Name: Clarence B. Chavez	**Date Performed:** Sept. 4, 2024
Course/Section: CPE31S2	**Date Submitted:** Sept. 4, 2024
Instructor: Engr. Robin Valenzuela	**Semester and SY:** 1st Sem (2024 - 2025)

Activity 2: SSH Key-Based Authentication and Setting up Git

1. **Objectives:**

1.1 Configure remote and local machine to connect via SSH using a KEY instead of using a password
1.2 Create a public key and private key
1.3 Verify connectivity
1.4 Setup Git Repository using local and remote repositories
1.5 Configure and Run ad hoc commands from local machine to remote servers

Part 1: Discussion

It is assumed that you are already done with the last Activity (**Activity 1: Configure Network using Virtual Machines).** *Provide screenshots for each task*.

It is also assumed that you have VMs running that you can SSH but requires a password. Our goal is to remotely login through SSH using a key without using a password. In this activity, we create a public and a private key. The private key resides in the local machine while the public key will be pushed to remote machines. Thus, instead of using a password, the local machine can connect automatically using SSH through an authorized key.

What Is ssh-keygen?

Ssh-keygen is a tool for creating new authentication key pairs for SSH. Such key pairs are used for automating logins, single sign-on, and for authenticating hosts.

SSH Keys and Public Key Authentication

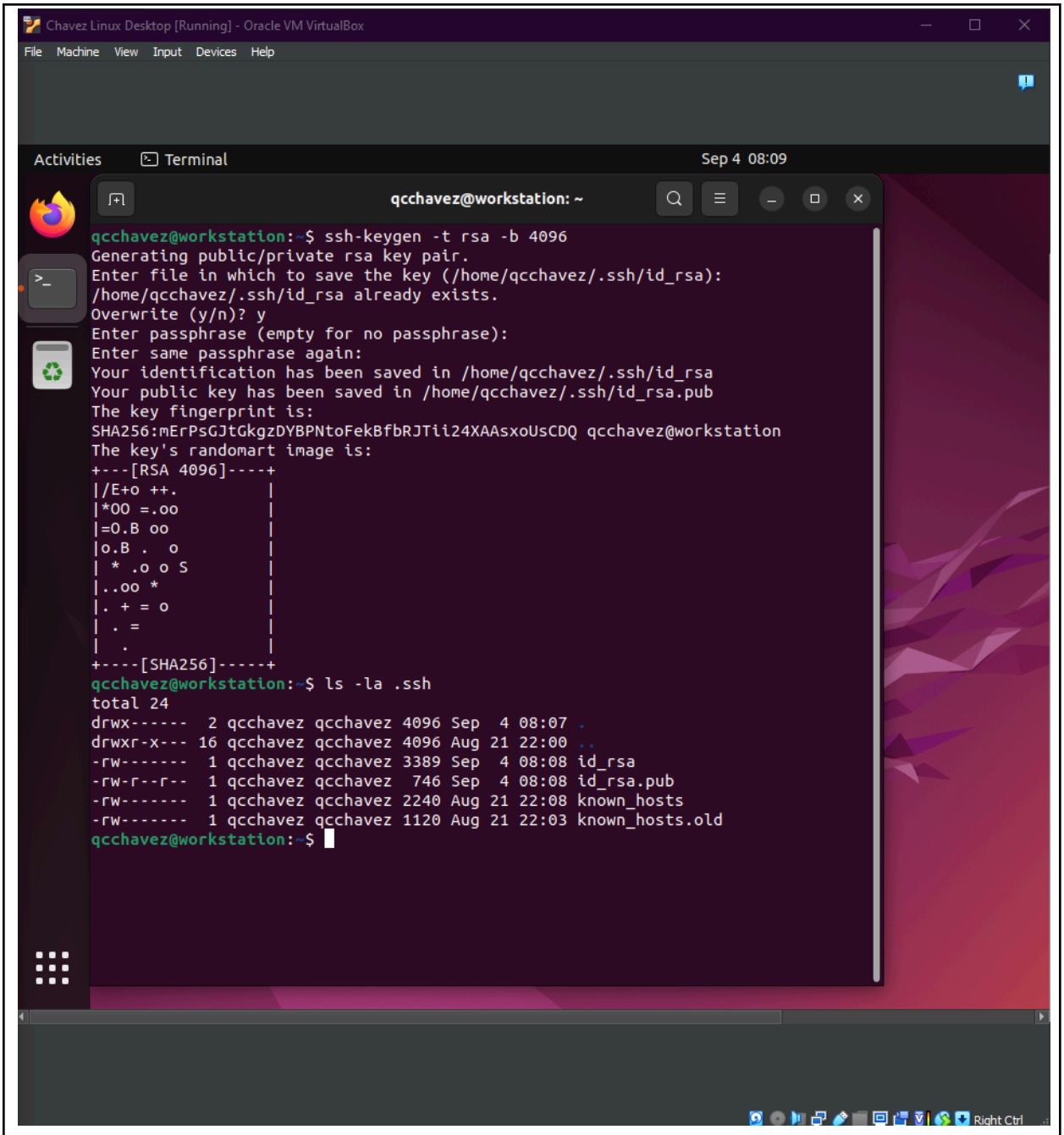
The SSH protocol uses public key cryptography for authenticating hosts and users. The authentication keys, called SSH keys, are created using the keygen program.

SSH introduced public key authentication as a more secure alternative to the older .rhosts authentication. It improved security by avoiding the need to have password stored in files and eliminated the possibility of a compromised server stealing the user's password.

However, SSH keys are authentication credentials just like passwords. Thus, they must be managed somewhat analogously to usernames and passwords. They should have a proper termination process so that keys are removed when no longer needed.

Task 1: Create an SSH Key Pair for User Authentication

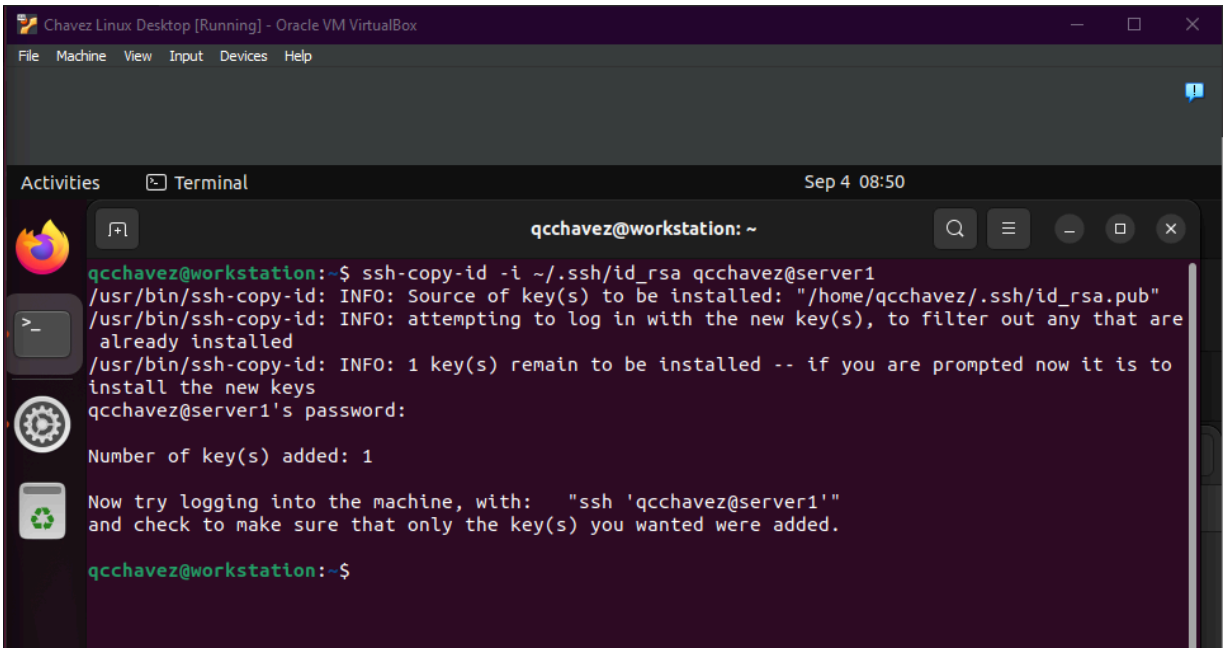
1. The simplest way to generate a key pair is to run *ssh-keygen* without arguments. In this case, it will prompt for the file in which to store keys. First, the tool asked where to save the file. SSH keys for user authentication are usually stored in the users .ssh directory under the home directory. However, in enterprise environments, the location is often different. The default key file name depends on the algorithm, in this case *id_rsa* when using the default RSA algorithm. It could also be, for example, *id_dsa* or *id_ecdsa*.
2. Issue the command *ssh-keygen -t rsa -b 4096.* The algorithm is selected using the -t option and key size using the -b option.
3. When asked for a passphrase, just press enter. The passphrase is used for encrypting the key, so that it cannot be used even if someone obtains the private key file. The passphrase should be cryptographically strong.
4. Verify that you have created the key by issuing the command *ls -la .ssh.* The command should show the .ssh directory containing a pair of keys. For example, id_rsa.pub and id_rsa.


Chavez Linux Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Sep 4 08:09
qcchavez@workstation: ~
qcchavez@workstation:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/qcchavez/.ssh/id_rsa):
/home/qcchavez/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/qcchavez/.ssh/id_rsa
Your public key has been saved in /home/qcchavez/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:mErPsGJtGkgzDYBPNtoFekBfbRJTii24XAAsxoUsCDQ qcchavez@workstation
The key's randomart image is:
+---[RSA 4096]----+
|/E+o ++. |
|*OO =.oo |
|=O.B oo |
|o.B . o |
| * .o o S |
|..oo * |
|. + = o |
| . = |
| . |
+----[SHA256]-----+
qcchavez@workstation:~$ ls -la .ssh
total 24
drwx------ 2 qcchavez qcchavez 4096 Sep 4 08:07 .
drwxr-x--- 16 qcchavez qcchavez 4096 Aug 21 22:00 ..
-rw------- 1 qcchavez qcchavez 3389 Sep 4 08:08 id_rsa
-rw-r--r-- 1 qcchavez qcchavez 746 Sep 4 08:08 id_rsa.pub
-rw------- 1 qcchavez qcchavez 2240 Aug 21 22:08 known_hosts
-rw------- 1 qcchavez qcchavez 1120 Aug 21 22:03 known_hosts.old
qcchavez@workstation:~$
Right Ctrl

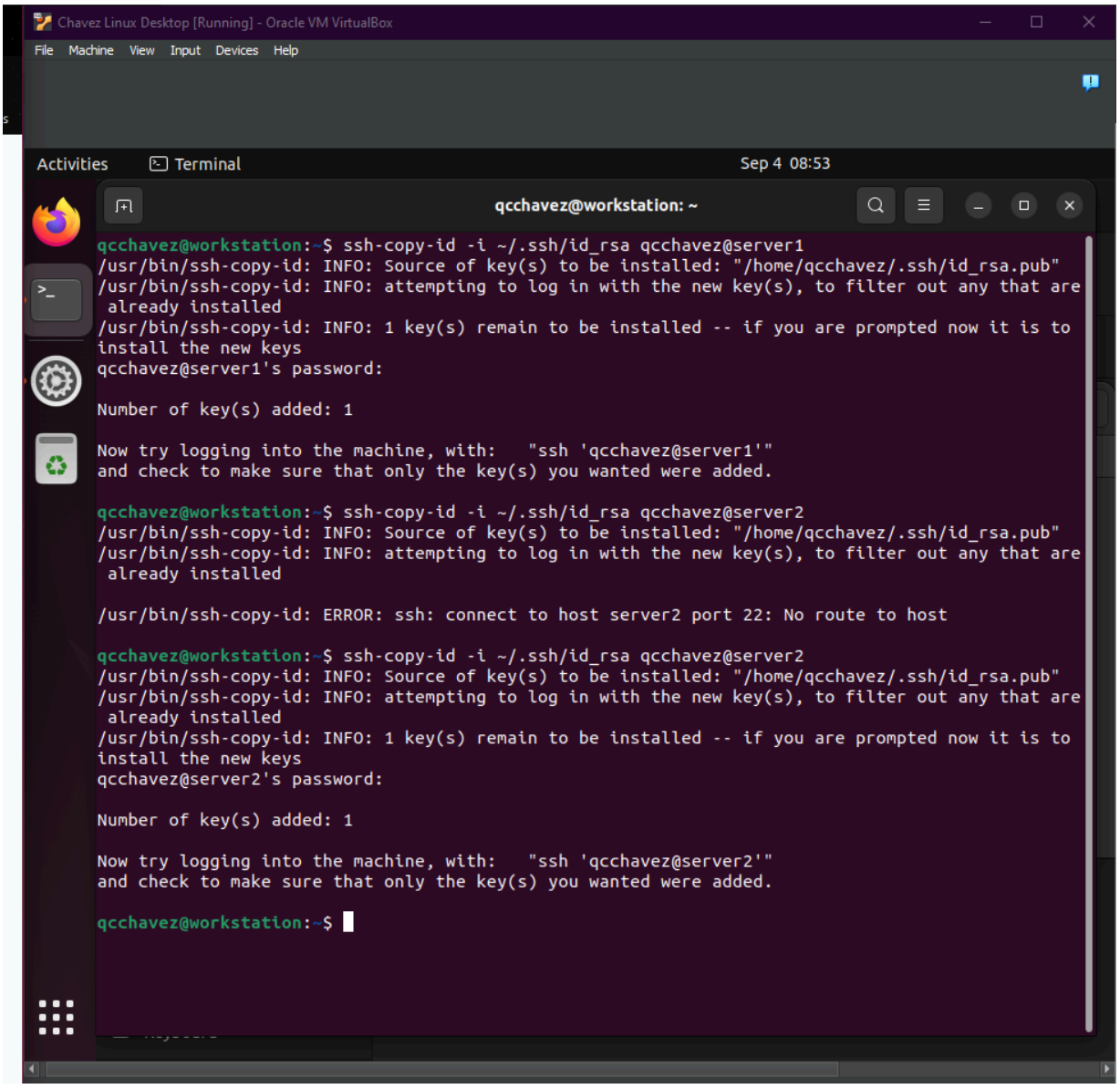
Task 2: Copying the Public Key to the remote servers

