

# Assignment 2

---

- **Name:** Arnab Sen
- **Roll:** 510519006
- **Gsuite:** [510519006.arnab@students.iiests.ac.in](mailto:510519006.arnab@students.iiests.ac.in)
- **Subject:** Computer Networks Lab (CS 3272)

## Question 1

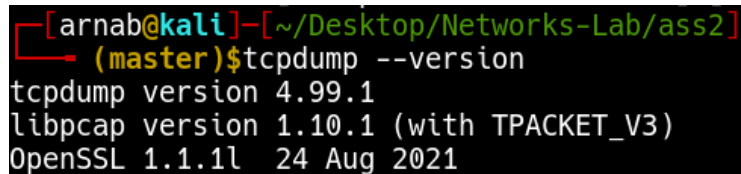
---

Check the version of the `tcpdump` and the `libpcap` utilities. Also, find the number of interfaces available with your computer. Switch the network of `eth0/eth1` (or the ethernet interface name as appeared) to promiscuous mode.

## Answer 1

---

```
tcpdump --version
```

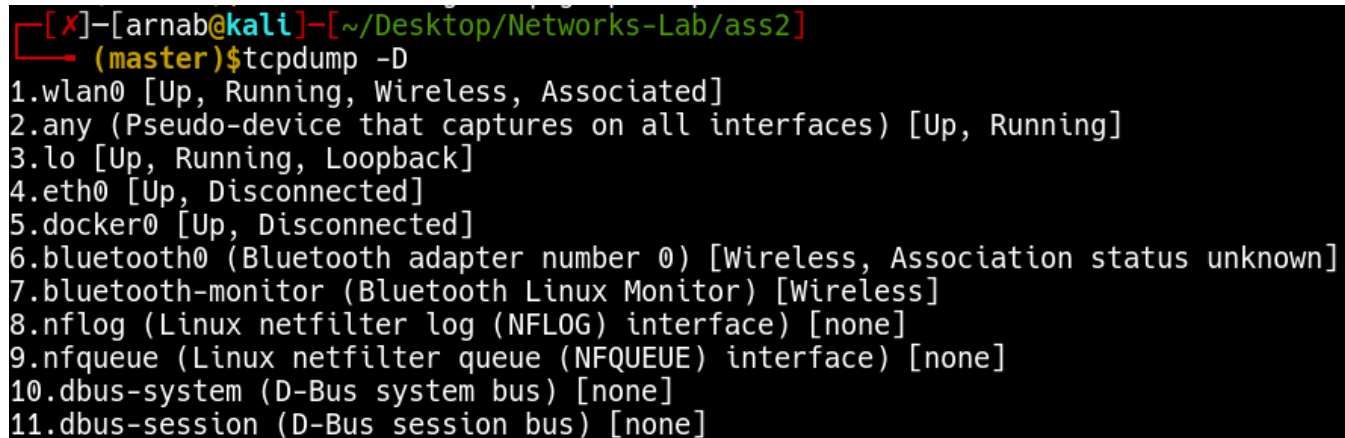


```
[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
(master)$tcpdump --version
tcpdump version 4.99.1
libpcap version 1.10.1 (with TPACKET_V3)
OpenSSL 1.1.1l 24 Aug 2021
```

- `tcpdump` version 4.99.1
- `libpcap` version 1.10.1

My network interfaces are:

```
tcpdump -D
```



```
[X]--[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
(master)$tcpdump -D
1.wlan0 [Up, Running, Wireless, Associated]
2.any (Pseudo-device that captures on all interfaces) [Up, Running]
3.lo [Up, Running, Loopback]
4.eth0 [Up, Disconnected]
5.docker0 [Up, Disconnected]
6.bluetooth0 (Bluetooth adapter number 0) [Wireless, Association status unknown]
7.bluetooth-monitor (Bluetooth Linux Monitor) [Wireless]
8.nflog (Linux netfilter log (NFLOG) interface) [none]
9.nfqueue (Linux netfilter queue (NFQUEUE) interface) [none]
10.dbus-system (D-Bus system bus) [none]
11.dbus-session (D-Bus session bus) [none]
```

So `wlan0` is my active interface. Enabled promiscuous mode of `wlan0`.

```
sudo ifconfig wlan0 promisc
sudo ifconfig -v | grep -i promisc
```

```
[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
(master)$sudo ifconfig wlan0 promisc
[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
(master)$sudo ifconfig -v | grep -i promisc
wlan0: flags=4419<UP,BROADCAST,RUNNING,PROMISC,MULTICAST> mtu 1500
```

## Question 2

---

Write the `tcpdump` command to capture 20 packets by listening to the promiscuous mode interface of your host and save the result as \*.pcap file (both with and without -n option).

## Answer 2

---

### Without -n option

```
sudo tcpdump -i wlan0 -c 20 -w capture1.pcap
```

```
[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
(master)$sudo tcpdump -i wlan0 -c 20 -w capture1.pcap
tcpdump: listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20 packets captured
143 packets received by filter
0 packets dropped by kernel
```

### With -n option

```
sudo tcpdump -n -i wlan0 -c 20 -w capture2.pcap
```

```
[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
(master)$sudo tcpdump -n -i wlan0 -c 20 -w capture2.pcap
tcpdump: listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
20 packets captured
79 packets received by filter
0 packets dropped by kernel
```

## Question 3

---

Read the above file and identify the different fields present in TCP/IP packets captured by `tcpdump`.

