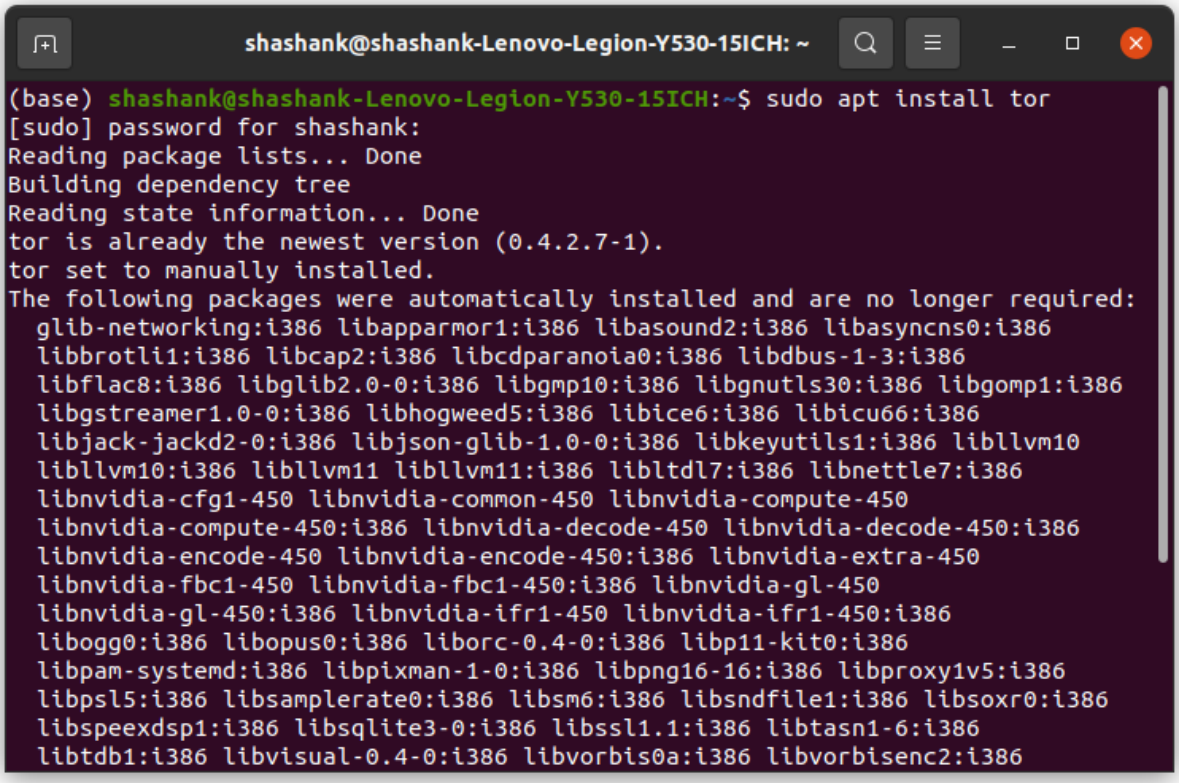
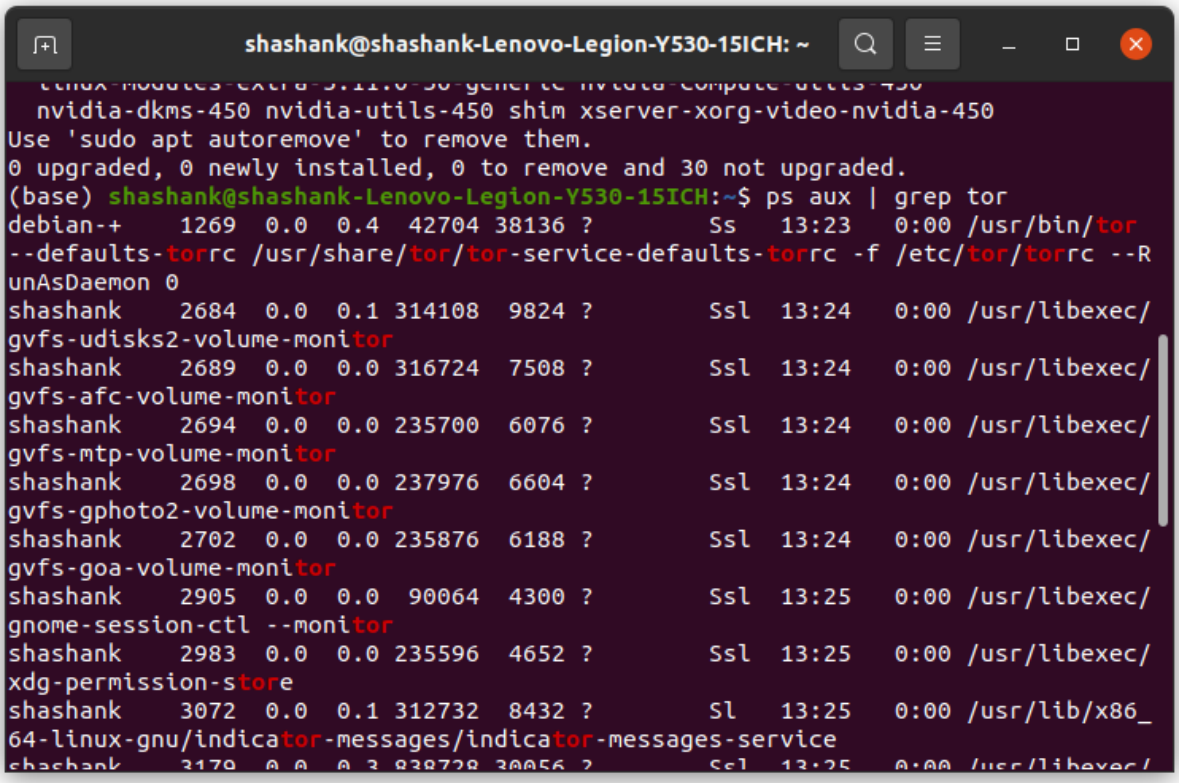
Q6

