



Subject: Computer Networks (01CT0503)

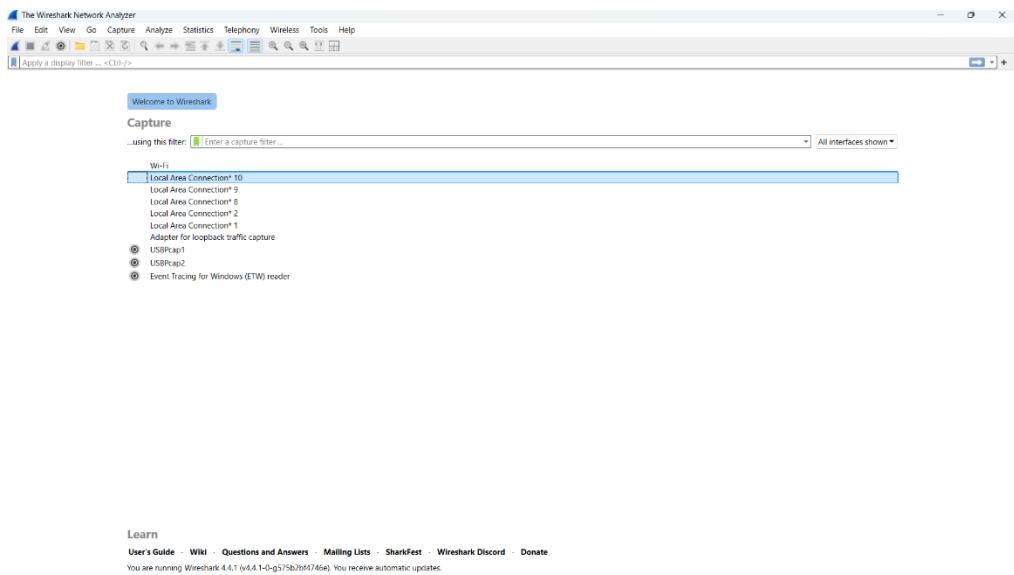
Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.

