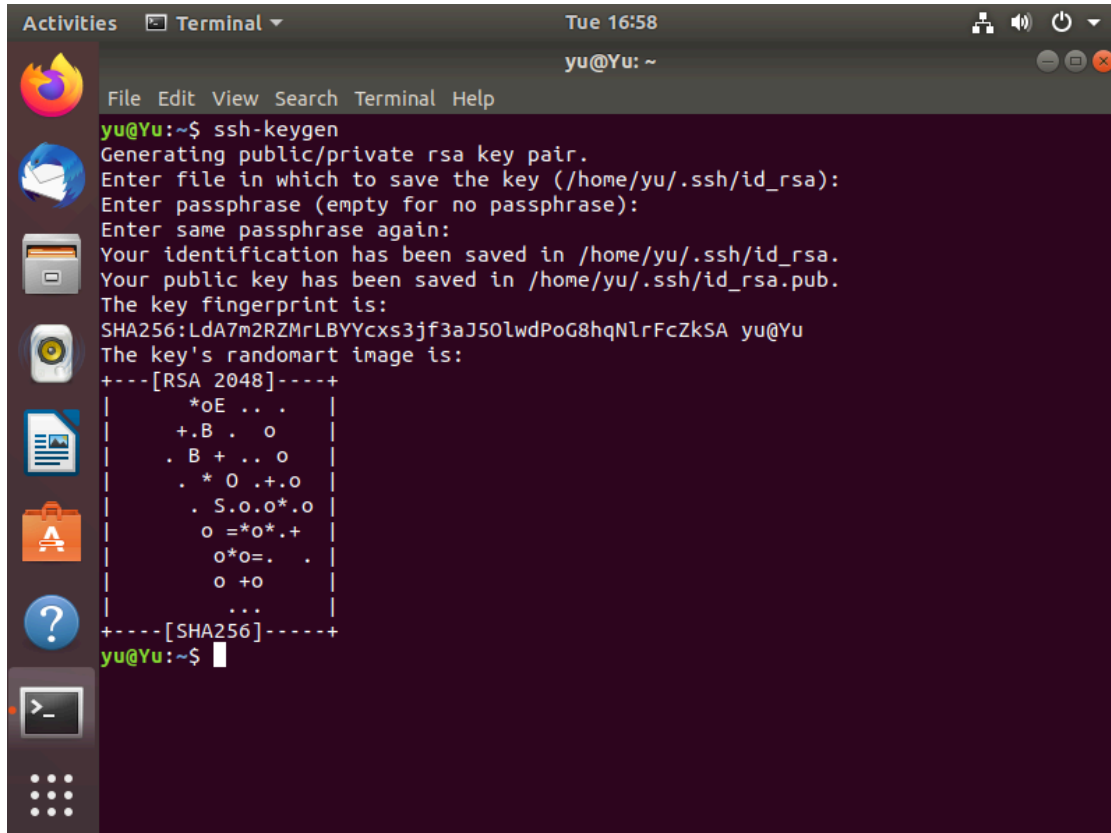


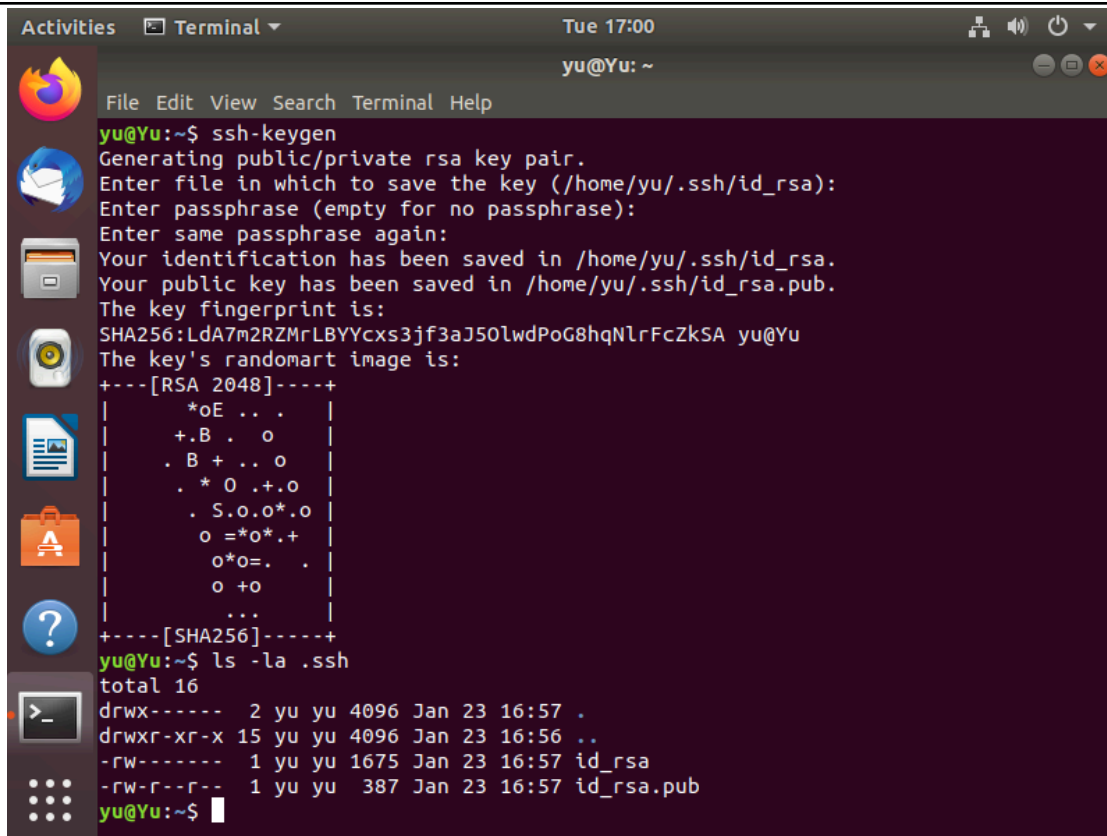
Name: Kenn Cherwin C. Yu	Date Performed: Jan 23, 2024
Course/Section: BSCPE - CPE31S1	Date Submitted: Jan 23, 2024
Instructor: Dr. Jonathan Taylar	Semester and SY: 2nd Sem 3rd Year
Activity 2: SSH Key-Based Authentication and Setting up Git	
1. Objectives: 1.1 Configure remote and local machine to connect 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). <i>Provide screenshots for each task.</i> 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 <i>ssh-keygen</i> 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`.



```
Activities Terminal Tue 16:58
yu@Yu: ~
File Edit View Search Terminal Help
yu@Yu:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/yu/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/yu/.ssh/id_rsa.
Your public key has been saved in /home/yu/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:LdA7m2RZMrLBYYcxS3jf3aJ50lwdPoG8hqNlrFcZkSA yu@Yu
The key's randomart image is:
+----[RSA 2048]-----+
|
|  *oE . . .
|+.B . . o
|. B + .. o
| . * O .+.o
| . S.o.o*.o
| o =*o*+.
| o*o=. .
| o +o
| . . .
+-----[SHA256]-----+
yu@Yu:~$
```

