Government Engineering College, Thrissur

CS334 – Network Programming Lab

Documentation -

Exp 7 – RAW Socket Programming in C.

Date of Submission

31 May 2021

Submitted By

Sarthak Anil

Roll No 53

TCR18CS053

GECT CSE S6

Experiment 7

a)Display the header information of UDP and TCP packets during client-server communication using raw sockets.

b) Develop a packet capturing and filtering application using raw sockets.

Compilation of Code

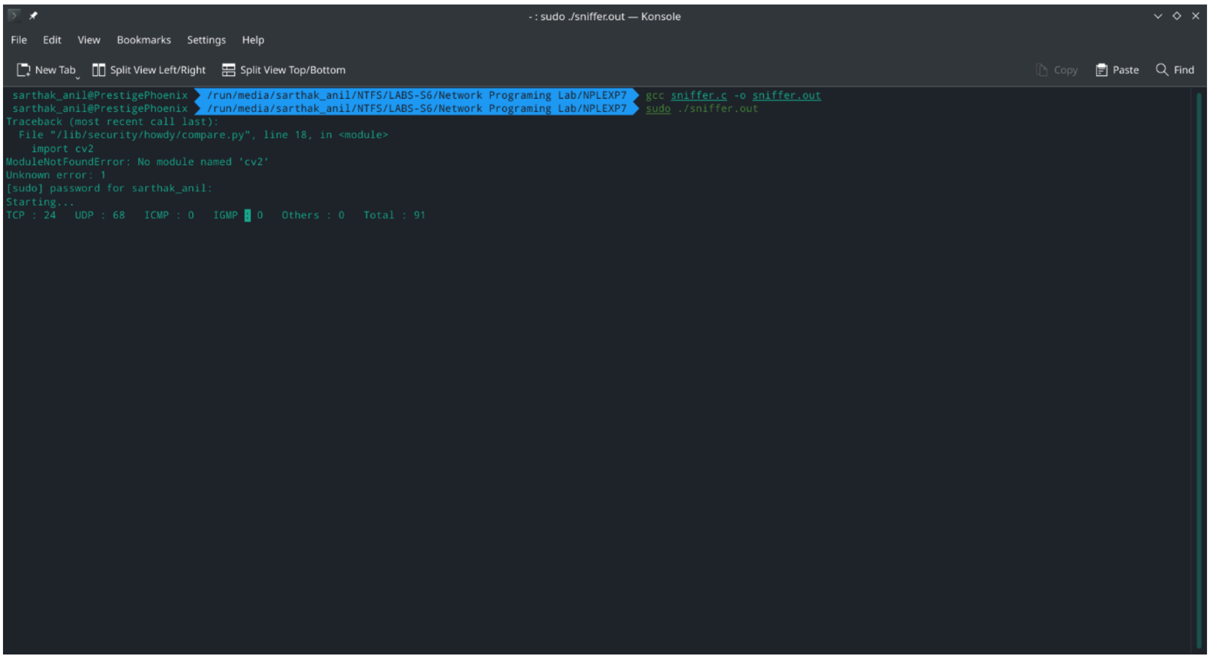
- The program is run with the help of C programming language .
- The code is provided in Client and Server
  - Run gcc raw_tcp.c -o tcp.out
  - Run gcc raw_udp.c -o udp.out
  - Run gcc sniffer.c -o sniffer.out
  - Run sudo ./tcp .out to send a tcp packet and see the header information
  - Run sudo ./udp.out to send a udp packet and see the header information
  - Run sudo ./sniffer.out to send a tcp packet and see the header information
- The code is tested on
  - Manjaro Linux gcc