1. To use public key authentication, the public key must be copied to a server and installed in an *authorized_keys* file. This can be conveniently done using the *ssh-copy-id* tool.
2. Issue the command similar to this: *ssh-copy-id -i ~/.ssh/id_rsa user@host*

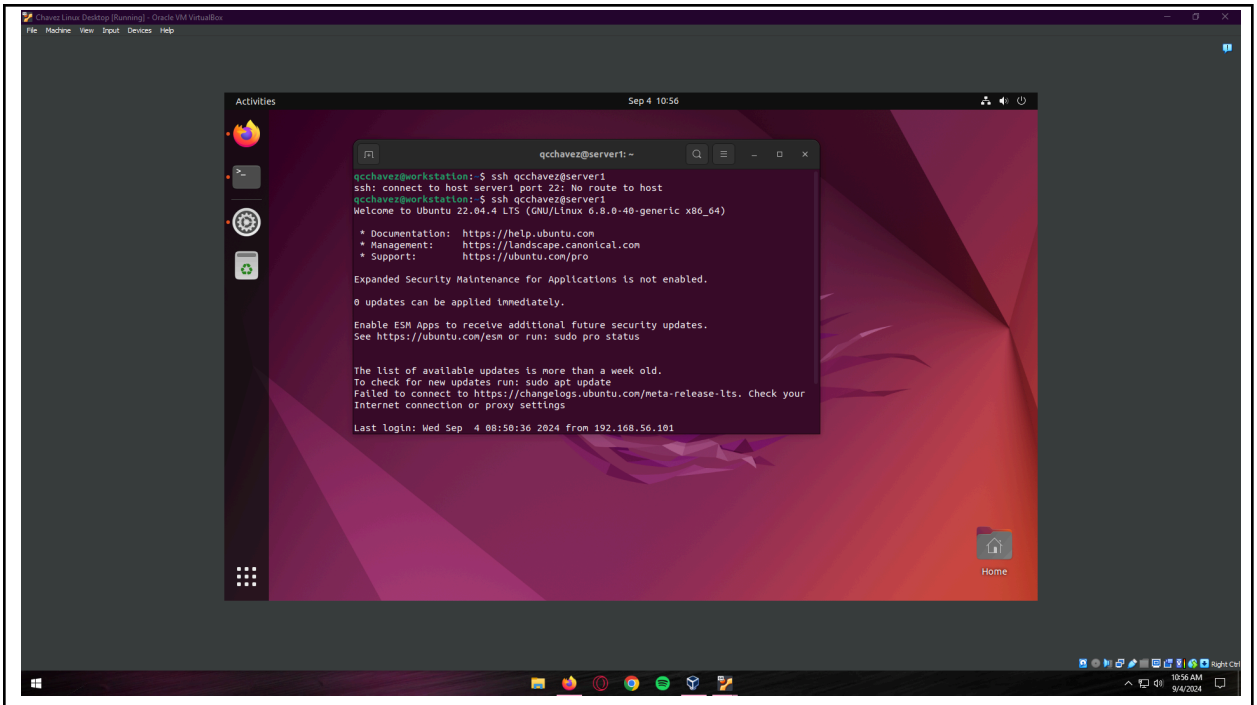
server1

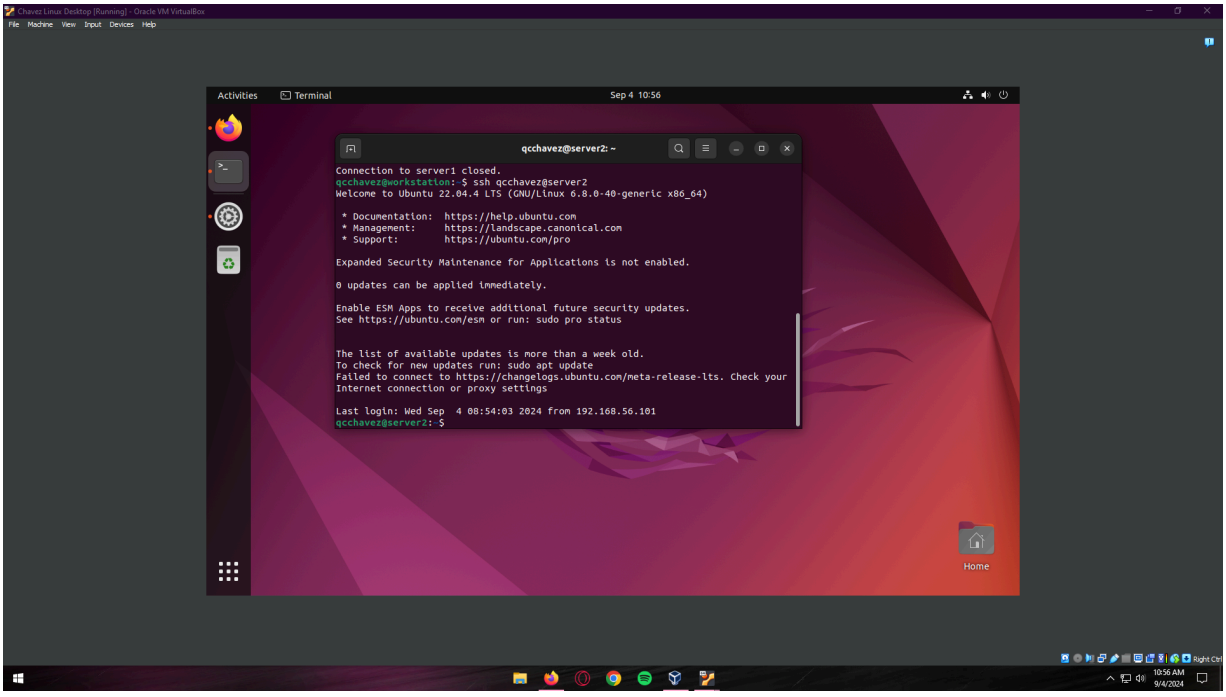


server2



3. Once the public key has been configured on the server, the server will allow any connecting user that has the private key to log in. During the login process, the client proves possession of the private key by digitally signing the key exchange.
4. On the local machine, verify that you can SSH with Server 1 and Server 2. What did you notice? Did the connection ask for a password? If not, why?





- It is because from the main desktop (the workstation host), I did not enter any passphrase, hence, the connection did not ask for a password.

Reflections:

Answer the following:

1. How will you describe the ssh-program? What does it do?

- **ssh-program** allows clients to access remote servers securely by providing a secure way to connect to a remote computer, transfer files, and even execute commands on it. It also uses strong encryption to protect the data that will be transmitted between the client and server.

2. How do you know that you already installed the public key to the remote servers?

- **Successful Login Attempt**, the terminal will give you a message that you have successfully logged in to the remote servers.
- **Checking Authorized Keys File**, by executing the command .ssh/authorized_keys
- **ssh-keygen command,** by executing this command with the combination of the necessary prefixes, you'll be able to find out if it is successfully installed.

Part 2: Discussion

Provide screenshots for each task.

It is assumed that you are done with the last activity (**Activity 2: SSH Key-Based Authentication**).

