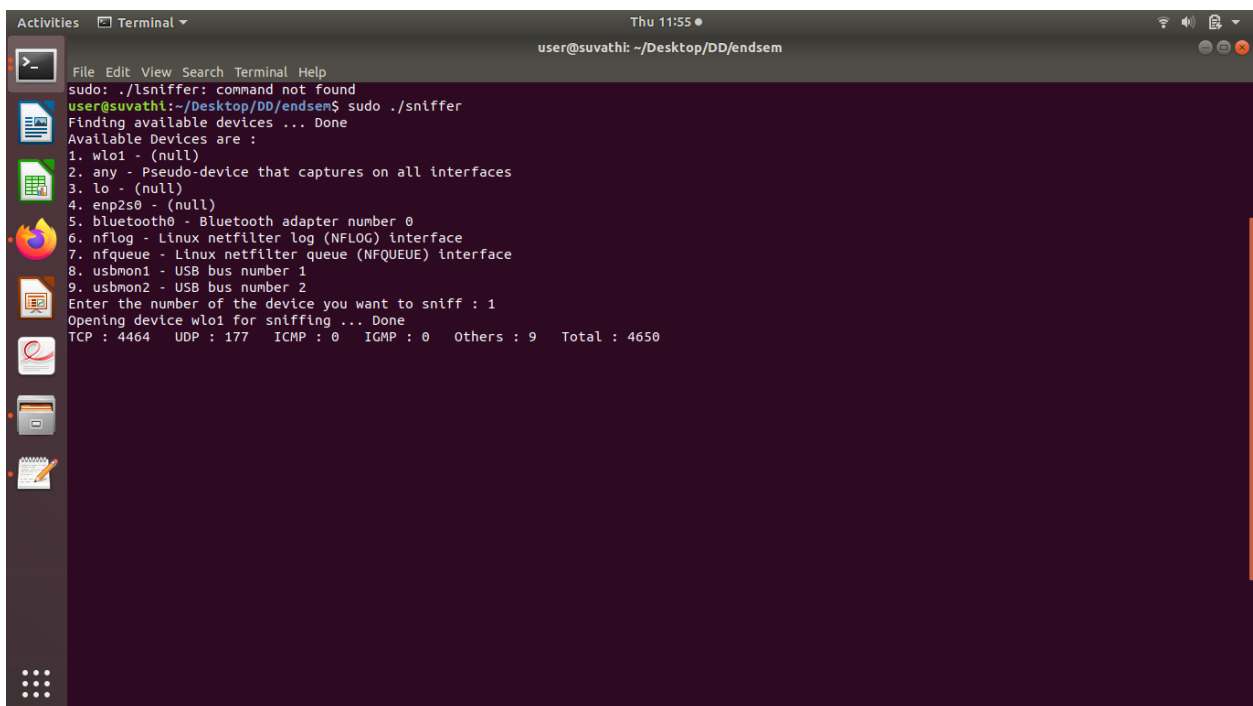


OBSERVATIONS

4. Write a C program to capture network packets

So to run the code i used two techniques one by incorporating libpcap(Libpcap is a packet capture library for linux which can be used to sniff packets or network traffic over a network interface.)and without libpcap. Since it took to long to show the output packets. I screenshoted them at different time intervals.

WITH LIBPCAP:



```
user@suvathi: ~/Desktop/DD/endsem
File Edit View Search Terminal Help
sudo: ./lsniffer: command not found
user@suvathi:~/Desktop/DD/endsem$ sudo ./sniffer
Finding available devices ... Done
Available Devices are :
1. wlo1 - (null)
2. any - Pseudo-device that captures on all interfaces
3. lo - (null)
4. enp2s0 - (null)
5. bluetooth0 - Bluetooth adapter number 0
6. nflog - Linux netfilter log (NFLOG) interface
7. nfqueue - Linux netfilter queue (NFQUEUE) interface
8. usbmon1 - USB bus number 1
9. usbmon2 - USB bus number 2
Enter the number of the device you want to sniff : 1
Opening device wlo1 for sniffing ... Done
TCP : 4464  UDP : 177  ICMP : 0  IGMP : 0  Others : 9  Total : 4650
```

