

Subject: Computer Networks (01CT0503)

Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.

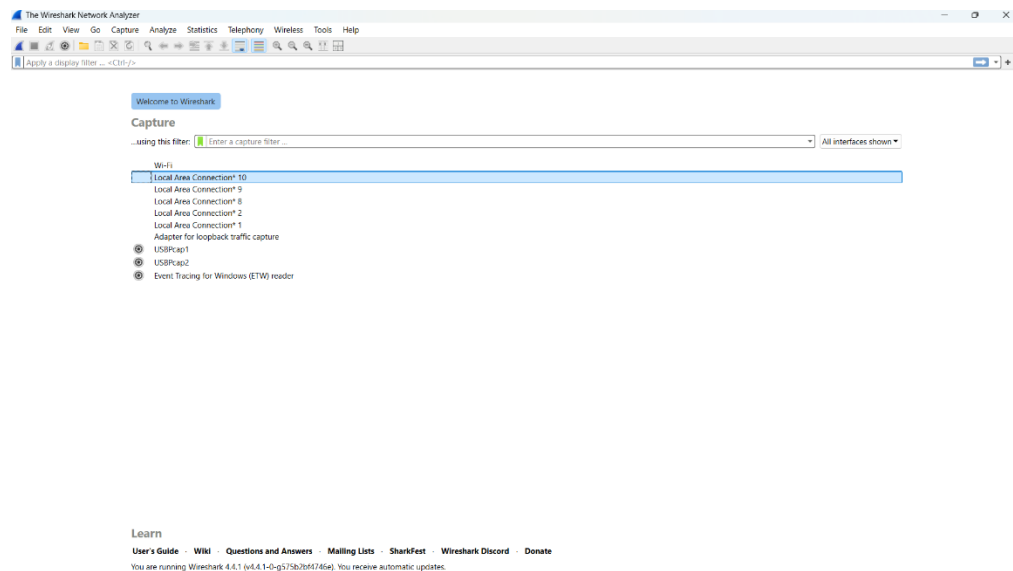
Experiment No: 11

Date: 14-09-2024

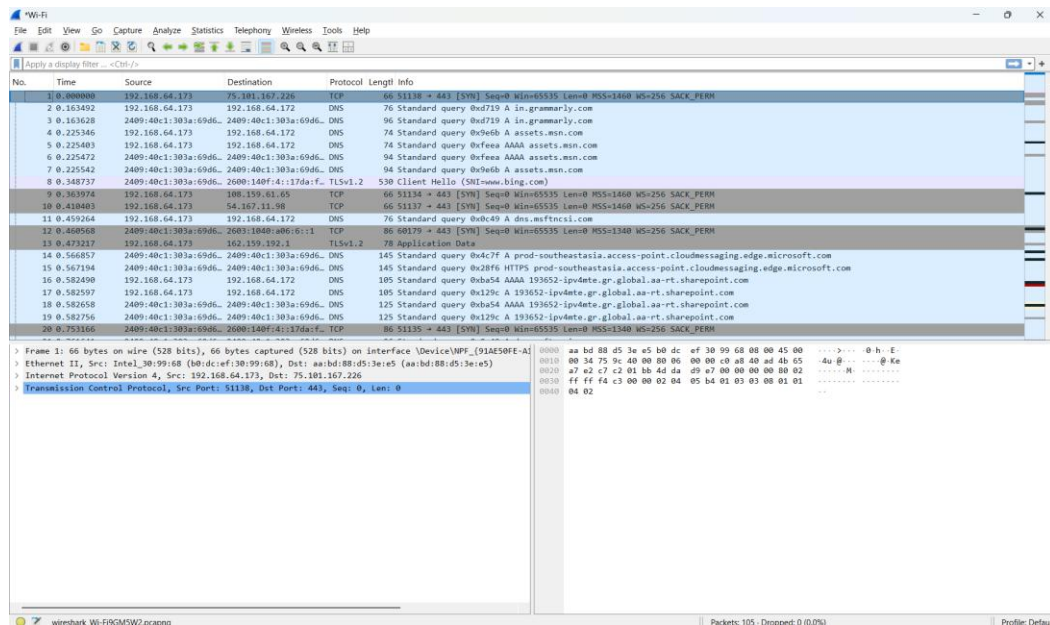
Enrolment No: 92200133030


Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.

