Ex No: 4B ANALYSE NETWORK TRAFFIC USING WIRESHARK TOOL

DATE:8/8/24

AIM:

To capture, save, filter and analyze network traffic on TCP / UDP / IP / HTTP / ARP /DHCP /ICMP /DNS using Wireshark Tool

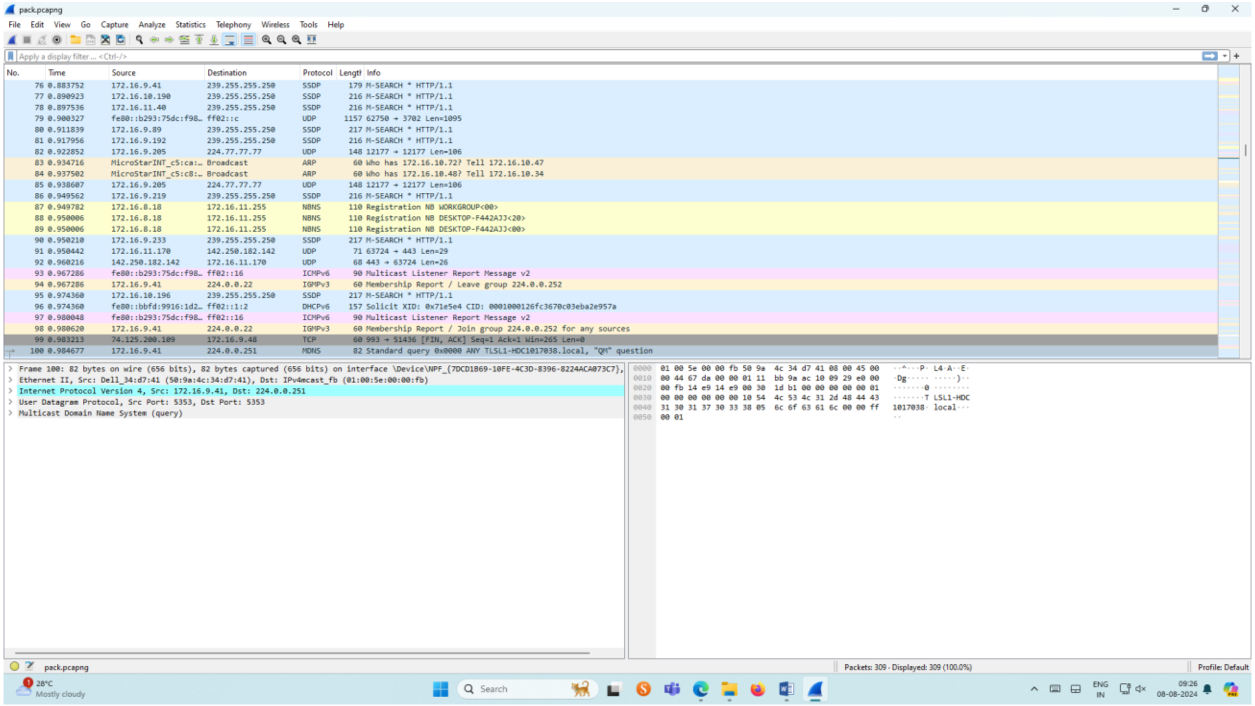
Exercises

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


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

```
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)
```

