

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
```

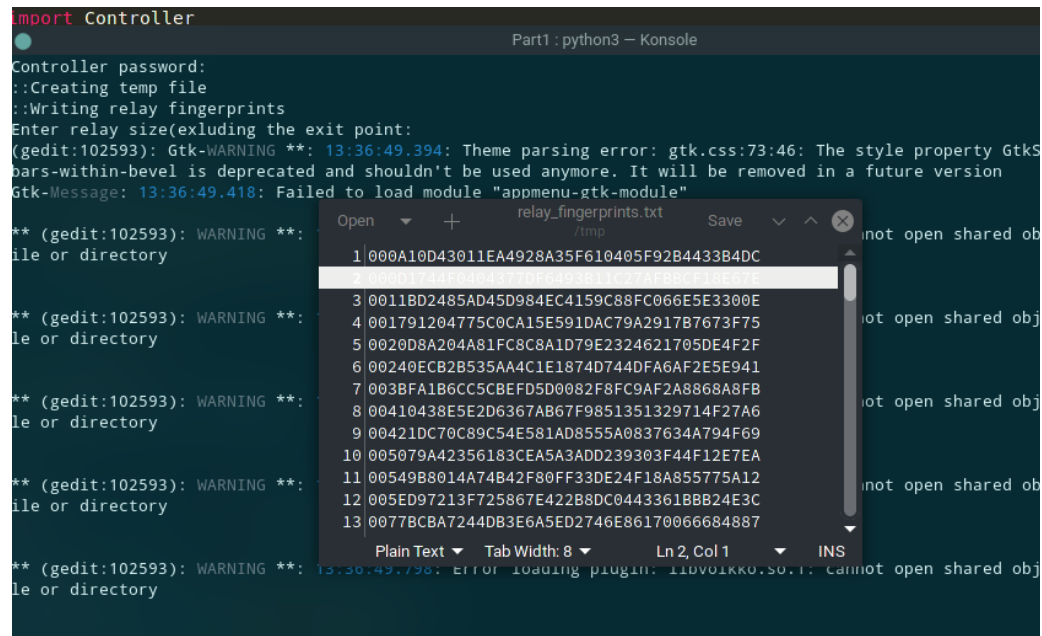
-
- Open /etc/tor/torrc file and add following lines:
ControlPort 9051 #control port for connection from python script
HashedControlPassword
16:32E20B95C2D71BC160D4C76D871A9347B291363E8A5E36337181B1BE19
#hashed password to make changes in tor network from python script

Creating a manual Circuit

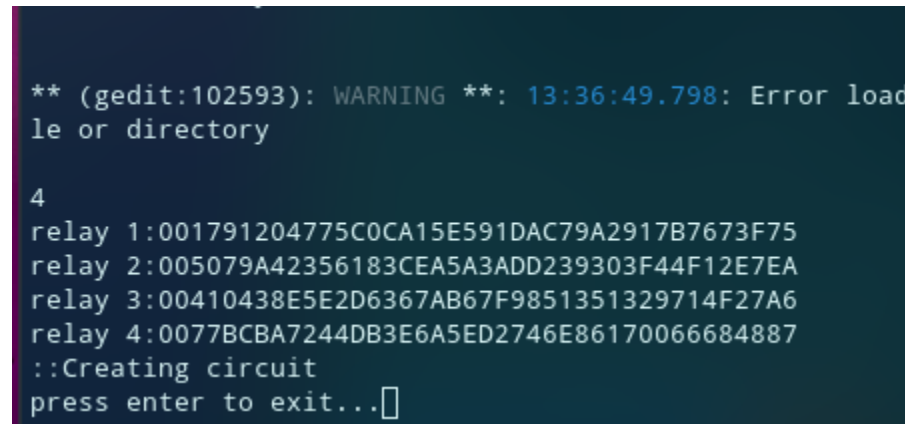
- Start the tor process using `sudo systemctl start tor`
- Use python script `automate_tor.py` (in the submission)
 - Enter password for control port,

```
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.

