EXP NO : 4B **S.KEERTHANA**
DATE: 19/08/24 **231901022**

PACKET SNIFFING USING WIRESHARK

AIM:

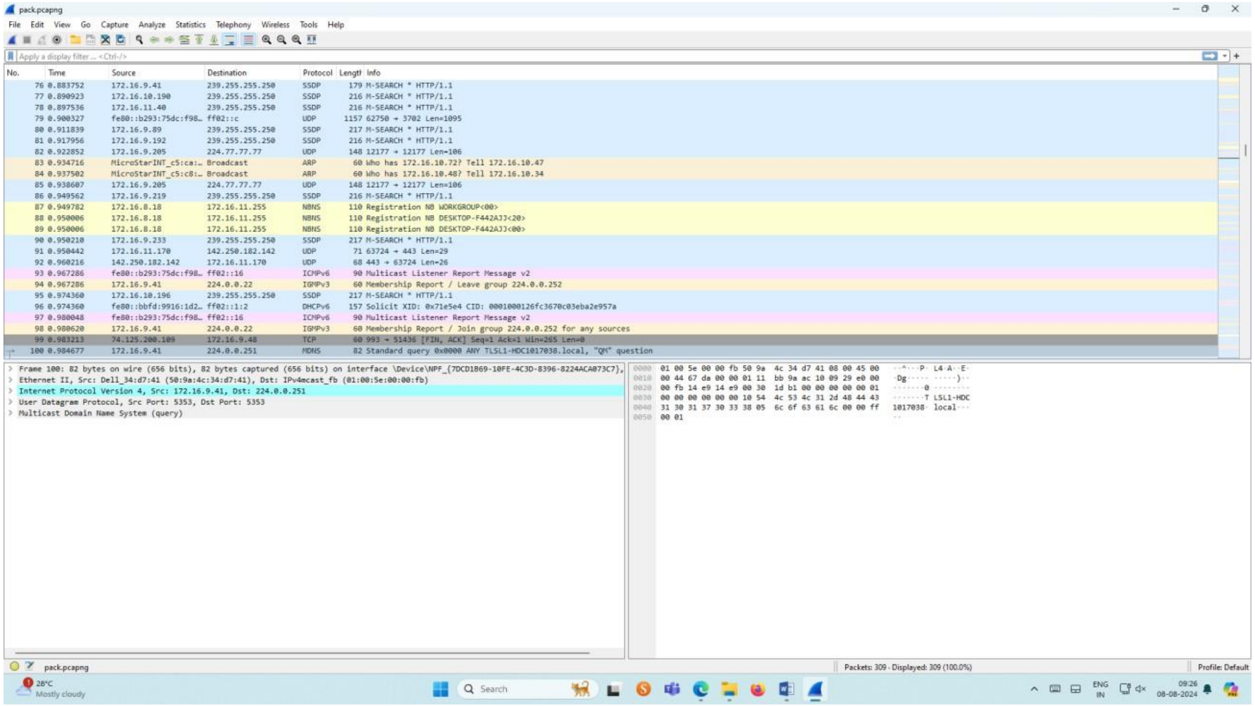
Exercises

1. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ⚇option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Save the packets.

Output



```
No.  Time      Source                 Destination      Protocol Length Info
 76 0.883752  172.16.9.41            239.255.255.250  SSDP      179 M-SEARCH * HTTP/1.1
 77 0.890923  172.16.10.190          239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
 78 0.897536  172.16.11.40           239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
 79 0.900327  fe80::b293:75dc:f98…   ff02::c          UDP      1157 62750 → 3702 Len=1095
 80 0.911839  172.16.9.89            239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
 81 0.917956  172.16.9.192           239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
 82 0.922852  172.16.9.205           224.77.77.77     UDP       148 12177 → 12177 Len=106
 83 0.934716  MicroStarINT_c5:ca:…   Broadcast        ARP        60 Who has 172.16.10.72? Tell 172.16.10.47
 84 0.937502  MicroStarINT_c5:c8:…   Broadcast        ARP        60 Who has 172.16.10.48? Tell 172.16.10.34
 85 0.938607  172.16.9.205           224.77.77.77     UDP       148 12177 → 12177 Len=106
 86 0.949562  172.16.9.219           239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
 87 0.949782  172.16.8.18            172.16.11.255    NBNS      110 Registration NB WORKGROUP<00>
 88 0.950006  172.16.8.18            172.16.11.255    NBNS      110 Registration NB DESKTOP-F442AJJ<20>
 89 0.950006  172.16.8.18            172.16.11.255    NBNS      110 Registration NB DESKTOP-F442AJJ<00>
 90 0.950210  172.16.9.233           239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
 91 0.950442  172.16.11.170          142.250.182.142  UDP        71 63724 → 443 Len=29
 92 0.960216  142.250.182.142        172.16.11.170    UDP        68 443 → 63724 Len=26
 93 0.967286  fe80::b293:75dc:f98…   ff02::16         ICMPv6     90 Multicast Listener Report Message v2
 94 0.967286  172.16.9.41            224.0.0.22       IGMPv3     60 Membership Report / Leave group 224.0.0.252
 95 0.974360  172.16.10.196          239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
 96 0.974360  fe80::bbfd:9916:1d2…   ff02::1:2        DHCPv6    157 Solicit XID: 0x71e5e4 CID: 0001000126fc3670c03eba2e957a
 97 0.980048  fe80::b293:75dc:f98…   ff02::16         ICMPv6     90 Multicast Listener Report Message v2
 98 0.980620  172.16.9.41            224.0.0.22       IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
 99 0.983213  74.125.200.109         172.16.9.48      TCP        60 993 → 51436 [FIN, ACK] Seq=1 Ack=1 Win=265 Len=0
100 0.984677  172.16.9.41            224.0.0.251      MDNS       82 Standard query 0x0000 ANY TLSL1-HDC1017038.local, "QM" question

> Frame 100: 82 bytes on wire (656 bits), 82 bytes captured (656 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7},
> Ethernet II, Src: Dell_34:d7:41 (50:9a:4c:34:d7:41), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 172.16.9.41, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)

0000  01 00 5e 00 00 fb 50 9a  4c 34 d7 41 08 00 45 00   ··^···P· L4·A··E·
0010  00 44 67 da 00 00 01 11  bb 9a ac 10 09 29 e0 00   ·Dg····· ·····)··
0020  00 fb 14 e9 14 e9 00 30  1d b1 00 00 00 00 00 01   ·······0 ········
0030  00 00 00 00 00 00 10 54  4c 53 4c 31 2d 48 44 43   ·······T LSL1-HDC
0040  31 30 31 37 30 33 38 05  6c 6f 63 61 6c 00 00 ff   1017038· local···
0050  00 01                                              ··

pack.pcapng          Packets: 309 · Displayed: 309 (100.0%)          Profile: Default
```

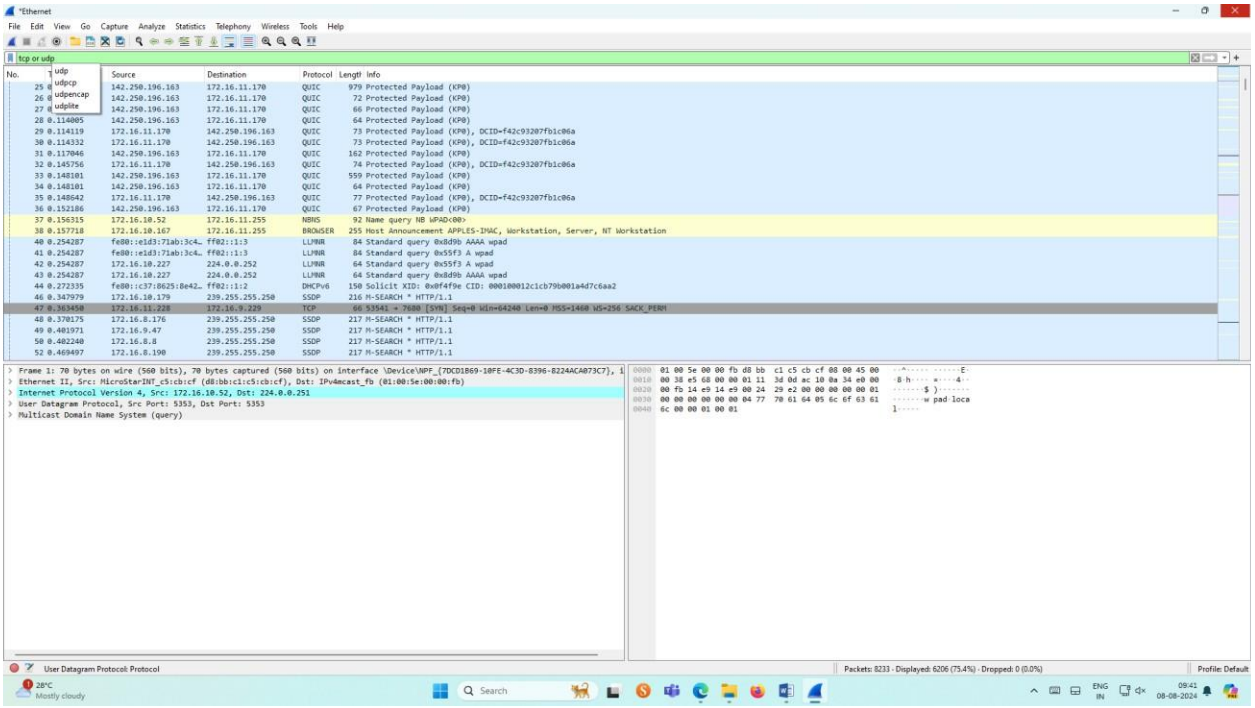
pack.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
28°C
Mostly cloudy
Search
ENG
IN
09:26
08-08-2024

2.Create a Filter to display only TCP/UDP packets, inspect the packets and provide the flow graph.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ⚇option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics⚇Flow graph.
- Save the packets.

