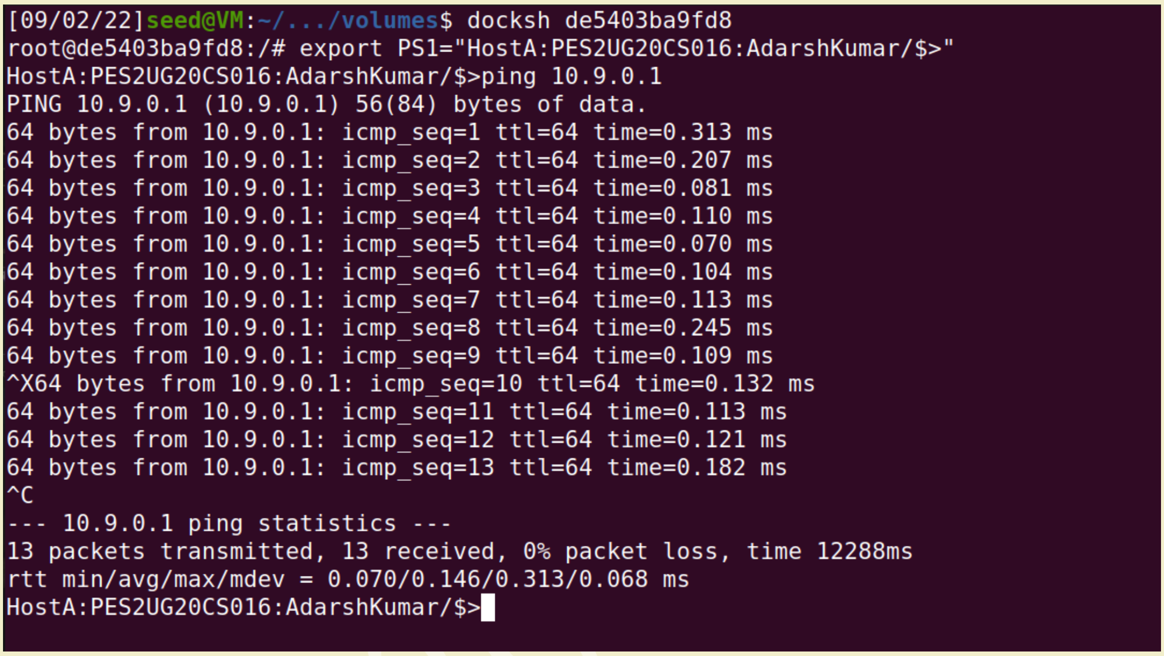
Name: Adarsh Kumar	SRN No: PES2UG20CS016	Assignment No: 02
	Section: B	Date: 02/09/2022

Task 2.1 A	Understanding how a Sniffer Works

Output Screenshot

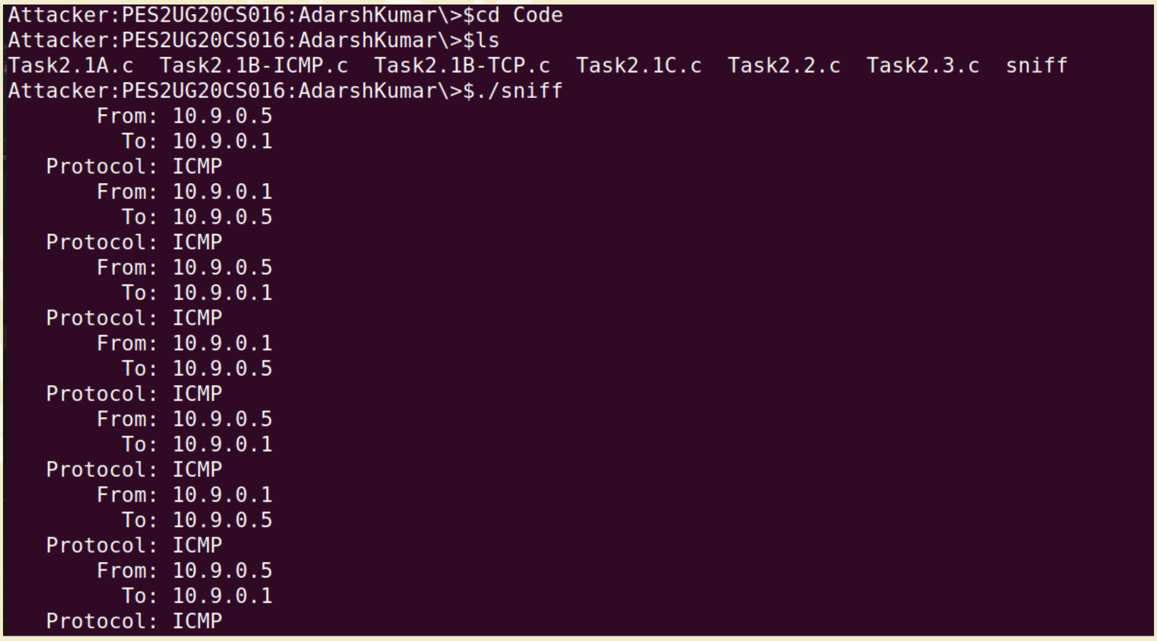
Host-A Terminal:



```
[09/02/22]seed@VM:~/.../volumes$ docksh de5403ba9fd8
root@de5403ba9fd8:/# export PS1="HostA:PES2UG20CS016:AdarshKumar/$>"
HostA:PES2UG20CS016:AdarshKumar/$>ping 10.9.0.1
PING 10.9.0.1 (10.9.0.1) 56(84) bytes of data.
64 bytes from 10.9.0.1: icmp_seq=1 ttl=64 time=0.313 ms
64 bytes from 10.9.0.1: icmp_seq=2 ttl=64 time=0.207 ms
64 bytes from 10.9.0.1: icmp_seq=3 ttl=64 time=0.081 ms
64 bytes from 10.9.0.1: icmp_seq=4 ttl=64 time=0.110 ms
64 bytes from 10.9.0.1: icmp_seq=5 ttl=64 time=0.070 ms
64 bytes from 10.9.0.1: icmp_seq=6 ttl=64 time=0.104 ms
64 bytes from 10.9.0.1: icmp_seq=7 ttl=64 time=0.113 ms
64 bytes from 10.9.0.1: icmp_seq=8 ttl=64 time=0.245 ms
64 bytes from 10.9.0.1: icmp_seq=9 ttl=64 time=0.109 ms
^X64 bytes from 10.9.0.1: icmp_seq=10 ttl=64 time=0.132 ms
64 bytes from 10.9.0.1: icmp_seq=11 ttl=64 time=0.113 ms
64 bytes from 10.9.0.1: icmp_seq=12 ttl=64 time=0.121 ms
64 bytes from 10.9.0.1: icmp_seq=13 ttl=64 time=0.182 ms
^C
--- 10.9.0.1 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12288ms
rtt min/avg/max/mdev = 0.070/0.146/0.313/0.068 ms
HostA:PES2UG20CS016:AdarshKumar/$>
```

From host-A pinging IP 10.9.0.1 and sent 13 packets

Attacker Terminal:



```
Attacker:PES2UG20CS016:AdarshKumar\>$cd Code
Attacker:PES2UG20CS016:AdarshKumar\>$ls
Task2.1A.c  Task2.1B-ICMP.c  Task2.1B-TCP.c  Task2.1C.c  Task2.2.c  Task2.3.c  sniff
Attacker:PES2UG20CS016:AdarshKumar\>$./sniff
       From: 10.9.0.5
         To: 10.9.0.1
   Protocol: ICMP
       From: 10.9.0.1
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.1
   Protocol: ICMP
       From: 10.9.0.1
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.1
   Protocol: ICMP
       From: 10.9.0.1
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.1
   Protocol: ICMP
```

Attacker sniffing packets from host-A and gathering information such destination IP & host IP.

Question 1:	Describe the sequence of the library calls that are essential for sniffer programs. This is meant to be a summary?

