ASSIGNMENT

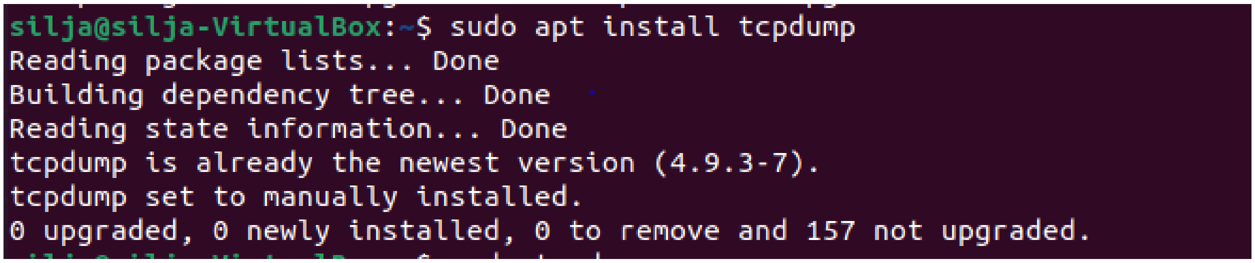
NETWORKING AND SYSTEM ADMINISTRATION

SILJA C K

RMCA B

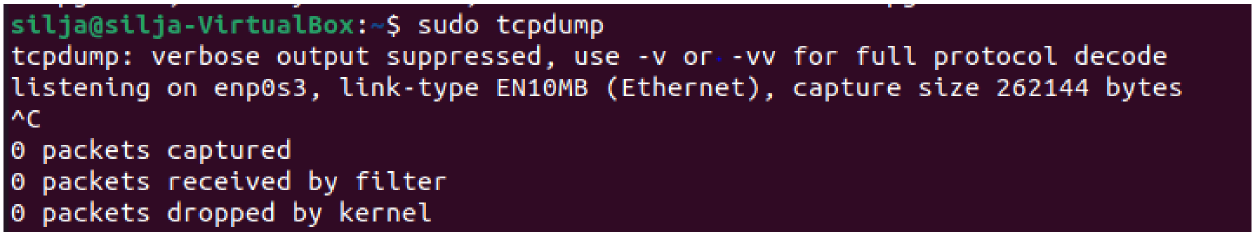
ROLL NO:20

1. Execute tcpdump and its options on your own system, and submit the output screenshot as a document.



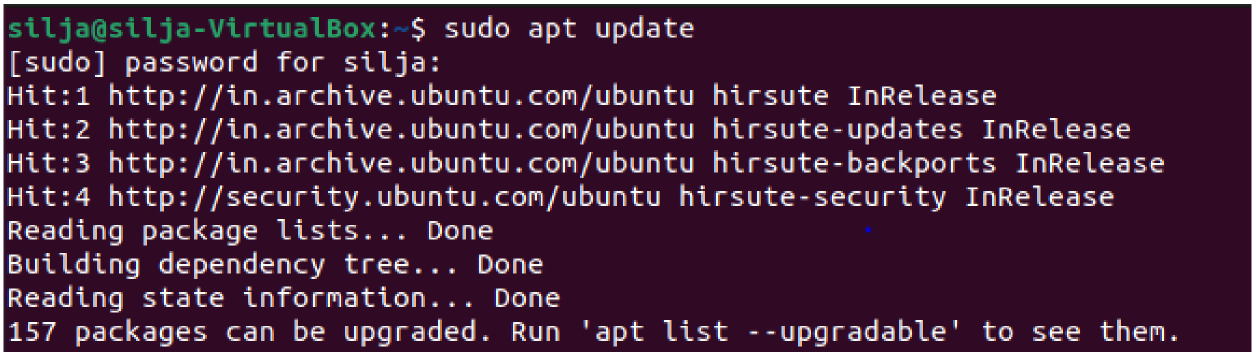
```
silja@silja-VirtualBox:~$ sudo apt install tcpdump
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
tcpdump is already the newest version (4.9.3-7).
tcpdump set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 157 not upgraded.
```