Experiment No: 12

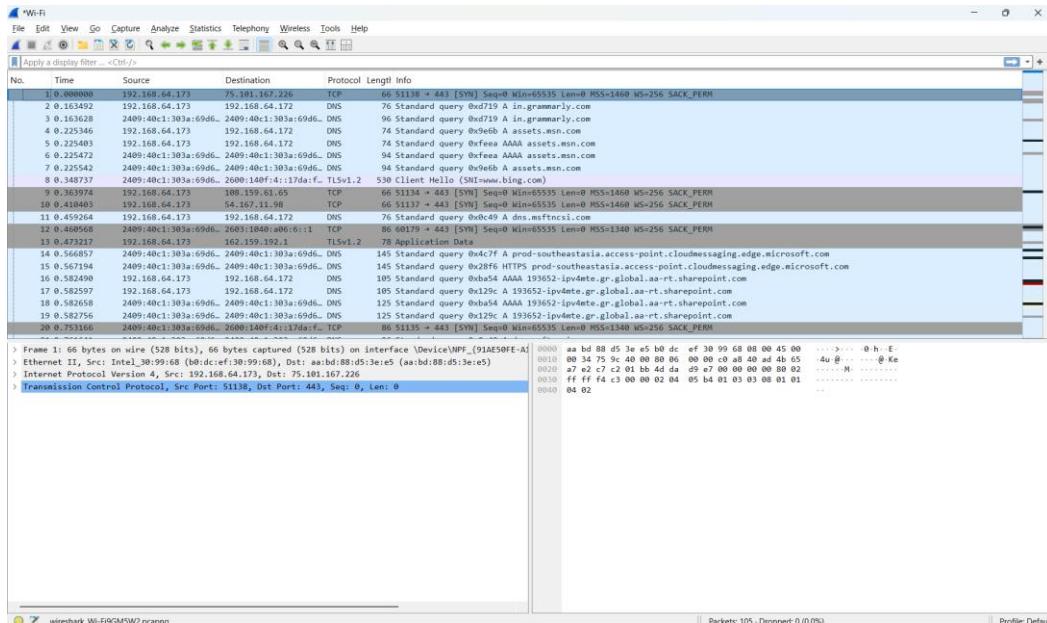
Date: 24-11-2025

Enrolment No: 92301733024

Step – 1:- Open Wireshark

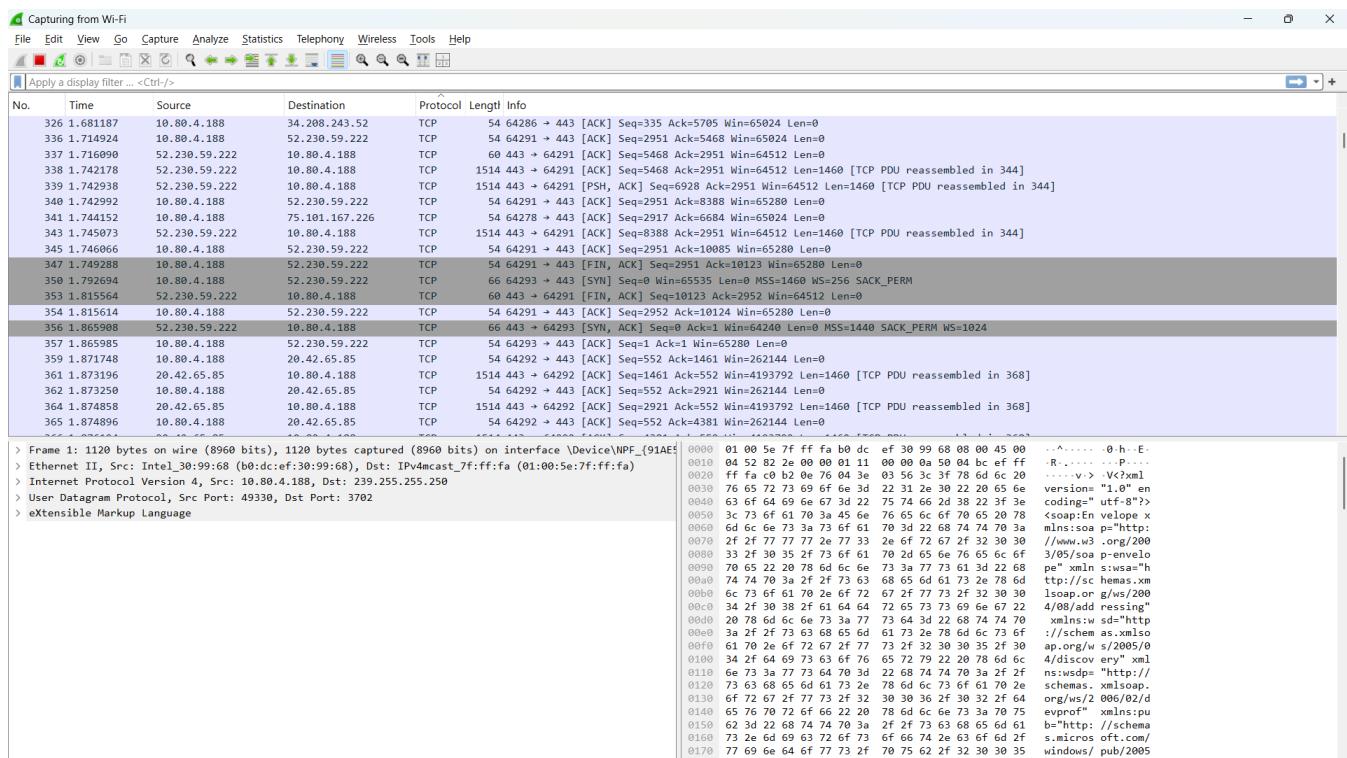


Step – 2 :- Select the Network from which you want to communicate



Subject: Computer Networks (01CT0503)
Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.
Experiment No: 12
Date: 24-11-2025
Enrolment No: 92301733024