To install and configure TOR without TOR browser and configure it to any browser in the machine, the steps are as follows:

1) Install TOR, using terminal command, sudo apt install tor

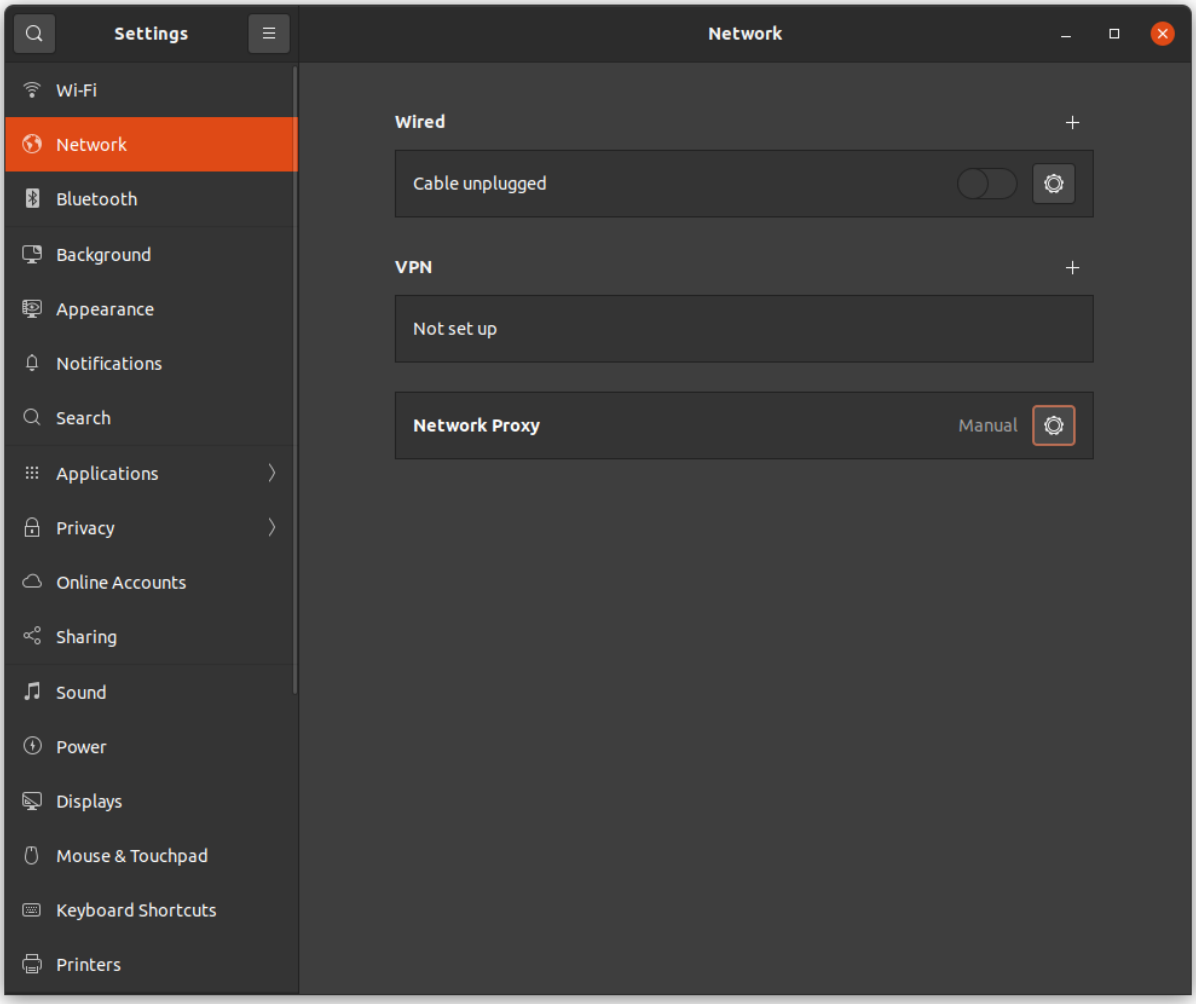


2) Once install tor, keeps running in the background

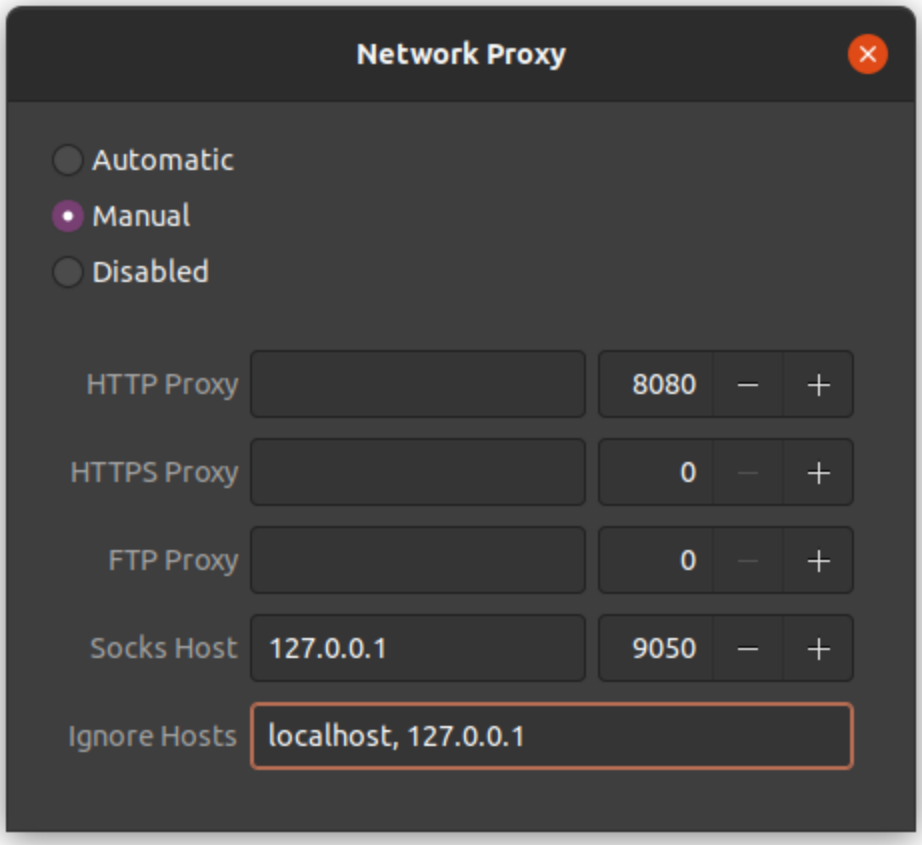


To configure Tor as default way to connect to internet for PC (regardless of browser) the steps are:

3) Open Settings (in ubuntu), Click on network

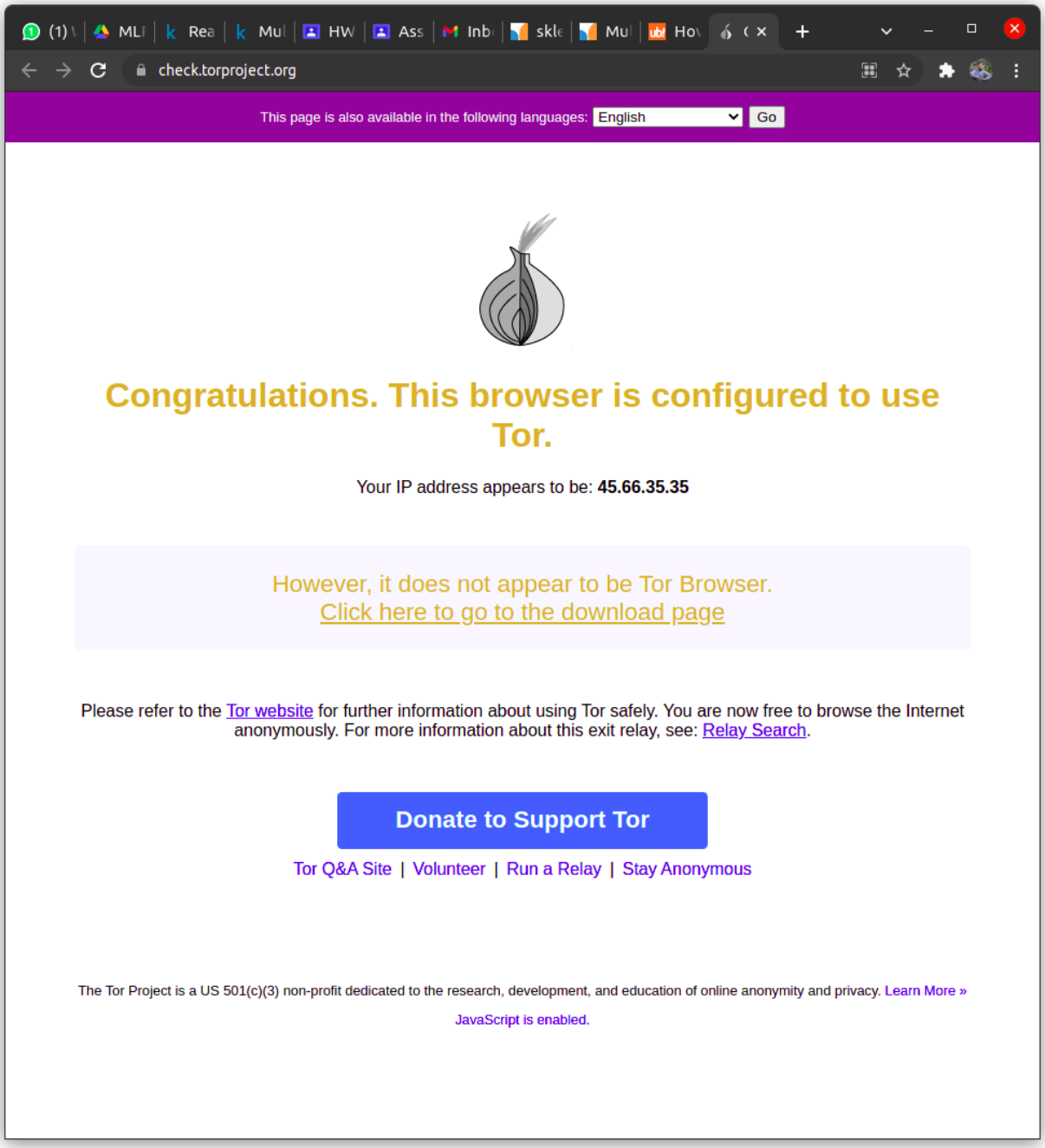


