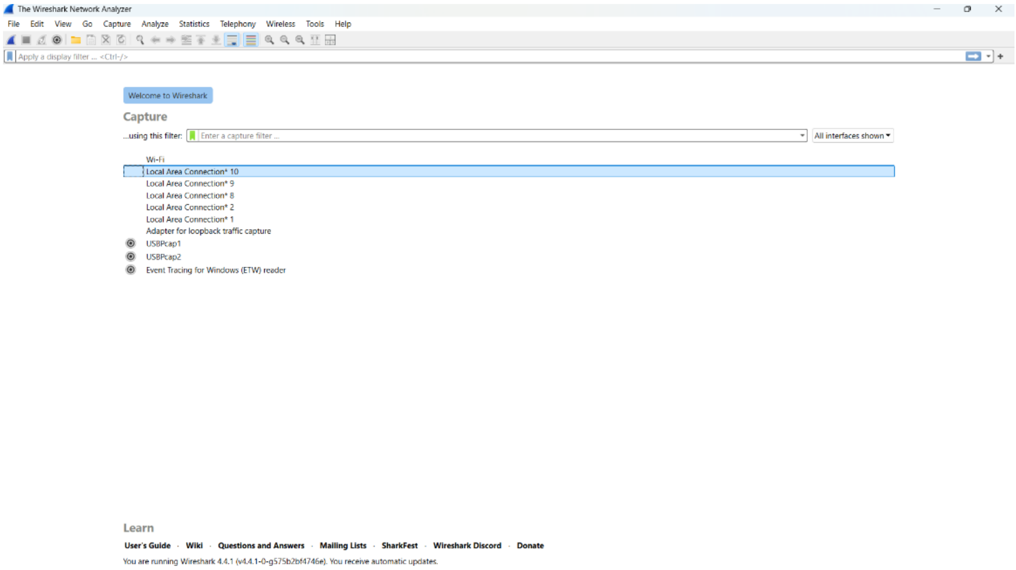
Marwadi University Marwadi Chandarana Group	Marwadi University Faculty of Engineering and Technology Department of Information and Communication Technology	
Subject: Computer Networks (01CT0503)	**Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.**	
Experiment No: 12	**Date: 14-11-2024**	**Enrolment No: 92200133030**

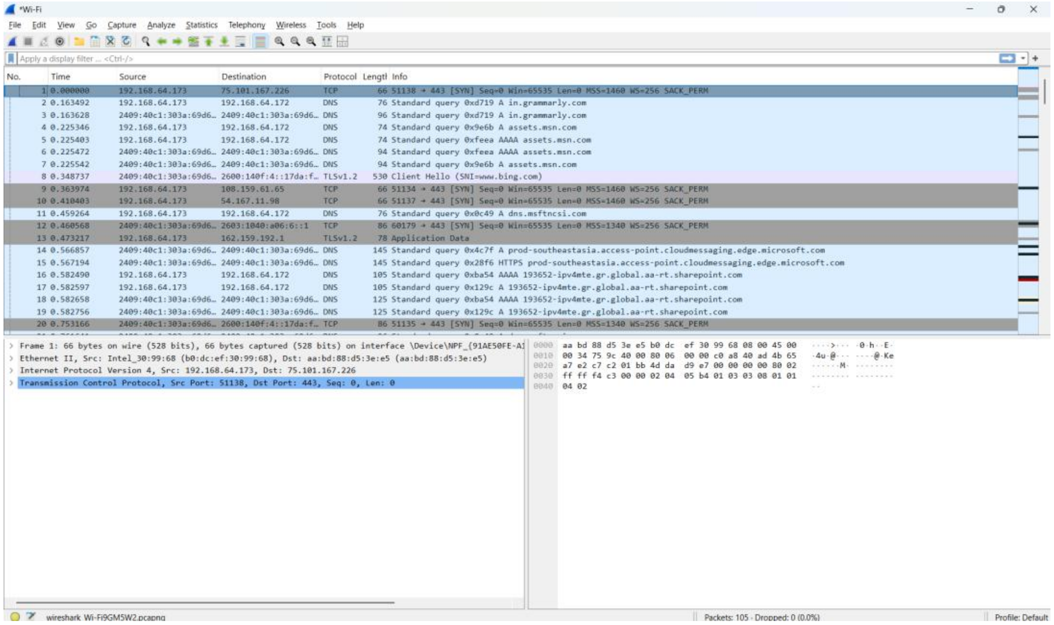
Aim: Monitor the live/real time network and analyze the concepts of various networking protocols like ARP, RARP, DHCP, HTTP, etc.

Step – 1:- Open Wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
Wi-Fi
Local Area Connection* 10
Local Area Connection* 9
Local Area Connection* 8
Local Area Connection* 2
Local Area Connection* 1
Adapter for loopback traffic capture
USBPcap1
USBPcap2
Event Tracing for Windows (ETW) reader
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.1 (v4.4.1-0-g575b2bf4746e). You receive automatic updates.

