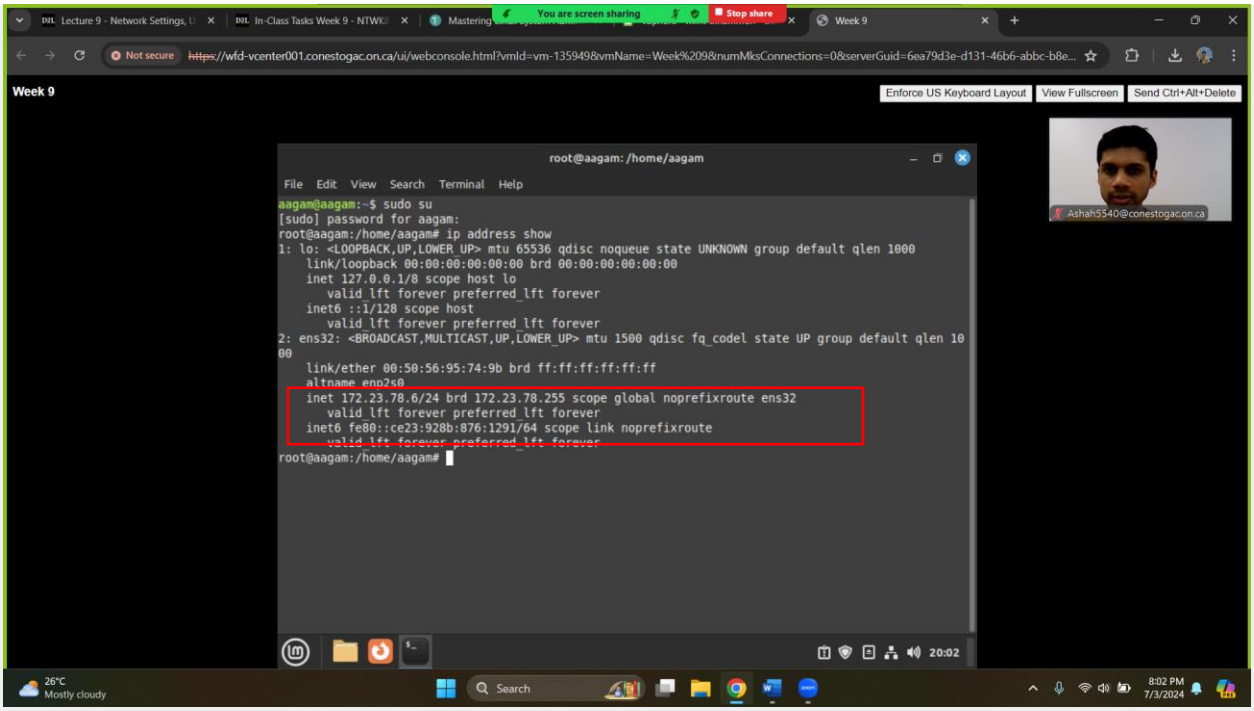
1. Week 9 Slide 16

DETERMINING THE NETWORK ENVIRONMENT

1. Log into your Linux server using the user account you created in Chapter 2 or Chapter 4, and acquire `root` privileges by using `su` or by using `sudo` with each of the following commands.

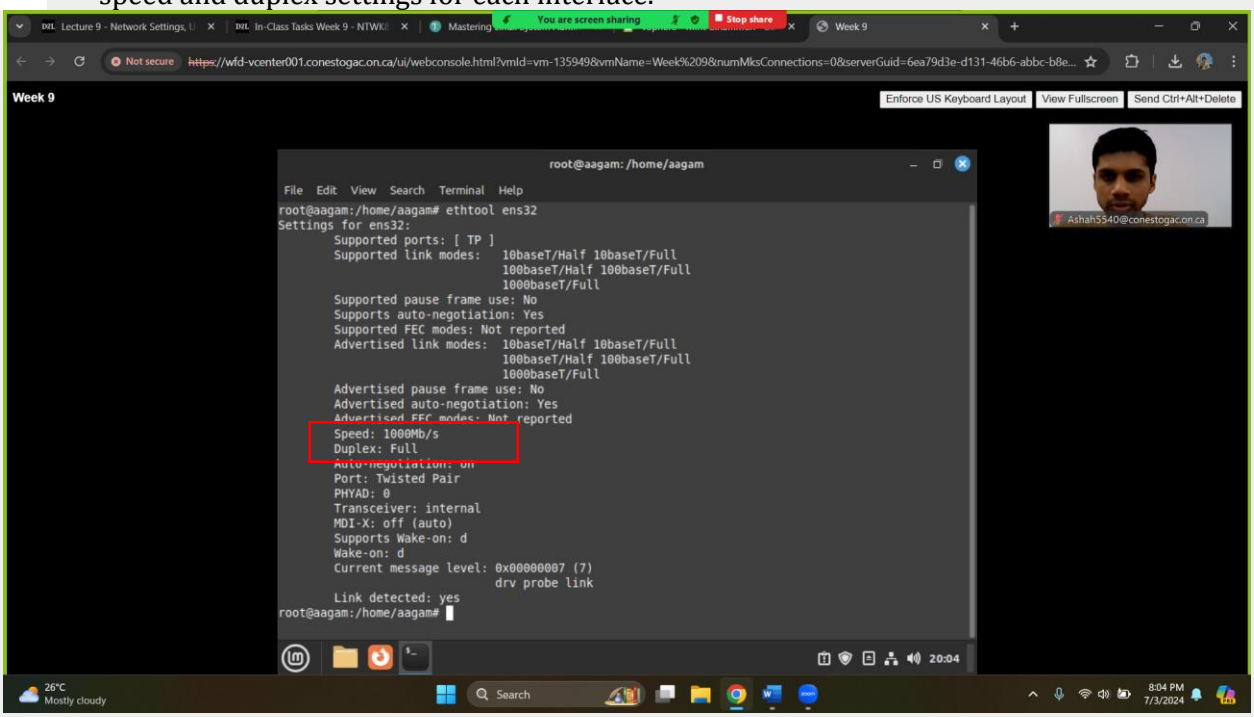


2. First, determine the network interfaces installed on the server. Type **`ip address show`** to display the current network interfaces. You will most likely see a loopback interface (named l0) and one or more network interfaces. Write down the IP address (called *inet*) and IPv6 address (called *inet6*) assigned to each network interface, along with the hardware address and the network mask address.

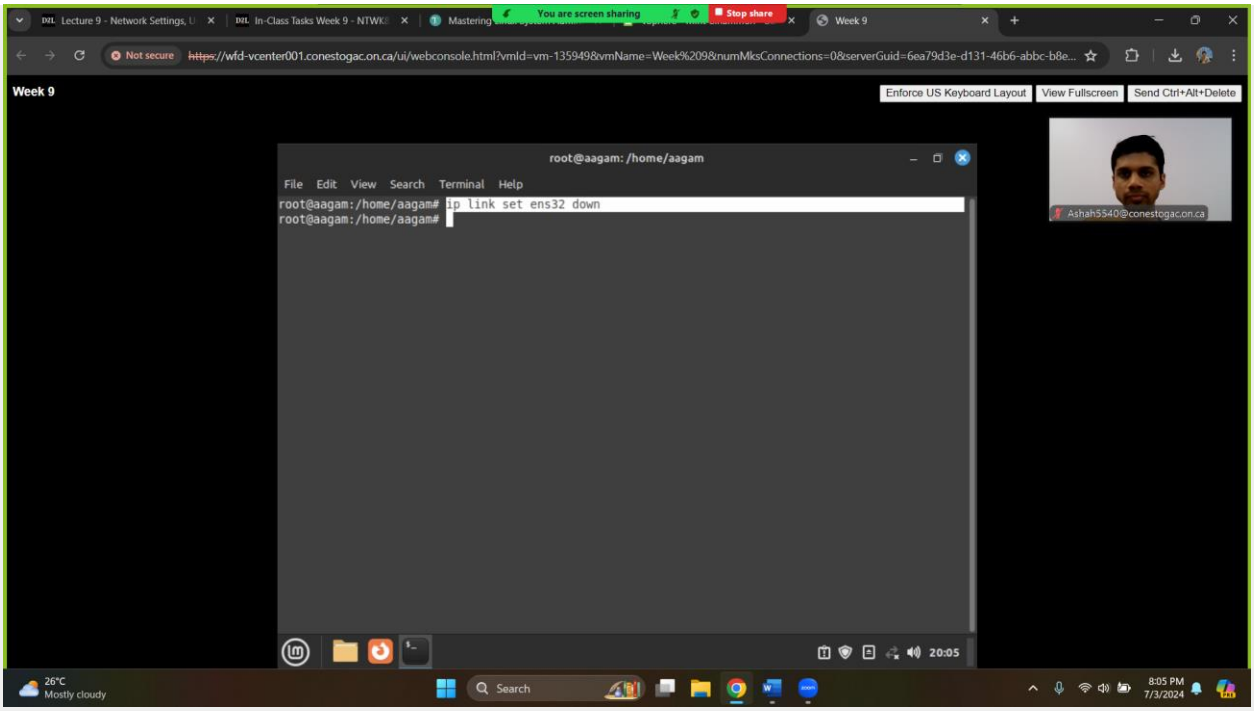


Inet →172.23.78.6/24 inet6 → fe80::ce23:928b:876:1291/64 (ens32)

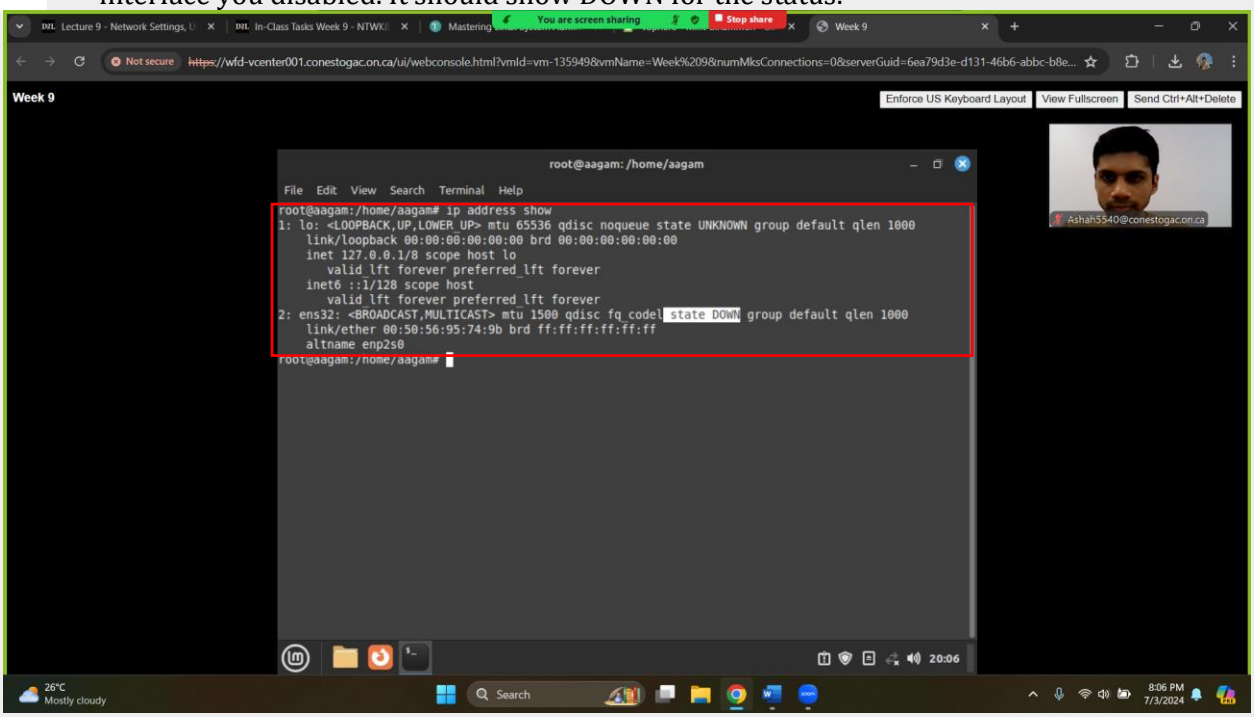
3. Use the `ethtool` command to determine the connection speed of the network interfaces. Type **`ethtool`** ***`int`***, where *`int`* is the name of each interface displayed in step 2. Note the speed and duplex settings for each interface.



