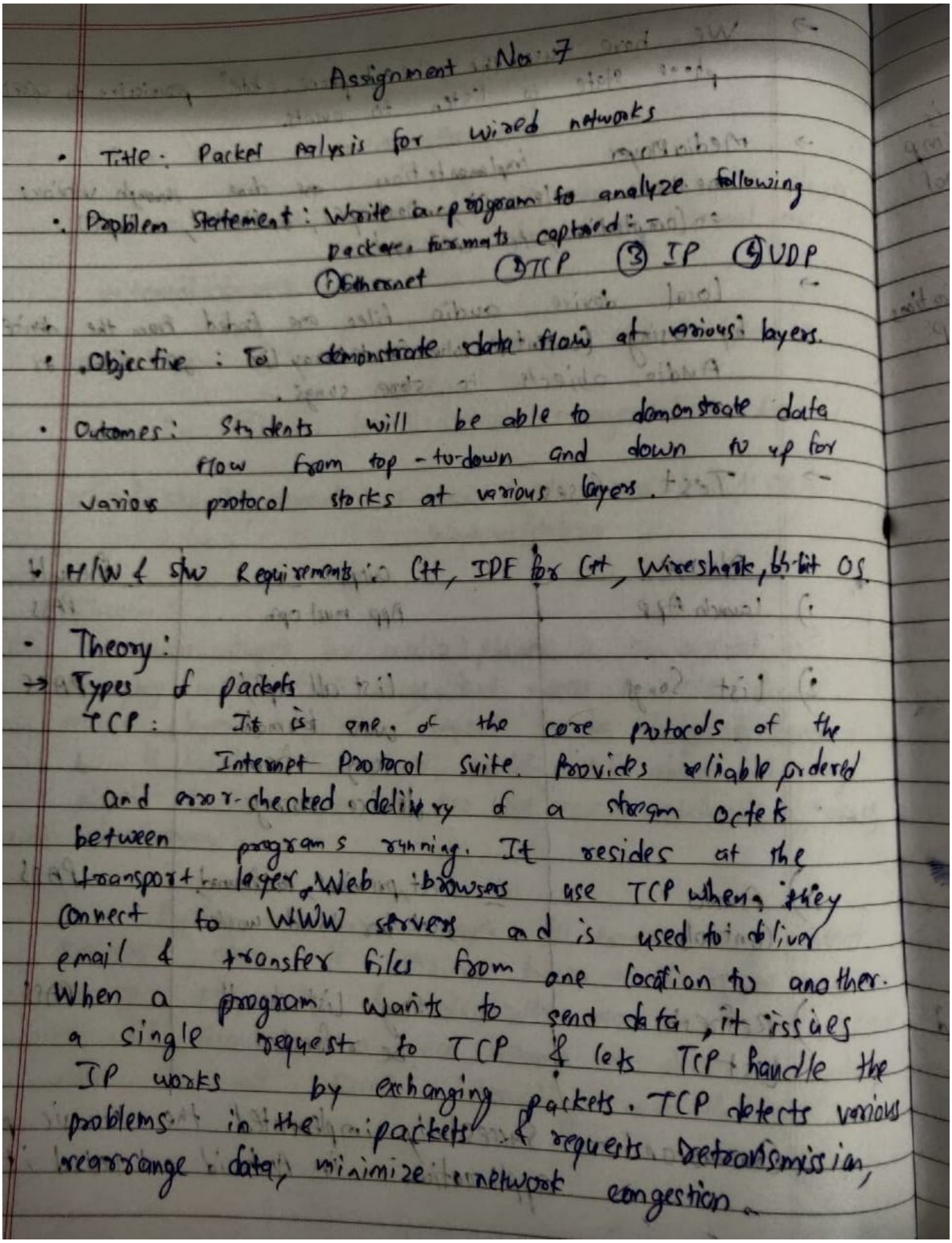
//31139- Durvesh- CNLA7 (packetanalyzer)

Write-up



Assignment No. 7

- Title: Packet Aalysis for wired networks
- Problem Statement: Write a program for analyze following packet formats captured:- ① Ethernet ② TCP ③ IP ④ UDP
- Objective: To demonstrate data flow at various layers.
- Outcomes: Students will be able to demonstrate data flow from top-to-down and down to up for various protocol stacks at various layers.
- H/W & S/W Requirements: C++, IDE for C++, Wireshark, 64-bit OS.
- Theory:

→ Types of packets

TCP: It is one of the core protocols of the Internet Protocol Suite. Provides reliable ordered and error-checked delivery of a stream octets between programs running. It resides at the transport layer. Web browsers use TCP when they connect to WWW servers and is used to deliver email & transfer files from one location to another. When a program wants to send data, it issues a single request to TCP & lets TCP handle the IP works by exchanging packets. TCP detects various problems in the packets & requests retransmission, rearrange data, minimize network congestion.