## Answer 3

---

To parse and read the content we use the `-r` tag.

```
tcpdump -r capture1.pcap
```

```
arnab@kali:~/Desktop/Networks-Lab/ass2]
(master)$tcpdump -r capture1.pcap
reading from file capture1.pcap, link-type EN10MB (Ethernet), snapshot length 262144
15:44:13.225178 IP kali.35626 > 74.125.250.13.19305: UDP, length 38
15:44:13.228633 IP kali.35626 > 74.125.250.13.19305: UDP, length 75
15:44:13.249125 IP a104-108-159-104.deploy.static.akamaitechnologies.com.https > kali.54610: Flags [.] , ack 2672421836, win 501, options [nop,nop,TS val 906379474 ecr 2384804085], length 0
15:44:13.249154 IP a104-108-159-104.deploy.static.akamaitechnologies.com.https > kali.54610: Flags [P.] , seq 0:454, ack 1, win 501, options [nop,nop,TS val 906379475 ecr 2384804085], length 454
15:44:13.249184 IP kali.54610 > a104-108-159-104.deploy.static.akamaitechnologies.com.https: Flags [.] , ack 454, win 498, options [nop,nop,TS val 2384804120 ecr 906379475], length 0
15:44:13.251063 IP kali.35626 > 74.125.250.13.19305: UDP, length 58
15:44:13.254429 IP kali.35626 > 74.125.250.13.19305: UDP, length 39
15:44:13.262156 IP bom12s12-in-f3.1e100.net.https > kali.45434: Flags [F.] , seq 149553653, ack 2120560349, win 261, options [nop,nop,TS val 1610047752 ecr 655262852], length 0
15:44:13.264349 IP 103.231.98.195.https > kali.36440: Flags [.] , ack 511917729, win 3835, options [nop,nop,TS val 1823346139 ecr 572194933], length 0
15:44:13.264373 IP 103.231.98.195.https > kali.36440: Flags [P.] , seq 0:6, ack 1, win 3835, options [nop,nop,TS val 1823346139 ecr 572194933], length 6
15:44:13.264389 IP kali.36440 > 103.231.98.195.https: Flags [.] , ack 6, win 501, options [nop,nop,TS val 572195207 ecr 1823346139], length 0
15:44:13.264418 IP 103.231.98.195.https > kali.36440: Flags [P.] , seq 6:51, ack 1, win 3835, options [nop,nop,TS val 1823346139 ecr 572194933], length 45
15:44:13.264426 IP kali.36440 > 103.231.98.195.https: Flags [.] , ack 51, win 501, options [nop,nop,TS val 572195207 ecr 1823346139], length 0
15:44:13.264434 IP 103.231.98.195.https > kali.36440: Flags [P.] , seq 51:107, ack 1, win 3835, options [nop,nop,TS val 1823346139 ecr 572194933], length 56
15:44:13.264440 IP kali.36440 > 103.231.98.195.https: Flags [.] , ack 107, win 501, options [nop,nop,TS val 572195207 ecr 1823346139], length 0
15:44:13.264448 IP 103.231.98.195.https > kali.36440: Flags [P.] , seq 107:145, ack 1, win 3835, options [nop,nop,TS val 1823346139 ecr 572194933], length 38
15:44:13.264453 IP kali.36440 > 103.231.98.195.https: Flags [.] , ack 145, win 501, options [nop,nop,TS val 572195207 ecr 1823346139], length 0
15:44:13.264460 IP 103.231.98.195.https > kali.36440: Flags [P.] , ack 581, win 3980, options [nop,nop,TS val 1823346140 ecr 572194934], length 0
15:44:13.264712 IP kali.36440 > 103.231.98.195.https: Flags [P.] , seq 581:610, ack 145, win 501, options [nop,nop,TS val 572195207 ecr 1823346140], length 38
15:44:13.269081 IP 103.231.98.195.https > kali.36440: Flags [P.] , seq 145:370, ack 581, win 3980, options [nop,nop,TS val 1823346144 ecr 572194934], length 225
```

```
tcpdump -r capture2.pcap
```

```
arnab@kali:~/Desktop/Networks-Lab/ass2]
(master)$tcpdump -r capture2.pcap
reading from file capture2.pcap, link-type EN10MB (Ethernet), snapshot length 262144
16:02:00.424504 IP 104.16.70.125.https > kali.36356: Flags [P.] , seq 3996260114:3996260153, ack 3435171818, win 73, length 39
16:02:00.424540 IP 104.16.70.125.https > kali.36356: Flags [P.] , seq 39:63, ack 1, win 73, length 24
16:02:00.424547 IP 104.16.70.125.https > kali.36356: Flags [F.] , seq 63, ack 1, win 73, length 0
16:02:00.424678 IP kali.36356 > 104.16.70.125.https: Flags [.] , ack 64, win 3483, length 0
16:02:00.424870 IP kali.36356 > 104.16.70.125.https: Flags [F.] , seq 1, ack 64, win 3483, length 0
16:02:00.464363 IP 104.16.70.125.https > kali.36356: Flags [.] , ack 2, win 73, length 0
16:02:02.058783 IP kali.51460 > 104.22.71.197.https: Flags [F.] , ack 3804549102, win 501, length 0
16:02:02.058824 IP kali.44144 > 103.216.204.11.https: Flags [.] , ack 3331014840, win 501, options [nop,nop,TS val 1586012541 ecr 3272069031], length 0
16:02:02.058837 IP kali.49700 > server-65-8-0-209.ccu50.r.cloudfront.net.https: Flags [F.] , ack 3595031057, win 501, options [nop,nop,TS val 3289045758 ecr 3705420271], length 0
16:02:02.058848 IP kali.39058 > 13.107.42.14.https: Flags [.] , ack 118821128, win 501, length 0
16:02:02.068250 IP 103.216.204.11.https > kali.44144: Flags [F.] , ack 1, win 246, options [nop,nop,TS val 3272114088 ecr 1585921527], length 0
16:02:02.068274 IP server-65-8-0-209.ccu50.r.cloudfront.net.https > kali.49700: Flags [F.] , ack 1, win 7, options [nop,nop,TS val 3705465327 ecr 3288954967], length 0
16:02:02.093754 IP 13.107.42.14.https > kali.39058: Flags [F.] , ack 1, win 2052, length 0
16:02:02.098058 IP 104.22.71.197.https > kali.51460: Flags [F.] , ack 1, win 70, length 0
16:02:02.939265 IP 13.67.9.5.https > kali.38670: Flags [R.] , seq 515718133, ack 44061616, win 0, length 0
16:02:04.102765 IP kali.59910 > 104.18.100.194.https: Flags [F.] , ack 1608868348, win 501, length 0
16:02:04.102789 IP kali.42366 > 199.232.254.137.https: Flags [F.] , ack 4243841041, win 501, options [nop,nop,TS val 2336754415 ecr 3470124656], length 0
16:02:04.102795 IP kali.43492 > server-54-230-237-19.ccu50.r.cloudfront.net.https: Flags [F.] , ack 8077873, win 501, options [nop,nop,TS val 4027449878 ecr 3347868021], length 0
16:02:04.112583 IP server-54-230-237-19.ccu50.r.cloudfront.net.https > kali.43492: Flags [F.] , ack 1, win 10, options [nop,nop,TS val 3347913429 ecr 4027359459], length 0
16:02:04.141660 IP 104.18.100.194.https > kali.59910: Flags [F.] , ack 1, win 71, length 0
```

