NSSII Exercise 4

Manavjeet Singh, 2018295

Part1

Downloading and Installing Tor

- Download tor source code from the official website(https://www.torproject.org/download/tor/) and unzip the file.
- Open readme and follow build instructions:

```
To build Tor from source:
        ./configure && make && make install
```

- Create a hashed code password by:

```
~ tor --hash-password "tor"
16:32E20B95C2D71BC160D4C76D871A9347B291363E8A5E36337181B1BE19
~
```

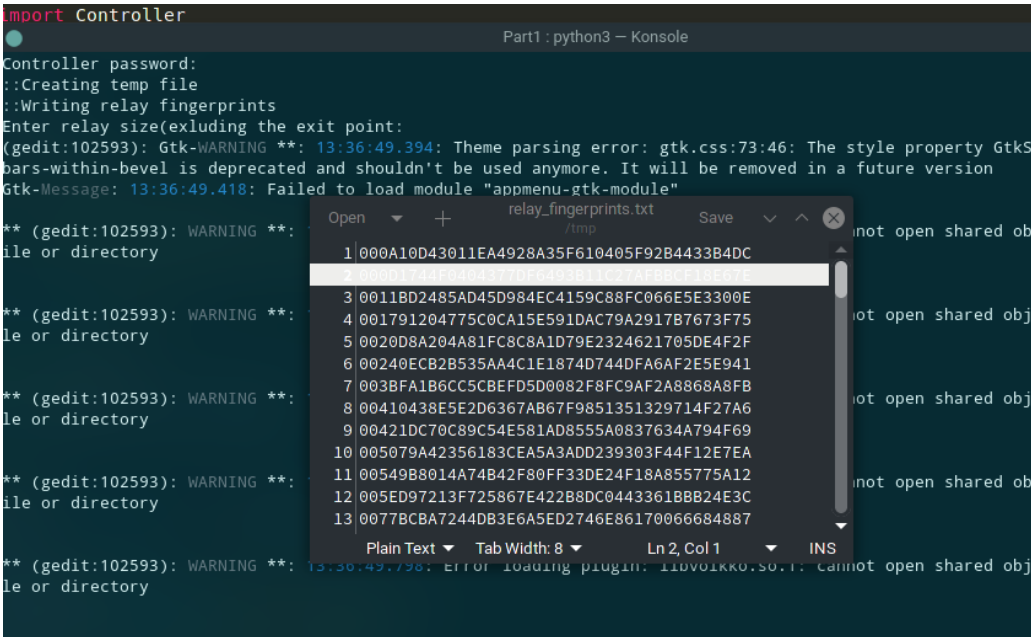
- Open /etc/tor/torrc file and add following lines:
  ControlPort 9051 `#control port for connection from python script`
  HashedControlPassword
  16:32E20B95C2D71BC160D4C76D871A9347B291363E8A5E36337181B1BE19
  `#hashed password to make changes in tor network from python script`

Creating a manual Circuit

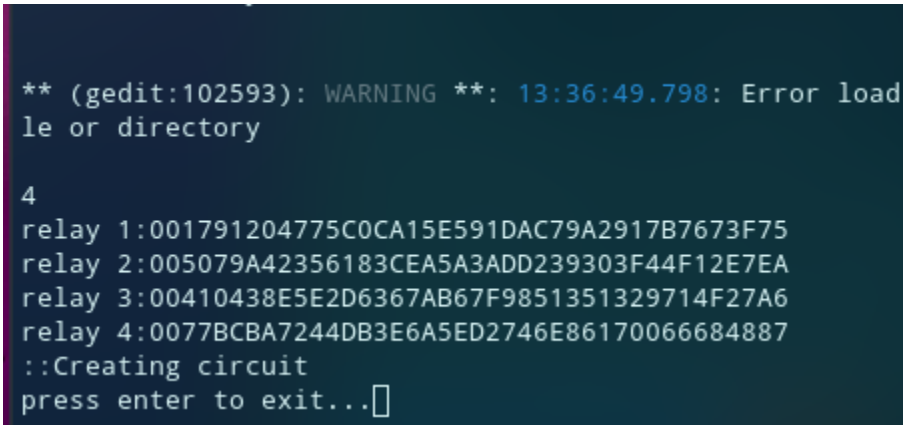
- Start the tor process using `sudo systemctl start tor`
- Use python script automate_tor.py (in the submission)
  - Enter password for control port,

```
Part1 : python3 — K
~/git/NSSII/Exercise_4/Part1  main  python3 automate_tor.py
pass: tor
Controller password:
```

- A text file with fingerprints will pop up.