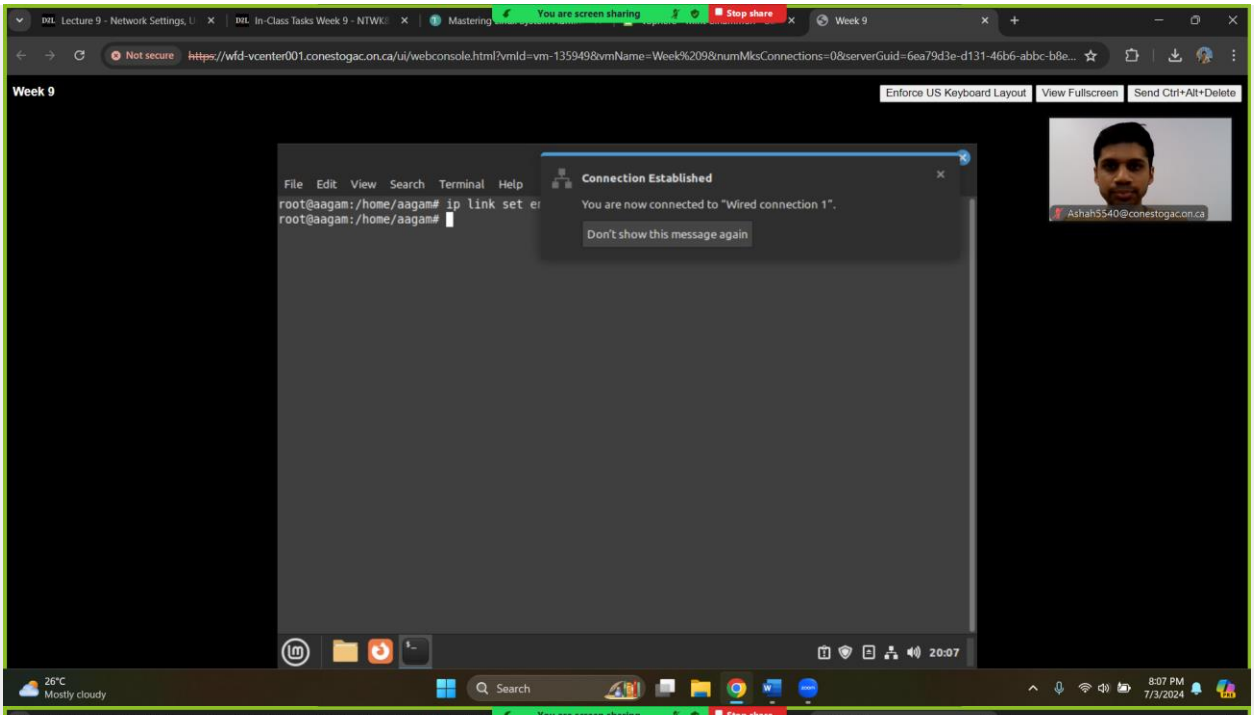
4. Disable one of the network interfaces on your Linux server. Type **`ip link set`** ***`int`*** **`down`**, where *`int`* is the interface name displayed in step 2.

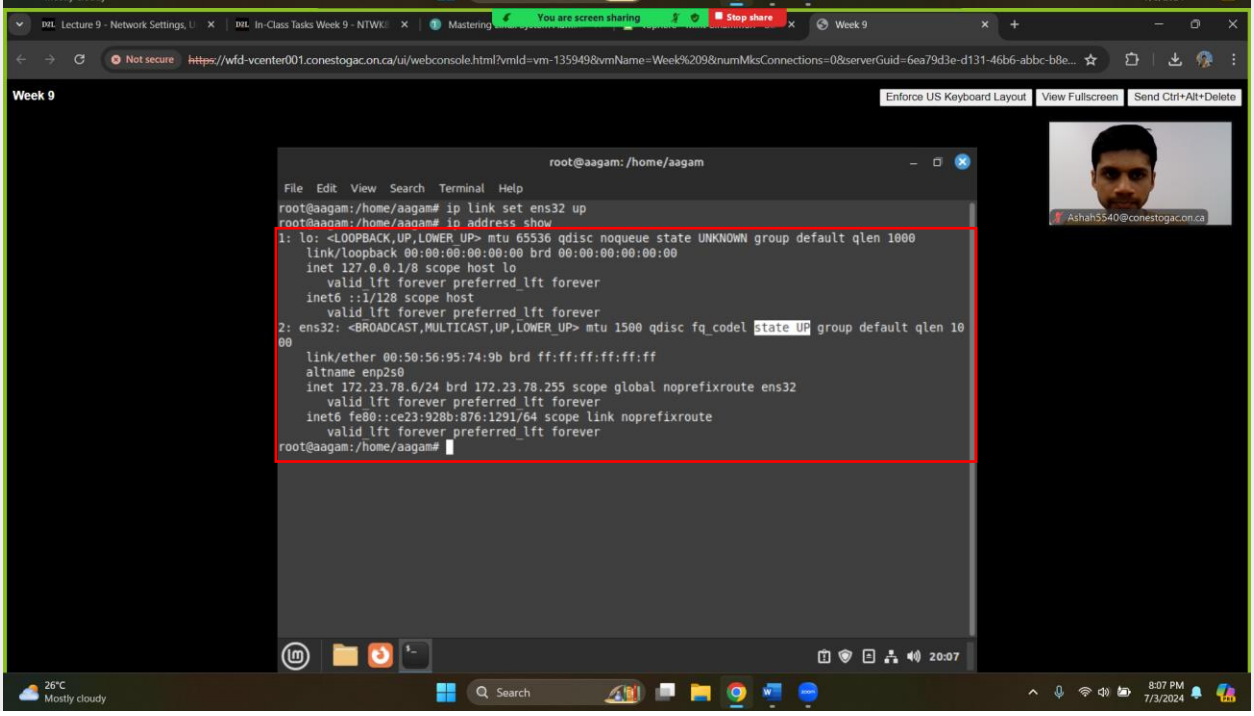


5. Type **`ip address show`** to display the network interfaces. Note the status displayed for the interface you disabled. It should show DOWN for the status.



6. Enable the interface by typing **`ip link set`** ***`int`*** **`up`**, where *`int`* is the interface you disabled in step 6. Type **`ip address show`** and note the status of the interface.