- Sudo tcpdump



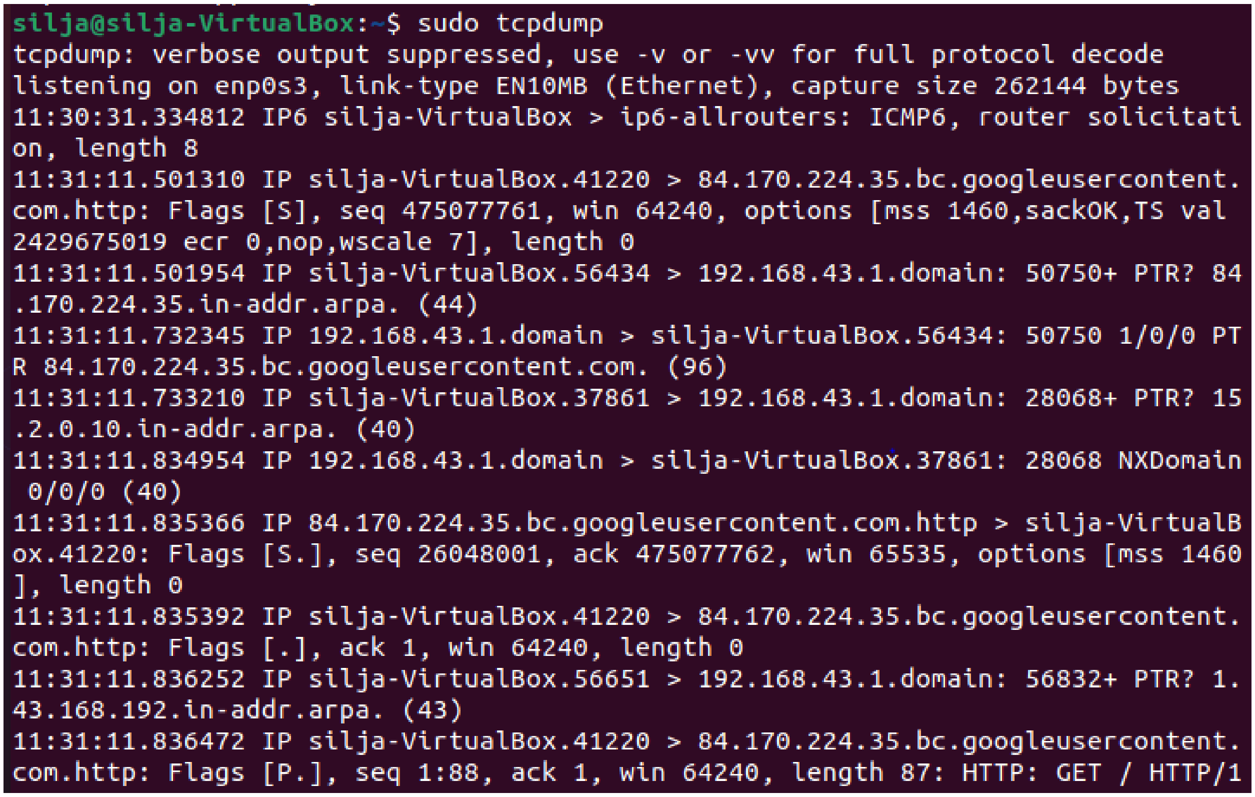
```
silja@silja-VirtualBox:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

- Sudo apt update



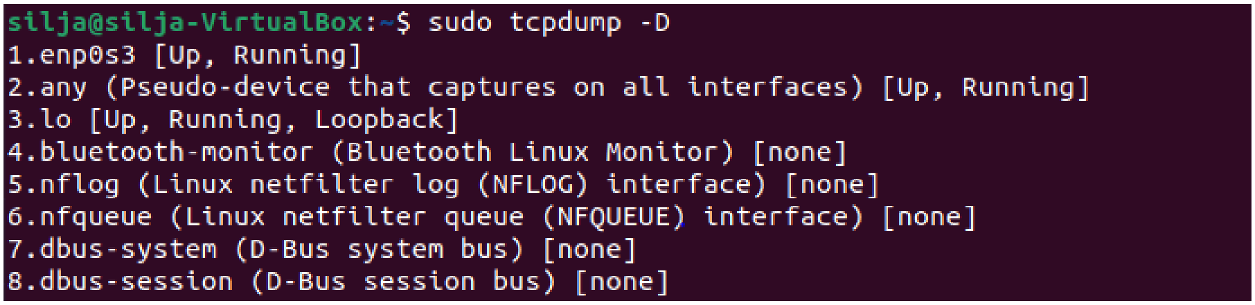
```
silja@silja-VirtualBox:~$ sudo apt update
[sudo] password for silja:
Hit:1 http://in.archive.ubuntu.com/ubuntu hirsute InRelease
Hit:2 http://in.archive.ubuntu.com/ubuntu hirsute-updates InRelease
Hit:3 http://in.archive.ubuntu.com/ubuntu hirsute-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu hirsute-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
157 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Sudo tcpdump