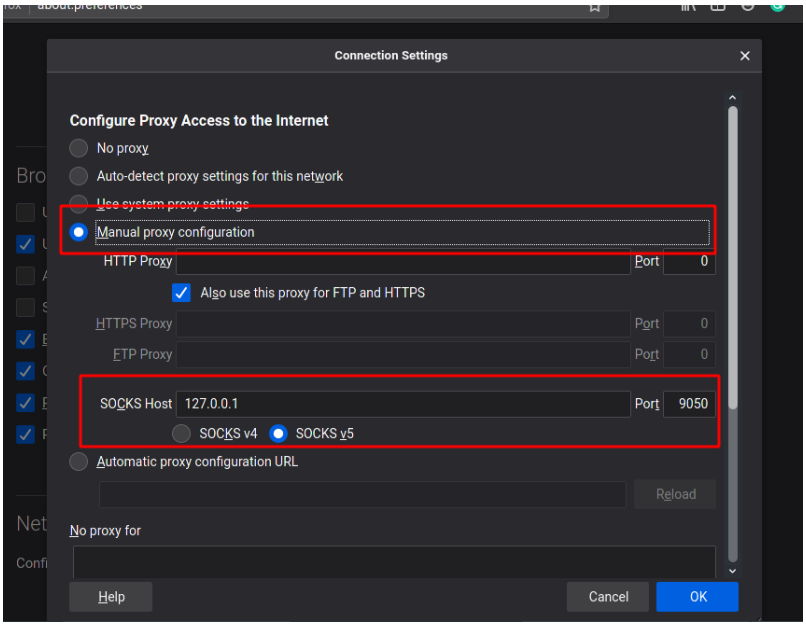


- Enter the number of relays in the tor network, excluding the exit link since it's fingerprint is hard coded. Then copy the fingerprints from the popup file and enter into the python script.

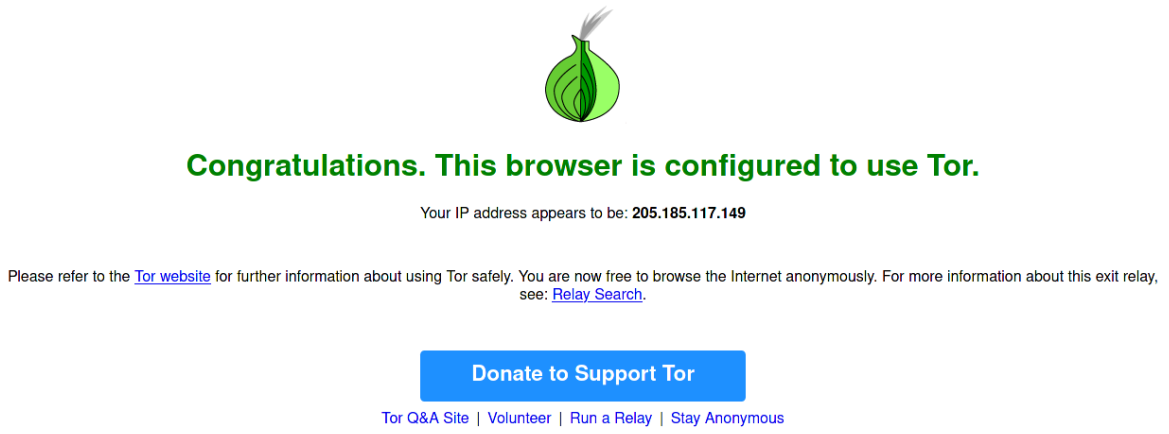


- Configuring firefox to use tor:
  - Open network setting from preferences in firefox.

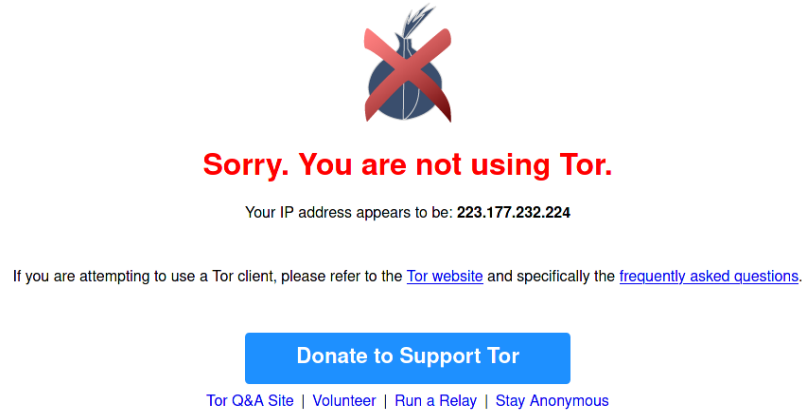
- Configure the settings as follows to enable forwarding of packets to socks port 9050.