Note

This program will only work on Linux and need sudo since raw socket is created

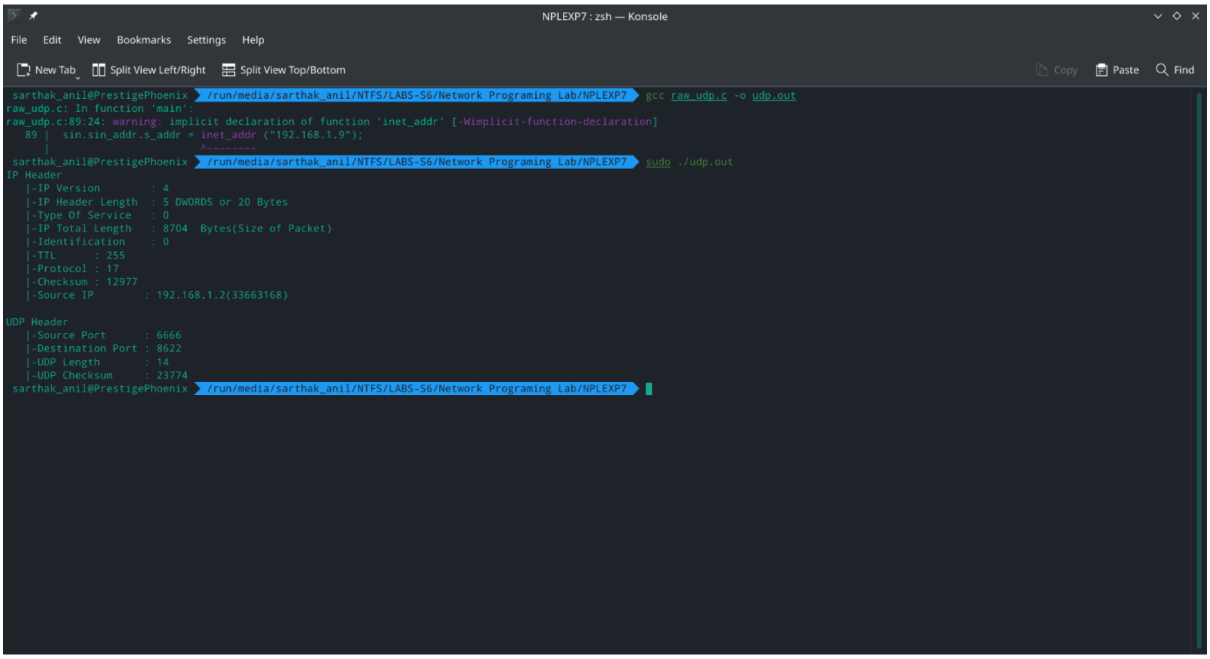
Screenshots

Running the sniffer program



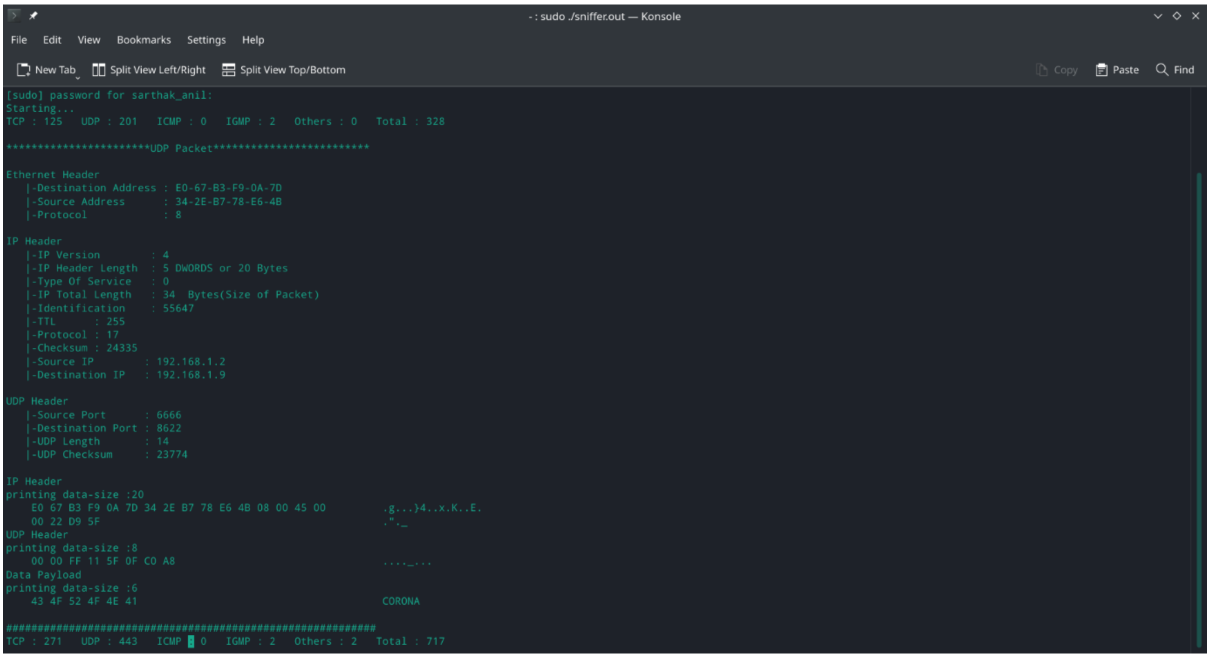
```
 sarthak_anil@PrestigePhoenix  /run/media/sarthak_anil/NTFS/LABS-S6/Network Programing Lab/NPLEXP7  gcc sniffer.c -o sniffer.out
 sarthak_anil@PrestigePhoenix  /run/media/sarthak_anil/NTFS/LABS-S6/Network Programing Lab/NPLEXP7  sudo ./sniffer.out
Traceback (most recent call last):
  File "/lib/security/howdy/compare.py", line 18, in <module>
    import cv2
ModuleNotFoundError: No module named 'cv2'
Unknown error: 1
[sudo] password for sarthak_anil:
Starting...
TCP : 24   UDP : 68   ICMP : 0   IGMP : 0   Others : 0   Total : 91
```