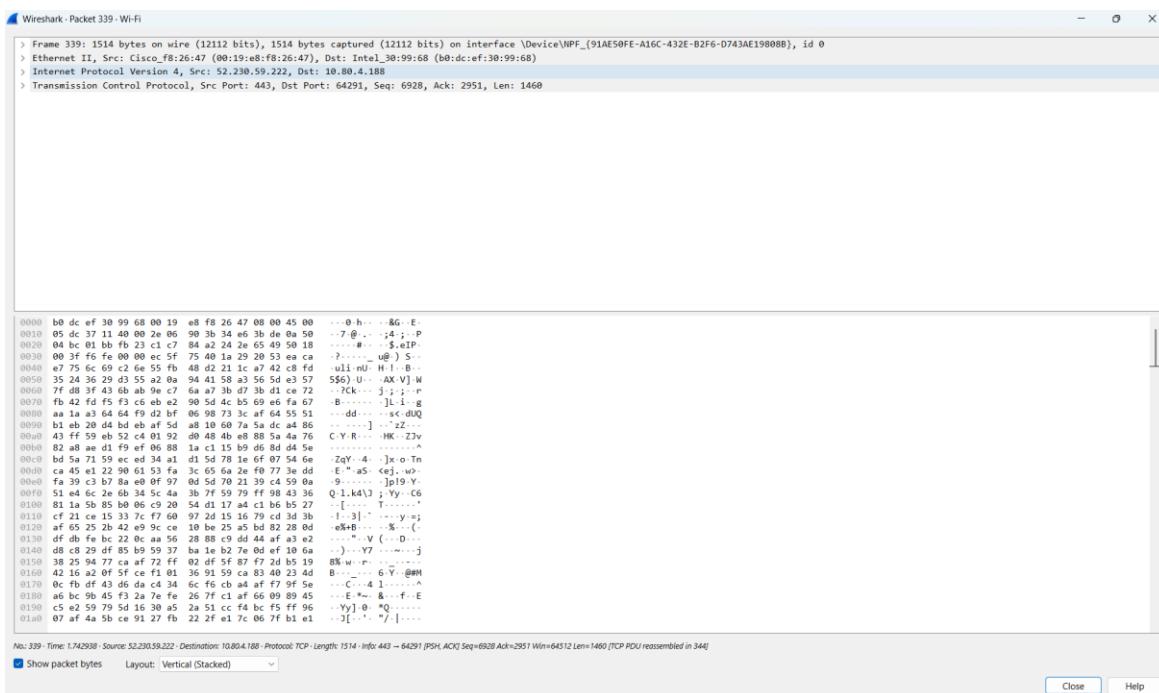
Step – 3 :- Now when we press Protocol button it will sort the packet based on protocol used.



The screenshot shows a Wireshark interface with the following details:

- Capturing from Wi-Fi**
- File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help**
- Apply a display filter ... <Ctrl-/>**
- No. Time Source Destination Protocol Length Info**
- Protocol column headers:** TCP, UDP, ICMP, ARP, Ethernet, HTTP, HTTPS, DNS, etc.
- Sampled Packets:** 326 to 635 (Total 309)
 - 326. 1.681187 10.80.4.188 34.208.243.52 TCP 54 64286 → 443 [ACK] Seq=335 Ack=5705 Win=65024 Len=0
 - 336. 1.714924 10.80.4.188 52.230.59.222 TCP 54 64291 → 443 [ACK] Seq=2951 Ack=5468 Win=65024 Len=0
 - 337. 1.716090 52.230.59.222 10.80.4.188 TCP 60 443 → 64291 [ACK] Seq=5468 Ack=2951 Win=64512 Len=0
 - 338. 1.742178 52.230.59.222 10.80.4.188 TCP 1514 443 → 64291 [PSH, ACK] Seq=5468 Ack=2951 Win=64512 Len=1460 [TCP PDU reassembled in 344]
 - 339. 1.742938 52.230.59.222 10.80.4.188 TCP 1514 443 → 64291 [ACK] Seq=2951 Ack=5388 Win=65280 Len=0
 - 340. 1.742992 10.80.4.188 52.230.59.222 TCP 54 64291 → 443 [ACK] Seq=2951 Ack=5388 Win=65280 Len=0
 - 341. 1.744152 10.80.4.188 75.181.167.226 TCP 54 64278 → 443 [ACK] Seq=2917 Ack=6088 Win=65024 Len=0
 - 343. 1.745073 52.230.59.222 10.80.4.188 TCP 1514 443 → 64291 [ACK] Seq=8388 Ack=2951 Win=64512 Len=1460 [TCP PDU reassembled in 344]
 - 345. 1.746066 10.80.4.188 52.230.59.222 TCP 54 64291 → 443 [ACK] Seq=2951 Ack=10085 Win=65280 Len=0
 - 347. 1.749288 10.80.4.188 52.230.59.222 TCP 54 64291 → 443 [FIN, ACK] Seq=2951 Ack=10123 Win=65280 Len=0
 - 350. 1.792694 10.80.4.188 52.230.59.222 TCP 66 64293 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
 - 353. 1.815564 52.230.59.222 10.80.4.188 TCP 60 443 → 64291 [FIN, ACK] Seq=10123 Ack=2952 Win=64512 Len=0
 - 354. 1.815614 10.80.4.188 52.230.59.222 TCP 54 64291 → 443 [ACK] Seq=2952 Ack=10124 Win=65280 Len=0
 - 356. 1.865988 52.230.59.222 10.80.4.188 TCP 66 443 → 64293 [SYN, ACK] Seq=1 Win=64240 Len=0 MSS=1440 SACK_PERM WS=1024
 - 357. 1.865985 10.80.4.188 52.230.59.222 TCP 54 64293 → 443 [ACK] Seq=1 Win=65280 Len=0
 - 359. 1.871748 10.80.4.188 20.42.65.85 TCP 54 64292 → 443 [ACK] Seq=552 Ack=1461 Win=262144 Len=0
 - 361. 1.873193 20.42.65.85 10.80.4.188 TCP 1514 443 → 64292 [ACK] Seq=1461 Ack=552 Win=4193792 Len=1460 [TCP PDU reassembled in 368]
 - 362. 1.873250 10.80.4.188 20.42.65.85 TCP 54 64292 → 443 [ACK] Seq=552 Ack=2921 Win=262144 Len=0
 - 364. 1.874858 20.42.65.85 10.80.4.188 TCP 1514 443 → 64292 [ACK] Seq=2921 Ack=552 Win=4193792 Len=1460 [TCP PDU reassembled in 368]
 - 365. 1.874896 10.80.4.188 20.42.65.85 TCP 54 64292 → 443 [ACK] Seq=552 Ack=481 Win=262144 Len=0