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


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

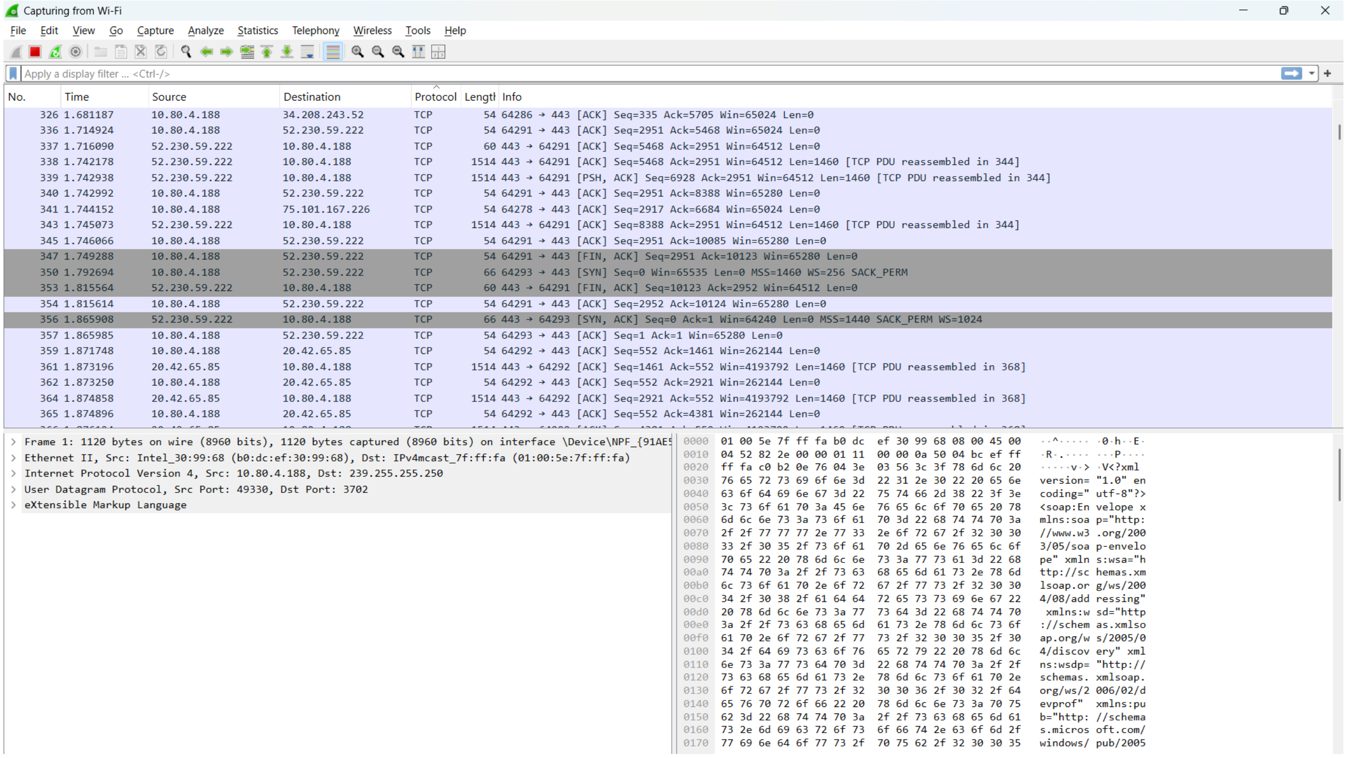
```
No.  Time      Source               Destination          Protocol Lengtl Info
   1 0.000000  192.168.64.173       75.101.167.226       TCP       66 51138 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
   2 0.163492  192.168.64.173       192.168.64.172       DNS       76 Standard query 0xd719 A in.grammarly.com
   3 0.163628  2409:40c1:303a:69d6… 2409:40c1:303a:69d6… DNS       96 Standard query 0xd719 A in.grammarly.com
   4 0.225346  192.168.64.173       192.168.64.172       DNS       74 Standard query 0x9e6b A assets.msn.com
   5 0.225403  192.168.64.173       192.168.64.172       DNS       74 Standard query 0xfeea AAAA assets.msn.com
   6 0.225472  2409:40c1:303a:69d6… 2409:40c1:303a:69d6… DNS       94 Standard query 0xfeea AAAA assets.msn.com
   7 0.225542  2409:40c1:303a:69d6… 2409:40c1:303a:69d6… DNS       94 Standard query 0x9e6b A assets.msn.com
   8 0.348737  2409:40c1:303a:69d6… 2600:140f:4::17da:f… TLSv1.2  530 Client Hello (SNI=www.bing.com)
   9 0.363974  192.168.64.173       108.159.61.65        TCP       66 51134 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  10 0.410403  192.168.64.173       54.167.11.98         TCP       66 51137 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  11 0.459264  192.168.64.173       192.168.64.172       DNS       76 Standard query 0x0c49 A dns.msftncsi.com
  12 0.460568  2409:40c1:303a:69d6… 2603:1040:a06:6::1   TCP       86 60179 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM
  13 0.473217  192.168.64.173       162.159.192.1        TLSv1.2   78 Application Data
  14 0.566857  2409:40c1:303a:69d6… 2409:40c1:303a:69d6… DNS      145 Standard query 0x4c7f A prod-southeastasia.access-point.cloudmessaging.edge.microsoft.com
  15 0.567194  2409:40c1:303a:69d6… 2409:40c1:303a:69d6… DNS      145 Standard query 0x28f6 HTTPS prod-southeastasia.access-point.cloudmessaging.edge.microsoft.com
  16 0.582490  192.168.64.173       192.168.64.172       DNS      105 Standard query 0xba54 AAAA 193652-ipv4mte.gr.global.aa-rt.sharepoint.com
  17 0.582597  192.168.64.173       192.168.64.172       DNS      105 Standard query 0x129c A 193652-ipv4mte.gr.global.aa-rt.sharepoint.com
  18 0.582658  2409:40c1:303a:69d6… 2409:40c1:303a:69d6… DNS      125 Standard query 0xba54 AAAA 193652-ipv4mte.gr.global.aa-rt.sharepoint.com
  19 0.582756  2409:40c1:303a:69d6… 2409:40c1:303a:69d6… DNS      125 Standard query 0x129c A 193652-ipv4mte.gr.global.aa-rt.sharepoint.com
  20 0.753166  2409:40c1:303a:69d6… 2600:140f:4::17da:f… TCP       86 51135 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1340 WS=256 SACK_PERM
```

```
> Frame 1: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{91AE50FE-A1
> Ethernet II, Src: Intel_30:99:68 (b0:dc:ef:30:99:68), Dst: aa:bd:88:d5:3e:e5 (aa:bd:88:d5:3e:e5)
> Internet Protocol Version 4, Src: 192.168.64.173, Dst: 75.101.167.226
> Transmission Control Protocol, Src Port: 51138, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  aa bd 88 d5 3e e5 b0 dc  ef 30 99 68 08 00 45 00   ····>··· ·0·h··E·
0010  00 34 75 9c 40 00 80 06  00 00 c0 a8 40 ad 4b 65   ·4u·@··· ····@·Ke
0020  a7 e2 c7 c2 01 bb 4d da  d9 e7 00 00 00 00 80 02   ······M· ········
0030  ff ff f4 c3 00 00 02 04  05 b4 01 03 03 08 01 01   ········ ········
0040  04 02                                              ··
```