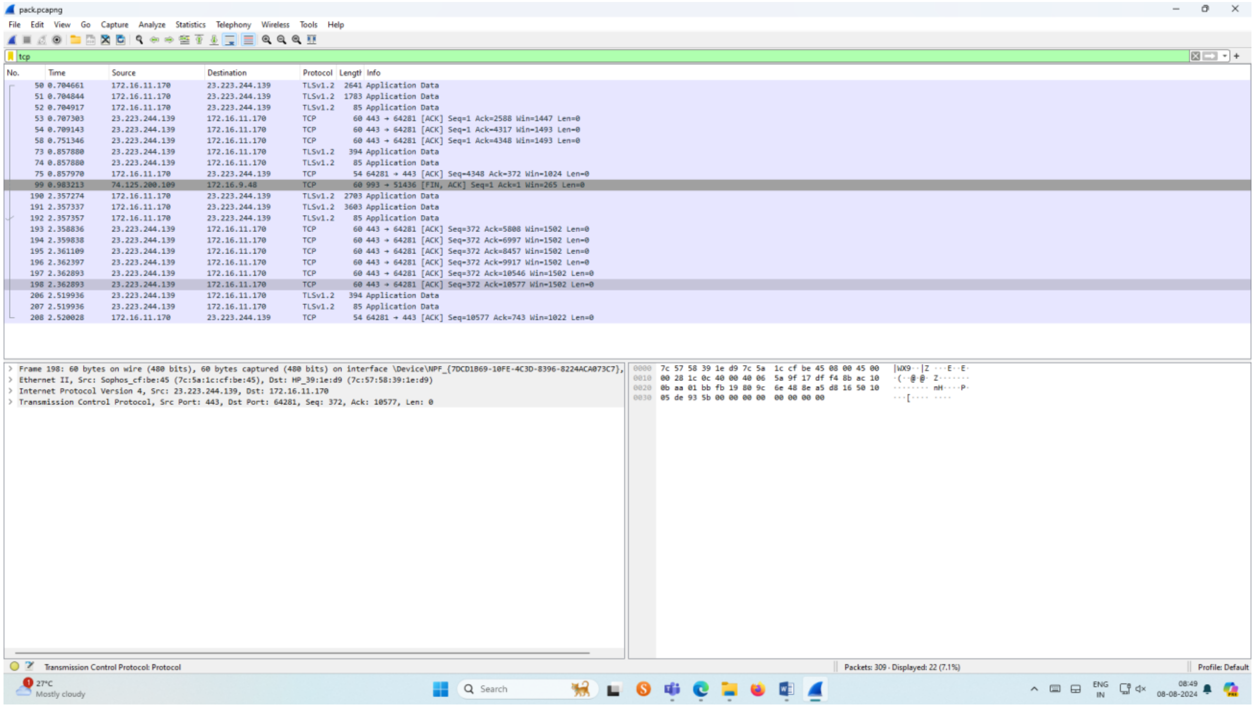
```
0000  01 00 5e 00 00 fb 50 9a  4c 34 d7 41 08 00 45 00   ··^···P· L4·A··E·
0010  00 44 67 da 00 00 01 11  bb 9a ac 10 09 29 e0 00   ·Dg····· ·····)··
0020  00 fb 14 e9 14 e9 00 30  1d b1 00 00 00 00 00 01   ·······0 ········
0030  00 00 00 00 00 00 10 54  4c 53 4c 31 2d 48 44 43   ·······T LSL1-HDC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

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

Procedure

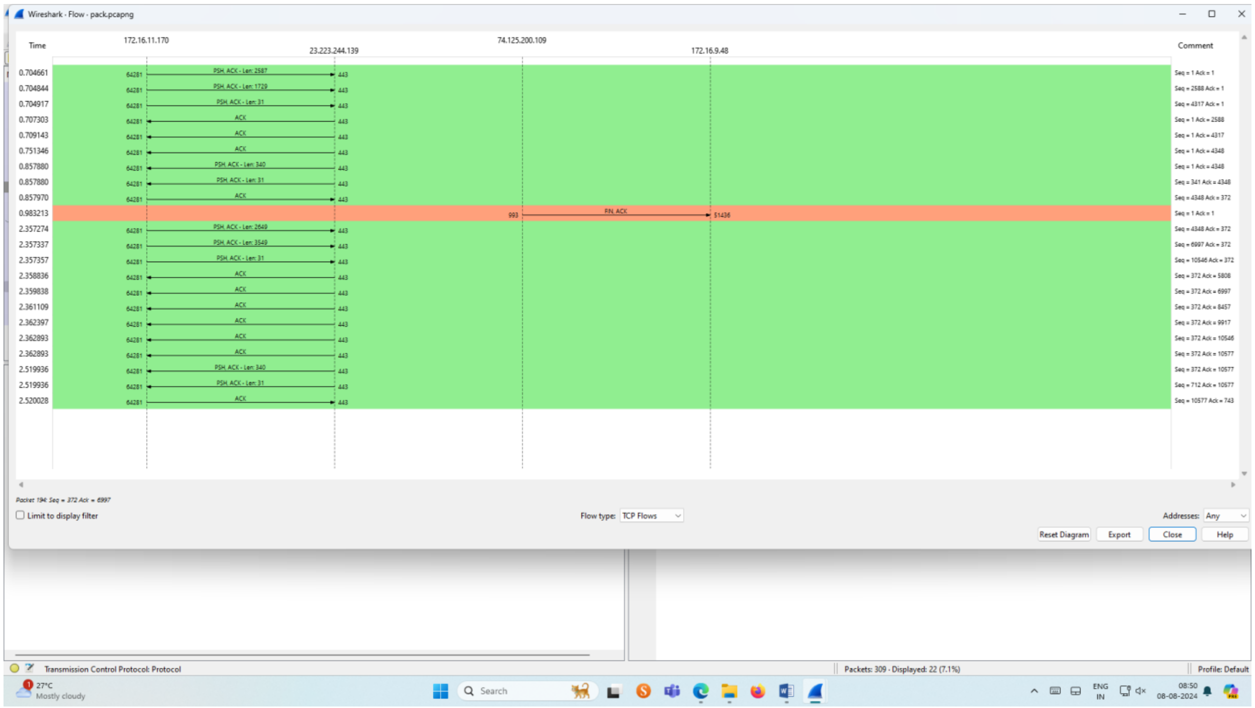
- Select Local Area Connection in Wireshark.
- Go to capture □ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics□Flow graph.
- Save the packets.

Output:


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