Taking look at one packet from capture1.pcap :

```
15:44:13.249154 IP a104-108-159-104.deploy.static.akamaitechnologies.com.https > kali.54610:
Flags [P.] , seq 0:454, ack 1, win 501, options [nop,nop,TS val 906379475 ecr 2384804085], length 454
```

Data	Description
15:44:13.249154	timestamp of the received packet as per the local clock.
IP	IP represents the network layer protocol—in this case, IPv4 .
a104-108-159-104.deploy.static.akamaitechnologies.com.https	source, since we didn't use the -n tag it shows the name instead of IP and PORT
kali.54610	destination, this is my local kali machine
Flags [P.]	P represents PUSH and . represents ACK hence [P.] means PUSH-ACK
seq 0:454	sequence number
ack 1	Ack Number which is 1 since this is the side sending data. For the side receiving data, this field represents the next expected byte (data) on this flow.
win 501	Window Size, which represents the number of bytes available in the receiving buffer
length 454	Packet Length, which represents the length, in bytes, of the payload data.

## Question 4

Extract packet arrival time, source IP address, destination IP address and port.

## Answer 4

---

```
$ tcpdump -tttt -n -r capture2.pcap -c 1
2022-01-18 16:02:00.424504 IP 104.16.70.125.443 > 192.168.1.4.36356:
Flags [P.], seq 3996260114:3996260153, ack 3435171818, win 73, length 39
```

```
[arnab@kali]~/Desktop/Networks-Lab/ass2
(master)$tcpdump -tttt -n -r capture2.pcap -c 1
reading from file capture2.pcap, link-type EN10MB (Ethernet), snapshot length 262144
2022-01-18 16:02:00.424504 IP 104.16.70.125.443 > 192.168.1.4.36356: Flags [P.], seq 3996260114:3996260153, ack 3435171818, win 73, length 39
```

- packet arrival time: 2022-01-18 16:02:00.424504
- source IP address is 104.16.70.125 and PORT is 443
- destination IP address is 192.168.1.4 and PORT is 36356

## Question 5

---

Extract source MAC address and destination MAC addresses.

## Answer 5

---

To get MAC address we use the `-e` tag.

```
$ tcpdump -tttt -en -r capture2.pcap -c 1
2022-01-18 16:02:00.424504 7c:a9:6b:33:c3:d6 > 24:ee:9a:81:09:25, ethertype IPv4 (0x0800), length 93:
104.16.70.125.443 > 192.168.1.4.36356: Flags [P.], seq 3996260114:3996260153, ack 3435171818, win 73, length 39
```

```
[arnab@kali]~/Desktop/Networks-Lab/ass2
(master)$tcpdump -tttt -en -r capture2.pcap -c 1
reading from file capture2.pcap, link-type EN10MB (Ethernet), snapshot length 262144
2022-01-18 16:02:00.424504 7c:a9:6b:33:c3:d6 > 24:ee:9a:81:09:25, ethertype IPv4 (0x0800), length 93: 104.16.70.125.443 > 192.168.1.4.36356: Flags
[P.], seq 3996260114:3996260153, ack 3435171818, win 73, length 39
```

- Source MAC address: 7c:a9:6b:33:c3:d6
- Destination MAC address: 24:ee:9a:81:09:25

## Question 6

---

Get the inter-arrival times while capturing packets.

## Answer 6

---

The `-ttt` tag allows us to capture packets and show inter-arrival time instead of arrival time in result.

```
sudo tcpdump -ttt
```

```

[~][X]-[arnab@kali]-[~/Desktop/Networks-Lab/ass2]
(master)$sudo tcpdump -ttt
[sudo] password for arnab:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
00:00:00.000000 IP 74.125.250.13.19305 > kali.35626: UDP, length 75
00:00:00.013746 IP kali.35626 > 74.125.250.13.19305: UDP, length 38
00:00:00.002308 IP 74.125.250.13.19305 > kali.35626: UDP, length 39
00:00:00.047806 IP kali.35626 > 74.125.250.13.19305: UDP, length 38
00:00:00.000260 IP kali.35626 > 74.125.250.13.19305: UDP, length 58
00:00:00.010123 IP kali.49647 > 10.10.0.1.domain: 43457+ PTR? 4.1.168.192.in-addr.arpa. (42)
00:00:00.005718 IP kali.35626 > 74.125.250.13.19305: UDP, length 58
00:00:00.038351 IP 10.10.0.1.domain > kali.49647: 43457 NXDomain 0/0/0 (42)
00:00:00.000478 IP kali.47990 > 10.10.0.1.domain: 38828+ PTR? 13.250.125.74.in-addr.arpa. (44)
00:00:00.005681 IP kali.35626 > 74.125.250.13.19305: UDP, length 58
00:00:00.037943 IP 10.10.0.1.domain > kali.47990: 38828 NXDomain 0/1/0 (104)
00:00:00.015038 IP kali.56660 > 10.10.0.1.domain: 22587+ PTR? 1.0.10.10.in-addr.arpa. (40)
00:00:00.044474 IP 10.10.0.1.domain > kali.56660: 22587 NXDomain 0/0/0 (40)

```

## Question 7

Use `tcpdump` to capture HTTP/HTTPS request and reply from `www.google.com`. Also print the packet content in ASCII format.