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`.



```
Activities Terminal Tue 17:00
yu@Yu: ~
File Edit View Search Terminal Help
yu@Yu:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/yu/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/yu/.ssh/id_rsa.
Your public key has been saved in /home/yu/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:LdA7m2RZMrLBYYCxs3jff3aJ50lwdPoG8hqNlrfCzKSA yu@Yu
The key's randomart image is:
+---[RSA 2048]-----+
|
|*oE .. .|
|+.B . o|
|. B + .. o|
|. * O .+.o|
|. S.o.o*.o|
|o =*o*.+|
|o*o=. .|
|o +o|
|...|
+-----[SHA256]-----+
yu@Yu:~$ ls -la .ssh
total 16
drwx----- 2 yu yu 4096 Jan 23 16:57 .
drwxr-xr-x 15 yu yu 4096 Jan 23 16:56 ..
-rw----- 1 yu yu 1675 Jan 23 16:57 id_rsa
-rw-r--r-- 1 yu yu 387 Jan 23 16:57 id_rsa.pub
yu@Yu:~$
```

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*
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.

```
Activities Terminal Tue 17:15
yu@Yu: ~
File Edit View Search Terminal Help
yu@Yu:~$ ssh-copy-id -i ~/.ssh/id_rsa Yu@192.168.56.111
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/yu/.ssh/id_rsa.pub"
^Z
[1]+  Stopped                  ssh-copy-id -i ~/.ssh/id_rsa Yu@192.168.56.111
yu@Yu:~$
```

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?

Reflections:

Answer the following:

1. How will you describe the ssh-program? What does it do?
 - **SSH is a secure network protocol enabling encrypted communication between two systems. The SSH program facilitates secure remote access, command execution, and file transfers over unsecured networks.**
2. How do you know that you already installed the public key to the remote servers?
sud
 - **Check the public key if it is installed on a remote server by attempting to connect using SSH. Successful login without entering a password indicates that your public key is already 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**).

