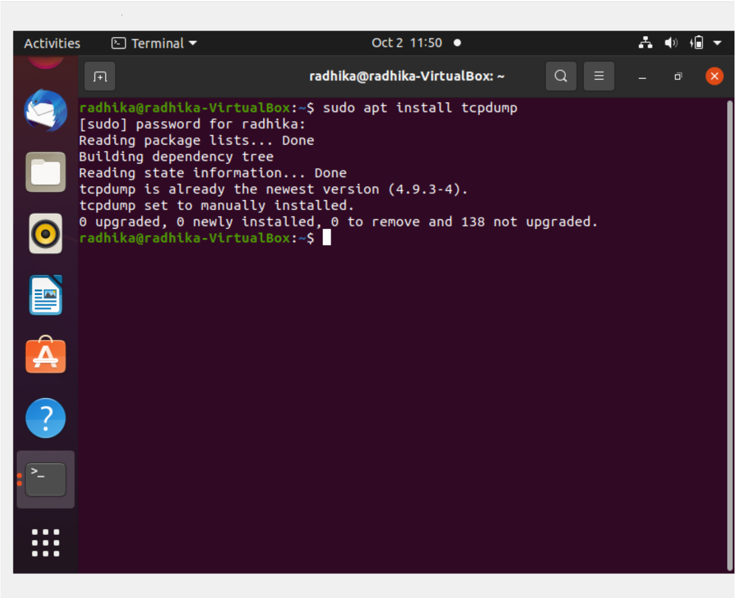
ASSIGNMENT

NETWORK AND SYSTEM ADMINISTRATION LAB

Radhika C
S2 RMCA B Batch
Roll no:13

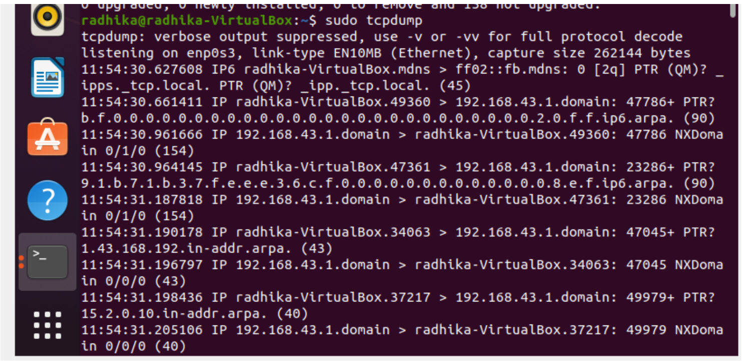
Installation of tcpdump

sudo apt install tcpdump

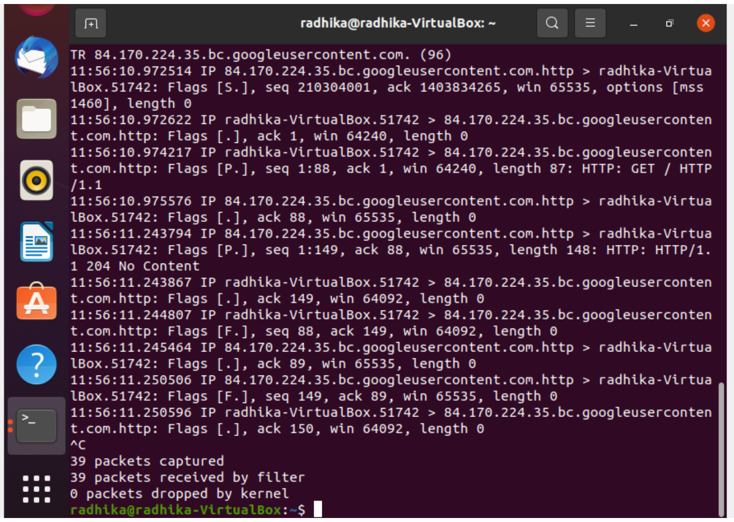


```
radhika@radhika-VirtualBox:~$ sudo apt install tcpdump
[sudo] password for radhika:
Reading package lists... Done
Building dependency tree
Reading state information... Done
tcpdump is already the newest version (4.9.3-4).
tcpdump set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 138 not upgraded.
radhika@radhika-VirtualBox:~$ 
```