## Answer 7

Since we want only HTTP/HTTPS requests so the port should be either `80` or `443`. We also have to specify the request source and destination as `www.google.com`. For printing the content in ASCII format we use the `-A` tag.

```
sudo tcpdump -A '(dst www.google.com or src www.google.com) and (port 80 or port 443)'
```

```

[arnab@kali]-[~/Desktop/Networks-Lab/ass2]
(master)$sudo tcpdump -A '(dst www.google.com or src www.google.com) and (port 80 or port 443)'
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
17:17:20.684320 IP kali.34396 > bom05s15-in-f4.1e100.net.https: UDP, length 290
E..>..@.@.....D.\...*.Zx...V...rk...~wy...3...4...'.8...tW.B..W...6M.....(.5.E@(.t..{.....&...z....)Nk
W..A.Xj9W....S..m.s/.....7.....Q....
..og....\.....$......J.mF..^.#m.m.....n....."uk.D.V...1..P86..A'cPL....[H.....n.|.o.F.B...4@..6Tk.FQ....H.Z...J...7.....&904..n....I
J.e...%.5
17:17:20.743785 IP kali.34396 > bom05s15-in-f4.1e100.net.https: UDP, length 33
E..=.@.@.....D.\...).Lx...V.....8..z..J..#.&|.j...
17:17:20.795143 IP kali.34396 > bom05s15-in-f4.1e100.net.https: UDP, length 39
E..C..@.@.....D.\.../.Lx...V....../..j..{.....eY2...6.....`....
17:17:20.806691 IP kali.34396 > bom05s15-in-f4.1e100.net.https: UDP, length 33
E..=.@.@.....D.\...).Ux...V..hvjv....(...Fs.2....I..
^C
4 packets captured
14 packets received by filter
0 packets dropped by kernel

```

## Question 8

For each command, use `tcpdump` to capture the associated packets, and explain the different fields of each request and reply: (i) `ping` (ii) `wget` (iii) `traceroute`.

## Answer 8

Running the corresponding command and the `tcpdump` simultaneously.

**ping**

```

[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
→ (master)$sudo tcpdump host www.github.com
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:20:34.744273 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 47531, seq 1, length 64
10:20:34.786154 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com > kali: ICMP echo reply, id 47531, seq 1, length 64
10:20:35.745544 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 47531, seq 2, length 64
10:20:35.789088 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com > kali: ICMP echo reply, id 47531, seq 2, length 64
10:20:36.746827 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 47531, seq 3, length 64
10:20:36.789193 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com > kali: ICMP echo reply, id 47531, seq 3, length 64
10:20:37.748388 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 47531, seq 4, length 64
10:20:37.791340 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com > kali: ICMP echo reply, id 47531, seq 4, length 64
10:20:38.750158 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 47531, seq 5, length 64
10:20:38.795410 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com > kali: ICMP echo reply, id 47531, seq 5, length 64
10:20:43.841795 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 36168, seq 1, length 64
10:20:43.884208 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com > kali: ICMP echo reply, id 36168, seq 1, length 64
10:20:44.842843 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 36168, seq 2, length 64
10:20:44.885320 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com > kali: ICMP echo reply, id 36168, seq 2, length 64
^C
14 packets captured
18 packets received by filter
0 packets dropped by kernel
[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
→ (master)$

/bin/bash 158x16
→ (master)$ping www.github.com
PING github.com (13.234.210.38) 56(84) bytes of data.
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=1 ttl=47 time=42.5 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=2 ttl=47 time=42.5 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=3 ttl=47 time=42.6 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=4 ttl=47 time=43.2 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=5 ttl=47 time=42.5 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=6 ttl=47 time=43.3 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=7 ttl=47 time=41.7 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=8 ttl=47 time=42.5 ms
^C
--- github.com ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7009ms
rtt min/avg/max/mdev = 41.650/42.604/43.318/0.479 ms

```

We know that `ping` uses the ICMP protocol and we can see in `tcpdump` that the requests from my machine are `icmp echo request` and the corresponding response is `icmp echo reply`.

```

10:20:34.744273 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com:
    ICMP echo request, id 47531, seq 1, length 64
10:20:34.786154 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com > kali:
    ICMP echo reply, id 47531, seq 1, length 64

```

In the first request the source is `kali` and the destination is `ec2-13-234-210-38.ap-south-1.compute.amazonaws.com` which is the github server. The protocol used is `ICMP` because it was `ping` command. And the packet length is `64` which is the default packet length for `ping`.

In the second reply the source is the github.com server `ec2-13-234-210-38.ap-south-1.compute.amazonaws.com` and the destination is `kali`. Everything else is the same.

## wget



```
arnab@kali:~/Desktop/Networks-Lab/ass2
(master)$ sudo tcpdump host www.github.com
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on wlan0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
10:27:52.701414 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [S], seq 3180707483, win 64240, options [mss 1460,sackOK,TS val 3886262508 ecr 0,nop,wscale 7], length 0
10:27:52.746862 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https > kali.40416: Flags [S.], seq 1198877882, ack 3180707484, win 65535, options [mss 1436,sackOK,TS val 66019864 ecr 3886262508,nop,wscale 10], length 0
10:27:52.746930 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [.], ack 1, win 502, options [nop,nop,TS val 3886262553 ecr 66019864], length 0
10:27:52.747855 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [P.], seq 1:518, ack 1, win 502, options [nop,nop,TS val 3886262554 ecr 66019864], length 517
10:27:52.794038 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https > kali.40416: Flags [P.], seq 1:2754, ack 518, win 66, options [nop,nop,TS val 66019911 ecr 3886262554], length 2753
10:27:52.794099 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [.], ack 2754, win 481, options [nop,nop,TS val 3886262600 ecr 66019911], length 0
10:27:52.795001 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [P.], seq 518:524, ack 2754, win 481, options [nop,nop,TS val 3886262601 ecr 66019911], length 6
10:27:52.879727 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https > kali.40416: Flags [.], ack 524, win 66, options [nop,nop,TS val 66019997 ecr 3886262601], length 0
10:27:52.879771 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [P.], seq 524:731, ack 2754, win 501, options [nop,nop,TS val 3886262686 ecr 66019997], length 207
10:27:52.924105 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https > kali.40416: Flags [.], ack 731, win 67, options [nop,nop,TS val 66020042 ecr 3886262686], length 0
10:27:52.924138 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https > kali.40416: Flags [P.], seq 2754:2833, ack 731, win 67, options [nop,nop,TS val 66020042 ecr 3886262686], length 79
10:27:52.924156 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [.], ack 2833, win 501, options [nop,nop,TS val 3886262730 ecr 66020042], length 0
10:27:52.924196 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https > kali.40416: Flags [P.], seq 2833:2912, ack 731, win 67, options [nop,nop,TS val 66020042 ecr 3886262686], length 79
10:27:52.924205 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [.], ack 2912, win 501, options [nop,nop,TS val 3886262730 ecr 66020042], length 0
^C
[~]-[arnab@kali:~/Desktop/Networks-Lab/ass2]
(master)$ wget www.github.com -O /tmp/index.html
URL transformed to HTTPS due to an HSTS policy
--2022-01-19 10:27:52-- https://www.github.com/
Resolving www.github.com (www.github.com)... 13.234.210.38
Connecting to www.github.com (www.github.com)[13.234.210.38]:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://github.com/ [following]
--2022-01-19 10:27:52-- https://github.com/
Resolving github.com (github.com)... 13.234.210.38
Connecting to github.com (github.com)[13.234.210.38]:443... connected.
```