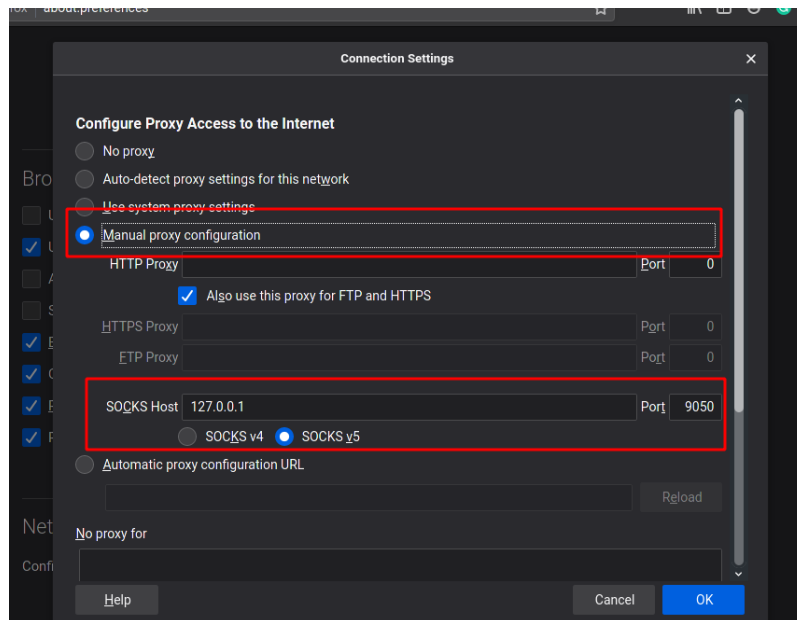


- Enter the number of relays in the tor network, excluding the exit link since it's fingerprint is hard coded. Then copy the fingerprints from the popup file and enter into the python script.



- 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:



Congratulations. This browser is configured to use Tor.

Your IP address appears to be: **205.185.117.149**

Please refer to the [Tor website](https://www.torproject.org/) 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](#)

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



Sorry. You are not using Tor.

Your IP address appears to be: 223.177.232.224

If you are attempting to use a Tor client, please refer to the [Tor website](#) and specifically the [frequently asked questions](#).

[Donate to Support Tor](#)

[Tor Q&A Site](#) | [Volunteer](#) | [Run a Relay](#) | [Stay Anonymous](#)

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

```
x user@VM2 ~/NSSII/Exercise_4/Part2/directory_auth$ main$ tor-gencert --create-identity-key
Enter PEM pass phrase: directory
Verifying - Enter PEM pass phrase:
user@VM2 ~/NSSII/Exercise_4/Part2/directory_auth$ main$
```

- 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.
- Copy 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

```
X user@VM2 ~/NSSII/Exercise_4/Part2/VM2 1 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, liblzma 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.org/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_4/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 authorities in your configuration. This is potentially dangerous: it can make you look different from all other Tor users, and hurt your anonymity. 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 08:59:35.076 [warn] TestingTorNetwork is set. This will make your node almost unusable in the public Tor network, 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

```
X user@VM3 ~/NSSII/Exercise_4/Part2/VM3 1 main ± tor -f VM3
Apr 17 08:59:31.810 [notice] Tor 0.4.5.7 running on Linux with Libevent 2.1.12-stable, OpenSSL 1.1.1i, Zlib 1.2.11, Liblzma 5.2.5, Libzstd 1.4.9 and Glibc 2.33 as libc.
Apr 17 08:59:31.810 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Apr 17 08:59:31.810 [notice] Read configuration file "/home/user/NSSII/Exercise_4/Part2/VM3/VM3".
Apr 17 08:59:31.816 [warn] Path for DataDirectory (./lib) is relative and will resolve 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 specify alternate directory authorities in your configuration. This is potentially dangerous: it can make you look different from all other Tor users, and hurt your anonymity. 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 almost unusable in the public Tor network, and is therefore only advised if you are building 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

```

ERROR: 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-stable, OpenSSL 1.1.1i, Zlib 1.2.11, Liblzma 5.2.5, Libzstd 1.4.9 and Glibc 2.33 as libc.
Apr 17 08:59:29.072 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/download/download#warning
Apr 17 08:59:29.073 [notice] Read configuration file "/home/user/NSSII/Exercise_4/Part2/VM4/VM4".
Apr 17 08:59:29.078 [warn] Path for DataDirectory (./lib) is relative and will resolve 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 specify alternate directory authorities in your configuration. This is potentially dangerous: it can make you look different from all other Tor users, and hurt your anonymity. 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 almost unusable in the public Tor network, and is therefore only advised if you are building 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 circuits
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:F8F8E18DA23876F5E672FB164C5D65F151159EB9
::Creating circuit
press enter to exit...
user@artixVM ~/git/NSSII/Exercise_4/Part2 main ±