wireshark_Wi-Fi9GM5W2.pcapng
Packets: 105 · Dropped: 0 (0.0%)
Profile: Default

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



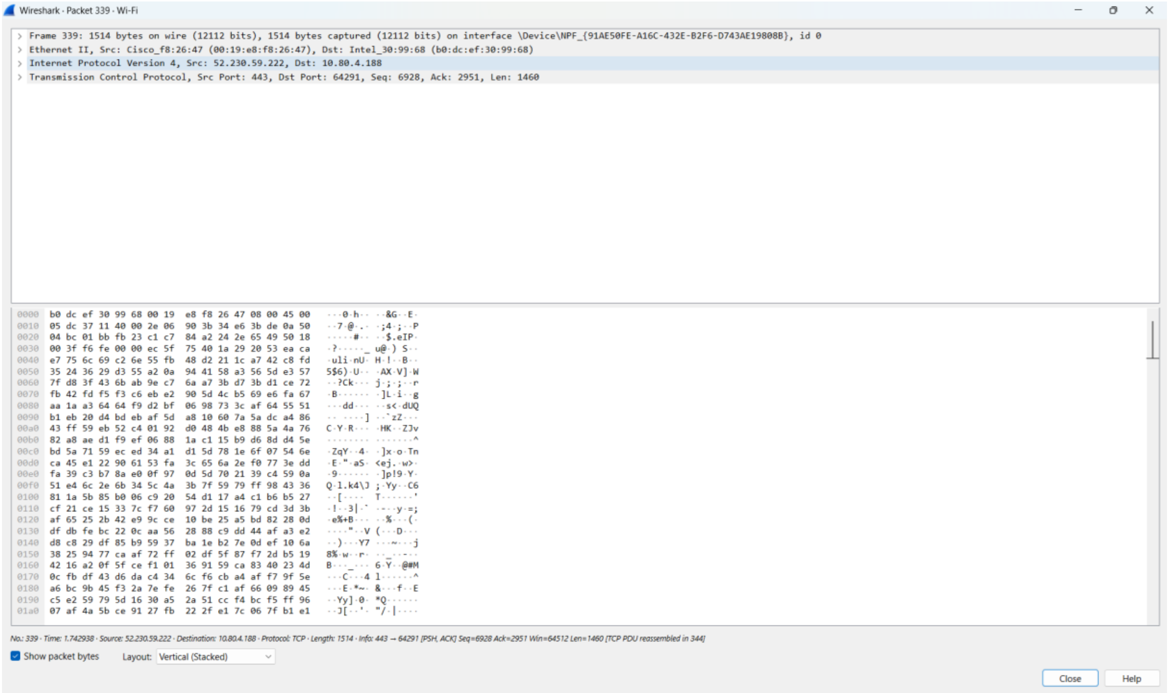
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time       Source          Destination      Protocol Lengtl Info
  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 [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 [PSH, ACK] Seq=6928 Ack=2951 Win=64512 Len=1460 [TCP PDU reassembled in 344]
  340 1.742992   10.80.4.188     52.230.59.222    TCP        54 64291 → 443 [ACK] Seq=2951 Ack=8388 Win=65280 Len=0
  341 1.744152   10.80.4.188     75.101.167.226   TCP        54 64278 → 443 [ACK] Seq=2917 Ack=6684 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 1.865908   52.230.59.222   10.80.4.188      TCP        66 443 → 64293 [SYN, ACK] Seq=0 Ack=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 Ack=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 1.873196   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=4381 Win=262144 Len=0
```

```
> Frame 1: 1120 bytes on wire (8960 bits), 1120 bytes captured (8960 bits) on interface \Device\NPF_{91AE5
> Ethernet II, Src: Intel_30:99:68 (b0:dc:ef:30:99:68), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
> Internet Protocol Version 4, Src: 10.80.4.188, Dst: 239.255.255.250
> User Datagram Protocol, Src Port: 49330, Dst Port: 3702
> eXtensible Markup Language
```

```
0000  01 00 5e 7f ff fa b0 dc  ef 30 99 68 08 00 45 00   ··^····· ·0·h··E·
0010  04 52 82 2e 00 00 01 11  00 00 0a 50 04 bc ef ff   ·R·.···· ···P····
0020  ff fa c0 b2 0e 76 04 3e  03 56 3c 3f 78 6d 6c 20   ·····v·> ·V<?xml 
0030  76 65 72 73 69 6f 6e 3d  22 31 2e 30 22 20 65 6e   version= "1.0" en
0040  63 6f 64 69 6e 67 3d 22  75 74 66 2d 38 22 3f 3e   coding=" utf-8"?>
0050  3c 73 6f 61 70 3a 45 6e  76 65 6c 6f 70 65 20 78   <soap:En velope x
0060  6d 6c 6e 73 3a 73 6f 61  70 3d 22 68 74 74 70 3a   mlns:soa p="http:
0070  2f 2f 77 77 77 2e 77 33  2e 6f 72 67 2f 32 30 30   //www.w3 .org/200
0080  33 2f 30 35 2f 73 6f 61  70 2d 65 6e 76 65 6c 6f   3/05/soa p-envelo
0090  70 65 22 20 78 6d 6c 6e  73 3a 77 73 61 3d 22 68   pe" xmln s:wsa="h
00a0  74 74 70 3a 2f 2f 73 63  68 65 6d 61 73 2e 78 6d   ttp://sc hemas.xm
00b0  6c 73 6f 61 70 2e 6f 72  67 2f 77 73 2f 32 30 30   lsoap.or g/ws/200
00c0  34 2f 30 38 2f 61 64 64  72 65 73 73 69 6e 67 22   4/08/add ressing"
00d0  20 78 6d 6c 6e 73 3a 77  73 64 3d 22 68 74 74 70    xmlns:w sd="http
00e0  3a 2f 2f 73 63 68 65 6d  61 73 2e 78 6d 6c 73 6f   ://schem as.xmlso
00f0  61 70 2e 6f 72 67 2f 77  73 2f 32 30 30 35 2f 30   ap.org/w s/2005/0
0100  34 2f 64 69 73 63 6f 76  65 72 79 22 20 78 6d 6c   4/discov ery" xml
0110  6e 73 3a 77 73 64 70 3d  22 68 74 74 70 3a 2f 2f   ns:wsdp= "http://
0120  73 63 68 65 6d 61 73 2e  78 6d 6c 73 6f 61 70 2e   schemas. xmlsoap.
0130  6f 72 67 2f 77 73 2f 32  30 30 36 2f 30 32 2f 64   org/ws/2 006/02/d
0140  65 76 70 72 6f 66 22 20  78 6d 6c 6e 73 3a 70 75   evprof"  xmlns:pu
0150  62 3d 22 68 74 74 70 3a  2f 2f 73 63 68 65 6d 61   b="http: //schema
0160  73 2e 6d 69 63 72 6f 73  6f 66 74 2e 63 6f 6d 2f   s.micros oft.com/
0170  77 69 6e 64 6f 77 73 2f  70 75 62 2f 32 30 30 35   windows/ pub/2005
```

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



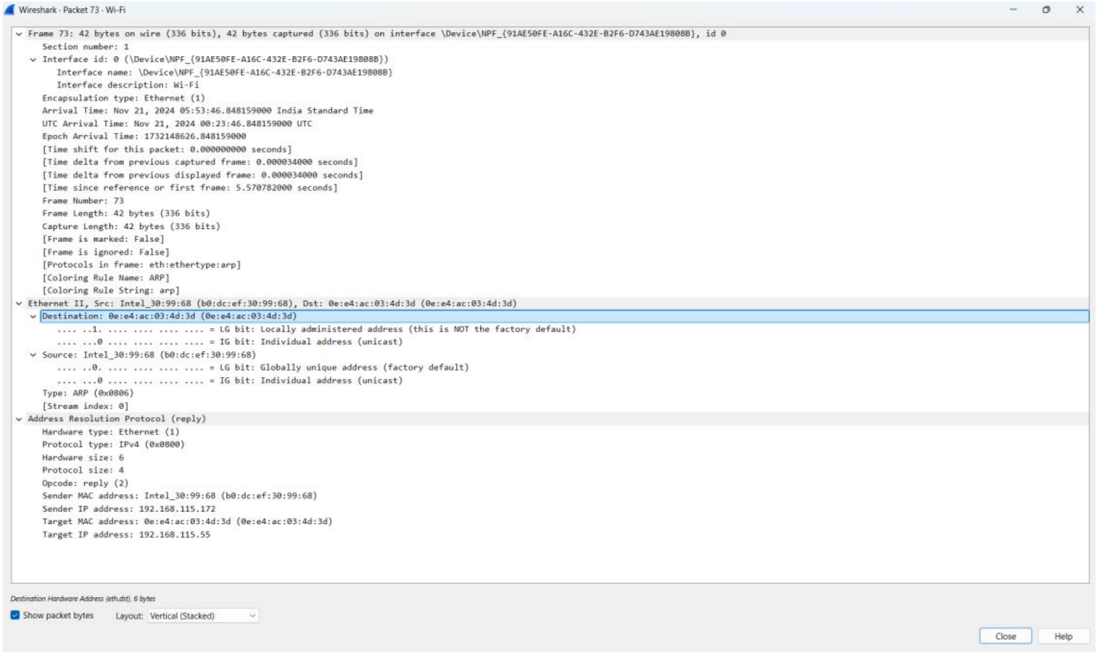
```
> Frame 339: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
> Ethernet II, Src: Cisco_f8:26:47 (00:19:e8:f8:26:47), Dst: Intel_30:99:68 (b0:dc:ef:30:99:68)
> Internet Protocol Version 4, Src: 52.230.59.222, Dst: 10.80.4.188
> Transmission Control Protocol, Src Port: 443, Dst Port: 64291, Seq: 6928, Ack: 2951, Len: 1460
```