Step – 1:- Open Wireshark

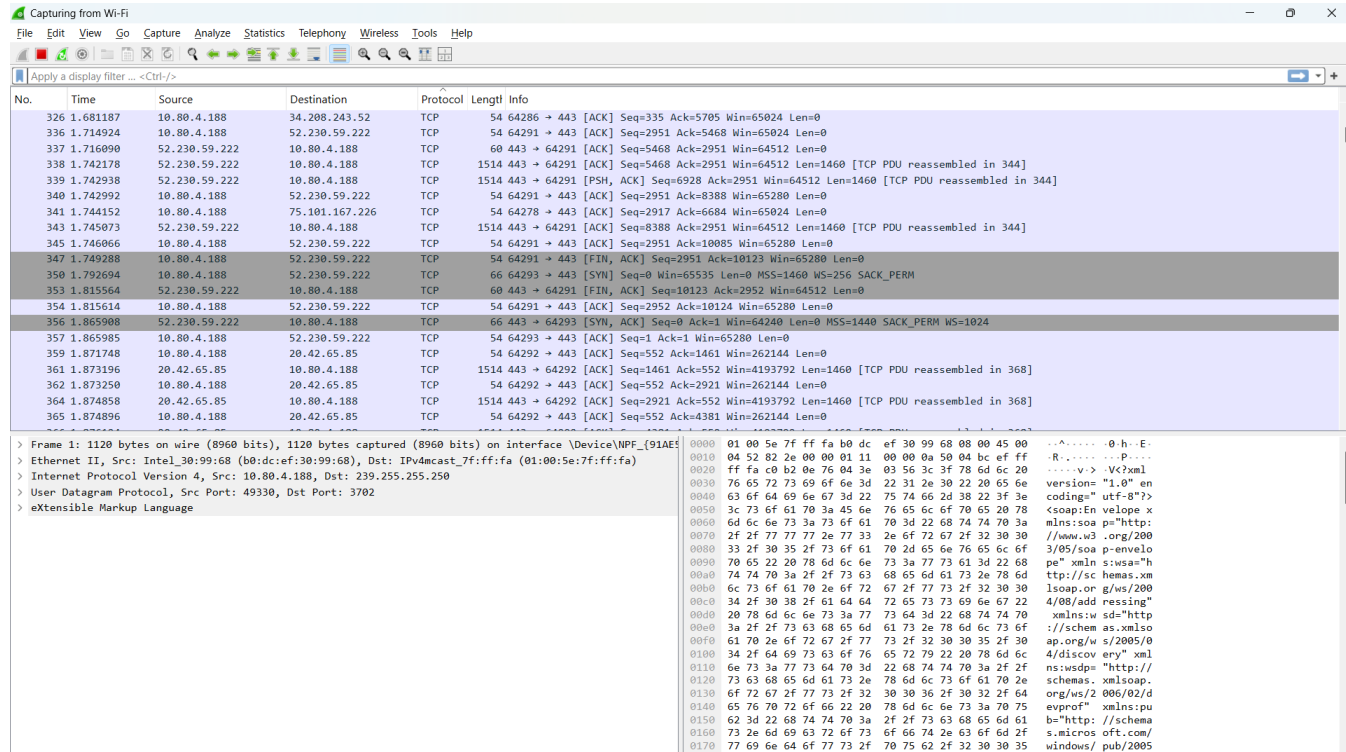


Step – 2 :- Select the Network from which you want to communicate



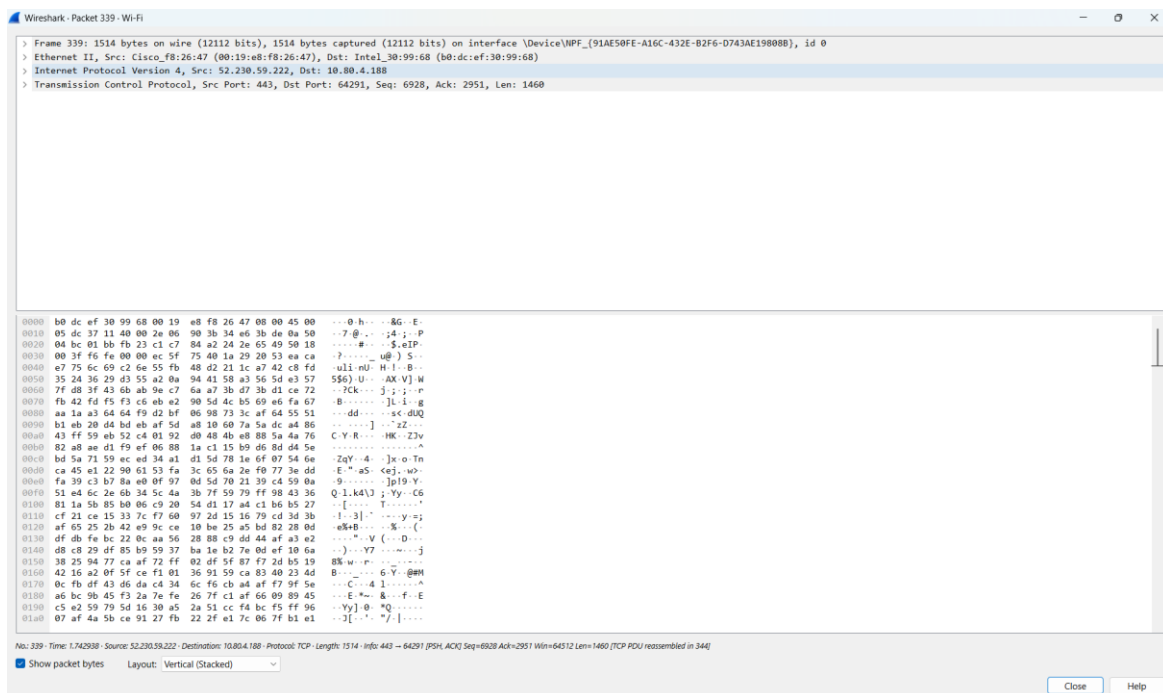
 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	Date: 14-09-2024	Enrolment No: 92200133030

Step – 3 :- Now when we press Protocol button it will sort the packet based on protocol used.




Wireshark packet capture interface showing a list of captured packets. The 'Protocol' column is selected, sorting packets by protocol. The list shows various TCP and SYN packets from 10.80.4.188 to 10.80.4.189.

Step – 4 :- Now when we press one of the packet it will open the packet and show every details.



Wireshark packet details and packet bytes pane for packet 339. The details pane shows Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol fields. The packet bytes pane shows the raw hex and ASCII data.

 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	Date: 14-09-2024	Enrolment No: 92200133030