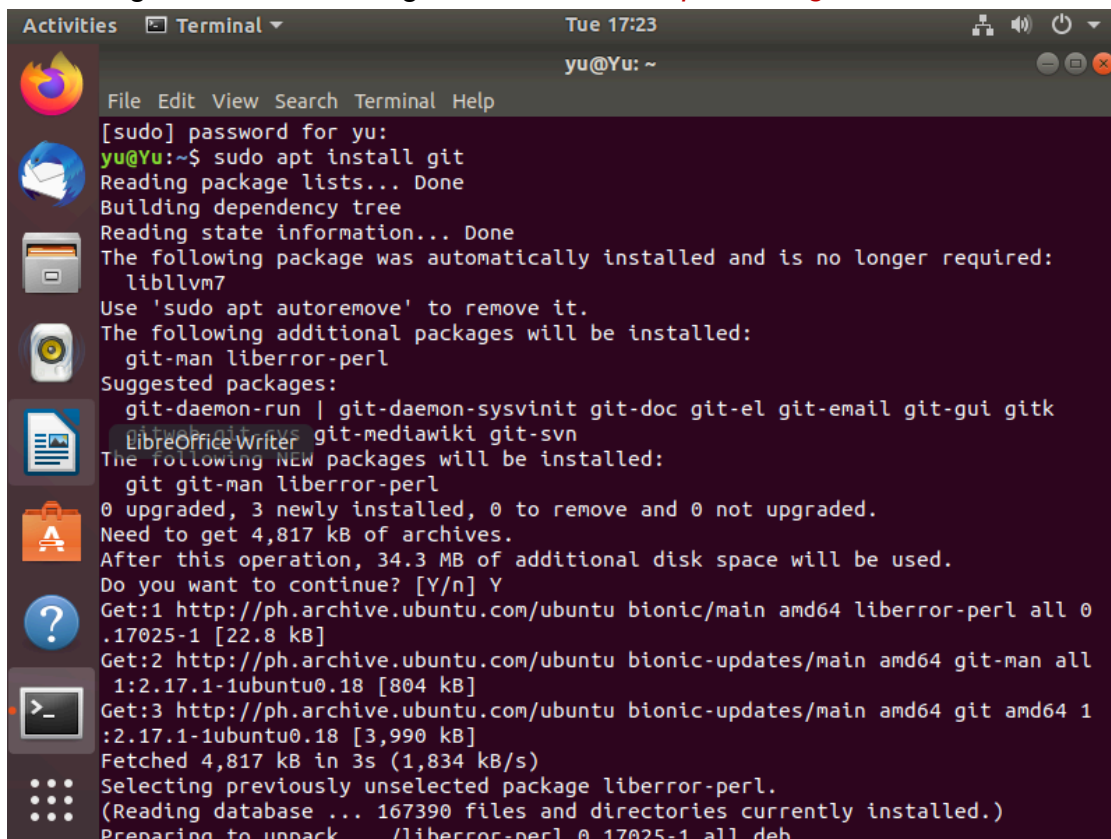
Set up Git

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*



```
Activities Terminal Tue 17:23
yu@Yu: ~
File Edit View Search Terminal Help
[sudo] password for yu:
yu@Yu:~$ sudo apt install git
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm7
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  git-man liberror-perl
Suggested packages:
  git-daemon-run | git-daemon-sysvinit git-doc git-el git-email git-gui gitk
  gitweb git-svn git-ldap-sso | git-auth-sudo git-crypt git-curl git-gnupg
  libssh2-1 git-mediawiki git-svn
The following NEW packages will be installed:
  git git-man liberror-perl
0 upgraded, 3 newly installed, 0 to remove and 0 not upgraded.
Need to get 4,817 kB of archives.
After this operation, 34.3 MB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://ph.archive.ubuntu.com/ubuntu bionic/main amd64 liberror-perl all 0
.17025-1 [22.8 kB]
Get:2 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 git-man all
1:2.17.1-1ubuntu0.18 [804 kB]
Get:3 http://ph.archive.ubuntu.com/ubuntu bionic-updates/main amd64 git amd64 1
:2.17.1-1ubuntu0.18 [3,990 kB]
Fetched 4,817 kB in 3s (1,834 kB/s)
Selecting previously unselected package liberror-perl.
(Reading database ... 167390 files and directories currently installed.)
Preparing to unpack .../liberror-perl_0.17025-1_all.deb ...
```

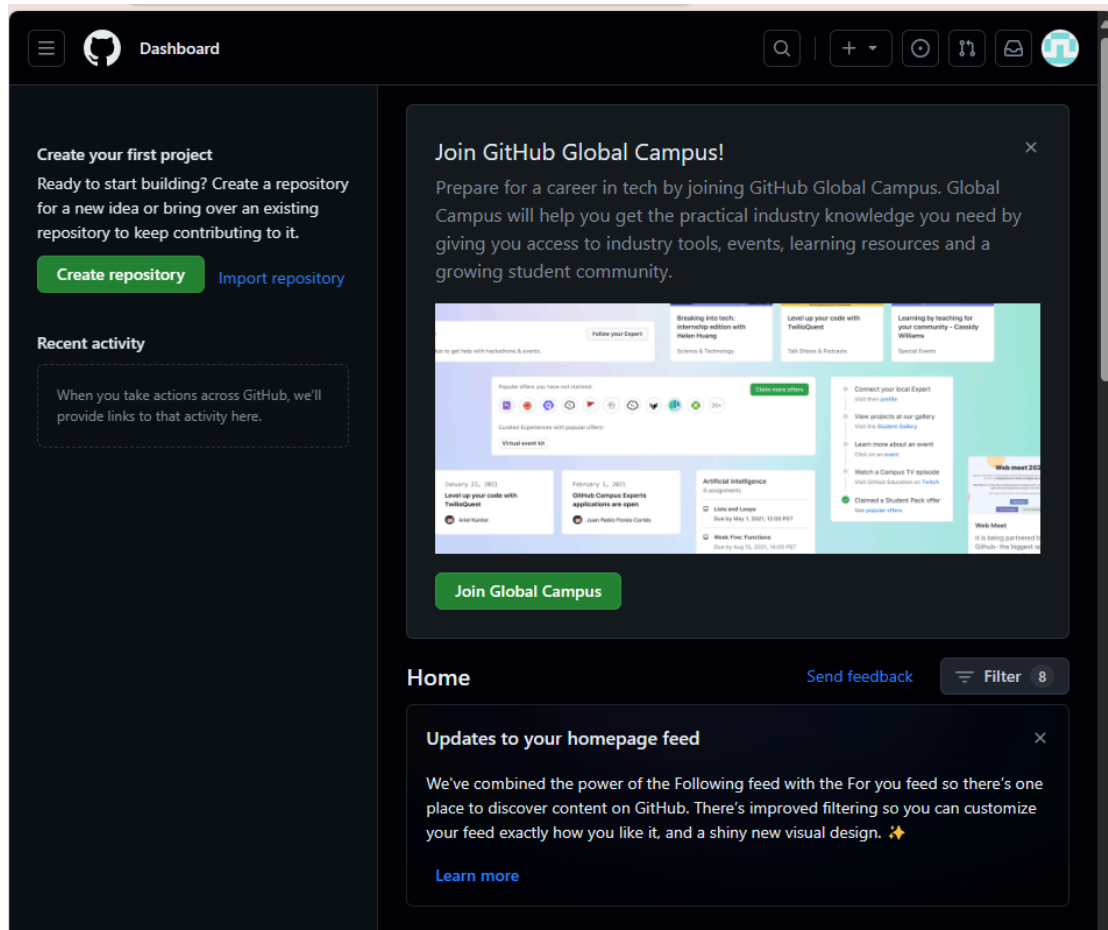
2. After the installation, issue the command *which git* again. The directory of git is usually installed in this location: *user/bin/git*.

```
yu@Yu:~$ which git
/usr/bin/git
yu@Yu:~$
```