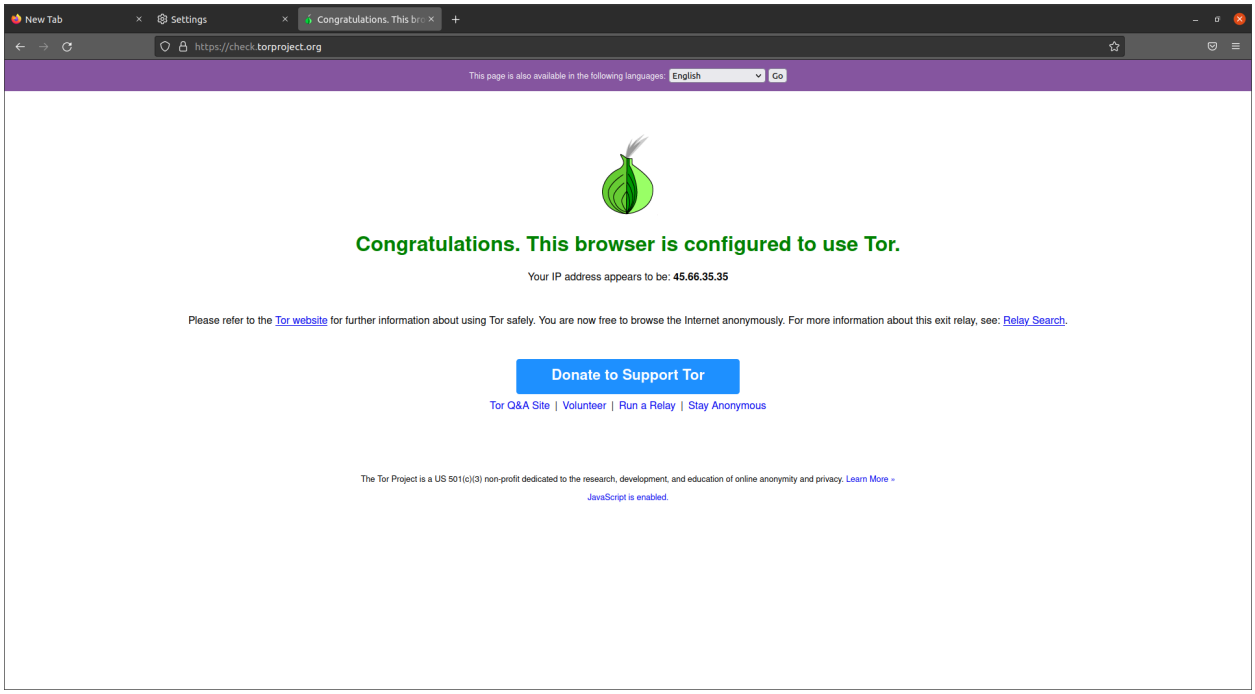
4) In Network Proxy, select Manual and fill the details as:



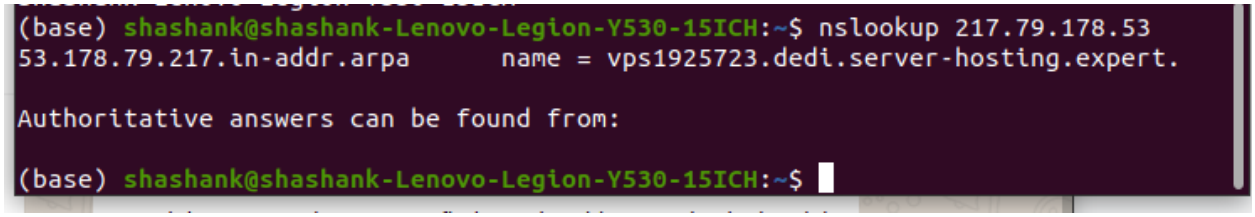
a) Socks Host: 127.0.0.1 and port as 9050
b) Ignore Localhosts.

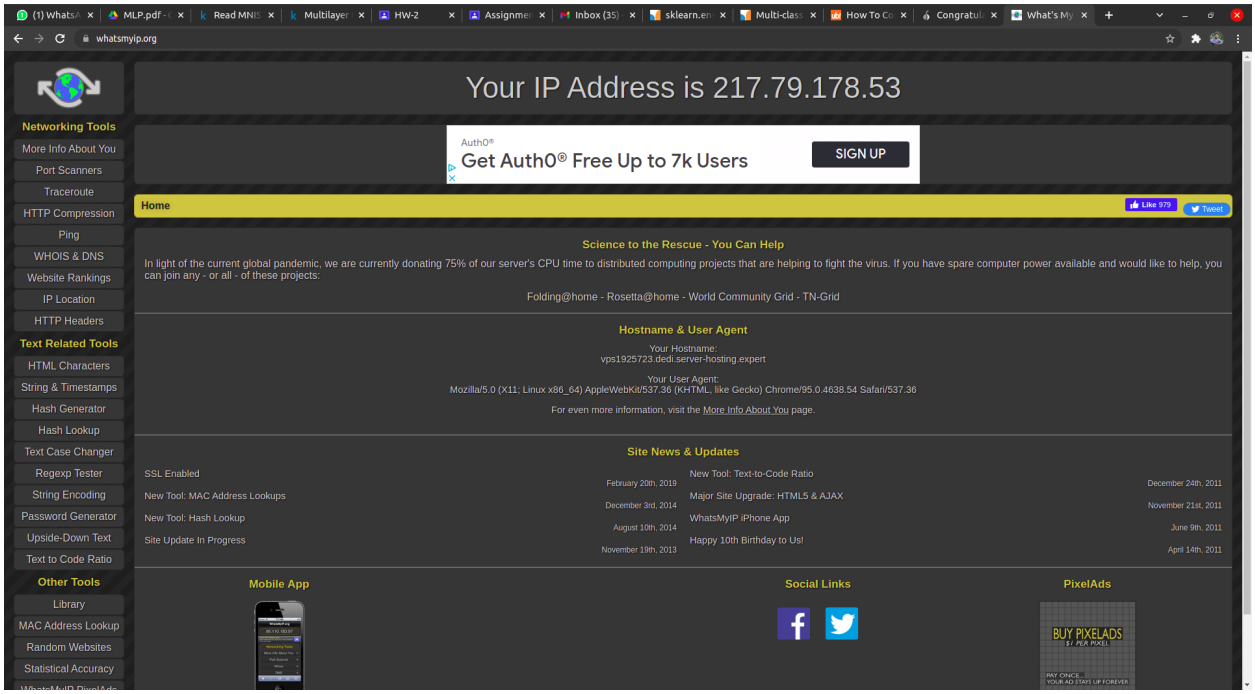
5) To check open https://check.torproject.org/ on any browser.


check.torproject.org
This page is also available in the following languages: English Go
Congratulations. This browser is configured to use Tor.
Your IP address appears to be: 45.66.35.35
However, it does not appear to be Tor Browser.
Click here to go to the download page
Please refer to the Tor website for further information about using Tor safely. You are now free to browse the Internet anonymously. For more information about this exit relay, see: Relay Search.
Donate to Support Tor
Tor Q&A Site | Volunteer | Run a Relay | Stay Anonymous
The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn More »
JavaScript is enabled.