TCP Header

	0	1	2	3
0	Source Port		Destination Port	
4	~~No~~ Sequence Number			
8	Acknowledgement Number			
12	Offset	Received	Flags TCP	Window
16	Checksum		Urgent Pointer	
20	TCP Options (Optional)			

20 Bytes

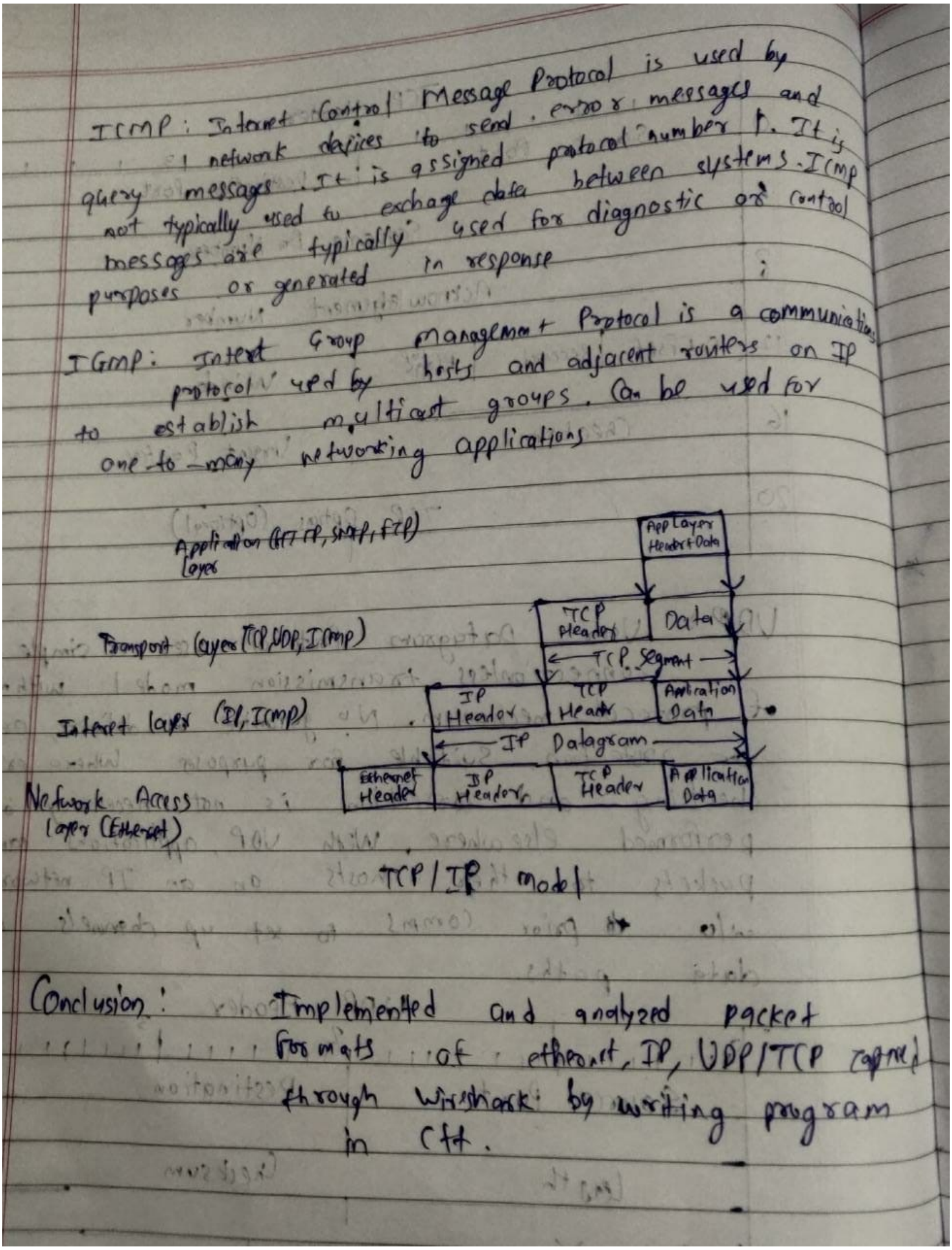
UDP : User Datagram Protocol uses a simple connectionless transmission model with minimum of protocol mechanism. No gurantee of delivery, ordering or protection. Suitable for purposes where error checking and correction is not necessary or is performed elsewhere. With UDP, applications can send packets to other hosts on an IP network w/o prior comms to set up channels or data paths.