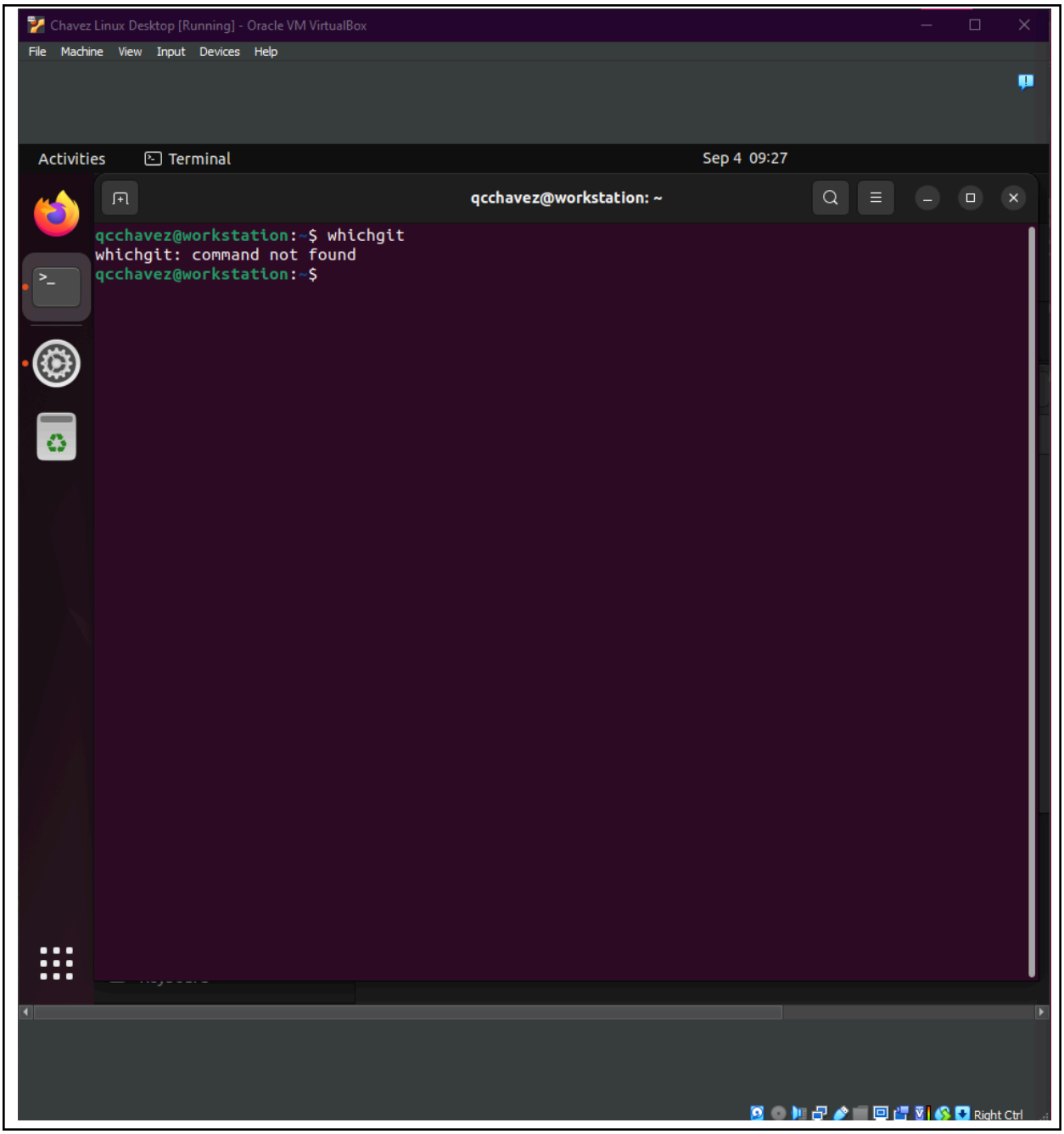
Set up Git

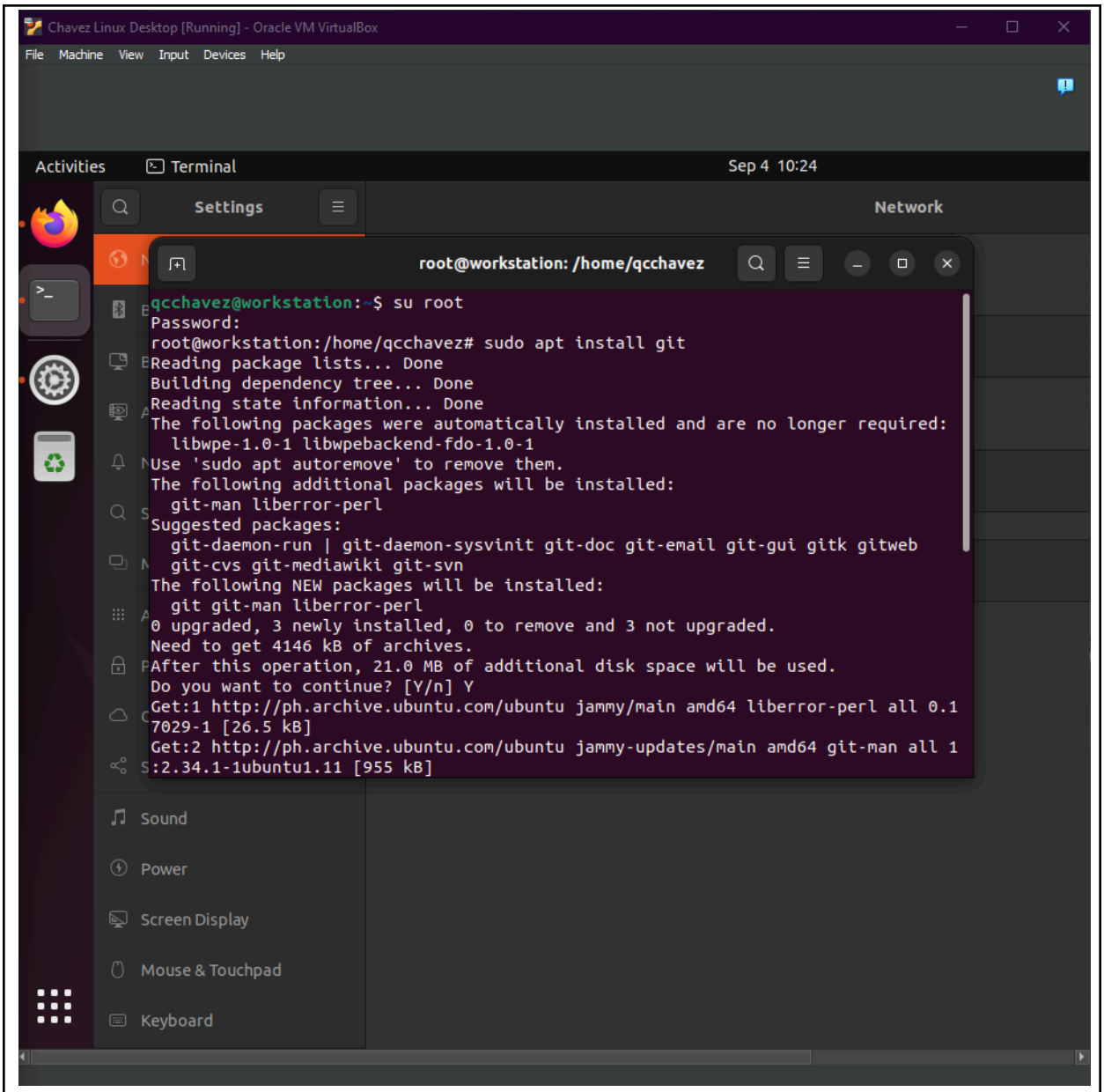
At the heart of GitHub is an open-source version control system (VCS) called Git. Git is responsible for everything GitHub-related that happens locally on your computer. To use Git on the command line, you'll need to download, install, and configure Git on your computer. You can also install GitHub CLI to use GitHub from the command line. If you don't need to work with files locally, GitHub lets you complete many Git-related actions directly in the browser, including:

- Creating a repository
- Forking a repository
- Managing files
- Being social

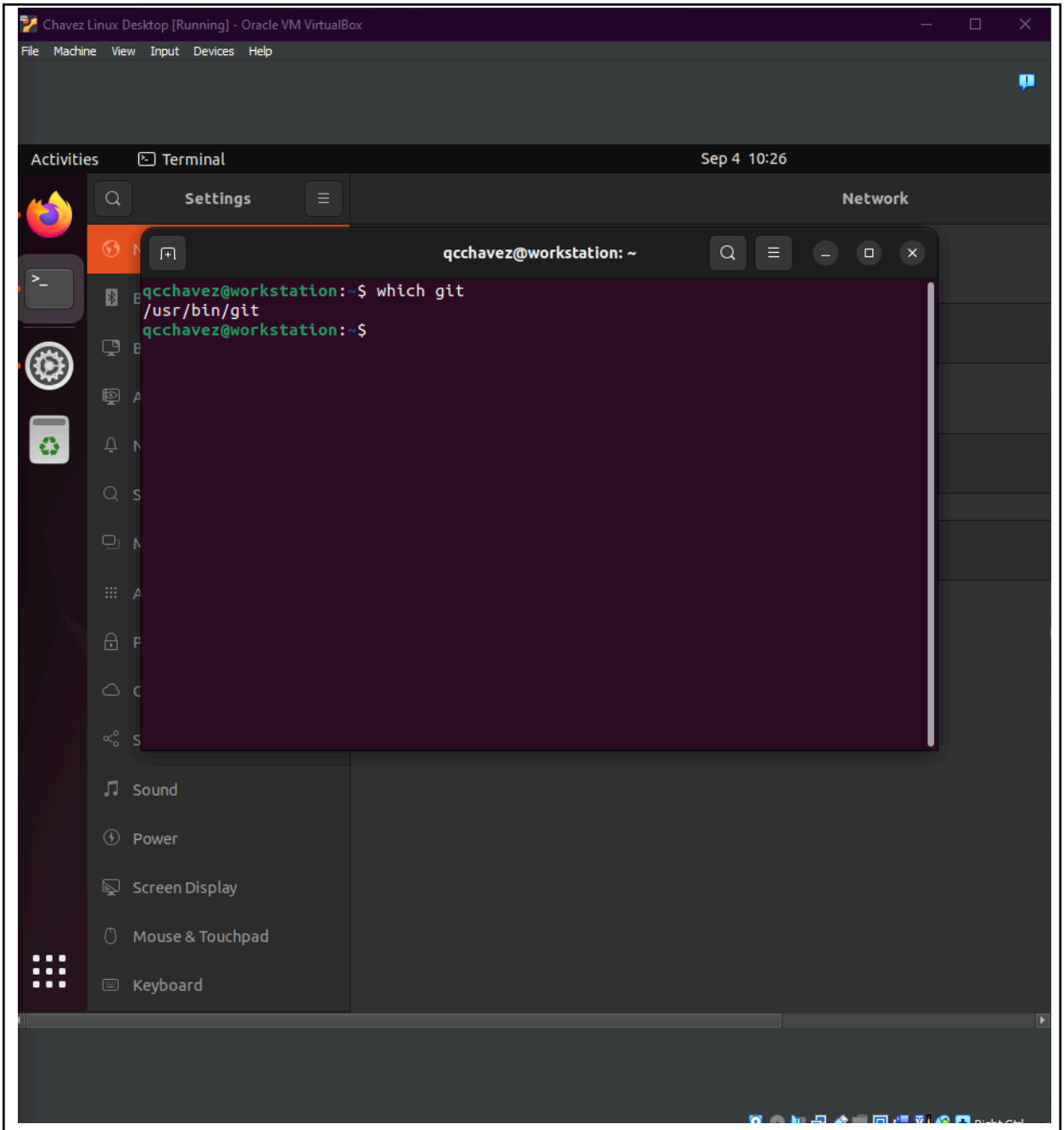
Task 3: Set up the Git Repository

1. On the local machine, verify the version of your git using the command *which git*. If a directory of git is displayed, then you don't need to install git. Otherwise, to install git, use the following command: *sudo apt install git*

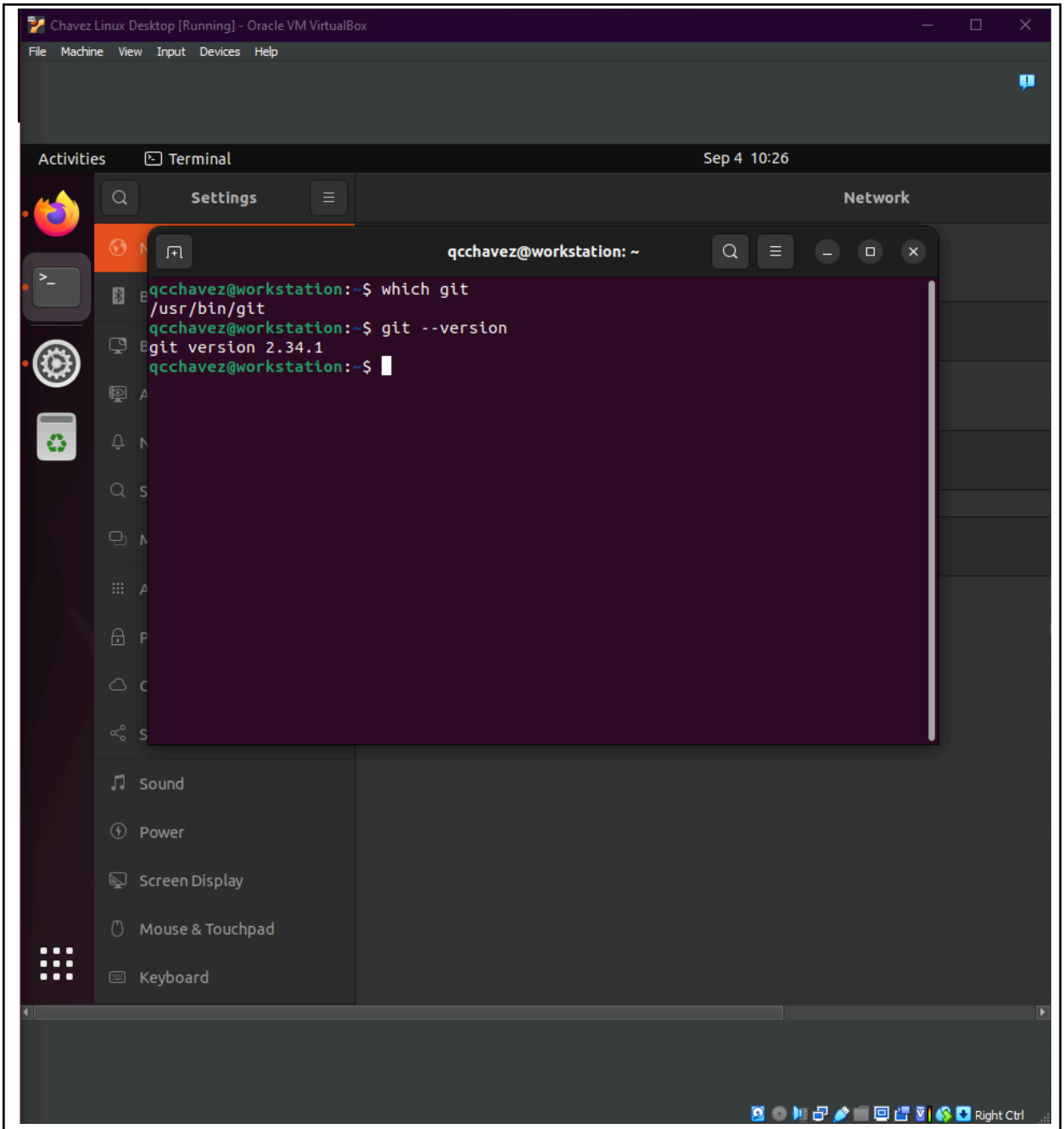

Chavez Linux Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Terminal
Sep 4 09:27
qcchavez@workstation: ~
qcchavez@workstation:~$ whichgit
whichgit: command not found
qcchavez@workstation:~$
Right Ctrl