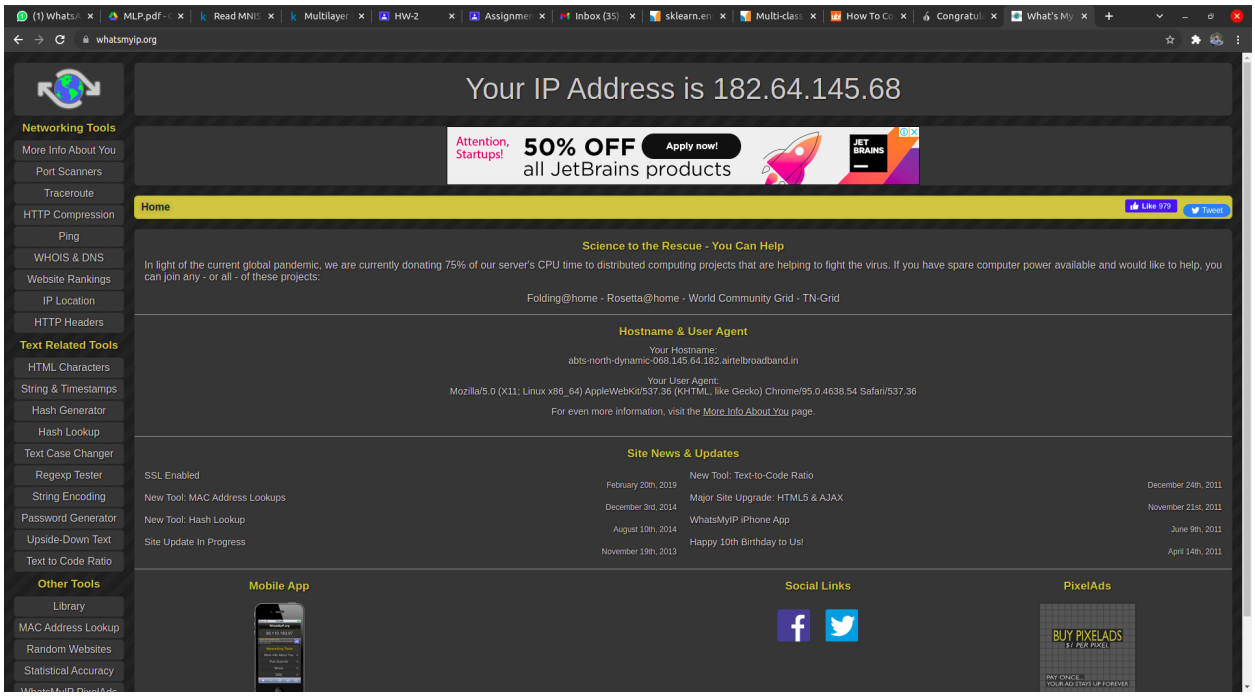


During tor connection, See IP and Hostname are endnodes of tor network
Hostname as visible on whatsmyip.com, vps1925723.dedi.server-hosting.expert