```
tcp

No.   Time      Source           Destination      Protocol Length Info
   50 0.704661  172.16.11.170    23.223.244.139   TLSv1.2  2641 Application Data
   51 0.704844  172.16.11.170    23.223.244.139   TLSv1.2  1783 Application Data
   52 0.704917  172.16.11.170    23.223.244.139   TLSv1.2    85 Application Data
   53 0.707303  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=1 Ack=2588 Win=1447 Len=0
   54 0.709143  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=1 Ack=4317 Win=1493 Len=0
   58 0.751346  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=1 Ack=4348 Win=1493 Len=0
   73 0.857880  23.223.244.139   172.16.11.170    TLSv1.2   394 Application Data
   74 0.857880  23.223.244.139   172.16.11.170    TLSv1.2    85 Application Data
   75 0.857970  172.16.11.170    23.223.244.139   TCP        54 64281 → 443 [ACK] Seq=4348 Ack=372 Win=1024 Len=0
   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
  190 2.357274  172.16.11.170    23.223.244.139   TLSv1.2  2703 Application Data
  191 2.357337  172.16.11.170    23.223.244.139   TLSv1.2  3603 Application Data
  192 2.357357  172.16.11.170    23.223.244.139   TLSv1.2    85 Application Data
  193 2.358836  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=372 Ack=5808 Win=1502 Len=0
  194 2.359838  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=372 Ack=6997 Win=1502 Len=0
  195 2.361109  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=372 Ack=8457 Win=1502 Len=0
  196 2.362397  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=372 Ack=9917 Win=1502 Len=0
  197 2.362893  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=372 Ack=10546 Win=1502 Len=0
  198 2.362893  23.223.244.139   172.16.11.170    TCP        60 443 → 64281 [ACK] Seq=372 Ack=10577 Win=1502 Len=0
  206 2.519936  23.223.244.139   172.16.11.170    TLSv1.2   394 Application Data
  207 2.519936  23.223.244.139   172.16.11.170    TLSv1.2    85 Application Data
  208 2.520028  172.16.11.170    23.223.244.139   TCP        54 64281 → 443 [ACK] Seq=10577 Ack=743 Win=1022 Len=0

> Frame 198: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{7DCD1869-10FE-4C3D-8396-8224ACA073C7},
> Ethernet II, Src: Sophos_cf:be:45 (7c:5a:1c:cf:be:45), Dst: HP_39:1e:d9 (7c:57:58:39:1e:d9)
> Internet Protocol Version 4, Src: 23.223.244.139, Dst: 172.16.11.170
> Transmission Control Protocol, Src Port: 443, Dst Port: 64281, Seq: 372, Ack: 10577, Len: 0

0000  7c 57 58 39 1e d9 7c 5a  1c cf be 45 08 00 45 00   |WX9··|Z ···E··E·
0010  00 28 1c 0c 40 00 40 06  5a 9f 17 df f4 8b ac 10   ·(··@·@· Z·······
0020  0b aa 01 bb fb 19 80 9c  6e 48 8e a5 d8 16 50 10   ········ nH····P·
0030  05 de 93 5b 00 00 00 00  00 00 00 00               ···[···· ····

Transmission Control Protocol: Protocol        Packets: 309 · Displayed: 22 (7.1%)        Profile: Default
```

Flow Graph output



Wireshark · Flow · pack.pcapng

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

☐ Limit to display filter

Flow type: TCP Flows

Addresses: Any

Transmission Control Protocol: Protocol

Packets: 309 · Displayed: 22 (7.1%)

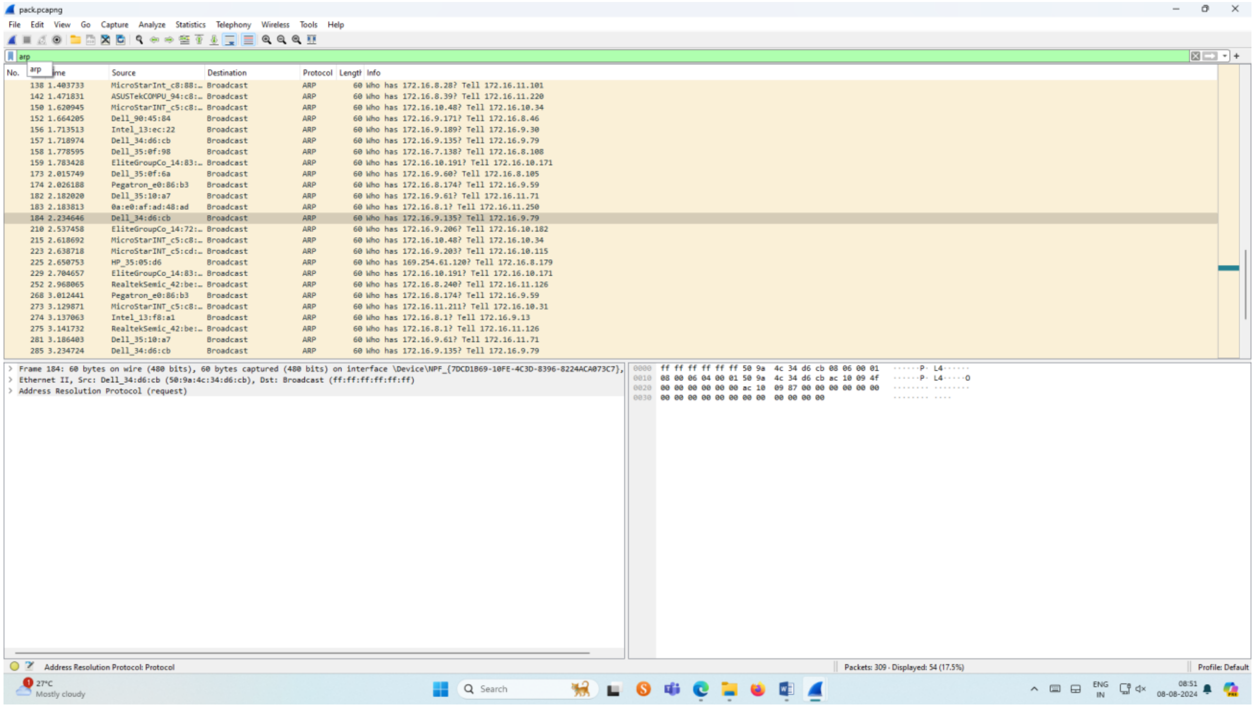
Profile: Default

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 ime         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_{7DCD1B69-10FE-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               ········ ····
```