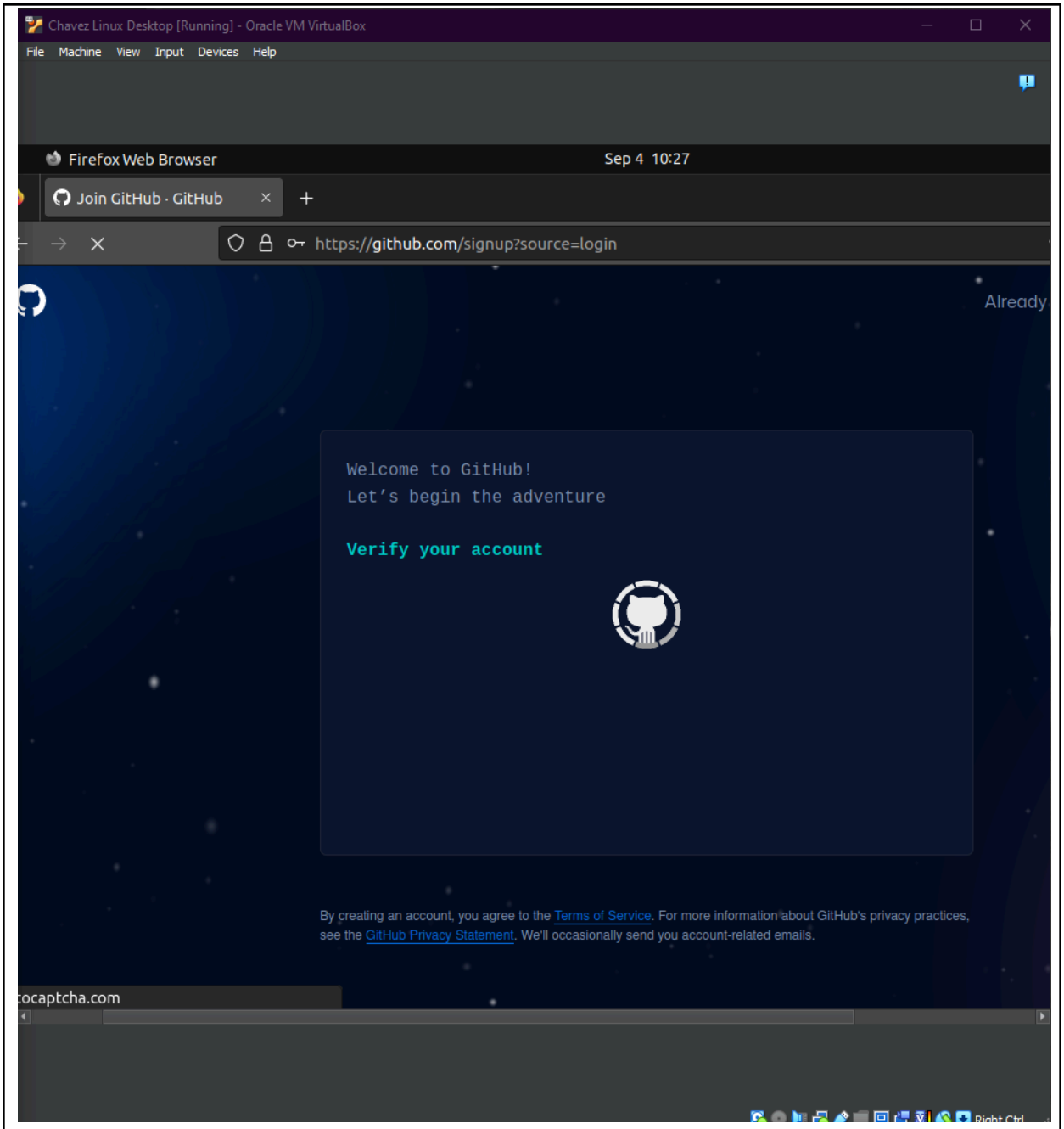
2. After the installation, issue the command *which git* again. The directory of git is usually installed in this location: *user/bin/git.*



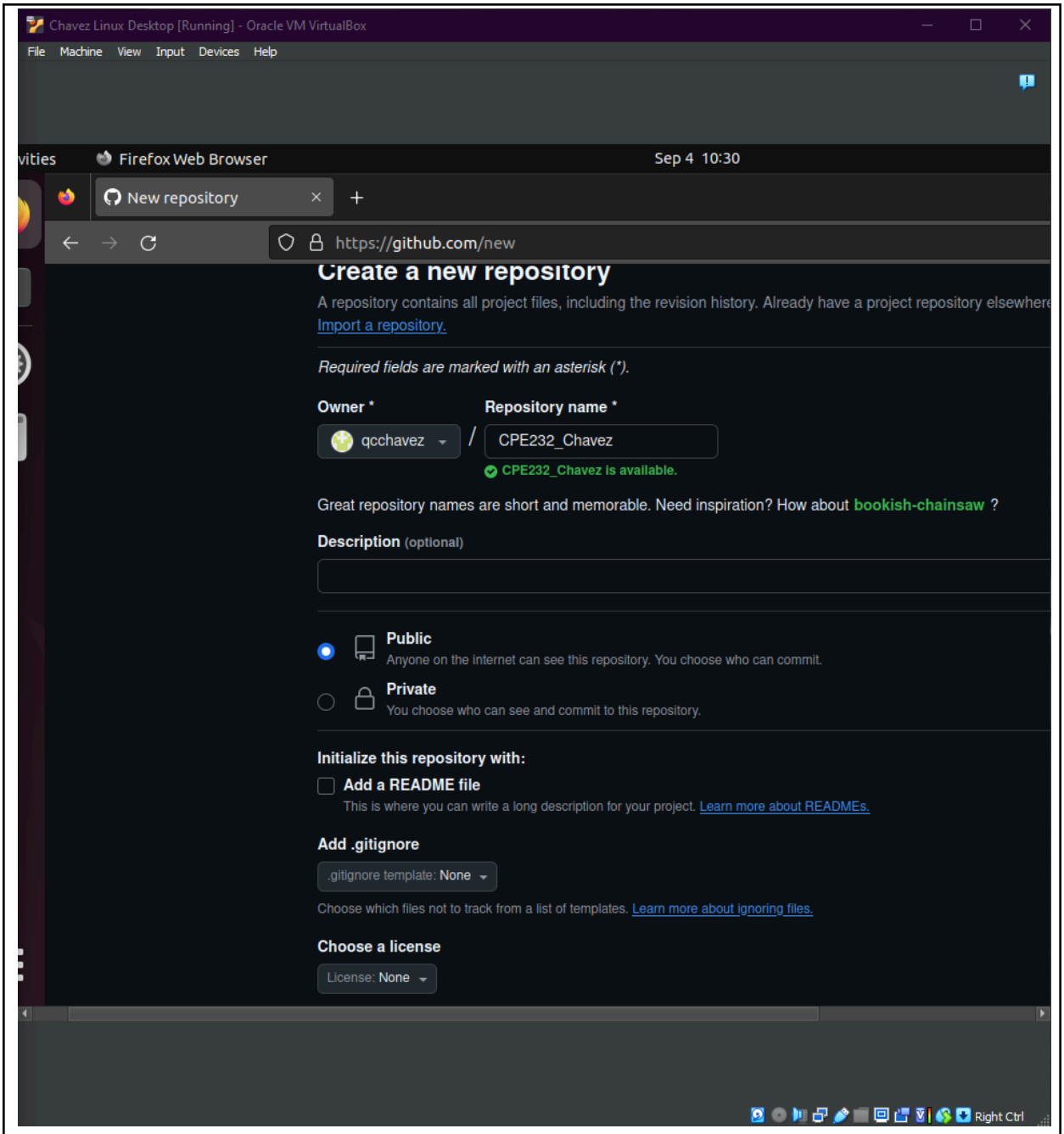
3. The version of git installed in your device is the latest. Try issuing the command *git --version* to know the version installed.



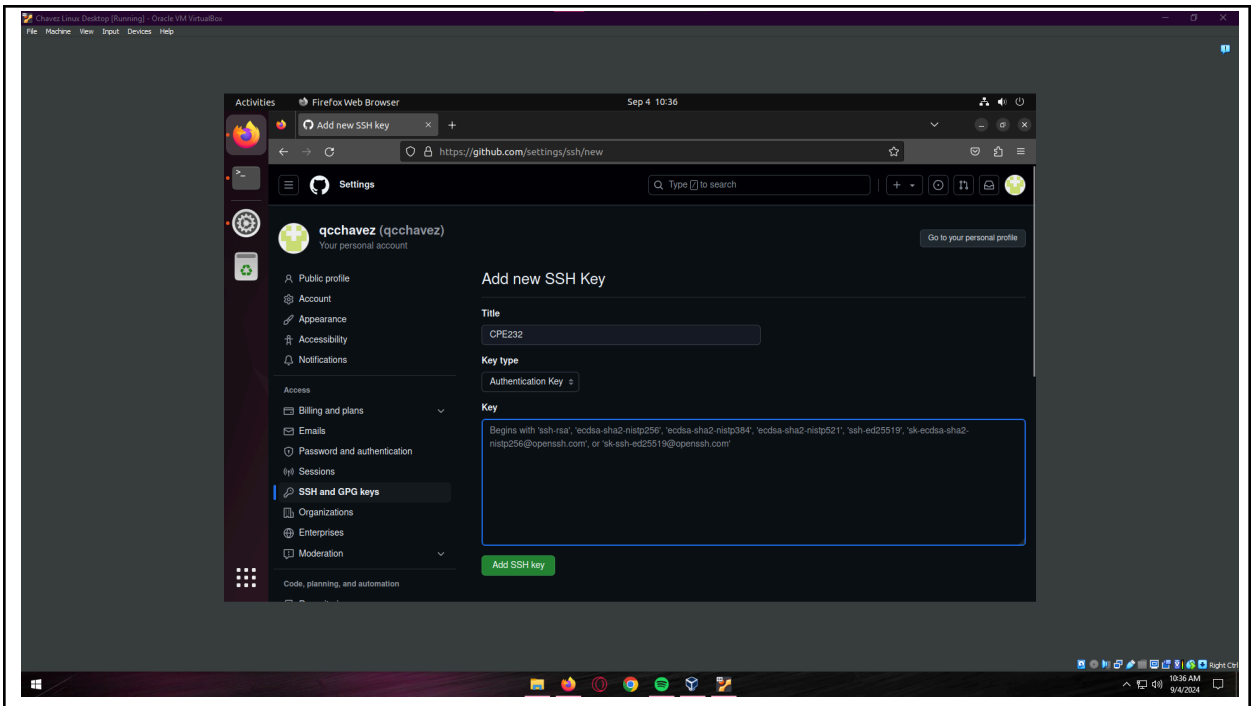
4. Using the browser in the local machine, go to www.github.com.
5. Sign up in case you don't have an account yet. Otherwise, login to your GitHub account.



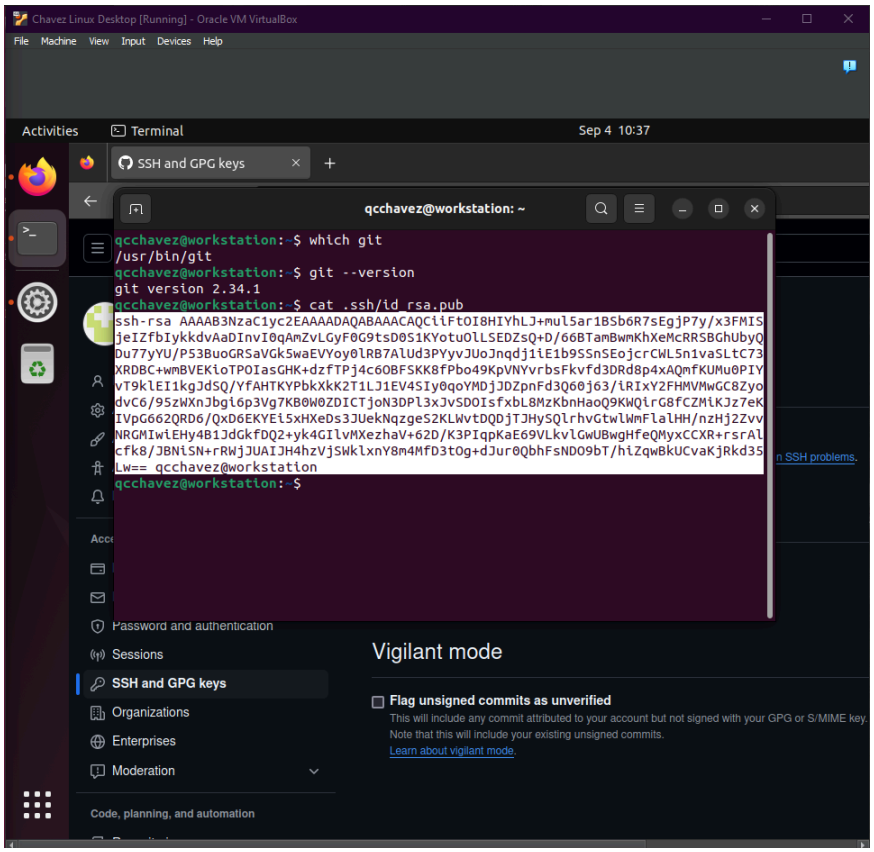
a. Create a new repository and name it as CPE232_yourname. Check Add a README file and click Create repository.