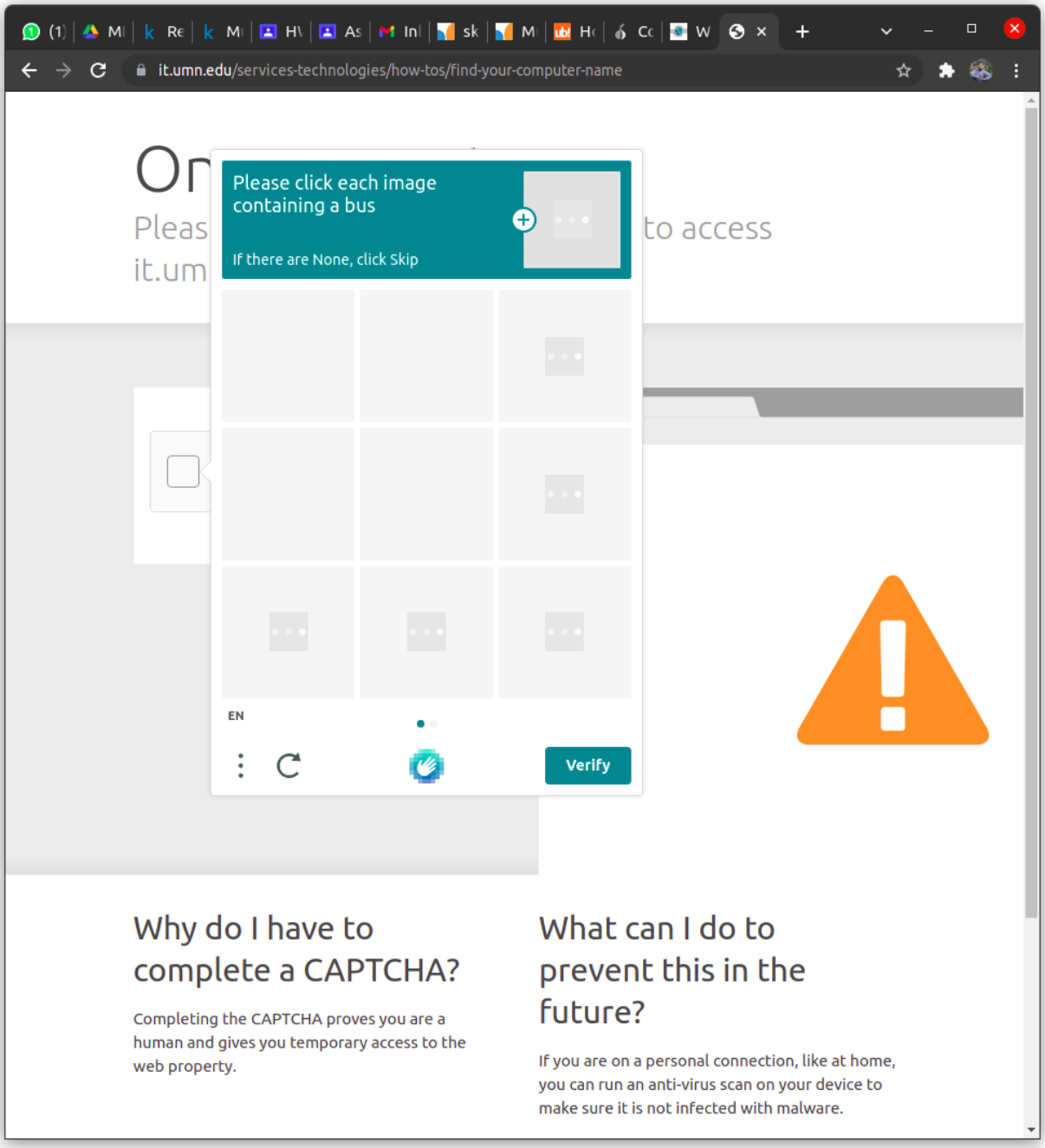




After termination, See IP and Hostname are my own ISP



While using tor,



Q7

Task 1: Using the ssl library to create a public key for my system and use it to access the assigned VM. The steps followed for the same are:

a) Firstly we will check if we already have a generated key-pair or not.
   Command: **ls -al ~/.ssh/id_*.pub**
b) Then, if we don't have a key-pair we will generate one using the ssh-keygen command, we can add our authentication credentials as comments.

Command: **ssh-keygen -t rsa -b 4096 -C "shashank19107@iiitd.ac.in"**
This command generates an rsa 4096 bit key pair with a given string as comment.

```
(base) shashank@shashank-Lenovo-Legion-Y530-15ICH:~$ ls -al ~/.ssh/id_*.pub
ls: cannot access '/home/shashank/.ssh/id_*.pub': No such file or directory
(base) shashank@shashank-Lenovo-Legion-Y530-15ICH:~$ ssh-keygen -t rsa -b 4096 -
C "shashank19107@iiitd.ac.in"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/shashank/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/shashank/.ssh/id_rsa
Your public key has been saved in /home/shashank/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:G/m2bWvvjK+frf73gVXcmC0oq13s0Jv6qJxhyIqobJo shashank19107@iiitd.ac.in
The key's randomart image is:
+---[RSA 4096]----+
|                 |
|              . =.|
|           . . + =|
|          . =   ..|
|         S o +  . |
|      . . * + oo  |
|       o = + +. . |
|.+ . . o + =oo oo|
|E.. .   +.++*OXo*|
+----[SHA256]-----+
(base) shashank@shashank-Lenovo-Legion-Y530-15ICH:~$ ls ~/.ssh/id_*
/home/shashank/.ssh/id_rsa  /home/shashank/.ssh/id_rsa.pub
(base) shashank@shashank-Lenovo-Legion-Y530-15ICH:~$ ssh-copy-id iiitd@192.168.2
```

c) Now we will copy our obtained key in the assigned VM, we will use the command ssh-copy-id followed by user@IP and enter password when prompted.
Command: ssh-copy-id iiitd@192.168.2.234