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



The screenshot shows a Wireshark interface with the following details:

- Frame 339: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE1980BB), 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: 52.230.59.222, Dst: 10.80.4.188**
- Transmission Control Protocol, Src Port: 443, Dst Port: 64291, Seq: 6928, Ack: 2951, Len: 1460**

Selected Packet Details:

0000	b0 dc ef 30 99 68 00 19	a8 f8 26 47 08 00 45 00	0 h - .8G E
0010	05 dc 37 11 40 00 2e 06	99 3b 34 e6 3b de 0a 50	-7 @ - .14 : - P
0020	04 bc 01 fb 23 c1 c7	84 a2 24 2e 65 49 50 18	... # - \$.IP
0030	00 3f f6 fe 00 00 ec	5f 75 49 1a 29 20 53 ea ca	? u@) S-
0040	e7 75 6c 69 <2 be> 00	fb 48 21 1c a7 42 c8 fd	e7 1mu H - B -
0050	07 75 6c 69 <2 be> 00	fb 48 21 1c a7 42 c8 fd	5560 - .0X V W
0060	f7 d8 3f 41 6b ab 9e	c7 a7 3b d7 3b d1 c2 72	?ck j - j - r
0070	fb 42 f4 f3 c6 eb e2	5a 5d 4c b5 69 e6 fa 67	B - . .JL i - g
0080	aa 1a c3 a4 64 f9 d2 bf	98 73 3c af 64 55 51	..dd - . .s <u>d</u> L
0090	b1 eb 29 4d eb e2 5d	a8 19 60 7a 5a dc 86	[] ..zZ -
0100	b1 eb 29 4d eb e2 5d	a8 19 60 7a 5a dc 86	[] ..zZ -
0110	82 a8 ae d1 f9 e6 88	1a c1 15 b9 de 8d 44	C Y R - HK Z3
0120	bd 51 71 59 ec ed 34 a1	d1 5d 78 1e 6f 07 54 6e	ZgY - 4 - jx o Tn
0130	ca 45 e1 22 90 61 53 fa	65 6a 2e 0f 77 dd	E " a5 <ej, w0 -
0140	fa 39 c3 b7 8a e0 0f 97	00 5d 70 21 39 cd 59 0a	9 - . .jp19 Y -
0150	a6 bc 98 45 f3 2a 7e fe	7f c1 a6 00 09 85	0 1.k4A ; Y - C6
0160	c5 e2 59 5b 29 20	54 d1 17 a4 c1 b6 b5 27	[-] - . .
0170	c1 21 ce 15 33 7c f7 60	97 2d 15 16 79 cd 3d 3b	[-] - . .y v ;
0180	a6 25 2b 42 e9 9c ce	be 25 a5 bd 82 2d 0d	e8kB - % - .(-
0190	df db fe cc 22 0c aa 56	28 88 c9 dd 44 af a3 e2	" . V (- D -
0200	c8 0d c9 df 85 5b 37	ba 7e 0f 0d 6a 5d 44	...Y - . .
0210	38 0d c9 df 85 5b 37	ba 7e 0f 0d 6a 5d 44	B - . .W - " -
0220	42 16 a2 0f 5f ce f1 01	36 91 59 ca 83 40 23 4d	B - . .6 Y - @#M
0230	0c fb d7 43 d6 da c4 34	f6 cb af a7 f7 9f 5e	C - 4 1 - . ^
0240	a6 bc 98 45 f3 2a 7e fe	7f c1 a6 00 09 85	E ~ - & - . f - E
0250	c5 e2 59 5b 16 30 a5	2a 51 c4 ff bc f5 ff 96	Yy 0 " 0 - .
0260	07 af 4a 5b ce 91 27 fb	22 2f e1 7c 06 7f b1 e1	[-] - . .