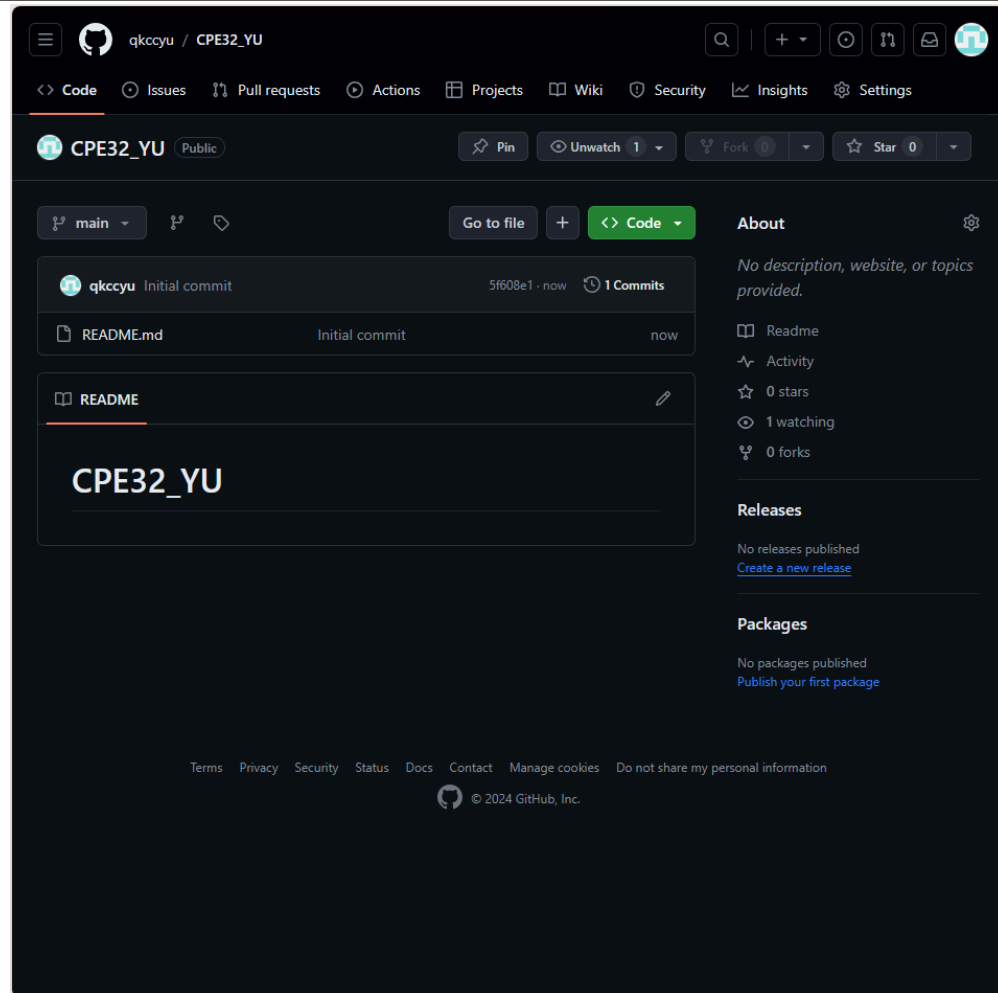
3. The version of git installed in your device is the latest. Try issuing the command `git --version` to know the version installed.

```
yu@Yu:~$ git --version
git version 2.17.1
yu@Yu:~$
```