- Open https://check.torproject.org/ to check if tor circuit is established or not.
- If the connection is established then the page will look as follows:



- If circuit is not established then the page will look as follows:



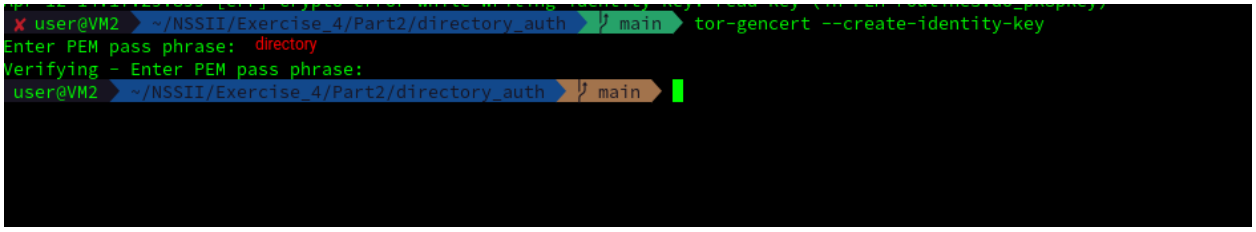
Private Tor network

Network Details

Nickname	IP address	Role
VM1	10.0.0.1	Client
VM2	10.0.0.2	Guard node, DirServ
VM3	10.0.0.3	Middle node, DirServ
VM4	10.0.0.4	Exit node, DirServ
VM5	10.0.0.5	Server

Creating a Directory Authority

- Generate key and certificate for the Directory server using the following command



- The following files will be created

    - authority_identity_key: long term key to sign authority certificate
    - authority_signing_key: medium-term key to sign directory information
    - authority_certificate: document signed by authority identity key to certify authority signing key.
- Coy these files to DataDirectory/keys folder.
- Add the following parameters to the torrc files of all the nodes in the network to enable them discover the authority.
  `DirServer <Nickname> orport=<port no> v3ident=<fingerprint from authority_certificate> 10.0.0.2:<port number for dirserv> <fingerprint from DataDirectory/fingerprint file>`
- Also add **TestingTorNetwork 1** to all the nodes in the torrc of all the nodes to enable testing so that it would work on private network and not on official tor network.
- Enable directory service by adding the following lines in torrc.
  `AuthoritativeDirectory 1`
  `V3AuthoritativeDirectory 1`
- Add directory port option in torrc along with the address of the machine
  Address 10.0.0.2
  DirPort 10.0.0.2:9031
- Add path to the data directory
  DataDirectory /path/to/datadir

Relays

- In torrc file add the following options
  Nickname VM2
  ORPort 9001 #Enable listing for incoming tor packets at this port
  ExitRelay 0 #do not allow exit
- For the exit node change the last line to
  ExitRelay 1 #allow exit
  ExitPolicy accept *:* #accept all to exit
- Also add the path to data directory folder.

Client

- Just add the dirserv info as mentioned in “Creating a Directory Authority” section.
- Also add the path to data directory folder.

Running

On each machine(except VM1) run tor process using the command **`tor -f /path/to/torrc.`** On VM run python script manual**`_tor.py.`**
Torrc files are attached in the submission folder.