Selected Packet Bytes:

```

No: 339 - Time: 1.749288 - Source: 52.230.59.222 - Destination: 10.80.4.188 - Protocol: TCP - Length: 1514 - Info: 443 → 64291 [PSH, ACK] Seq=6928 Ack=2951 Win=64512 Len=1460 [TCP PDU reassembled in 344]
Show packet bytes Layout: Vertical (Stacked)

```



Subject: Computer Networks (01CT0503)

Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.

Experiment No: 12

Date: 24-11-2025

Enrolment No: 92301733024

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

The screenshot shows the Wireshark interface with the following details:

- Frame 73:** 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
- Interface id:** 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B})
- Interface name:** \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}
- Interface description:** Wi-Fi
- Encapsulation type:** Ethernet (1)
- Arrival Time:** Nov 21, 2024 05:53:46.848159000 India Standard Time
- UTC Arrival Time:** Nov 21, 2024 00:23:46.848159000 UTC
- Epoch Arrival Time:** 1732148626.848159000
- [Time shift for this frame]:** 0.000000000 seconds
- [Time delta from previous captured frame]:** 0.000034000 seconds
- [Time delta from previous displayed frame]:** 0.000034000 seconds
- [Time since reference or first frame]:** 5.570782000 seconds
- Frame Number:** 73
- Frame length:** 42 bytes (336 bits)
- Capture Length:** 42 bytes (336 bits)
- [Frame is marked]:** False
- [Frame is ignored]:** False
- [Protocol in frame: eth:ethertype:arp]**
- [Coloring Rule Name: ARP]**
- [Coloring Rule String: arp]**
- Ethernet II, Src: Intel_30:99:68 (00:dc:ef:30:99:68), Dst: 0:e4:ac:03:4d:3d (0:e4:ac:03:4d:3d)**
 - Destination MAC Address:** 0:e4:ac:03:4d:3d (0:e4:ac:03:4d:3d)
 -0..... - 16 bit: Locally administered address (this is NOT the factory default)**
 -0..... - 16 bit: Individual address (unicast)**
- Source: Intel_30:99:68 (00:dc:ef:30:99:68)**
 -0..... - 16 bit: Globally unique address (factory default)**
 -0..... - 16 bit: Individual address (unicast)**
- Type: ARP (0x0806)**
 - [Stream index: 0]**
- Address Resolution Protocol (reply)**
 - Hardware type: Ethernet (1)**
 - Protocol type: IPv4 (0x0800)**
 - Hardware size: 6**
 - Protocol size: 4**
 - Opcodes: reply (2)**
 - Sender MAC address: Intel_30:99:68 (00:dc:ef:30:99:68)**
 - Sender IP address: 192.168.115.172**
 - Target MAC address: 0:e4:ac:03:4d:3d (0:e4:ac:03:4d:3d)**
 - Target IP address: 192.168.115.55**

Step – 7 :- Analysis of ARP Packet

The screenshot shows the Wireshark interface with the following details:

- Frame 73:** 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
- Section number:** 1
- Interface id:** 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B})
- Interface name:** \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}
- Interface description:** Wi-Fi
- Encapsulation type:** Ethernet (1)
- Arrival Time:** Nov 21, 2024 05:53:46.848159000 India Standard Time
- UTC Arrival Time:** Nov 21, 2024 00:23:46.848159000 UTC
- Epoch Arrival Time:** 1732148626.848159000
- [Time shift for this packet]:** 0.000000000 seconds
- [Time delta from previous captured frame]:** 0.000034000 seconds
- [Time delta from previous displayed frame]:** 0.000034000 seconds
- [Time since reference or first frame]:** 5.570782000 seconds
- Frame Number:** 73
- Frame Length:** 42 bytes (336 bits)
- Capture Length:** 42 bytes (336 bits)
- [Frame is marked]:** False
- [Frame is ignored]:** False
- [Protocols in frame: eth:ethertype:arp]**
- [Coloring Rule Name: ARP]**
- [Coloring Rule String: arp]**

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



Subject: Computer Networks (01CT0503)

Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.

Experiment No: 12

Date: 24-11-2025

Enrolment No: 92301733024

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

```

Frame 73: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
  ✓ Ethernet II, Src: Intel_30:99:68 (b0:dc:ef:30:99:68), Dst: 0e:e4:ac:03:4d:3d (0e:e4:ac:03:4d:3d)
    ✓ Destination: 0e:e4:ac:03:4d:3d (0e:e4:ac:03:4d:3d)
      .... ..1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ..0. .... .... .... = IG bit: Individual address (unicast)
    ✓ Source: Intel_30:99:68 (b0:dc:ef:30:99:68)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
      .... ..0. .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 0]
  ✓ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Intel_30:99:68 (b0:dc:ef:30:99:68)
    Sender IP address: 192.168.115.172
    Target MAC address: 0e:e4:ac:03:4d:3d (0e:e4:ac:03:4d:3d)
    Target IP address: 192.168.115.55
  