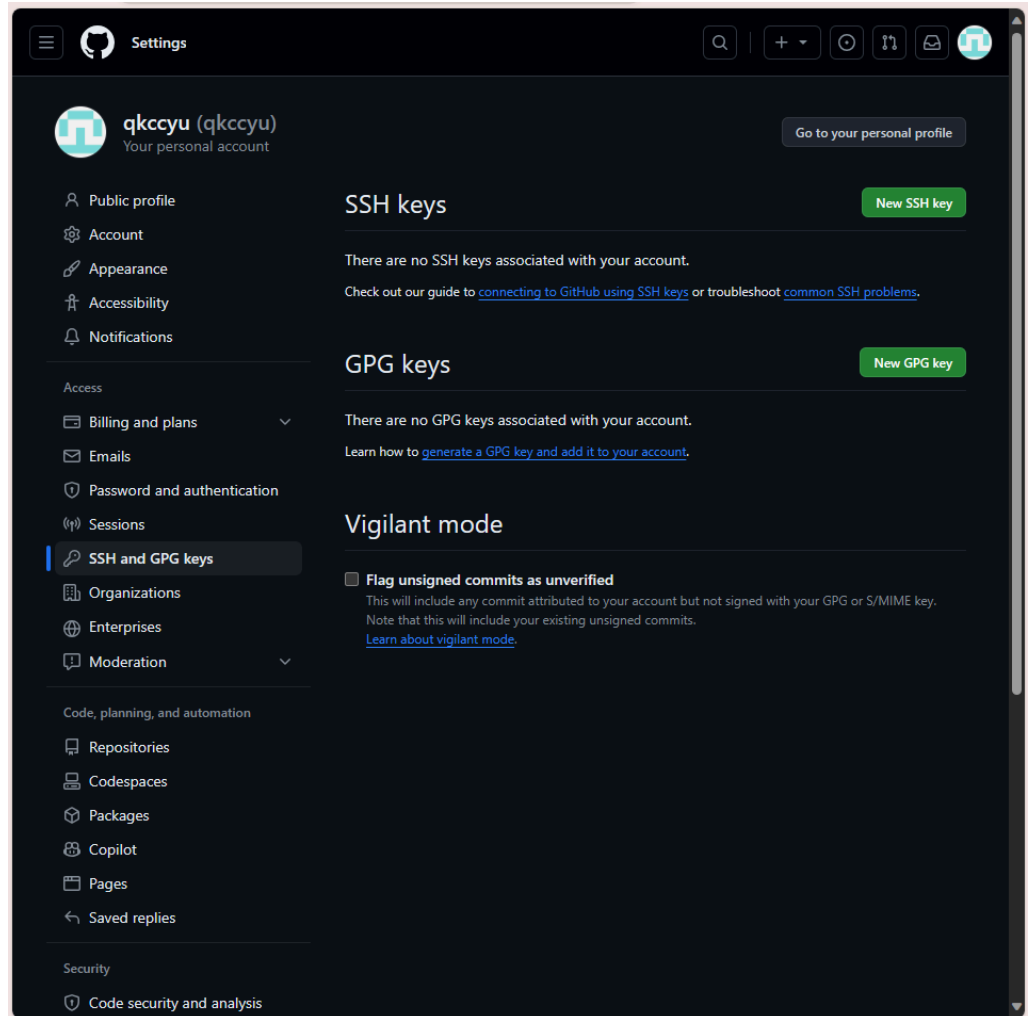
4. Using the browser in the local machine, go to www.github.com.



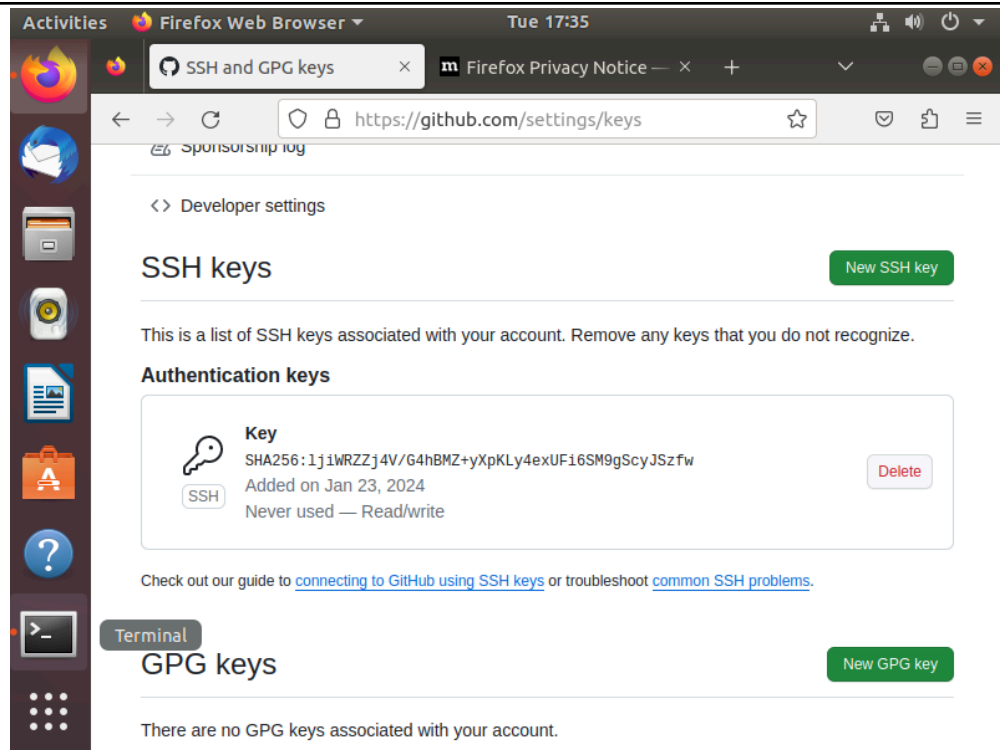
5. Sign up in case you don't have an account yet. Otherwise, login to your GitHub account.
- Create a new repository and name it as CPE232_yourname. Check Add a README file and click Create repository.