Ans: Fundamental function calls that are used for sniffing programs include

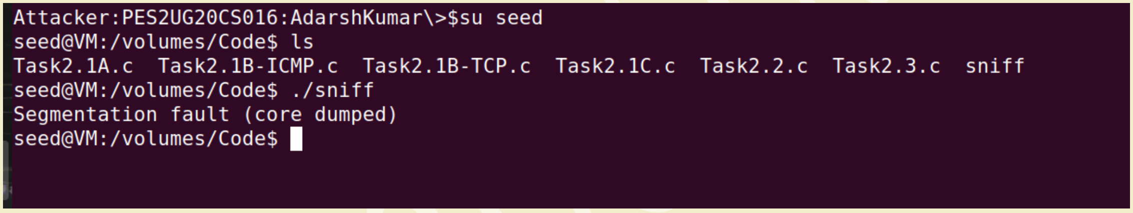
1. Determining and setting up type of ethernet interface that the program will utilize.
2. The initialization of the PCAP to create a session, typically there is on session per device to be sniffed.
3. The call to set traffic filtering rules, this ensures that the type of traffic sniffed on an interface is the type one is going for.
4. The execution of the sniff.
5. Termination of the session

Question 2:

Why do you need the root privilege to run sniffex? Where does the program fail if executed without the root privilege?

Ans: In Linux whenever network interfaces need to be access it is required to have root access, in this case, the program needs the ability to utilize raw sockets to send packets in the way it does, without the root user capacities the Network Interface Card would be inaccessible hence the ability to use/create raw sockets is lost.

Screenshots:



```
Attacker:PES2UG20CS016:AdarshKumar\>$su seed
seed@VM:/volumes/Code$ ls
Task2.1A.c  Task2.1B-ICMP.c  Task2.1B-TCP.c  Task2.1C.c  Task2.2.c  Task2.3.c  sniff
seed@VM:/volumes/Code$ ./sniff
Segmentation fault (core dumped)
seed@VM:/volumes/Code$ 
```

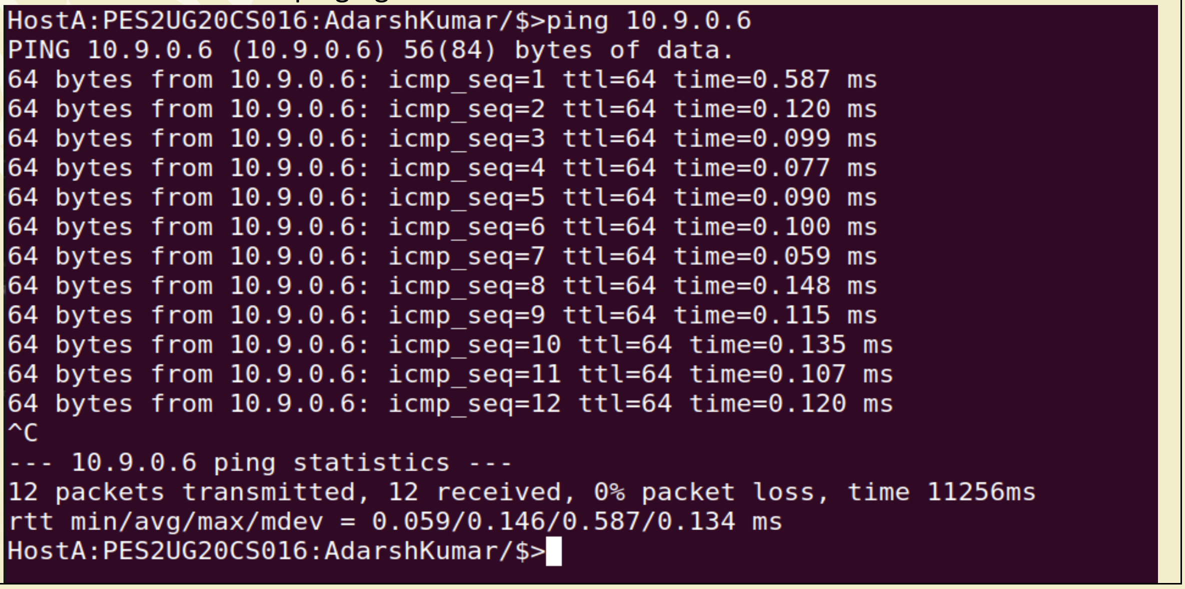
Question 3:

Please turn on and turn off the promiscuous mode in your sniffer program. The value 1 of the third parameter in the pcap_open_live() function turns on the promiscuous mode (use 0 to turn it off).

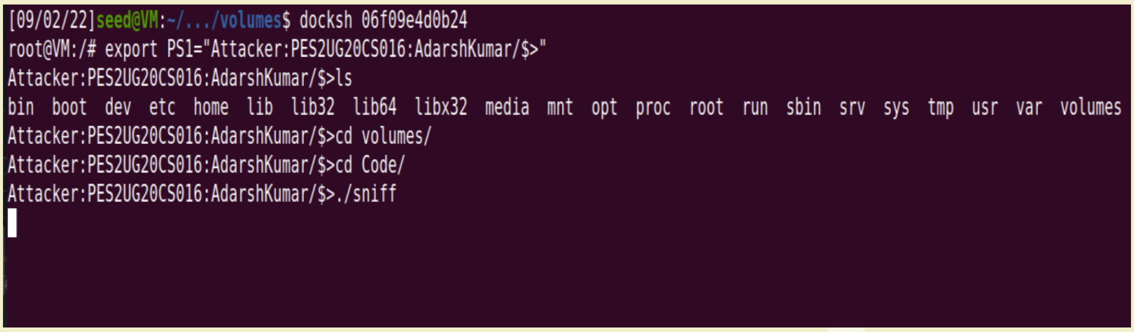
Ans: switching of the promiscuous mode will not let us see network traffic of other IP address i.e those IP address which are not ours and it will not allow us to use both wifi and network ethernet at same time.

Output screenshots:

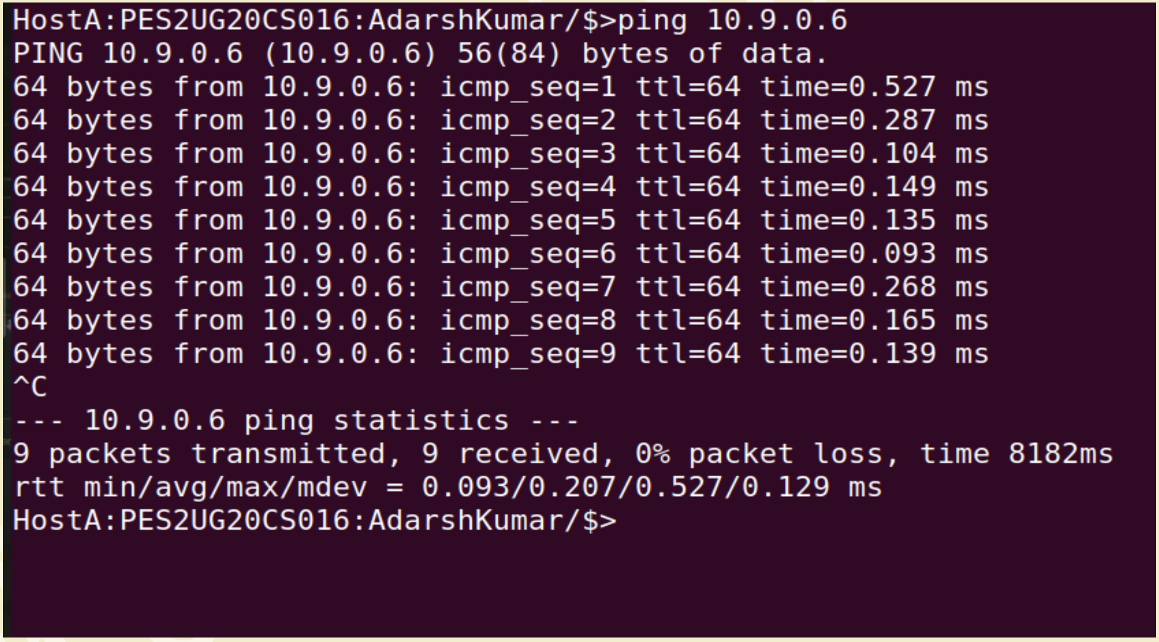
Host-A Terminal: I am pinging to IP 10.9.0.6