Sudo tcpdump



```
0 upgraded, 0 newly installed, 0 to remove and 138 not upgraded.
radhika@radhika-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
11:54:30.627608 IP6 radhika-VirtualBox.mdns > ff02::fb.mdns: 0 [2q] PTR (QM)? _
ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
11:54:30.661411 IP radhika-VirtualBox.49360 > 192.168.43.1.domain: 47786+ PTR?
b.f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.f.f.ip6.arpa. (90)
11:54:30.961666 IP 192.168.43.1.domain > radhika-VirtualBox.49360: 47786 NXDoma
in 0/1/0 (154)
11:54:30.964145 IP radhika-VirtualBox.47361 > 192.168.43.1.domain: 23286+ PTR?
9.1.b.7.1.b.3.7.f.e.e.e.3.6.c.f.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.ip6.arpa. (90)
11:54:31.187818 IP 192.168.43.1.domain > radhika-VirtualBox.47361: 23286 NXDoma
in 0/1/0 (154)
11:54:31.190178 IP radhika-VirtualBox.34063 > 192.168.43.1.domain: 47045+ PTR?
1.43.168.192.in-addr.arpa. (43)
11:54:31.196797 IP 192.168.43.1.domain > radhika-VirtualBox.34063: 47045 NXDoma
in 0/0/0 (43)
11:54:31.198436 IP radhika-VirtualBox.37217 > 192.168.43.1.domain: 49979+ PTR?
15.2.0.10.in-addr.arpa. (40)
11:54:31.205106 IP 192.168.43.1.domain > radhika-VirtualBox.37217: 49979 NXDoma
in 0/0/0 (40)
```

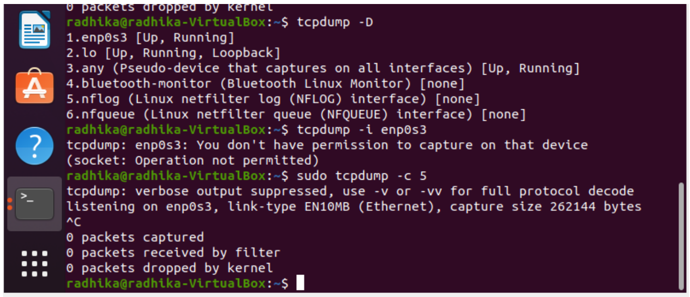


```
TR 84.170.224.35.bc.googleusercontent.com. (96)
11:56:10.972514 IP 84.170.224.35.bc.googleusercontent.com.http > radhika-Virtua
lBox.51742: Flags [S.], seq 210304001, ack 1403834265, win 65535, options [mss
1460], length 0
11:56:10.972622 IP radhika-VirtualBox.51742 > 84.170.224.35.bc.googleusercontent.com.http: Flags [.], ack 1, win 64240, length 0
11:56:10.974217 IP radhika-VirtualBox.51742 > 84.170.224.35.bc.googleuserconten
t.com.http: Flags [P.], seq 1:88, ack 1, win 64240, length 87: HTTP: GET / HTTP
/1.1
11:56:10.975576 IP 84.170.224.35.bc.googleusercontent.com.http > radhika-Virtua
lBox.51742: Flags [.], ack 88, win 65535, length 0
11:56:11.243794 IP 84.170.224.35.bc.googleusercontent.com.http > radhika-Virtua
lBox.51742: Flags [P.], seq 1:149, ack 88, win 65535, length 148: HTTP: HTTP/1.
1 204 No Content
11:56:11.243867 IP radhika-VirtualBox.51742 > 84.170.224.35.bc.googleuserconten
t.com.http: Flags [.], ack 149, win 64092, length 0
11:56:11.244807 IP radhika-VirtualBox.51742 > 84.170.224.35.bc.googleuserconten
t.com.http: Flags [F.], seq 88, ack 149, win 64092, length 0
11:56:11.245464 IP 84.170.224.35.bc.googleusercontent.com.http > radhika-Virtua
lBox.51742: Flags [.], ack 89, win 65535, length 0
11:56:11.250506 IP 84.170.224.35.bc.googleusercontent.com.http > radhika-Virtua
lBox.51742: Flags [F.], seq 149, ack 89, win 65535, length 0
11:56:11.250596 IP radhika-VirtualBox.51742 > 84.170.224.35.bc.googleuserconten
t.com.http: Flags [.], ack 150, win 64092, length 0
^C
39 packets captured
39 packets received by filter
0 packets dropped by kernel
radhika@radhika-VirtualBox:~$
```