UDP Header

0	1	2	3
Source Port		Destination	
Length		Checksum	

8 Bytes

Nibble ← → Byte ← → Word



ICMP: Internet Control Message Protocol is used by network devices to send error messages and query messages. It is assigned protocol number 1. It is not typically used to exchage data between systems. ICMP messages are typically used for diagnostic or control purposes or generated in response

IGMP: Internet Group Management Protocol is a communication protocol used by hosts and adjacent routers on IP to establish multicast groups. Can be used for one-to-many networking applications

TCP/IP model

Conclusion: Implemented and analyzed packet formats of ethernet, IP, UDP/TCP captured through Wireshark by writing program in C++.

Code

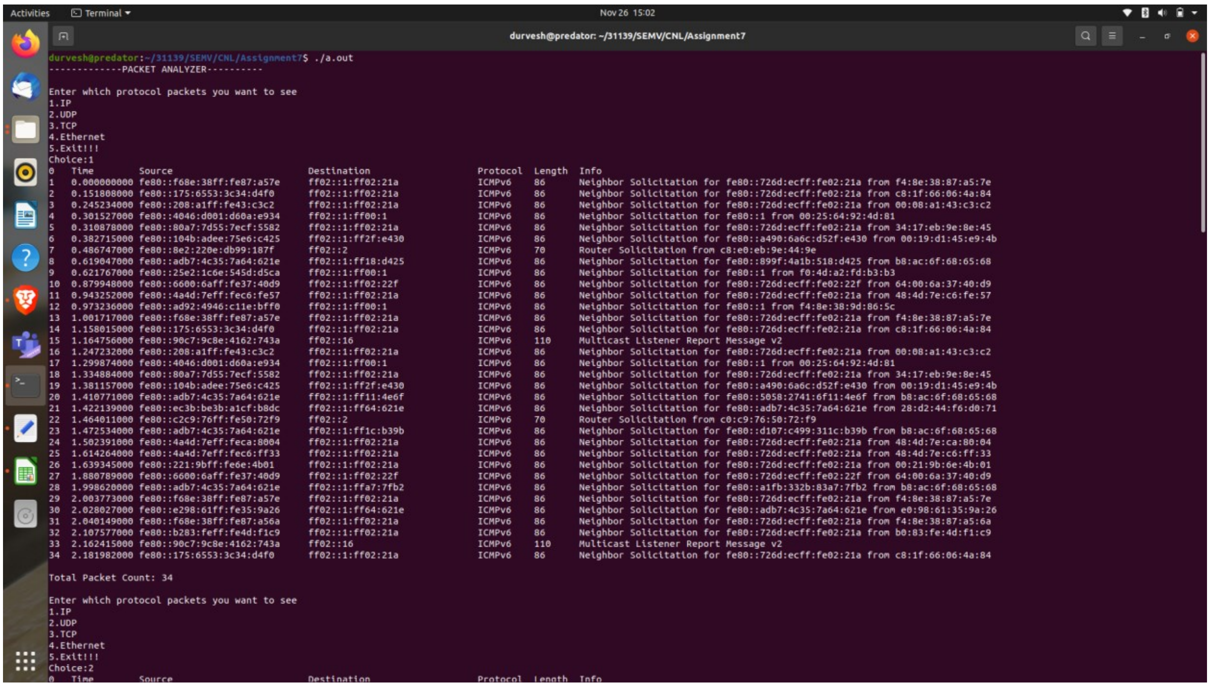
-----packetanalyzer.cpp

```
#include <iostream>
```