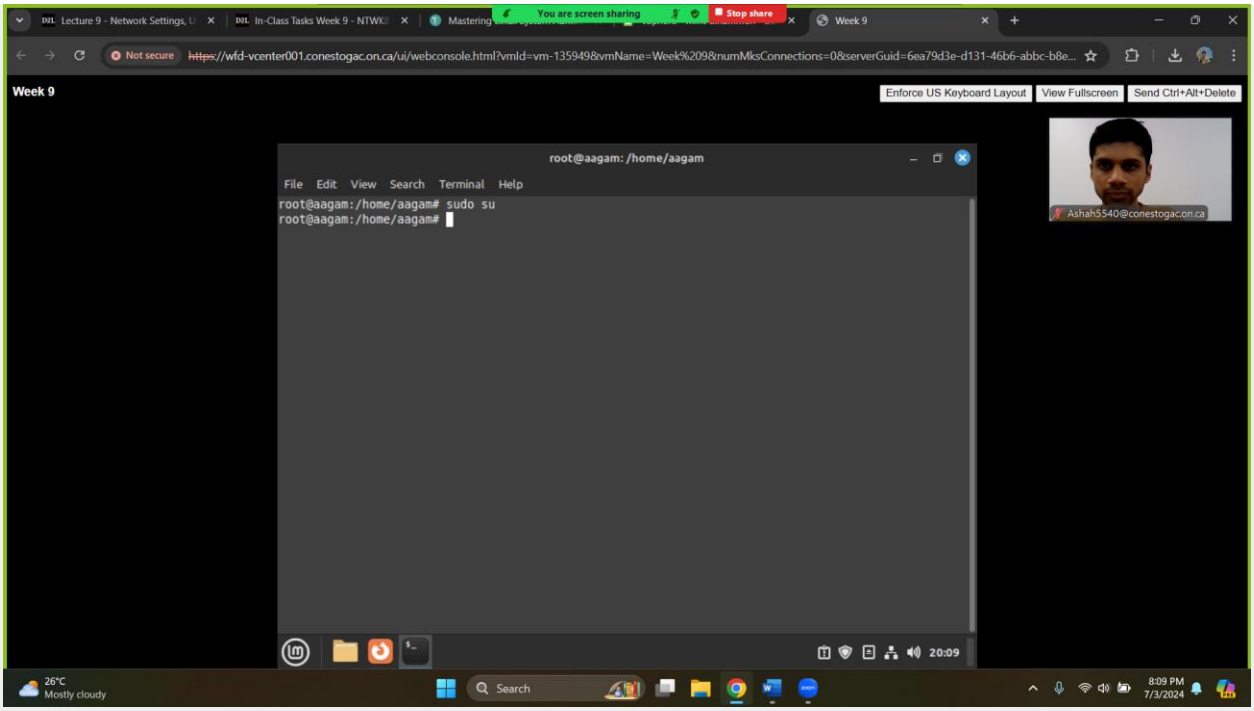




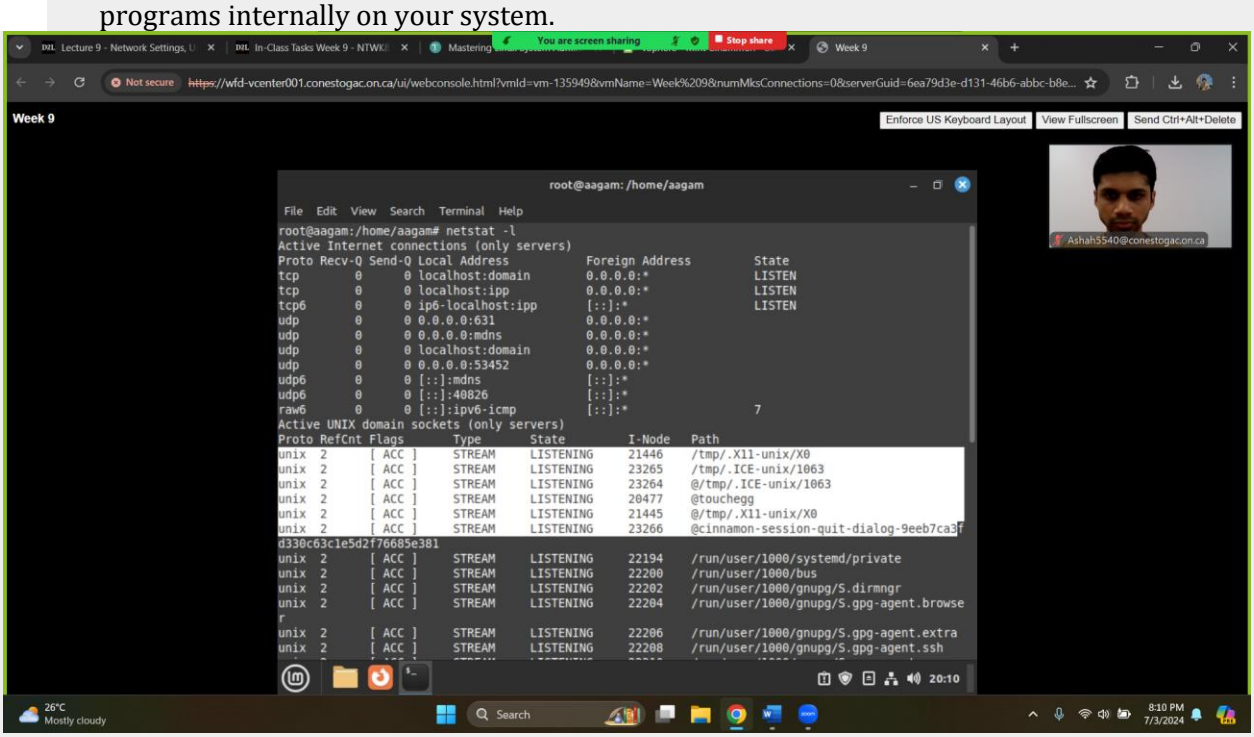
2. Week 9 Slide 19

WATCHING FOR NETWORK CONNECTIONS

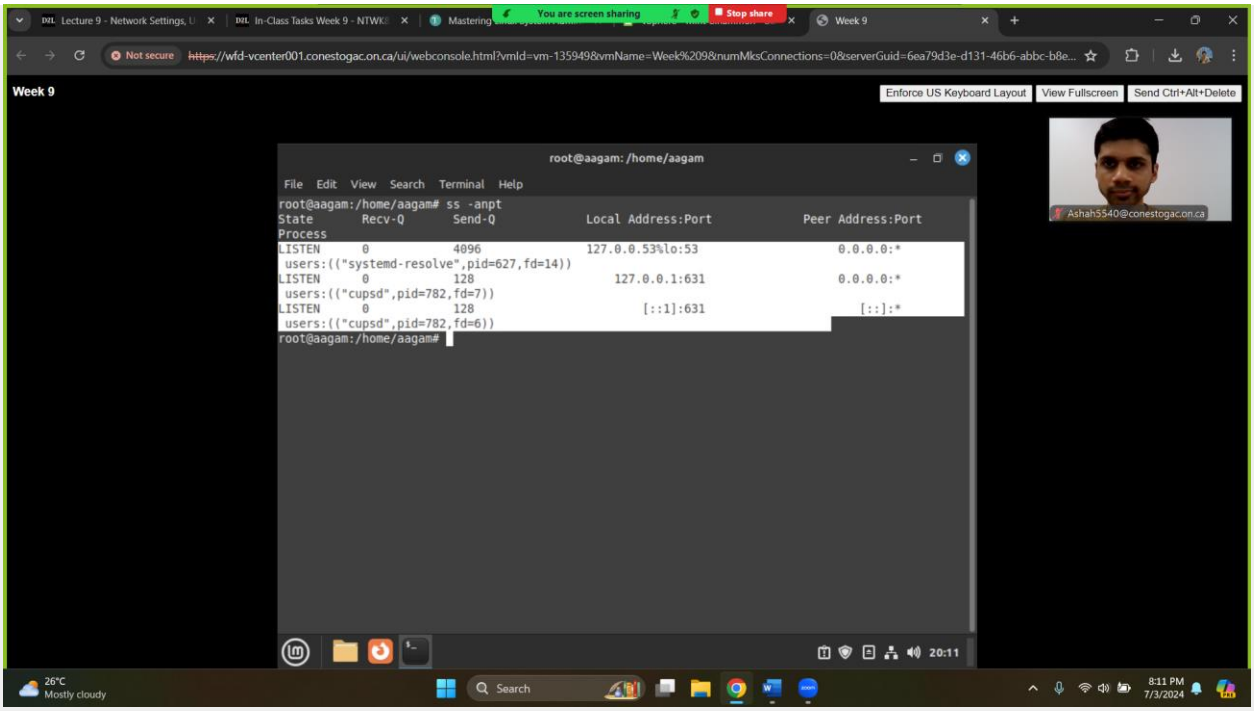
1. Log into your Linux server using the user account you created in Chapter 2 or Chapter 4, and acquire `root` privileges by using `su` or by using `sudo` with each of the following commands.



2. Type **`netstat -l`** to display the programs listening for incoming network connections. The entries marked as `unix` are using the loopback address to communicate with other programs internally on your system.



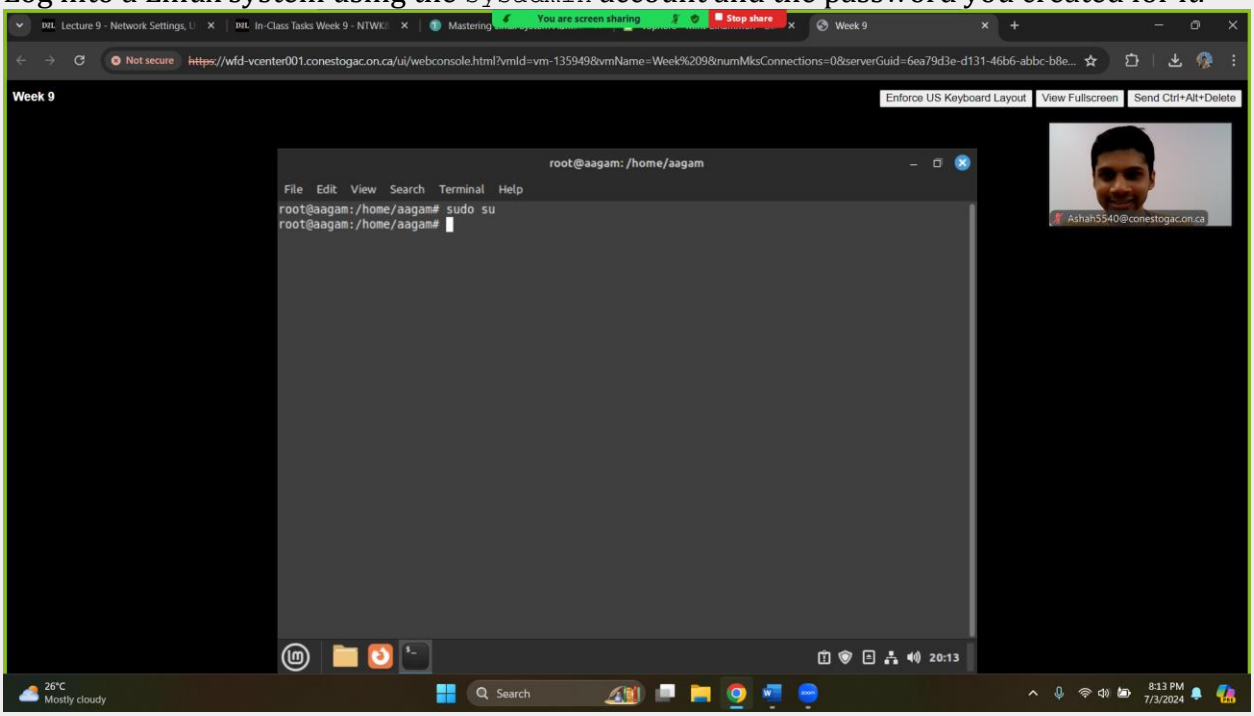
3. Type **`ss -anpt`** to display the processes that have active network ports open on your system.



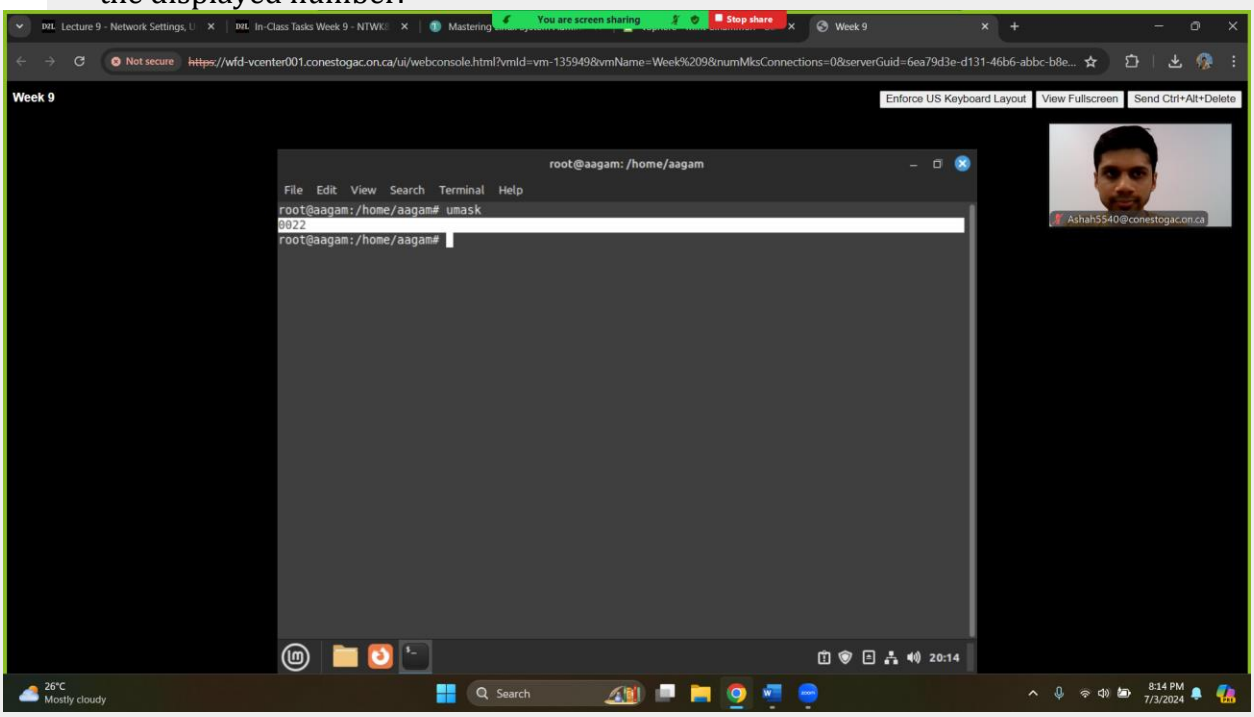
3. Week 9 Slide 29

EXPLORING THE EFFECT OF THE USER MASK ON PERMISSIONS

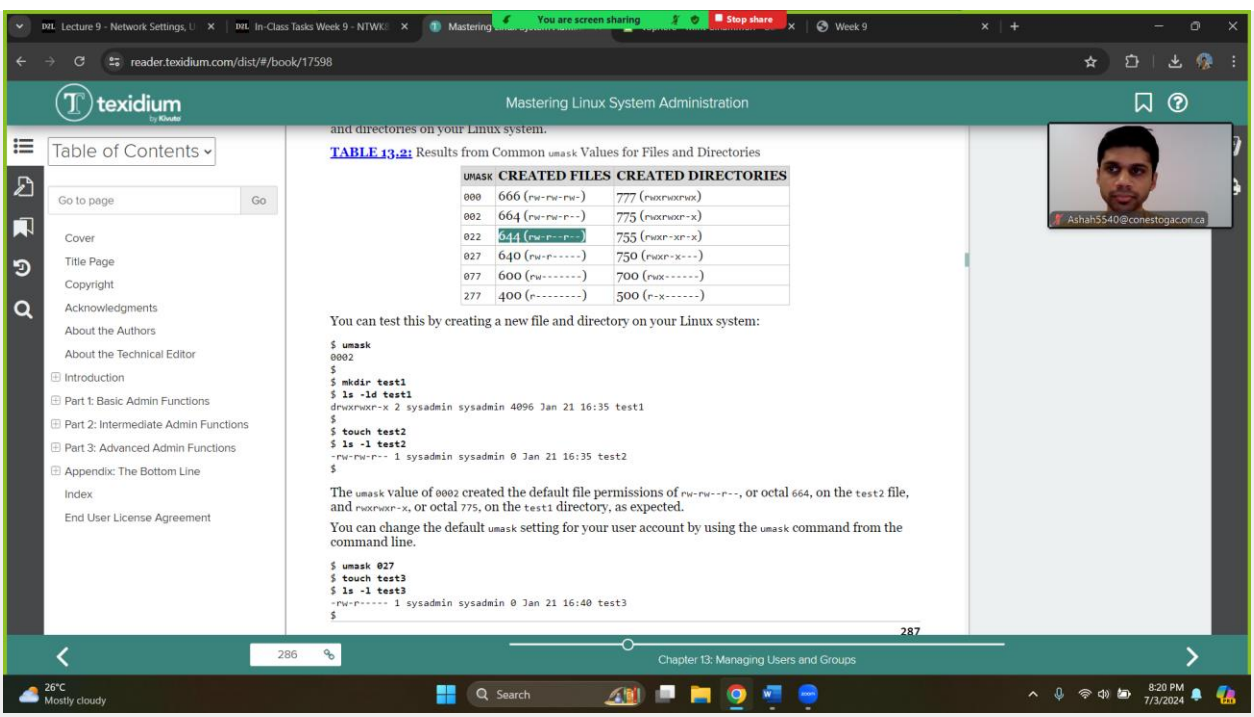
Log into a Linux system using the `sysadmin` account and the password you created for it.