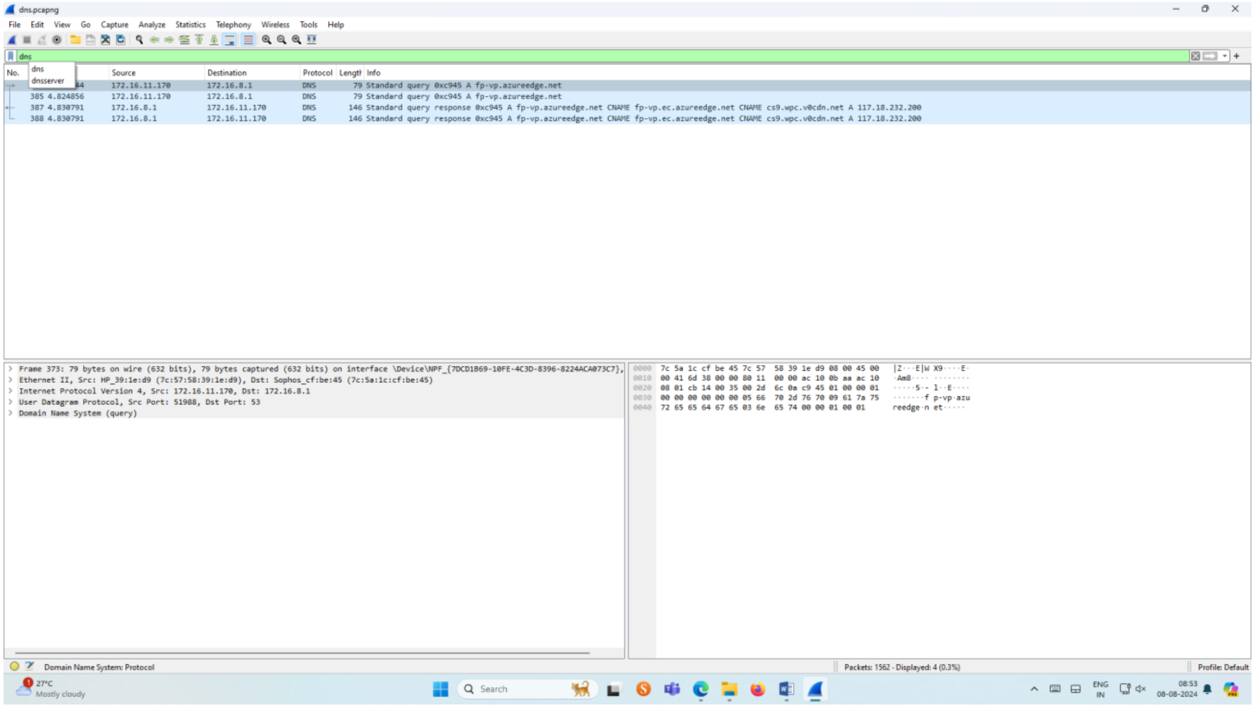
Address Resolution Protocol: Protocol | Packets: 309 · Displayed: 54 (17.5%) | Profile: Default

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 StatisticsFlow graph.
- ➢ Save the packets.