Going through the first few packets:

```
10:27:52.701414 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [S],
seq 3180707483, win 64240, options [mss 1460,sackOK,TS val 3886262508 ecr 0,nop,wscale 7], length 0
10:27:52.746862 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https > kali.40416: Flags [S.],
seq 1198877882, ack 3180707484, win 65535, options [mss 1436,sackOK,TS val 66019864 ecr,nop,wscale 10], length 0
10:27:52.746930 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [.],
ack 1, win 502, options [nop,nop,TS val 3886262553 ecr 66019864], length 0
10:27:52.747855 IP kali.40416 > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https: Flags [P.],
seq 1:518, ack 1, win 502, options [nop,nop,TS val 3886262554 ecr 66019864], length 517
10:27:52.794038 IP ec2-13-234-210-38.ap-south-1.compute.amazonaws.com.https > kali.40416: Flags [P.],
seq 1:2754, ack 518, win 66, options [nop,nop,TS val 66019911 ecr 3886262554], length 2753
```

Packet #	Source	Destination	Packet type	Packet Length
1	kali	ec2-13-234-210-38.ap-south-1.compute.amazonaws.com	HTTPS request with SYN flag	0
2	ec2-13-234-210-38.ap-south-1.compute.amazonaws.com	kali	HTTPS reply with SYN-ACK flag	0
3	kali	ec2-13-234-210-38.ap-south-1.compute.amazonaws.com	HTTPS request with ACK flag	0
4	kali	ec2-13-234-210-38.ap-south-1.compute.amazonaws.com	HTTPS request with PUSH-ACK flag	517
5	ec2-13-234-210-38.ap-south-1.compute.amazonaws.com	kali	HTTPS reply with PUSH-ACK flag	2753

## traceroute

```

11:21:47.696631 IP 10.10.0.1.domain > kali.57211: 58638 1/1/0 CNAME github.com. (130)
11:21:47.698829 IP 10.10.0.1.domain > kali.57211: 7174 2/0/0 CNAME github.com., A 13.234.210.38 (62)
11:21:47.699343 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 1, length 40
11:21:47.699394 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 2, length 40
11:21:47.699411 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 3, length 40
11:21:47.699429 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 4, length 40
11:21:47.699443 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 5, length 40
11:21:47.699458 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 6, length 40
11:21:47.699476 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 7, length 40
11:21:47.699490 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 8, length 40
11:21:47.699505 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 9, length 40
11:21:47.699521 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 10, length 40
11:21:47.699537 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 11, length 40
11:21:47.699553 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 12, length 40
11:21:47.699570 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 13, length 40
11:21:47.699584 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 14, length 40
11:21:47.699597 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 15, length 40
11:21:47.699615 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 16, length 40
11:21:47.705001 IP 10.10.0.5 > kali: ICMP time exceeded in-transit, length 68
11:21:47.705001 IP 103.10.208.13 > kali: ICMP time exceeded in-transit, length 36
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.705399 IP kali.36202 > 10.10.0.1.domain: 53279+ PTR? 1.1.168.192.in-addr.arpa. (42)
11:21:47.707406 IP 172.29.30.1 > kali: ICMP time exceeded in-transit, length 36
11:21:47.744860 IP 103.27.170.190 > kali: ICMP time exceeded in-transit, length 36
11:21:47.752567 IP 10.10.0.1.domain > kali.36202: 53279 NXDomain 0/0/0 (42)
11:21:47.754543 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 17, length 40
11:21:47.754602 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 18, length 40
11:21:47.754636 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 19, length 40
11:21:47.754661 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 20, length 40
11:21:47.754685 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com: ICMP echo request, id 63001, seq 21, length 40
11:21:47.754960 IP kali.43891 > 10.10.0.1.domain: 25496+ PTR? 1.30.29.172.in-addr.arpa. (42)
11:21:47.706700 IP 52.95.66.156 > kali: ICMP time exceeded in-transit, length 148
/bin/bash158x6

traceroute to www.github.com (13.234.210.38), 30 hops max, 60 byte packets
 1 _gateway (192.168.1.1) 5.769 ms 5.686 ms 5.666 ms
 2 * * 172.29.30.1 (172.29.30.1) 7.953 ms
 3 10.10.0.5 (10.10.0.5) 5.531 ms * *
 4 103.10.208.13 (103.10.208.13) 5.485 ms * *
 5 * * *
 6 103.27.170.190 (103.27.170.190) 45.250 ms 44.700 ms *

```

Since I am using `traceroute` with `-I` it will send `ICMP` requests and we can see that. If we analyse the packets we see first a DNS resolution happens.

```

11:21:47.696631 IP 10.10.0.1.domain > kali.57211: 58638 1/1/0 CNAME github.com. (130)
11:21:47.698829 IP 10.10.0.1.domain > kali.57211: 7174 2/0/0 CNAME github.com., A 13.234.210.38 (62)