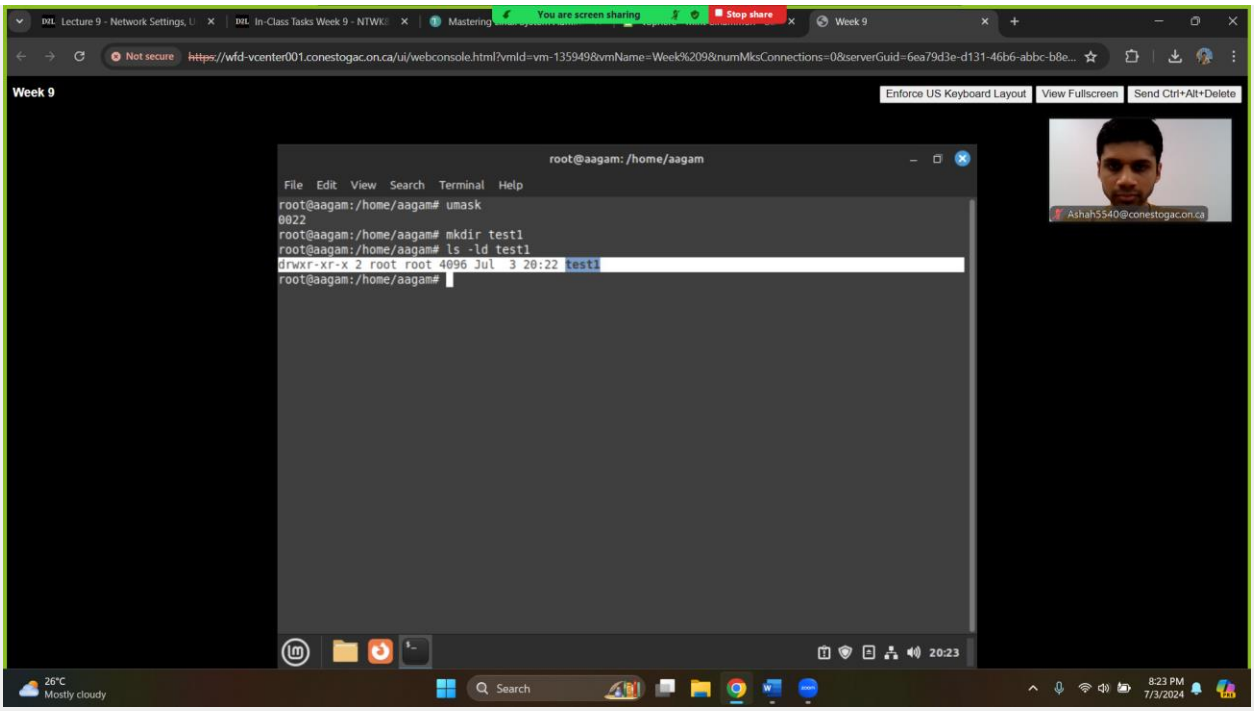
1. View your account's current user mask by typing **umask** and pressing Enter. Record the displayed number.



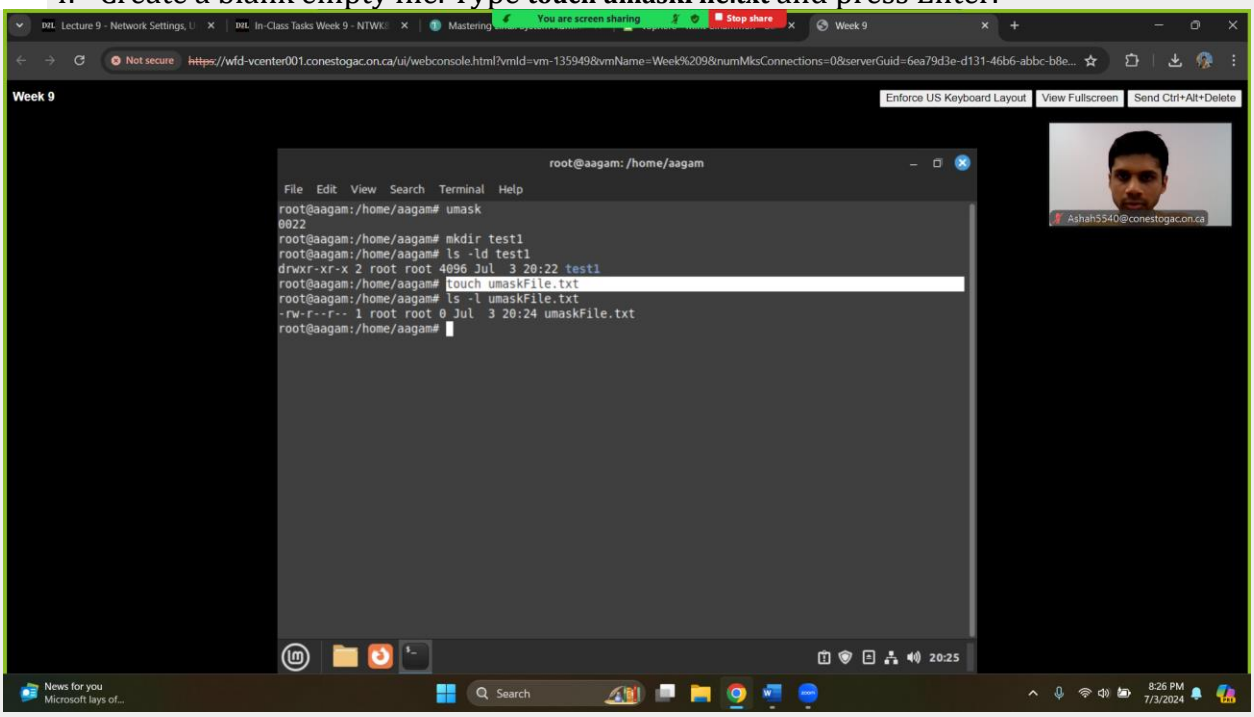
2. Determine the default permissions for a file on Linux. You can find this information near the beginning of the "Managing Default Permissions" section of this chapter. Record the octal code of default file permissions.



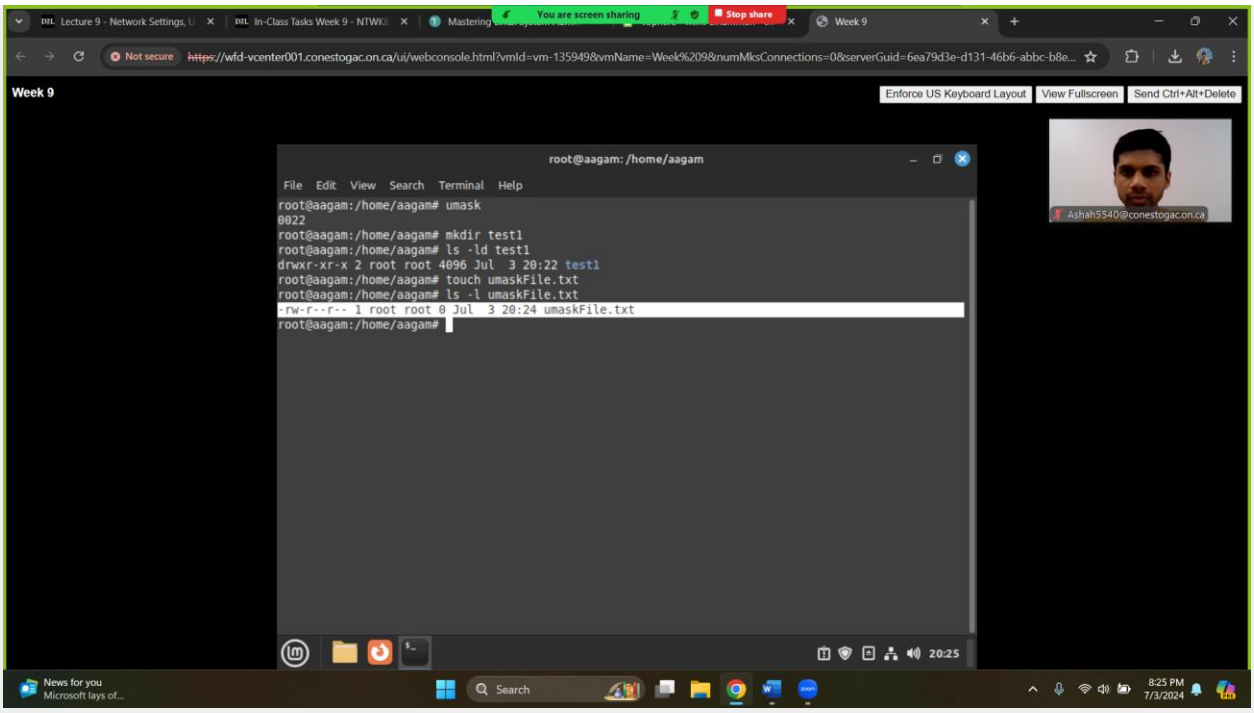
3. From the information you recorded in the previous two steps, calculate the permission settings for a newly created file on your system and record your answer.



4. Create a blank empty file. Type **touch umaskFile.txt** and press Enter.



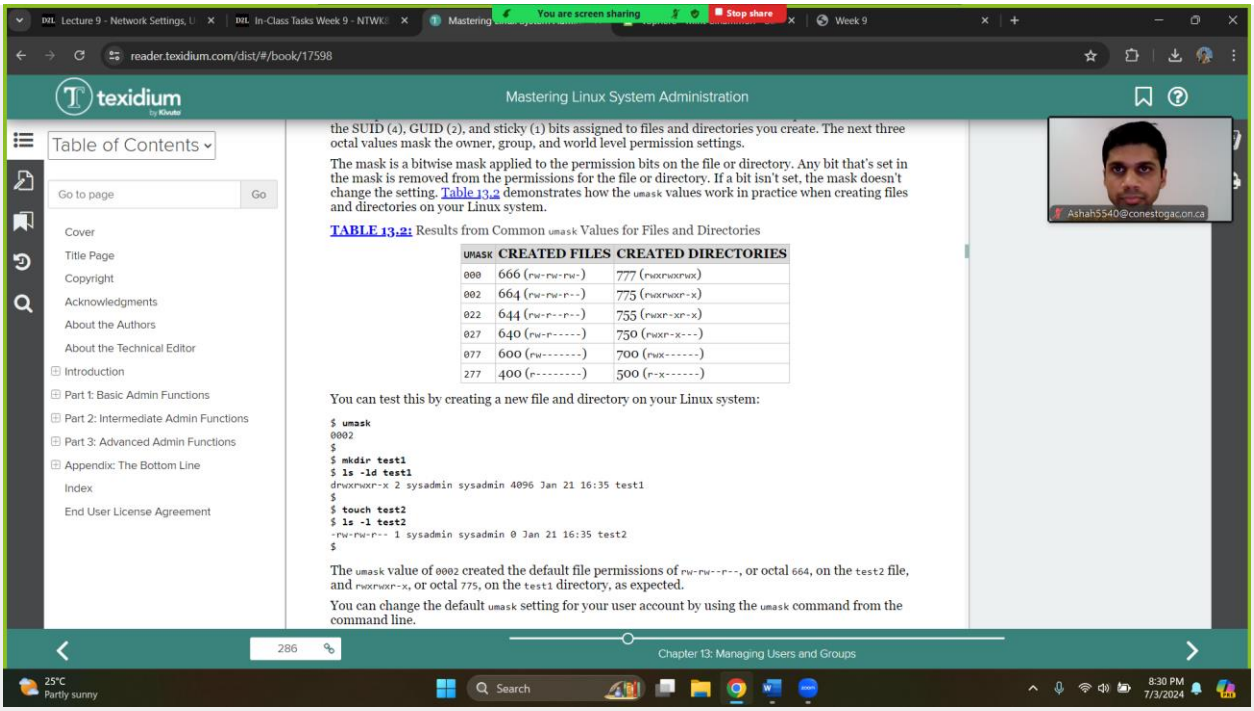
5. View the file's current permission settings by typing **ls -l umaskFile.txt** and pressing Enter. Record the owner, group, and world level permissions.



6. Compare the information you recorded in step 6 to your calculation in step 4. If the data does not match, determine where you made a mistake in your calculations.

➔ It matched the 644 (`rw-r--r--`) permission of 0022 (umask)

7. Determine the default permissions for a directory on Linux. You can find this information near the beginning of the "Managing Default Permissions" section of this chapter. Record the octal code of default directory permissions.



the SUID (4), GUID (2), and sticky (1) bits assigned to files and directories you create. The next three octal values mask the owner, group, and world level permission settings.

The mask is a bitwise mask applied to the permission bits on the file or directory. Any bit that's set in the mask is removed from the permissions for the file or directory. If a bit isn't set, the mask doesn't change the setting. Table 13.2 demonstrates how the `umask` values work in practice when creating files and directories on your Linux system.