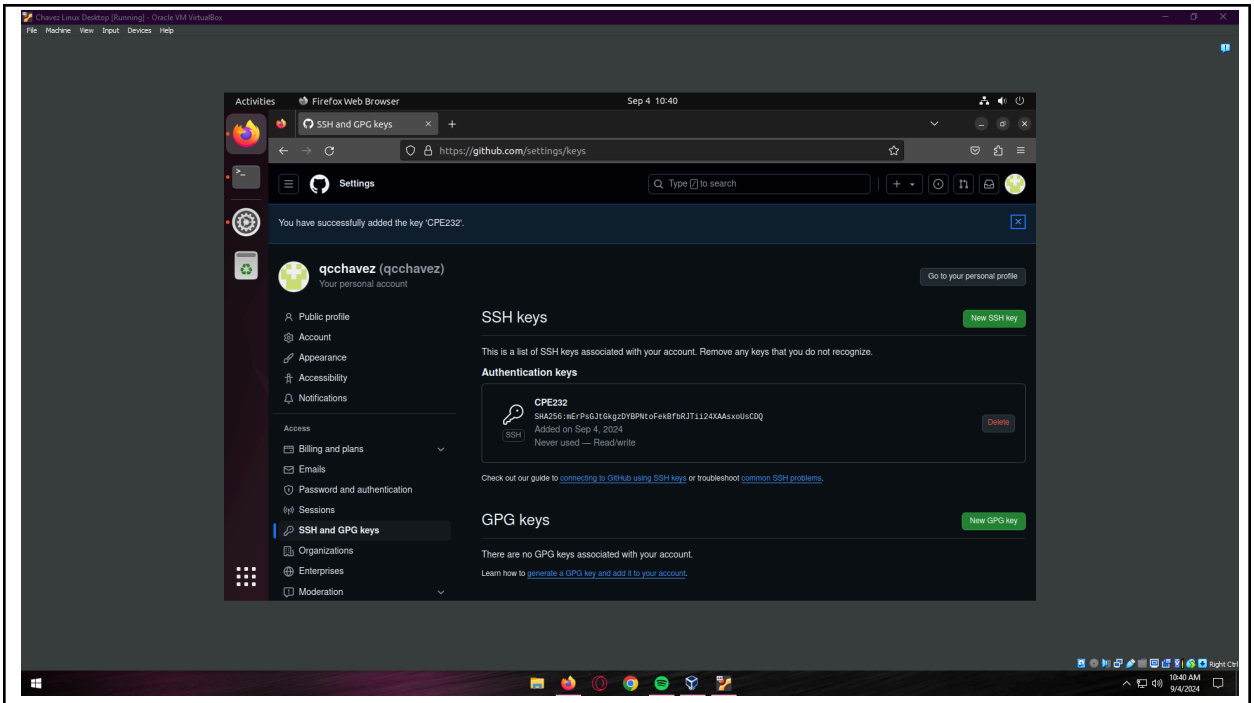


b. Create a new SSH key on GitHub. Go your profile's setting and click SSH and GPG keys. If there is an existing key, make sure to delete it. To create a new SSH keys, click New SSH Key. Write CPE232 key as the title of the key.

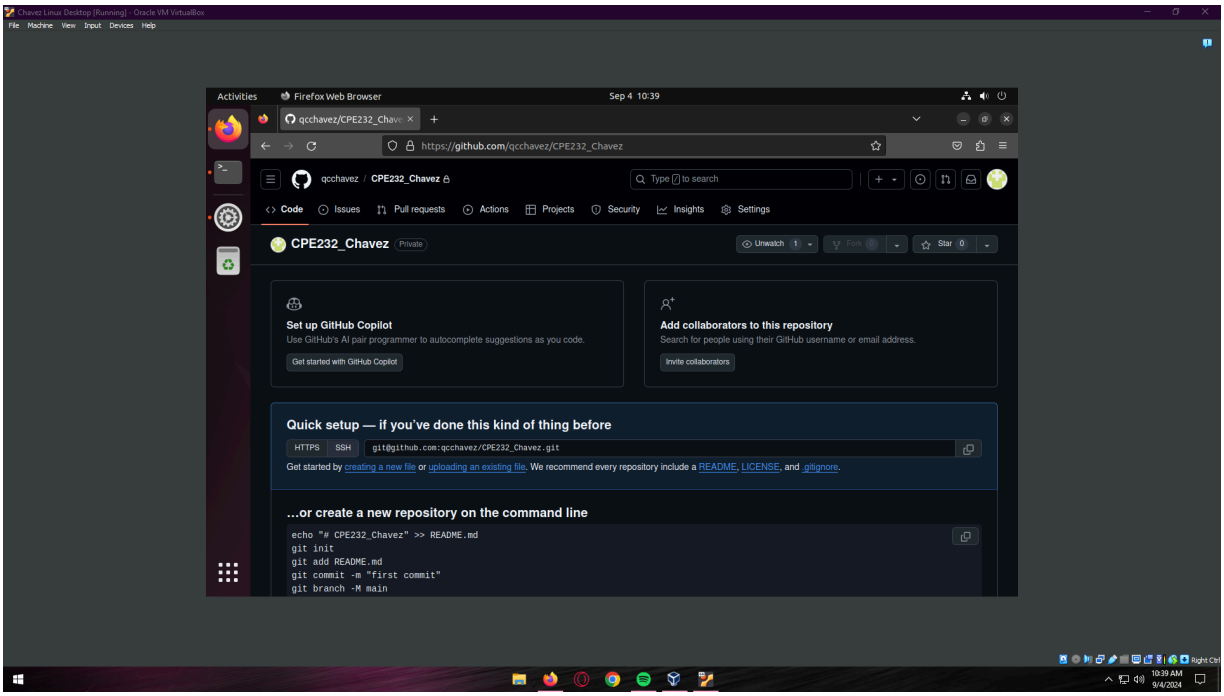


c. On the local machine's terminal, issue the command cat .ssh/id_rsa.pub and copy the public key. Paste it on the GitHub key and press Add SSH key.

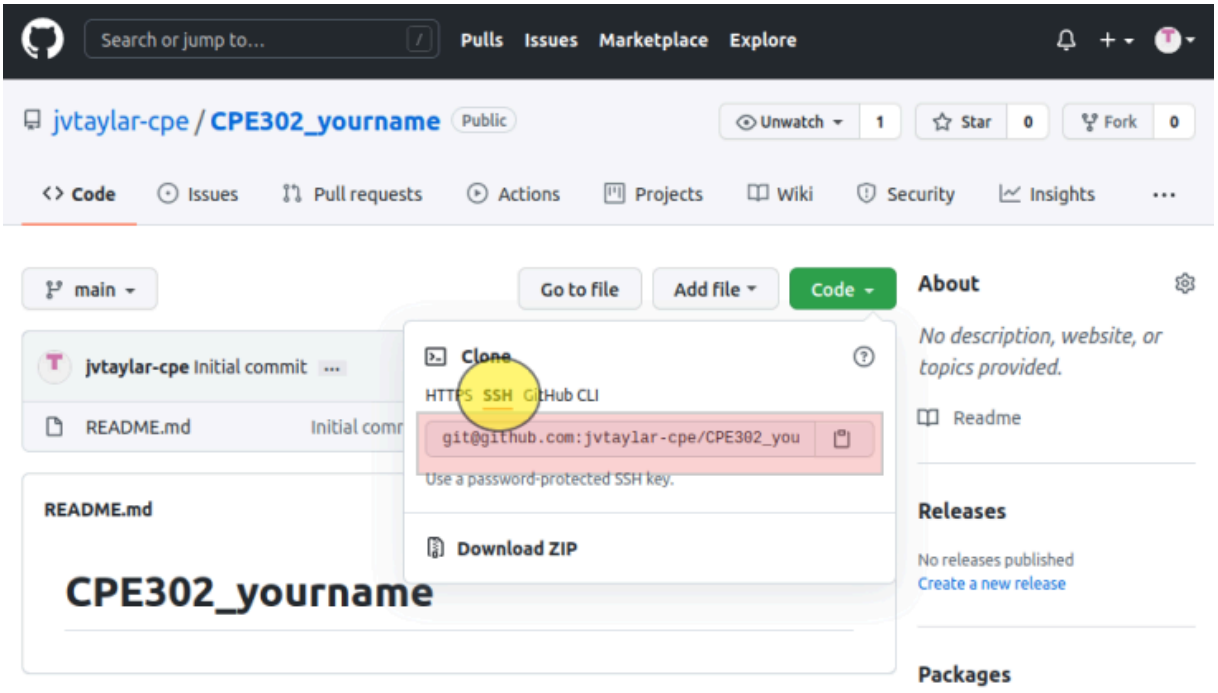




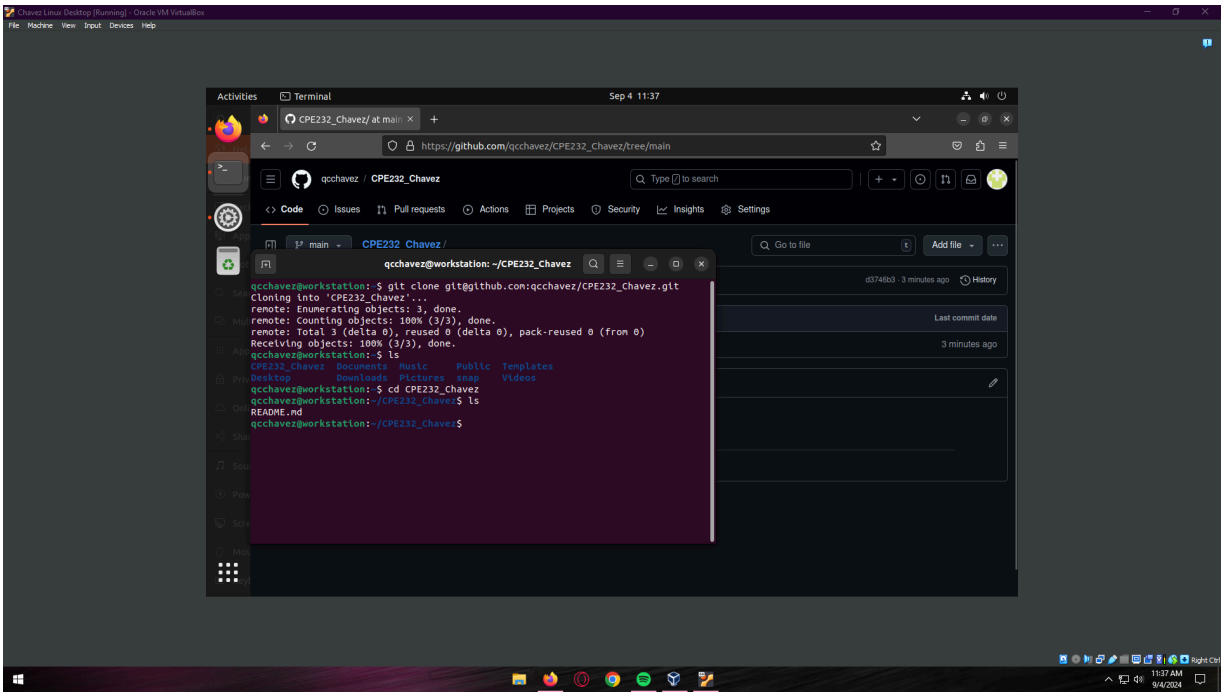
d. Clone the repository that you created. In doing this, you need to get the link from GitHub. Browse to your repository as shown below. Click on the Code drop down menu. Select SSH and copy the link.