Step – 5 :- Now we will analyze one TCP Packet

```

Wireshark - Packet 5398 - Wi-Fi
> Frame 5398: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE198088}, id 0
> Ethernet II, Src: Cisco_f8:26:47 (00:19:e8:f8:26:47), Dst: Intel_30:99:68 (b0:dc:ef:30:99:68)
> Internet Protocol Version 4, Src: 34.230.234.180, Dst: 10.80.4.188
> Transmission Control Protocol, Src Port: 443, Dst Port: 64361, Seq: 209657, Ack: 3799, Len: 1460

0000  b0 dc ef 30 99 68 00 19  e8 f8 26 47 08 00 45 00  ...0 h...&G..E-
0010  05 dc 6f 4c 40 00 e6 06  03 29 22 e6 ea b4 0a 50  ...ol@...)"....P
0020  04 bc 01 bb fb 69 7a ad  1b f1 7c 86 8c 7a 50 10  ...iz...].zP-
0030  00 d5 00 27 00 00 68 47  aa b9 02 3a de b7 37 96  ...f..HG...:7-
0040  6c 60 46 fc 28 ef 54 29  d8 5b 32 31 c6 c0 e9 f4  1"F(-T)[21....
0050  e4 ba 17 ab 29 86 09 fe  b5 93 b3 bd 43 2e 79 e2  ...)...C.y
0060  c1 57 f6 84 54 e9 bd 5e  d5 5b 08 e2 07 e2 c8 89  -W-T-^[-.....
0070  48 ac ee f8 ef 98 ff b7  0a 81 71 49 bf 62 07 bb  H.....qI b-
0080  fa f4 ae 3d 22 e3 78 2a  a3 1a 77 3b cf a0 b2 27  ...x*...w;...
0090  72 e0 a1 b8 85 97 e0 5c  02 72 da e8 1b 6a 1a 54  p.....\...j-T
00a0  5f 1c 8b df f7 b2 83 90  c0 0d 47 8d ed b1 08 d4  -.....G....
00b0  67 19 c9 86 08 20 2d 34  3f e2 e3 f0 49 ec 9c 2d  g....4?..I...
00c0  69 ed 98 05 84 dd 62 38  c3 ce 09 a2 63 0a ff ee  i....b8....c...
00d0  96 b6 28 d5 7d 7e b5 0f  03 68 0a d6 14 24 0a 1e  -(.)...h...$...
00e0  bf 9a 00 57 40 cf 9c d8  f8 e1 dd 97 9b 86 b9 f2  ...M.....
00f0  a2 c8 6c 5d 25 f7 5f c0  96 a9 40 28 27 72 20 38  -l]%....@('r 8
0100  30 44 8c 05 d1 c5 06 93  ec b1 2b 6b 78 02 45 2d  00.....+kx:E-
0110  d1 ac b6 e7 3c 25 c4 39  3a fc 38 dc a4 77 35 80  ....x%9...:8..w5-
0120  28 2b c6 ac 2d f6 8c 07  13 32 2f bc be 13 43 b7  (+.....2/...C-
0130  06 40 f9 3a a6 8f c9 29  db 1e 78 34 62 1f d6 f8  -@:....)x4b...
0140  71 12 d4 6a d0 2b a2 c2  19 f1 61 9f 9f 99 3d 27  q..j+...a...=
0150  4c d5 4a 0d 0e d4 ac 00  54 46 01 85 5e 60 e0 26  L-D...TF..^&
0160  41 5c ff b2 14 23 b7 63  21 70 78 d9 64 9b 22 f1  A\...#..c lpx d."-
0170  28 e4 82 c2 b3 6f 78 a9  9a 5f 8e 25 18 3a cd 77  (-...ox...%...:w
0180  02 61 d3 28 92 68 fe 9b  84 ec 84 e4 5c d0 f1 8e  -a(-h...)\...
0190  54 b3 6e 1e 82 86 2d 0c  83 eb e8 aa 62 a2 6c 3d  T.n......b-le
01a0  b1 03 1a c0 fb 2b a9 84  c2 9a 29 d7 52 d1 3c 5b  ....+...R<[

```


Step – 7 :- Analysis of TCP Packet

```

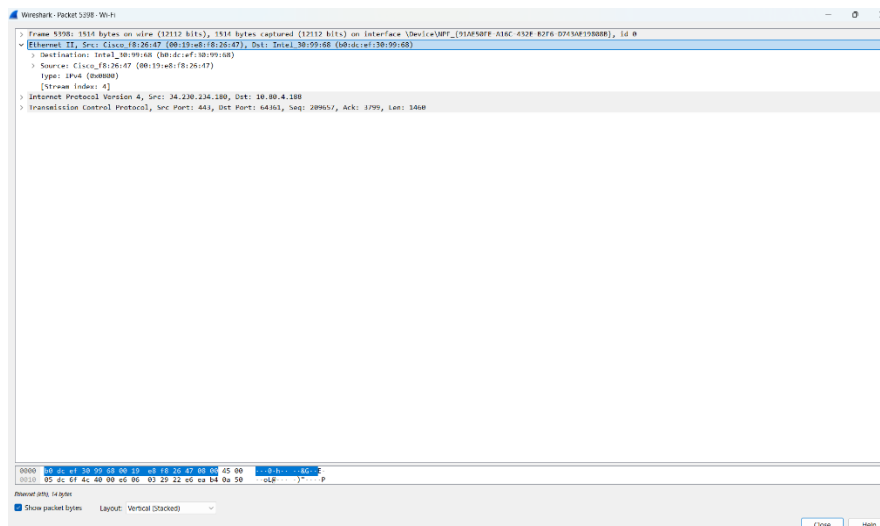
Wireshark - Packet 5398 - Wi-Fi
▼ Frame 5398: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE198088}, id 0
  Section number: 1
  > Interface id: 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE198088})
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 18, 2024 12:06:42.969050000 India Standard Time
  UTC Arrival Time: Nov 18, 2024 06:36:42.969050000 UTC
  Epoch Arrival Time: 1731911802.969050000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.001820000 seconds]
  [Time delta from previous displayed frame: 0.001820000 seconds]
  [Time since reference or first frame: 104.970838000 seconds]
  Frame Number: 5398
  Frame Length: 1514 bytes (12112 bits)
  Capture Length: 1514 bytes (12112 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp]
  [Coloring Rule Name: TCP]
  [Coloring Rule String: tcp]