```
0000  b0 dc ef 30 99 68 00 19  e8 f8 26 47 08 00 45 00   ···0·h·· ··&G··E·
0010  05 dc 37 11 40 00 2e 06  90 3b 34 e6 3b de 0a 50   ··7·@·.· ·;4·;··P
0020  04 bc 01 bb fb 23 c1 c7  84 a2 24 2e 65 49 50 18   ·····#·· ··$.eIP·
0030  00 3f f6 fe 00 00 ec 5f  75 40 1a 29 20 53 ea ca   ·?·····_ u@·) S··
0040  e7 75 6c 69 c2 6e 55 fb  48 d2 21 1c a7 42 c8 fd   ·uli·nU· H·!··B··
0050  35 24 36 29 d3 55 a2 0a  94 41 58 a3 56 5d e3 57   5$6)·U·· ·AX·V]·W
0060  7f d8 3f 43 6b ab 9e c7  6a a7 3b d7 3b d1 ce 72   ··?Ck··· j·;·;··r
0070  fb 42 fd f5 f3 c6 eb e2  90 5d 4c b5 69 e6 fa 67   ·B······ ·]L·i··g
0080  aa 1a a3 64 64 f9 d2 bf  06 98 73 3c af 64 55 51   ···dd··· ··s<·dUQ
0090  b1 eb 20 d4 bd eb af 5d  a8 10 60 7a 5a dc a4 86   ·· ····] ··`zZ···
00a0  43 ff 59 eb 52 c4 01 92  d0 48 4b e8 88 5a 4a 76   C·Y·R··· ·HK··ZJv
00b0  82 a8 ae d1 f9 ef 06 88  1a c1 15 b9 d6 8d d4 5e   ········ ·······^
00c0  bd 5a 71 59 ec ed 34 a1  d1 5d 78 1e 6f 07 54 6e   ·ZqY··4· ·]x·o·Tn
00d0  ca 45 e1 22 90 61 53 fa  3c 65 6a 2e f0 77 3e dd   ·E·"·aS· <ej.·w>·
00e0  fa 39 c3 b7 8a e0 0f 97  0d 5d 70 21 39 c4 59 0a   ·9······ ·]p!9·Y·
00f0  51 e4 6c 2e 6b 34 5c 4a  3b 7f 59 79 ff 98 43 36   Q·l.k4\J ;·Yy··C6
0100  81 1a 5b 85 b0 06 c9 20  54 d1 17 a4 c1 b6 b5 27   ··[····  T······'
0110  cf 21 ce 15 33 7c f7 60  97 2d 15 16 79 cd 3d 3b   ·!··3|·` ·-··y·=;
0120  af 65 25 2b 42 e9 9c ce  10 be 25 a5 bd 82 28 0d   ·e%+B··· ··%···(·
0130  df db fe bc 22 0c aa 56  28 88 c9 dd 44 af a3 e2   ····"··V (···D···
0140  d8 c8 29 df 85 b9 59 37  ba 1e b2 7e 0d ef 10 6a   ··)···Y7 ···~···j
0150  38 25 94 77 ca af 72 ff  02 df 5f 87 f7 2d b5 19   8%·w··r· ··_··-··
0160  42 16 a2 0f 5f ce f1 01  36 91 59 ca 83 40 23 4d   B···_··· 6·Y··@#M
0170  0c fb df 43 d6 da c4 34  6c f6 cb a4 af f7 9f 5e   ···C···4 l······^
0180  a6 bc 9b 45 f3 2a 7e fe  26 7f c1 af 66 09 89 45   ···E·*~· &···f··E
0190  c5 e2 59 79 5d 16 30 a5  2a 51 cc f4 bc f5 ff 96   ··Yy]·0· *Q······
01a0  07 af 4a 5b ce 91 27 fb  22 2f e1 7c 06 7f b1 e1   ··J[··'· "/·|····
```

No.: 339 · Time: 1.742938 · 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)

<u>Step – 5 :-</u> Now we will analyze one ARP Packet

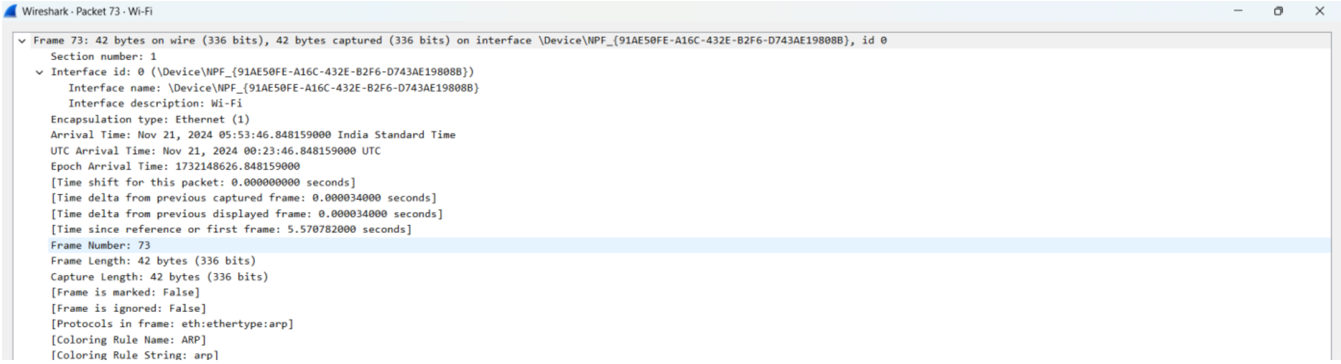