```

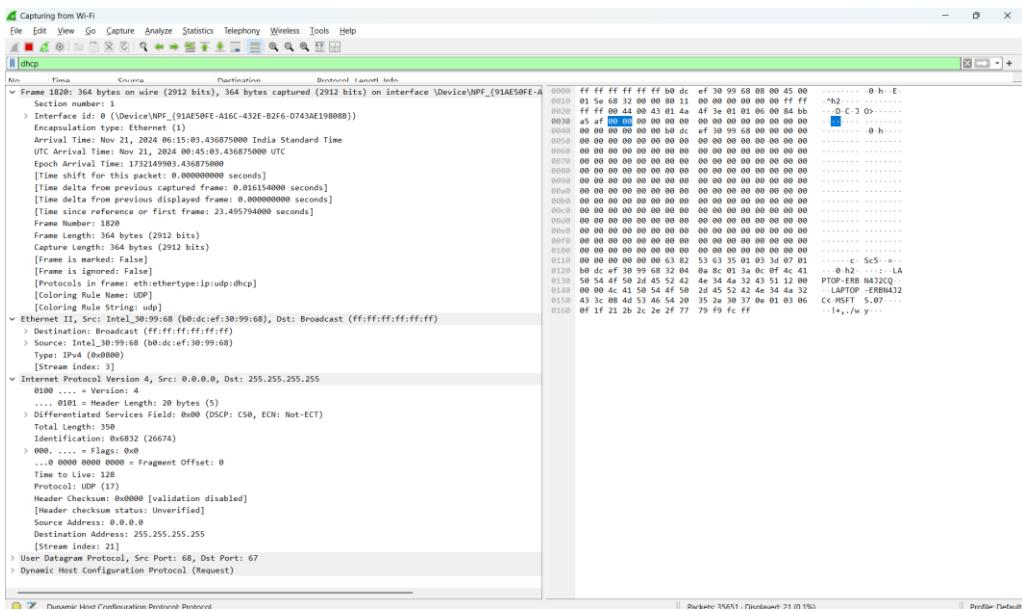
Step – 9:- It is showing the TCP related details stored in the packets: like header section src and destination port no flags , checksum , length , timestamps.

```

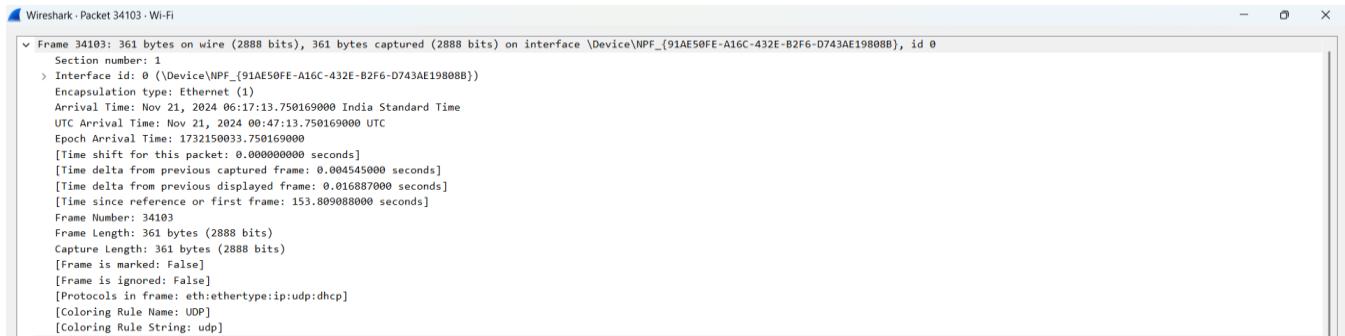
Frame 73: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
  Section number: 1
  ✓ Interface id: 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B})
    Interface name: \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}
    Interface description: Wi-Fi
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 21, 2024 05:53:46.848159000 India Standard Time
    UTC Arrival Time: Nov 21, 2024 08:23:46.848159000 UTC
    Epoch Arrival Time: 1732148626.848159000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000034000 seconds]
    [Time delta from previous displayed frame: 0.000034000 seconds]
    [Time since reference or first frame: 5.570782000 seconds]
    Frame Number: 73
    Frame Length: 42 bytes (336 bits)
    Capture Length: 42 bytes (336 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocol in frame: eth:ethertype:arp]
    [Coloring Rule Name: ARP]
    [Coloring Rule String: arp]
  ✓ Ethernet II, Src: Intel_30:99:68 (b0:dc:ef:30:99:68), Dst: 0e:e4:ac:03:4d:3d (0e:e4:ac:03:4d:3d)
    ✓ Destination: 0e:e4:ac:03:4d:3d (0e:e4:ac:03:4d:3d)
      .... ..1. .... .... .... = LG bit: Locally administered address (this is NOT the factory default)
      .... ..0. .... .... .... = IG bit: Individual address (unicast)
    ✓ Source: Intel_30:99:68 (b0:dc:ef:30:99:68)
      .... ..0. .... .... .... = LG bit: Globally unique address (factory default)
      .... ..0. .... .... .... = IG bit: Individual address (unicast)
    Type: ARP (0x0806)
    [Stream index: 0]
  ✓ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Intel_30:99:68 (b0:dc:ef:30:99:68)
    Sender IP address: 192.168.115.172
    Target MAC address: 0e:e4:ac:03:4d:3d (0e:e4:ac:03:4d:3d)
    Target IP address: 192.168.115.55
  
```

Subject: Computer Networks (01CT0503)
Experiment No: 12
Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.
Date: 24-11-2025
Enrolment No: 92301733024

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



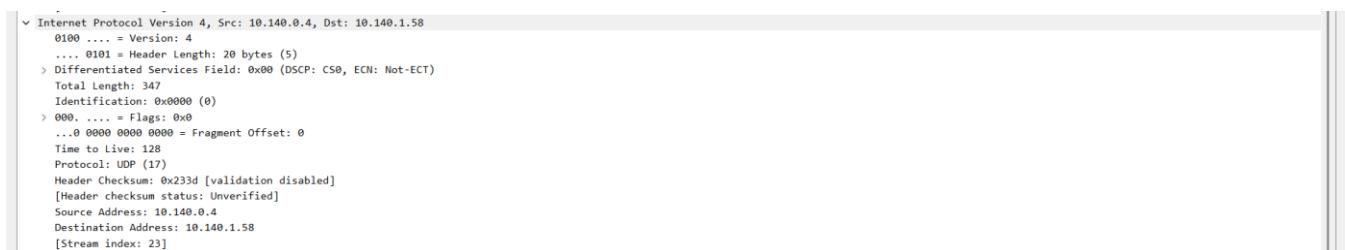
Step - 12:- It us showing the timing related details of DHCP Packet.