```

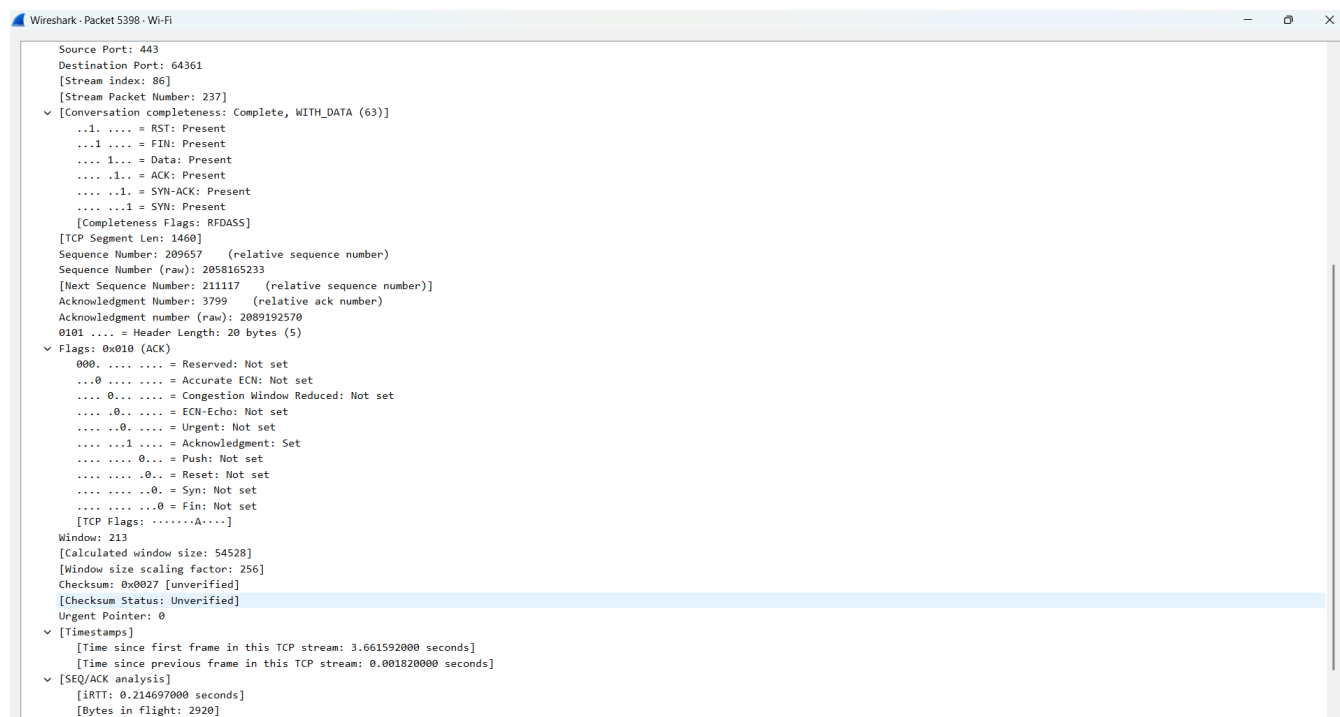
- It is the timing details and frame length and frame no.


 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	Date: 14-09-2024	Enrolment No: 92200133030

Step – 8:- It is showing the source and destination IP Address:-



Step – 9:- It is showing the TCP related details stored in the packets: like header section src and destination port no flags , checksum , length , timestamps.



 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	Date: 14-09-2024	Enrolment No: 92200133030

- Source Port (65527):
- It is the port number the client (source) uses to send the packet.
- Destination Port (443):
- This is the port number used by the server (destination), which is associated with HTTPS most of the time.
- Sequence Number (2299):
- This is the relative sequence number of the first byte in the data of the segment. It's used for keeping track of the order in which bytes were sent.
- Acknowledgment Number (98531):
- Indicates the next byte of data the sender of this segment expects to receive. It's an acknowledgment of the previous packet.
- TCP Segment Length (0):
- Length of data payload in this TCP segment. In this case, it is 0 which means no data is carried in this packet. It most probably is an acknowledgment.
- Flags (0x010 - ACK):
- Indicates what kind of control information in the packet is. In this case, ACK means it is an acknowledgment.
- Header Length (20 bytes):
- The size of the TCP header. The average minimum size is 20 bytes.
- Ethernet II and IP Information:
- Source MAC Address Intel_30:99:68: The source MAC address of the device which transmitted the packet.
- Destination MAC Address Cisco_f8:26:47: The destination MAC address of the device which will receive the packet.
- Source IP 10.80.4.192: The source IP address of the client.
- Destination IP 142.250.192.142: The destination IP address of the server.

Subject: Computer Networks (01CT0503)