Output:



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
udp
udpcp
udpencap
udplite

tcp or udp

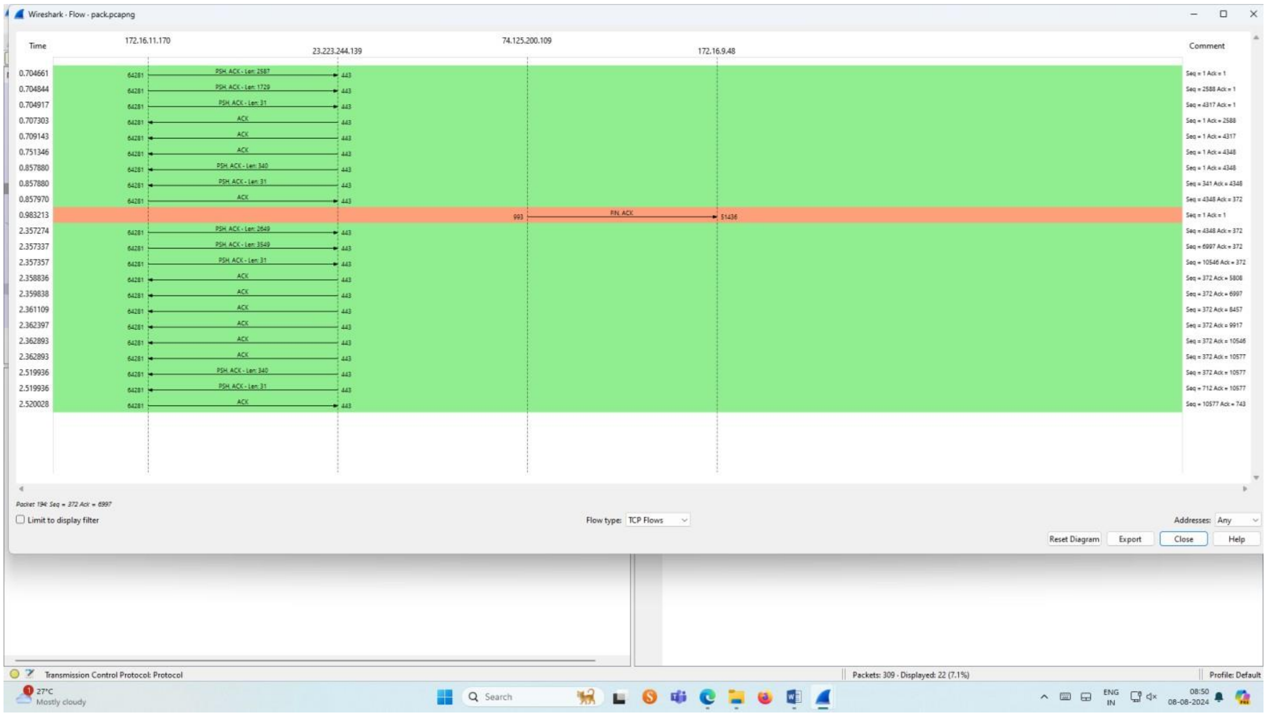
```
No.   Time      Source               Destination      Protocol Length Info
   25 0         142.250.196.163      172.16.11.170    QUIC      979 Protected Payload (KP0)
   26 0         142.250.196.163      172.16.11.170    QUIC       72 Protected Payload (KP0)
   27 0         142.250.196.163      172.16.11.170    QUIC       66 Protected Payload (KP0)
   28 0.114005  142.250.196.163      172.16.11.170    QUIC       64 Protected Payload (KP0)
   29 0.114119  172.16.11.170        142.250.196.163  QUIC       73 Protected Payload (KP0), DCID=f42c93207fb1c06a
   30 0.114332  172.16.11.170        142.250.196.163  QUIC       73 Protected Payload (KP0), DCID=f42c93207fb1c06a
   31 0.117046  142.250.196.163      172.16.11.170    QUIC      162 Protected Payload (KP0)
   32 0.145756  172.16.11.170        142.250.196.163  QUIC       74 Protected Payload (KP0), DCID=f42c93207fb1c06a
   33 0.148101  142.250.196.163      172.16.11.170    QUIC      559 Protected Payload (KP0)
   34 0.148101  142.250.196.163      172.16.11.170    QUIC       64 Protected Payload (KP0)
   35 0.148642  172.16.11.170        142.250.196.163  QUIC       77 Protected Payload (KP0), DCID=f42c93207fb1c06a
   36 0.152186  142.250.196.163      172.16.11.170    QUIC       67 Protected Payload (KP0)
   37 0.156315  172.16.10.52         172.16.11.255    NBNS       92 Name query NB WPAD<00>
   38 0.157718  172.16.10.167        172.16.11.255    BROWSER   255 Host Announcement APPLES-IMAC, Workstation, Server, NT Workstation
   40 0.254287  fe80::e1d3:71ab:3c4… ff02::1:3        LLMNR      84 Standard query 0x8d9b AAAA wpad
   41 0.254287  fe80::e1d3:71ab:3c4… ff02::1:3        LLMNR      84 Standard query 0x55f3 A wpad
   42 0.254287  172.16.10.227        224.0.0.252      LLMNR      64 Standard query 0x55f3 A wpad
   43 0.254287  172.16.10.227        224.0.0.252      LLMNR      64 Standard query 0x8d9b AAAA wpad
   44 0.272335  fe80::c37:8625:8e42… ff02::1:2        DHCPv6    150 Solicit XID: 0x0f4f9e CID: 000100012c1cb79b001a4d7c6aa2
   46 0.347979  172.16.10.179        239.255.255.250  SSDP      216 M-SEARCH * HTTP/1.1
   47 0.363450  172.16.11.228        172.16.9.229     TCP        66 53541 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
   48 0.370175  172.16.8.176         239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
   49 0.401971  172.16.9.47          239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
   50 0.402240  172.16.8.8           239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
   52 0.469497  172.16.8.190         239.255.255.250  SSDP      217 M-SEARCH * HTTP/1.1
```

```
> Frame 1: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7}, i
> Ethernet II, Src: MicroStarINT_c5:cb:cf (d8:bb:c1:c5:cb:cf), Dst: IPv4mcast_fb (01:00:5e:00:00:fb)
> Internet Protocol Version 4, Src: 172.16.10.52, Dst: 224.0.0.251
> User Datagram Protocol, Src Port: 5353, Dst Port: 5353
> Multicast Domain Name System (query)
```

```
0000  01 00 5e 00 00 fb d8 bb  c1 c5 cb cf 08 00 45 00   ··^····· ······E·
0010  00 38 e5 68 00 00 01 11  3d 0d ac 10 0a 34 e0 00   ·8·h···· =····4··
0020  00 fb 14 e9 14 e9 00 24  29 e2 00 00 00 00 00 01   ·······$ )·······
0030  00 00 00 00 00 00 04 77  70 61 64 05 6c 6f 63 61   ·······w pad·loca
0040  6c 00 00 01 00 01                                  l·····
```

User Datagram Protocol: Protocol | Packets: 8233 · Displayed: 6206 (75.4%) · Dropped: 0 (0.0%) | Profile: Default

Flow Graph output



Time	172.16.11.170		23.223.244.139	74.125.200.109		172.16.9.48	Comment
0.704661	64281	PSH, ACK - Len: 2587 →	443				Seq = 1 Ack = 1
0.704844	64281	PSH, ACK - Len: 1729 →	443				Seq = 2588 Ack = 1
0.704917	64281	PSH, ACK - Len: 31 →	443				Seq = 4317 Ack = 1
0.707303	64281	← ACK	443				Seq = 1 Ack = 2588
0.709143	64281	← ACK	443				Seq = 1 Ack = 4317
0.751346	64281	← ACK	443				Seq = 1 Ack = 4348
0.857880	64281	← PSH, ACK - Len: 340	443				Seq = 1 Ack = 4348
0.857880	64281	← PSH, ACK - Len: 31	443				Seq = 341 Ack = 4348
0.857970	64281	ACK →	443				Seq = 4348 Ack = 372
0.983213				993	FIN, ACK →	51436	Seq = 1 Ack = 1
2.357274	64281	PSH, ACK - Len: 2649 →	443				Seq = 4348 Ack = 372
2.357337	64281	PSH, ACK - Len: 3549 →	443				Seq = 6997 Ack = 372
2.357357	64281	PSH, ACK - Len: 31 →	443				Seq = 10546 Ack = 372
2.358836	64281	← ACK	443				Seq = 372 Ack = 5808
2.359838	64281	← ACK	443				Seq = 372 Ack = 6997
2.361109	64281	← ACK	443				Seq = 372 Ack = 8457
2.362397	64281	← ACK	443				Seq = 372 Ack = 9917
2.362893	64281	← ACK	443				Seq = 372 Ack = 10546
2.362893	64281	← ACK	443				Seq = 372 Ack = 10577
2.519936	64281	← PSH, ACK - Len: 340	443				Seq = 372 Ack = 10577
2.519936	64281	← PSH, ACK - Len: 31	443				Seq = 712 Ack = 10577
2.520028	64281	ACK →	443				Seq = 10577 Ack = 743

Packet 194: Seq = 372 Ack = 6997

Flow type: TCP Flows

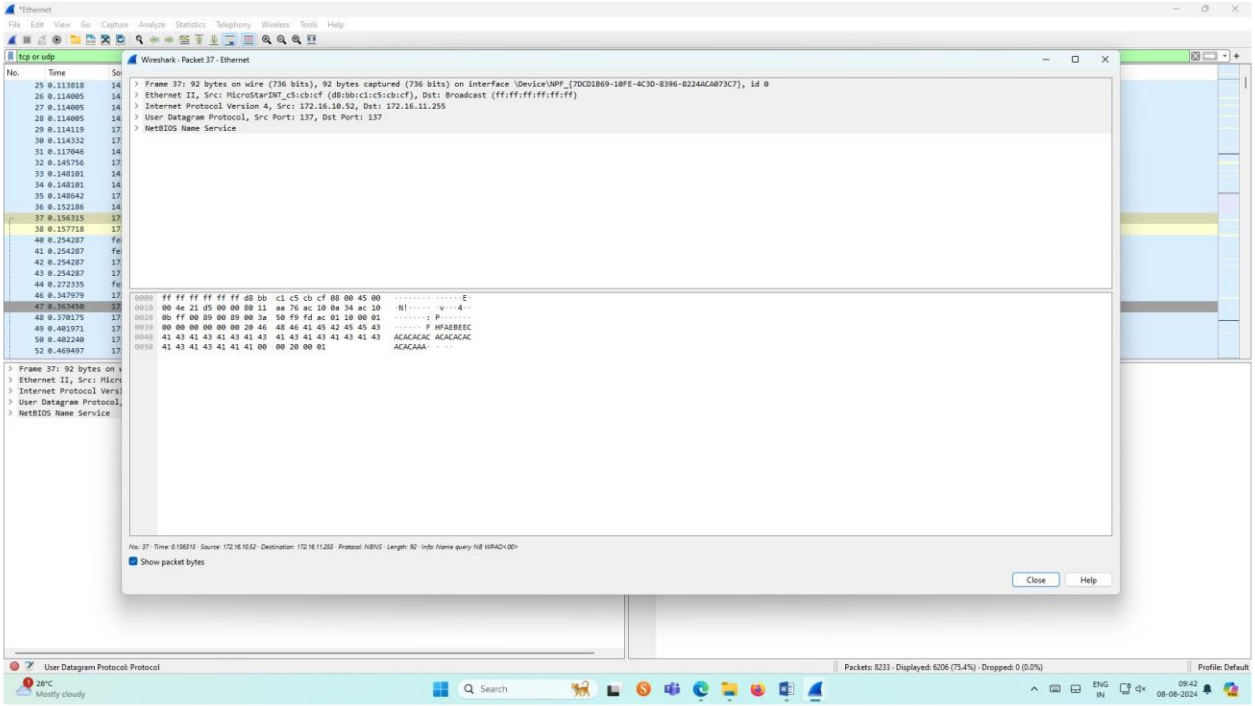
Addresses: Any

Transmission Control Protocol: Protocol

Packets: 309 · Displayed: 22 (7.1%)