```

Packet Capture

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

The screenshot shows a Wireshark interface with a packet capture on interface eth1. The packet list shows 12 packets. Packets 1 and 12 are ARP announcements. Packets 2 through 11 are TLS traffic (Application Data and ACKs) between 10.0.0.1 and 10.0.0.2. The packet details pane shows the first packet (Frame 1) as an ARP announcement for 169.254.186.3.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PcsCompu_07:7c:38	Broadcast	ARP	42	ARP Announcement for 169.254.186.3
2	0.407336556	10.0.0.1	10.0.0.2	TLSv1.2	602	Application Data
3	0.407629520	10.0.0.2	10.0.0.1	TCP	66	9001 → 56292 [ACK] Seq=1 Ack=537 Win=501 Len=0 TS
4	0.419044111	10.0.0.2	10.0.0.1	TLSv1.2	602	Application Data
5	0.419058442	10.0.0.1	10.0.0.2	TCP	66	56292 → 9001 [ACK] Seq=537 Ack=537 Win=501 Len=0
6	0.419377746	10.0.0.1	10.0.0.2	TLSv1.2	602	Application Data
7	0.419487524	10.0.0.2	10.0.0.1	TCP	66	9001 → 56292 [ACK] Seq=537 Ack=1073 Win=501 Len=0
8	0.441355916	10.0.0.2	10.0.0.1	TLSv1.2	602	Application Data
9	0.441369979	10.0.0.1	10.0.0.2	TCP	66	56292 → 9001 [ACK] Seq=1073 Ack=1073 Win=501 Len=
10	1.347575804	10.0.0.1	10.0.0.4	TLSv1.2	602	Application Data
11	1.347897666	10.0.0.4	10.0.0.1	TCP	66	9005 → 60852 [ACK] Seq=1 Ack=537 Win=501 Len=0 TS
12	2.319585740	PcsCompu_07:7c:38	Broadcast	ARP	42	ARP Announcement for 169.254.186.3

Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth1, id 0
Ethernet II, Src: PcsCompu_07:7c:38 (08:00:27:07:7c:38), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

0000 ff ff ff ff ff ff 00 27 07 7c 38 08 06 00 01
0010 08 00 06 04 00 01 08 00 27 07 7c 38 a9 fe ba 03
0020 00 00 00 00 00 00 a9 fe ba 03

wireshark_eth1GFS10.pcapng Packets: 12 · Displayed: 12 (100.0%) Profile: Default

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

The screenshot shows a Wireshark interface with a packet capture on interface eth1. The packet list shows 36 packets. Packets 22-36 are a mix of TCP, TLS, and HTTP traffic. Packets 27-30 are unencrypted HTTP traffic (GET, 304 Not Modified, ACK). Packets 31-36 are TLS traffic (Application Data, ACKs). The packet details pane shows the first packet (Frame 1) as an HTTP GET request for / HTTP/1.1.