TABLE 13.2: Results from Common `umask` Values for Files and Directories

UMASK	CREATED FILES	CREATED DIRECTORIES
000	666 (rw-rw-rw-)	777 (rwxrwxrwx)
002	664 (rw-rw-r--)	775 (rwxrwxr-x)
022	644 (rw-r--r--)	755 (rwxr-xr-x)
027	640 (rw-r-----)	750 (rwxr-x---)
077	600 (rw-------)	700 (rwx------)
277	400 (r--------)	500 (r-x------)

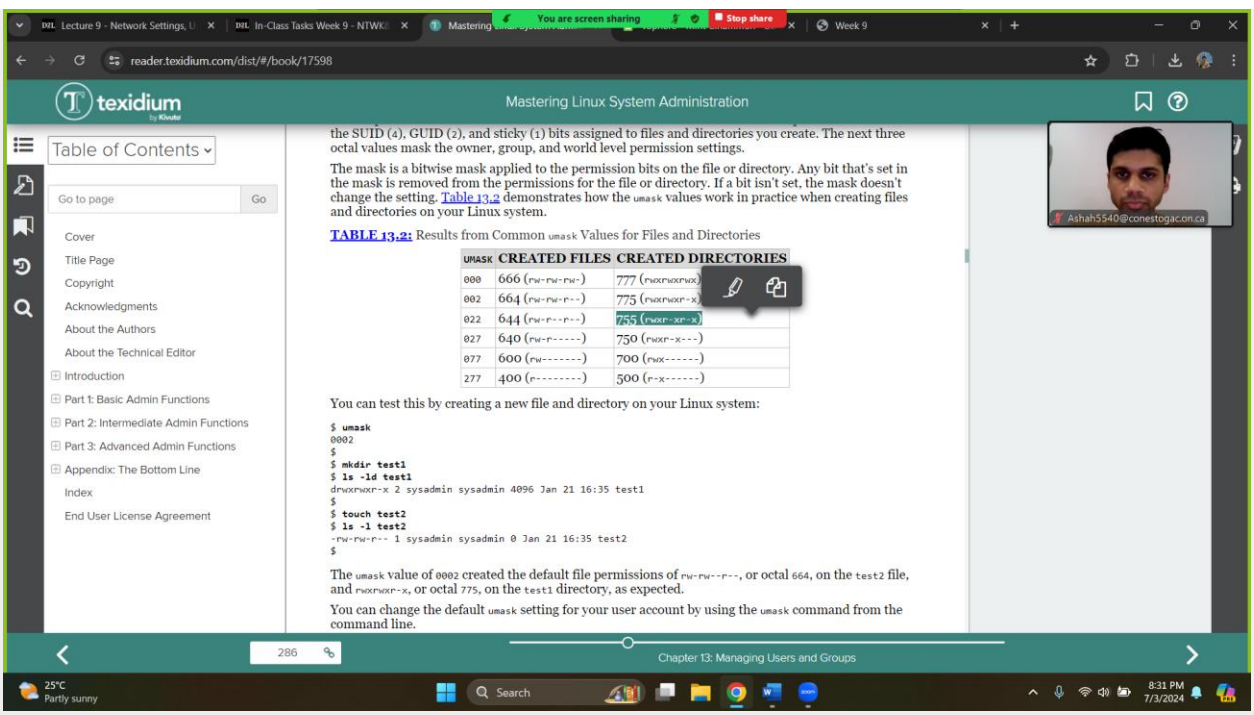
You can test this by creating a new file and directory on your Linux system:

```
$ umask
0002
$
$ mkdir test1
$ ls -ld test1
drwxrwxr-x 2 sysadmin sysadmin 4096 Jan 21 16:35 test1
$
$ touch test2
$ ls -l test2
-rw-rw-r-- 1 sysadmin sysadmin 0 Jan 21 16:35 test2
$
```

The `umask` value of `0002` created the default file permissions of `rw-rw-r--`, or octal `664`, on the `test2` file, and `rwxrwxr-x`, or octal `775`, on the `test1` directory, as expected.

You can change the default `umask` setting for your user account by using the `umask` command from the command line.

8. From the information you recorded in step 2 and step 8, calculate the permission settings for a newly created directory on your system and record your answer.



the SUID (4), GUID (2), and sticky (1) bits assigned to files and directories you create. The next three octal values mask the owner, group, and world level permission settings.

The mask is a bitwise mask applied to the permission bits on the file or directory. Any bit that's set in the mask is removed from the permissions for the file or directory. If a bit isn't set, the mask doesn't change the setting. Table 13.2 demonstrates how the `umask` values work in practice when creating files and directories on your Linux system.

TABLE 13.2: Results from Common `umask` Values for Files and Directories

UMASK	CREATED FILES	CREATED DIRECTORIES
000	666 (rw-rw-rw-)	777 (rwxrwxrwx)
002	664 (rw-rw-r--)	775 (rwxrwxr-x)
022	644 (rw-r--r--)	755 (rwxr-xr-x)
027	640 (rw-r-----)	750 (rwxr-x---)
077	600 (rw-------)	700 (rwx------)
277	400 (r--------)	500 (r-x------)

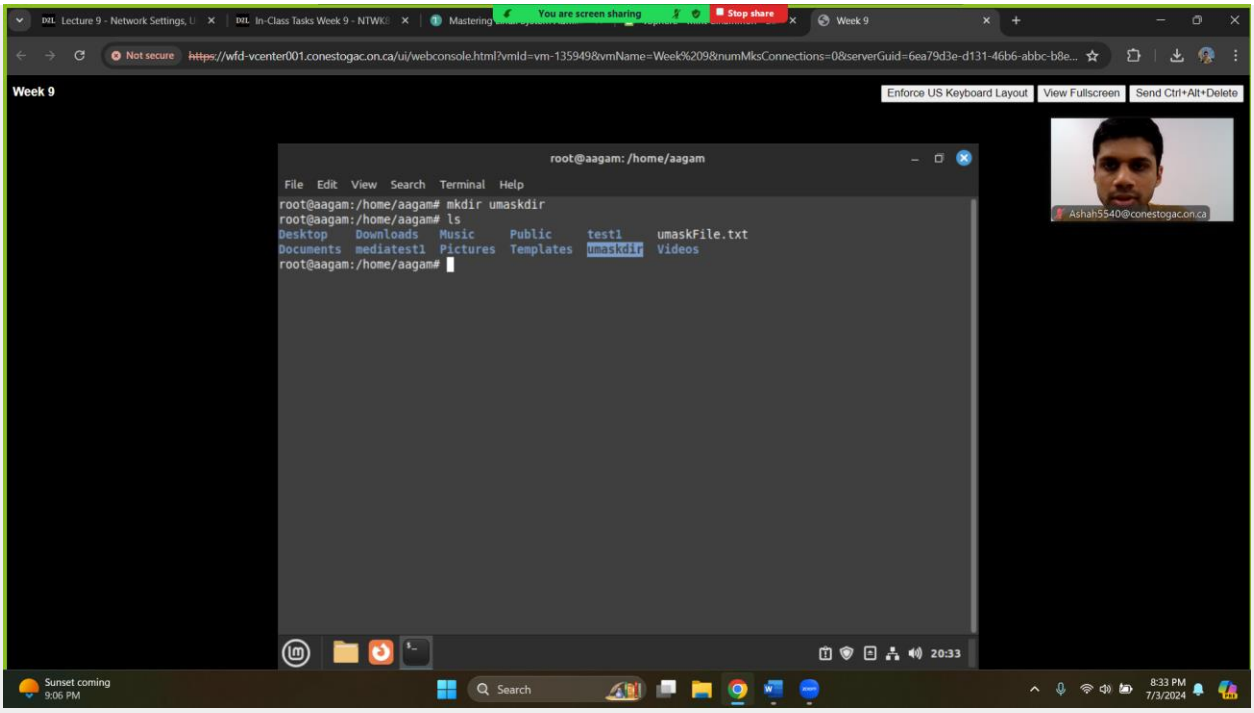
You can test this by creating a new file and directory on your Linux system:

```
$ umask
0002
$
$ mkdir test1
$ ls -ld test1
drwxrwxr-x 2 sysadmin sysadmin 4096 Jan 21 16:35 test1
$
$ touch test2
$ ls -l test2
-rw-rw-r-- 1 sysadmin sysadmin 0 Jan 21 16:35 test2
$
```

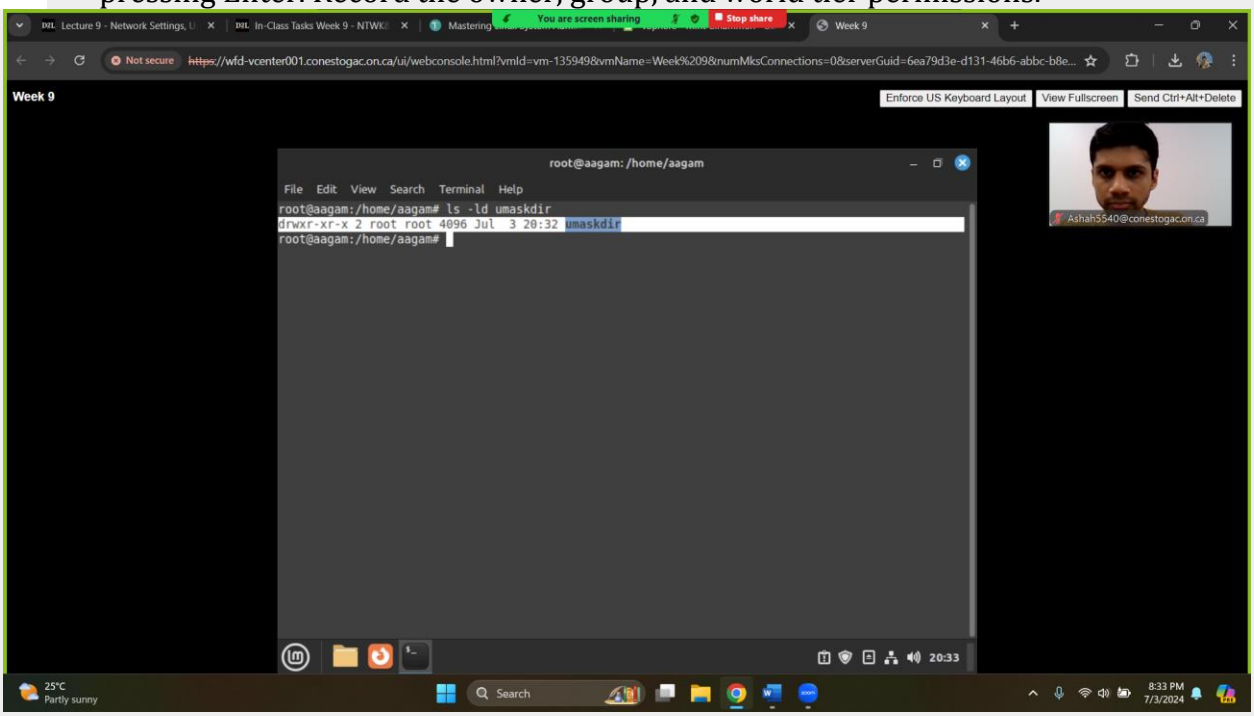
The `umask` value of `0002` created the default file permissions of `rw-rw-r--`, or octal `664`, on the `test2` file, and `rwxrwxr-x`, or octal `775`, on the `test1` directory, as expected.

You can change the default `umask` setting for your user account by using the `umask` command from the command line.

9. Create a new directory. Type **mkdir umaskDir** and press Enter.



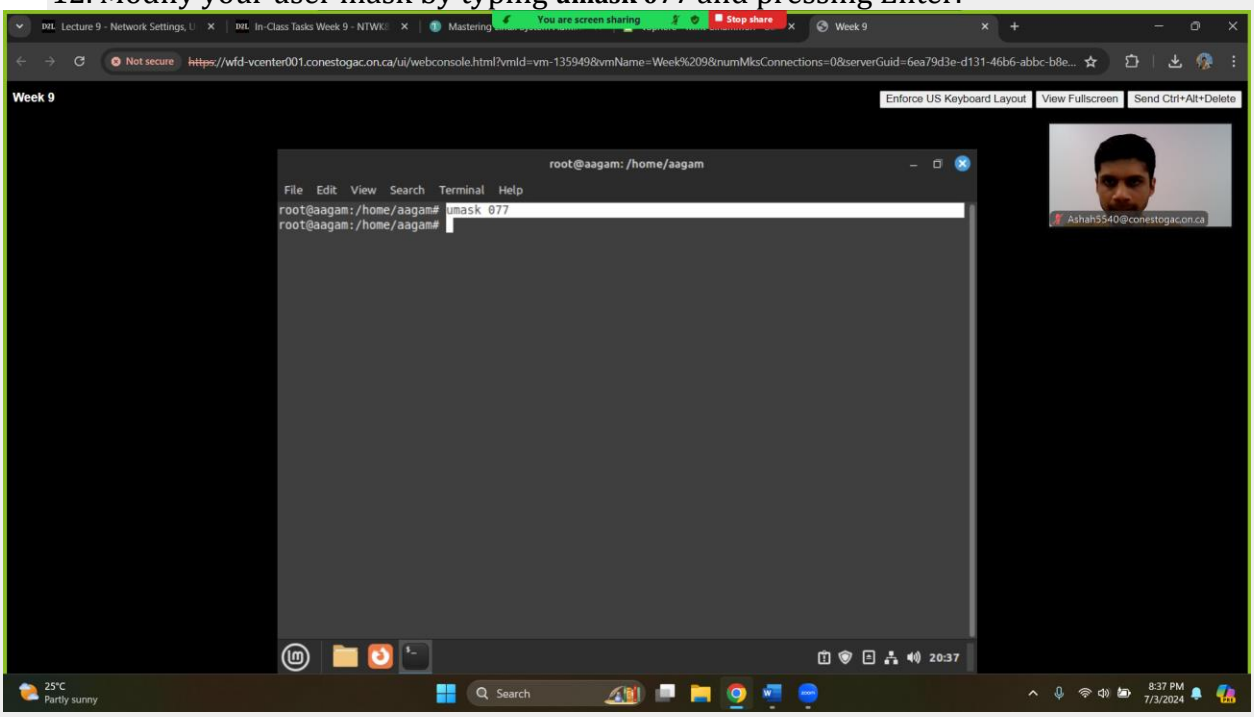
10. View the directory's current permission settings by typing **ls -ld umaskDir** and pressing Enter. Record the owner, group, and world tier permissions.