Running raw_udp.c to send a packet and to see the header information



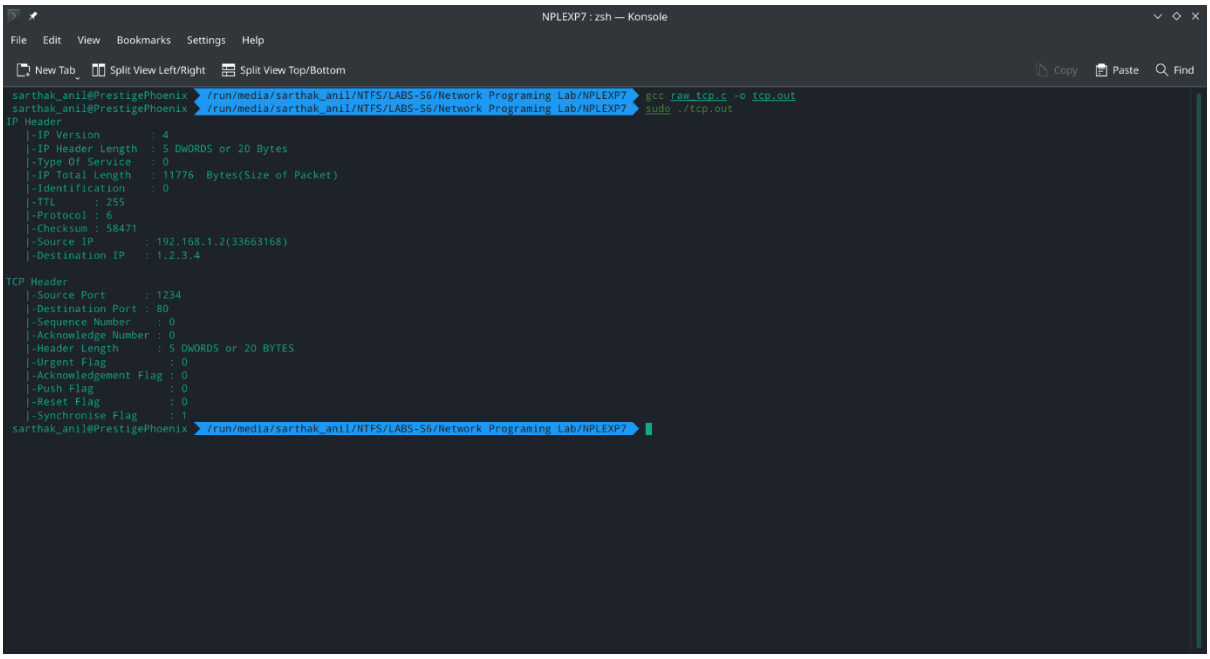
```
 sarthak_anil@PrestigePhoenix  /run/media/sarthak_anil/NTFS/LABS-S6/Network Programing Lab/NPLEXP7  gcc raw_udp.c -o udp.out
raw_udp.c: In function 'main':
raw_udp.c:89:24: warning: implicit declaration of function 'inet_addr' [-Wimplicit-function-declaration]
   89 |   sin.sin_addr.s_addr = inet_addr ("192.168.1.9");
      |                         ^~~~~~~~~
 sarthak_anil@PrestigePhoenix  /run/media/sarthak_anil/NTFS/LABS-S6/Network Programing Lab/NPLEXP7  sudo ./udp.out
IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 8704  Bytes(Size of Packet)
   |-Identification    : 0
   |-TTL      : 255
   |-Protocol : 17
   |-Checksum : 12977
   |-Source IP        : 192.168.1.2(33663168)

UDP Header
   |-Source Port      : 6666
   |-Destination Port : 8622
   |-UDP Length       : 14
   |-UDP Checksum     : 23774
 sarthak_anil@PrestigePhoenix  /run/media/sarthak_anil/NTFS/LABS-S6/Network Programing Lab/NPLEXP7 
```