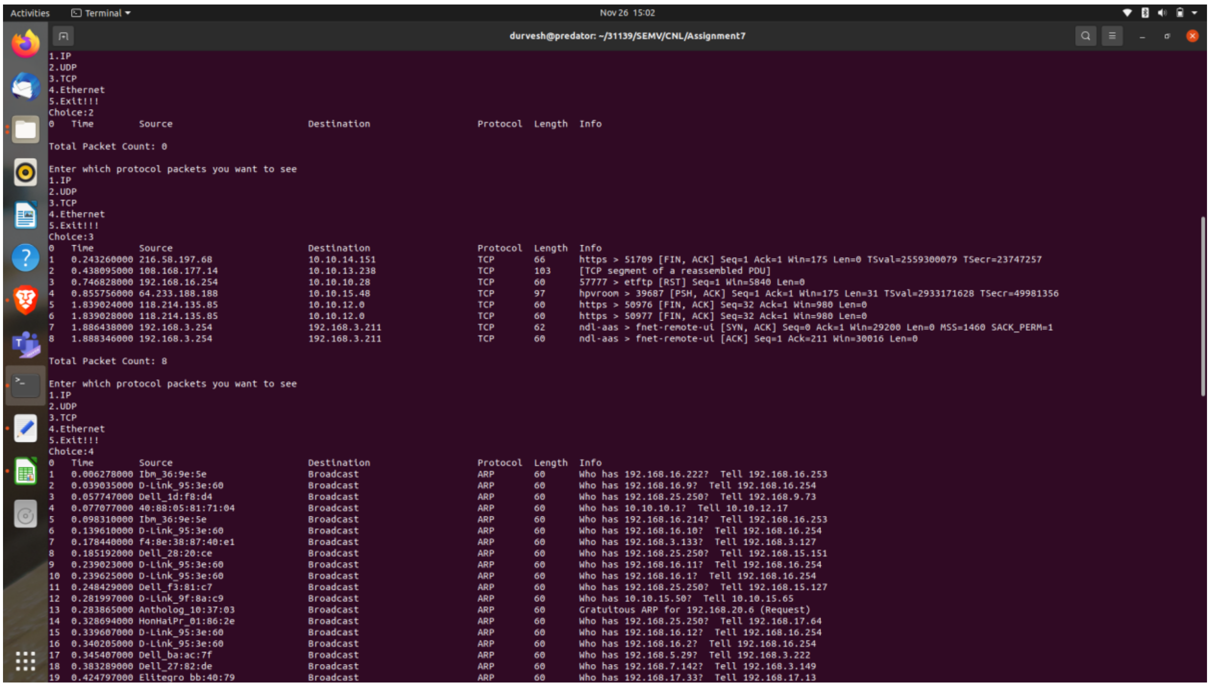
```
#include<fstream>
#include <iomanip>
#include<string>
using namespace std;

int main() {
	cout << "-------------PACKET ANALYZER----------" << endl;
	string value, sr_no,time,source,destination,info,protocol,len;
	int count=-1,i=0;

	int choice=0;
	while(choice!=5)
	{
		ifstream file("data.csv");
		count=-1;
		i=0;
	cout<<"\nEnter which protocol packets you want to see"<<endl;
	cout<<"1.IP\n2.UDP\n3.TCP\n4.Ethernet\n5.Exit!!!\nChoice:";
	cin>>choice;
	string protocolChoice;
	string[] protocolChoices=["ICMPv6","UDP","TCP","ARP"];
	if (choice>5 || choice<1){
		protocolChoice = "ARP";
	}
	else if(choice==5){
	break;

	}
	else{
		protocolChoice = protocolChoices[choice-1];
	}
if(choice==5){
break;
}
while(file.good())
{
    getline(file,sr_no,',');
    getline(file,time,',');
    getline(file,source,',');
    getline(file,destination,',');
    getline(file,protocol,',');
    getline(file,len,',');
    getline(file,info,'\n');

    protocol=string(protocol,1,protocol.length()-2);

    if(protocol=="Protocol"||protocol==protocolChoice)
    {
        cout <<setw(4)<<left<<i++;
        cout <<setw(12)<<left<< string( time, 1, time.length()-2 );
        cout << setw(30)<<left<<string( source, 1, source.length()-2 );
        cout << setw(30)<<left<<string( destination, 1, destination.length()-2 );
        cout <<setw(8)<<left<<protocol<<"  ";
        cout <<setw(8)<<left<< string( len, 1, len.length()-2 );
        cout << string( info, 1, info.length()-2 )<<"\n";
        count++;
    }
}
file.close();
cout<<"\nTotal Packet Count: "<<count<<endl;
}while(choice!=5);
return 0;
```

```
}
```