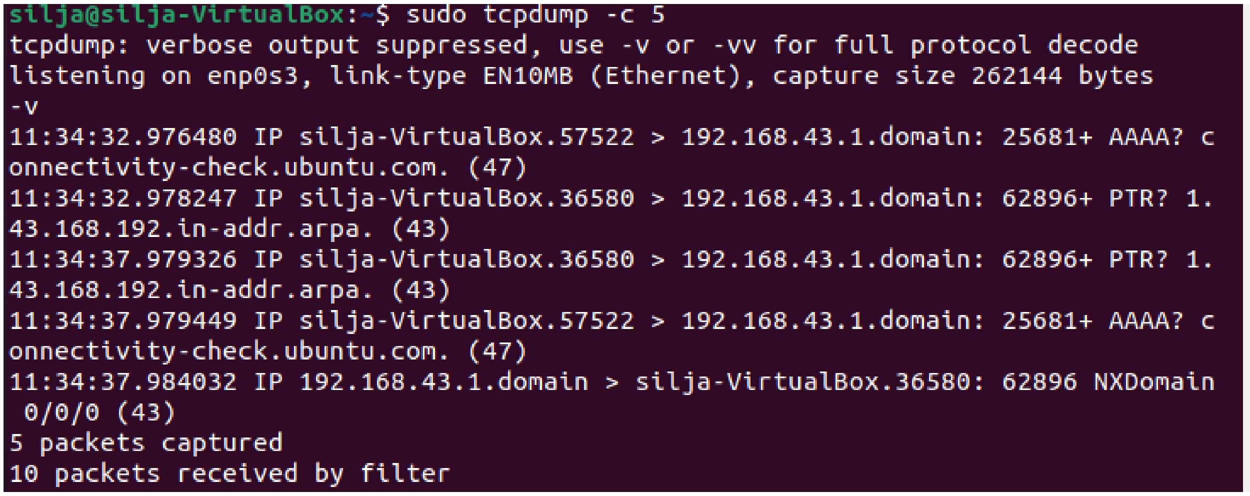
```
silja@silja-VirtualBox:~$ sudo tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
11:30:31.334812 IP6 silja-VirtualBox > ip6-allrouters: ICMP6, router solicitati
on, length 8
11:31:11.501310 IP silja-VirtualBox.41220 > 84.170.224.35.bc.googleusercontent.
com.http: Flags [S], seq 475077761, win 64240, options [mss 1460,sackOK,TS val
2429675019 ecr 0,nop,wscale 7], length 0
11:31:11.501954 IP silja-VirtualBox.56434 > 192.168.43.1.domain: 50750+ PTR? 84
.170.224.35.in-addr.arpa. (44)
11:31:11.732345 IP 192.168.43.1.domain > silja-VirtualBox.56434: 50750 1/0/0 PT
R 84.170.224.35.bc.googleusercontent.com. (96)
11:31:11.733210 IP silja-VirtualBox.37861 > 192.168.43.1.domain: 28068+ PTR? 15
.2.0.10.in-addr.arpa. (40)
11:31:11.834954 IP 192.168.43.1.domain > silja-VirtualBox.37861: 28068 NXDomain
 0/0/0 (40)
11:31:11.835366 IP 84.170.224.35.bc.googleusercontent.com.http > silja-VirtualB
ox.41220: Flags [S.], seq 26048001, ack 475077762, win 65535, options [mss 1460
], length 0
11:31:11.835392 IP silja-VirtualBox.41220 > 84.170.224.35.bc.googleusercontent.
com.http: Flags [.], ack 1, win 64240, length 0
11:31:11.836252 IP silja-VirtualBox.56651 > 192.168.43.1.domain: 56832+ PTR? 1.
43.168.192.in-addr.arpa. (43)
11:31:11.836472 IP silja-VirtualBox.41220 > 84.170.224.35.bc.googleusercontent.
com.http: Flags [P.], seq 1:88, ack 1, win 64240, length 87: HTTP: GET / HTTP/1
```