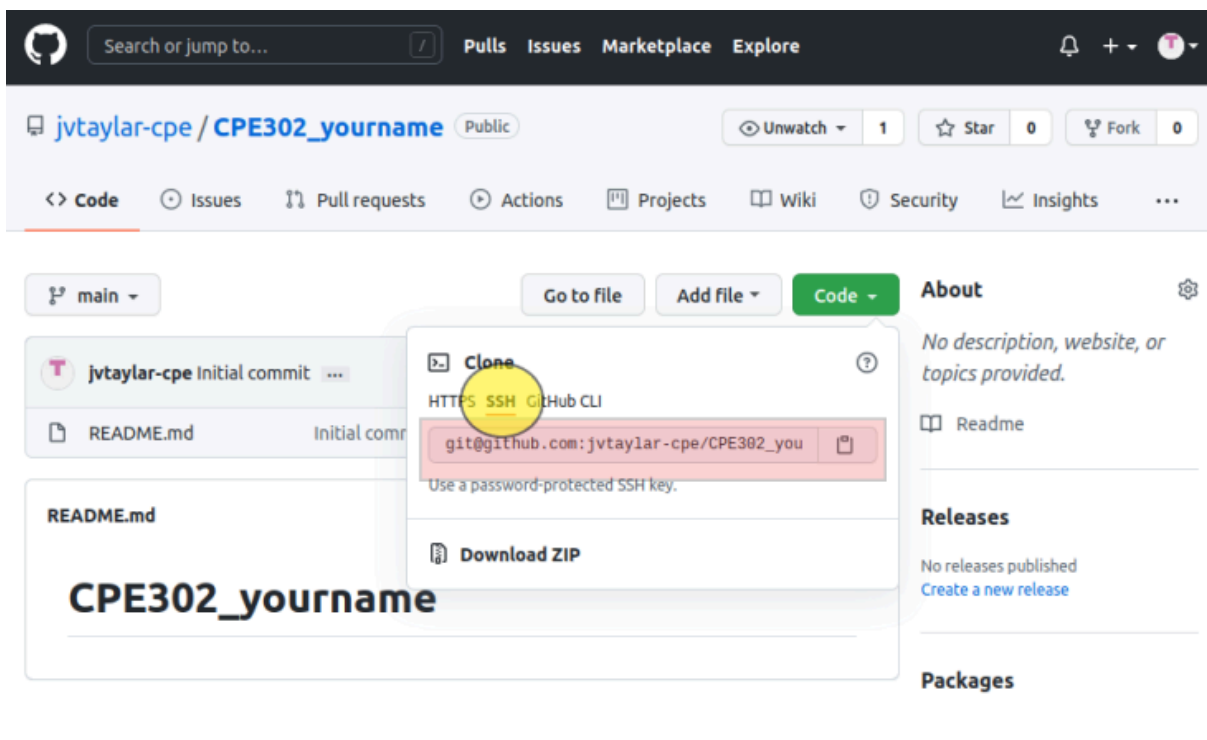
- b. Create a new SSH key on GitHub. Go your profile's setting and click SSH and GPG keys. If there is an existing key, make sure to delete it. To create a new SSH keys, click New SSH Key. Write CPE232 key as the title of the key.



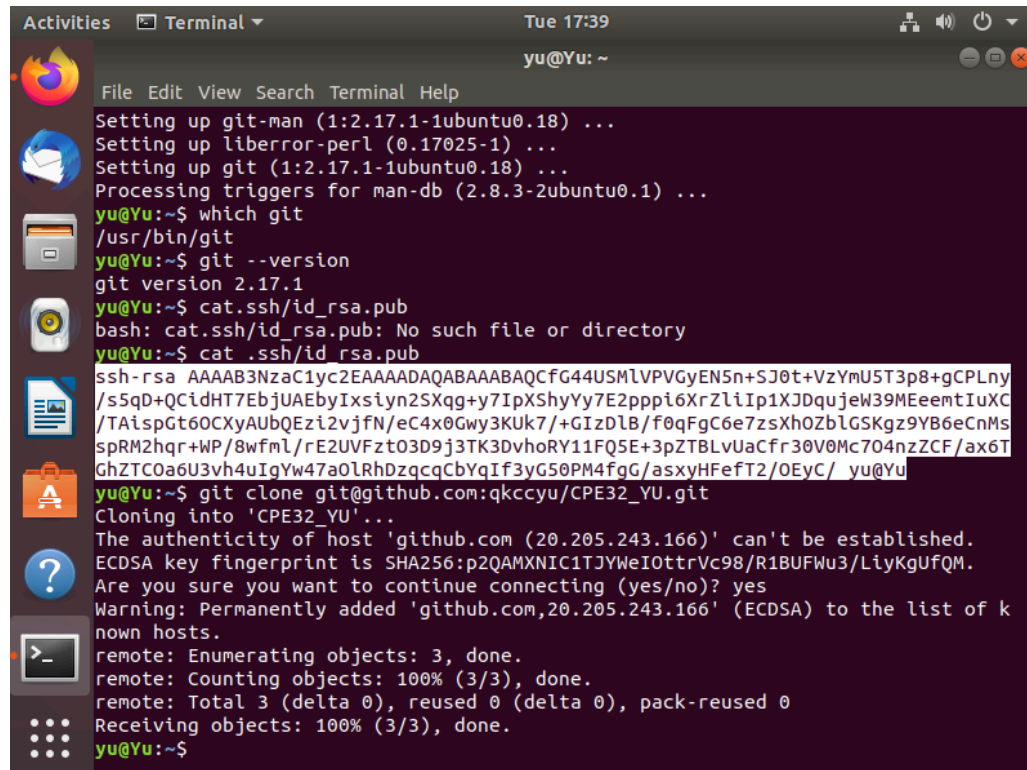
- c. On the local machine's terminal, issue the command `cat .ssh/id_rsa.pub` and copy the public key. Paste it on the GitHub key and press Add SSH key.