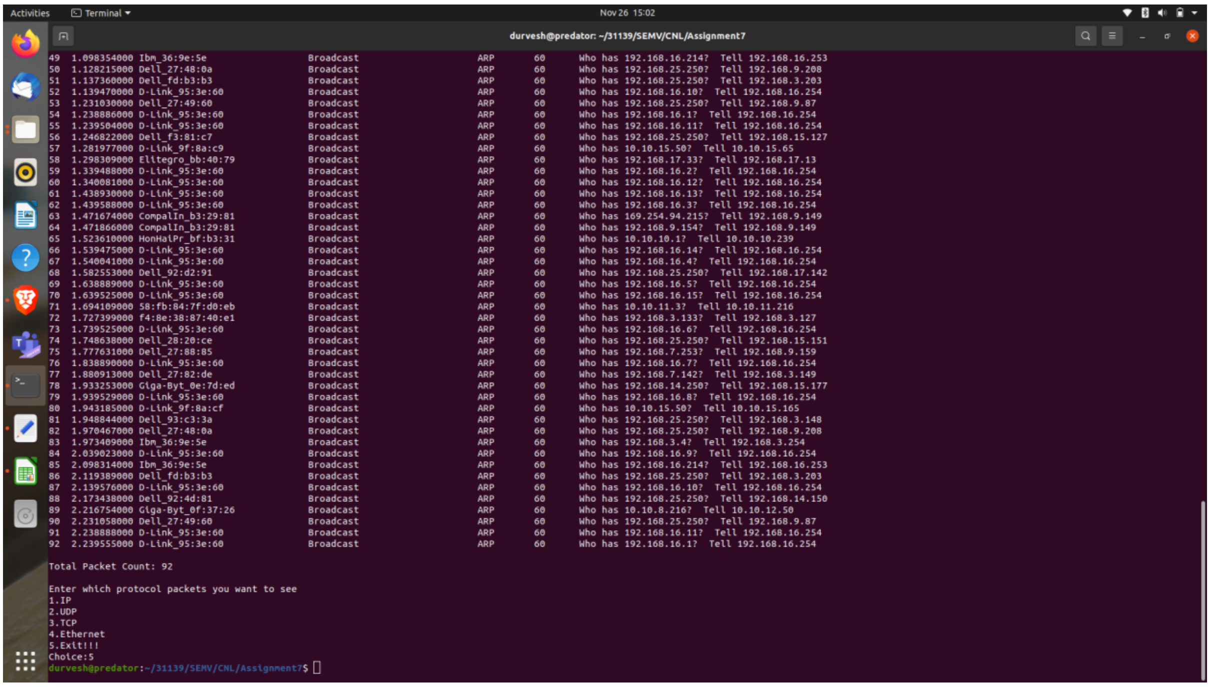
Outputs:



```
durvesh@predator:~/31139/SEMV/CNL/Assignment7$ ./a.out
------------PACKET ANALYZER----------

Enter which protocol packets you want to see
1.IP
2.UDP
3.TCP
4.Ethernet
5.Exit!!!
Choice:1
0   Time        Source                        Destination                   Protocol  Length  Info
1   0.000000000 fe80::f68e:38ff:fe87:a57e     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from f4:8e:38:87:a5:7e
2   0.151808000 fe80::175:6553:3c34:d4f0      ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from c8:1f:66:06:4a:84
3   0.245234000 fe80::208:a1ff:fe43:c3c2      ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from 00:08:a1:43:c3:c2
4   0.301527000 fe80::4046:d001:d60a:e934     ff02::1:ff00:1                ICMPv6    86      Neighbor Solicitation for fe80::1 from 00:25:64:92:4d:81
5   0.310878000 fe80::80a7:7d55:7ecf:5582     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from 34:17:eb:9e:8e:45
6   0.382715000 fe80::104b:adee:75e6:c425     ff02::1:ff2f:e430             ICMPv6    86      Neighbor Solicitation for fe80::a490:6a6c:d52f:e430 from 00:19:d1:45:e9:4b
7   0.486747000 fe80::8e2:220e:db99:187f      ff02::2                       ICMPv6    70      Router Solicitation from c8:e0:eb:9e:44:9e
8   0.619047000 fe80::adb7:4c35:7a64:621e     ff02::1:ff18:d425             ICMPv6    86      Neighbor Solicitation for fe80::899f:4a1b:518:d425 from b8:ac:6f:68:65:68
9   0.621767000 fe80::25e2:1c6e:545d:d5ca     ff02::1:ff00:1                ICMPv6    86      Neighbor Solicitation for fe80::1 from f0:4d:a2:fd:b3:b3
10  0.879948000 fe80::6600:6aff:fe37:40d9     ff02::1:ff02:22f              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:22f from 64:00:6a:37:40:d9
11  0.943252000 fe80::4a4d:7eff:fec6:fe57     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from 48:4d:7e:c6:fe:57
12  0.973236000 fe80::ad92:4946:c11e:bff0     ff02::1:ff00:1                ICMPv6    86      Neighbor Solicitation for fe80::1 from f4:8e:38:9d:86:5c
13  1.001717000 fe80::f68e:38ff:fe87:a57e     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from f4:8e:38:87:a5:7e
14  1.158015000 fe80::175:6553:3c34:d4f0      ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from c8:1f:66:06:4a:84
15  1.164756000 fe80::90c7:9c8e:4162:743a     ff02::16                      ICMPv6    110     Multicast Listener Report Message v2
16  1.247232000 fe80::208:a1ff:fe43:c3c2      ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from 00:08:a1:43:c3:c2
17  1.299874000 fe80::4046:d001:d60a:e934     ff02::1:ff00:1                ICMPv6    86      Neighbor Solicitation for fe80::1 from 00:25:64:92:4d:81
18  1.334884000 fe80::80a7:7d55:7ecf:5582     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from 34:17:eb:9e:8e:45
19  1.381157000 fe80::104b:adee:75e6:c425     ff02::1:ff2f:e430             ICMPv6    86      Neighbor Solicitation for fe80::a490:6a6c:d52f:e430 from 00:19:d1:45:e9:4b
20  1.410771000 fe80::adb7:4c35:7a64:621e     ff02::1:ff11:4e6f             ICMPv6    86      Neighbor Solicitation for fe80::5058:2741:6f11:4e6f from b8:ac:6f:68:65:68
21  1.422139000 fe80::ec3b:be3b:a1cf:b8dc     ff02::1:ff64:621e             ICMPv6    86      Neighbor Solicitation for fe80::adb7:4c35:7a64:621e from 28:d2:44:f6:d0:71
22  1.464011000 fe80::c2c9:76ff:fe50:72f9     ff02::2                       ICMPv6    70      Router Solicitation from c0:c9:76:50:72:f9
23  1.472534000 fe80::adb7:4c35:7a64:621e     ff02::1:ff1c:b39b             ICMPv6    86      Neighbor Solicitation for fe80::d107:c499:311c:b39b from b8:ac:6f:68:65:68
24  1.502391000 fe80::4a4d:7eff:feca:8004     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from 48:4d:7e:ca:80:04