Output

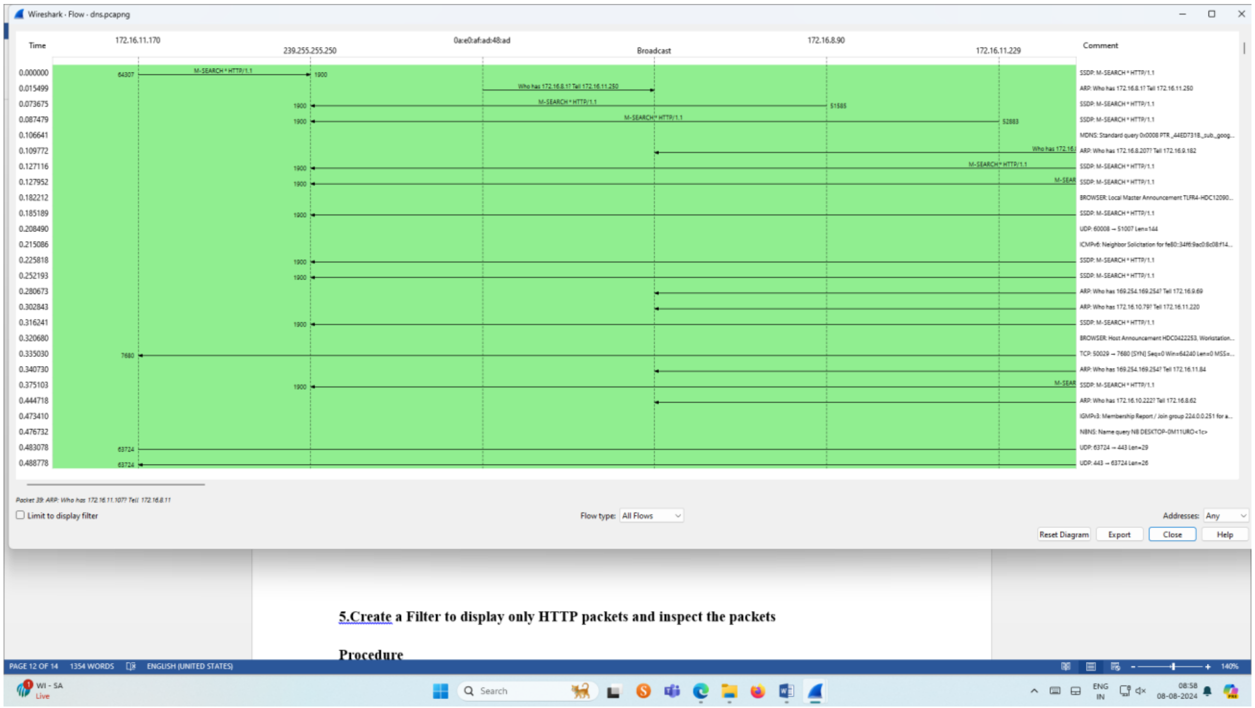

dns.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
dns
dnsserver
Domain Name System: Protocol
Packets: 1562 · Displayed: 4 (0.3%)
Profile: Default
27°C
Mostly cloudy
Search
ENG
IN
08:53
08-08-2024

```
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_{7DCD1B69-10FE-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·····
```

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 _44ED731B._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::34f6:9ac0:8c08: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 39: ARP: Who has 172.16.11.107? Tell 172.16.8.11

□ Limit to display filter

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

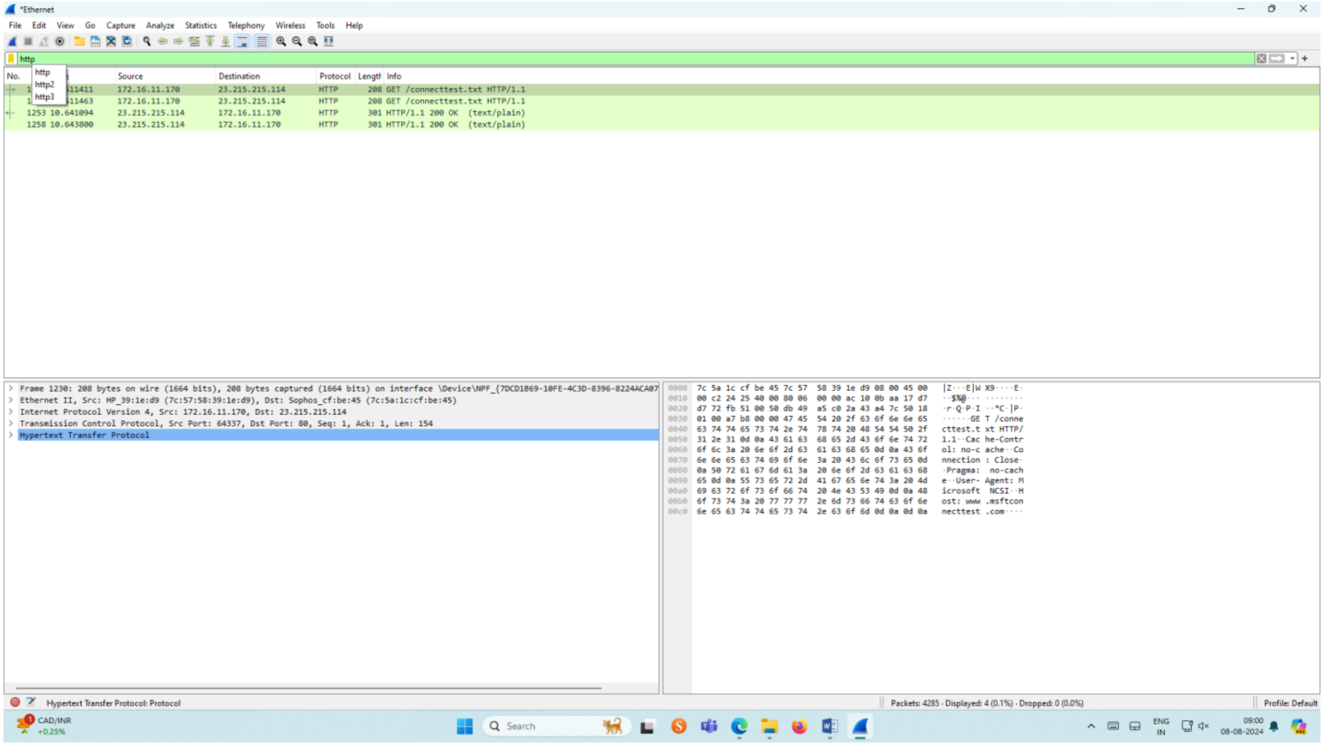
Procedure

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
Hypertext Transfer Protocol: Protocol
CAD/INR
+0.25%
Search
ENG
IN
09:00
08-08-2024

http

```
No.                   Source          Destination     Protocol Length Info
1        511411       172.16.11.170   23.215.215.114  HTTP     208 GET /connecttest.txt HTTP/1.1
1        511463       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)
```