Example:

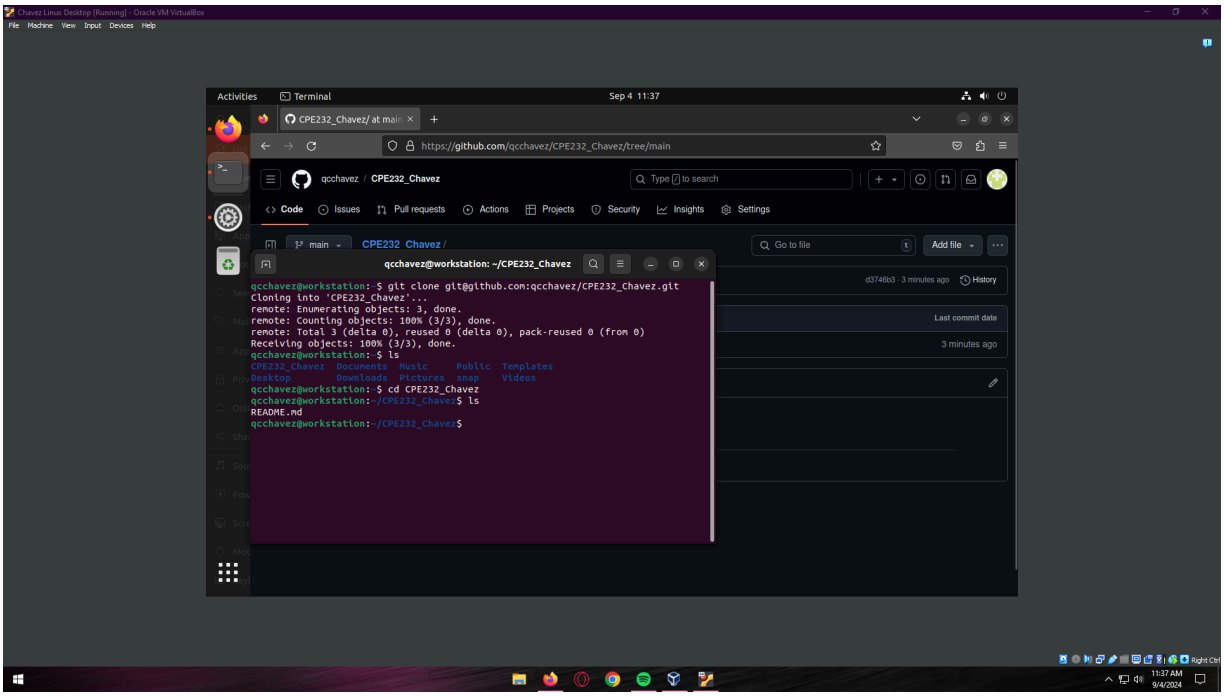


e. Issue the command git clone followed by the copied link. For example, *git clone git@github.com:jvtaylar-cpe/CPE232_yourname.git*. When prompted to continue connecting, type yes and press enter.

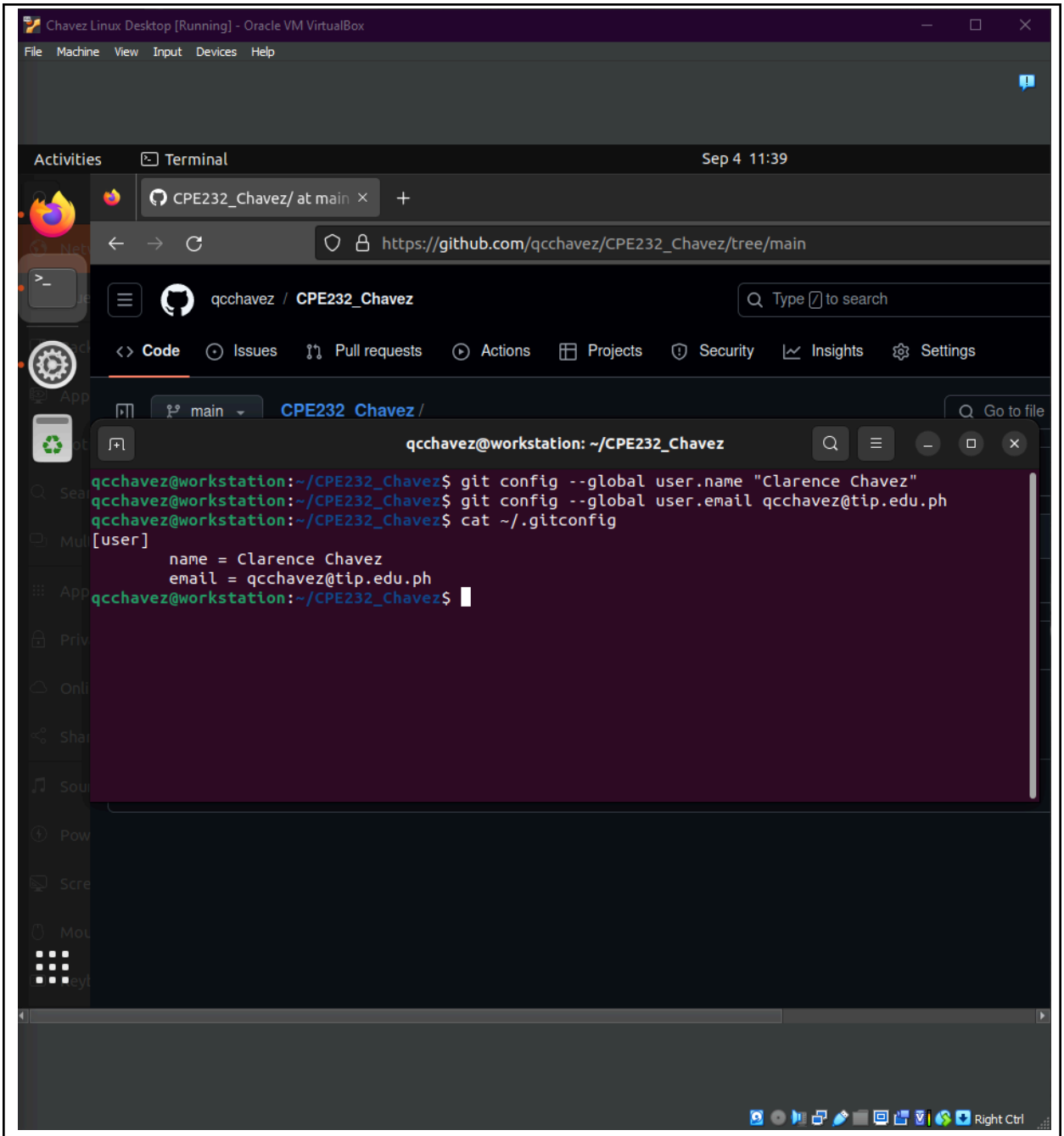


f. To verify that you have cloned the GitHub repository, issue the command *ls*. Observe that you have the CPE232_yourname in the list of

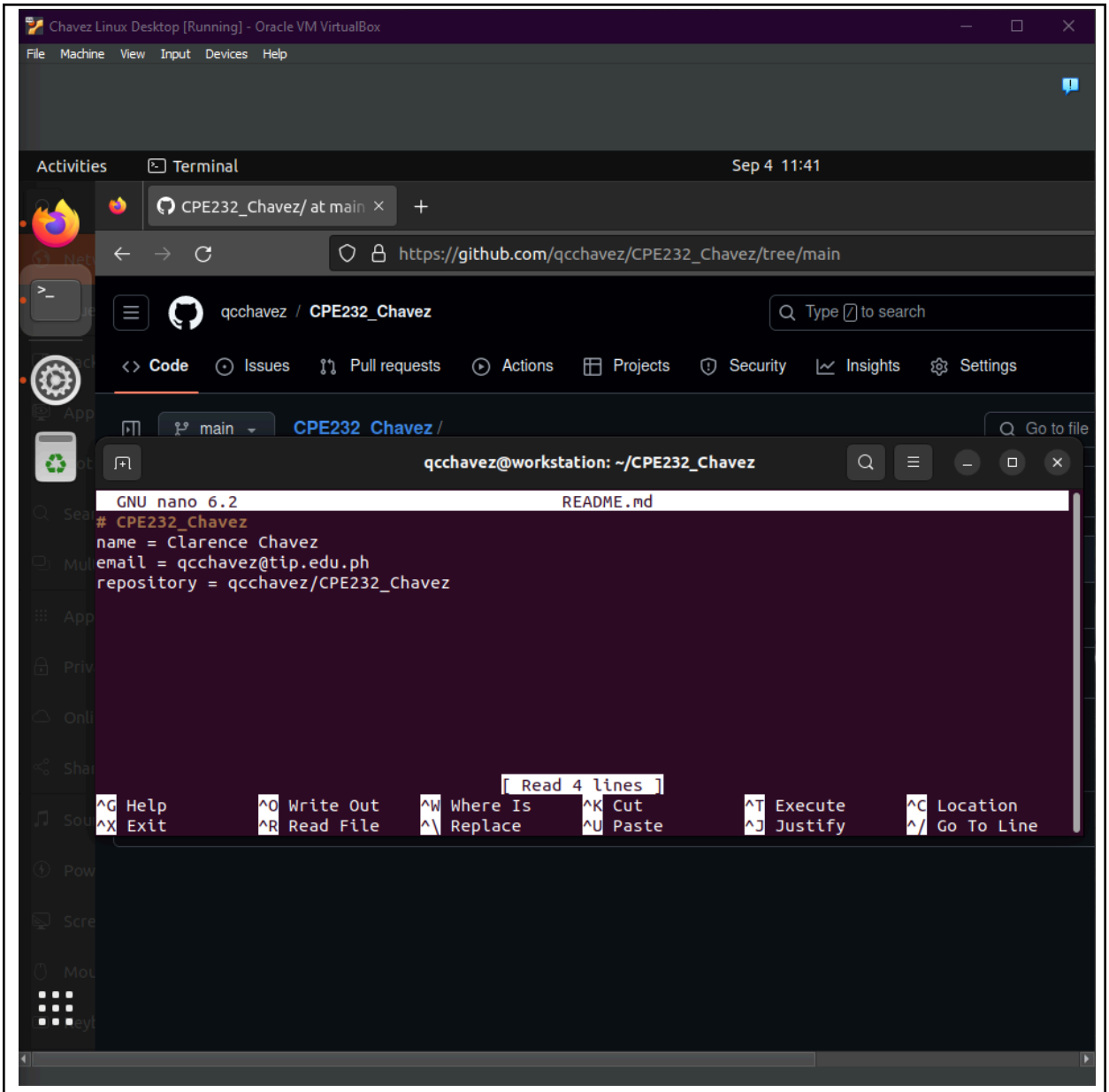
your directories. Use CD command to go to that directory and LS command to see the file README.md.



g. Use the following commands to personalize your git.
   - *git config --global user.name "Your Name"*
   - *git config --global user.email yourname@email.com*
   - Verify that you have personalized the config file using the command *cat ~/.gitconfig*