Profile: Default

Inspecting the packets



tcp or udp

```
No.   Time
   25 0.113818
   26 0.114005
   27 0.114005
   28 0.114005
   29 0.114119
   30 0.114332
   31 0.117046
   32 0.145756
   33 0.148101
   34 0.148101
   35 0.148642
   36 0.152186
   37 0.156315
   38 0.157718
   40 0.254287
   41 0.254287
   42 0.254287
   43 0.254287
   44 0.272335
   46 0.347979
   47 0.363450
   48 0.370175
   49 0.401971
   50 0.402240
   52 0.469497
```

```
> Frame 37: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7}, id 0
> Ethernet II, Src: MicroStarINT_c5:cb:cf (d8:bb:c1:c5:cb:cf), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 172.16.10.52, Dst: 172.16.11.255
> User Datagram Protocol, Src Port: 137, Dst Port: 137
> NetBIOS Name Service
```

```
0000  ff ff ff ff ff ff d8 bb  c1 c5 cb cf 08 00 45 00   ········ ······E·
0010  00 4e 21 d5 00 00 80 11  aa 76 ac 10 0a 34 ac 10   ·N!····· ·v···4··
0020  0b ff 00 89 00 89 00 3a  50 f9 fd ac 01 10 00 01   ·······: P·······
0030  00 00 00 00 00 00 20 46  48 46 41 45 42 45 45 43   ······ F HFAEBEEC
0040  41 43 41 43 41 43 41 43  41 43 41 43 41 43 41 43   ACACACAC ACACACAC
0050  41 43 41 43 41 41 41 00  00 20 00 01               ACACAAA· · ··
```

No.: 37 · Time: 0.156315 · Source: 172.16.10.52 · Destination: 172.16.11.255 · Protocol: NBNS · Length: 92 · Info: Name query NB WPAD<00>

☑ Show packet bytes

User Datagram Protocol: Protocol

Packets: 8233 · Displayed: 6206 (75.4%) · Dropped: 0 (0.0%)

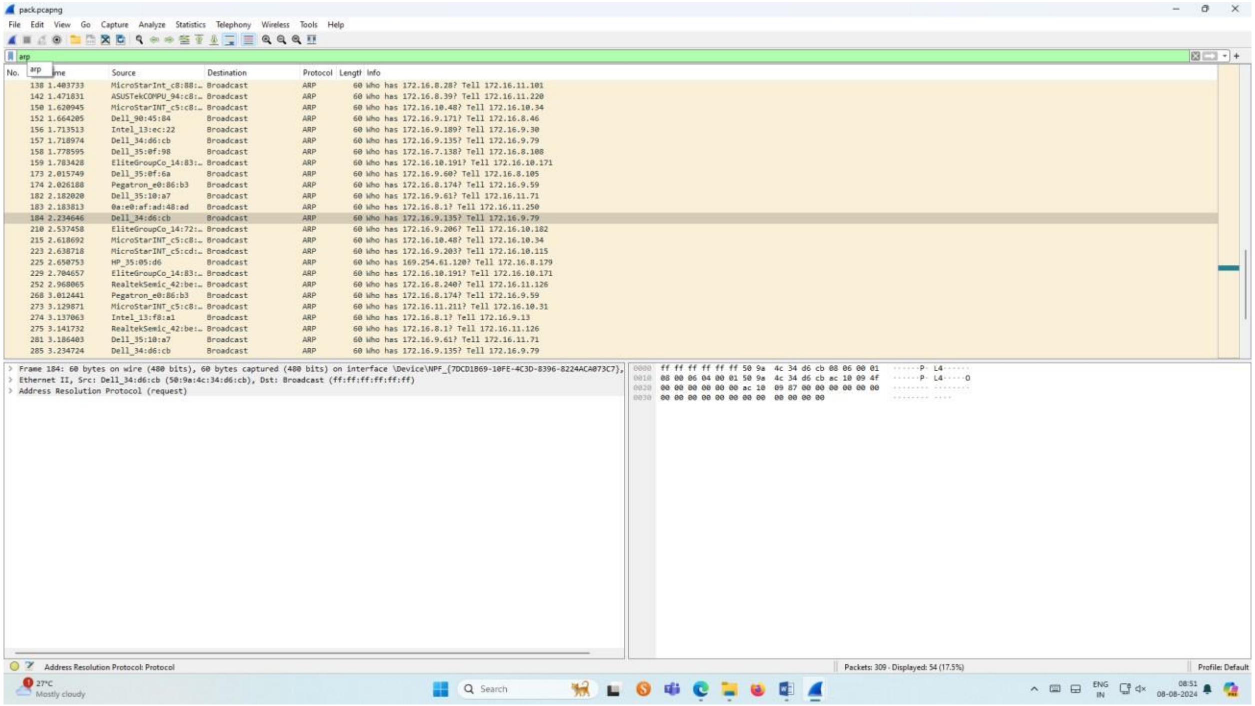
Profile: Default

3.Create a Filter to display only ARP packets and inspect the packets.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ⚇option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ARP packets in search bar.
- Save the packets.

Output


pack.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp

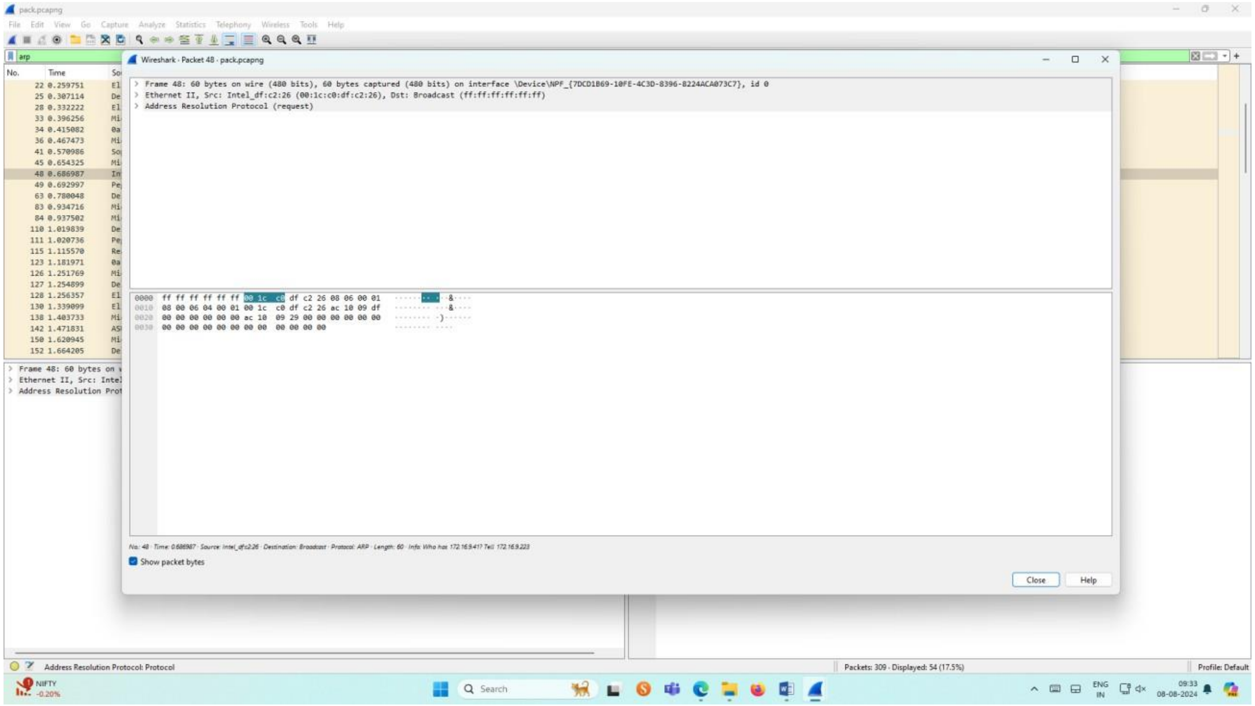
```
No.   arp me      Source               Destination   Protocol Lengtł Info
   138 1.403733   MicroStarInt_c8:88:… Broadcast     ARP        60 Who has 172.16.8.28? Tell 172.16.11.101
   142 1.471831   ASUSTekCOMPU_94:c8:… Broadcast     ARP        60 Who has 172.16.8.39? Tell 172.16.11.220
   150 1.620945   MicroStarINT_c5:c8:… Broadcast     ARP        60 Who has 172.16.10.48? Tell 172.16.10.34
   152 1.664205   Dell_90:45:84        Broadcast     ARP        60 Who has 172.16.9.171? Tell 172.16.8.46
   156 1.713513   Intel_13:ec:22       Broadcast     ARP        60 Who has 172.16.9.189? Tell 172.16.9.30
   157 1.718974   Dell_34:d6:cb        Broadcast     ARP        60 Who has 172.16.9.135? Tell 172.16.9.79
   158 1.778595   Dell_35:0f:98        Broadcast     ARP        60 Who has 172.16.7.138? Tell 172.16.8.108
   159 1.783428   EliteGroupCo_14:83:… Broadcast     ARP        60 Who has 172.16.10.191? Tell 172.16.10.171
   173 2.015749   Dell_35:0f:6a        Broadcast     ARP        60 Who has 172.16.9.60? Tell 172.16.8.105
   174 2.026188   Pegatron_e0:86:b3    Broadcast     ARP        60 Who has 172.16.8.174? Tell 172.16.9.59
   182 2.182020   Dell_35:10:a7        Broadcast     ARP        60 Who has 172.16.9.61? Tell 172.16.11.71
   183 2.183813   0a:e0:af:ad:48:ad    Broadcast     ARP        60 Who has 172.16.8.1? Tell 172.16.11.250
   184 2.234646   Dell_34:d6:cb        Broadcast     ARP        60 Who has 172.16.9.135? Tell 172.16.9.79
   210 2.537458   EliteGroupCo_14:72:… Broadcast     ARP        60 Who has 172.16.9.206? Tell 172.16.10.182
   215 2.618692   MicroStarINT_c5:c8:… Broadcast     ARP        60 Who has 172.16.10.48? Tell 172.16.10.34
   223 2.638718   MicroStarINT_c5:cd:… Broadcast     ARP        60 Who has 172.16.9.203? Tell 172.16.10.115
   225 2.650753   HP_35:05:d6          Broadcast     ARP        60 Who has 169.254.61.120? Tell 172.16.8.179
   229 2.704657   EliteGroupCo_14:83:… Broadcast     ARP        60 Who has 172.16.10.191? Tell 172.16.10.171
   252 2.968065   RealtekSemic_42:be:… Broadcast     ARP        60 Who has 172.16.8.240? Tell 172.16.11.126
   268 3.012441   Pegatron_e0:86:b3    Broadcast     ARP        60 Who has 172.16.8.174? Tell 172.16.9.59
   273 3.129871   MicroStarINT_c5:c8:… Broadcast     ARP        60 Who has 172.16.11.211? Tell 172.16.10.31
   274 3.137063   Intel_13:f8:a1       Broadcast     ARP        60 Who has 172.16.8.1? Tell 172.16.9.13
   275 3.141732   RealtekSemic_42:be:… Broadcast     ARP        60 Who has 172.16.8.1? Tell 172.16.11.126
   281 3.186403   Dell_35:10:a7        Broadcast     ARP        60 Who has 172.16.9.61? Tell 172.16.11.71
   285 3.234724   Dell_34:d6:cb        Broadcast     ARP        60 Who has 172.16.9.135? Tell 172.16.9.79
```

```
> Frame 184: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DCD1869-10FE-4C3D-8396-8224ACA073C7},
> Ethernet II, Src: Dell_34:d6:cb (50:9a:4c:34:d6:cb), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 50 9a  4c 34 d6 cb 08 06 00 01   ······P· L4······
0010  08 00 06 04 00 01 50 9a  4c 34 d6 cb ac 10 09 4f   ······P· L4·····O
0020  00 00 00 00 00 00 ac 10  09 87 00 00 00 00 00 00   ········ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

```
Address Resolution Protocol: Protocol        Packets: 309 · Displayed: 54 (17.5%)        Profile: Default
```

Inspecting the packets



pack.pcapng — filter: arp