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



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

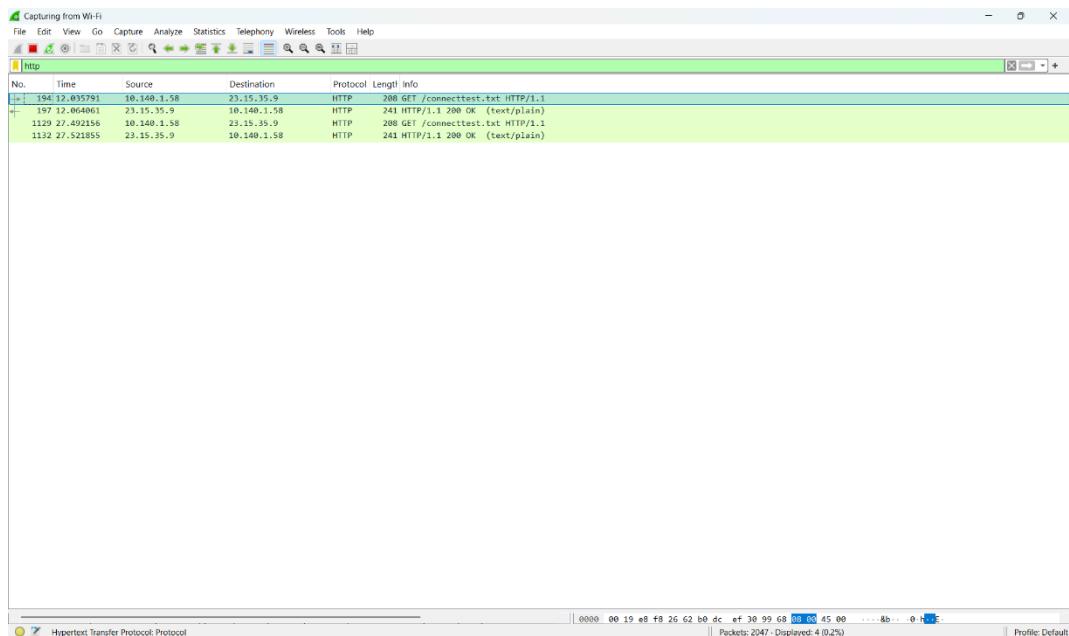


Subject: Computer Networks (01CT0503)	Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.	
Experiment No: 12	Date: 24-11-2025	Enrolment No: 92301733024

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

```
v 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)
```

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



Step - 17:- These are the timing related details of http packet

 <p>Marwadi University Marwadi Chandarana Group</p>	<p>Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology</p>	
<p>Subject: Computer Networks (01CT0503)</p>	<p>Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.</p>	
<p>Experiment No: 12</p>	<p>Date: 24-11-2025</p>	<p>Enrolment No: 92301733024</p>

```
Wireshark - Packet 194 - Wi-Fi
Frame 194: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
  Section number: 1
> Interface id: 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B})
  Encapsulation type: Ethernet (1)
  Arrival Time: Nov 21, 2024 06:29:04.101295000 India Standard Time
  UTC Arrival Time: Nov 21, 2024 00:59:04.101295000 UTC
  Epoch Arrival Time: 1732150744.101295000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000258000 seconds]
  [Time delta from previous displayed frame: 0.000000000 seconds]
  [Time since reference or first frame: 12.035791000 seconds]
  Frame Number: 194
  Frame Length: 208 bytes (1664 bits)
  Capture Length: 208 bytes (1664 bits)
  [Frame is marked: False]
  [Frame is ignored: False]
  [Protocols in frame: eth:ethertype:ip:tcp:http]
  [Coloring Rule Name: HTTP]
  [Coloring Rule String: http || tcp.port == 80 || http2]
```

Step - 18:- these are the fields of http packets :-

```
    <!-- payload (100 bytes) -->
    Hypertext Transfer Protocol
    > GET /connecttest.txt HTTP/1.1\r\n
        Cache-Control: no-cache\r\n
        Connection: Close\r\n
        Pragma: no-cache\r\n
        User-Agent: Microsoft NCSI\r\n
        Host: www.msftconnecttest.com\r\n
        \r\n
    [Response in frame: 197]
    [full request URL: http://www.msftconnecttest.com/connecttest.txt]
```