

Q1.

Output of question 1:

```
manav@kali ~
File Actions Edit View Help
Destination IP: 10.0.2.15
Source Port: 443
Destination Port: 37568
Source IP: 31.13.79.53
Destination IP: 10.0.2.15
Source Port: 443
Destination Port: 37568
^C

manav@kali ~
$ nano myfile.c
manav@kali ~
$ gcc myfile.c -o myfile
manav@kali ~
$ ./myfile
The sum of roll numbers modulo 3 is 12
Source IP: 52.139.250.209
Destination IP: 10.0.2.15
Source Port: 443
Destination Port: 45668
Source IP: 52.139.250.209
Destination IP: 10.0.2.15
Source Port: 443
Destination Port: 45668
Source IP: 107.23.224.36
Destination IP: 10.0.2.15
Source Port: 443
Destination Port: 44526
Source IP: 107.23.224.36
Destination IP: 10.0.2.15
Source Port: 443
Destination Port: 44526
Source IP: 31.13.79.53
Destination IP: 10.0.2.15
Source Port: 443
Destination Port: 37568
Source IP: 31.13.79.53
Destination IP: 10.0.2.15
Source Port: 443
Destination Port: 37568
Source IP: 142.251.42.118
Destination IP: 10.0.2.15
Source Port: 443
```