```
v Frame 73: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
    Section number: 1
  v Interface id: 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B})
      Interface name: \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}
      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]
v 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)
  v 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)
  v 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]
v 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
```

Destination Hardware Address (eth.dst), 6 bytes

☑ Show packet bytes   Layout: Vertical (Stacked)

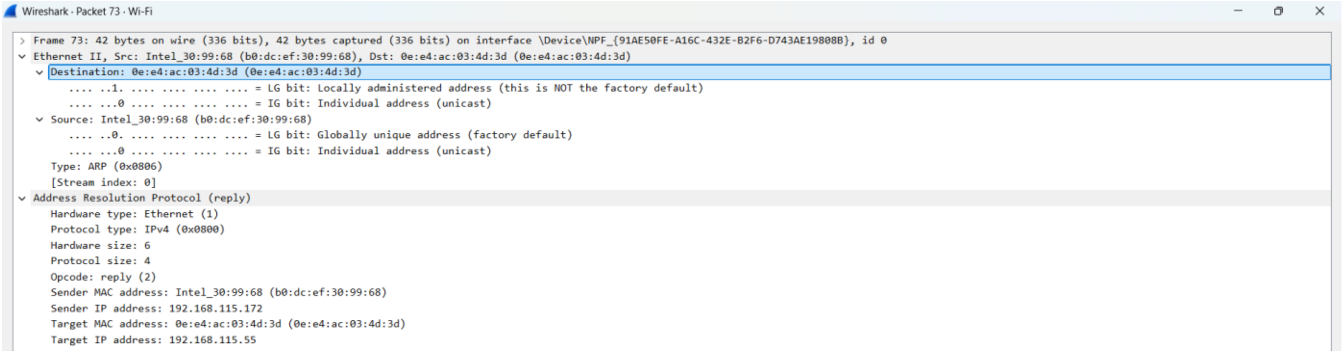
<u>Step – 7 :-</u> Analysis of ARP Packet



```
v 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
  v 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.

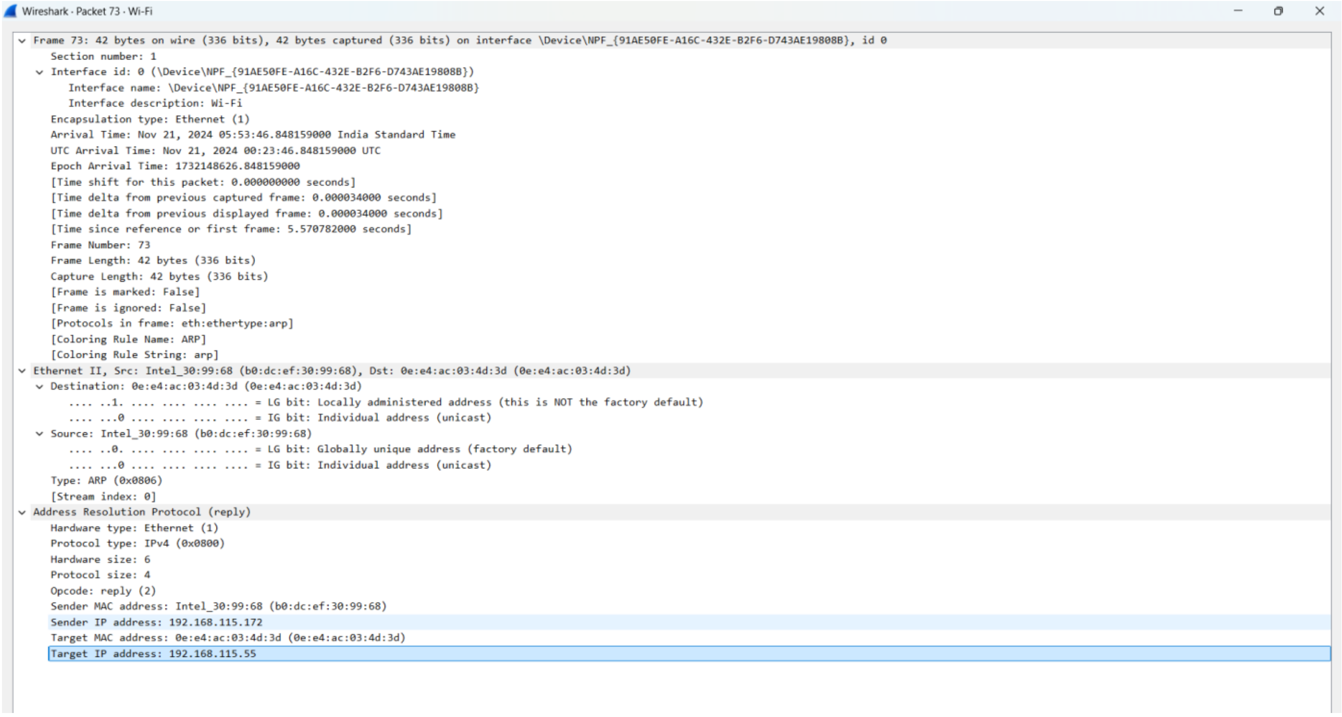
<u>Step – 8:-</u> It is showing the source and destination IP Address:-



Wireshark · Packet 73 · Wi-Fi

```
> Frame 73: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
v 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)
  v 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)
  v 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]
v 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
```

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



Wireshark · Packet 73 · Wi-Fi

```
v 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
  v 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]
v 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)
  v 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)
  v 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]
v 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
```

□ **Destination MAC Address**:

- 0e:e4:ac:03:4d:3d
- This is the MAC address of the device receiving the ARP reply.
- LG Bit indicates it's a **locally administered address**, not factory default.

□ **Source MAC Address**:

- b0:dc:ef:30:99:68

- This is the MAC address of the device sending the ARP reply.
- IG Bit indicates it's an **individually assigned address**, meaning it's a unique address for this device.

□ **Type**:

- 0x0806 (ARP)
- Indicates this is an ARP packet.

□ **Hardware Type**:

- Ethernet (1)
- Specifies the hardware type for the network, in this case, Ethernet.

□ **Protocol Type**:

- IPv4 (0x0800)
- Indicates the protocol type used, which is IPv4.

□ **Hardware Size**:

- 6
- Represents the size (in bytes) of the hardware address (MAC address).

□ **Protocol Size**:

- 4
- Represents the size (in bytes) of the protocol address (IPv4 address).