- 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.



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

A terminal window titled 'Terminal' with a dark background and light text. The window shows the output of several commands. First, it shows the installation of git-man, liberror-perl, and git. Then, the user runs 'which git' and 'git --version', both returning the path to the binary and version 2.17.1. Next, the user attempts to cat the RSA public key file at '.ssh/id_rsa.pub' but gets an error because the file doesn't exist. Then, the user cat's the file at '.ssh/id_rsa.pub' and the output is a long string of base64-encoded data. Finally, the user runs 'git clone git@github.com:qkccyu/CPE32_YU.git'. The terminal shows the cloning progress, including enumerating objects, counting objects, and receiving objects. It also shows a warning about the authenticity of the host 'github.com' and a confirmation to add it to the list of known hosts. The clone process completes successfully.

```
Activities Terminal Tue 17:39
yu@Yu: ~
File Edit View Search Terminal Help
Setting up git-man (1:2.17.1-1ubuntu0.18) ...
Setting up liberror-perl (0.17025-1) ...
Setting up git (1:2.17.1-1ubuntu0.18) ...
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
yu@Yu:~$ which git
/usr/bin/git
yu@Yu:~$ git --version
git version 2.17.1
yu@Yu:~$ cat.ssh/id_rsa.pub
bash: cat.ssh/id_rsa.pub: No such file or directory
yu@Yu:~$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCFG44USMLVPVGYEN5n+SJ0t+VzYmU5T3p8+gCPLNy
/s5qD+QcidHT7EbjuAEbyIxsyn2SXqg+y7IpXShyYy7E2pppi6XrZliIp1XJDqujeW39MEemtIuXC
/TAispGt60CXyAubQEzi2vjfN/ec4x0Gwy3Kuk7/+GizDLB/f0qFgC6e7zsXh0ZbLGSkgz9YB6eCnMs
spRM2hqr+WP/8wfml/rE2UVFzt03D9j3TK3DvhoRY11FQ5E+3pZTBLvUaCfr30V0Mc704nzZCF/ax6T
GhZTC0a6U3vh4uIqYw47a0LRhDzqcqCbYqIf3yG50PM4fgG/asxyHFefT2/0EyC/ yu@Yu
yu@Yu:~$ git clone git@github.com:qkccyu/CPE32_YU.git
Cloning into 'CPE32_YU'...
The authenticity of host 'github.com (20.205.243.166)' can't be established.
ECDSA key fingerprint is SHA256:p2QAMXNIC1TJYWeIOttrVc98/R1BUFWu3/LiyKgUfQM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'github.com,20.205.243.166' (ECDSA) to the list of k
nown hosts.
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
yu@Yu:~$
```

- 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`.

```
Activities Terminal Tue 17:39
yu@Yu: ~

File Edit View Search Terminal Help
Processing triggers for man-db (2.8.3-2ubuntu0.1) ...
yu@Yu:~$ which git
/usr/bin/git
yu@Yu:~$ git --version
git version 2.17.1
yu@Yu:~$ cat.ssh/id_rsa.pub
bash: cat.ssh/id_rsa.pub: No such file or directory
yu@Yu:~$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCFg44USMlVPVGYEN5n+SJ0t+VzYmU5T3p8+gCPLny
/s5qD+QCidHT7EbJUAByIxstyn2SXqg+y7IpXShyY7E2pppi6XrZliIp1XJDqujeW39MEemtIuXC
/TAispGt6OCXyAubQEzi2vjfN/ec4x0Gwy3Kuk7/+GIzDLB/f0qFgC6e7zsXh0ZbLGSKgz9YB6eCnMs
sPRM2hqr+WP/8wfml/rE2UVFzt03D9j3TK3DvhoRY11FQ5E+3pZTBLvUaCfr30V0Mc704nzZCF/ax6T
GhZTC0a6U3vh4uIqYw47a0LRhDzqcCbYqIf3yG50PM4fgG/asxyHfFeT2/OEYc/ yu@Yu
yu@Yu:~$ git clone git@github.com:qkccyu/CPE32_YU.git
Cloning into 'CPE32_YU'...
The authenticity of host 'github.com (20.205.243.166)' can't be established.
ECDSA key fingerprint is SHA256:p2QAMXNIC1TJYWeIOtrVc98/R1BUFWu3/LiyKgUfQM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'github.com,20.205.243.166' (ECDSA) to the list of k
nown hosts.
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
yu@Yu:~$ ls
CPE32_YU  Documents  examples.desktop  Pictures  Templates
Desktop  Downloads  Music           Public   Videos
yu@Yu:~$
```