```
No.   Time       So
  22 0.259751   El
  25 0.307114   De
  28 0.332222   El
  33 0.396256   Mi
  34 0.415082   0a
  36 0.467473   Mi
  41 0.570986   So
  45 0.654325   Mi
  48 0.686987   In
  49 0.692997   Pe
  63 0.780048   De
  83 0.934716   Mi
  84 0.937502   Mi
 110 1.019839   De
 111 1.020736   Pe
 115 1.115570   Re
 123 1.181971   0a
 126 1.251769   Mi
 127 1.254899   De
 128 1.256357   El
 130 1.339099   El
 138 1.403733   Mi
 142 1.471831   AS
 150 1.620945   Mi
 152 1.664205   De
```

Wireshark · Packet 48 · pack.pcapng

```
> Frame 48: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7}, id 0
> Ethernet II, Src: Intel_df:c2:26 (00:1c:c0:df:c2:26), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 1c  c0 df c2 26 08 06 00 01   ·········· &····
0010  08 00 06 04 00 01 00 1c  c0 df c2 26 ac 10 09 df   ·········· &····
0020  00 00 00 00 00 00 ac 10  09 29 00 00 00 00 00 00   ·········)······
0030  00 00 00 00 00 00 00 00  00 00 00 00               ············
```

No.: 48 · Time: 0.686987 · Source: Intel_df:c2:26 · Destination: Broadcast · Protocol: ARP · Length: 60 · Info: Who has 172.16.9.41? Tell 172.16.9.223

☑ Show packet bytes

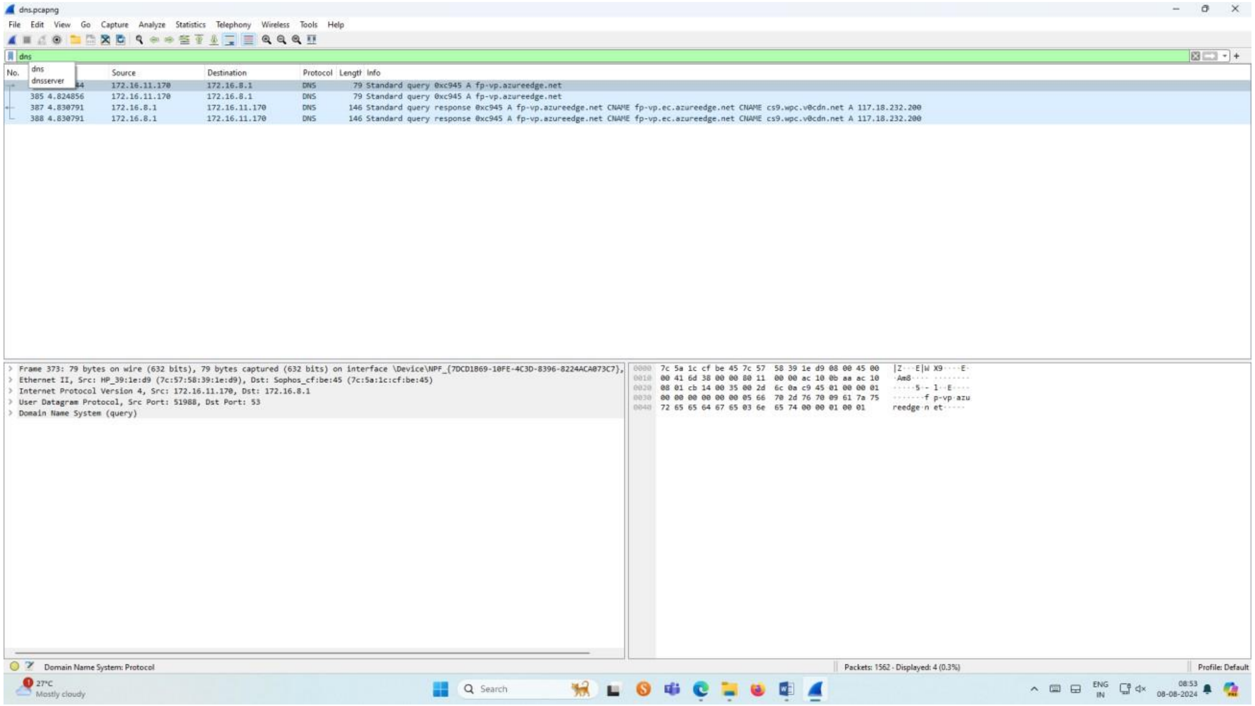
Address Resolution Protocol: Protocol — Packets: 309 · Displayed: 54 (17.5%) — Profile: Default

4.Create a Filter to display only DNS packets and provide the flow graph.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ⚇option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics⚇Flow graph.
- Save the packets.

Output


dns.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dnsserver

dns

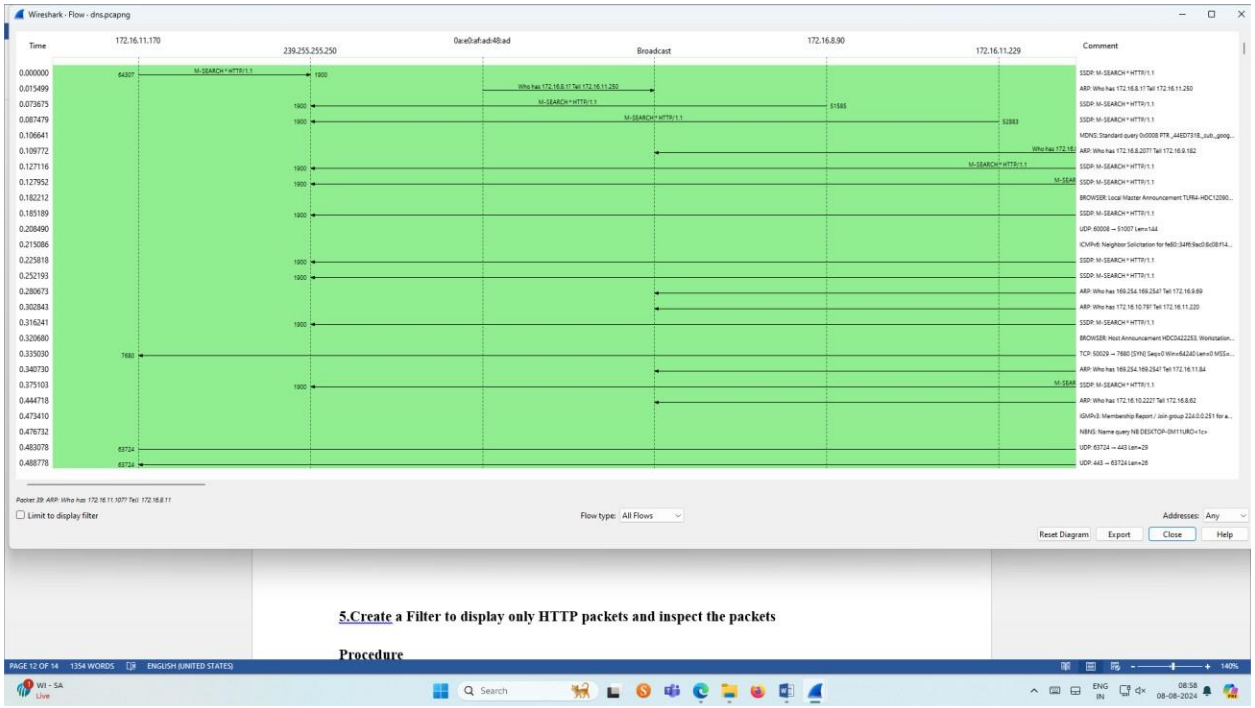
```
No.  Time      Source          Destination     Protocol Length Info
     ...44     172.16.11.170   172.16.8.1      DNS      79 Standard query 0xc945 A fp-vp.azureedge.net
 385 4.824856  172.16.11.170   172.16.8.1      DNS      79 Standard query 0xc945 A fp-vp.azureedge.net
 387 4.830791  172.16.8.1      172.16.11.170   DNS     146 Standard query response 0xc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.wpc.v0cdn.net A 117.18.232.200
 388 4.830791  172.16.8.1      172.16.11.170   DNS     146 Standard query response 0xc945 A fp-vp.azureedge.net CNAME fp-vp.ec.azureedge.net CNAME cs9.wpc.v0cdn.net A 117.18.232.200
```

```
> Frame 373: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF_{7DCD1869-10FE-4C3D-8396-8224ACA073C7},
> Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
> Internet Protocol Version 4, Src: 172.16.11.170, Dst: 172.16.8.1
> User Datagram Protocol, Src Port: 51988, Dst Port: 53
> Domain Name System (query)
```

```
0000  7c 5a 1c cf be 45 7c 57  58 39 1e d9 08 00 45 00   |Z···E|W X9····E·
0010  00 41 6d 38 00 00 80 11  00 00 ac 10 0b aa ac 10   ·Am8···· ········
0020  08 01 cb 14 00 35 00 2d  6c 0a c9 45 01 00 00 01   ·····5·- l··E····
0030  00 00 00 00 00 00 05 66  70 2d 76 70 09 61 7a 75   ·······f p-vp·azu
0040  72 65 65 64 67 65 03 6e  65 74 00 00 01 00 01      reedge·n et·····
```

Domain Name System: Protocol | Packets: 1562 · Displayed: 4 (0.3%) | Profile: Default

Graph output