Activities Terminal Thu 13:01 user@suvathi: ~/Desktop/DD/endsem

```
File Edit View Search Terminal Help
Opening device wlo1 for sniffing ... Done
TCP : 4464  UDP : 177  ICMP : 0  IGMP : 0  Others : 9  Total : 4650
```

TCP : 4478 UDP : 177 ICMP : 0 IGMP : 0 Others : 9 Total : 4664
TCP : 98102 UDP : 4449 ICMP : 0 IGMP : 21 Others : 489 Total : 103061

Activities Terminal Thu 13:14 user@suvathi: ~/Desktop/DD/endsem

```
File Edit View Search Terminal Help
Opening device wlo1 for sniffing ... Done
TCP : 4464  UDP : 177  ICMP : 0  IGMP : 0  Others : 9  Total : 4650
```

TCP : 4478 UDP : 177 ICMP : 0 IGMP : 0 Others : 9 Total : 4664
TCP : 139158 UDP : 5056 ICMP : 2 IGMP : 21 Others : 606 Total : 144842

WITHOUT LIBPCAP:

```
Activities Terminal Thu 12:15 ● user@suvathi: ~/Desktop/DD/endsem

File Edit View Search Terminal Help
sniff.c:38:8: warning: implicit declaration of function 'pcap_compile' [-Wimplicit-function-declaration]
    if(pcap_compile(descr, &fp, argv[1], 0, netp) == -1) {
    ^
sniff.c:39:9: warning: incompatible implicit declaration of built-in function 'fprintf'
    fprintf(stderr, "Error calling pcap_compile\n");
    ^
sniff.c:39:9: note: include '<stdio.h>' or provide a declaration of 'fprintf'
sniff.c:40:9: warning: incompatible implicit declaration of built-in function 'exit'
    exit(1);
    ^
sniff.c:40:9: note: include '<stdlib.h>' or provide a declaration of 'exit'
sniff.c:44:8: warning: implicit declaration of function 'pcap_setfilter' [-Wimplicit-function-declaration]
    if(pcap_setfilter(descr, &fp) == -1) {
    ^
sniff.c:45:9: warning: incompatible implicit declaration of built-in function 'fprintf'
    fprintf(stderr, "Error setting filter\n");
    ^
sniff.c:45:9: note: include '<stdio.h>' or provide a declaration of 'fprintf'
sniff.c:46:9: warning: incompatible implicit declaration of built-in function 'exit'
    exit(1);
    ^
sniff.c:46:9: note: include '<stdlib.h>' or provide a declaration of 'exit'
sniff.c:50:5: warning: implicit declaration of function 'pcap_loop' [-Wimplicit-function-declaration]
    pcap_loop(descr, -1, my_callback, NULL);
    ^
sniff.c:50:26: error: 'my_callback' undeclared (first use in this function)
    pcap_loop(descr, -1, my_callback, NULL);
                           ^
[1]+  Done                  gedit qn4.c
user@suvathi:~/Desktop/DD/endsem$ gcc sniff.c && sudo ./a.out
sniff.c: In function 'main':
sniff.c:54:2: warning: implicit declaration of function 'close'; did you mean 'pclose'? [-Wimplicit-function-declaration]
    close(sock_raw);
    ^
    pclose
[sudo] password for user:
Starting...
TCP : 18695  UDP : 0  ICMP : 0  IGMP : 0  Others : 0  Total : 18694
```

```
Activities Terminal Thu 13:01 ● user@suvathi: ~/Desktop/DD/endsem

File Edit View Search Terminal Help
sniff.c:38:8: warning: implicit declaration of function 'pcap_compile' [-Wimplicit-function-declaration]
    if(pcap_compile(descr, &fp, argv[1], 0, netp) == -1) {
    ^
sniff.c:39:9: warning: incompatible implicit declaration of built-in function 'fprintf'
    fprintf(stderr, "Error calling pcap_compile\n");
    ^
sniff.c:39:9: note: include '<stdio.h>' or provide a declaration of 'fprintf'
sniff.c:40:9: warning: incompatible implicit declaration of built-in function 'exit'
    exit(1);
    ^