```

Then some `ICMP ECHO` requests are sent.

```

11:21:47.699343 IP kali > ec2-13-234-210-38.ap-south-1.compute.amazonaws.com:
    ICMP echo request, id 63001, seq 1, length 40

```

Few of them respond with `ICMP time exceeded in-transit` which is expected since that's how `traceroute` works.

```

11:21:47.705001 IP 10.10.0.5 > kali: ICMP time exceeded in-transit, length 68
11:21:47.705001 IP 103.10.208.13 > kali: ICMP time exceeded in-transit, length 36
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.707406 IP 172.29.30.1 > kali: ICMP time exceeded in-transit, length 36
11:21:47.744860 IP 103.27.170.190 > kali: ICMP time exceeded in-transit, length 36
11:21:47.796708 IP 52.95.66.156 > kali: ICMP time exceeded in-transit, length 148
11:21:47.799213 IP 103.27.170.190 > kali: ICMP time exceeded in-transit, length 36
11:21:50.015732 IP 52.95.64.186 > kali: ICMP time exceeded in-transit, length 36
11:21:50.023428 IP 99.83.76.135 > kali: ICMP time exceeded in-transit, length 148
11:21:50.113708 IP 99.83.76.142 > kali: ICMP time exceeded in-transit, length 36

```



```

[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
(master)$sudo tcpdump host 192.168.1.4 -r trace.pcap | grep -i 'ICMP time exceeded in-transit'
reading from file trace.pcap, link-type EN10MB (Ethernet), snapshot length 262144
11:21:47.705001 IP 10.10.0.5 > kali: ICMP time exceeded in-transit, length 68
11:21:47.705001 IP 103.10.208.13 > kali: ICMP time exceeded in-transit, length 36
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.705071 IP _gateway > kali: ICMP time exceeded in-transit, length 68
11:21:47.707406 IP 172.29.30.1 > kali: ICMP time exceeded in-transit, length 36
11:21:47.744860 IP 103.27.170.190 > kali: ICMP time exceeded in-transit, length 36
11:21:47.796708 IP 52.95.66.156 > kali: ICMP time exceeded in-transit, length 148
11:21:47.799213 IP 103.27.170.190 > kali: ICMP time exceeded in-transit, length 36
11:21:50.015732 IP 52.95.64.186 > kali: ICMP time exceeded in-transit, length 36
11:21:50.023428 IP 99.83.76.135 > kali: ICMP time exceeded in-transit, length 148
11:21:50.113708 IP 99.83.76.142 > kali: ICMP time exceeded in-transit, length 36
[arnab@kali]--[~/Desktop/Networks-Lab/ass2]
(master)$

```

```

(bin/bash 158x22)
(master)$sudo traceroute -I www.github.com
traceroute to www.github.com (13.234.210.38), 30 hops max, 60 byte packets
 1 _gateway (192.168.1.1) 5.769 ms 5.686 ms 5.666 ms
 2 * * 172.29.30.1 (172.29.30.1) 7.953 ms
 3 10.10.0.5 (10.10.0.5) 5.531 ms * *
 4 103.10.208.13 (103.10.208.13) 5.485 ms * *
 5 * * *
 6 103.27.170.190 (103.27.170.190) 45.250 ms 44.700 ms *
 7 52.95.66.156 (52.95.66.156) 42.082 ms * *
 8 52.95.64.186 (52.95.64.186) 42.033 ms * *
 9 * * *
10 99.83.76.135 (99.83.76.135) 49.570 ms * *
11 99.83.76.142 (99.83.76.142) 43.663 ms * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38) 44.317 ms * *

```

Also, we can notice that the IPs from the ICMP Time Limit Exceeded match exactly with the IPs from the traceroute command.

## Question 9

Write the `tcpdump` command that captures packets containing TCP packets with a specific IP address as (i) both source and destination, (ii) only source, and (iii) only destination.