No.	Time	Source	Destination	Protocol	Length	Info
22	2.814915562	10.0.0.2	10.0.0.1	TCP	66	9001 → 56292 [ACK] Seq=1073 Ack=1073 Win=501 Len=0
23	2.824335088	10.0.0.2	10.0.0.3	TLSv1.2	602	Application Data
24	2.824502920	10.0.0.3	10.0.0.2	TCP	66	9003 → 38682 [ACK] Seq=537 Ack=1073 Win=501 Len=0
25	2.824785101	10.0.0.3	10.0.0.4	TLSv1.2	602	Application Data
26	2.824805851	10.0.0.4	10.0.0.3	TCP	66	9005 → 46516 [ACK] Seq=537 Ack=1073 Win=501 Len=0
27	2.825050822	10.0.0.4	10.0.0.5	HTTP	490	GET / HTTP/1.1
28	2.825499340	10.0.0.5	10.0.0.4	TCP	66	80 → 51650 [ACK] Seq=1 Ack=425 Win=64768 Len=0
29	2.825554962	10.0.0.5	10.0.0.4	HTTP	270	HTTP/1.1 304 Not Modified
30	2.825560143	10.0.0.4	10.0.0.5	TCP	66	51650 → 80 [ACK] Seq=425 Ack=205 Win=64128 Len=0
31	2.825741292	10.0.0.4	10.0.0.3	TLSv1.2	602	Application Data
32	2.834952695	10.0.0.3	10.0.0.2	TLSv1.2	602	Application Data
33	2.835396433	10.0.0.2	10.0.0.3	TCP	66	38682 → 9003 [ACK] Seq=1073 Ack=1073 Win=501 Len=0
34	2.836068341	10.0.0.2	10.0.0.1	TLSv1.2	602	Application Data
35	2.836659496	10.0.0.1	10.0.0.2	TCP	66	56292 → 9001 [ACK] Seq=1073 Ack=1609 Win=501 Len=0
36	2.867045185	10.0.0.3	10.0.0.4	TCP	66	46516 → 9005 [ACK] Seq=1073 Ack=1073 Win=501 Len=0

Frame 1: 602 bytes on wire (4816 bits), 602 bytes captured (4816 bits) on interface eth1, id 0

0000 08 00 27 b1 d9 65 08 00 27 07 7c 38 08 00 45 00e...
0010 02 4c 33 d2 40 00 40 06 f0 d5 0a 00 00 01 0a 00 ...L3:@:@
0020 00 04 ed b4 23 2d 5f 58 5f 14 fd 98 81 c9 80 18#-_X

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

Wireshark interface showing packet capture on eth1. The packet list displays 10 packets, including DHCP Discover and HTTP GET requests. The packet details pane shows the structure of the first packet (Frame 1: 590 bytes on wire). The status bar at the bottom shows 10 packets displayed, 100.0% profile, and system metrics like memory and network speed.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0xdfc61604
2	0.446422952	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0x9ed50c69
3	0.876123538	10.0.0.1	10.0.0.5	TCP	74	80 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
4	0.878186747	10.0.0.5	10.0.0.1	TCP	74	80 → 48248 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0
5	0.878230475	10.0.0.1	10.0.0.5	TCP	66	48248 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
6	0.878565964	10.0.0.1	10.0.0.5	HTTP	490	GET / HTTP/1.1
7	0.879148966	10.0.0.5	10.0.0.1	TCP	66	80 → 48248 [ACK] Seq=1 Ack=425 Win=64768 Len=0 T
8	0.879660456	10.0.0.5	10.0.0.1	HTTP	270	HTTP/1.1 304 Not Modified
9	0.879682973	10.0.0.1	10.0.0.5	TCP	66	48248 → 80 [ACK] Seq=425 Ack=205 Win=64128 Len=0
10	2.083742430	0.0.0.0	255.255.255.255	DHCP	590	DHCP Discover - Transaction ID 0xd841f87e

Frame 1: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface eth1, id 0
 Ethernet II Src: PcsComm h1:d9:65 (08:00:27:b1:d9:65) Dst: Broadcast (ff:ff:ff:ff:ff:ff)

0000 ff ff ff ff ff ff 08 00 27 b1 d9 65 08 00 45 00
 0010 02 40 00 00 00 00 40 11 78 ae 00 00 00 00 ff ff
 0020 ff ff 00 44 00 43 02 2c 5a f8 01 01 06 00 df c6 ...D.C.,
 0030 16 04 00 00 00 00 00 00 00 00 00 00 00 00 00
 0040 00 00 00 00 00 00 08 00 27 b1 d9 65 00 00 00
 wireshark_eth1Q0PK10.pcapng Packets: 10 · Displayed: 10 (100.0%) Profile: Default

1 2 3 10 IPv6 | W: down | E: 10.0.2.15 (1000 Mbit/s) | FULL 100.00% | 39.6 GiB | 0.00 | MEMORY < 232.0 MiB | 2021-04-15 00:09:1