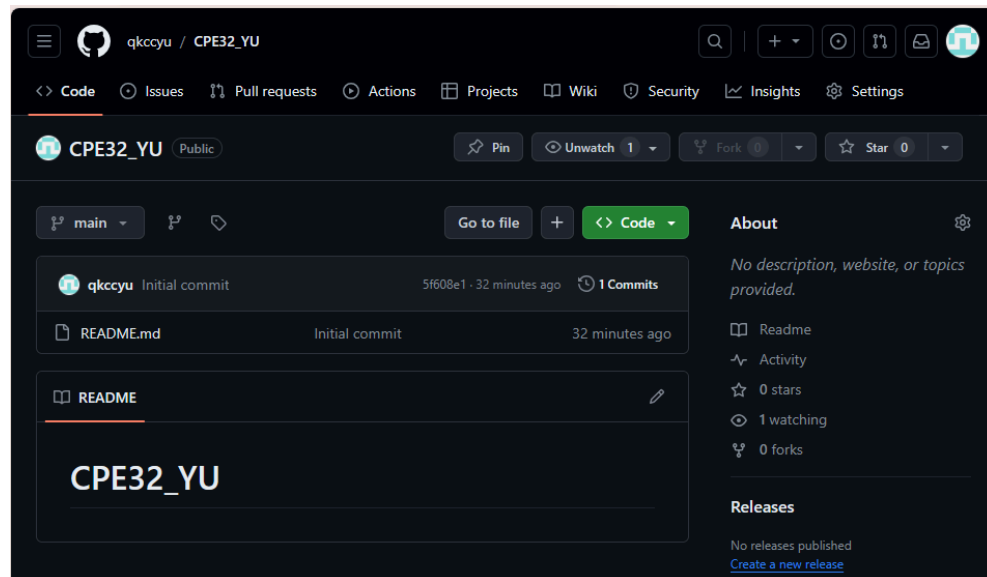
g. Use the following commands to personalize your git.

- `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`

```
Activities Terminal Tue 17:41
yu@Yu: ~

File Edit View Search Terminal Help
bash: cat.ssh/id_rsa.pub: No such file or directory
yu@Yu:~$ cat .ssh/id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCFg44USMlVPVGYEN5n+SJ0t+VzYmU5T3p8+gCPLny
/s5qD+QCidHT7EbJUAByIxstyn2SXqg+y7IpXShyY7E2pppi6XrZliIp1XJDqujeW39MEemtIuXC
/TAispGt6OCXyAubQEzi2vjfN/ec4x0Gwy3Kuk7/+GIzDLB/f0qFgC6e7zsXh0ZbLGSKgz9YB6eCnMs
sPRM2hqr+WP/8wfml/rE2UVFzt03D9j3TK3DvhoRY11FQ5E+3pZTBLvUaCfr30V0Mc704nzZCF/ax6T
GhZTC0a6U3vh4uIqYw47a0LRhDzqcCbYqIf3yG50PM4fgG/asxyHfFeT2/OEYc/ yu@Yu
yu@Yu:~$ git clone git@github.com:qkccyu/CPE32_YU.git
Cloning into 'CPE32_YU'...
The authenticity of host 'github.com (20.205.243.166)' can't be established.
ECDSA key fingerprint is SHA256:p2QAMXNIC1TJYWeIOtrVc98/R1BUFWu3/LiyKgUfQM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'github.com,20.205.243.166' (ECDSA) to the list of k
nown hosts.
remote: Enumerating objects: 3, done.
remote: Counting objects: 100% (3/3), done.
remote: Total 3 (delta 0), reused 0 (delta 0), pack-reused 0
Receiving objects: 100% (3/3), done.
yu@Yu:~$ ls
CPE32_YU  Documents  examples.desktop  Pictures  Templates
Desktop  Downloads  Music           Public   Videos
yu@Yu:~$ git config --global user.name "yu"
yu@Yu:~$ git config --global user.email qkccyu@tip.edu.ph
yu@Yu:~$ cat ~/.gitconfig
[user]
    name = yu
    email = qkccyu@tip.edu.ph
yu@Yu:~$
```

- 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?
- 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.



Reflections:

Answer the following:

3. What sort of things have we so far done to the remote servers using ansible commands?

- ***In the remote servers if you remove the servers or the data it requires to input the password, thus allowing us to create and access the servers. We can also create an SSH key and can copy to access the other servers.***

4. How important is the inventory file?

- ***The inventory file is important for specifying hosts and organizing infrastructure, enabling effective task execution and configuration management.***

Conclusions/Learnings:

- ***From what I learn this activity is that we can create our own SSH Key to use to other servers and it has two types of keys these are the Private and Public. These keys is used to the data or passwords that are very important. Some of the tasks I struggled even though some of it I did not finished, but still I've managed to the activity.***