□ **Opcode**:

- reply (2)
- Indicates that this is an ARP reply packet.

□ **Sender MAC Address**:

- b0:dc:ef:30:99:68
- The MAC address of the sender (the device replying to the ARP request).

□ **Sender IP Address**:

- 192.168.115.172
- The IP address associated with the sender's MAC address.

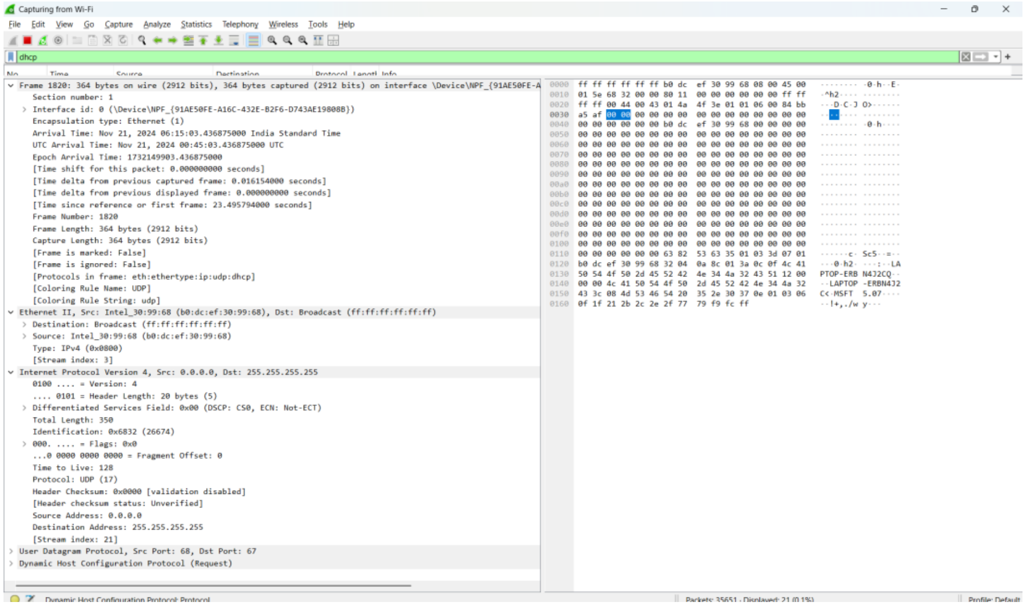
□ **Target MAC Address**:

- 0e:e4:ac:03:4d:3d
- The MAC address of the device that sent the ARP request (target device).

□ **Target IP Address**:

- 192.168.115.55
- The IP address of the target device that the ARP request was intended for.

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



Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
No. Time Source Destination Protocol Length Info

```
v Frame 1820: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF_{91AE50FE-A
    Section number: 1
  > Interface id: 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 21, 2024 06:15:03.436875000 India Standard Time
    UTC Arrival Time: Nov 21, 2024 00:45:03.436875000 UTC
    Epoch Arrival Time: 1732149903.436875000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.016154000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 23.495794000 seconds]
    Frame Number: 1820
    Frame Length: 364 bytes (2912 bits)
    Capture Length: 364 bytes (2912 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dhcp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
v Ethernet II, Src: Intel_30:99:68 (b0:dc:ef:30:99:68), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Intel_30:99:68 (b0:dc:ef:30:99:68)
    Type: IPv4 (0x0800)
    [Stream index: 3]
v Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 350
    Identification: 0x6832 (26674)
  > 000. .... = Flags: 0x0
    ...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: 0.0.0.0
    Destination Address: 255.255.255.255
    [Stream index: 21]
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