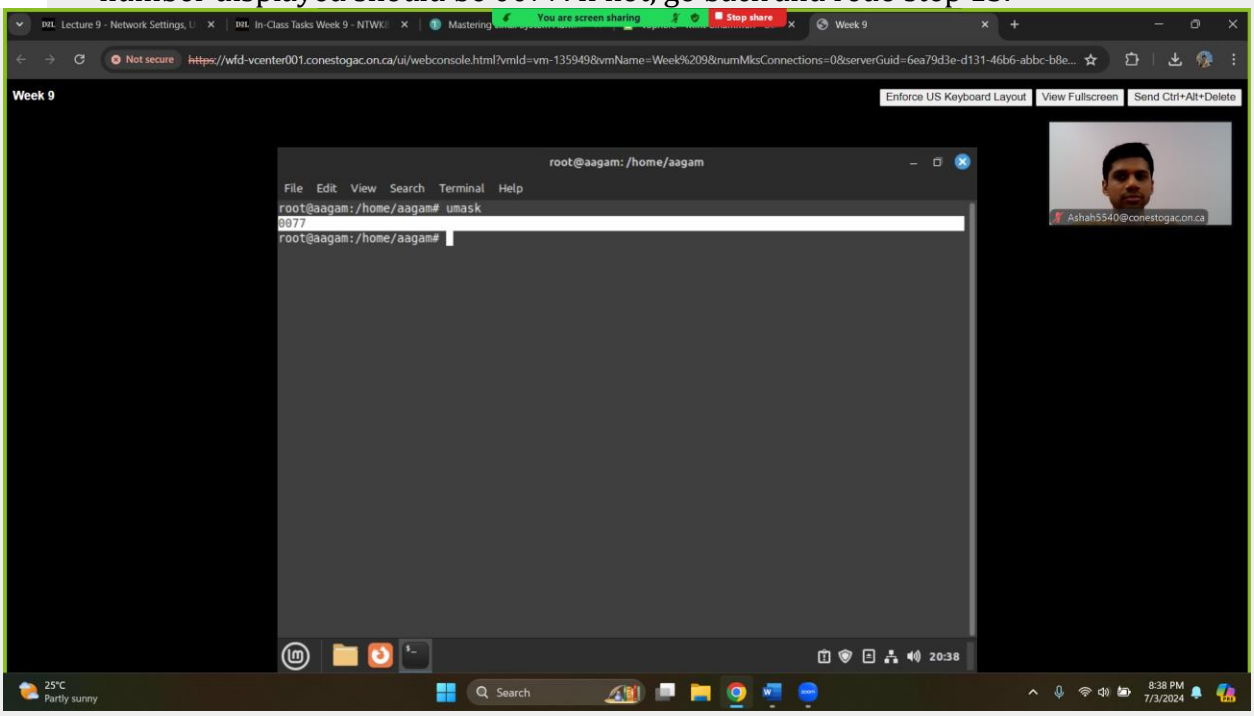
11. Compare the information you recorded in step 11 to your calculation in step 9. If the data does not match, determine where you made a mistake in your calculations.

→It matches the 755 (`rwxr-xr-x`) permissions of umaskdir (755)

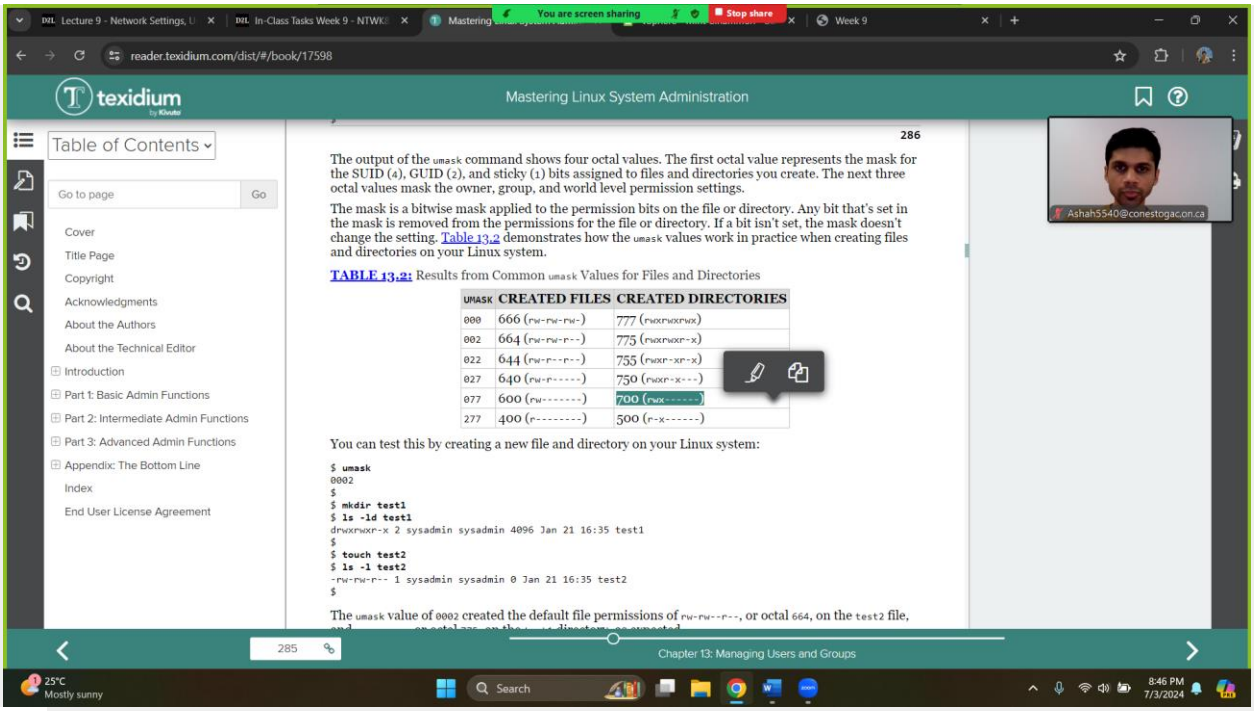
12. Modify your user mask by typing **umask 077** and pressing Enter.



13. Check that the user mask was set correctly by typing **umask** and pressing Enter. The number displayed should be 0077. If not, go back and redo step 13.

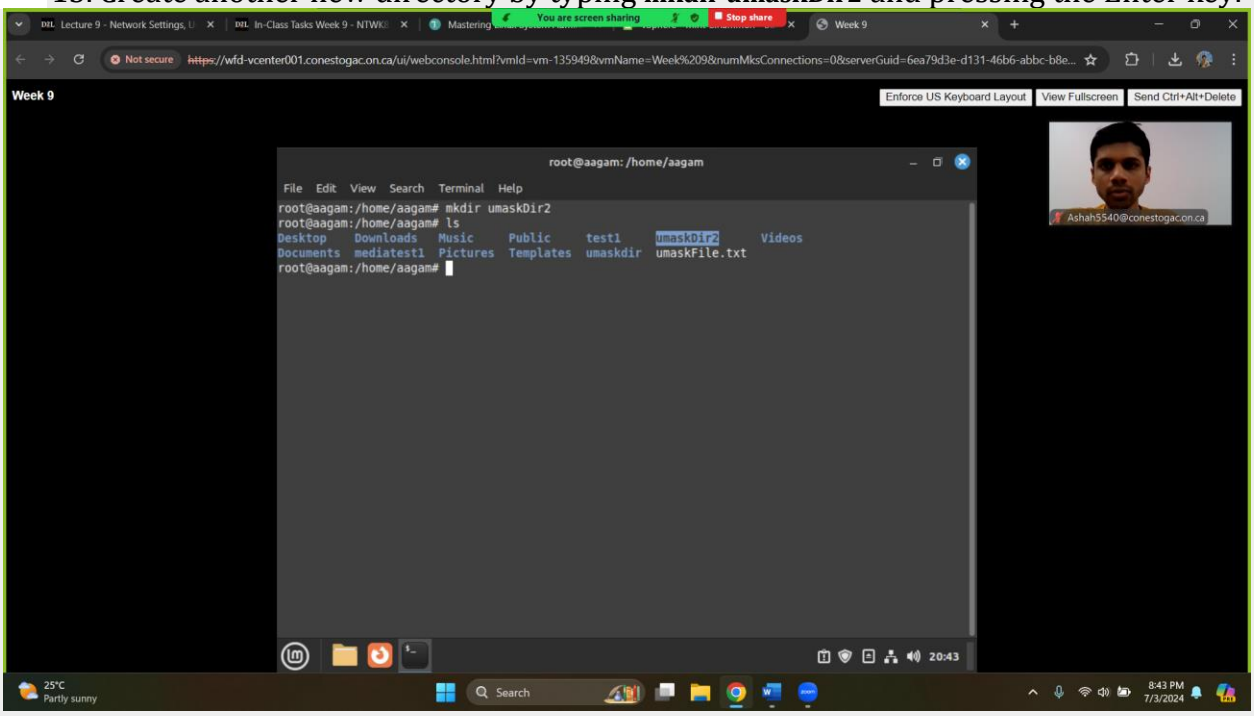


14. With this new user mask setting, determine the permission settings for a newly created directory on your system and record your answer.

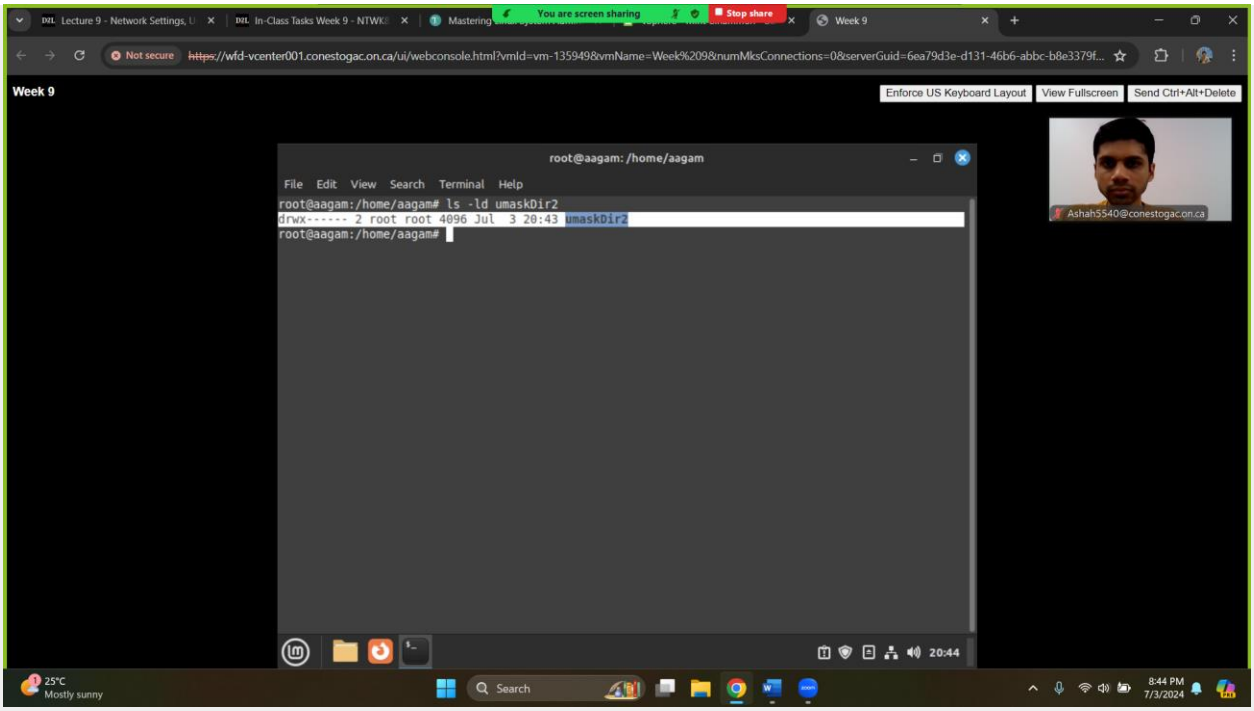


➔ 700 (rwx------)

15. Create another new directory by typing **mkdir umaskDir2** and pressing the Enter key.



16. View the newly created directory's current permission settings by typing **ls -ld umaskDir2** and pressing Enter. Record the owner, group, and world tier permissions.