tcpdump -D

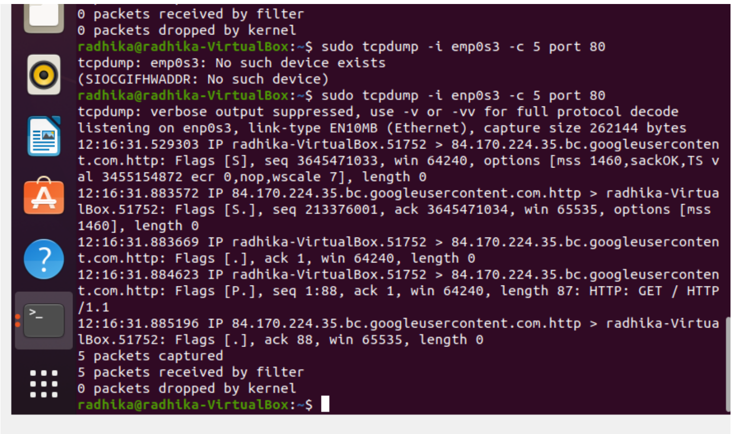
tcpdump –I emp0s3

sudo tcpdump –c 5



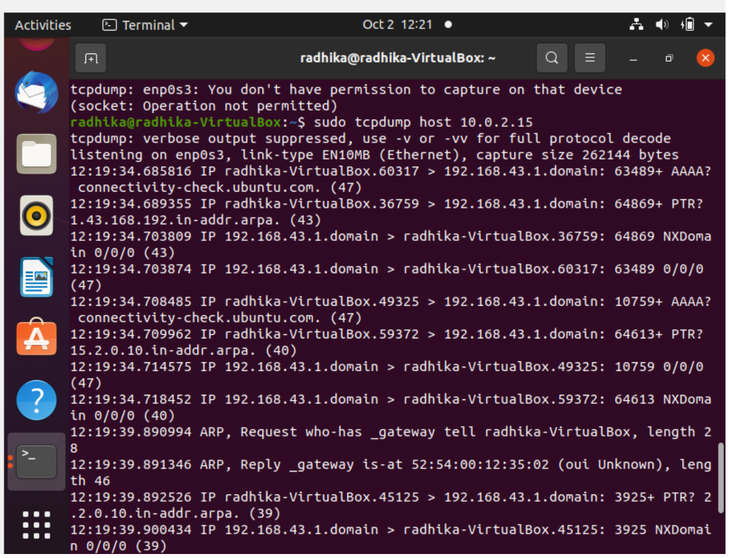
```
0 packets dropped by kernel
radhika@radhika-VirtualBox:~$ tcpdump -D
1.enp0s3 [Up, Running]
2.lo [Up, Running, Loopback]
3.any (Pseudo-device that captures on all interfaces) [Up, Running]
4.bluetooth-monitor (Bluetooth Linux Monitor) [none]
5.nflog (Linux netfilter log (NFLOG) interface) [none]
6.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
radhika@radhika-VirtualBox:~$ tcpdump -i enp0s3
tcpdump: enp0s3: You don't have permission to capture on that device
(socket: Operation not permitted)
radhika@radhika-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
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
radhika@radhika-VirtualBox:~$
```

