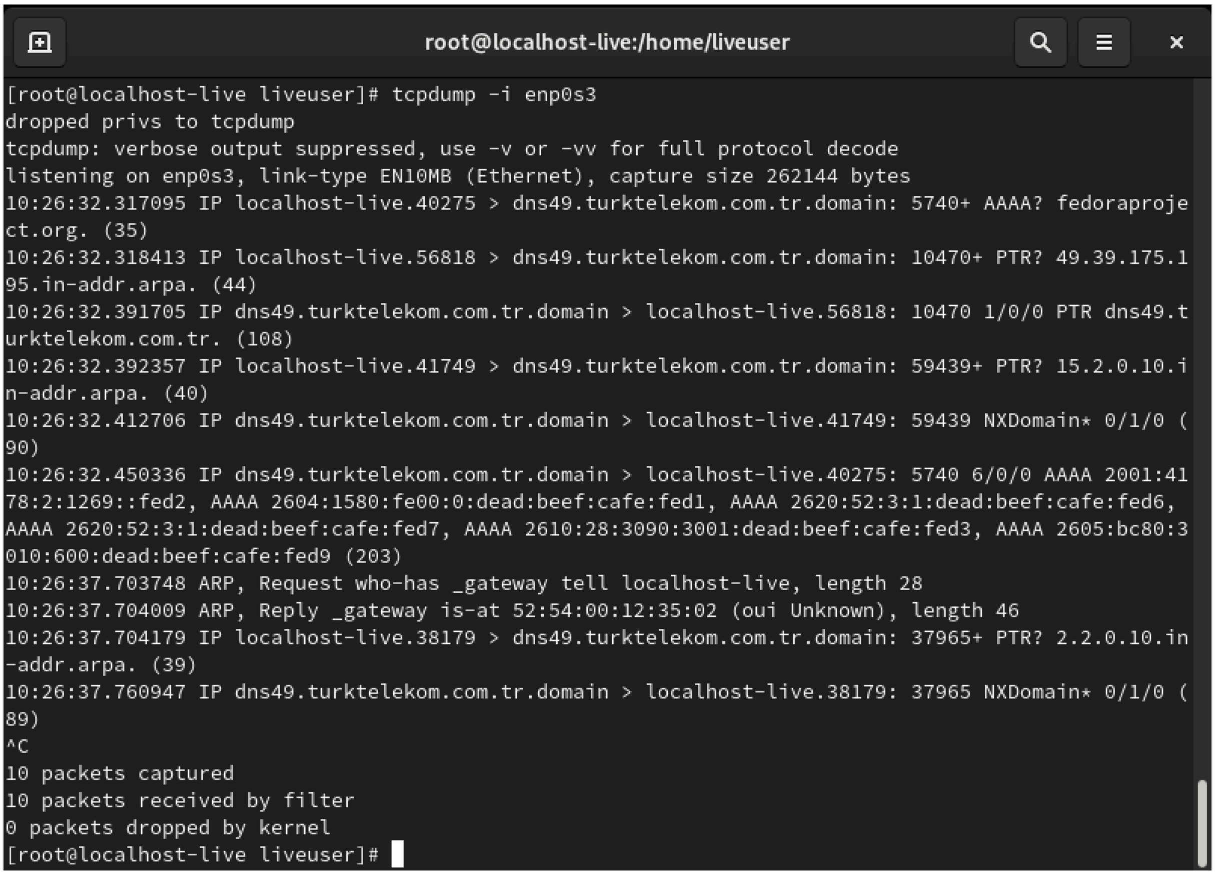
Behiye Erdemir
240206013

CENG 421 NETWORK PROGRAMMING – ASSIGNMENT 2

40- ‘dnf’ that is a package manager is used for the installation of the tcpdump by typing **$ sudo dnf install tcpdump.** Besides, for the finding the network interface numbers **$ ip addr show** commmand is used; the interfaces are ‘lo’ and ‘enp0s3’.