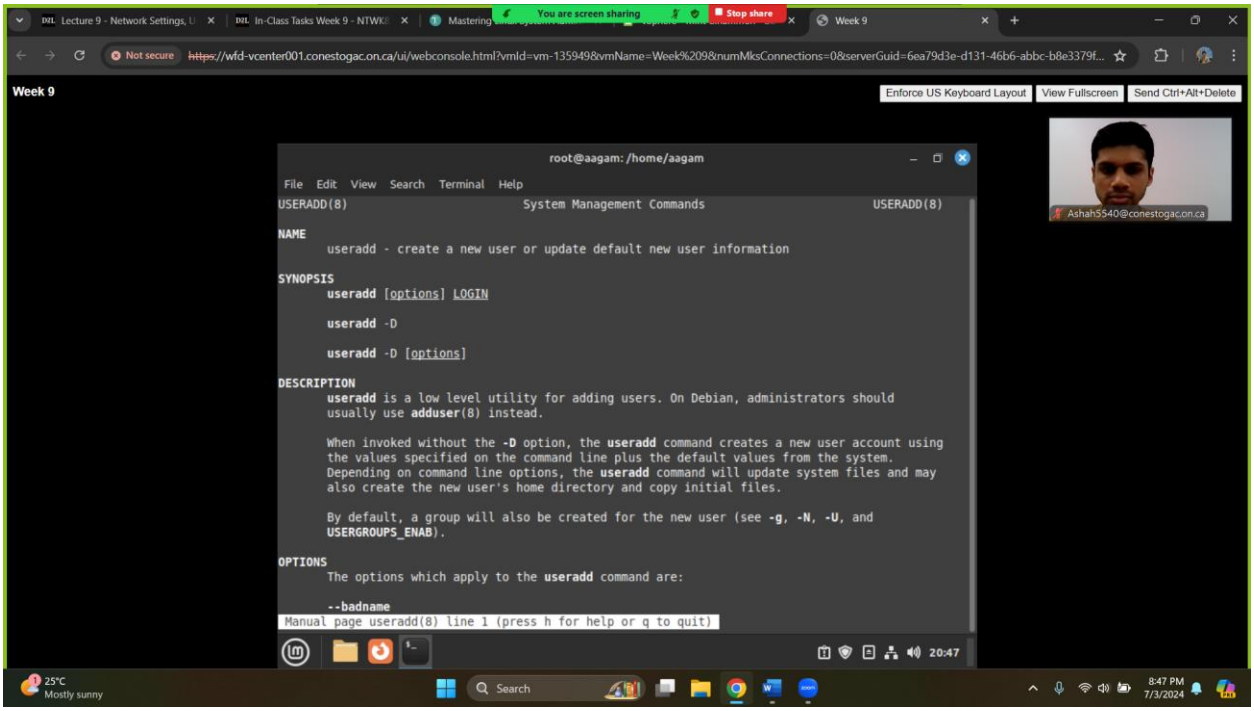
17. Compare the information you recorded in step 17 to your calculation in step 15. If the data does not match, determine where you made a mistake in your calculations.

➔ It matches the 700(rwx------) permission of umaskDir2

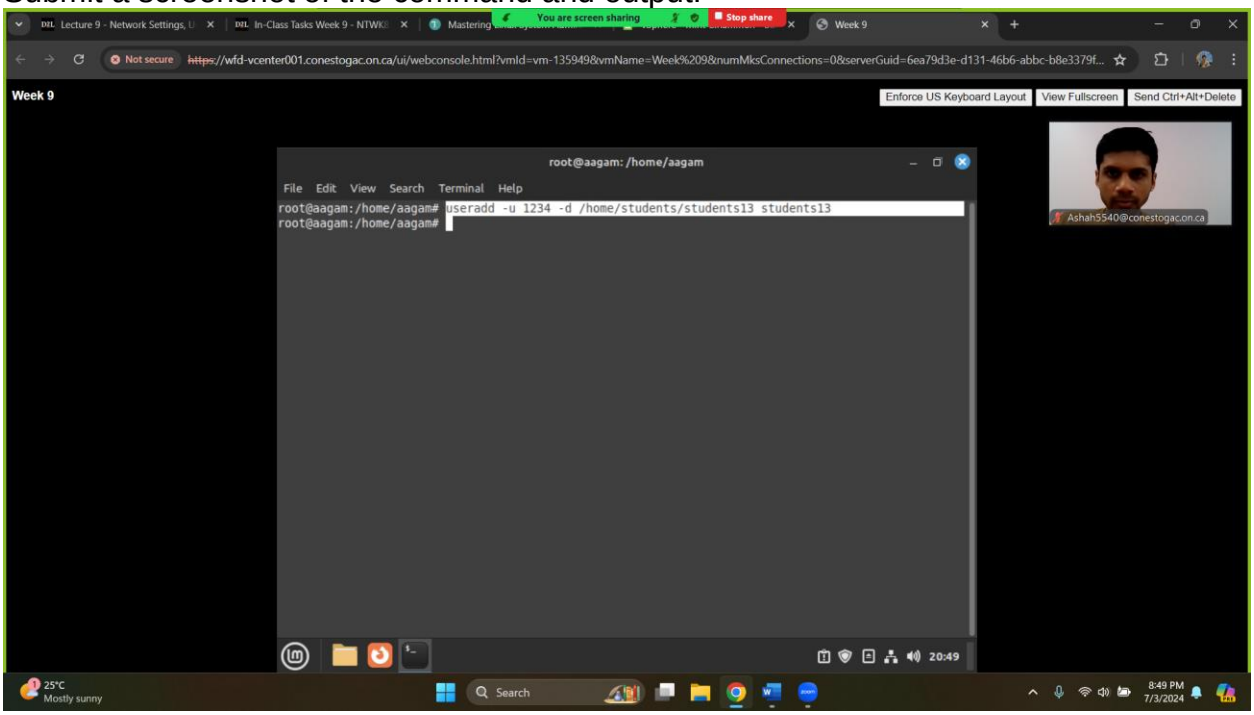
4. Week 9 Slide 41

In Class Task: useradd

Type man useradd and review the available options.

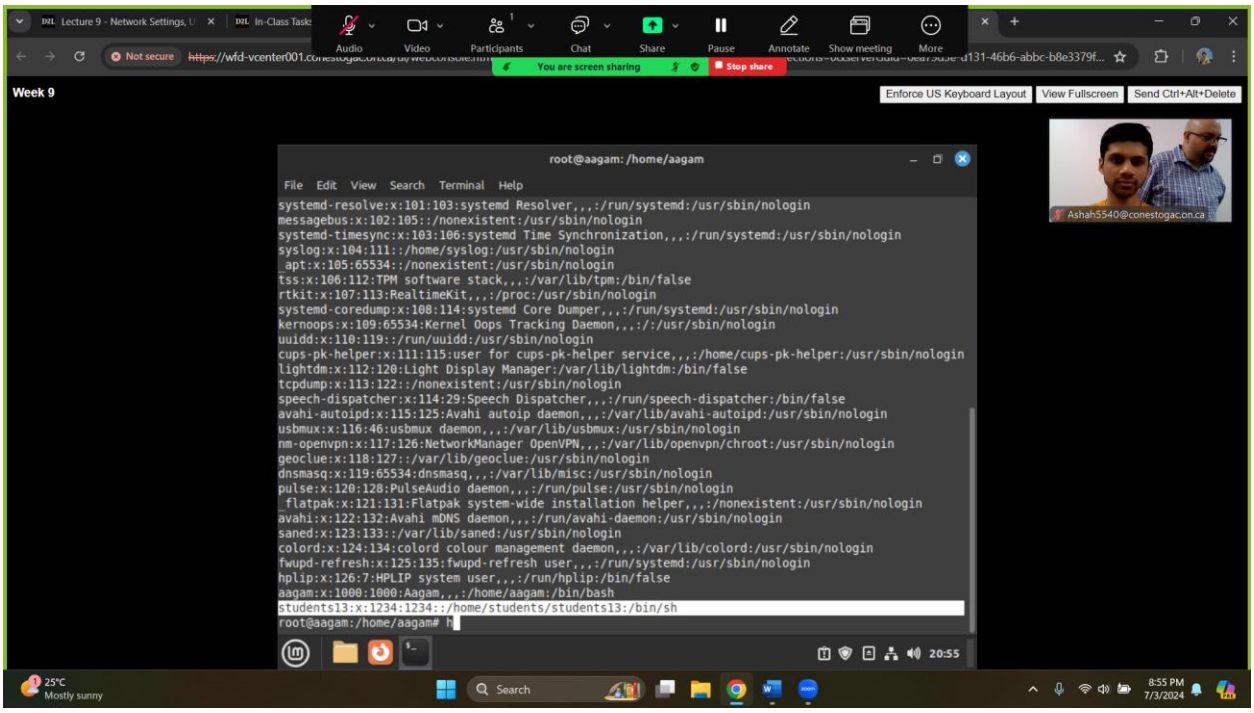


Create a user “student13” with a UID/GID of 1234 and a home directory of “/home/students/student13”
Submit a screenshot of the command and output.



Did you need to do anything besides the useradd command to get this to work?