```
Time      Comment
0.000000  SSDP: M-SEARCH * HTTP/1.1
0.015499  ARP: Who has 172.16.8.1? Tell 172.16.11.250
0.073675  SSDP: M-SEARCH * HTTP/1.1
0.087479  SSDP: M-SEARCH * HTTP/1.1
0.106641  MDNS: Standard query 0x0008 PTR _44ED7318._sub._goog...
0.109772  ARP: Who has 172.16.8.207? Tell 172.16.9.182
0.127116  SSDP: M-SEARCH * HTTP/1.1
0.127952  SSDP: M-SEARCH * HTTP/1.1
0.182212  BROWSER: Local Master Announcement TLFR4-HDC12090...
0.185189  SSDP: M-SEARCH * HTTP/1.1
0.208490  UDP: 60008 → 51007 Len=144
0.215086  ICMPv6: Neighbor Solicitation for fe80::34f6:9ac0:6c08:f14...
0.225818  SSDP: M-SEARCH * HTTP/1.1
0.252193  SSDP: M-SEARCH * HTTP/1.1
0.280673  ARP: Who has 169.254.169.254? Tell 172.16.9.69
0.302843  ARP: Who has 172.16.10.79? Tell 172.16.11.220
0.316241  SSDP: M-SEARCH * HTTP/1.1
0.320680  BROWSER: Host Announcement HDC0422253, Workstation...
0.335030  TCP: 50029 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=...
0.340730  ARP: Who has 169.254.169.254? Tell 172.16.11.84
0.375103  SSDP: M-SEARCH * HTTP/1.1
0.444718  ARP: Who has 172.16.10.222? Tell 172.16.8.62
0.473410  IGMPv3: Membership Report / Join group 224.0.0.251 for a...
0.476732  NBNS: Name query NB DESKTOP-0M11URO<1c>
0.483078  UDP: 63724 → 443 Len=29
0.488778  UDP: 443 → 63724 Len=26
```

Packet 29: ARP: Who has 172.16.11.107? Tell 172.16.8.11

□ Limit to display filter   Flow type: All Flows   Addresses: Any

5.Create a Filter to display only HTTP packets and inspect the packets

Procedure

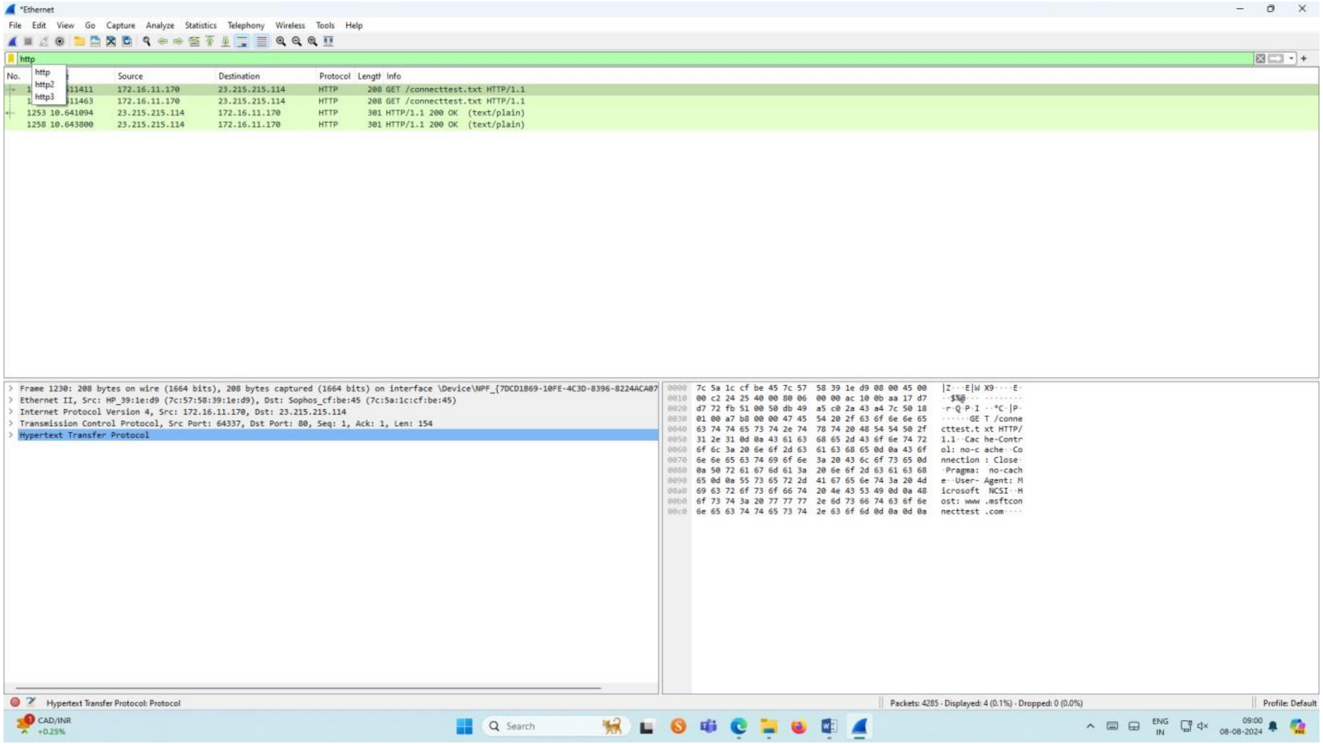
PAGE 12 OF 14 1354 WORDS ENGLISH (UNITED STATES)

5.Create a Filter to display only HTTP packets and inspect the packets

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ⚙option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search HTTP packets in the search bar.
- Save the packets.

Output


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
http2
http3
CAD/INR
+0.25%
Search
ENG
IN
09:00
08-08-2024

http

```
No.                 Source           Destination      Protocol Length Info
  1        11411    172.16.11.170    23.215.215.114   HTTP      208 GET /connecttest.txt HTTP/1.1
  1        11463    172.16.11.170    23.215.215.114   HTTP      208 GET /connecttest.txt HTTP/1.1
  1253 10.641094    23.215.215.114   172.16.11.170    HTTP      301 HTTP/1.1 200 OK  (text/plain)
  1258 10.643800    23.215.215.114   172.16.11.170    HTTP      301 HTTP/1.1 200 OK  (text/plain)
```

```
> Frame 1230: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA07
> Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
> Internet Protocol Version 4, Src: 172.16.11.170, Dst: 23.215.215.114
> Transmission Control Protocol, Src Port: 64337, Dst Port: 80, Seq: 1, Ack: 1, Len: 154
> Hypertext Transfer Protocol
```

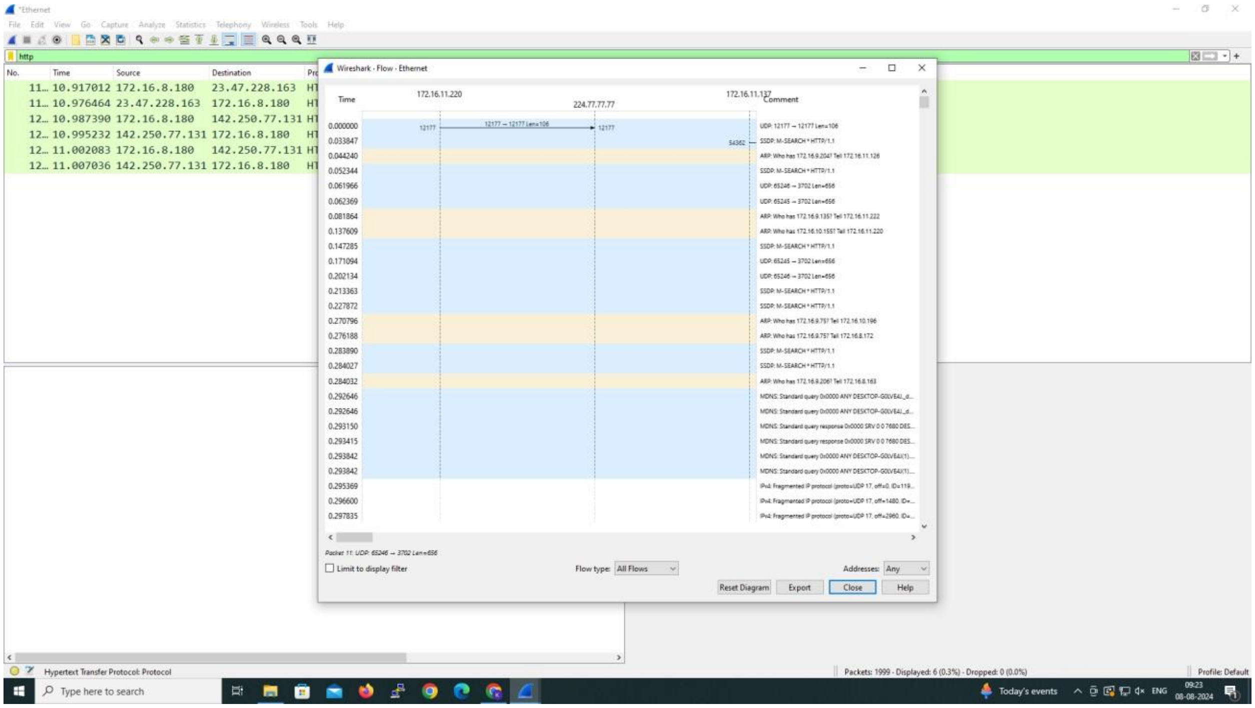
```
0000  7c 5a 1c cf be 45 7c 57  58 39 1e d9 08 00 45 00   |Z···E|W X9····E·
0010  00 c2 24 25 40 00 80 06  00 00 ac 10 0b aa 17 d7   ··$%@··· ········
0020  d7 72 fb 51 00 50 db 49  a5 c0 2a 43 a4 7c 50 18   ·r·Q·P·I ··*C·|P·
0030  01 00 a7 b8 00 00 47 45  54 20 2f 63 6f 6e 6e 65   ······GE T /conne
0040  63 74 74 65 73 74 2e 74  78 74 20 48 54 54 50 2f   cttest.t xt HTTP/
0050  31 2e 31 0d 0a 43 61 63  68 65 2d 43 6f 6e 74 72   1.1··Cac he-Contr
0060  6f 6c 3a 20 6e 6f 2d 63  61 63 68 65 0d 0a 43 6f   ol: no-c ache··Co
0070  6e 6e 65 63 74 69 6f 6e  3a 20 43 6c 6f 73 65 0d   nnection : Close·
0080  0a 50 72 61 67 6d 61 3a  20 6e 6f 2d 63 61 63 68   ·Pragma:  no-cach
0090  65 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   e··User- Agent: M
00a0  69 63 72 6f 73 6f 66 74  20 4e 43 53 49 0d 0a 48   icrosoft  NCSI··H
00b0  6f 73 74 3a 20 77 77 77  2e 6d 73 66 74 63 6f 6e   ost: www .msftcon
00c0  6e 65 63 74 74 65 73 74  2e 63 6f 6d 0d 0a 0d 0a   necttest .com····
```

Hypertext Transfer Protocol: Protocol

Packets: 4285 · Displayed: 4 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

Flow Graph output