25  1.614264000 fe80::4a4d:7eff:fec6:ff33     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from 48:4d:7e:c6:ff:33
26  1.639345000 fe80::221:9bff:fe6e:4b01      ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from 00:21:9b:6e:4b:01
27  1.880789000 fe80::6600:6aff:fe37:40d9     ff02::1:ff02:22f              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:22f from 64:00:6a:37:40:d9
28  1.998620000 fe80::adb7:4c35:7a64:621e     ff02::1:ffa7:7fb2             ICMPv6    86      Neighbor Solicitation for fe80::a1fb:332b:83a7:7fb2 from b8:ac:6f:68:65:68
29  2.003773000 fe80::f68e:38ff:fe87:a57e     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from f4:8e:38:87:a5:7e
30  2.028027000 fe80::e298:61ff:fe35:9a26     ff02::1:ff64:621e             ICMPv6    86      Neighbor Solicitation for fe80::adb7:4c35:7a64:621e from e0:98:61:35:9a:26
31  2.040149000 fe80::f68e:38ff:fe87:a56a     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from f4:8e:38:87:a5:6a
32  2.107577000 fe80::b283:feff:fe4d:f1c9     ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from b0:83:fe:4d:f1:c9
33  2.162415000 fe80::90c7:9c8e:4162:743a     ff02::16                      ICMPv6    110     Multicast Listener Report Message v2
34  2.181982000 fe80::175:6553:3c34:d4f0      ff02::1:ff02:21a              ICMPv6    86      Neighbor Solicitation for fe80::726d:ecff:fe02:21a from c8:1f:66:06:4a:84

Total Packet Count: 34

Enter which protocol packets you want to see
1.IP
2.UDP
3.TCP
4.Ethernet
5.Exit!!!
Choice:2
0   Time        Source                        Destination                   Protocol  Length  Info
```



```
1.IP
2.UDP
3.TCP
4.Ethernet
5.Exit!!!
Choice:2
0   Time        Source                        Destination                   Protocol  Length  Info

Total Packet Count: 0

Enter which protocol packets you want to see
1.IP
2.UDP
3.TCP
4.Ethernet
5.Exit!!!
Choice:3
0   Time        Source                        Destination                   Protocol  Length  Info
1   0.243260000 216.58.197.68                 10.10.14.151                  TCP       66      https > 51709 [FIN, ACK] Seq=1 Ack=1 Win=175 Len=0 TSval=2559300079 TSecr=23747257
2   0.438095000 108.168.177.14                10.10.13.238                  TCP       103     [TCP segment of a reassembled PDU]
3   0.746828000 192.168.16.254                10.10.10.28                   TCP       60      57777 > etftp [RST] Seq=1 Win=5840 Len=0
4   0.855756000 64.233.188.188                10.10.15.48                   TCP       97      hpvroom > 39687 [PSH, ACK] Seq=1 Ack=1 Win=175 Len=31 TSval=2933171628 TSecr=49981356
5   1.839024000 118.214.135.85                10.10.12.0                    TCP       60      https > 50976 [FIN, ACK] Seq=32 Ack=1 Win=980 Len=0
6   1.839028000 118.214.135.85                10.10.12.0                    TCP       60      https > 50977 [FIN, ACK] Seq=32 Ack=1 Win=980 Len=0
7   1.886438000 192.168.3.254                 192.168.3.211                 TCP       62      ndl-aas > fnet-remote-ui [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460 SACK_PERM=1
8   1.888346000 192.168.3.254                 192.168.3.211                 TCP       60      ndl-aas > fnet-remote-ui [ACK] Seq=1 Ack=211 Win=30016 Len=0

Total Packet Count: 8

Enter which protocol packets you want to see
1.IP
2.UDP
3.TCP
4.Ethernet
5.Exit!!!
Choice:4
0   Time        Source                        Destination                   Protocol  Length  Info
1   0.006278000 Ibm_36:9e:5e                  Broadcast                     ARP       60      Who has 192.168.16.222?  Tell 192.168.16.253
2   0.039035000 D-Link_95:3e:60               Broadcast                     ARP       60      Who has 192.168.16.9?  Tell 192.168.16.254