After running the code (as our proc file is 2.cap), the result obtained is as follows:
tcpreplay -i eth0 --mbps 1 -v 2.pcap

```
manav@kali ~/Downloads
File Actions Edit View Help
23:28:52.169281532 IP 146.185.79.121.443 > 192.168.122.197.48996: Flags [P..], seq 1536466:154622, ack 3314, win 501, options [nop,nop,TS val 69343369 ecr 973014708], length 976
23:28:52.169281532 IP 192.168.122.197.48996 > 146.185.79.121.443: Flags [-], ack 152248, win 22186, options [nop,nop,TS val 973014875 ecr 69343369], length 0
23:28:52.169281532 IP 192.168.122.197.48996 > 146.185.79.121.443: Flags [-], ack 152248, win 22179, options [nop,nop,TS val 973014875 ecr 69343369,nop,nop,sack 1 [153646:154622]], length 0
23:28:52.169281532 IP 146.185.79.121.443 > 192.168.122.197.48996: Flags [P..], seq 152248:153646, ack 3314, win 501, options [nop,nop,TS val 69343369 ecr 973014708], length 1396
23:28:52.169281532 IP 146.185.79.121.443 > 192.168.122.197.48996: Flags [P..], seq 154622:154653, ack 3314, win 501, options [nop,nop,TS val 69343369 ecr 973014708], length 31
23:28:52.169281532 IP 192.168.122.197.48996 > 146.185.79.121.443: Flags [-], ack 154622, win 22152, options [nop,nop,TS val 973014875 ecr 69343369], length 0
23:28:52.169281532 IP 192.168.122.197.48996 > 146.185.79.121.443: Flags [-], ack 154653, win 22152, options [nop,nop,TS val 973014875 ecr 69343369], length 0
23:28:52.169281532 IP 146.185.79.121.443 > 192.168.122.197.48996: Flags [P..], seq 154653:157449, ack 3314, win 501, options [nop,nop,TS val 69343395 ecr 973014708], length 2796
Warning in send_packets:send_packets() line 489:
Unable to send packet: Error with PF_PACKET send() [5567]: Message too long (errno = 90)
23:28:52.169281532 IP 192.168.122.197.48996 > 146.185.79.121.443: Flags [-], seq 157449, win 22195, options [nop,nop,TS val 973014901 ecr 69343395], length 0
23:28:52.169281532 IP 146.185.79.121.443 > 192.168.122.197.48996: Flags [P..], seq 157449:157977, ack 3314, win 501, options [nop,nop,TS val 69343395 ecr 973014708], length 528
23:28:52.169281532 IP 146.185.79.121.443 > 192.168.122.197.48996: Flags [P..], seq 157977:158088, ack 3314, win 501, options [nop,nop,TS val 69343395 ecr 973014708], length 31
23:28:52.169281532 IP 192.168.122.197.48996 > 146.185.79.121.443: Flags [-], ack 157977, win 22195, options [nop,nop,TS val 973014901 ecr 69343395], length 0
23:28:52.169281532 IP 192.168.122.197.48996 > 146.185.79.121.443: Flags [-], ack 158088, win 22195, options [nop,nop,TS val 973014901 ecr 69343395], length 0
23:28:52.169281532 IP 180.149.52.217.443 > 192.168.122.197.45308: Flags [P..], seq 4580:4524, ack 799, win 585, options [nop,nop,TS val 240263968 ecr 255893948], length 24
23:28:52.169281532 IP 180.149.52.217.443 > 192.168.122.197.45308: Flags [-], seq 4524, ack 799, win 585, options [nop,nop,TS val 240263968 ecr 255893948], length 0
23:28:52.169281532 IP 192.168.122.197.45308 > 180.149.52.217.443: Flags [P..], seq 799:838, ack 4525, win 581, options [nop,nop,TS val 2558923886 ecr 240263968], length 39
23:28:52.169281532 IP 192.168.122.197.45308 > 180.149.52.217.443: Flags [-], seq 838:862, ack 4525, win 581, options [nop,nop,TS val 2558923886 ecr 240263968], length 24
23:28:52.169281532 IP 192.168.122.197.45308 > 180.149.52.217.443: Flags [-], seq 862, ack 4525, win 581, options [nop,nop,TS val 2558923886 ecr 240263968], length 0
23:28:52.169281532 IP 180.149.52.217.443 > 192.168.122.197.45308: Flags [R], seq 1357918183, win 0, length 0
23:28:52.169281532 IP 180.149.52.217.443 > 192.168.122.197.45308: Flags [R], seq 1357918183, win 0, length 0
23:28:52.169281532 IP 180.149.52.217.443 > 192.168.122.197.45308: Flags [R], seq 1357918183, win 0, length 0
23:28:52.169281532 IP 192.168.122.197.45828 > 20.196.145.142.443: Flags [-], ack 6430, win 581, length 0
23:28:52.169281532 IP 20.196.145.142.443 > 192.168.122.197.45828: Flags [-], ack 1547, win 16355, length 0
23:28:52.169281532 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:45:3f:66.8001, length 35
23:28:53.169281533 IP 192.168.122.197.48862 > 48.126.17.135.443: Flags [-], ack 5385, win 581, length 0
23:28:53.169281533 IP 48.126.17.135.443 > 192.168.122.197.48862: Flags [-], ack 1330, win 16379, length 0
23:28:54.169281534 IP 192.168.122.197.39288 > 142.250.183.14.443: Flags [P..], seq 4674:4621, ack 8961, win 501, options [nop,nop,TS val 2573439249 ecr 786688458], length 147
23:28:54.169281534 IP 192.168.122.197.39288 > 142.250.183.14.443: Flags [-], seq 4621:5280, ack 8961, win 501, options [nop,nop,TS val 2573439249 ecr 786688458], length 659
23:28:54.169281534 IP 142.250.183.14.443 > 192.168.122.197.39288: Flags [-], ack 4621, win 317, options [nop,nop,TS val 786717836 ecr 2573439249], length 0
23:28:54.169281534 IP 142.250.183.14.443 > 192.168.122.197.39288: Flags [-], ack 5280, win 327, options [nop,nop,TS val 786717836 ecr 2573439249], length 0
23:28:54.169281534 IP 142.250.183.14.443 > 192.168.122.197.39288: Flags [P..], seq 8961:9810, ack 5280, win 327, options [nop,nop,TS val 786717943 ecr 2573439249], length 69
23:28:54.169281534 IP 142.250.183.14.443 > 192.168.122.197.39288: Flags [-], seq 9810:9410, ack 5280, win 327, options [nop,nop,TS val 786717943 ecr 2573439249], length 380
23:28:54.169281534 IP 192.168.122.197.39288 > 142.250.183.14.443: Flags [-], ack 9410, win 581, options [nop,nop,TS val 2573439372 ecr 786717943], length 0
23:28:54.169281534 IP 142.250.183.14.443 > 192.168.122.197.39288: Flags [-], seq 9410:9666, ack 5280, win 327, options [nop,nop,TS val 786717946 ecr 2573439249], length 256
23:28:54.169281534 IP 142.250.183.14.443 > 192.168.122.197.39288: Flags [-], seq 9666:9785, ack 5280, win 327, options [nop,nop,TS val 786717946 ecr 2573439249], length 39
23:28:54.169281534 IP 192.168.122.197.39288 > 142.250.183.14.443: Flags [-], ack 9785, win 501, options [nop,nop,TS val 2573439375 ecr 786717946], length 0
23:28:54.169281534 IP 192.168.122.197.39288 > 142.250.183.14.443: Flags [-], seq 5280:5319, ack 9785, win 501, options [nop,nop,TS val 2573439375 ecr 786717946], length 39
23:28:54.169281534 IP 142.250.183.14.443 > 192.168.122.197.39288: Flags [-], ack 5319, win 327, options [nop,nop,TS val 786717961 ecr 2573439375], length 0
23:28:55.169281535 STP 802.1d, Config, Flags [none], bridge-id 8000.52:54:00:45:3f:66.8001, length 25
Actual: 4266 packets (1247027 bytes) sent in 9.99 seconds
Rated: 124793.1 Bps, 0.998 Mbps, 428.71 pps
Flows: 188 flows, 14.41 fpps, 5596 unique flow packets, 2 unique non-flow packets
Statistics for network device: eth0
Successful packets: 4266
Failed packets: 1314
Truncated packets: 0
Retried packets (RDBUFF): 0
Retried packets (EAGAIN): 0
manav@kali ~
$
```