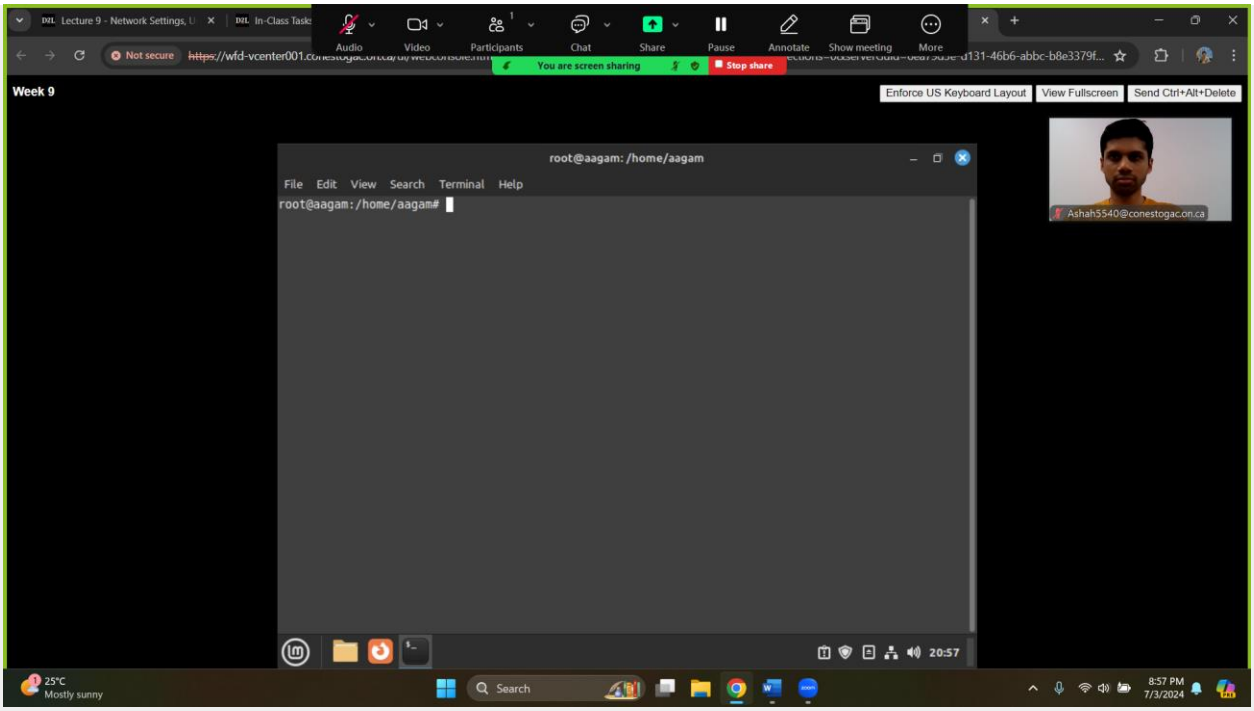
cat /etc/passwd



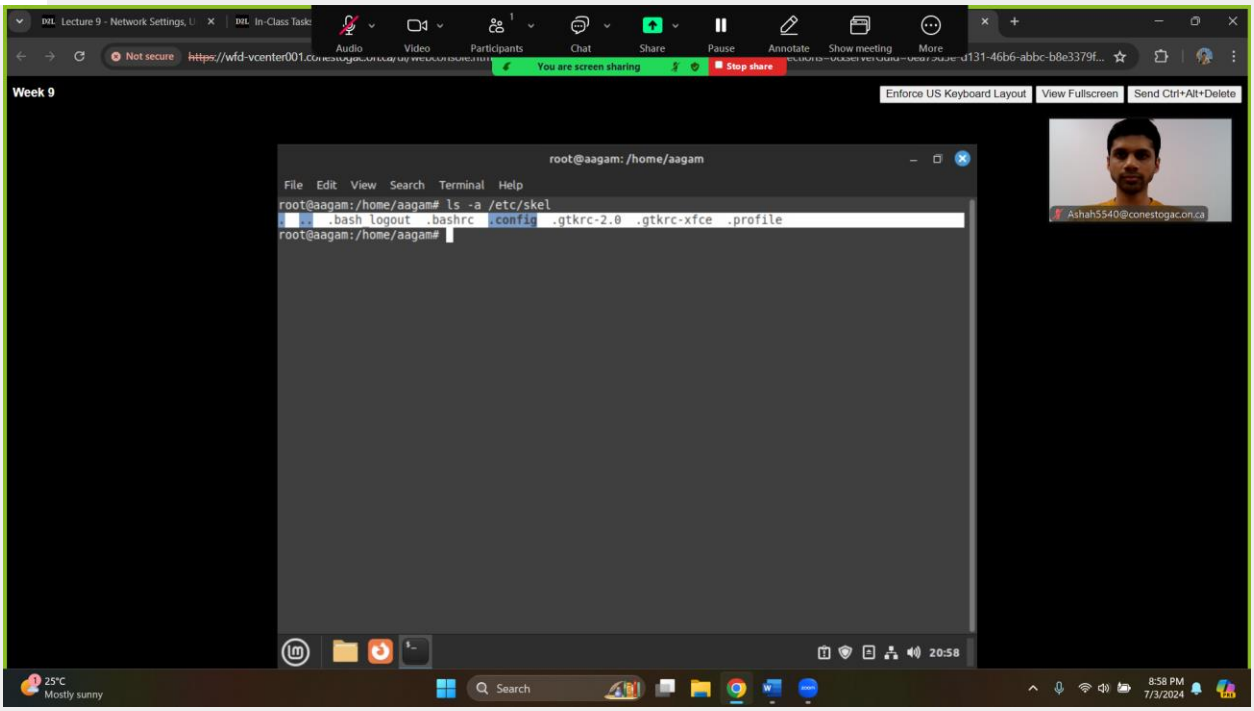
5. Week 9 Slide 44

DETERMINING THE EXISTENCE OF SYSTEM ENVIRONMENT FILES

1. Log into a Linux system using the `sysadmin` account and the password you created for it.



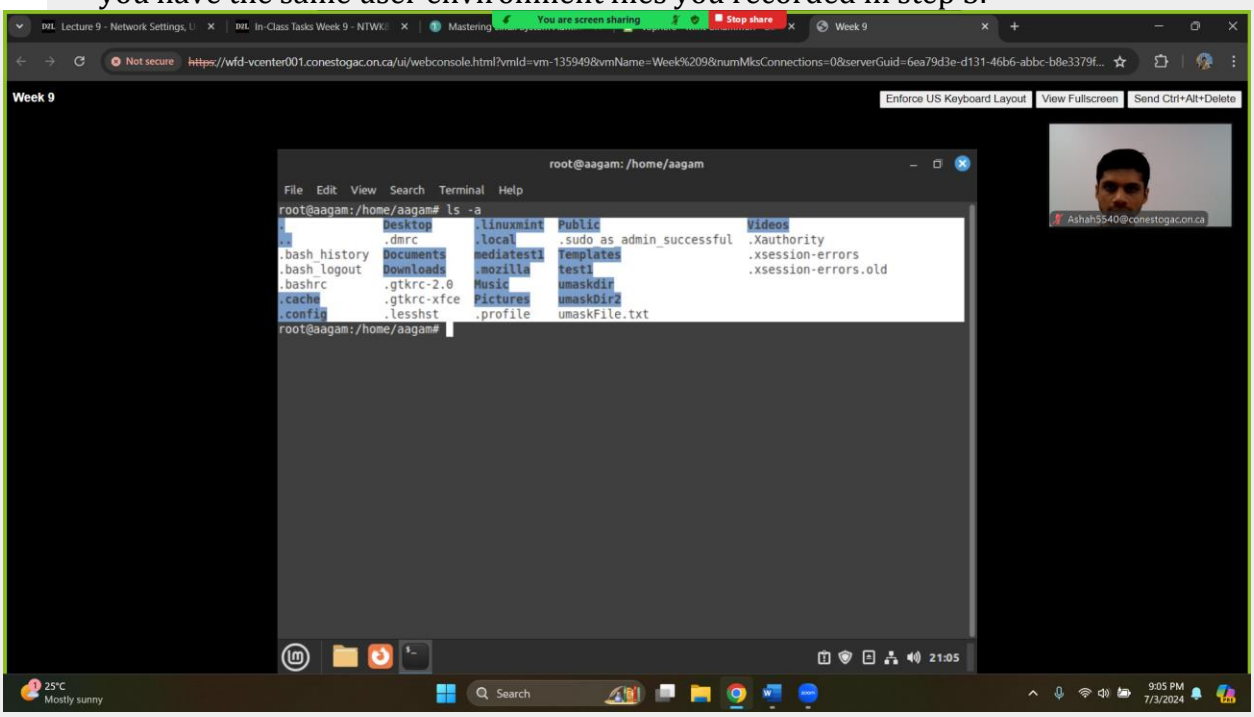
2. View your system's skeleton directory by typing **ls -a /etc/skel** and pressing Enter. Record the names of the files found there.



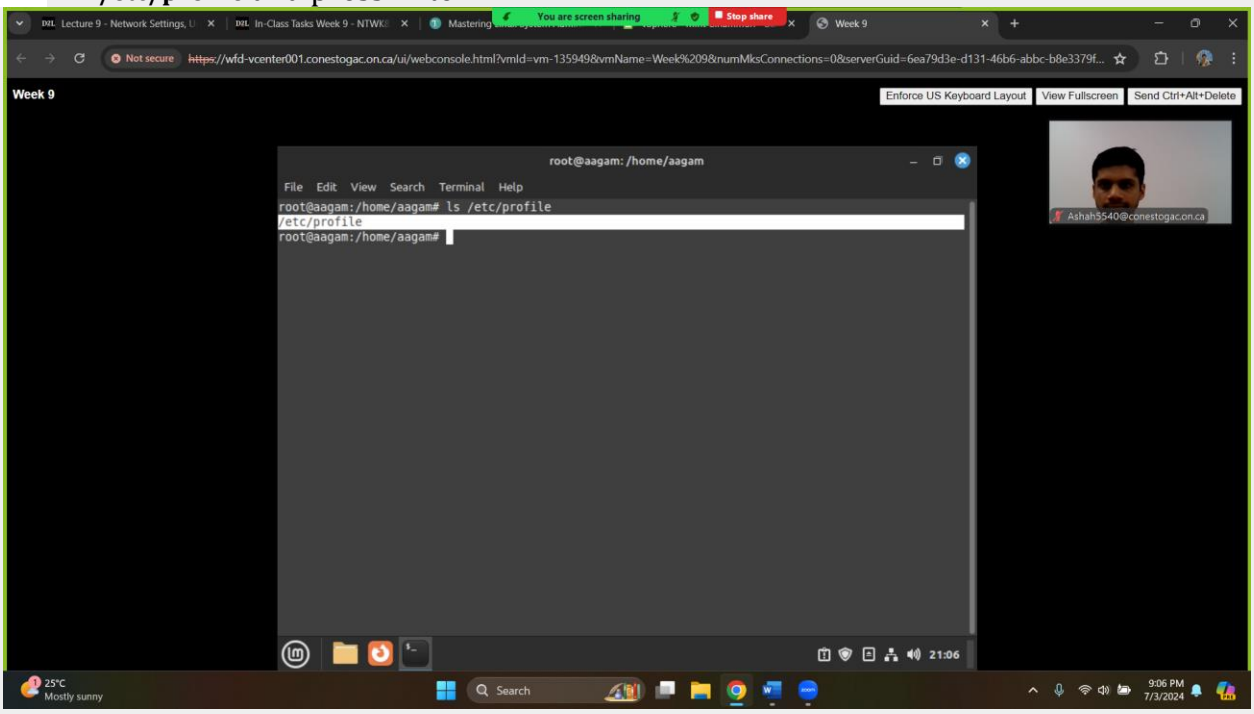
3. From the reading, determine which of the files you found in the previous step are user environment files. Record the names of those files here.

➔ **.bashrc** and **.profile**

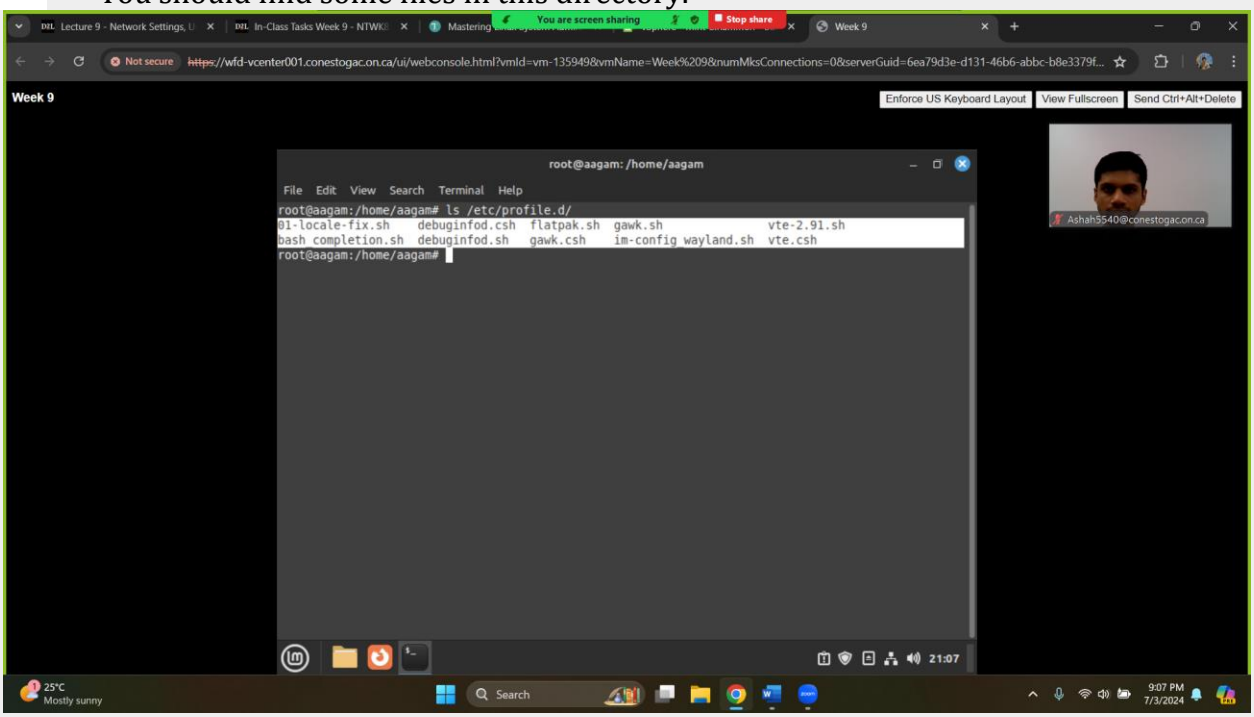
4. View the files in your home directory by typing **ls -a** and pressing Enter. Determine if you have the same user environment files you recorded in step 3.



5. See if the global environment file, `/etc/profile`, exists on your system. Type **ls /etc/profile** and press Enter.



6. Determine if there are already any files in the `/etc/profile.d/` directory where you can create customized environment scripts. Type **ls /etc/profile.d/** and press Enter. You should find some files in this directory.



7. See which global environment file your system has on it, **/etc/bashrc** or **/etc/bash.bashrc**. Type **ls /etc/*bashrc** and press Enter. Record your findings.