

# CENG 421 NETWORK PROGRAMMING HOMEWORK

Esin Sanem İmamoğlu

Student ID:240206006

Inspecting segments of packets of a network interface requires some basic steps. First of all, here is typed “sudo yum install tcpdump” to the terminal of the Fedora. It automatically installed tcpdump. Then, “ip addr show” is typed in order to take knowledge of the network interface as shown in the figures below.

```
esin@localhost:~  
[esin@localhost ~]$ sudo yum install tcpdump  
[sudo] password for esin:  
Fedora 32 openh264 (From Cisco) - x86_64          1.5 kB/s | 986 B      00:00  
Fedora Modular 32 - x86_64                      35 kB/s | 23 kB      00:00  
Fedora Modular 32 - x86_64 - Updates             26 kB/s | 12 kB      00:00  
Fedora Modular 32 - x86_64 - Updates             171 kB/s | 468 kB    00:02  
Fedora 32 - x86_64 - Updates                     11 kB/s | 8.0 kB     00:00  
Fedora 32 - x86_64 - Updates                     602 kB/s | 7.2 MB    00:12  
Fedora 32 - x86_64                               22 kB/s | 23 kB      00:01  
google-chrome                                   4.1 kB/s | 1.3 kB     00:00  
google-chrome                                   4.9 kB/s | 3.6 kB     00:00  
teams                                           4.3 kB/s | 3.0 kB     00:00  
Package tcpdump-14:4.9.3-2.fc32.x86_64 is already installed.  
Dependencies resolved.  
Nothing to do.  
Complete!  
[esin@localhost ~]$
```

```
[esin@localhost ~]$ ip addr show  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000  
    link/ether 10:7b:44:26:7f:86 brd ff:ff:ff:ff:ff:ff  
3: wlp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000  
    link/ether f8:59:71:36:39:1d brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.196/24 brd 192.168.1.255 scope global dynamic noprefixroute wlp3s0  
        valid_lft 85990sec preferred_lft 85990sec  
    inet6 fe80::2629:1a14:1775:c88e/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

Second step is typing “tcpdump -i wlp3s0. Wlp3s0 is my interface address. Traffic stopped by typing ctrl+c. Thus, packets of the interface are obtained.

```
[esin@localhost ~]$ sudo su -
[sudo] password for esin:
[root@localhost ~]# tcpdump -i wlp3s0
dropped privs to tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on wlp3s0, link-type EN10MB (Ethernet), capture size 262144 bytes
22:34:41.401228 IP localhost.localdomain.40272 > 52.114.75.149.https: Flags [.], ack 399431939, win 501, length 0
22:34:41.402583 IP localhost.localdomain.37972 > _gateway.domain: 17932+ PTR? 149.75.114.52.in-addr.arpa. (44)
22:34:41.610992 IP 52.114.75.149.https > localhost.localdomain.40272: Flags [.], ack 1, win 1026, length 0
22:34:41.611029 IP _gateway.domain > localhost.localdomain.37972: 17932 NXDomain 0/1/0 (123)
22:34:41.612263 IP localhost.localdomain.51866 > _gateway.domain: 27603+ PTR? 196.1.168.192.in-addr.arpa. (44)
22:34:41.626822 IP _gateway.domain > localhost.localdomain.51866: 27603 NXDomain 0/0/0 (44)
22:34:41.627581 IP localhost.localdomain.39292 > _gateway.domain: 48539+ PTR? 1.1.168.192.in-addr.arpa. (42)
22:34:41.644311 IP _gateway.domain > localhost.localdomain.39292: 48539 NXDomain 0/0/0 (42)
^C
8 packets captured
8 packets received by filter
0 packets dropped by kernel
[root@localhost ~]#
```