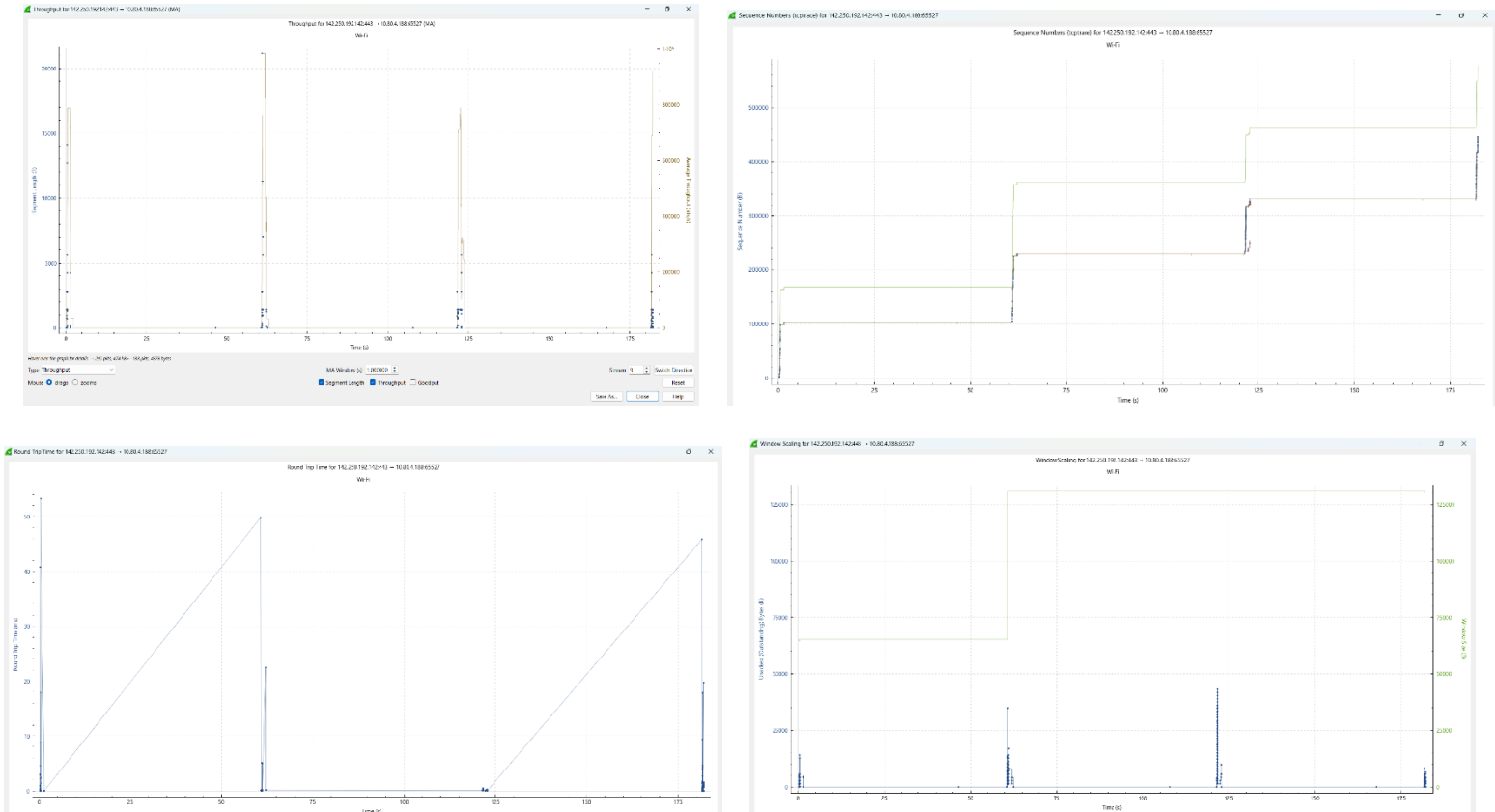
Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.

Experiment No: 11

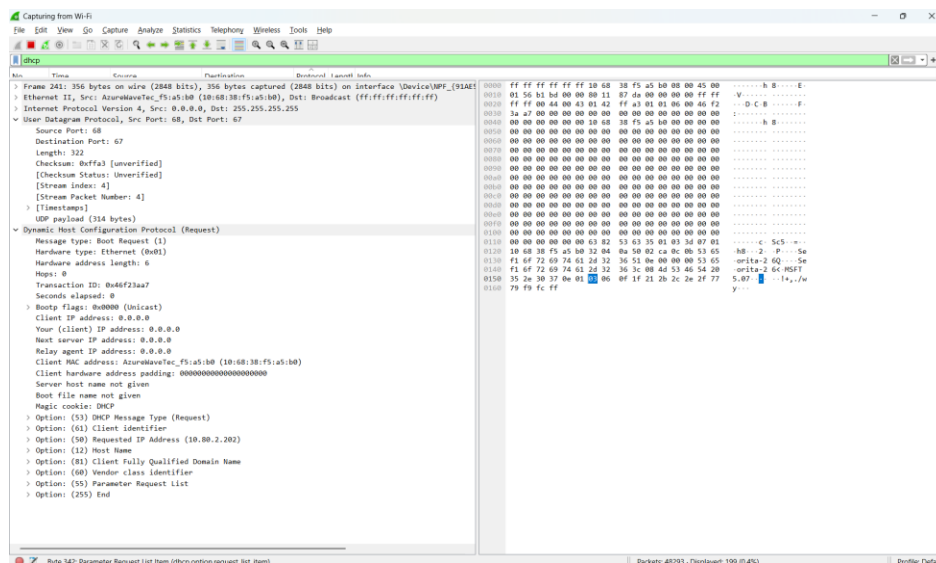
Date: 14-09-2024


Enrolment No: 92200133030

Step – 10:- It is showing the TCP related details stored in the packets: like header section src and destination port no flags , checksum , length , timestamps



Step - 11:- now we will analyze the UDP Packet.



 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	Date: 14-09-2024	Enrolment No: 92200133030

UDP Packet Details


- Source Port (68):**
The port used by the client to send the packet. This is the standard DHCP Client port.
- Destination Port (67):**
The port used by the server to receive the packet. This is the standard DHCP Server port.
- Length (322):**
Represents the total size of the UDP packet, including both the header and the payload.
- Checksum:**
Used to verify the integrity of the UDP packet. In this capture, it is marked as "unverified."
- UDP Payload (314 bytes):**
The actual data being transported in the UDP segment.

Step - 12:- It is showing the timing related details of UDP Packet.

```

▼ Frame 1705: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}
  Section number: 1
  > Interface id: 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B})
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 19, 2024 08:36:32.307111000 India Standard Time
  UTC Arrival Time: Nov 19, 2024 03:06:32.307111000 UTC
  Epoch Arrival Time: 1731985592.307111000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000089000 seconds]
  [Time delta from previous displayed frame: 0.000089000 seconds]
  [Time since reference or first frame: 50.995135000 seconds]
  Frame Number: 1705
  Frame Length: 81 bytes (648 bits)
  Capture Length: 81 bytes (648 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:udp:dns]
  [Coloring Rule Name: UDP]
  [Coloring Rule String: udp]

```


 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	Date: 14-09-2024	Enrolment No: 92200133030

Step - 13:- It is showing the ip related details of UDP Packet.

```

▼ Ethernet II, Src: Intel_30:99:68 (b0:dc:ef:30:99:68), Dst: 5a:03:b1:74:c8:0c (5a:03:b1:74:c8:0c)
  > Destination: 5a:03:b1:74:c8:0c (5a:03:b1:74:c8:0c)
  > Source: Intel_30:99:68 (b0:dc:ef:30:99:68)
    Type: IPv4 (0x0800)
    [Stream index: 2]