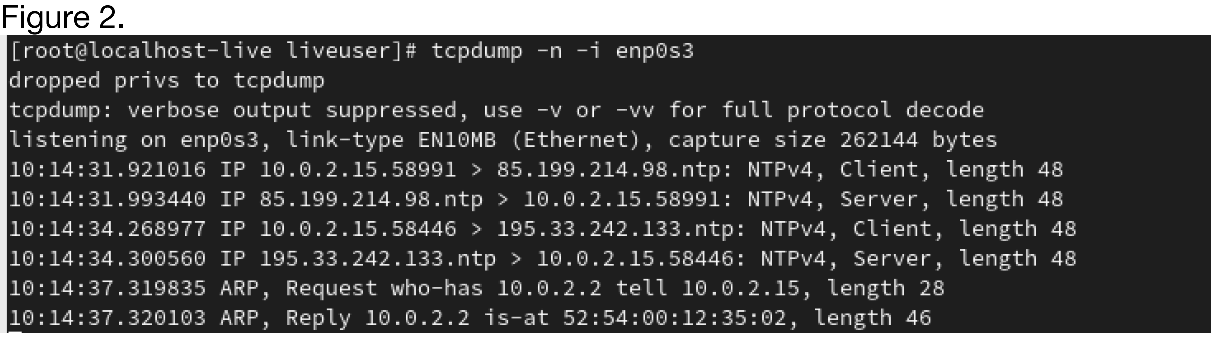
To get the network packets from a single interface **$ tcpdump -i enp0s3** was typed as can be seen in Figure 1.



```
[root@localhost-live liveuser]# tcpdump -i enp0s3
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
10:26:32.317095 IP localhost-live.40275 > dns49.turktelekom.com.tr.domain: 5740+ AAAA? fedoraproje
ct.org. (35)
10:26:32.318413 IP localhost-live.56818 > dns49.turktelekom.com.tr.domain: 10470+ PTR? 49.39.175.1
95.in-addr.arpa. (44)
10:26:32.391705 IP dns49.turktelekom.com.tr.domain > localhost-live.56818: 10470 1/0/0 PTR dns49.t
urktelekom.com.tr. (108)
10:26:32.392357 IP localhost-live.41749 > dns49.turktelekom.com.tr.domain: 59439+ PTR? 15.2.0.10.i
n-addr.arpa. (40)
10:26:32.412706 IP dns49.turktelekom.com.tr.domain > localhost-live.41749: 59439 NXDomain* 0/1/0 (
90)
10:26:32.450336 IP dns49.turktelekom.com.tr.domain > localhost-live.40275: 5740 6/0/0 AAAA 2001:41
78:2:1269::fed2, AAAA 2604:1580:fe00:0:dead:beef:cafe:fed1, AAAA 2620:52:3:1:dead:beef:cafe:fed6,
AAAA 2620:52:3:1:dead:beef:cafe:fed7, AAAA 2610:28:3090:3001:dead:beef:cafe:fed3, AAAA 2605:bc80:3
010:600:dead:beef:cafe:fed9 (203)
10:26:37.703748 ARP, Request who-has _gateway tell localhost-live, length 28
10:26:37.704009 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), length 46
10:26:37.704179 IP localhost-live.38179 > dns49.turktelekom.com.tr.domain: 37965+ PTR? 2.2.0.10.in
-addr.arpa. (39)
10:26:37.760947 IP dns49.turktelekom.com.tr.domain > localhost-live.38179: 37965 NXDomain* 0/1/0 (
89)
^C
10 packets captured
10 packets received by filter
0 packets dropped by kernel
[root@localhost-live liveuser]#
```

Figure 1: The packets on the interface enp0s3.

To capture the network interface and IP adresses $ tcpdump -n -i enp0s3 [1] is typed. With the -n flag, adresses cant be converted into names as can be seen in Figure 2.



```
[root@localhost-live liveuser]# tcpdump -n -i enp0s3
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
10:14:31.921016 IP 10.0.2.15.58991 > 85.199.214.98.ntp: NTPv4, Client, length 48
10:14:31.993440 IP 85.199.214.98.ntp > 10.0.2.15.58991: NTPv4, Server, length 48
10:14:34.268977 IP 10.0.2.15.58446 > 195.33.242.133.ntp: NTPv4, Client, length 48
10:14:34.300560 IP 195.33.242.133.ntp > 10.0.2.15.58446: NTPv4, Server, length 48
10:14:37.319835 ARP, Request who-has 10.0.2.2 tell 10.0.2.15, length 28
10:14:37.320103 ARP, Reply 10.0.2.2 is-at 52:54:00:12:35:02, length 46
```

Kaynakça

[1] «Manpage of TCPDUMP,» TCPDUMP, 10 08 2020. [Çevrimiçi]. Available: https://www.tcpdump.org/manpages/tcpdump.1.html.