3   0.057747000 Dell_1d:f8:d4                 Broadcast                     ARP       60      Who has 192.168.25.250?  Tell 192.168.9.73
4   0.077077000 40:88:05:81:71:04             Broadcast                     ARP       60      Who has 10.10.10.1?  Tell 10.10.12.17
5   0.098310000 Ibm_36:9e:5e                  Broadcast                     ARP       60      Who has 192.168.16.214?  Tell 192.168.16.253
6   0.139610000 D-Link_95:3e:60               Broadcast                     ARP       60      Who has 192.168.16.10?  Tell 192.168.16.254
7   0.178440000 f4:8e:38:87:40:e1             Broadcast                     ARP       60      Who has 192.168.3.133?  Tell 192.168.3.127
8   0.185192000 Dell_28:20:ce                 Broadcast                     ARP       60      Who has 192.168.25.250?  Tell 192.168.15.151
9   0.239023000 D-Link_95:3e:60               Broadcast                     ARP       60      Who has 192.168.16.11?  Tell 192.168.16.254
10  0.239625000 D-Link_95:3e:60               Broadcast                     ARP       60      Who has 192.168.16.1?  Tell 192.168.16.254
11  0.248429000 Dell_f3:81:c7                 Broadcast                     ARP       60      Who has 192.168.25.250?  Tell 192.168.15.127
12  0.281997000 D-Link_9f:8a:c9               Broadcast                     ARP       60      Who has 10.10.15.50?  Tell 10.10.15.65
13  0.283865000 Antholog_10:37:03             Broadcast                     ARP       60      Gratuitous ARP for 192.168.20.6 (Request)
14  0.328694000 HonHaiPr_01:86:2e             Broadcast                     ARP       60      Who has 192.168.25.250?  Tell 192.168.17.64
15  0.339607000 D-Link_95:3e:60               Broadcast                     ARP       60      Who has 192.168.16.12?  Tell 192.168.16.254
16  0.340205000 D-Link_95:3e:60               Broadcast                     ARP       60      Who has 192.168.16.2?  Tell 192.168.16.254
17  0.345407000 Dell_ba:ac:7f                 Broadcast                     ARP       60      Who has 192.168.5.29?  Tell 192.168.3.222
18  0.383289000 Dell_27:82:de                 Broadcast                     ARP       60      Who has 192.168.7.142?  Tell 192.168.3.149
19  0.424797000 Elitegro_bb:40:79             Broadcast                     ARP       60      Who has 192.168.17.33?  Tell 192.168.17.13
```



```
49  1.098354000 Ibm_36:9e:5e                  Broadcast                      ARP       60      Who has 192.168.16.214?  Tell 192.168.16.253
50  1.128215000 Dell_27:48:0a                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.9.208
51  1.137360000 Dell_fd:b3:b3                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.3.203
52  1.139470000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.10?  Tell 192.168.16.254
53  1.231030000 Dell_27:49:60                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.9.87
54  1.238886000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.1?  Tell 192.168.16.254
55  1.239504000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.11?  Tell 192.168.16.254
56  1.246822000 Dell_f3:81:c7                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.15.127
57  1.281977000 D-Link_9f:8a:c9               Broadcast                      ARP       60      Who has 10.10.15.50?  Tell 10.10.15.65
58  1.298309000 Elitegro_bb:40:79             Broadcast                      ARP       60      Who has 192.168.17.33?  Tell 192.168.17.13
59  1.339488000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.2?  Tell 192.168.16.254
60  1.340081000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.12?  Tell 192.168.16.254
61  1.438930000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.13?  Tell 192.168.16.254