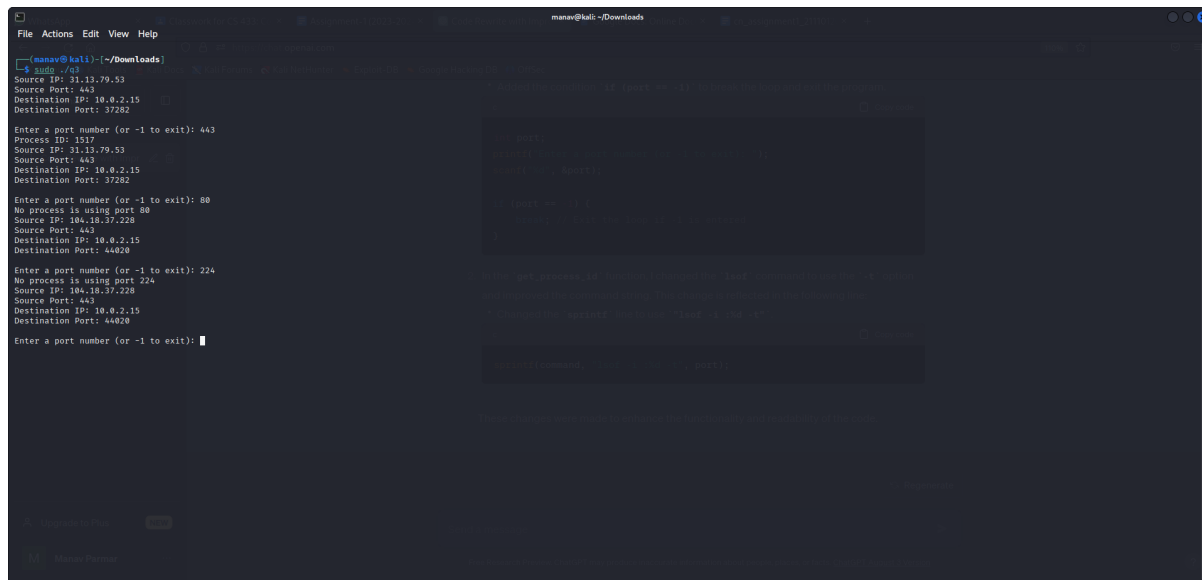
```
manan@kali: ~/Downloads
File Actions Edit View Help
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 40862
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 40862
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 45034
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 45034
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 40862
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 40862
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.183.110, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 48524
IP: 142.250.183.110 resolves to host: bom12s13-in-f14.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 40862
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 40862
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.183.110, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 48524
IP: 142.250.183.110 resolves to host: bom12s13-in-f14.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.183.110, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 48524
IP: 142.250.183.110 resolves to host: bom12s13-in-f14.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.183.110, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 48524
IP: 142.250.183.110 resolves to host: bom12s13-in-f14.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.183.110, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 48524
IP: 142.250.183.110 resolves to host: bom12s13-in-f14.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.182.202, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 40862
IP: 142.250.182.202 resolves to host: bom07s28-in-f10.1e100.net
IP: 0.0.0.0 resolves to host: 0.0.0.0
Source IP: 142.250.183.110, Source Port: 443, Destination IP: 0.0.0.0, Destination Port: 48524
```