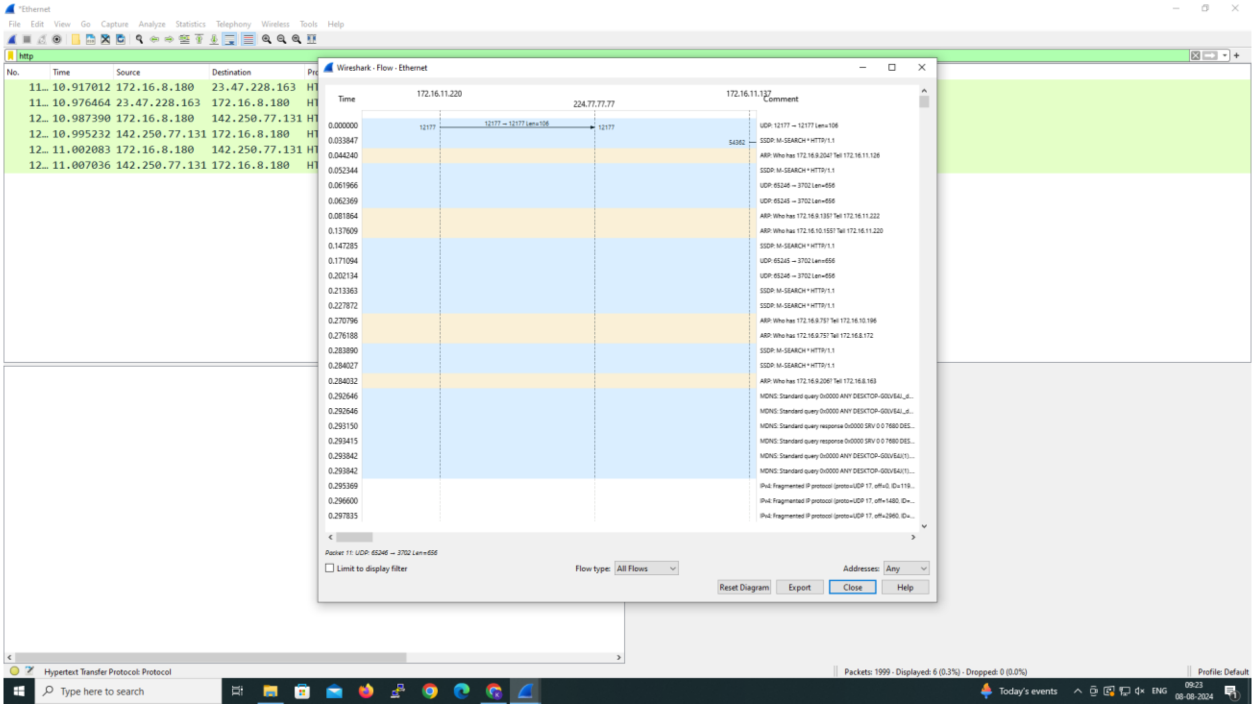
```
> Frame 1230: 208 bytes on wire (1664 bits), 208 bytes captured (1664 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA07
> Ethernet II, Src: HP_39:1e:d9 (7c:57:58:39:1e:d9), Dst: Sophos_cf:be:45 (7c:5a:1c:cf:be:45)
> Internet Protocol Version 4, Src: 172.16.11.170, Dst: 23.215.215.114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

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

Profile: Default

Flow Graph output


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Flow · Ethernet
Reset Diagram
Export
Close
Help

http

```
No.    Time       Source          Destination     Pro
 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
```

```
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-G0LVE4J._d...
0.292646                                                        MDNS: Standard query 0x0000 ANY DESKTOP-G0LVE4J._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-G0LVE4J(1)....
0.293842                                                        MDNS: Standard query 0x0000 ANY DESKTOP-G0LVE4J(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