```
0000  ff ff ff ff ff ff b0 dc  ef 30 99 68 08 00 45 00   ········ ·0·h··E·
0010  01 5e 68 32 00 00 80 11  00 00 00 00 00 00 ff ff   ·^h2···· ········
0020  ff ff 00 44 00 43 01 4a  4f 3e 01 01 06 00 84 bb   ···D·C·J O>······
0030  a5 af 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 b0 dc  ef 30 99 68 00 00 00 00   ········ ·0·h····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c· Sc5··=··
0120  b0 dc ef 30 99 68 32 04  0a 8c 01 3a 0c 0f 4c 41   ···0·h2· ···:··LA
0130  50 54 4f 50 2d 45 52 42  4e 34 4a 32 43 51 12 00   PTOP-ERB N4J2CQ··
0140  00 00 4c 41 50 54 4f 50  2d 45 52 42 4e 34 4a 32   ··LAPTOP -ERBN4J2
0150  43 3c 08 4d 53 46 54 20  35 2e 30 37 0e 01 03 06   C<·MSFT  5.07····
0160  0f 1f 21 2b 2c 2e 2f 77  79 f9 fc ff               ··!+,./w y···
```

Dynamic Host Configuration Protocol: Protocol
Packets: 35651 · Displayed: 21 (0.1%)
Profile: Default

DHCP Packet Details

1. Destination MAC Address:
   - Intel_30:99:68 (b0:dc:ef:30:99:68)
   - The MAC address of the destination device (the DHCP client).
2. Source MAC Address:
   - HewlettPacka_6e:03:5c (00:0b:86:6e:03:5c)
   - The MAC address of the source device (the DHCP server).
3. Type:
   - IPv4 (0x0800)
   - Indicates the packet is an IPv4 protocol.
   -

Internet Protocol Version 4 (IPv4)

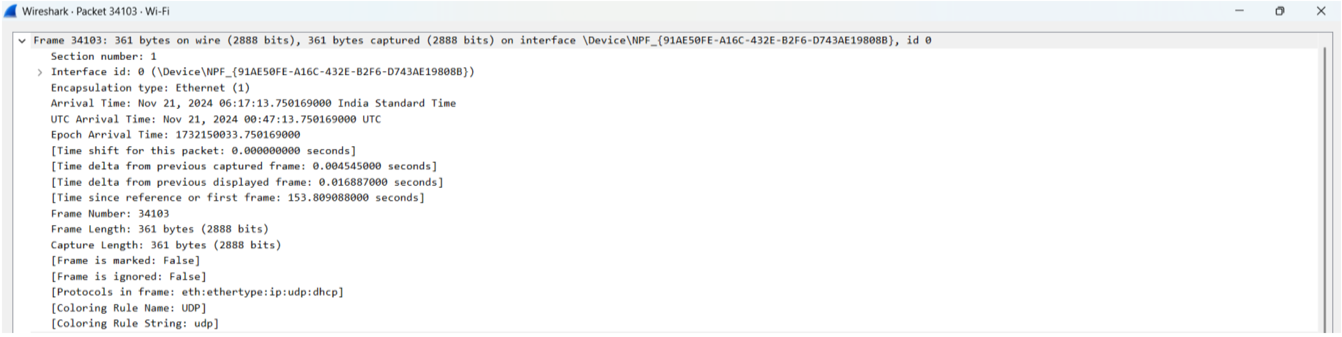
1. Version:
   - 4
   - The version of the Internet Protocol, here IPv4.
2. Header Length:
   - 20 bytes
   - Length of the IPv4 header.
3. Differentiated Services Field:
   - 0x00
   - DSCP (Differentiated Services Code Point) and ECN (Explicit Congestion Notification) values.
4. Total Length:
   - 347
   - Total length of the IP packet, including headers and payload.

5. Identification:
   - 0x0000
   - Used for packet reassembly; all fragments of the same packet have the same identification.
6. Flags:
   - 0x0
   - Indicates fragmentation; here, no fragmentation is used.
7. Time to Live (TTL):
   - 128
   - Maximum hops the packet can take before being discarded.
8. Protocol:
   - UDP (17)
   - The transport protocol used.
9. Header Checksum:
   - 0x233d
   - Verifies the integrity of the IP header.
10. Source Address:
    - 10.140.0.4
    - The IP address of the DHCP server.
11. Destination Address:
    - 10.140.1.58
    - The IP address of the DHCP client.

User Datagram Protocol (UDP)

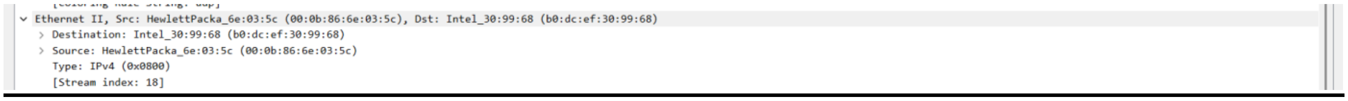
1. Source Port:
   - 67
   - The port used by the DHCP server.
2. Destination Port:
   - 68
   - The port used by the DHCP client.
3. Length:
   - 327
   - Length of the UDP header and payload.
4. Checksum:
   - Verifies the integrity of the UDP header and payload. Value not explicitly shown here.

<u>Step - 12:-</u> It us showing the timing related details of DHCP Packet.



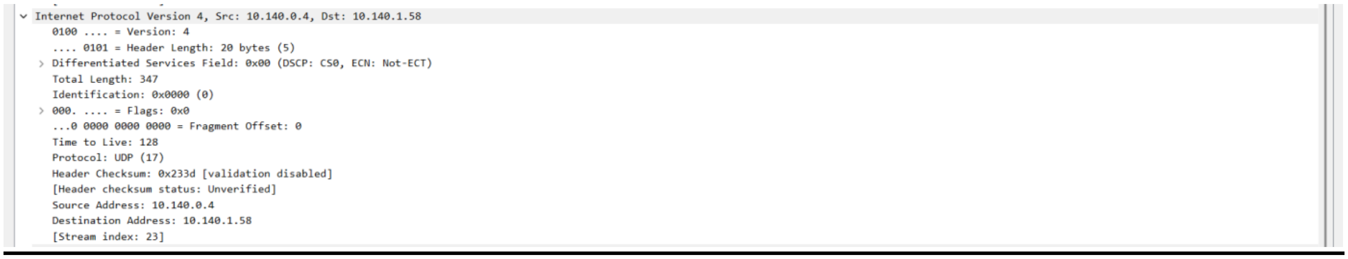
```
Frame 34103: 361 bytes on wire (2888 bits), 361 bytes captured (2888 bits) on interface \Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B}, id 0
    Section number: 1
  > Interface id: 0 (\Device\NPF_{91AE50FE-A16C-432E-B2F6-D743AE19808B})
    Encapsulation type: Ethernet (1)
    Arrival Time: Nov 21, 2024 06:17:13.750169000 India Standard Time
    UTC Arrival Time: Nov 21, 2024 00:47:13.750169000 UTC
    Epoch Arrival Time: 1732150033.750169000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.004545000 seconds]
    [Time delta from previous displayed frame: 0.016887000 seconds]
    [Time since reference or first frame: 153.809088000 seconds]
    Frame Number: 34103
    Frame Length: 361 bytes (2888 bits)
    Capture Length: 361 bytes (2888 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:dhcp]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
```

<u>Step - 13:-</u> It is showing the ip related details of DHCP Packet.



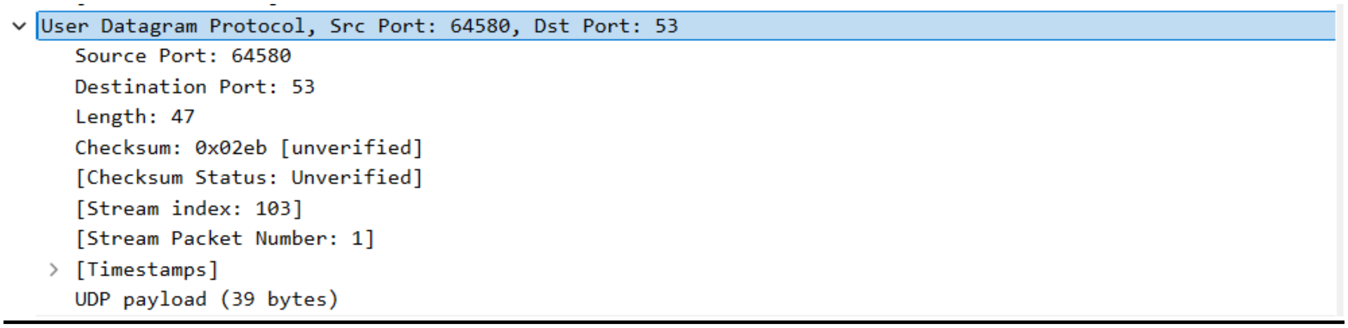
```
Ethernet II, Src: HewlettPacka_6e:03:5c (00:0b:86:6e:03:5c), Dst: Intel_30:99:68 (b0:dc:ef:30:99:68)
  > Destination: Intel_30:99:68 (b0:dc:ef:30:99:68)
  > Source: HewlettPacka_6e:03:5c (00:0b:86:6e:03:5c)
    Type: IPv4 (0x0800)
    [Stream index: 18]
```

<u>Step - 14:-</u> It is showing the details about the flags of DHCP Packet.



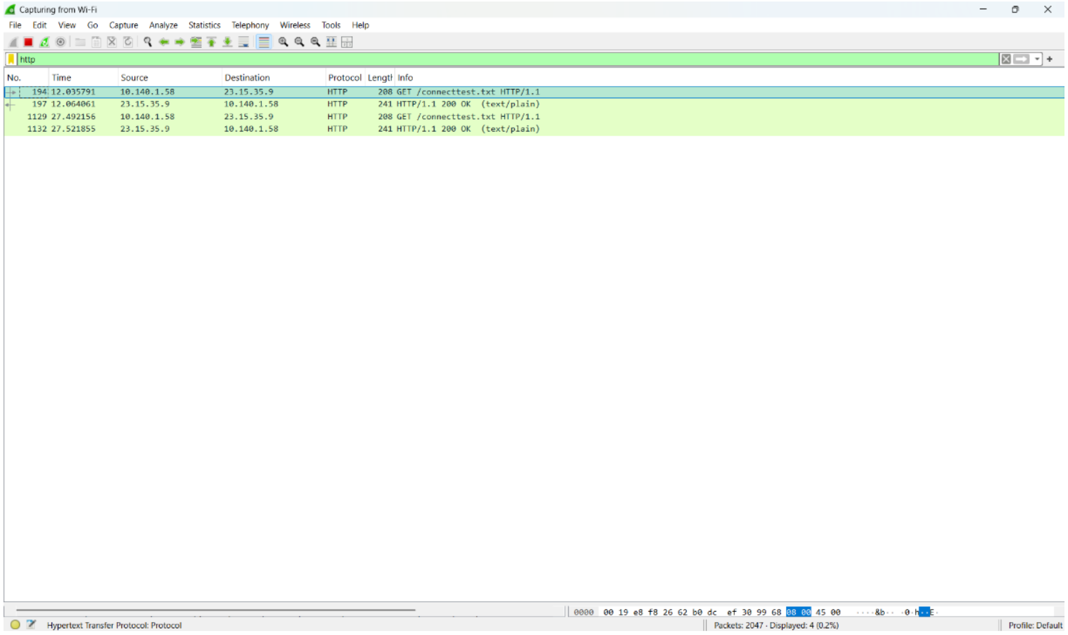
```
Internet Protocol Version 4, Src: 10.140.0.4, Dst: 10.140.1.58
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 347
    Identification: 0x0000 (0)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 128
    Protocol: UDP (17)
    Header Checksum: 0x233d [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 10.140.0.4
    Destination Address: 10.140.1.58
    [Stream index: 23]
```

<u>Step - 15:-</u> It is showing the details about the header of DHCP 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)
```