VM2

```
✘ user@VM2 ~/NSSII/Exercise_4/Part2/VM2  main ± tor -f ./VM2
Apr 17 08:59:35.070 [notice] Tor 0.4.5.7 running on Linux with Libevent 2.1.12-stable, OpenSSL 1.1.1i, Zlib 1.2.11,
iblzma 5.2.5, Libzstd 1.4.9 and Glibc 2.33 as libc.
Apr 17 08:59:35.070 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.
rg/download/download#warning
Apr 17 08:59:35.070 [notice] Read configuration file "/home/user/NSSII/Exercise_4/Part2/VM2/./VM2".
Apr 17 08:59:35.076 [warn] Path for DataDirectory (./lib) is relative and will resolve to /home/user/NSSII/Exercise_
/Part2/VM2/./lib. Is this what you wanted?
Apr 17 08:59:35.076 [notice] Based on detected system memory, MaxMemInQueues is set to 737 MB. You can override this
by setting MaxMemInQueues by hand.
Apr 17 08:59:35.076 [warn] You have used DirAuthority or AlternateDirAuthority to specify alternate directory author
ties in your configuration. This is potentially dangerous: it can make you look different from all other Tor users,
nd hurt your anonymity. Even if you've specified the same authorities as Tor uses by default, the defaults could cha
ge in the future. Be sure you know what you're doing.
Apr 17 08:59:35.076 [warn] TestingTorNetwork is set. This will make your node almost unusable in the public Tor netw
rk, and is therefore only advised if you are building a testing Tor network!
Apr 17 08:59:35.077 [notice] Opening OR listener on 0.0.0.0:9001
Apr 17 08:59:35.077 [notice] Opened OR listener connection (ready) on 0.0.0.0:9001
Apr 17 08:59:35.077 [notice] Opening OR listener on [::]:9001
Apr 17 08:59:35.077 [notice] Opened OR listener connection (ready) on [::]:9001
Apr 17 08:59:35.077 [notice] Opening Directory listener on 10.0.0.2:9031
Apr 17 08:59:35.077 [notice] Opened Directory listener connection (ready) on 10.0.0.2:9031
```

VM3

```
✘ user@VM3 ~/NSSII/Exercise_4/Part2/VM3  main ± tor -f VM3
Apr 17 08:59:31.810 [notice] Tor 0.4.5.7 running on Linux with Libevent 2.1.12-stab
le, OpenSSL 1.1.1i, Zlib 1.2.11, Liblzma 5.2.5, Libzstd 1.4.9 and Glibc 2.33 as lib
c.
Apr 17 08:59:31.810 [notice] Tor can't help you if you use it wrong! Learn how to b
e safe at https://www.torproject.org/download/download#warning
Apr 17 08:59:31.810 [notice] Read configuration file "/home/user/NSSII/Exercise_4/P
art2/VM3/VM3".
Apr 17 08:59:31.816 [warn] Path for DataDirectory (./lib) is relative and will reso
lve to /home/user/NSSII/Exercise_4/Part2/VM3/./lib. Is this what you wanted?
Apr 17 08:59:31.816 [notice] Based on detected system memory, MaxMemInQueues is set
 to 737 MB. You can override this by setting MaxMemInQueues by hand.
Apr 17 08:59:31.816 [warn] You have used DirAuthority or AlternateDirAuthority to s
pecify alternate directory authorities in your configuration. This is potentially d
angerous: it can make you look different from all other Tor users, and hurt your an
onymity. Even if you've specified the same authorities as Tor uses by default, the
defaults could change in the future. Be sure you know what you're doing.
Apr 17 08:59:31.817 [warn] TestingTorNetwork is set. This will make your node almos
t unusable in the public Tor network, and is therefore only advised if you are buil
ding a testing Tor network!
Apr 17 08:59:31.817 [notice] Opening OR listener on 0.0.0.0:9003
Apr 17 08:59:31.817 [notice] Opened OR listener connection (ready) on 0.0.0.0:9003
Apr 17 08:59:31.817 [notice] Opening OR listener on [::]:9003
Apr 17 08:59:31.817 [notice] Opened OR listener connection (ready) on [::]:9003
Apr 17 08:59:31.817 [notice] Opening Directory listener on 10.0.0.3:9033
Apr 17 08:59:31.825 [notice] Opened Directory listener connection (ready) on 10.0.0
.3:9033
```