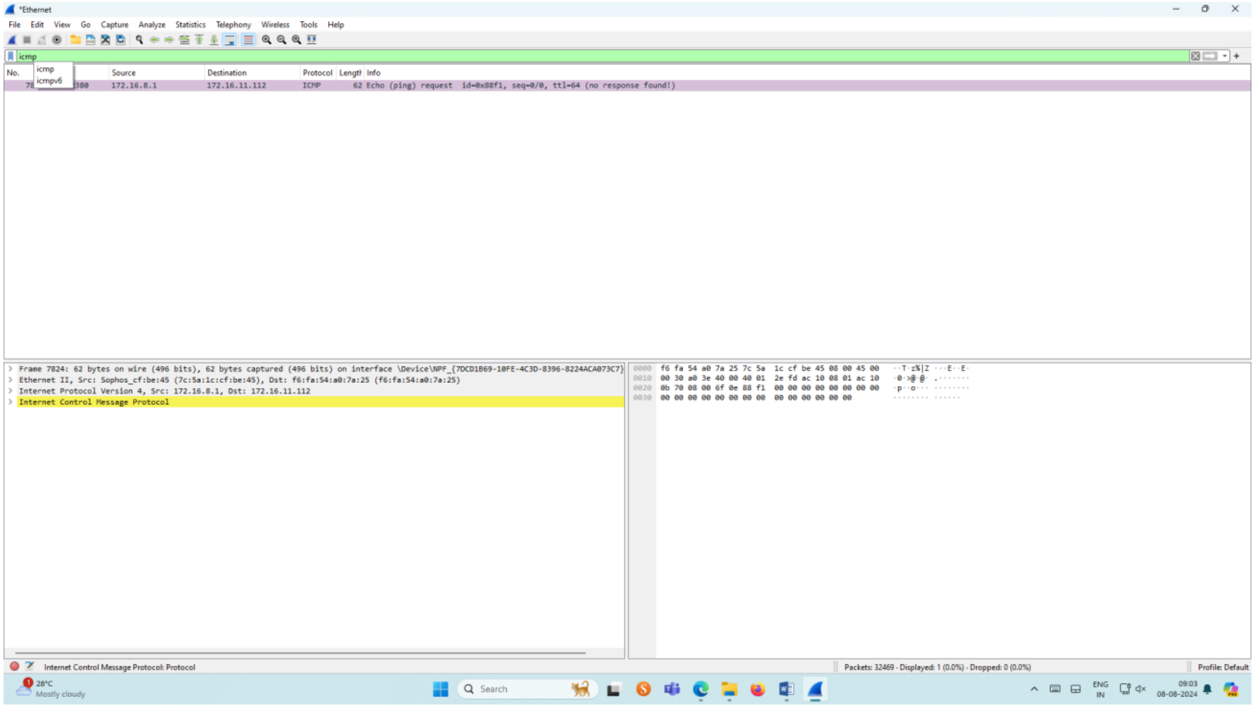
Type here to search   Today's events   ENG   09:23 08-08-2024

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



*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
icmp
icmpv6

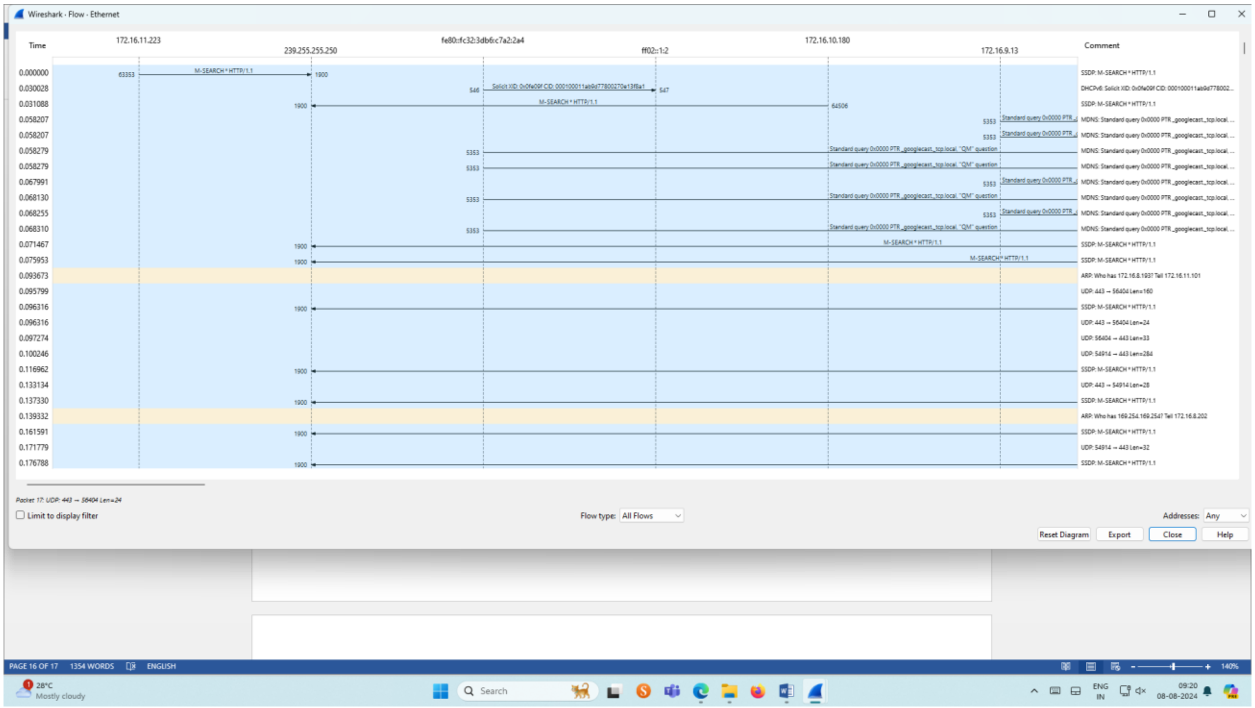
```
No.          Source         Destination     Protocol Length Info
  78...380   172.16.8.1     172.16.11.112   ICMP         62 Echo (ping) request  id=0x88f1, seq=0/0, ttl=64 (no response found!)
```

```
> Frame 7824: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface \Device\NPF_{7DCD1B69-10FE-4C3D-8396-8224ACA073C7}
> Ethernet II, Src: Sophos_cf:be:45 (7c:5a:1c:cf:be:45), Dst: f6:fa:54:a0:7a:25 (f6:fa:54:a0:7a:25)
> Internet Protocol Version 4, Src: 172.16.8.1, Dst: 172.16.11.112
> Internet Control Message Protocol
```

```
0000  f6 fa 54 a0 7a 25 7c 5a  1c cf be 45 08 00 45 00   ··T·z%|Z ···E··E·
0010  00 30 a0 3e 40 00 40 01  2e fd ac 10 08 01 ac 10   ·0·>@·@· .·······
0020  0b 70 08 00 6f 0e 88 f1  00 00 00 00 00 00 00 00   ·p··o··· ········
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00         ········ ······
```

```
Internet Control Message Protocol: Protocol
Packets: 32469 · Displayed: 1 (0.0%) · Dropped: 0 (0.0%)
Profile: Default
```