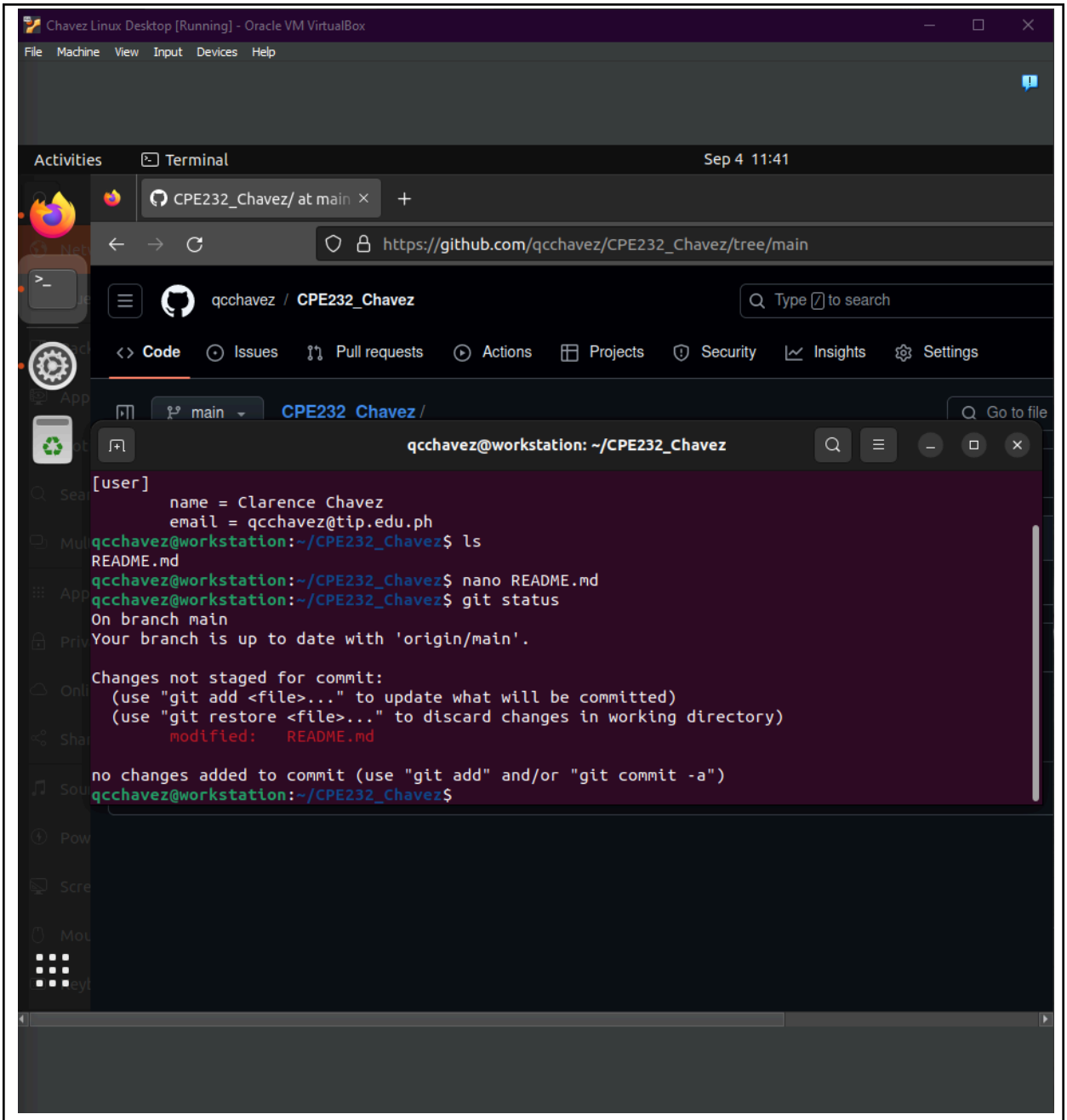


h. Edit the README.md file using nano command. Provide any information on the markdown file pertaining to the repository you created. Make sure to write out or save the file and exit.

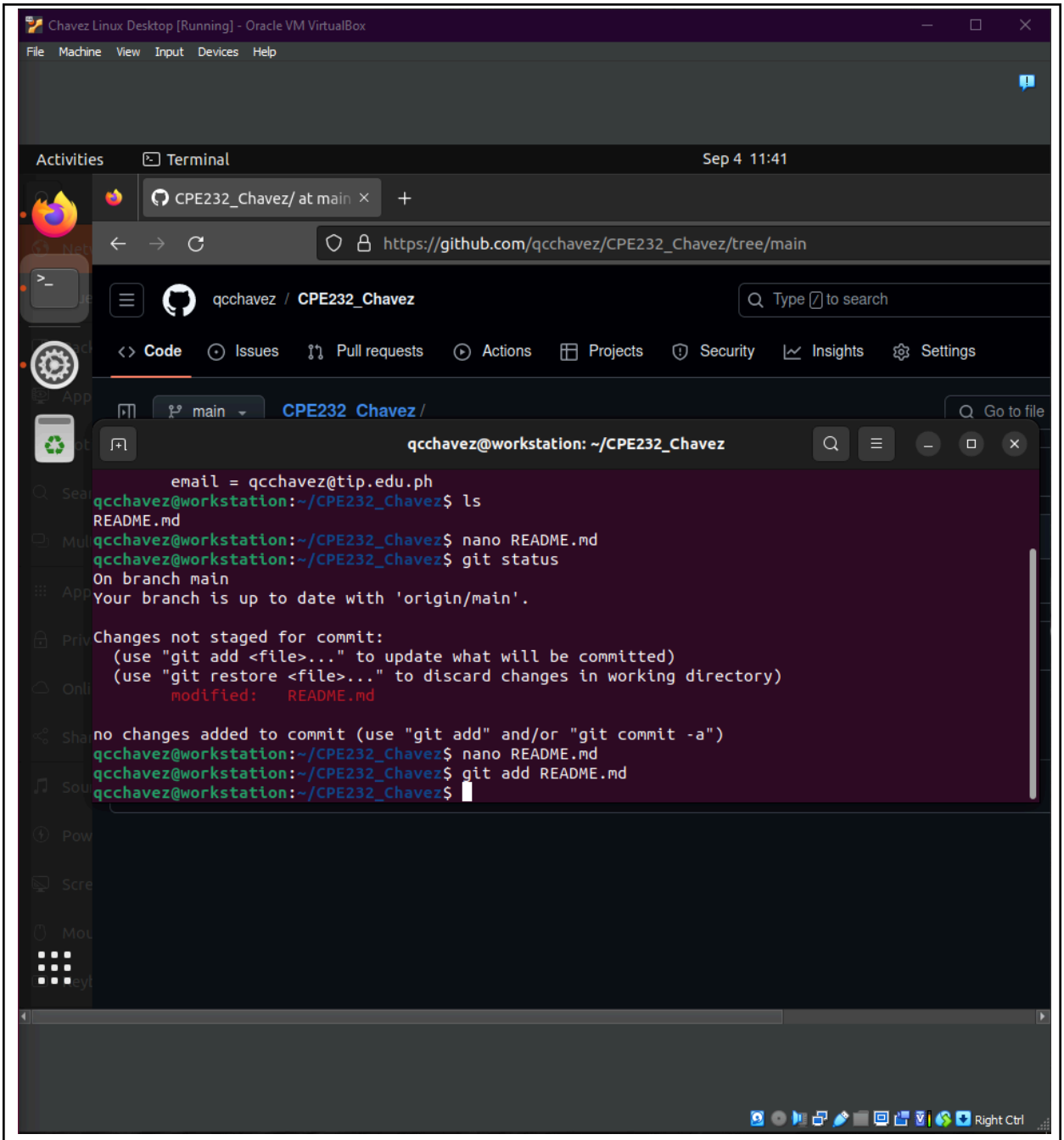


i. Use the *git status* command to display the state of the working directory and the staging area. This command shows which changes have been staged, which haven't, and which files aren't being tracked by Git. Status output does not show any information regarding the committed project history. What is the result of issuing this command?

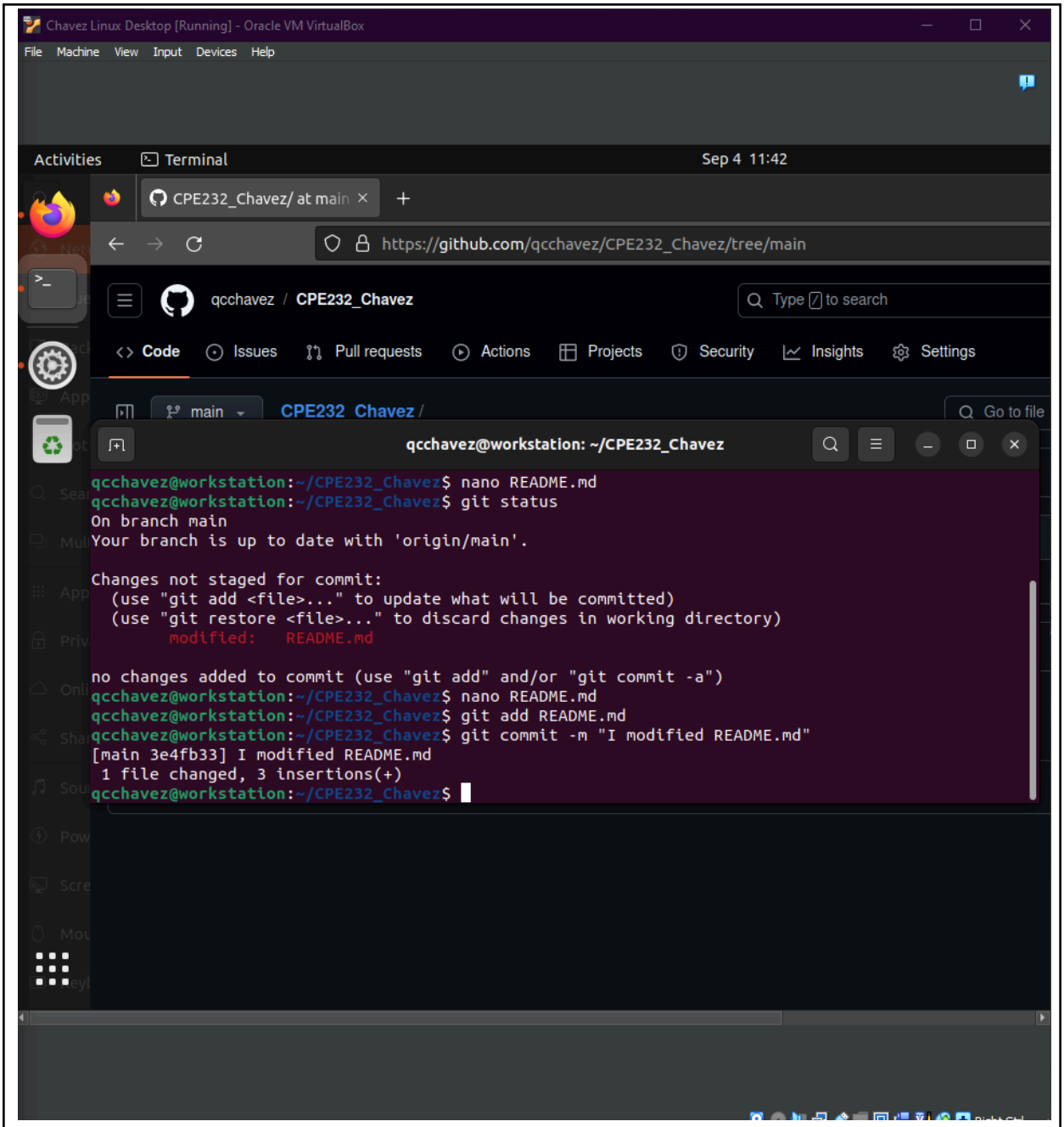
- By issuing this command, it says that the changes were not yet made to the commit. It also specifies the file that was modified which is the **README.md**



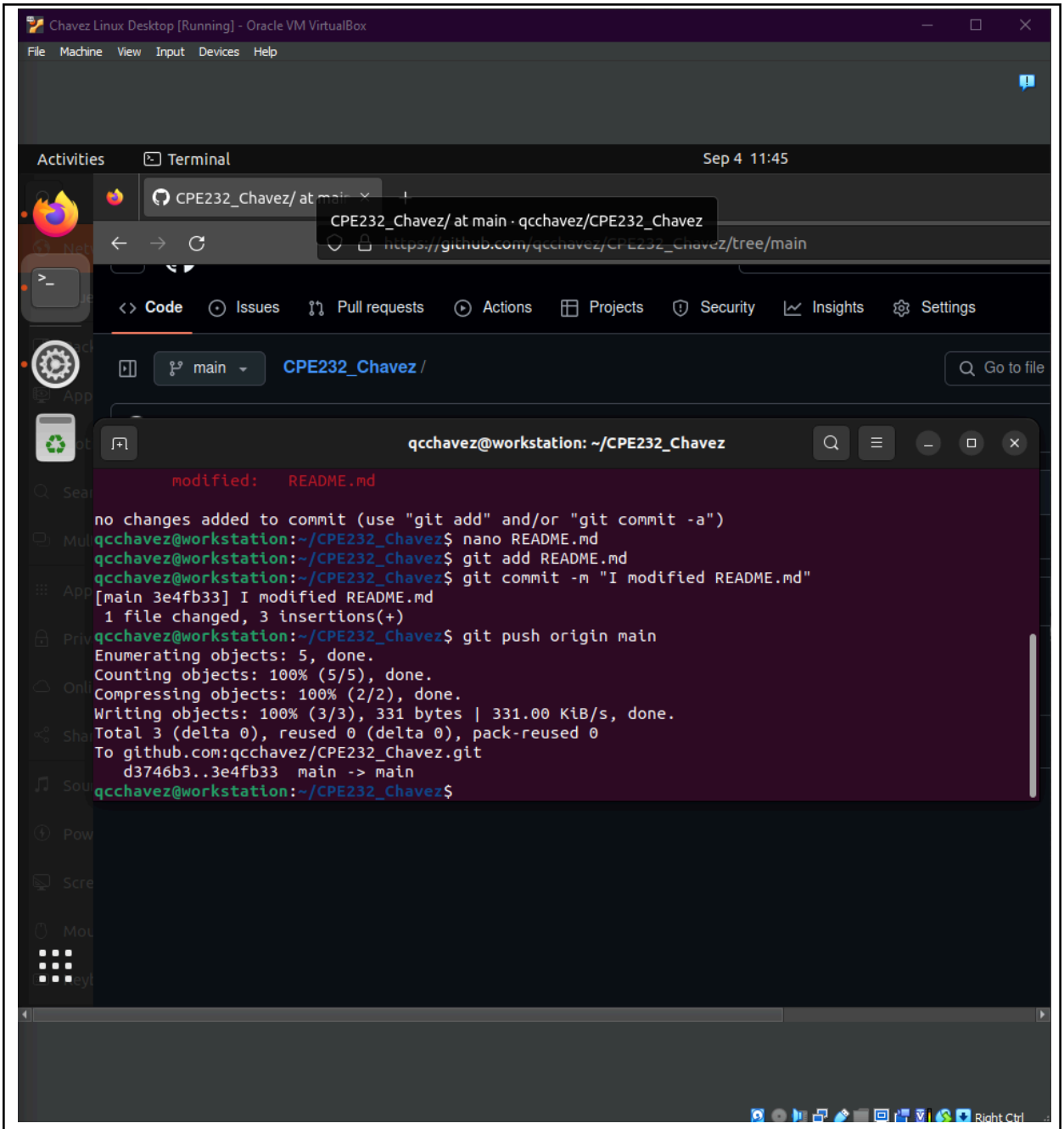
j. Use the command *git add README.md* to add the file into the staging area.