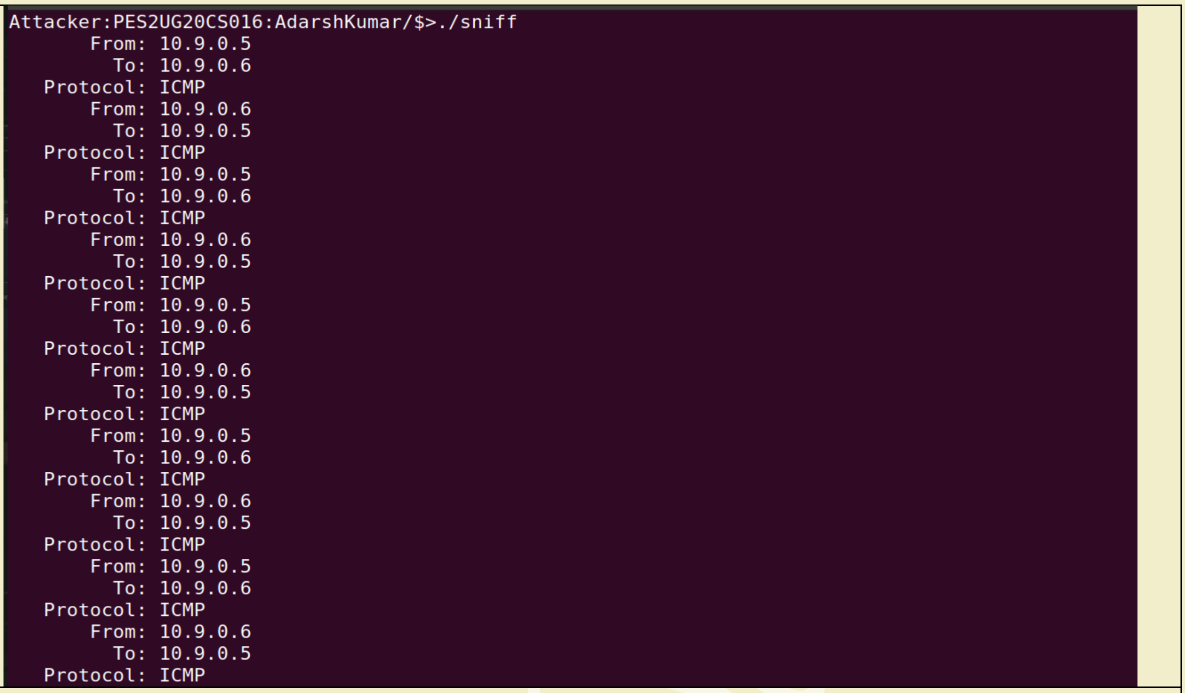


```
HostA:PES2UG20CS016:AdarshKumar/$>ping 10.9.0.6
PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.
64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=0.587 ms
64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.120 ms
64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.099 ms
64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.077 ms
64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.090 ms
64 bytes from 10.9.0.6: icmp_seq=6 ttl=64 time=0.100 ms
64 bytes from 10.9.0.6: icmp_seq=7 ttl=64 time=0.059 ms
64 bytes from 10.9.0.6: icmp_seq=8 ttl=64 time=0.148 ms
64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.115 ms
64 bytes from 10.9.0.6: icmp_seq=10 ttl=64 time=0.135 ms
64 bytes from 10.9.0.6: icmp_seq=11 ttl=64 time=0.107 ms
64 bytes from 10.9.0.6: icmp_seq=12 ttl=64 time=0.120 ms
^C
--- 10.9.0.6 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11256ms
rtt min/avg/max/mdev = 0.059/0.146/0.587/0.134 ms
HostA:PES2UG20CS016:AdarshKumar/$>
```

	Attacker Terminal:
	
	`[09/02/22]seed@VM:~/.../volumes$ docksh 06f09e4d0b24`
	`root@VM:/# export PS1="Attacker:PES2UG20CS016:AdarshKumar/$>"`
	`Attacker:PES2UG20CS016:AdarshKumar/$>ls`
	`bin  boot  dev  etc  home  lib  lib32  lib64  libx32  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  volumes`
	`Attacker:PES2UG20CS016:AdarshKumar/$>cd volumes/`
	`Attacker:PES2UG20CS016:AdarshKumar/$>cd Code/`
	`Attacker:PES2UG20CS016:AdarshKumar/$>./sniff`
	If we switch of the promiscuous mode then we are unable to sniff packet which are not intended for our IP.

Task 2.1 B	Capture the ICMP packets between two specific hosts?

Output Screenshot	<u>Host-A Terminal</u>
	From host-A pinging to 10.9.0.6, 9 packet transmitted .
	
	`HostA:PES2UG20CS016:AdarshKumar/$>ping 10.9.0.6`
	`PING 10.9.0.6 (10.9.0.6) 56(84) bytes of data.`
	`64 bytes from 10.9.0.6: icmp_seq=1 ttl=64 time=0.527 ms`
	`64 bytes from 10.9.0.6: icmp_seq=2 ttl=64 time=0.287 ms`
	`64 bytes from 10.9.0.6: icmp_seq=3 ttl=64 time=0.104 ms`
	`64 bytes from 10.9.0.6: icmp_seq=4 ttl=64 time=0.149 ms`
	`64 bytes from 10.9.0.6: icmp_seq=5 ttl=64 time=0.135 ms`
	`64 bytes from 10.9.0.6: icmp_seq=6 ttl=64 time=0.093 ms`
	`64 bytes from 10.9.0.6: icmp_seq=7 ttl=64 time=0.268 ms`
	`64 bytes from 10.9.0.6: icmp_seq=8 ttl=64 time=0.165 ms`
	`64 bytes from 10.9.0.6: icmp_seq=9 ttl=64 time=0.139 ms`
	`^C`
	`--- 10.9.0.6 ping statistics ---`
	`9 packets transmitted, 9 received, 0% packet loss, time 8182ms`
	`rtt min/avg/max/mdev = 0.093/0.207/0.527/0.129 ms`
	`HostA:PES2UG20CS016:AdarshKumar/$>`
	<u>Attacker Terminal:</u>
	On attacker terminal all ICMP packet received send by the host-A.



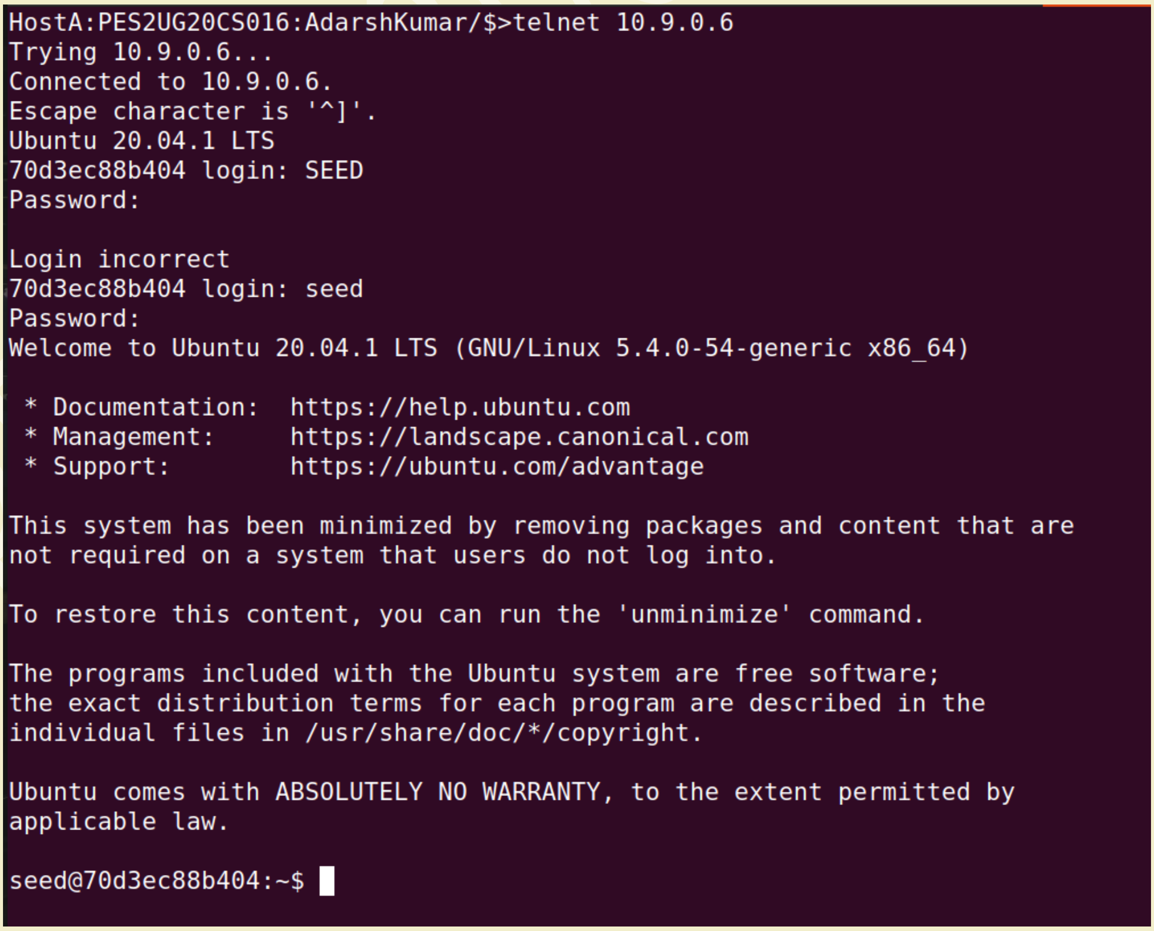
```
Attacker:PES2UG20CS016:AdarshKumar/$>./sniff
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: ICMP
       From: 10.9.0.6
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: ICMP
       From: 10.9.0.6
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: ICMP
       From: 10.9.0.6
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: ICMP
       From: 10.9.0.6
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 10.9.0.6
   Protocol: ICMP
       From: 10.9.0.6
         To: 10.9.0.5
   Protocol: ICMP
```