VM4

```
OSError: Reached a 90 second timeout without success
user@VM4 ~/NSSII/Exercise_4/Part2/VM4 main ± tor -f VM4
Apr 17 08:59:29.069 [notice] Tor 0.4.5.7 running on Linux with Libevent 2.1.12-stab
le, OpenSSL 1.1.1i, Zlib 1.2.11, Liblzma 5.2.5, Libzstd 1.4.9 and Glibc 2.33 as lib
c.
Apr 17 08:59:29.072 [notice] Tor can't help you if you use it wrong! Learn how to b
e safe at https://www.torproject.org/download/download#warning
Apr 17 08:59:29.073 [notice] Read configuration file "/home/user/NSSII/Exercise_4/P
art2/VM4/VM4".
Apr 17 08:59:29.078 [warn] Path for DataDirectory (./lib) is relative and will reso
lve to /home/user/NSSII/Exercise_4/Part2/VM4/./lib. Is this what you wanted?
Apr 17 08:59:29.079 [notice] Based on detected system memory, MaxMemInQueues is set
 to 737 MB. You can override this by setting MaxMemInQueues by hand.
Apr 17 08:59:29.079 [warn] You have used DirAuthority or AlternateDirAuthority to s
pecify alternate directory authorities in your configuration. This is potentially d
angerous: it can make you look different from all other Tor users, and hurt your an
onymity. Even if you've specified the same authorities as Tor uses by default, the
defaults could change in the future. Be sure you know what you're doing.
Apr 17 08:59:29.079 [warn] TestingTorNetwork is set. This will make your node almos
t unusable in the public Tor network, and is therefore only advised if you are buil
ding a testing Tor network!
Apr 17 08:59:29.080 [notice] Opening OR listener on 0.0.0.0:9005
Apr 17 08:59:29.080 [notice] Opened OR listener connection (ready) on 0.0.0.0:9005
Apr 17 08:59:29.080 [notice] Opening OR listener on [::]:9005
Apr 17 08:59:29.080 [notice] Opened OR listener connection (ready) on [::]:9005
Apr 17 08:59:29.080 [notice] Opening Directory listener on 10.0.0.4:9035
Apr 17 08:59:29.080 [notice] Opened Directory listener connection (ready) on 10.0.0
.4:9035
```

VM1

VM1 [Running] - Oracle VM VirtualBox

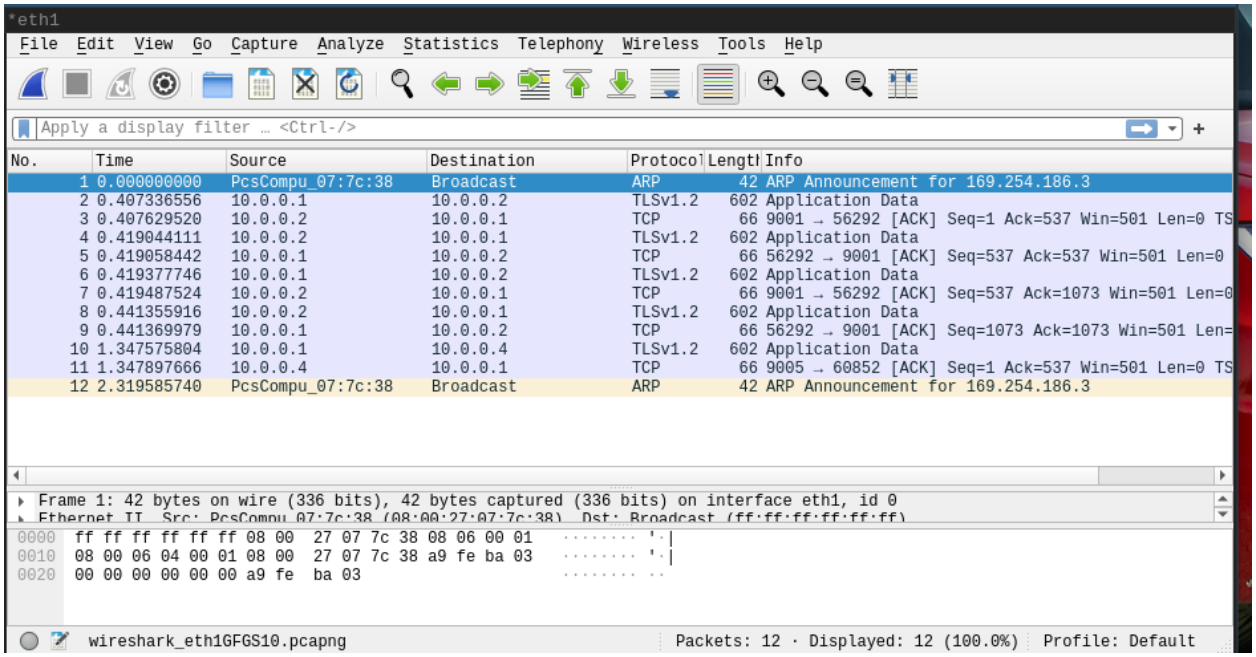
user@artixVM:~/git/NSSII/Exercise_4/Part2