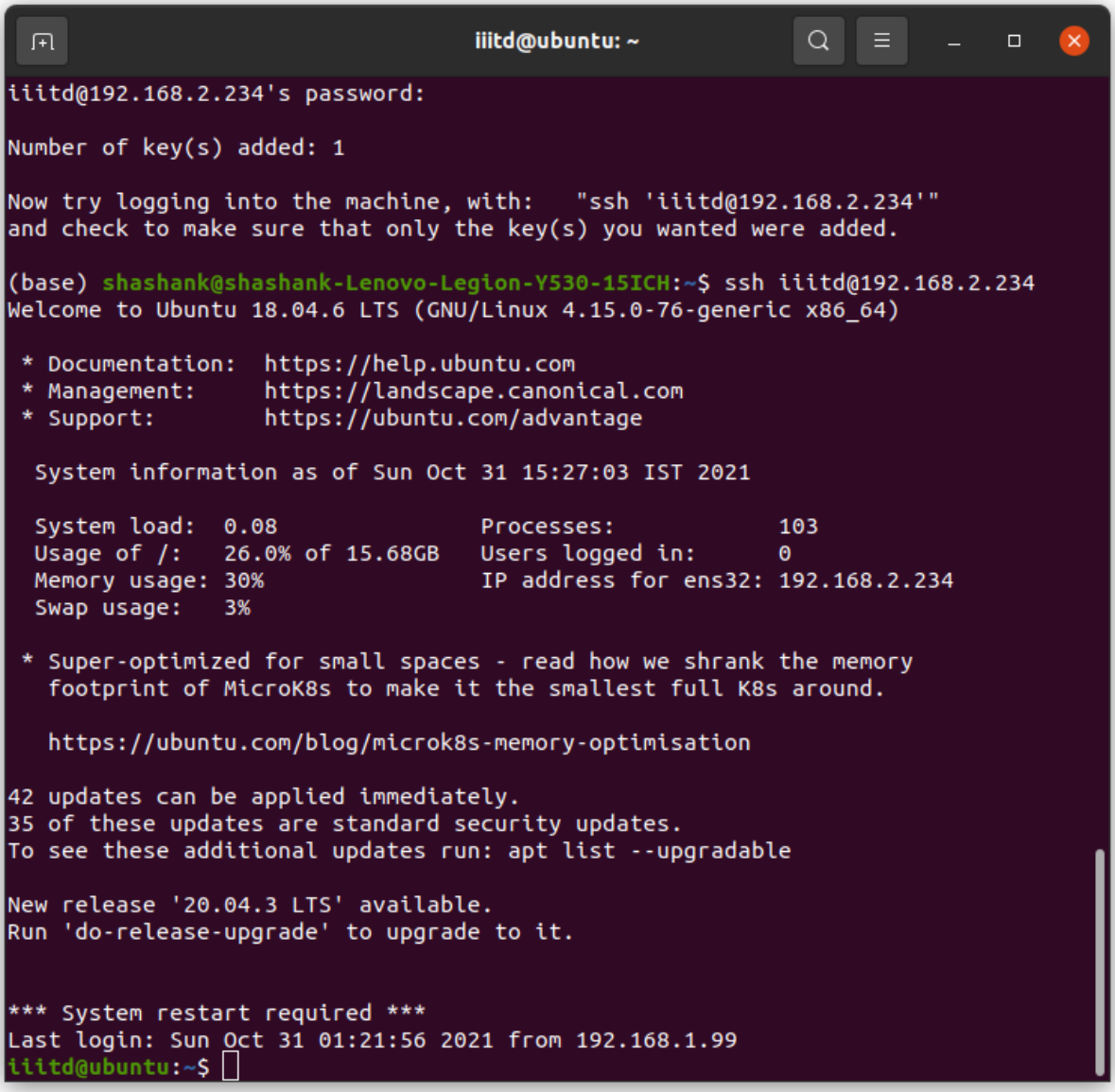
```
(base) shashank@shashank-Lenovo-Legion-Y530-15ICH:~$ ls ~/.ssh/id_*
/home/shashank/.ssh/id_rsa  /home/shashank/.ssh/id_rsa.pub
(base) shashank@shashank-Lenovo-Legion-Y530-15ICH:~$ ssh-copy-id iiitd@192.168.2
.234
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
iiitd@192.168.2.234's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'iiitd@192.168.2.234'"
and check to make sure that only the key(s) you wanted were added.

(base) shashank@shashank-Lenovo-Legion-Y530-15ICH:~$ ssh iiitd@192.168.2.234
```

d) We will receive a success acknowledgment, we can check if our keys were added successfully by doing ssh user@IP, we should be logged in without password. Command: ssh iiitd@192.168.2.234



Q7 Task 2:

Having a public key is a much safer method especially when we are required to log in any system very frequently because managing different passwords is often very complicated and time consuming, multiple users can use this method to access a system without going through the hassle of remaining a common password, in case of any breach, the user can be individually obtained, it can be pinpointed just by looking at the login logs.

Public key cryptography also eliminates the possibility of unauthorised access due to password breach, having a public key adds a layer of security without compromising on the user experience or by prompting for annoying authorisations.

Q4.