Sudo tcpdump –i emp0s3 –c 5 port 80

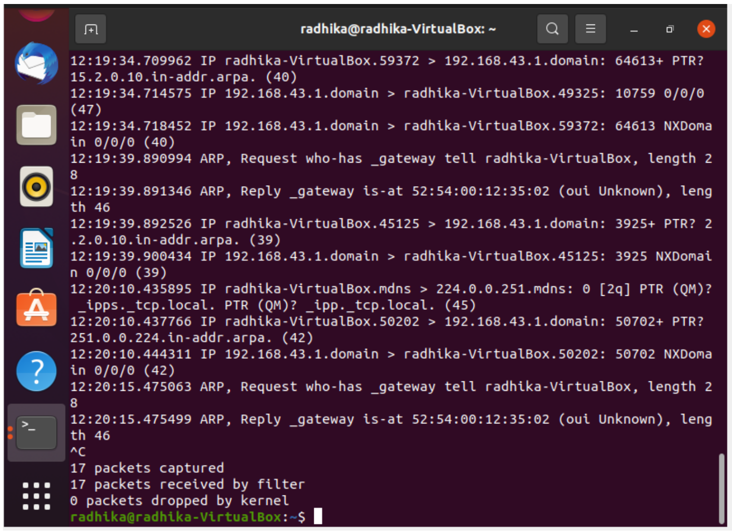


```
0 packets received by filter
0 packets dropped by kernel
radhika@radhika-VirtualBox:~$ sudo tcpdump -i emp0s3 -c 5 port 80
tcpdump: emp0s3: No such device exists
(SIOCGIFHWADDR: No such device)
radhika@radhika-VirtualBox:~$ sudo tcpdump -i enp0s3 -c 5 port 80
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
12:16:31.529303 IP radhika-VirtualBox.51752 > 84.170.224.35.bc.googleuserconten
t.com.http: Flags [S], seq 3645471033, win 64240, options [mss 1460,sackOK,TS v
al 3455154872 ecr 0,nop,wscale 7], length 0
12:16:31.883572 IP 84.170.224.35.bc.googleusercontent.com.http > radhika-Virtua
lBox.51752: Flags [S.], seq 213376001, ack 3645471034, win 65535, options [mss
1460], length 0
12:16:31.883669 IP radhika-VirtualBox.51752 > 84.170.224.35.bc.googleuserconten
t.com.http: Flags [.], ack 1, win 64240, length 0
12:16:31.884623 IP radhika-VirtualBox.51752 > 84.170.224.35.bc.googleuserconten
t.com.http: Flags [P.], seq 1:88, ack 1, win 64240, length 87: HTTP: GET / HTTP
/1.1
12:16:31.885196 IP 84.170.224.35.bc.googleusercontent.com.http > radhika-Virtua
lBox.51752: Flags [.], ack 88, win 65535, length 0
5 packets captured
5 packets received by filter
0 packets dropped by kernel
radhika@radhika-VirtualBox:~$
```

Sudo tcpdump host 10.0.2.15

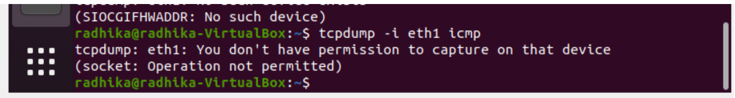


```
tcpdump: enp0s3: You don't have permission to capture on that device
(socket: Operation not permitted)
radhika@radhika-VirtualBox:~$ sudo tcpdump host 10.0.2.15
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
12:19:34.685816 IP radhika-VirtualBox.60317 > 192.168.43.1.domain: 63489+ AAAA?
 connectivity-check.ubuntu.com. (47)
12:19:34.689355 IP radhika-VirtualBox.36759 > 192.168.43.1.domain: 64869+ PTR?
1.43.168.192.in-addr.arpa. (43)
12:19:34.703809 IP 192.168.43.1.domain > radhika-VirtualBox.36759: 64869 NXDoma
in 0/0/0 (43)
12:19:34.703874 IP 192.168.43.1.domain > radhika-VirtualBox.60317: 63489 0/0/0
(47)
12:19:34.708485 IP radhika-VirtualBox.49325 > 192.168.43.1.domain: 10759+ AAAA?
 connectivity-check.ubuntu.com. (47)
12:19:34.709962 IP radhika-VirtualBox.59372 > 192.168.43.1.domain: 64613+ PTR?
15.2.0.10.in-addr.arpa. (40)
12:19:34.714575 IP 192.168.43.1.domain > radhika-VirtualBox.49325: 10759 0/0/0
(47)
12:19:34.718452 IP 192.168.43.1.domain > radhika-VirtualBox.59372: 64613 NXDoma
in 0/0/0 (40)
12:19:39.890994 ARP, Request who-has _gateway tell radhika-VirtualBox, length 2
8
12:19:39.891346 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), leng
th 46
12:19:39.892526 IP radhika-VirtualBox.45125 > 192.168.43.1.domain: 3925+ PTR? 2
.2.0.10.in-addr.arpa. (39)
12:19:39.900434 IP 192.168.43.1.domain > radhika-VirtualBox.45125: 3925 NXDomai
n 0/0/0 (39)
```