File Edit View Search Terminal Help

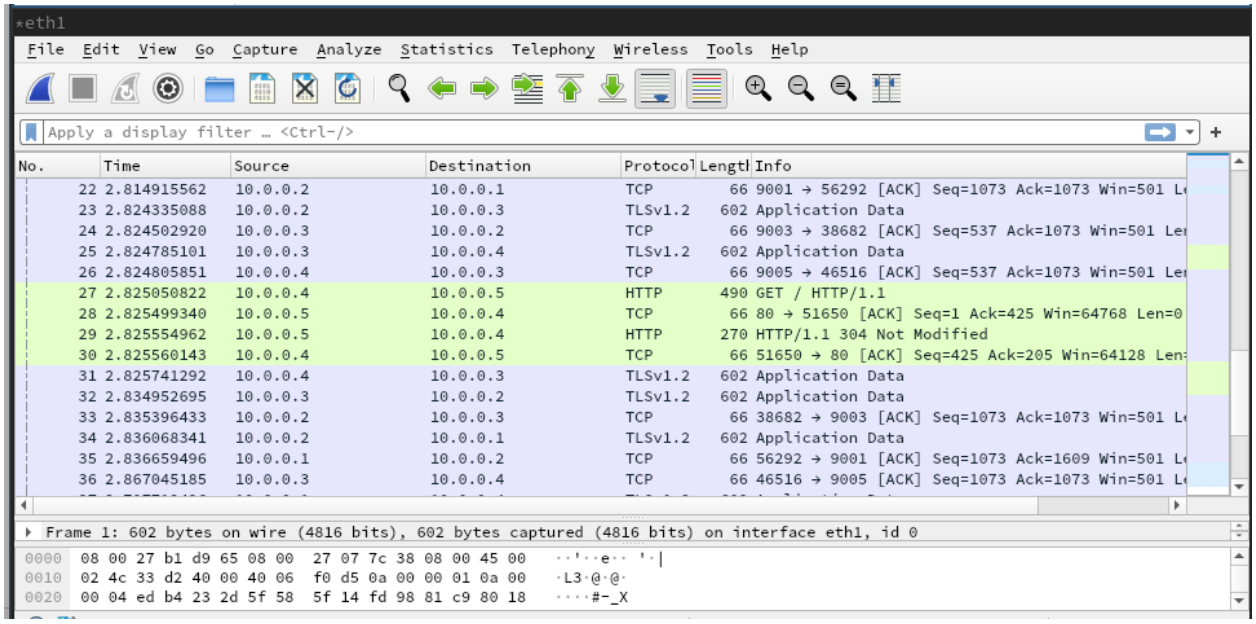
```
user@artixVM ~/git/NSSII/Exercise_4/Part2 main ± sudo python manual_tor.py
Apr 17 09:14:37.000 [notice] Bootstrapped 0% (starting): Starting
Apr 17 09:14:38.000 [notice] Bootstrapped 5% (conn): Connecting to a relay
Apr 17 09:14:38.000 [notice] Bootstrapped 10% (conn_done): Connected to a relay
Apr 17 09:14:38.000 [notice] Bootstrapped 14% (handshake): Handshaking with a relay
Apr 17 09:14:38.000 [notice] Bootstrapped 15% (handshake_done): Handshake with a relay done
Apr 17 09:14:38.000 [notice] Bootstrapped 75% (enough_dirinfo): Loaded enough directory info to build circuits
Apr 17 09:14:38.000 [notice] Bootstrapped 90% (ap_handshake_done): Handshake finished with a relay to build circu
its
Apr 17 09:14:38.000 [notice] Bootstrapped 95% (circuit_create): Establishing a Tor circuit
Apr 17 09:14:38.000 [notice] Bootstrapped 100% (done): Done
pass: tor
Controller password:
Enter relay size:3
relay 1:9AD686225BDF05B0695531BAD0E628DD9530071A
relay 2:82DAFF6C68669F7B9B262AA54057BFEC35F2C2B7
relay 3:FBF8E18DA23876F5E672FB164C5D65F151159EB9
::Creating circuit
press enter to exit...
user@artixVM ~/git/NSSII/Exercise_4/Part2 main ±
```

Packet Capture

- Packet capture from VM1 to the guard tor relay(VM2) while accessing the server from VM5. As expected all the packets are TLS encrypted.



- Packet capture from exit node to the server VM5 on the request from client VM1. Packets are not encrypted between VM4 and VM4.



- The packet capture of VM1 accessing server VM5 without tor. Packets are not encrypted.