## Answer 9

### (i) Both Source and Destination

```

[arnab@kali]~[~/Desktop/Networks-Lab/ass2]
(master)$sudo tcpdump -n src 192.168.1.4 and dst 13.234.210.38 -r github.pcap
reading from file github.pcap, link-type EN10MB (Ethernet), snapshot length 262144
11:31:43.532092 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 3799350412:3799351428, ack 445516143, win 2304, options [nop,nop,TS val 3890093338 ecr 69844504], length 1016
11:31:43.968846 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 2785, win 2348, options [nop,nop,TS val 3890093775 ecr 69850694], length 0
11:31:43.968880 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 4248, win 2371, options [nop,nop,TS val 3890093775 ecr 69850694], length 0
11:31:43.985705 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 4248, win 2371, options [nop,nop,TS val 3890093792 ecr 69850800,nop,nop,sack 1 {4209:4248}], length 0
11:31:44.482386 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 1016:2216, ack 4248, win 2371, options [nop,nop,TS val 3890094289 ecr 69850800], length 1200
11:31:44.857246 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 2216:2992, ack 4248, win 2371, options [nop,nop,TS val 3890094663 ecr 69851341], length 776
11:31:45.226263 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 5640, win 2393, options [nop,nop,TS val 3890095032 ecr 69851938], length 0
11:31:45.226327 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 7032, win 2415, options [nop,nop,TS val 3890095032 ecr 69851938], length 0
11:31:45.226360 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 9816, win 2458, options [nop,nop,TS val 3890095033 ecr 69851938], length 0
11:31:45.226422 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 24056, win 2681, options [nop,nop,TS val 3890095033 ecr 69851938], length 0
11:31:45.226455 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 32600, win 2673, options [nop,nop,TS val 3890095033 ecr 69851939], length 0
11:31:45.232617 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 43698, win 2854, options [nop,nop,TS val 3890095039 ecr 69851939], length 0
11:31:45.232712 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 45090, win 2876, options [nop,nop,TS val 3890095039 ecr 69851981], length 0
11:31:45.232734 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 47874, win 2920, options [nop,nop,TS val 3890095039 ecr 69851981], length 0
11:31:45.232750 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 47987, win 2920, options [nop,nop,TS val 3890095039 ecr 69851981], length 0
11:31:45.421428 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 2992:4040, ack 47987, win 2920, options [nop,nop,TS val 3890095528 ecr 69851981], length 1048
11:31:45.458613 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4040:4177, ack 47987, win 2920, options [nop,nop,TS val 3890095265 ecr 69851981], length 137
11:31:45.460073 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4177:4288, ack 47987, win 2920, options [nop,nop,TS val 3890095266 ecr 69851981], length 111
11:31:45.460196 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4288:4410, ack 47987, win 2920, options [nop,nop,TS val 3890095266 ecr 69851981], length 122
11:31:45.460374 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4410:4513, ack 47987, win 2920, options [nop,nop,TS val 3890095267 ecr 69851981], length 103
11:31:45.721841 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 49379, win 2942, options [nop,nop,TS val 3890095528 ecr 69852532], length 0
11:31:45.721875 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 50771, win 2964, options [nop,nop,TS val 3890095528 ecr 69852532], length 0
11:31:45.721884 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 51177, win 2985, options [nop,nop,TS val 3890095528 ecr 69852532], length 0
11:31:45.722518 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4513:4548, ack 51177, win 2985, options [nop,nop,TS val 3890095529 ecr 69852532], length 35
11:31:45.874341 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 52569, win 3007, options [nop,nop,TS val 3890095680 ecr 69852688], length 0
11:31:45.874394 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 53961, win 3029, options [nop,nop,TS val 3890095681 ecr 69852688], length 0
11:31:45.874411 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 54455, win 3051, options [nop,nop,TS val 3890095681 ecr 69852688], length 0
11:31:45.875516 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4548:4583, ack 54455, win 3051, options [nop,nop,TS val 3890095682 ecr 69852688], length 35
11:31:45.880528 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4583:4665, ack 54455, win 3051, options [nop,nop,TS val 3890095687 ecr 69852688], length 82
11:31:45.886608 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 55847, win 3072, options [nop,nop,TS val 3890095693 ecr 69852701], length 0
11:31:45.886683 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 57725, win 3102, options [nop,nop,TS val 3890095693 ecr 69852701], length 0
11:31:45.888203 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4665:4700, ack 57725, win 3102, options [nop,nop,TS val 3890095694 ecr 69852701], length 35
11:31:45.913900 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 60985, win 3140, options [nop,nop,TS val 3890095720 ecr 69852728], length 0
11:31:45.914375 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 4700:4735, ack 60985, win 3140, options [nop,nop,TS val 3890095721 ecr 69852728], length 35

```

Here the source is my local IP and destination is 13.234.210.38 ([www.github.com](https://www.github.com)'s IP)

## (ii) Only Source

```

[arnab@kali]~[~/Desktop/Networks-Lab/ass2]
(master)$sudo tcpdump -n src 13.234.210.38 -r github.pcap
reading from file github.pcap, link-type EN10MB (Ethernet), snapshot length 262144
11:31:43.578110 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [.], ack 3799351428, win 80, options [nop,nop,TS val 69850392 ecr 3890093338], length 0
11:31:43.968786 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 0:1392, ack 1, win 80, options [nop,nop,TS val 69850694 ecr 3890093338], length 1392
11:31:43.968827 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 1392:2784, ack 1, win 80, options [nop,nop,TS val 69850694 ecr 3890093338], length 1392
11:31:43.968872 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 2784:4247, ack 1, win 80, options [nop,nop,TS val 69850694 ecr 3890093338], length 1463
11:31:43.985667 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 4208:4247, ack 1, win 80, options [nop,nop,TS val 69850800 ecr 3890093338], length 39
11:31:44.526830 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [.], ack 1201, win 83, options [nop,nop,TS val 69851341 ecr 3890094289], length 0
11:31:44.902919 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [.], ack 1977, win 86, options [nop,nop,TS val 69851717 ecr 3890094663], length 0
11:31:45.226189 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 4247:5639, ack 1977, win 86, options [nop,nop,TS val 69851938 ecr 3890094663], length 1392
11:31:45.226303 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 5639:7031, ack 1977, win 86, options [nop,nop,TS val 69851938 ecr 3890094663], length 1392
11:31:45.226359 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 7031:9815, ack 1977, win 86, options [nop,nop,TS val 69851938 ecr 3890094663], length 2784
11:31:45.226384 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [.], seq 9815:24055, ack 1977, win 86, options [nop,nop,TS val 69851938 ecr 3890094663], length 14240
11:31:45.226439 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [.], seq 24055:32599, ack 1977, win 86, options [nop,nop,TS val 69851939 ecr 3890094663], length 8544
11:31:45.232572 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 32599:43697, ack 1977, win 86, options [nop,nop,TS val 69851939 ecr 3890094663], length 11098
11:31:45.232697 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 43697:45089, ack 1977, win 86, options [nop,nop,TS val 69851981 ecr 3890094663], length 1392
11:31:45.232726 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 45089:47873, ack 1977, win 86, options [nop,nop,TS val 69851981 ecr 3890094663], length 2784
11:31:45.232744 IP 13.234.210.38.443 > 192.168.1.4.41670: Flags [P.], seq 47873:47986, ack 1977, win 86, options [nop,nop,TS val 69851981 ecr 3890094663], length 113

```

Here source is 13.234.210.38 .