```

Step - 14:- It is showing the details about the flags of UDP Packet.

```

▼ Internet Protocol Version 4, Src: 192.168.64.173, Dst: 192.168.64.172
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 67
  Identification: 0x0f21 (3873)
  ▼ 000. .... = Flags: 0x0
    0... .... = Reserved bit: Not set
    .0.. .... = Don't fragment: Not set
    ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x0000 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.64.173
    Destination Address: 192.168.64.172
    [Stream index: 1]


```

Step - 15:- It is showing the details about the header of UDP Packet.

```

▼ User Datagram Protocol, Src Port: 64580, Dst Port: 53
  Source Port: 64580
  Destination Port: 53
  Length: 47
  Checksum: 0x02eb [unverified]
  [Checksum Status: Unverified]
  [Stream index: 103]
  [Stream Packet Number: 1]
  > [Timestamps]
  UDP payload (39 bytes)

```


 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	Date: 14-09-2024	Enrolment No: 92200133030

Step - 16:- Now we will analyze the IP Protocol.

Definition:-

- Internet Protocol (IP) is a set of rules that defines the format of data carried over the internet or a local network. It is the primary communication protocol for forwarding packets across network boundaries, which permits internetworking.

Types of IP:-

- IPv4: Uses a 32-bit address format (for example 192.168.1.1). It supports around 4.3 billion unique addresses.
- IPv6: Uses a 128-bit address format (for example 2001:0db8:85a3::8a2e:0370:7334). It supports a vastly larger address space.

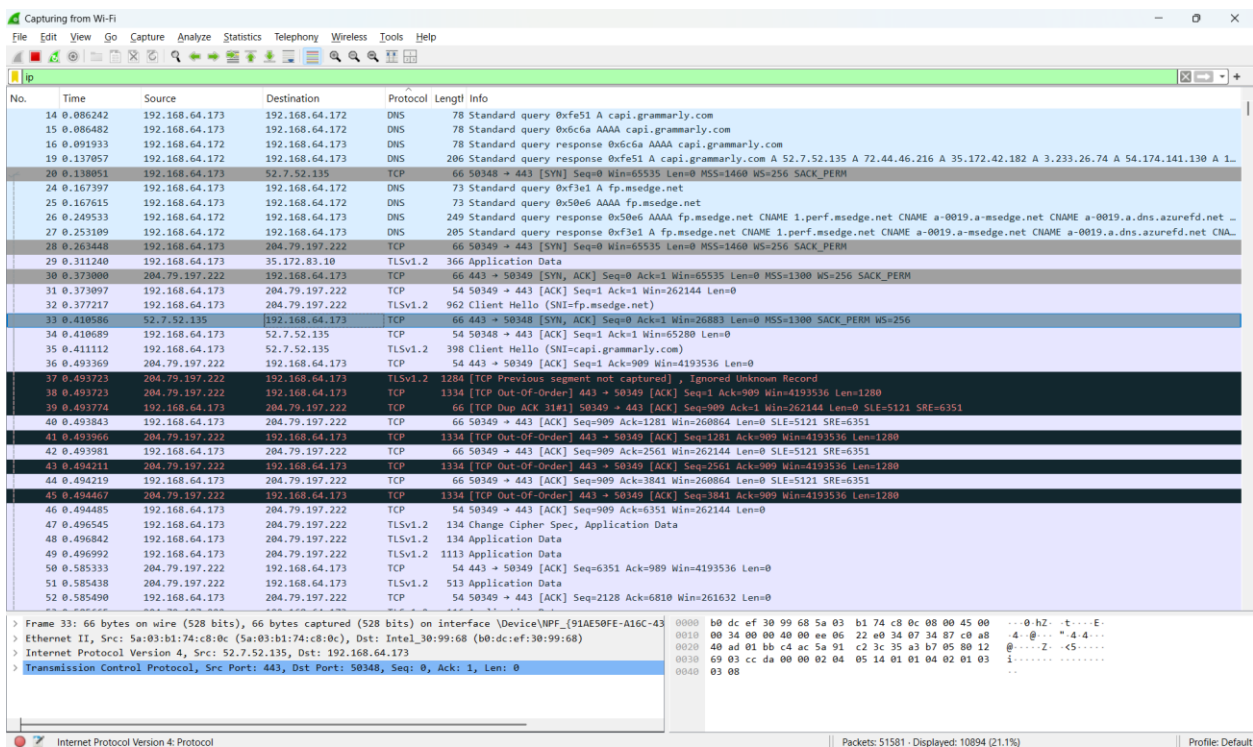
Applications :-

- Identifying: Scans a network for its devices.
- Routing: Transfers the data packets between one device and another, but on different networks.

Protocols Built on IP:-

- **TCP (Transmission Control Protocol):** Reliable, connection-oriented protocol.
- **UDP (User Datagram Protocol):** Faster, connectionless protocol.

To analyze the IP search ip in search bar



The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The main window is divided into three panes:

- Packet List:** Displays a list of captured packets. The selected packet is No. 52, a TCP packet from 192.168.64.173 to 204.79.197.222, Seq=2128, Ack=6810, Len=0.
- Packet Details:** Shows the hierarchical structure of the selected packet. It is identified as a Transmission Control Protocol (TCP) packet. The details include the source and destination ports (443 and 50348 respectively), sequence number (2128), acknowledgment number (6810), and length (0).
- Packet Bytes:** Displays the raw data of the packet in hexadecimal and ASCII. The data is mostly zeros, indicating a FIN or RST packet.

The search bar at the top of the packet list contains the text 'ip', which has filtered the display to show only IP-related packets.