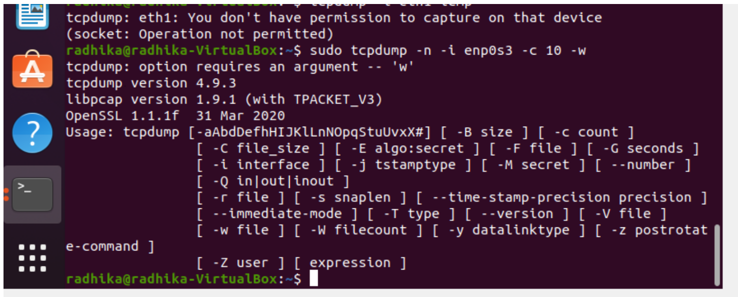
```
12:19:34.709962 IP radhika-VirtualBox.59372 > 192.168.43.1.domain: 64613+ PTR?
15.2.0.10.in-addr.arpa. (40)
12:19:34.714575 IP 192.168.43.1.domain > radhika-VirtualBox.49325: 10759 0/0/0
(47)
12:19:34.718452 IP 192.168.43.1.domain > radhika-VirtualBox.59372: 64613 NXDoma
in 0/0/0 (40)
12:19:39.890994 ARP, Request who-has _gateway tell radhika-VirtualBox, length 2
8
12:19:39.891346 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), leng
th 46
12:19:39.892526 IP radhika-VirtualBox.45125 > 192.168.43.1.domain: 3925+ PTR? 2
.2.0.10.in-addr.arpa. (39)
12:19:39.900434 IP 192.168.43.1.domain > radhika-VirtualBox.45125: 3925 NXDomai
n 0/0/0 (39)
12:20:10.435895 IP radhika-VirtualBox.mdns > 224.0.0.251.mdns: 0 [2q] PTR (QM)?
 _ipps._tcp.local. PTR (QM)? _ipp._tcp.local. (45)
12:20:10.437766 IP radhika-VirtualBox.50202 > 192.168.43.1.domain: 50702+ PTR?
251.0.0.224.in-addr.arpa. (42)
12:20:10.444311 IP 192.168.43.1.domain > radhika-VirtualBox.50202: 50702 NXDoma
in 0/0/0 (42)
12:20:15.475063 ARP, Request who-has _gateway tell radhika-VirtualBox, length 2
8
12:20:15.475499 ARP, Reply _gateway is-at 52:54:00:12:35:02 (oui Unknown), leng
th 46
^C
17 packets captured
17 packets received by filter
0 packets dropped by kernel
radhika@radhika-VirtualBox:~$
```

tcpdump -i ethi icmp



```
(SIOCGIFHWADDR: No such device)
radhika@radhika-VirtualBox:~$ tcpdump -i eth1 icmp
tcpdump: eth1: You don't have permission to capture on that device
(socket: Operation not permitted)
radhika@radhika-VirtualBox:~$
```

sudo tcpdump -n -i enp0s3 -c 10 -w



```
tcpdump: eth1: You don't have permission to capture on that device
(socket: Operation not permitted)
radhika@radhika-VirtualBox:~$ sudo tcpdump -n -i enp0s3 -c 10 -w
tcpdump: option requires an argument -- 'w'
tcpdump version 4.9.3
libpcap version 1.9.1 (with TPACKET_V3)
OpenSSL 1.1.1f  31 Mar 2020
Usage: tcpdump [-aAbdDefhHIJKlLnNOpqStuUvxX#] [ -B size ] [ -c count ]
                [ -C file_size ] [ -E algo:secret ] [ -F file ] [ -G seconds ]
                [ -i interface ] [ -j tstamptype ] [ -M secret ] [ --number ]
                [ -Q in|out|inout ]
                [ -r file ] [ -s snaplen ] [ --time-stamp-precision precision ]
                [ --immediate-mode ] [ -T type ] [ --version ] [ -V file ]
                [ -w file ] [ -W filecount ] [ -y datalinktype ] [ -z postrotat
e-command ]
                [ -Z user ] [ expression ]
radhika@radhika-VirtualBox:~$ 
```