```
http
No.  Time      Source         Destination
11… 10.917012 172.16.8.180   23.47.228.163  HT
11… 10.976464 23.47.228.163  172.16.8.180   HT
12… 10.987390 172.16.8.180   142.250.77.131 HT
12… 10.995232 142.250.77.131 172.16.8.180   HT
12… 11.002083 172.16.8.180   142.250.77.131 HT
12… 11.007036 142.250.77.131 172.16.8.180   HT
```

Wireshark · Flow · Ethernet

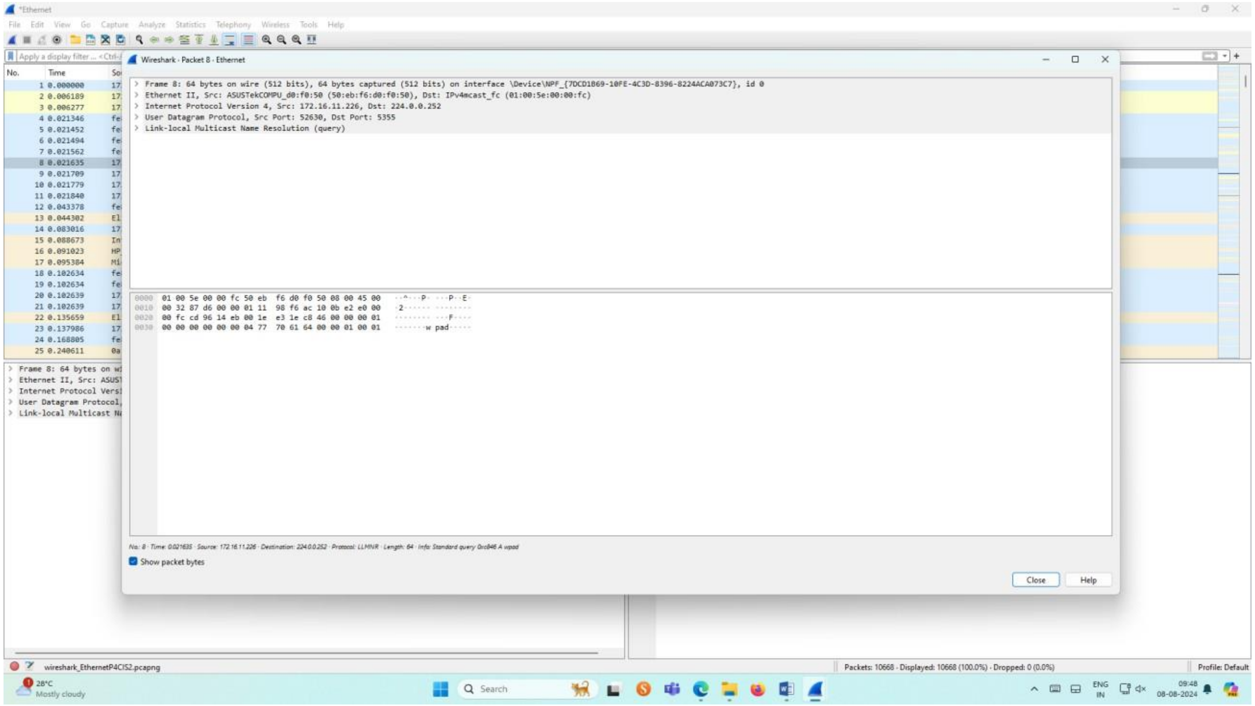
```
Time      172.16.11.220   224.77.77.77   172.16.11.137   Comment
0.000000  12177 —— 12177 → 12177 Len=106 —→ 12177        UDP: 12177 → 12177 Len=106
0.033847                                 54362 —         SSDP: M-SEARCH * HTTP/1.1
0.044240                                                 ARP: Who has 172.16.9.204? Tell 172.16.11.126
0.052344                                                 SSDP: M-SEARCH * HTTP/1.1
0.061966                                                 UDP: 65246 → 3702 Len=656
0.062369                                                 UDP: 65245 → 3702 Len=656
0.081864                                                 ARP: Who has 172.16.9.135? Tell 172.16.11.222
0.137609                                                 ARP: Who has 172.16.10.155? Tell 172.16.11.220
0.147285                                                 SSDP: M-SEARCH * HTTP/1.1
0.171094                                                 UDP: 65245 → 3702 Len=656
0.202134                                                 UDP: 65246 → 3702 Len=656
0.213363                                                 SSDP: M-SEARCH * HTTP/1.1
0.227872                                                 SSDP: M-SEARCH * HTTP/1.1
0.270796                                                 ARP: Who has 172.16.9.75? Tell 172.16.10.196
0.276188                                                 ARP: Who has 172.16.9.75? Tell 172.16.8.172
0.283890                                                 SSDP: M-SEARCH * HTTP/1.1
0.284027                                                 SSDP: M-SEARCH * HTTP/1.1
0.284032                                                 ARP: Who has 172.16.9.206? Tell 172.16.8.163
0.292646                                                 MDNS: Standard query 0x0000 ANY DESKTOP-G0LVE4I._d…
0.292646                                                 MDNS: Standard query 0x0000 ANY DESKTOP-G0LVE4I._d…
0.293150                                                 MDNS: Standard query response 0x0000 SRV 0 0 7680 DES…
0.293415                                                 MDNS: Standard query response 0x0000 SRV 0 0 7680 DES…
0.293842                                                 MDNS: Standard query 0x0000 ANY DESKTOP-G0LVE4I(1)…
0.293842                                                 MDNS: Standard query 0x0000 ANY DESKTOP-G0LVE4I(1)…
0.295369                                                 IPv4: Fragmented IP protocol (proto=UDP 17, off=0, ID=119…
0.296600                                                 IPv4: Fragmented IP protocol (proto=UDP 17, off=1480, ID=…
0.297835                                                 IPv4: Fragmented IP protocol (proto=UDP 17, off=2960, ID=…

Packet 11: UDP: 65246 → 3702 Len=656
```

☐ Limit to display filter   Flow type: All Flows   Addresses: Any

Hypertext Transfer Protocol: Protocol   Packets: 1999 · Displayed: 6 (0.3%) · Dropped: 0 (0.0%)   Profile: Default

Inspecting the packets



```
No.  Time
 1 0.000000   17
 2 0.006189   17
 3 0.006277   17
 4 0.021346   fe
 5 0.021452   fe
 6 0.021494   fe
 7 0.021562   fe
 8 0.021635   17
 9 0.021709   17
10 0.021779   17
11 0.021840   17
12 0.043378   fe
13 0.044302   El
14 0.083016   17
15 0.088673   In
16 0.091023   HP
17 0.095384   Mi
18 0.102634   fe
19 0.102634   fe
20 0.102639   17
21 0.102639   17
22 0.135659   El
23 0.137986   17
24 0.168805   fe
25 0.240611   0a
```

Wireshark · Packet 8 · Ethernet

```
> Frame 8: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7}, id 0
> Ethernet II, Src: ASUSTekCOMPU_d0:f0:50 (50:eb:f6:d0:f0:50), Dst: IPv4mcast_fc (01:00:5e:00:00:fc)
> Internet Protocol Version 4, Src: 172.16.11.226, Dst: 224.0.0.252
> User Datagram Protocol, Src Port: 52630, Dst Port: 5355
> Link-local Multicast Name Resolution (query)

0000  01 00 5e 00 00 fc 50 eb  f6 d0 f0 50 08 00 45 00   ··^···P· ··P··E·
0010  00 32 87 d6 00 00 01 11  98 f6 ac 10 0b e2 e0 00   ·2······ ········
0020  00 fc cd 96 14 eb 00 1e  e3 1e c8 46 00 00 00 01   ········ ···F····
0030  00 00 00 00 00 00 04 77  70 61 64 00 00 01 00 01   ·······w pad·····

No.: 8 · Time: 0.021635 · Source: 172.16.11.226 · Destination: 224.0.0.252 · Protocol: LLMNR · Length: 64 · Info: Standard query 0xc846 A wpad
```

☑ Show packet bytes

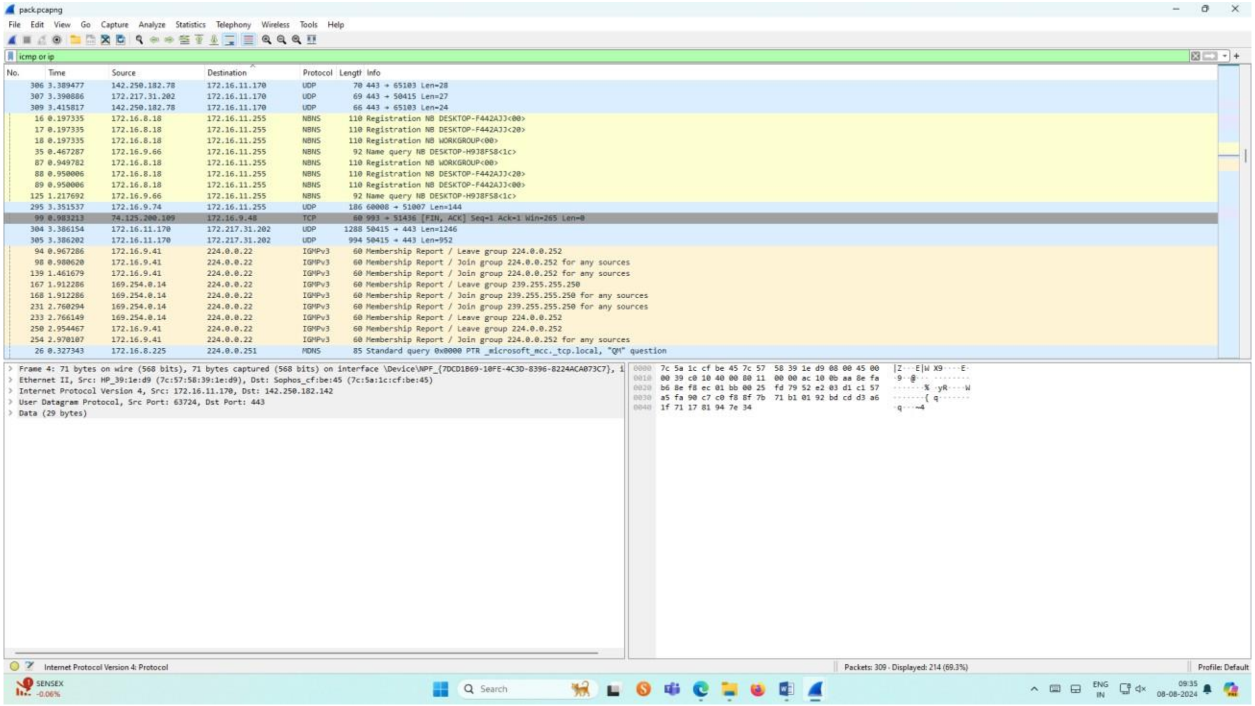
wireshark_EthernetP4CIS2.pcapng   Packets: 10668 · Displayed: 10668 (100.0%) · Dropped: 0 (0.0%)   Profile: Default

6.Create a Filter to display only IP/ICMP packets and inspect the packets.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ⚇option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search ICMP/IP packets in search bar.
- Save the packets

Output



pack.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp or ip

```
No.   Time      Source          Destination     Protocol Length Info
  306 3.389477  142.250.182.78  172.16.11.170   UDP        70 443 → 65103 Len=28
  307 3.390886  172.217.31.202  172.16.11.170   UDP        69 443 → 50415 Len=27
  309 3.415817  142.250.182.78  172.16.11.170   UDP        66 443 → 65103 Len=24
   16 0.197335  172.16.8.18     172.16.11.255   NBNS      110 Registration NB DESKTOP-F442AJJ<00>
   17 0.197335  172.16.8.18     172.16.11.255   NBNS      110 Registration NB DESKTOP-F442AJJ<20>
   18 0.197335  172.16.8.18     172.16.11.255   NBNS      110 Registration NB WORKGROUP<00>
   35 0.467287  172.16.9.66     172.16.11.255   NBNS       92 Name query NB DESKTOP-H9J8FS8<1c>
   87 0.949782  172.16.8.18     172.16.11.255   NBNS      110 Registration NB WORKGROUP<00>
   88 0.950006  172.16.8.18     172.16.11.255   NBNS      110 Registration NB DESKTOP-F442AJJ<20>
   89 0.950006  172.16.8.18     172.16.11.255   NBNS      110 Registration NB DESKTOP-F442AJJ<00>
  125 1.217692  172.16.9.66     172.16.11.255   NBNS       92 Name query NB DESKTOP-H9J8FS8<1c>
  295 3.351537  172.16.9.74     172.16.11.255   UDP       186 60008 → 51007 Len=144
   99 0.983213  74.125.200.109  172.16.9.48     TCP        60 993 → 51436 [FIN, ACK] Seq=1 Ack=1 Win=265 Len=0
  304 3.386154  172.16.11.170   172.217.31.202  UDP      1288 50415 → 443 Len=1246
  305 3.386202  172.16.11.170   172.217.31.202  UDP       994 50415 → 443 Len=952
   94 0.967286  172.16.9.41     224.0.0.22      IGMPv3     60 Membership Report / Leave group 224.0.0.252
   98 0.980620  172.16.9.41     224.0.0.22      IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
  139 1.461679  172.16.9.41     224.0.0.22      IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
  167 1.912286  169.254.0.14    224.0.0.22      IGMPv3     60 Membership Report / Leave group 239.255.255.250
  168 1.912286  169.254.0.14    224.0.0.22      IGMPv3     60 Membership Report / Join group 239.255.255.250 for any sources
  231 2.760294  169.254.0.14    224.0.0.22      IGMPv3     60 Membership Report / Join group 239.255.255.250 for any sources
  233 2.766149  169.254.0.14    224.0.0.22      IGMPv3     60 Membership Report / Leave group 224.0.0.252
  250 2.954467  172.16.9.41     224.0.0.22      IGMPv3     60 Membership Report / Leave group 224.0.0.252
  254 2.970107  172.16.9.41     224.0.0.22      IGMPv3     60 Membership Report / Join group 224.0.0.252 for any sources
   26 0.327343  172.16.8.225    224.0.0.251     MDNS       85 Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
```