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



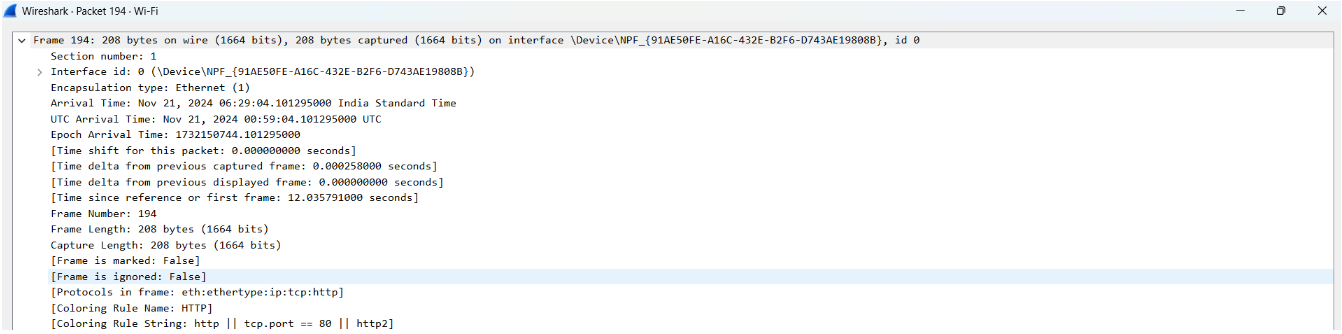
Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http

```
No.   Time       Source       Destination  Protocol Lengtl Info
  194 12.035791  10.140.1.58  23.15.35.9   HTTP     208 GET /connecttest.txt HTTP/1.1
  197 12.064061  23.15.35.9   10.140.1.58  HTTP     241 HTTP/1.1 200 OK  (text/plain)
 1129 27.492156  10.140.1.58  23.15.35.9   HTTP     208 GET /connecttest.txt HTTP/1.1
 1132 27.521855  23.15.35.9   10.140.1.58  HTTP     241 HTTP/1.1 200 OK  (text/plain)

0000  00 19 e8 f8 26 62 b0 dc  ef 30 99 68 08 00 45 00   ····&b·· ·0·h··E·
```

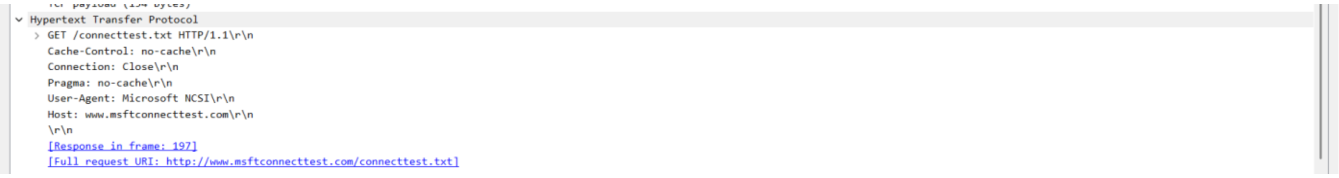
Hypertext Transfer Protocol: Protocol
Packets: 2047 · Displayed: 4 (0.2%)
Profile: Default

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



```
v 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 :-



```
    TCP payload (154 bytes)
v 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 URI: http://www.msftconnecttest.com/connecttest.txt]
```

- HTTP/1.1

- Version: This shows that the request and response are operating with the Hypertext Transfer Protocol version 1.1. This version brought along several enhancements of HTTP/1.0, such as persistent connection and pipelining.

- Cache-Control: no-cache
- Purposes: This header tells both the client and intermediate caches not to cache the response. It is applied on dynamic content when it is changing frequently or sensitive information that should not be cached.

- Connection: close

- Purpose: This header tells the client and server to close the connection after this request/response cycle. That is to say that further requests will need a new connection to be opened.

- Pragma: no-cache

- Purpose: Although this header is considered deprecated in HTTP/1.1, some clients may still make use of this. This has exactly the same effect as Cache-Control: no-cache.

- User-Agent: Microsoft MSI

- Purpose: This header indicates what client software is making the request. In this example, it's a part of Microsoft Installer (MSI).
- Host: www.msftconnecttest.com [invalid URL deleted]
- [middle]
- Purpose: This header names the domain name of the server that the client wishes to connect to.
- Response in frame: 197
- [middle]
- Purpose: This means that the response to the query is framed in frame number 197 of the captured packet.

<u>Conclusion:-</u>

By Performing this experiment I analyzed the packes of ARP , DHCP and HTTP.I seen how ARP translates IP addresses to MAC addresses, enabling devices to communicate within a local network .
I analyzed how device acquires IP address and other network configurations dynamically.I analzed Discover, Offer, Request, and Acknowledgement packets, and at the end Ianalyzed http request packet understood how client-server communication operates in retrieving or sending data over the web.