Explanation about the implementation

- 1a.
 - 1. The program defines two functions:
 - process_packet: This function takes two arguments pointer to the package and the data size. It extracts the IP header and the TCP header from the data packet. It extracts the source and destination IP addresses using inet_ntop and stores them in sourceIP and destIP, respectively. It extracts the source and destination port numbers from the TCP header and stores them in sourcePort and destPort.Finally, it prints the source IP, destination IP, source port, and destination port to the console.
 - 2. In the main function:
 - It creates a raw socket to capture all TCP packets. Then, it enters an infinite loop to capture the process packets. It receives the package in the packet buffer. It captures the package and sends it to the process_packet. This loop continues indefinitely, capturing and processing the incoming packets.
 - 3. When the user exits, the program closes the socket and terminates.

Q3.

Here is the output after running:



```
manav@kali: ~/Downloads
File Actions Edit View Help
[manav@kali:~/Downloads]
$ ./sund ./q3
Source IP: 31.13.79.53
Source Port: 443
Destination IP: 10.0.2.15
Destination Port: 37282
Enter a port number (or -1 to exit): 443
Process ID: 1517
Source IP: 31.13.79.53
Source Port: 443
Destination IP: 10.0.2.15
Destination Port: 37282
Enter a port number (or -1 to exit): 80
No process is using port 80
Source IP: 104.18.37.228
Source Port: 443
Destination IP: 10.0.2.15
Destination Port: 44020
Enter a port number (or -1 to exit): 224
No process is using port 224
Source IP: 104.18.37.228
Source Port: 443
Destination IP: 10.0.2.15
Destination Port: 44020
Enter a port number (or -1 to exit):
```

Installed Packages

Package Name	Version
python3	3.11.2
python3-pip	23.0.1
python3-venv	3.11.2
python3-wheel	0.40.0
python3-setuptools	68.0.0
python3-distutils	3.11.2
python3-idle	3.11.2
python3-tk	3.11.2
python3-urllib3	2.0.4
python3-yaml	6.0.1
python3-certifi	2023.7.22
python3-cryptography	40.0.0
python3-requests	2.31.0
python3-urllib	1.26.12
python3-urllib3	2.0.4
python3-yaml	6.0.1
python3-certifi	2023.7.22
python3-cryptography	40.0.0
python3-requests	2.31.0
python3-urllib	1.26.12

Running Processes

Process Name	Process ID
python3	1517
python3-pip	1517
python3-venv	1517
python3-wheel	1517
python3-setuptools	1517
python3-distutils	1517
python3-idle	1517
python3-tk	1517
python3-urllib3	1517
python3-yaml	1517
python3-certifi	1517
python3-cryptography	1517
python3-requests	1517
python3-urllib	1517

References:

Portions of code are written with the help of OpenAI's ChatGPT 3.5