62  1.439588000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.3?  Tell 192.168.16.254
63  1.471674000 CompalIn_b3:29:81             Broadcast                      ARP       60      Who has 169.254.94.215?  Tell 192.168.9.149
64  1.471866000 CompalIn_b3:29:81             Broadcast                      ARP       60      Who has 192.168.9.154?  Tell 192.168.9.149
65  1.523610000 HonHaiPr_bf:b3:31             Broadcast                      ARP       60      Who has 10.10.10.1?  Tell 10.10.10.239
66  1.539475000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.14?  Tell 192.168.16.254
67  1.540041000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.4?  Tell 192.168.16.254
68  1.582553000 Dell_92:d2:91                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.17.142
69  1.638889000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.5?  Tell 192.168.16.254
70  1.639525000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.15?  Tell 192.168.16.254
71  1.694109000 58:fb:84:7f:d0:eb             Broadcast                      ARP       60      Who has 10.10.11.3?  Tell 10.10.11.216
72  1.727399000 f4:8e:38:87:40:e1             Broadcast                      ARP       60      Who has 192.168.3.133?  Tell 192.168.3.127
73  1.739525000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.6?  Tell 192.168.16.254
74  1.748638000 Dell_28:20:ce                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.15.151
75  1.777631000 Dell_27:88:85                 Broadcast                      ARP       60      Who has 192.168.7.253?  Tell 192.168.9.159
76  1.838890000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.7?  Tell 192.168.16.254
77  1.880913000 Dell_27:82:de                 Broadcast                      ARP       60      Who has 192.168.7.142?  Tell 192.168.3.149
78  1.933253000 Giga-Byt_0e:7d:ed             Broadcast                      ARP       60      Who has 192.168.14.250?  Tell 192.168.15.177
79  1.939529000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.8?  Tell 192.168.16.254
80  1.943185000 D-Link_9f:8a:cf               Broadcast                      ARP       60      Who has 10.10.15.50?  Tell 10.10.15.165
81  1.948844000 Dell_93:c3:3a                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.3.148
82  1.970467000 Dell_27:48:0a                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.9.208
83  1.973409000 Ibm_36:9e:5e                  Broadcast                      ARP       60      Who has 192.168.3.4?  Tell 192.168.3.254
84  2.039023000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.9?  Tell 192.168.16.254
85  2.098314000 Ibm_36:9e:5e                  Broadcast                      ARP       60      Who has 192.168.16.214?  Tell 192.168.16.253
86  2.119389000 Dell_fd:b3:b3                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.3.203
87  2.139576000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.10?  Tell 192.168.16.254
88  2.173438000 Dell_92:4d:81                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.14.150
89  2.216754000 Giga-Byt_0f:37:26             Broadcast                      ARP       60      Who has 10.10.8.216?  Tell 10.10.12.50
90  2.231058000 Dell_27:49:60                 Broadcast                      ARP       60      Who has 192.168.25.250?  Tell 192.168.9.87
91  2.238888000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.11?  Tell 192.168.16.254
92  2.239555000 D-Link_95:3e:60               Broadcast                      ARP       60      Who has 192.168.16.1?  Tell 192.168.16.254

Total Packet Count: 92

Enter which protocol packets you want to see
1.IP
2.UDP
3.TCP
4.Ethernet
5.Exit!!!
Choice:5
durvesh@predator:~/31139/SEMV/CNL/Assignment7$ 
```