sniff.c:40:9: note: include '<stdlib.h>' or provide a declaration of 'exit'
sniff.c:44:8: warning: implicit declaration of function 'pcap_setfilter' [-Wimplicit-function-declaration]
    if(pcap_setfilter(descr, &fp) == -1) {
    ^
sniff.c:45:9: warning: incompatible implicit declaration of built-in function 'fprintf'
    fprintf(stderr, "Error setting filter\n");
    ^
sniff.c:45:9: note: include '<stdio.h>' or provide a declaration of 'fprintf'
sniff.c:46:9: warning: incompatible implicit declaration of built-in function 'exit'
    exit(1);
    ^
sniff.c:46:9: note: include '<stdlib.h>' or provide a declaration of 'exit'
sniff.c:50:5: warning: implicit declaration of function 'pcap_loop' [-Wimplicit-function-declaration]
    pcap_loop(descr, -1, my_callback, NULL);
    ^
sniff.c:50:26: error: 'my_callback' undeclared (first use in this function)
    pcap_loop(descr, -1, my_callback, NULL);
                           ^
[1]+  Done                  gedit qn4.c
user@suvathi:~/Desktop/DD/endsem$ gcc sniff.c && sudo ./a.out
sniff.c: In function 'main':
sniff.c:54:2: warning: implicit declaration of function 'close'; did you mean 'pclose'? [-Wimplicit-function-declaration]
    close(sock_raw);
    ^
    pclose
[sudo] password for user:
Starting...
TCP : 59248  UDP : 0  ICMP : 0  IGMP : 0  Others : 0  Total : 59247
```

```
Activities Terminal Thu 13:14 user@suvathi: ~/Desktop/DD/endsem

File Edit View Search Terminal Help

sniff.c:38:8: warning: implicit declaration of function 'pcap_compile' [-Wimplicit-function-declaration]
    if(pcap_compile(descr, &fp, argv[1], 0, netp) == -1) {
sniff.c:39:9: warning: incompatible implicit declaration of built-in function 'fprintf'
    fprintf(stderr, "Error calling pcap_compile\n");
sniff.c:39:9: note: include '<stdio.h>' or provide a declaration of 'fprintf'
sniff.c:40:9: warning: incompatible implicit declaration of built-in function 'exit'
    exit(1);
sniff.c:40:9: note: include '<stdlib.h>' or provide a declaration of 'exit'
sniff.c:44:8: warning: implicit declaration of function 'pcap_setfilter' [-Wimplicit-function-declaration]
    if(pcap_setfilter(descr, &fp) == -1) {
sniff.c:45:9: warning: incompatible implicit declaration of built-in function 'fprintf'
    fprintf(stderr, "Error setting filter\n");
sniff.c:45:9: note: include '<stdio.h>' or provide a declaration of 'fprintf'
sniff.c:46:9: warning: incompatible implicit declaration of built-in function 'exit'
    exit(1);
sniff.c:46:9: note: include '<stdlib.h>' or provide a declaration of 'exit'
sniff.c:50:5: warning: implicit declaration of function 'pcap_loop' [-Wimplicit-function-declaration]
    pcap_loop(descr, -1, my_callback, NULL);
sniff.c:50:26: error: 'my_callback' undeclared (first use in this function)
    pcap_loop(descr, -1, my_callback, NULL);
[1]+ Done gedit qn4.c
user@suvathi:~/Desktop/DD/endsem$ gcc sniff.c && sudo ./a.out
sniff.c: In function 'main':
sniff.c:54:2: warning: implicit declaration of function 'close'; did you mean 'pclose'? [-Wimplicit-function-declaration]
    close(sock_raw);
pclose
[sudo] password for user:
Starting...
TCP : 83122 UDP : 0 ICMP : 0 IGMP : 0 Others : 0 Total : 83122
```

Since i could conclude the result , i recorded the packets recived by each of them.With libpcap it shows less packets compared to without libpcap.