## (iii) Only Destination

```

[arnab@kali]~[~/Desktop/Networks-Lab/ass2]
(master)$sudo tcpdump -n dst 13.234.210.38 -r github.pcap
reading from file github.pcap, link-type EN10MB (Ethernet), snapshot length 262144
11:31:43.532092 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 3799350412:3799351428, ack 445516143, win 2304, options [nop,nop,TS val 3890093338 ecr 69844504], length 1016
11:31:43.968846 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 2785, win 2348, options [nop,nop,TS val 3890093775 ecr 69850694], length 0
11:31:43.968880 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 4248, win 2371, options [nop,nop,TS val 3890093775 ecr 69850694], length 0
11:31:43.985705 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 4248, win 2371, options [nop,nop,TS val 3890093792 ecr 69850800,nop,nop,sack 1 {4209:4248}], length 0
11:31:44.482386 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 1016:2216, ack 4248, win 2371, options [nop,nop,TS val 3890094289 ecr 69850800], length 1200
11:31:44.857246 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [P.], seq 2216:2992, ack 4248, win 2371, options [nop,nop,TS val 3890094663 ecr 69851341], length 776
11:31:45.226263 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 5640, win 2393, options [nop,nop,TS val 3890095032 ecr 69851938], length 0
11:31:45.226327 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 7032, win 2415, options [nop,nop,TS val 3890095032 ecr 69851938], length 0
11:31:45.226360 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 9816, win 2458, options [nop,nop,TS val 3890095033 ecr 69851938], length 0
11:31:45.226422 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 24056, win 2681, options [nop,nop,TS val 3890095033 ecr 69851938], length 0
11:31:45.226455 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 32600, win 2673, options [nop,nop,TS val 3890095033 ecr 69851939], length 0
11:31:45.232617 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 43698, win 2854, options [nop,nop,TS val 3890095039 ecr 69851939], length 0
11:31:45.232712 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 45090, win 2876, options [nop,nop,TS val 3890095039 ecr 69851981], length 0
11:31:45.232734 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 47874, win 2920, options [nop,nop,TS val 3890095039 ecr 69851981], length 0
11:31:45.232750 IP 192.168.1.4.41670 > 13.234.210.38.443: Flags [.], ack 47987, win 2920, options [nop,nop,TS val 3890095039 ecr 69851981], length 0

```

Here destination is 13.234.210.38

## Question 10

Write the tcpdump command that captures packets containing ICMP packets between two hosts with different IP addresses.

## Answer 10

We know `ping` uses ICMP protocol, so using it to generate some ICMP requests. Since, we need the IP so we are using the `-n` flag as well.

```
(master)$sudo tcpdump -n icmp -r icmp.pcap
reading from file icmp.pcap, link-type EN10MB (Ethernet), snapshot length 262144
11:46:27.188197 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 1, length 64
11:46:27.230230 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 1, length 64
11:46:28.189879 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 2, length 64
11:46:28.235675 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 2, length 64
11:46:29.190905 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 3, length 64
11:46:29.234456 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 3, length 64
11:46:30.192775 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 4, length 64
11:46:30.237372 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 4, length 64
11:46:31.193853 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 5, length 64
11:46:31.237372 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 5, length 64
11:46:32.195363 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 6, length 64
11:46:32.238292 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 6, length 64
11:46:33.196791 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 7, length 64
11:46:33.239475 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 7, length 64
11:46:34.197789 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 8, length 64
11:46:34.240218 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 8, length 64
11:46:35.198861 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 9, length 64
11:46:35.242847 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 9, length 64
11:46:36.200247 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 10, length 64
11:46:36.243823 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 10, length 64
11:46:37.202180 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 11, length 64
11:46:37.246033 IP 13.234.210.38 > 192.168.1.4: ICMP echo reply, id 62442, seq 11, length 64
11:46:38.202910 IP 192.168.1.4 > 13.234.210.38: ICMP echo request, id 62442, seq 12, length 64
```

```
(master)$ping www.github.com
PING github.com (13.234.210.38) 56(84) bytes of data.
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=1 ttl=47 time=42.1 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=2 ttl=47 time=45.8 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=3 ttl=47 time=43.6 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=4 ttl=47 time=44.6 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=5 ttl=47 time=43.6 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=6 ttl=47 time=43.0 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=7 ttl=47 time=42.7 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=8 ttl=47 time=42.5 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=9 ttl=47 time=44.0 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=10 ttl=47 time=43.6 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=11 ttl=47 time=43.9 ms
64 bytes from ec2-13-234-210-38.ap-south-1.compute.amazonaws.com (13.234.210.38): icmp_seq=12 ttl=47 time=160 ms
```

## Question 11

Write the `tcpdump` command to capture packets containing SSH request and reply between two specific IP addresses (hint: use port number 22 for SSH)

## Answer 11

```
sudo tcpdump -n port 22 -r ssh.pcap
```

```
(master)$sudo tcpdump -n port 22 -r ssh.pcap
reading from file ssh.pcap, link-type EN10MB (Ethernet), snapshot length 262144
12:43:16.703530 IP 192.168.1.4.41768 > 205.166.94.16.22: Flags [S], seq 2356424034, win 64240, options [mss 1460,sackOK,TS val 2144646823 ecr 0,nop,wscale 7], length 0
12:43:17.114580 IP 205.166.94.16.22 > 192.168.1.4.41768: Flags [S.], seq 3903069022, ack 2356424035, win 32768, options [mss 1460,nop,wscale 3,sackOK,TS val 1 ecr 2144646823], length 0
12:43:17.114642 IP 192.168.1.4.41768 > 205.166.94.16.22: Flags [.], ack 1, win 502, options [nop,nop,TS val 2144647234 ecr 1], length 0
12:43:17.115853 IP 192.168.1.4.41768 > 205.166.94.16.22: Flags [P.], seq 1:33, ack 1, win 502, options [nop,nop,TS val 2144647235 ecr 1], length 32: SSH: SSH-2.0-OpenSSH_8.4p1 Debian-6
12:43:17.502362 IP 205.166.94.16.22 > 192.168.1.4.41768: Flags [P.], seq 1:22, ack 33, win 4193, options [nop,nop,TS val 2 ecr 2144647235], length 21: SSH: SSH-2.0-OpenSSH_8.4
12:43:17.502416 IP 192.168.1.4.41768 > 205.166.94.16.22: Flags [.], ack 22, win 502, options [nop,nop,TS val 2144647622 ecr 2], length 0
12:43:17.503554 IP 192.168.1.4.41768 > 205.166.94.16.22: Flags [P.], seq 33:1545, ack 22, win 502, options [nop,nop,TS val 2144647623 ecr 2], length 1512
12:43:17.832029 IP 205.166.94.16.22 > 192.168.1.4.41768: Flags [P.], seq 22:1046, ack 33, win 4197, options [nop,nop,TS val 3 ecr 2144647622], length 1024
12:43:17.832081 IP 192.168.1.4.41768 > 205.166.94.16.22: Flags [.], ack 1046, win 494, options [nop,nop,TS val 2144647951 ecr 3], length 0
```