The UDP packet being captured by sniffers



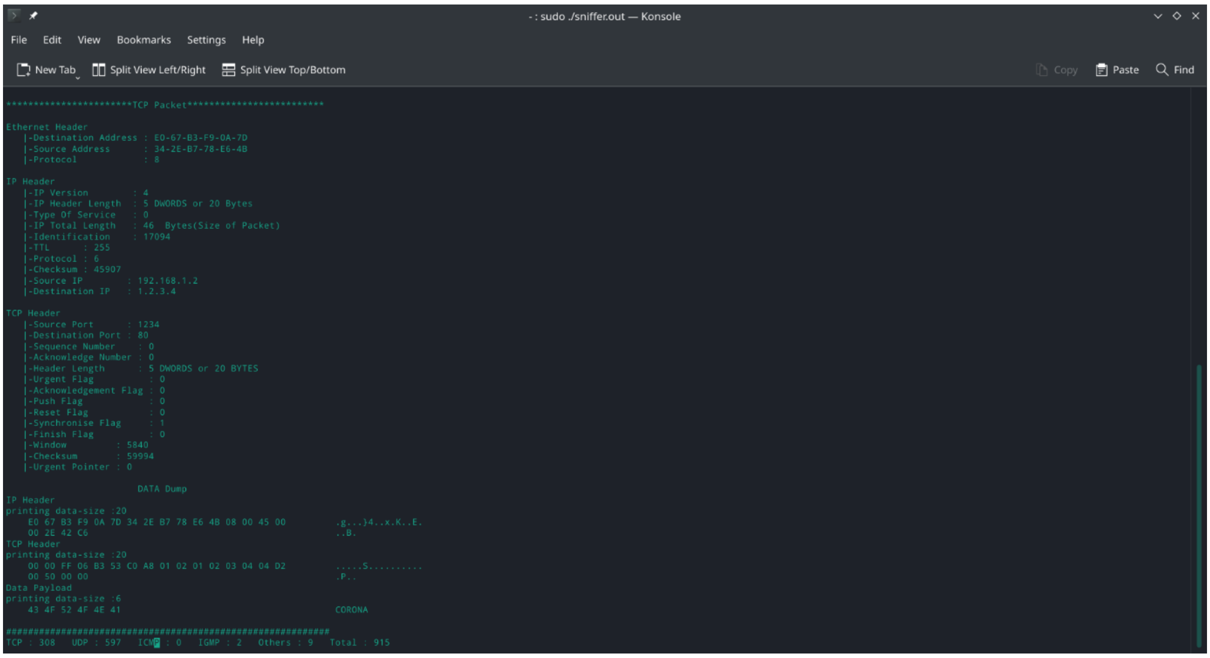
```
[sudo] password for sarthak_anil:
Starting...
TCP : 125   UDP : 201   ICMP : 0   IGMP : 2   Others : 0   Total : 328

***********************UDP Packet*************************

Ethernet Header
   |-Destination Address : E0-67-B3-F9-0A-7D
   |-Source Address      : 34-2E-B7-78-E6-4B
   |-Protocol            : 8

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 34  Bytes(Size of Packet)
   |-Identification    : 55647
   |-TTL      : 255
   |-Protocol : 17
   |-Checksum : 24335
   |-Source IP        : 192.168.1.2
   |-Destination IP   : 192.168.1.9

UDP Header
   |-Source Port      : 6666
   |-Destination Port : 8622
   |-UDP Length       : 14
   |-UDP Checksum     : 23774

IP Header
printing data-size :20
    E0 67 B3 F9 0A 7D 34 2E B7 78 E6 4B 08 00 45 00         .g...}4..x.K..E.
    00 22 D9 5F                                             ."._
UDP Header
printing data-size :8
    00 00 FF 11 5F 0F C0 A8                                 ...._...
Data Payload
printing data-size :6
    43 4F 52 4F 4E 41                                       CORONA

###########################################################
TCP : 271   UDP : 443   ICMP : 0   IGMP : 2   Others : 2   Total : 717
```