Q) Capture the TCP packets that have a destination port range from to sort 10 - 100.

Output Screenshot

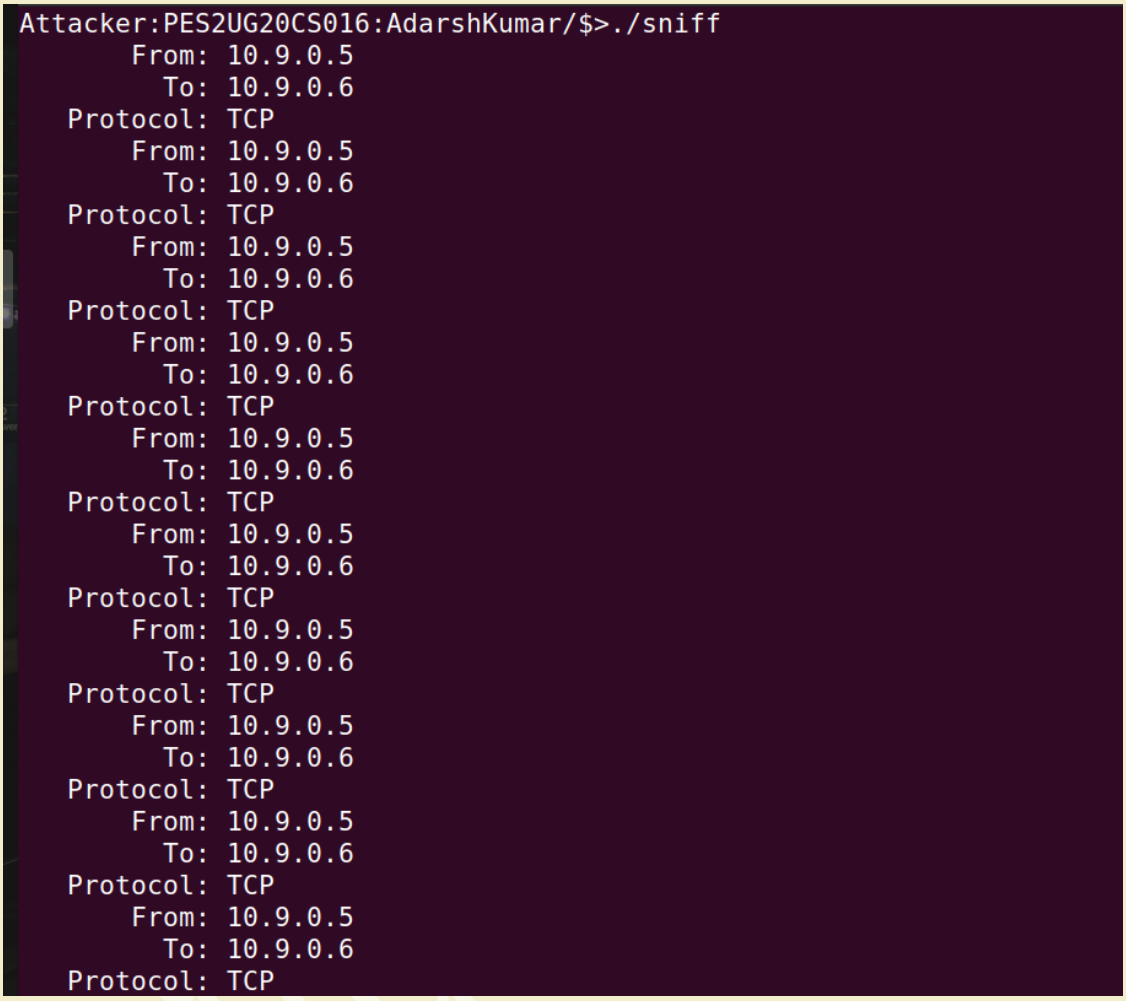
Host-A Terminal:

Pinging to telnet 10.9.0.6 it will initiate a TCP connection to login to telnet portal.



```
HostA:PES2UG20CS016:AdarshKumar/$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
70d3ec88b404 login: SEED
Password:

Login incorrect
70d3ec88b404 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

seed@70d3ec88b404:~$ █
```

Attacker Terminal



```
Attacker:PES2UG20CS016:AdarshKumar/$>./sniff
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
        From: 10.9.0.5
          To: 10.9.0.6
    Protocol: TCP
```

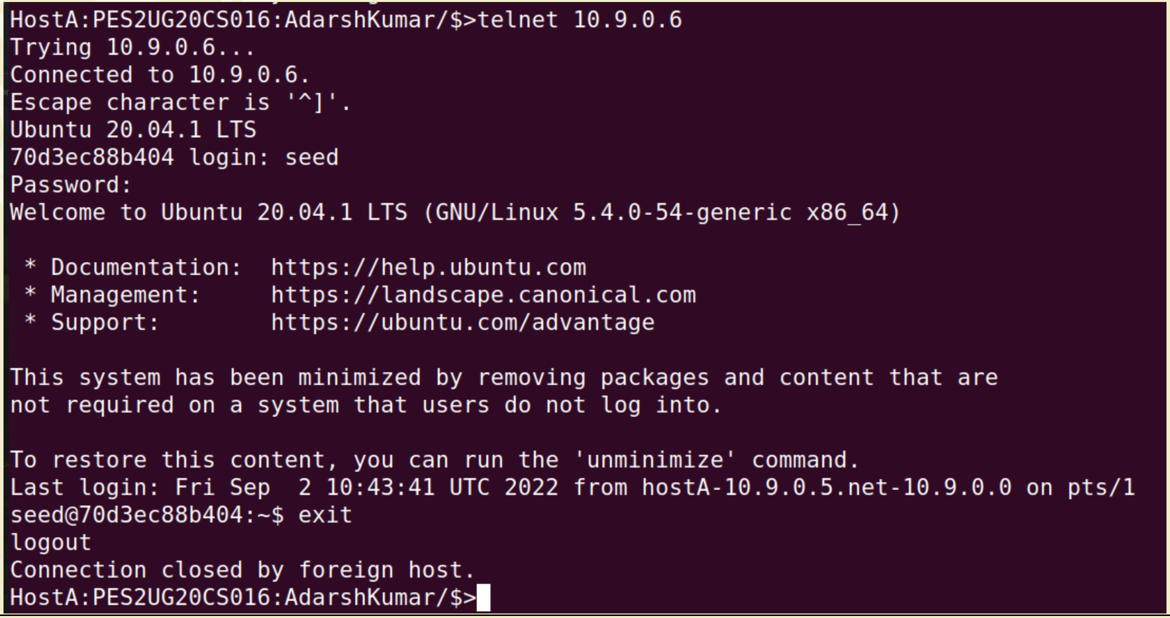
As we can see that the Protocol field IS TCP now it is capturing TCP packets only.