Flow Graph output



Wireshark · Flow · Ethernet
172.16.11.223
239.255.255.250
fe80::fc32:3db6:c7a2:2a4
ff02::1:2
172.16.10.180
172.16.9.13
63353
1900
M-SEARCH * HTTP/1.1
546
547
Solicit XID: 0x0fe09f CID: 000100011ab9d77800270e13f8a1
64506
5353
Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question

```
Time       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
```

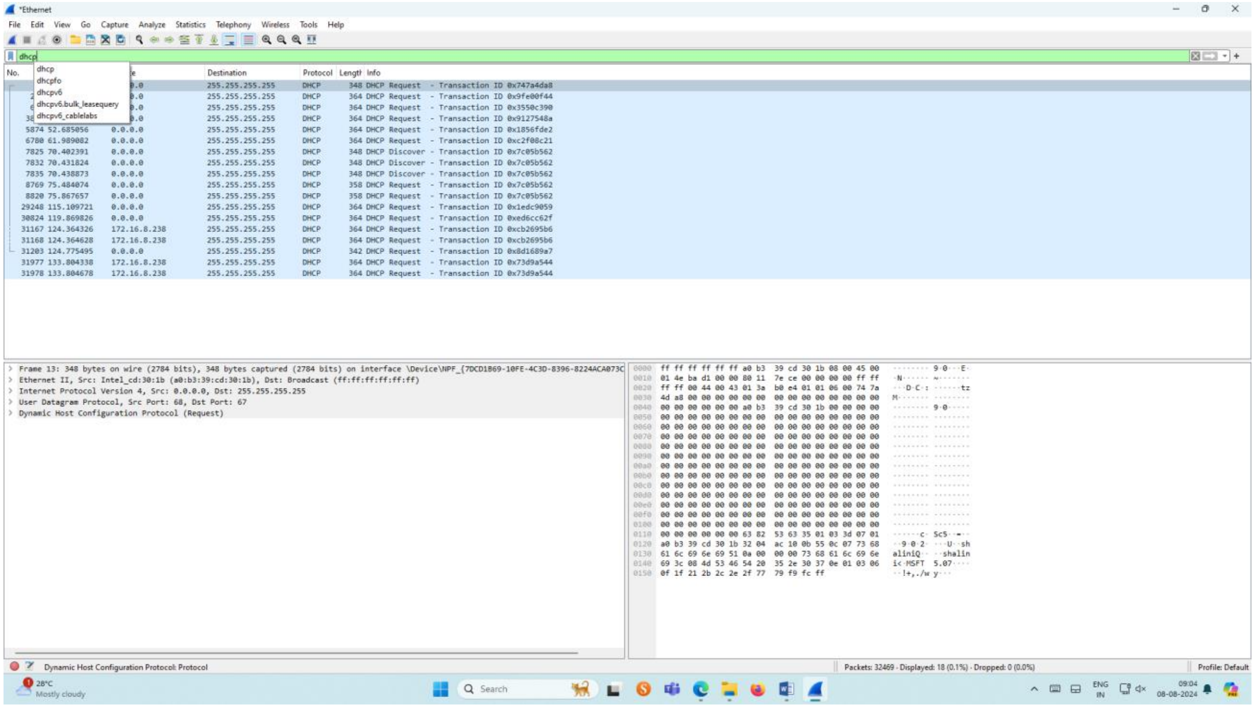
```
Packet 17: UDP: 443 → 56404 Len=24
☐ Limit to display filter          Flow type: All Flows          Addresses: Any
```

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


*Ethernet
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
dhcp
dhcpfo
dhcpv6
dhcpv6.bulk_leasequery
dhcpv6_cablelabs

No.	Time	Source	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

RESULT:

The analysing of network traffic using wireshark tool is studied and the output is verified.