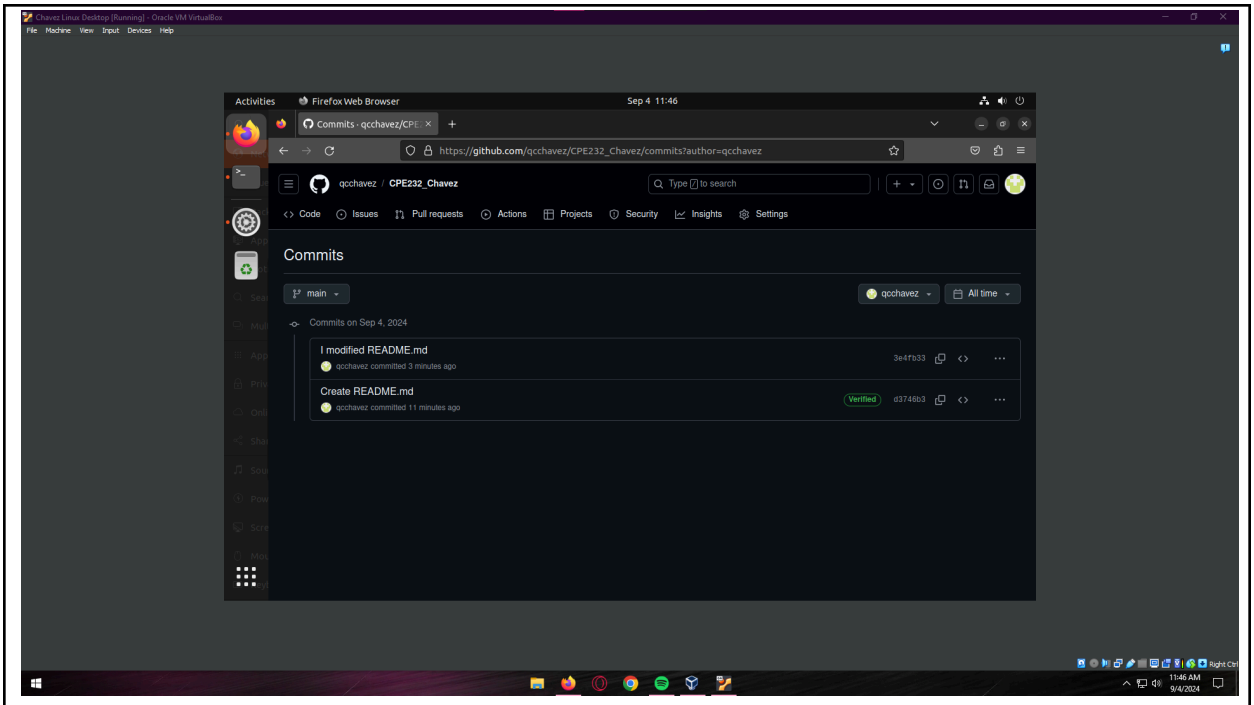
k. Use the *git commit -m "your message"* to create a snapshot of the staged changes along the timeline of the Git projects history. The use of this command is required to select the changes that will be staged for the next commit.

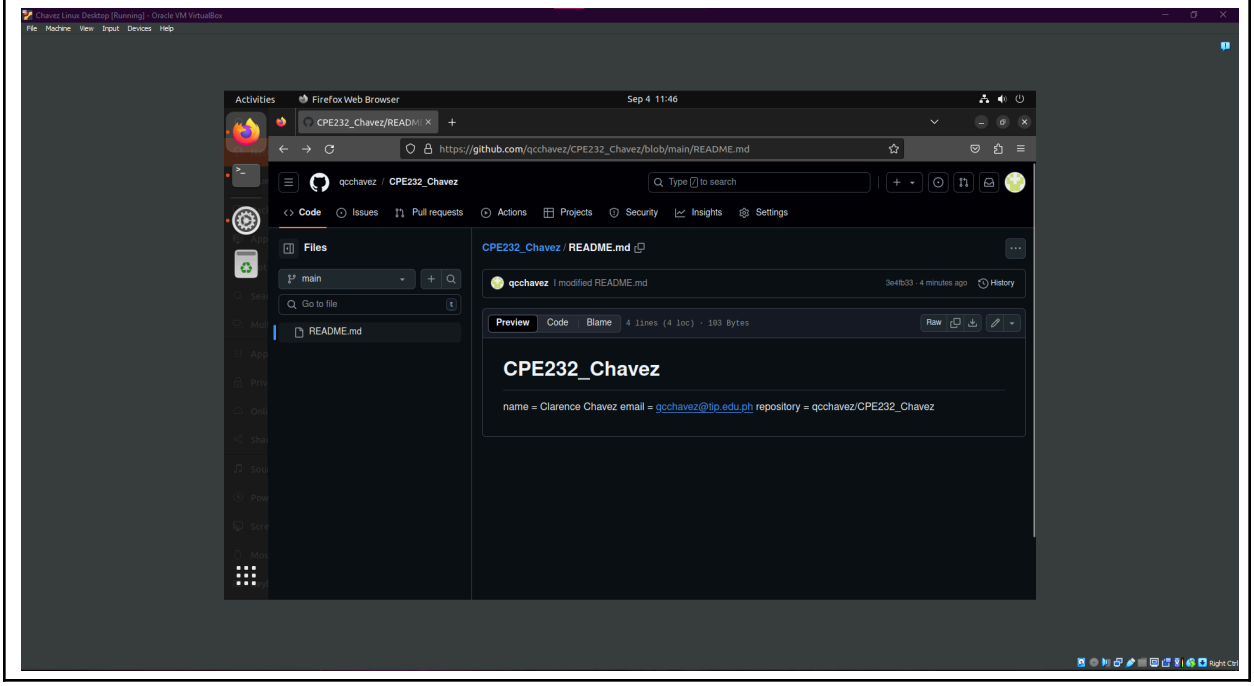


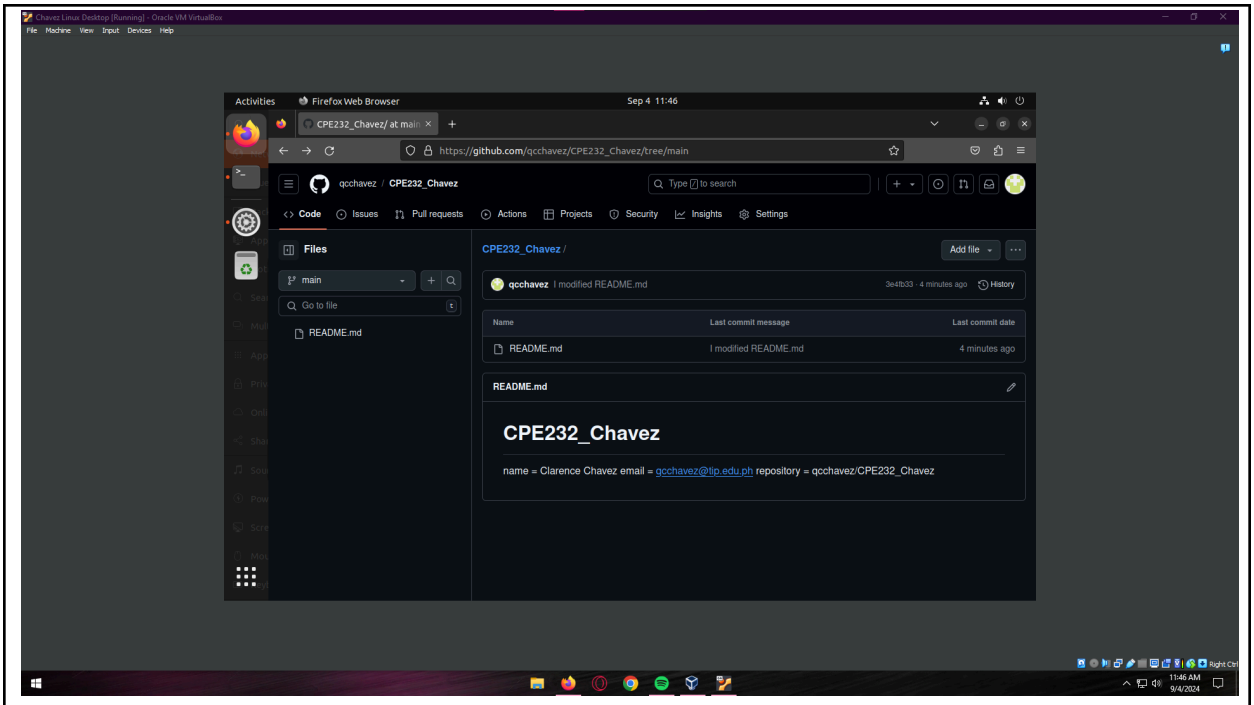
l. Use the command *git push <remote><branch>* to upload the local repository content to GitHub repository. Pushing means to transfer commits from the local repository to the remote repository. As an example, you may issue *git push origin main.*



m. On the GitHub repository, verify that the changes have been made to README.md by refreshing the page. Describe the README.md file. You can notice the how long was the last commit. It should be some minutes ago and the message you typed on the git commit command should be there. Also, the README.md file should have been edited according to the text you wrote.


Activities
Firefox Web Browser
Sep 4 11:46
https://github.com/qcchavez/CPE232_Chavez/commits?author=qcchavez
qcchavez / CPE232_Chavez
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
Commits
main
qcchavez
All time
Commits on Sep 4, 2024
I modified README.md
qcchavez committed 3 minutes ago
3e4fb33
Create README.md
qcchavez committed 11 minutes ago
Verified
d3746b3
11:46 AM
9/4/2024


Activities
Firefox Web Browser
Sep 4 11:46
https://github.com/qcchavez/CPE232_Chavez/blob/main/README.md
qcchavez / CPE232_Chavez
Code
Issues
Pull requests
Actions
Projects
Security
Insights
Settings
Files
main
Go to file
README.md
CPE232_Chavez / README.md
qcchavez I modified README.md
3e4fb33 · 4 minutes ago
History
Preview
Code
Blame
4 lines (4 loc) · 103 Bytes
Raw
CPE232_Chavez
name = Clarence Chavez email = qcchavez@tip.edu.ph repository = qcchavez/CPE232_Chavez



Reflections:

Answer the following:

3. What sort of things have we so far done to the remote servers using ansible commands?
    - In this activity, using ansible commands, we have installed, configured, and used the git repository to transfer files from the github website to the linux and vice-versa. I also used the SSH by installing it, copying the key from the linux to github. I also ensured that the connection between the two is secured.

4. How important is the inventory file?
    - Inventory file is important because it is where you store your files whenever you make changes or modifications.

Conclusions/Learnings:

- In this activity, I have learned that GitHub is a very essential tool for tracking and making changes in a project. It allows you to transfer directly from Ubuntu Desktop to the GitHub repository, and vice-versa. Using also SSH for secure connection between clients and servers is also useful because it requires several authentication like username and passwords, depending on the administrator's preferences.