Task 2.1 C	Please show how you can use your sniffer program to capture the password when somebody is using telnet on the network that you are monitoring

Output Screenshot

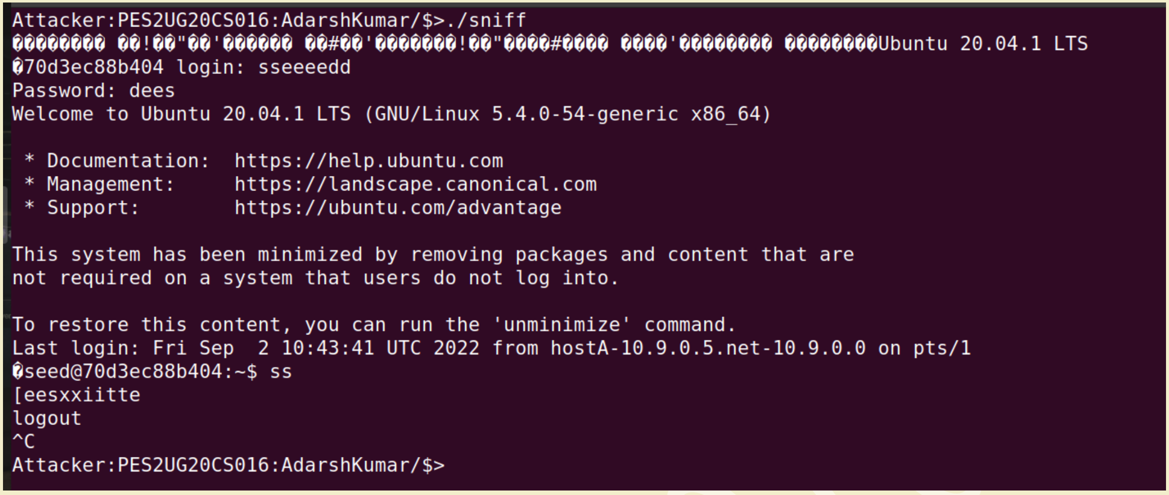
Host-A Terminal:

Host -A is trying to login to the telnet portal by pinging to telnet IP 10.9.0.6



```
HostA:PES2UG20CS016:AdarshKumar/$>telnet 10.9.0.6
Trying 10.9.0.6...
Connected to 10.9.0.6.
Escape character is '^]'.
Ubuntu 20.04.1 LTS
70d3ec88b404 login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Sep  2 10:43:41 UTC 2022 from hostA-10.9.0.5.net-10.9.0.0 on pts/1
seed@70d3ec88b404:~$ exit
logout
Connection closed by foreign host.
HostA:PES2UG20CS016:AdarshKumar/$>
```

Attacker Terminal:



```
Attacker:PES2UG20CS016:AdarshKumar/$>./sniff
�������� ��!��"��'������ ��#��'�������!��"����#���� ����'�������� ��������Ubuntu 20.04.1 LTS
�70d3ec88b404 login: sseeeedd
Password: dees
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-54-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Fri Sep  2 10:43:41 UTC 2022 from hostA-10.9.0.5.net-10.9.0.0 on pts/1
�seed@70d3ec88b404:~$ ss
[eesxxiitte
logout
^C
Attacker:PES2UG20CS016:AdarshKumar/$>
```

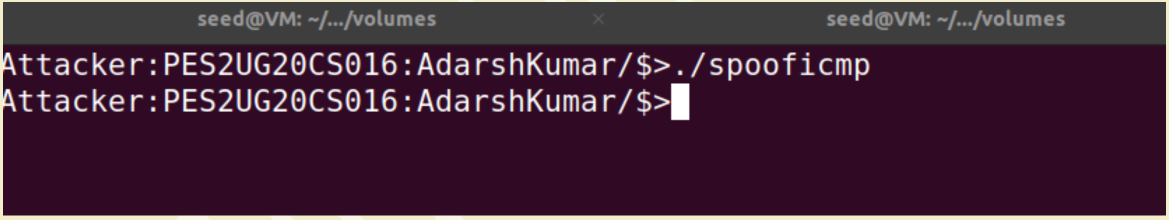
As we can see in the above picture that when host-A was logging to telnet portal our program sniffed that packet and able to locate information like login ID and login Password. As well as the telnet welcome page.

Task 2.2	Spoof an ICMP Echo Request packets

Output Screenshot

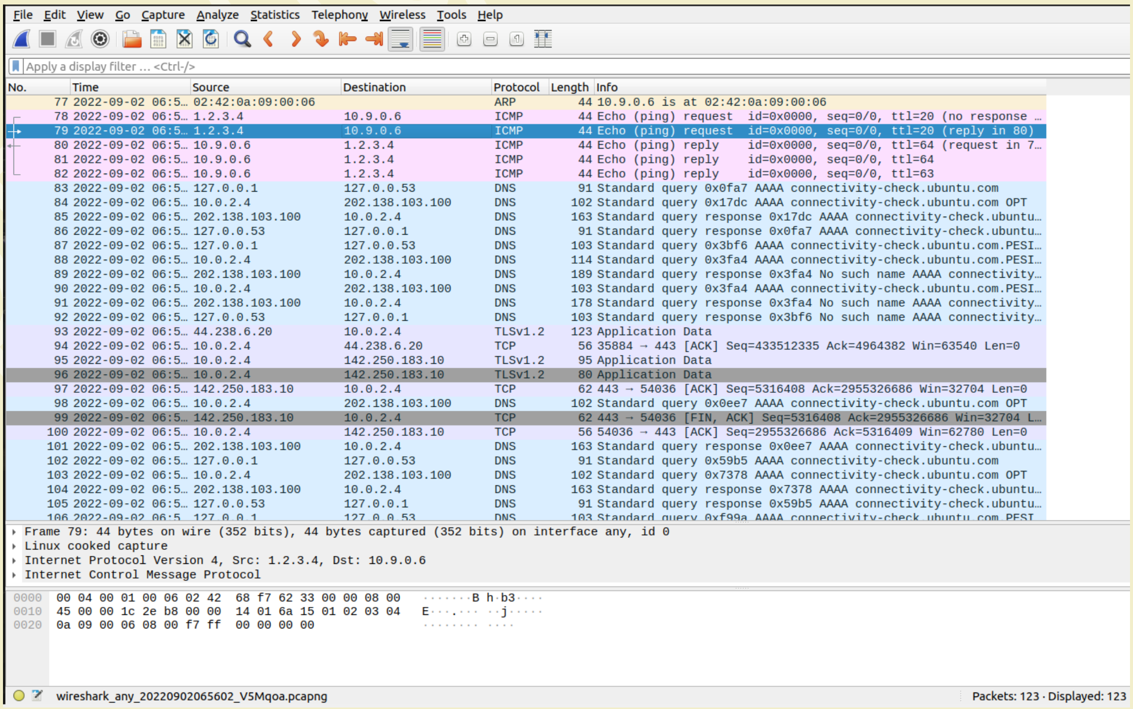
Attacker Terminal:

Trying to spoof a echo request packet with IP of 1.2.3.4



```
Attacker:PES2UG20CS016:AdarshKumar/$>./spoofcmp
Attacker:PES2UG20CS016:AdarshKumar/$>
```

Wireshark:

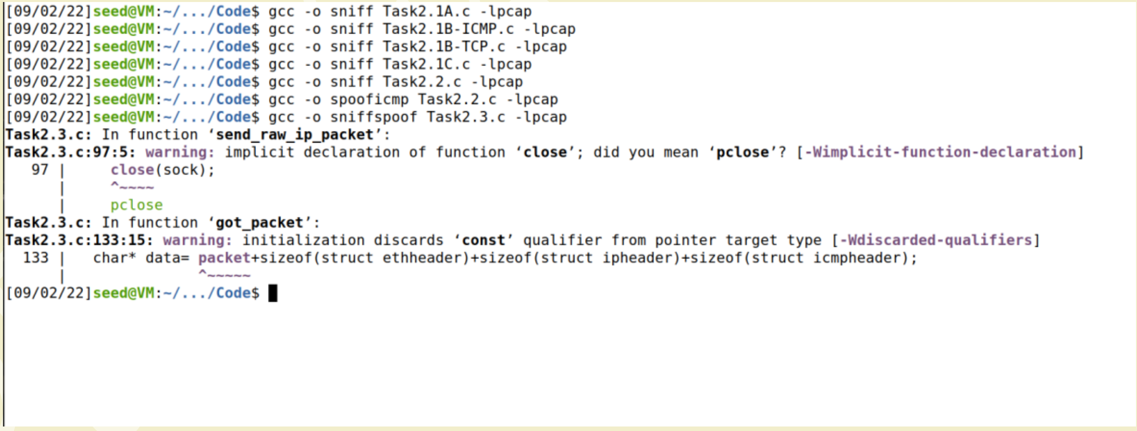

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time              Source             Destination        Protocol Length Info
   77 2022-09-02 06:5… 02:42:0a:09:00:06                     ARP       44 10.9.0.6 is at 02:42:0a:09:00:06
   78 2022-09-02 06:5… 1.2.3.4            10.9.0.6           ICMP      44 Echo (ping) request  id=0x0000, seq=0/0, ttl=20 (no response …
   79 2022-09-02 06:5… 1.2.3.4            10.9.0.6           ICMP      44 Echo (ping) request  id=0x0000, seq=0/0, ttl=20 (reply in 80)
   80 2022-09-02 06:5… 10.9.0.6           1.2.3.4            ICMP      44 Echo (ping) reply    id=0x0000, seq=0/0, ttl=64 (request in 7…
   81 2022-09-02 06:5… 10.9.0.6           1.2.3.4            ICMP      44 Echo (ping) reply    id=0x0000, seq=0/0, ttl=64
   82 2022-09-02 06:5… 10.9.0.6           1.2.3.4            ICMP      44 Echo (ping) reply    id=0x0000, seq=0/0, ttl=63
   83 2022-09-02 06:5… 127.0.0.1          127.0.0.53         DNS       91 Standard query 0x0fa7 AAAA connectivity-check.ubuntu.com
   84 2022-09-02 06:5… 10.0.2.4           202.138.103.100    DNS      102 Standard query 0x17dc AAAA connectivity-check.ubuntu.com OPT
   85 2022-09-02 06:5… 202.138.103.100    10.0.2.4           DNS      163 Standard query response 0x17dc AAAA connectivity-check.ubuntu…
   86 2022-09-02 06:5… 127.0.0.53         127.0.0.1          DNS       91 Standard query response 0x0fa7 AAAA connectivity-check.ubuntu…
   87 2022-09-02 06:5… 127.0.0.1          127.0.0.53         DNS      103 Standard query 0x3bf6 AAAA connectivity-check.ubuntu.com.PESI…
   88 2022-09-02 06:5… 10.0.2.4           202.138.103.100    DNS      114 Standard query 0x3fa4 AAAA connectivity-check.ubuntu.com.PESI…
   89 2022-09-02 06:5… 202.138.103.100    10.0.2.4           DNS      189 Standard query response 0x3fa4 No such name AAAA connectivity…
   90 2022-09-02 06:5… 10.0.2.4           202.138.103.100    DNS      103 Standard query 0x3fa4 AAAA connectivity-check.ubuntu.com.PESI…
   91 2022-09-02 06:5… 202.138.103.100    10.0.2.4           DNS      178 Standard query response 0x3fa4 No such name AAAA connectivity…
   92 2022-09-02 06:5… 127.0.0.53         127.0.0.1          DNS      103 Standard query response 0x3bf6 No such name AAAA connectivity…
   93 2022-09-02 06:5… 44.238.6.20        10.0.2.4           TLSv1.2  123 Application Data
   94 2022-09-02 06:5… 10.0.2.4           44.238.6.20        TCP       56 35884 → 443 [ACK] Seq=433512335 Ack=4964382 Win=63540 Len=0
   95 2022-09-02 06:5… 10.0.2.4           142.250.183.10     TLSv1.2   95 Application Data
   96 2022-09-02 06:5… 10.0.2.4           142.250.183.10     TLSv1.2   80 Application Data
   97 2022-09-02 06:5… 142.250.183.10     10.0.2.4           TCP       62 443 → 54036 [ACK] Seq=5316408 Ack=2955326686 Win=32704 Len=0
   98 2022-09-02 06:5… 10.0.2.4           202.138.103.100    DNS      102 Standard query 0x0ee7 AAAA connectivity-check.ubuntu.com OPT
   99 2022-09-02 06:5… 142.250.183.10     10.0.2.4           TCP       62 443 → 54036 [FIN, ACK] Seq=5316408 Ack=2955326686 Win=32704 L…
  100 2022-09-02 06:5… 10.0.2.4           142.250.183.10     TCP       56 54036 → 443 [ACK] Seq=2955326686 Ack=5316409 Win=62780 Len=0
  101 2022-09-02 06:5… 202.138.103.100    10.0.2.4           DNS      163 Standard query response 0x0ee7 AAAA connectivity-check.ubuntu…
  102 2022-09-02 06:5… 127.0.0.1          127.0.0.53         DNS       91 Standard query 0x59b5 AAAA connectivity-check.ubuntu.com
  103 2022-09-02 06:5… 10.0.2.4           202.138.103.100    DNS      102 Standard query 0x7378 AAAA connectivity-check.ubuntu.com OPT
  104 2022-09-02 06:5… 202.138.103.100    10.0.2.4           DNS      163 Standard query response 0x7378 AAAA connectivity-check.ubuntu…
  105 2022-09-02 06:5… 127.0.0.53         127.0.0.1          DNS       91 Standard query response 0x59b5 AAAA connectivity-check.ubuntu…
  106 2022-09-02 06:5… 127.0.0.1          127.0.0.53         DNS      103 Standard query 0xf99a AAAA connectivity-check.ubuntu.com.PESI

› Frame 79: 44 bytes on wire (352 bits), 44 bytes captured (352 bits) on interface any, id 0
› Linux cooked capture
› Internet Protocol Version 4, Src: 1.2.3.4, Dst: 10.9.0.6
› Internet Control Message Protocol

0000  00 04 00 01 00 06 02 42  68 f7 62 33 00 00 08 00   ·······B h·b3····
0010  45 00 00 1c 2e b8 00 00  14 01 6a 15 01 02 03 04   E···.··· ··j·····
0020  0a 09 00 06 08 00 f7 ff  00 00 00 00               ········ ····

wireshark_any_20220902065602_V5Mqoa.pcapng                    Packets: 123 · Displayed: 123
```

In Wireshark we can see that a packet is sent to IP of 10.9.0.6 from IP source IP 1.2.3.4
And echo reply is also being sent to 10.9.0.6

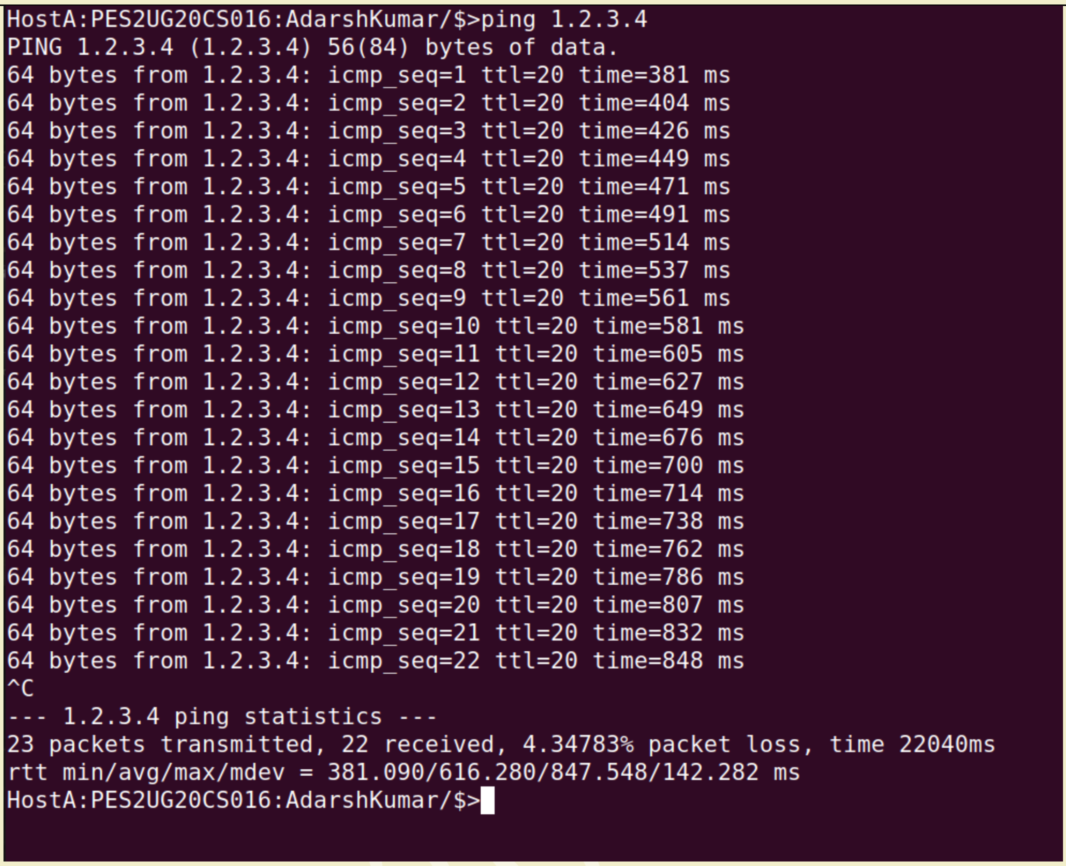
Question 4:	Using the raw socket programming, do you have to calculate the checksum for the IP header? Ans: With the raw socket programming, checksum is not to be calculated separately. This is because Ubuntu calculate the checksum of IP header before transmitting it, irrespective of the fact whether the value is mentioned or not. The kernel or the underlying operating system builds the packet including the checksum for your data. NOTE: ICMP IP packet will not be formed if some arbitrary value is given to the IP length field. This is because the length should actually be the sum of the size of IP header and the size of the ICMP header. If the condition is not met, the packet is considered unfit and dropped away, thus yielding of failed attack.
Question 5:	Why do you need the root privilege to run the programs that use raw sockets? Where does the program fail if executed without the root privilege? Ans: yes, need root privilege to run raw program. To perform the spoofing of the packets, we need to have the access to an NIC. In short this is how it is defined by the authorities who set networking rules. Due to the fact one can create custom packets that could prove detrimental to a network configuration.
Task 2.3	Sniff and then Spoof at same time?

While complaining got some warning request invigilator to explain why