Subject: Computer Networks (01CT0503)

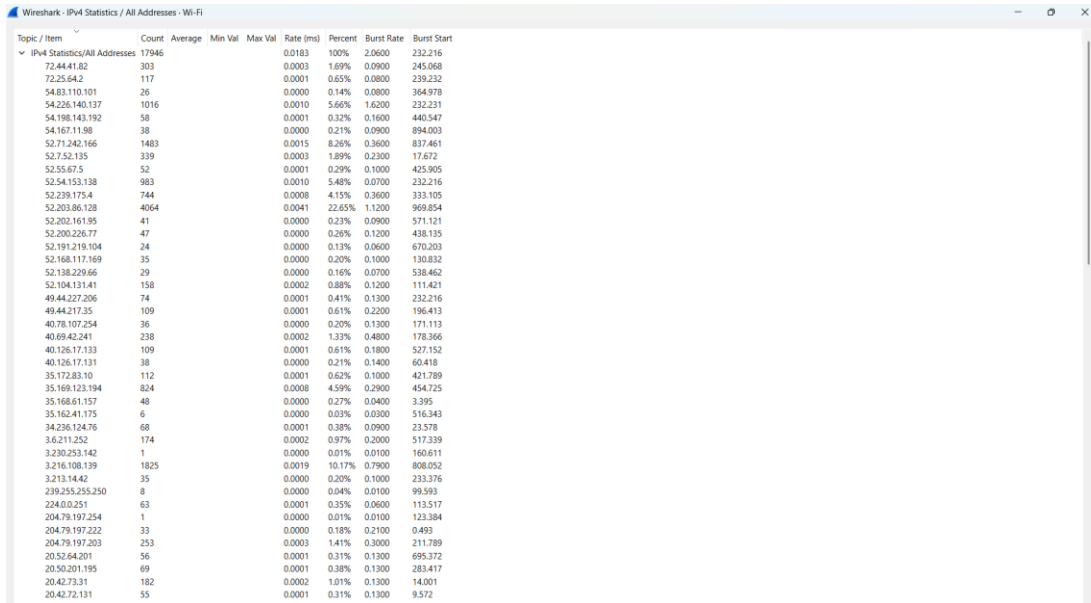
Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.

Experiment No: 11

Date: 14-09-2024

Enrolment No: 92200133030

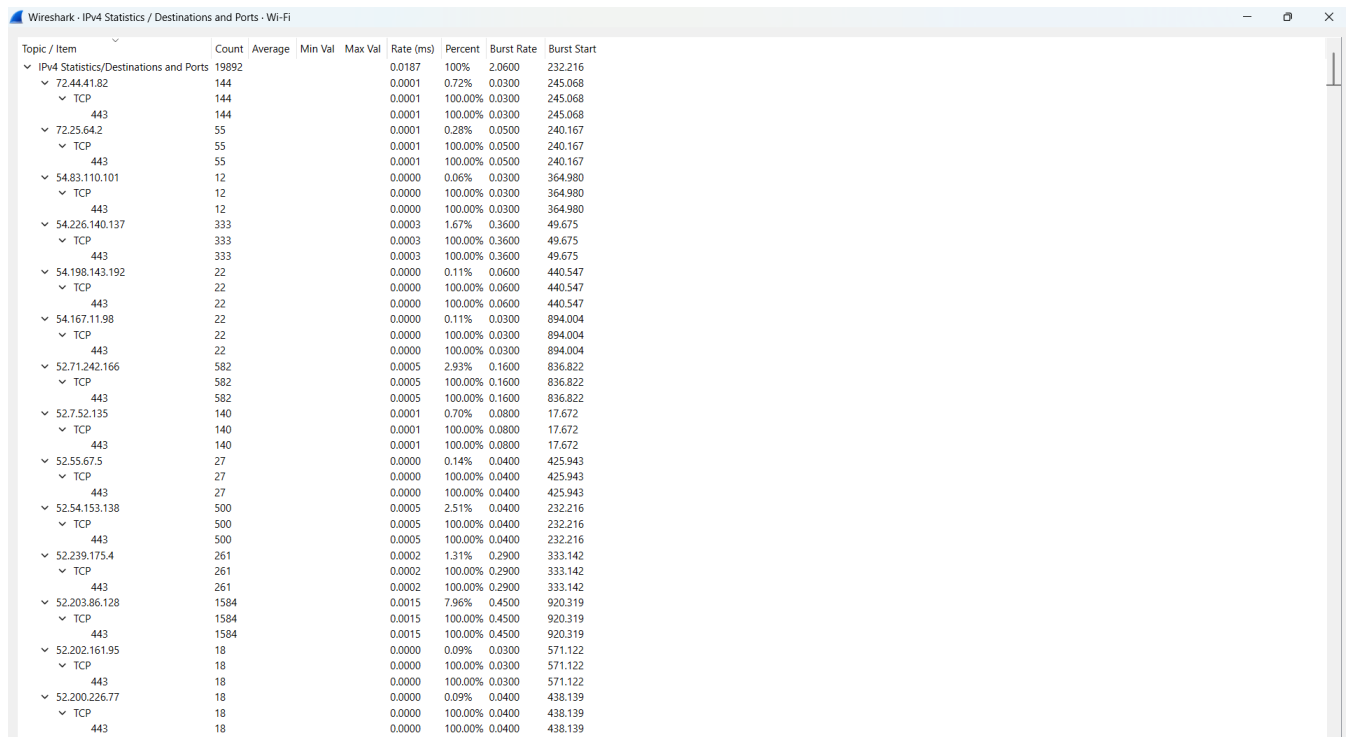
Step - 17:- Now we go to the Statistics > IPv4 Statistics > all address