Sudo tcpdump -D



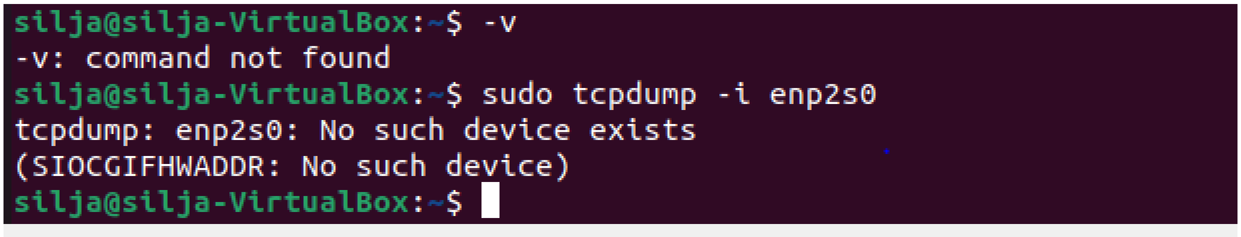
```
silja@silja-VirtualBox:~$ sudo tcpdump -D
1.enp0s3 [Up, Running]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
7.dbus-system (D-Bus system bus) [none]
8.dbus-session (D-Bus session bus) [none]
```

Sudo tcpdump –c 5



```
silja@silja-VirtualBox:~$ sudo tcpdump -c 5
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
-v
11:34:32.976480 IP silja-VirtualBox.57522 > 192.168.43.1.domain: 25681+ AAAA? c
onnectivity-check.ubuntu.com. (47)
11:34:32.978247 IP silja-VirtualBox.36580 > 192.168.43.1.domain: 62896+ PTR? 1.
43.168.192.in-addr.arpa. (43)
11:34:37.979326 IP silja-VirtualBox.36580 > 192.168.43.1.domain: 62896+ PTR? 1.
43.168.192.in-addr.arpa. (43)
11:34:37.979449 IP silja-VirtualBox.57522 > 192.168.43.1.domain: 25681+ AAAA? c
onnectivity-check.ubuntu.com. (47)
11:34:37.984032 IP 192.168.43.1.domain > silja-VirtualBox.36580: 62896 NXDomain
 0/0/0 (43)
5 packets captured
10 packets received by filter
```

Sudo tcpdump –i enp2s0



```
silja@silja-VirtualBox:~$ -v
-v: command not found
silja@silja-VirtualBox:~$ sudo tcpdump -i enp2s0
tcpdump: enp2s0: No such device exists
(SIOCGIFHWADDR: No such device)
silja@silja-VirtualBox:~$ 
```