```
[09/02/22]seed@VM:~/.../Code$ gcc -o sniff Task2.1A.c -lpcap
[09/02/22]seed@VM:~/.../Code$ gcc -o sniff Task2.1B-ICMP.c -lpcap
[09/02/22]seed@VM:~/.../Code$ gcc -o sniff Task2.1B-TCP.c -lpcap
[09/02/22]seed@VM:~/.../Code$ gcc -o sniff Task2.1C.c -lpcap
[09/02/22]seed@VM:~/.../Code$ gcc -o sniff Task2.2.c -lpcap
[09/02/22]seed@VM:~/.../Code$ gcc -o spooficmp Task2.2.c -lpcap
[09/02/22]seed@VM:~/.../Code$ gcc -o sniffspoof Task2.3.c -lpcap
Task2.3.c: In function ‘send_raw_ip_packet’:
Task2.3.c:97:5: warning: implicit declaration of function ‘close’; did you mean ‘pclose’? [-Wimplicit-function-declaration]
   97 |     close(sock);
      |     ^~~~~
      |     pclose
Task2.3.c: In function ‘got_packet’:
Task2.3.c:133:15: warning: initialization discards ‘const’ qualifier from pointer target type [-Wdiscarded-qualifiers]
  133 |   char* data= packet+sizeof(struct ethheader)+sizeof(struct ipheader)+sizeof(struct icmpheader);
      |               ^~~~~~
[09/02/22]seed@VM:~/.../Code$ █
```

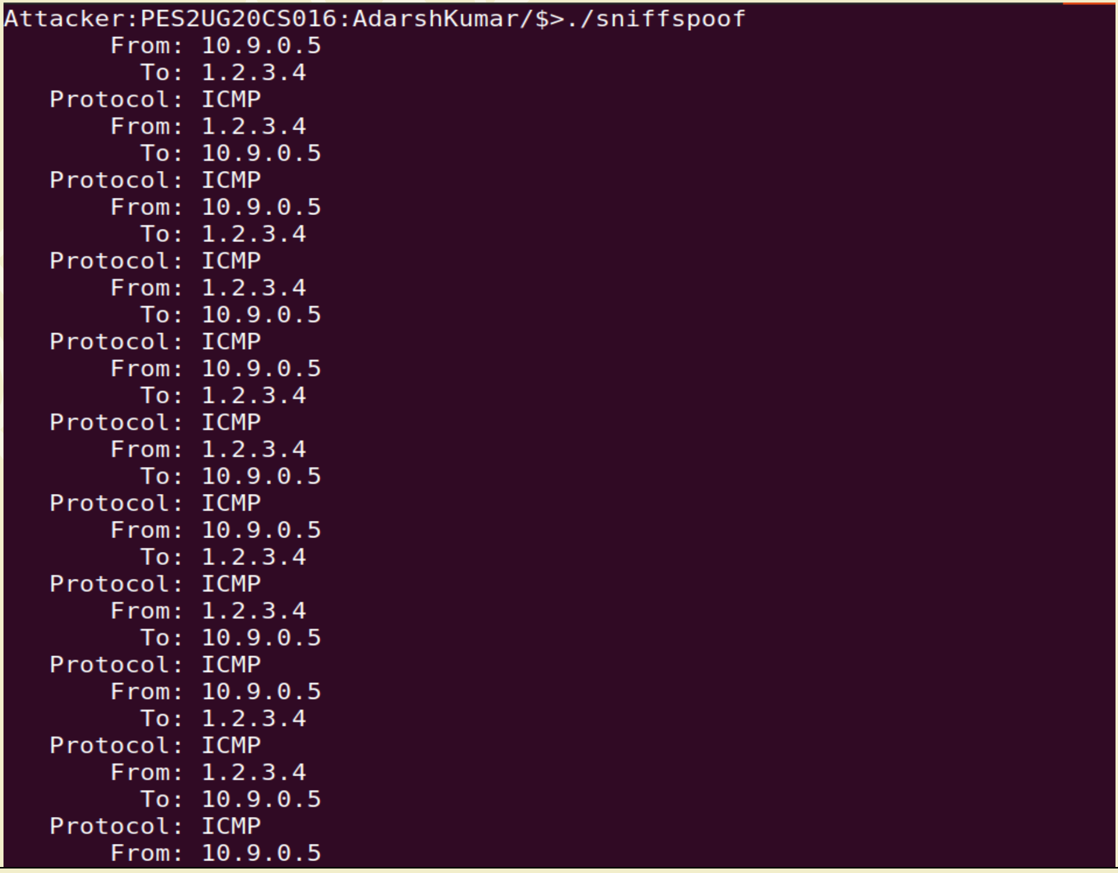
Host-A Terminal:



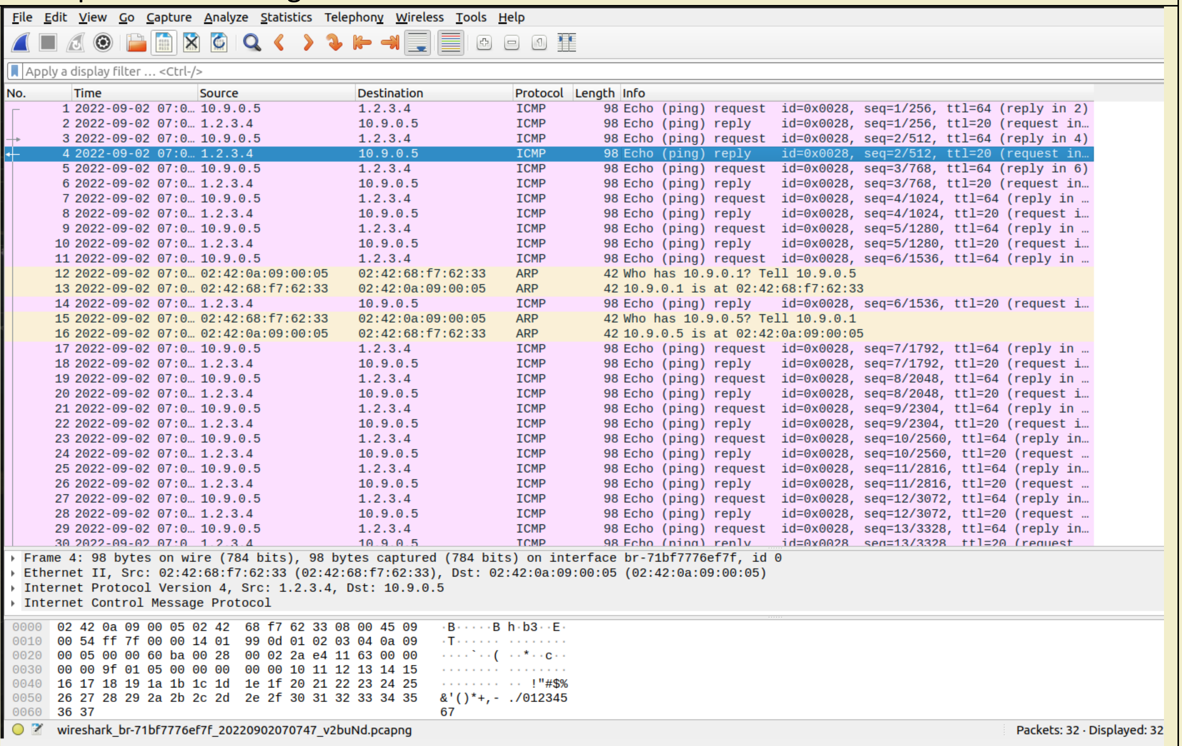
```
HostA:PES2UG20CS016:AdarshKumar/$>ping 1.2.3.4
PING 1.2.3.4 (1.2.3.4) 56(84) bytes of data.
64 bytes from 1.2.3.4: icmp_seq=1 ttl=20 time=381 ms
64 bytes from 1.2.3.4: icmp_seq=2 ttl=20 time=404 ms
64 bytes from 1.2.3.4: icmp_seq=3 ttl=20 time=426 ms
64 bytes from 1.2.3.4: icmp_seq=4 ttl=20 time=449 ms
64 bytes from 1.2.3.4: icmp_seq=5 ttl=20 time=471 ms
64 bytes from 1.2.3.4: icmp_seq=6 ttl=20 time=491 ms
64 bytes from 1.2.3.4: icmp_seq=7 ttl=20 time=514 ms
64 bytes from 1.2.3.4: icmp_seq=8 ttl=20 time=537 ms
64 bytes from 1.2.3.4: icmp_seq=9 ttl=20 time=561 ms
64 bytes from 1.2.3.4: icmp_seq=10 ttl=20 time=581 ms
64 bytes from 1.2.3.4: icmp_seq=11 ttl=20 time=605 ms
64 bytes from 1.2.3.4: icmp_seq=12 ttl=20 time=627 ms
64 bytes from 1.2.3.4: icmp_seq=13 ttl=20 time=649 ms
64 bytes from 1.2.3.4: icmp_seq=14 ttl=20 time=676 ms
64 bytes from 1.2.3.4: icmp_seq=15 ttl=20 time=700 ms
64 bytes from 1.2.3.4: icmp_seq=16 ttl=20 time=714 ms
64 bytes from 1.2.3.4: icmp_seq=17 ttl=20 time=738 ms
64 bytes from 1.2.3.4: icmp_seq=18 ttl=20 time=762 ms
64 bytes from 1.2.3.4: icmp_seq=19 ttl=20 time=786 ms
64 bytes from 1.2.3.4: icmp_seq=20 ttl=20 time=807 ms
64 bytes from 1.2.3.4: icmp_seq=21 ttl=20 time=832 ms
64 bytes from 1.2.3.4: icmp_seq=22 ttl=20 time=848 ms
^C
--- 1.2.3.4 ping statistics ---
23 packets transmitted, 22 received, 4.34783% packet loss, time 22040ms
rtt min/avg/max/mdev = 381.090/616.280/847.548/142.282 ms
HostA:PES2UG20CS016:AdarshKumar/$>
```

Pinging to some non-existing IP address 1.2.3.4 but still able to ping then.

Attacker Terminal:



```
Attacker:PES2UG20CS016:AdarshKumar/$>./sniffspoof
       From: 10.9.0.5
         To: 1.2.3.4
   Protocol: ICMP
       From: 1.2.3.4
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 1.2.3.4
   Protocol: ICMP
       From: 1.2.3.4
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 1.2.3.4
   Protocol: ICMP
       From: 1.2.3.4
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 1.2.3.4
   Protocol: ICMP
       From: 1.2.3.4
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
         To: 1.2.3.4
   Protocol: ICMP
       From: 1.2.3.4
         To: 10.9.0.5
   Protocol: ICMP
       From: 10.9.0.5
```

	As we can see that messages that are sent from 10.9.0.5 are sniffed here and it is using ICMP protocol. Message are intended for the IP 1.2.3.4
Wireshark	 We can see in Wireshark both ICMP echo request and response messages are exchanged between IP 10.9.0.5 and 1.2.3.4

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.     Time              Source              Destination         Protocol Length Info
      1 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=1/256, ttl=64 (reply in 2)
      2 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=1/256, ttl=20 (request in…
      3 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=2/512, ttl=64 (reply in 4)
      4 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=2/512, ttl=20 (request in…
      5 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=3/768, ttl=64 (reply in 6)
      6 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=3/768, ttl=20 (request in…
      7 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=4/1024, ttl=64 (reply in …
      8 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=4/1024, ttl=20 (request i…
      9 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=5/1280, ttl=64 (reply in …
     10 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=5/1280, ttl=20 (request i…
     11 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=6/1536, ttl=64 (reply in …
     12 2022-09-02 07:0… 02:42:0a:09:00:05   02:42:68:f7:62:33   ARP       42 Who has 10.9.0.1? Tell 10.9.0.5
     13 2022-09-02 07:0… 02:42:68:f7:62:33   02:42:0a:09:00:05   ARP       42 10.9.0.1 is at 02:42:68:f7:62:33
     14 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=6/1536, ttl=20 (request i…
     15 2022-09-02 07:0… 02:42:68:f7:62:33   02:42:0a:09:00:05   ARP       42 Who has 10.9.0.5? Tell 10.9.0.1
     16 2022-09-02 07:0… 02:42:0a:09:00:05   02:42:68:f7:62:33   ARP       42 10.9.0.5 is at 02:42:0a:09:00:05
     17 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=7/1792, ttl=64 (reply in …
     18 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=7/1792, ttl=20 (request i…
     19 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=8/2048, ttl=64 (reply in …
     20 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=8/2048, ttl=20 (request i…
     21 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=9/2304, ttl=64 (reply in …
     22 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=9/2304, ttl=20 (request i…
     23 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=10/2560, ttl=64 (reply in…
     24 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=10/2560, ttl=20 (request …
     25 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=11/2816, ttl=64 (reply in…
     26 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=11/2816, ttl=20 (request …
     27 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=12/3072, ttl=64 (reply in…
     28 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=12/3072, ttl=20 (request …
     29 2022-09-02 07:0… 10.9.0.5            1.2.3.4             ICMP      98 Echo (ping) request  id=0x0028, seq=13/3328, ttl=64 (reply in…
     30 2022-09-02 07:0… 1.2.3.4             10.9.0.5            ICMP      98 Echo (ping) reply    id=0x0028, seq=13/3328, ttl=20 (request
```

```
› Frame 4: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface br-71bf7776ef7f, id 0
› Ethernet II, Src: 02:42:68:f7:62:33 (02:42:68:f7:62:33), Dst: 02:42:0a:09:00:05 (02:42:0a:09:00:05)
› Internet Protocol Version 4, Src: 1.2.3.4, Dst: 10.9.0.5
› Internet Control Message Protocol
```

```
0000  02 42 0a 09 00 05 02 42  68 f7 62 33 08 00 45 09   ·B·····B h·b3··E·
0010  00 54 ff 7f 00 00 14 01  99 0d 01 02 03 04 0a 09   ·T······ ········
0020  00 05 00 00 60 ba 00 28  00 02 2a e4 11 63 00 00   ····`··( ··*··c··
0030  00 00 9f 01 05 00 00 00  00 00 10 11 12 13 14 15   ········ ········
0040  16 17 18 19 1a 1b 1c 1d  1e 1f 20 21 22 23 24 25   ········ ·· !"#$%
0050  26 27 28 29 2a 2b 2c 2d  2e 2f 30 31 32 33 34 35   &'()*+,- ./012345
0060  36 37                                              67
```

wireshark_br-71bf7776ef7f_20220902070747_v2buNd.pcapng
Packets: 32 · Displayed: 32