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/All Addresses	17946				0.0183	100%	2.0600	232.216
72.44.41.82	303				0.0003	1.69%	0.0900	245.068
72.25.64.2	117				0.0001	0.63%	0.0800	239.232
54.83.110.101	26				0.0000	0.14%	0.0800	364.978
54.226.140.137	1016				0.0010	5.66%	1.6200	232.231
54.198.143.192	58				0.0001	0.32%	0.1600	440.547
54.167.11.98	38				0.0000	0.21%	0.0900	894.003
52.71.242.166	1483				0.0015	8.26%	0.3600	837.461
52.7.52.135	339				0.0003	1.89%	0.2300	17.672
52.55.67.5	52				0.0001	0.29%	0.1000	425.905
52.54.153.138	983				0.0010	5.48%	0.0700	232.216
52.239.175.4	744				0.0008	4.15%	0.3600	333.105
52.203.86.128	4064				0.0041	22.65%	1.1200	969.854
52.202.161.95	41				0.0000	0.23%	0.0900	571.121
52.200.226.77	47				0.0000	0.26%	0.1200	438.135
52.191.219.104	24				0.0000	0.13%	0.0600	670.203
52.168.117.169	35				0.0000	0.20%	0.1000	130.832
52.138.229.66	29				0.0000	0.16%	0.0700	538.462
52.104.131.41	158				0.0002	0.88%	0.1200	111.421
49.44.227.206	74				0.0001	0.41%	0.1300	232.216
49.44.217.35	109				0.0001	0.61%	0.2200	196.413
40.78.107.254	36				0.0000	0.20%	0.1300	171.113
40.69.42.241	238				0.0002	1.33%	0.4800	178.366
40.126.17.133	109				0.0001	0.61%	0.1800	527.152
40.136.17.131	38				0.0000	0.21%	0.1400	60.418
35.172.83.10	112				0.0001	0.62%	0.1000	421.789
35.169.123.194	824				0.0008	4.59%	0.2900	454.725
35.168.61.157	48				0.0000	0.27%	0.0400	3.395
35.162.41.175	6				0.0000	0.03%	0.0300	516.343
34.236.124.76	68				0.0001	0.38%	0.0900	23.578
3.6.211.252	174				0.0002	0.97%	0.2000	517.339
3.230.253.142	1				0.0000	0.01%	0.0100	160.611
3.216.108.139	1825				0.0019	10.17%	0.7900	808.052
3.213.14.42	35				0.0000	0.20%	0.1000	233.376
239.255.255.250	8				0.0000	0.04%	0.0100	99.393
224.0.0.251	63				0.0001	0.35%	0.0600	113.517
204.79.197.254	1				0.0000	0.01%	0.0100	123.384
204.79.197.222	33				0.0000	0.18%	0.2100	0.493
204.79.197.203	253				0.0003	1.41%	0.3000	211.789
203.54.201	56				0.0001	0.31%	0.1300	695.372
20.50.201.195	69				0.0001	0.38%	0.1300	283.417
20.42.73.31	182				0.0002	1.01%	0.1300	14.001
20.42.72.131	55				0.0001	0.31%	0.1300	9.572


It is Showing all IP Address to which my laptop is communication

Step - 18:- Now we go to the Statistics > IPv4 Statistics > Destination and Ports



Topic / Item	Count	Average	Min Val	Max Val	Rate (ms)	Percent	Burst Rate	Burst Start
IPv4 Statistics/Destinations and Ports	19892				0.0187	100%	2.0600	232.216
72.44.41.82	144				0.0001	0.72%	0.0300	245.068
TCP	144				0.0001	100.00%	0.0300	245.068
443	144				0.0001	100.00%	0.0300	245.068
72.25.64.2	55				0.0001	0.28%	0.0500	240.167
TCP	55				0.0001	100.00%	0.0500	240.167
443	55				0.0001	100.00%	0.0500	240.167
54.83.110.101	12				0.0000	0.06%	0.0300	364.980
TCP	12				0.0000	100.00%	0.0300	364.980
443	12				0.0000	100.00%	0.0300	364.980
54.226.140.137	333				0.0003	1.67%	0.3600	49.675
TCP	333				0.0003	100.00%	0.3600	49.675
443	333				0.0003	100.00%	0.3600	49.675
54.198.143.192	22				0.0000	0.11%	0.0600	440.547
TCP	22				0.0000	100.00%	0.0600	440.547
443	22				0.0000	100.00%	0.0600	440.547
54.167.11.98	22				0.0000	0.11%	0.0300	894.004
TCP	22				0.0000	100.00%	0.0300	894.004
443	22				0.0000	100.00%	0.0300	894.004
52.71.242.166	582				0.0005	2.93%	0.1600	836.822
TCP	582				0.0005	100.00%	0.1600	836.822
443	582				0.0005	100.00%	0.1600	836.822
52.7.52.135	140				0.0001	0.70%	0.0800	17.672
TCP	140				0.0001	100.00%	0.0800	17.672
443	140				0.0001	100.00%	0.0800	17.672
52.55.67.5	27				0.0000	0.14%	0.0400	425.943
TCP	27				0.0000	100.00%	0.0400	425.943
443	27				0.0000	100.00%	0.0400	425.943
52.54.153.138	500				0.0005	2.51%	0.0400	232.216
TCP	500				0.0005	100.00%	0.0400	232.216
443	500				0.0005	100.00%	0.0400	232.216
52.239.175.4	261				0.0002	1.31%	0.2900	333.142
TCP	261				0.0002	100.00%	0.2900	333.142
443	261				0.0002	100.00%	0.2900	333.142
52.203.86.128	1584				0.0015	7.96%	0.4500	920.319
TCP	1584				0.0015	100.00%	0.4500	920.319
443	1584				0.0015	100.00%	0.4500	920.319
52.202.161.95	18				0.0000	0.09%	0.0300	571.122
TCP	18				0.0000	100.00%	0.0300	571.122
443	18				0.0000	100.00%	0.0300	571.122
52.200.226.77	18				0.0000	0.09%	0.0400	438.139
TCP	18				0.0000	100.00%	0.0400	438.139
443	18				0.0000	100.00%	0.0400	438.139

It shows the Destination Adress Protocol and Port No Used for Communication.

 Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like IP, TCP, UDP, etc.	
Experiment No: 11	Date: 14-09-2024	Enrolment No: 92200133030

Conclusion:-

Through this experiment, I learned to analyze TCP packets and what types of details with the data is sent. And the importance of all flags. How ACK is important. and show the actual packet what is sent and what is received. I learned to analyze the UDP packets ,its header and flags we learned the theory about the protocol by performing this experiment I learned to live monitor the packets and learned how IP address is used in various Protocol like TCP and UDP.