Running raw_tcp.c to send a tcp packet and to see the header information



```
 sarthak_anil@PrestigePhoenix  /run/media/sarthak_anil/NTFS/LABS-S6/Network Programing Lab/NPLEXP7  gcc raw_tcp.c -o tcp.out
 sarthak_anil@PrestigePhoenix  /run/media/sarthak_anil/NTFS/LABS-S6/Network Programing Lab/NPLEXP7  sudo ./tcp.out
IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 11776  Bytes(Size of Packet)
   |-Identification    : 0
   |-TTL      : 255
   |-Protocol : 6
   |-Checksum : 58471
   |-Source IP        : 192.168.1.2(33663168)
   |-Destination IP   : 1.2.3.4

TCP Header
   |-Source Port      : 1234
   |-Destination Port : 80
   |-Sequence Number    : 0
   |-Acknowledge Number : 0
   |-Header Length      : 5 DWORDS or 20 BYTES
   |-Urgent Flag          : 0
   |-Acknowledgement Flag : 0
   |-Push Flag            : 0
   |-Reset Flag           : 0
   |-Synchronise Flag     : 1
 sarthak_anil@PrestigePhoenix  /run/media/sarthak_anil/NTFS/LABS-S6/Network Programing Lab/NPLEXP7 
```

The TCP packet being captured by sniffers



```
***********************TCP Packet*************************

Ethernet Header
   |-Destination Address : E0-67-B3-F9-0A-7D
   |-Source Address      : 34-2E-B7-78-E6-4B
   |-Protocol            : 8

IP Header
   |-IP Version        : 4
   |-IP Header Length  : 5 DWORDS or 20 Bytes
   |-Type Of Service   : 0
   |-IP Total Length   : 46  Bytes(Size of Packet)
   |-Identification    : 17094
   |-TTL      : 255
   |-Protocol : 6
   |-Checksum : 45907
   |-Source IP        : 192.168.1.2
   |-Destination IP   : 1.2.3.4

TCP Header
   |-Source Port      : 1234
   |-Destination Port : 80
   |-Sequence Number    : 0
   |-Acknowledge Number : 0
   |-Header Length      : 5 DWORDS or 20 BYTES
   |-Urgent Flag          : 0
   |-Acknowledgement Flag : 0
   |-Push Flag            : 0
   |-Reset Flag           : 0
   |-Synchronise Flag     : 1
   |-Finish Flag          : 0
   |-Window         : 5840
   |-Checksum       : 59994
   |-Urgent Pointer : 0

                        DATA Dump
IP Header
printing data-size :20
    E0 67 B3 F9 0A 7D 34 2E B7 78 E6 4B 08 00 45 00         .g...}4..x.K..E.
    00 2E 42 C6                                             ..B.
TCP Header
printing data-size :20
    00 00 FF 06 B3 53 C0 A8 01 02 01 02 03 04 04 D2         .....S..........
    00 50 00 00                                             .P..
Data Payload
printing data-size :6
    43 4F 52 4F 4E 41                                       CORONA

###########################################################
TCP : 308   UDP : 597   ICMP : 0   IGMP : 2   Others : 9   Total : 915
```