```
> Frame 4: 71 bytes on wire (568 bits), 71 bytes captured (568 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7}, i
> Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
> Internet Protocol Version 4, Src: 172.16.11.170, Dst: 142.250.182.142
> User Datagram Protocol, Src Port: 63724, Dst Port: 443
> Data (29 bytes)
```

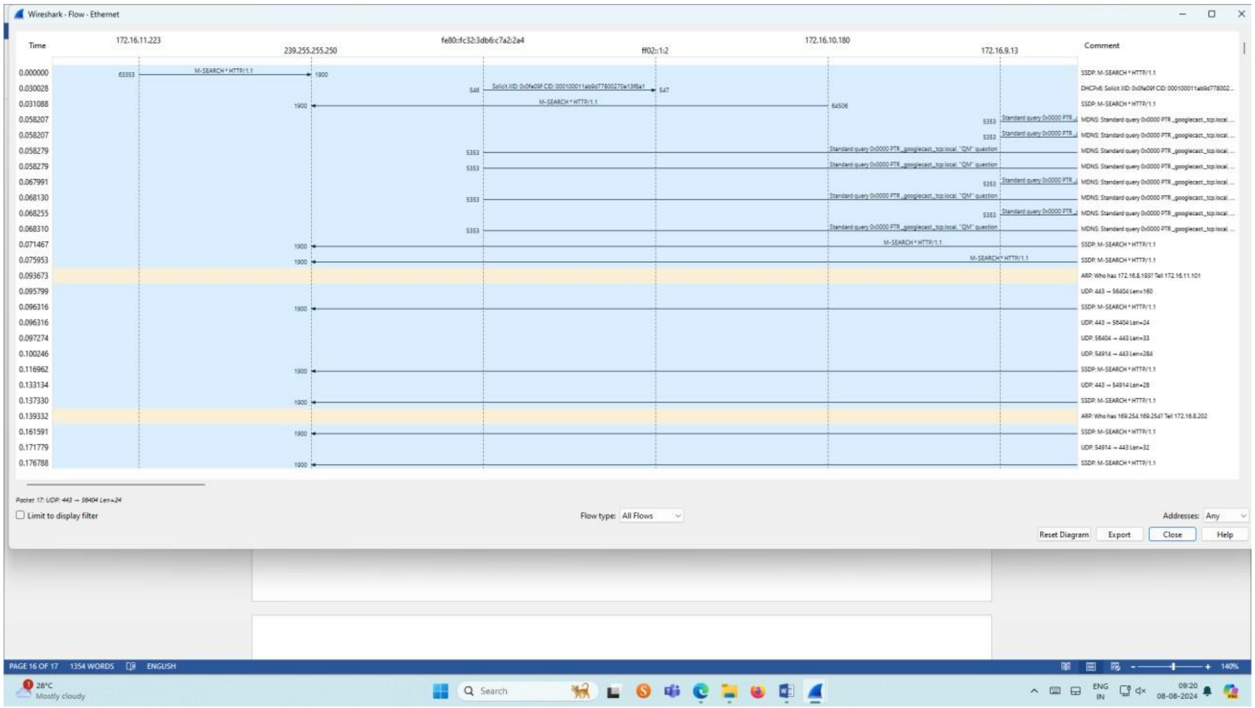
```
0000  7c 5a 1c cf be 45 7c 57  58 39 1e d9 08 00 45 00   |Z···E|W X9····E·
0010  00 39 c0 10 40 00 80 11  00 00 ac 10 0b aa 8e fa   ·9··@··· ········
0020  b6 8e f8 ec 01 bb 00 25  fd 79 52 e2 03 d1 c1 57   ·······% ·yR····W
0030  a5 fa 90 c7 c0 f8 8f 7b  71 b1 01 92 bd cd d3 a6   ·······{ q·······
0040  1f 71 17 81 94 7e 34                               ·q···~4
```

Internet Protocol Version 4: Protocol

Packets: 309 · Displayed: 214 (69.3%)

Profile: Default

Flow Graph output



Wireshark · Flow · Ethernet

```
Time      172.16.11.223  239.255.255.250  fe80::fc32:3db6:c7a2:2a4  ff02::1:2  172.16.10.180  172.16.9.13   Comment
0.000000  SSDP: M-SEARCH * HTTP/1.1
0.030028  DHCPv6: Solicit XID: 0x0fe09f CID: 000100011ab9d778002...
0.031088  SSDP: M-SEARCH * HTTP/1.1
0.058207  MDNS: Standard query 0x0000 PTR _googlecast._tcp.local, ...
0.058207  MDNS: Standard query 0x0000 PTR _googlecast._tcp.local, ...
0.058279  MDNS: Standard query 0x0000 PTR _googlecast._tcp.local, ...
0.058279  MDNS: Standard query 0x0000 PTR _googlecast._tcp.local, ...
0.067991  MDNS: Standard query 0x0000 PTR _googlecast._tcp.local, ...
0.068130  MDNS: Standard query 0x0000 PTR _googlecast._tcp.local, ...
0.068255  MDNS: Standard query 0x0000 PTR _googlecast._tcp.local, ...
0.068310  MDNS: Standard query 0x0000 PTR _googlecast._tcp.local, ...
0.071467  SSDP: M-SEARCH * HTTP/1.1
0.075953  SSDP: M-SEARCH * HTTP/1.1
0.093673  ARP: Who has 172.16.8.193? Tell 172.16.11.101
0.095799  UDP: 443 → 56404 Len=160
0.096316  SSDP: M-SEARCH * HTTP/1.1
0.096316  UDP: 443 → 56404 Len=24
0.097274  UDP: 56404 → 443 Len=33
0.100246  UDP: 54914 → 443 Len=284
0.116962  SSDP: M-SEARCH * HTTP/1.1
0.133134  UDP: 443 → 54914 Len=28
0.137330  SSDP: M-SEARCH * HTTP/1.1
0.139332  ARP: Who has 169.254.169.254? Tell 172.16.8.202
0.161591  SSDP: M-SEARCH * HTTP/1.1
0.171779  UDP: 54914 → 443 Len=32
0.176788  SSDP: M-SEARCH * HTTP/1.1
```

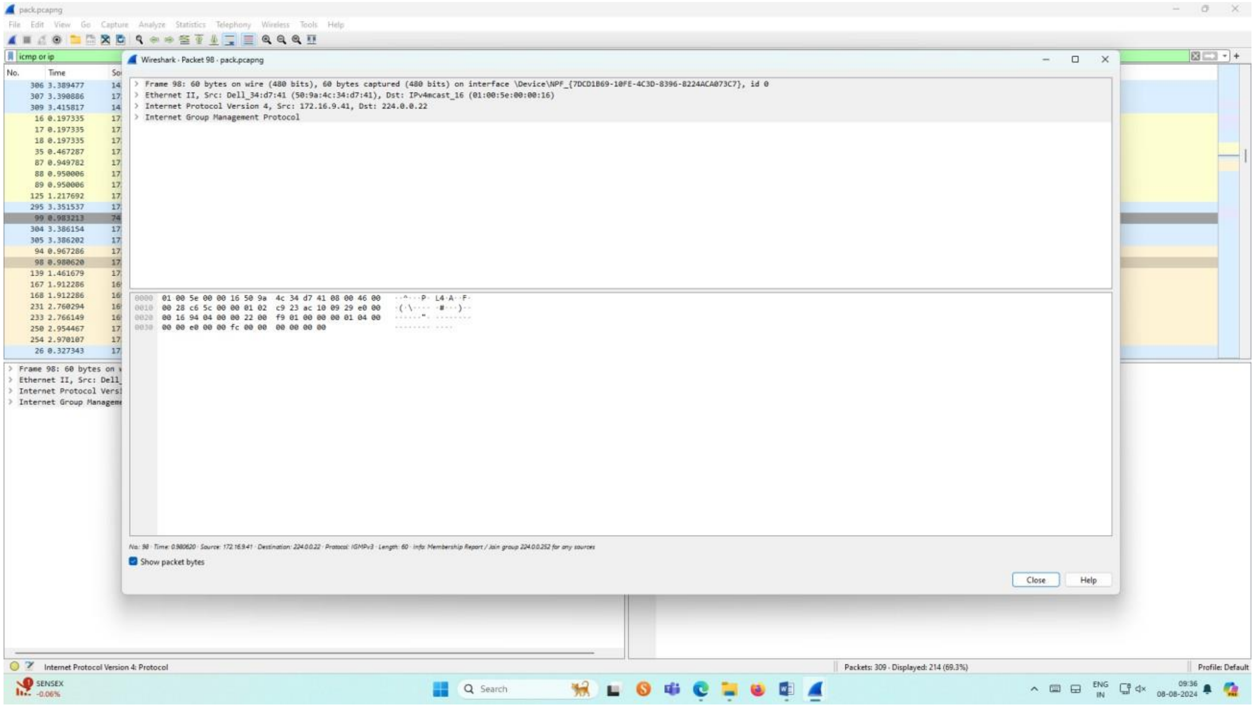
Packet 17: UDP: 443 → 56404 Len=24

☐ Limit to display filter

Flow type: All Flows

Addresses: Any

Inspecting the packets



pack.pcapng

icmp or ip

```
No.  Time
306 3.389477
307 3.390886
309 3.415817
 16 0.197335
 17 0.197335
 18 0.197335
 35 0.467287
 87 0.949782
 88 0.950006
 89 0.950006
125 1.217692
295 3.351537
 99 0.983213
304 3.386154
305 3.386202
 94 0.967286
 98 0.980620
139 1.461679
167 1.912286
168 1.912286
231 2.760294
233 2.766149
250 2.954467
254 2.970107
 26 0.327343
```

Wireshark · Packet 98 · pack.pcapng

```
> Frame 98: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7}, id 0
> Ethernet II, Src: Dell_34:d7:41 (50:9a:4c:34:d7:41), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
> Internet Protocol Version 4, Src: 172.16.9.41, Dst: 224.0.0.22
> Internet Group Management Protocol
```

```
0000  01 00 5e 00 00 16 50 9a  4c 34 d7 41 08 00 46 00   ··^···P· L4·A··F·
0010  00 28 c6 5c 00 00 01 02  c9 23 ac 10 09 29 e0 00   ·(·\···· ·#···)··
0020  00 16 94 04 00 00 22 00  f9 01 00 00 00 01 04 00   ······"· ········
0030  00 00 e0 00 00 fc 00 00  00 00 00 00               ········ ····
```

No.: 98 · Time: 0.980620 · Source: 172.16.9.41 · Destination: 224.0.0.22 · Protocol: IGMPv3 · Length: 60 · Info: Membership Report / Join group 224.0.0.252 for any sources

☑ Show packet bytes

Internet Protocol Version 4: Protocol

Packets: 309 · Displayed: 214 (69.3%)

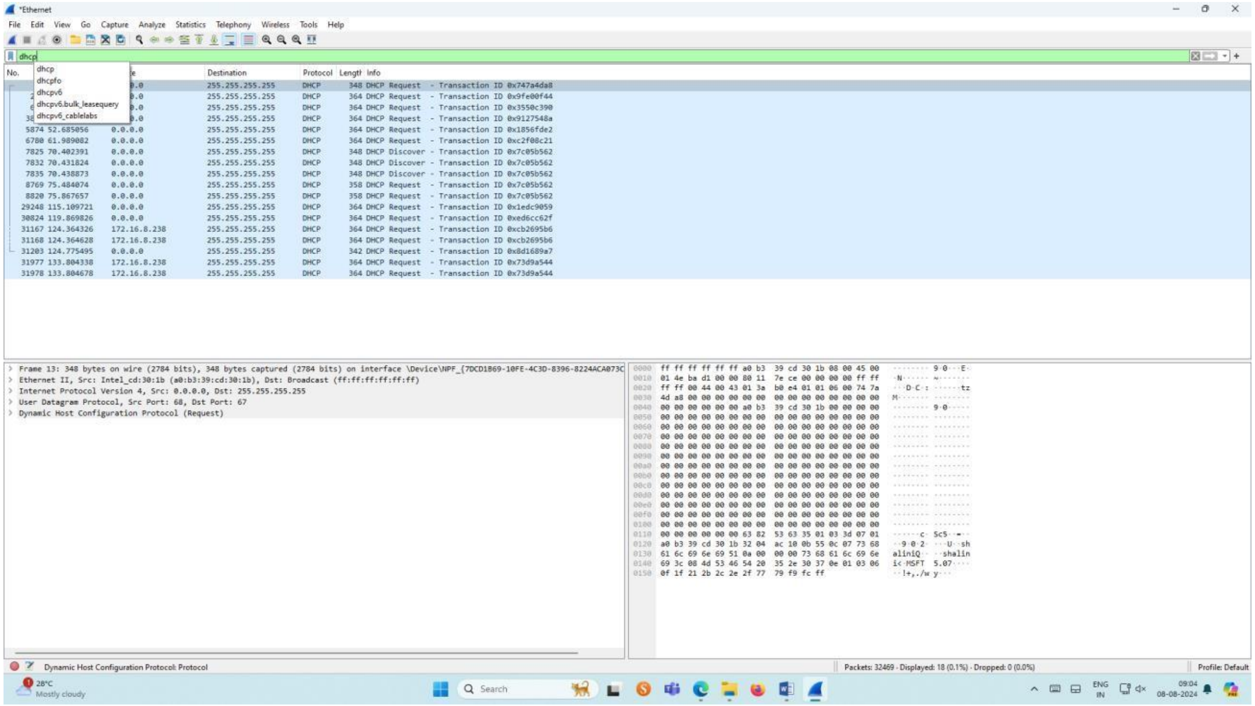
Profile: Default

7.Create a Filter to display only DHCP packets and inspect the packets.

Procedure

- Select Local Area Connection in Wireshark.
- Go to capture ⚇option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DHCP packets in search bar.
- Save the packets

Output



dhcp

```
No.                         Destination      Protocol Length Info
                       .0   255.255.255.255  DHCP     348 DHCP Request  - Transaction ID 0x747a4da8
   2                   .0   255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0x9fe00f44
   6                   .0   255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0x3550c390
  38                   .0   255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0x9127548a
  5874 52.685056   0.0.0.0      255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0x1856fde2
  6780 61.989082   0.0.0.0      255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0xc2f08c21
  7825 70.402391   0.0.0.0      255.255.255.255  DHCP     348 DHCP Discover - Transaction ID 0x7c05b562
  7832 70.431824   0.0.0.0      255.255.255.255  DHCP     348 DHCP Discover - Transaction ID 0x7c05b562
  7835 70.438873   0.0.0.0      255.255.255.255  DHCP     348 DHCP Discover - Transaction ID 0x7c05b562
  8769 75.484074   0.0.0.0      255.255.255.255  DHCP     358 DHCP Request  - Transaction ID 0x7c05b562
  8820 75.867657   0.0.0.0      255.255.255.255  DHCP     358 DHCP Request  - Transaction ID 0x7c05b562
 29248 115.109721  0.0.0.0      255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0x1edc9059
 30824 119.869826  0.0.0.0      255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0xed6cc62f
 31167 124.364326  172.16.8.238 255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0xcb2695b6
 31168 124.364628  172.16.8.238 255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0xcb2695b6
 31203 124.775495  0.0.0.0      255.255.255.255  DHCP     342 DHCP Request  - Transaction ID 0x8d1689a7
 31977 133.804338  172.16.8.238 255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0x73d9a544
 31978 133.804678  172.16.8.238 255.255.255.255  DHCP     364 DHCP Request  - Transaction ID 0x73d9a544
```

```
> Frame 13: 348 bytes on wire (2784 bits), 348 bytes captured (2784 bits) on interface \Device\NPF_{7DCD1869-10FE-4C3D-8396-8224ACA073C
> Ethernet II, Src: Intel_cd:30:1b (a0:b3:39:cd:30:1b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

```
0000  ff ff ff ff ff ff a0 b3  39 cd 30 1b 08 00 45 00   ········ 9·0···E·
0010  01 4e ba d1 00 00 80 11  7e ce 00 00 00 00 ff ff   ·N······ ~·······
0020  ff ff 00 44 00 43 01 3a  b0 e4 01 01 06 00 74 7a   ···D·C·: ······tz
0030  4d a8 00 00 00 00 00 00  00 00 00 00 00 00 00 00   M······· ········
0040  00 00 00 00 00 00 a0 b3  39 cd 30 1b 00 00 00 00   ········ 9·0·····
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  a0 b3 39 cd 30 1b 32 04  ac 10 0b 55 0c 07 73 68   ··9·0·2· ···U··sh
0130  61 6c 69 6e 69 51 0a 00  00 00 73 68 61 6c 69 6e   aliniQ·· ··shalin
0140  69 3c 08 4d 53 46 54 20  35 2e 30 37 0e 01 03 06   i<·MSFT  5.07····
0150  0f 1f 21 2b 2c 2e 2f 77  79 f9 fc ff               ··!+,./w y···
```

Dynamic Host Configuration Protocol: Protocol

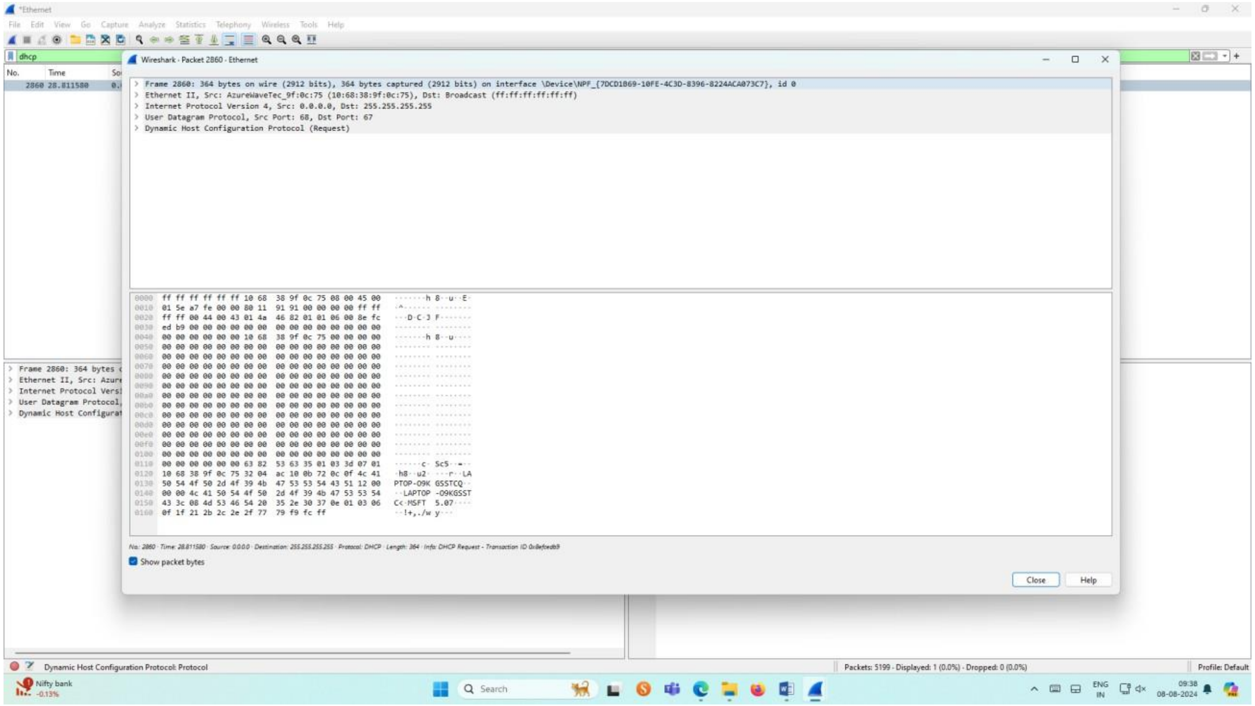
Packets: 32469 · Displayed: 18 (0.1%) · Dropped: 0 (0.0%)

Profile: Default

28°C
Mostly cloudy

09:04
08-08-2024

Inspecting the packets


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
No. Time So
2860 28.811580 0.
Wireshark · Packet 2860 · Ethernet
Close
Help
Search
Nifty bank
-0.13%
ENG
IN
09:38
08-08-2024

```
> Frame 2860: 364 bytes on wire (2912 bits), 364 bytes captured (2912 bits) on interface \Device\NPF_{7DCD1869-10FE-4C3D-8396-8224ACA073C7}, id 0
> Ethernet II, Src: AzureWaveTec_9f:0c:75 (10:68:38:9f:0c:75), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
> Dynamic Host Configuration Protocol (Request)
```

```
0000  ff ff ff ff ff ff 10 68  38 9f 0c 75 08 00 45 00   ······h 8··u··E·
0010  01 5e a7 fe 00 00 80 11  91 91 00 00 00 00 ff ff   ·^······ ········
0020  ff ff 00 44 00 43 01 4a  46 82 01 01 06 00 8e fc   ···D·C·J F·······
0030  ed b9 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········ ········
0040  00 00 00 00 00 00 10 68  38 9f 0c 75 00 00 00 00   ······h 8··u····
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  10 68 38 9f 0c 75 32 04  ac 10 0b 72 0c 0f 4c 41   ·h8··u2· ···r··LA
0130  50 54 4f 50 2d 4f 39 4b  47 53 53 54 43 51 12 00   PTOP-O9K GSSTCQ··
0140  00 00 4c 41 50 54 4f 50  2d 4f 39 4b 47 53 53 54   ··LAPTOP -O9KGSST
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···
```

No.: 2860 · Time: 28.811580 · Source: 0.0.0.0 · Destination: 255.255.255.255 · Protocol: DHCP · Length: 364 · Info: DHCP Request - Transaction ID 0x8efcedb9

☑ Show packet bytes

```
> Frame 2860: 364 bytes o
> Ethernet II, Src: Azure
> Internet Protocol Versi
> User Datagram Protocol,
> Dynamic Host Configurat
```

Dynamic Host Configuration Protocol: Protocol

Packets: 5199 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)

Profile: Default