

## Ex No: 14 b PACKET SNIFFING USING WIRESHARK

DATE:19.8.24


AIM:

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

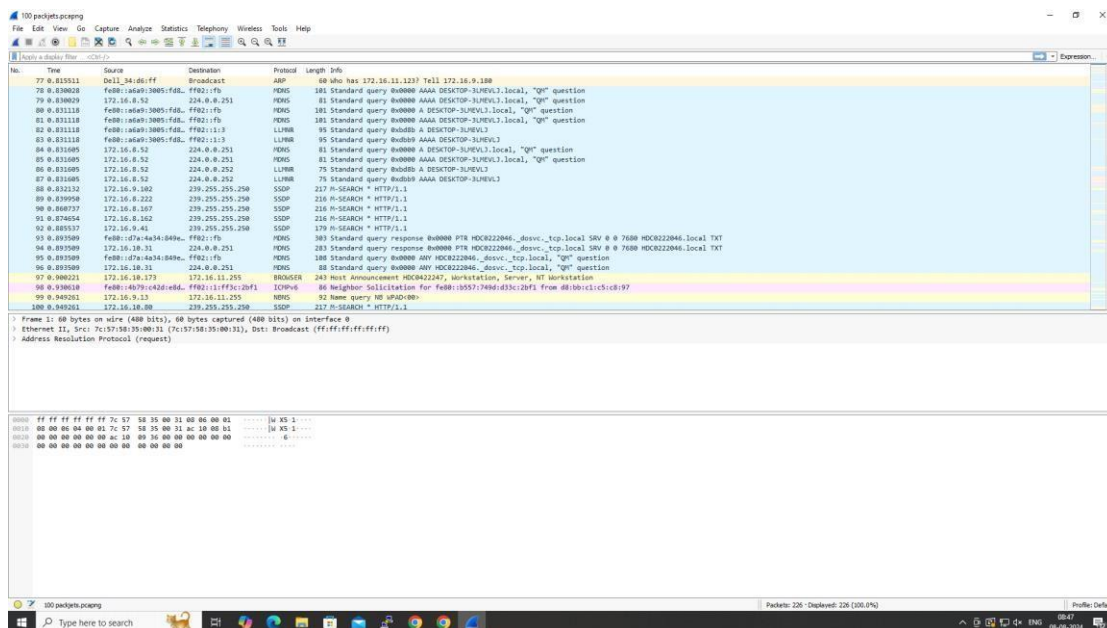
### Exercises

#### 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



#### 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:


The image shows the Wireshark interface with a packet capture list on the left and a packet details pane on the right. The packet list shows various protocols including HTTP, DNS, and User Datagram Protocol (UDP). The packet details pane shows the structure of a selected packet, including Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Simple Service Discovery Protocol (SSDP).

## Flow Graph output:

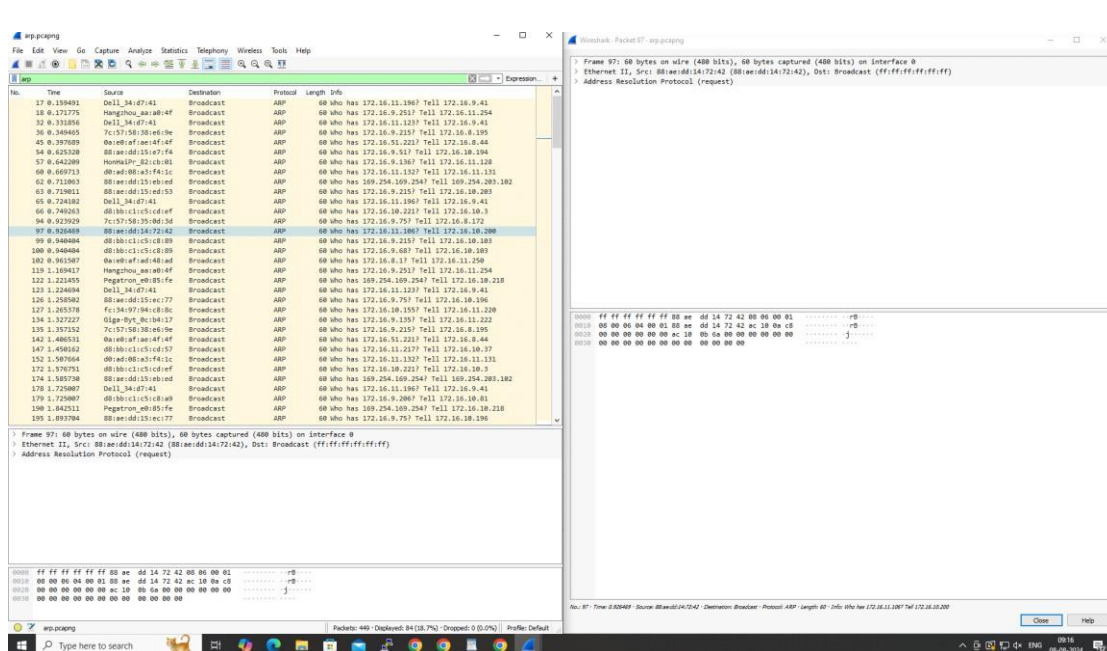
The image shows the Wireshark flow graph window, which displays a sequence of network flows between different IP addresses. The flows are represented as horizontal bars with labels indicating the protocol and the destination IP address. The flow graph shows a sequence of flows for various protocols, including HTTP, DNS, and User Datagram Protocol (UDP).

### 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

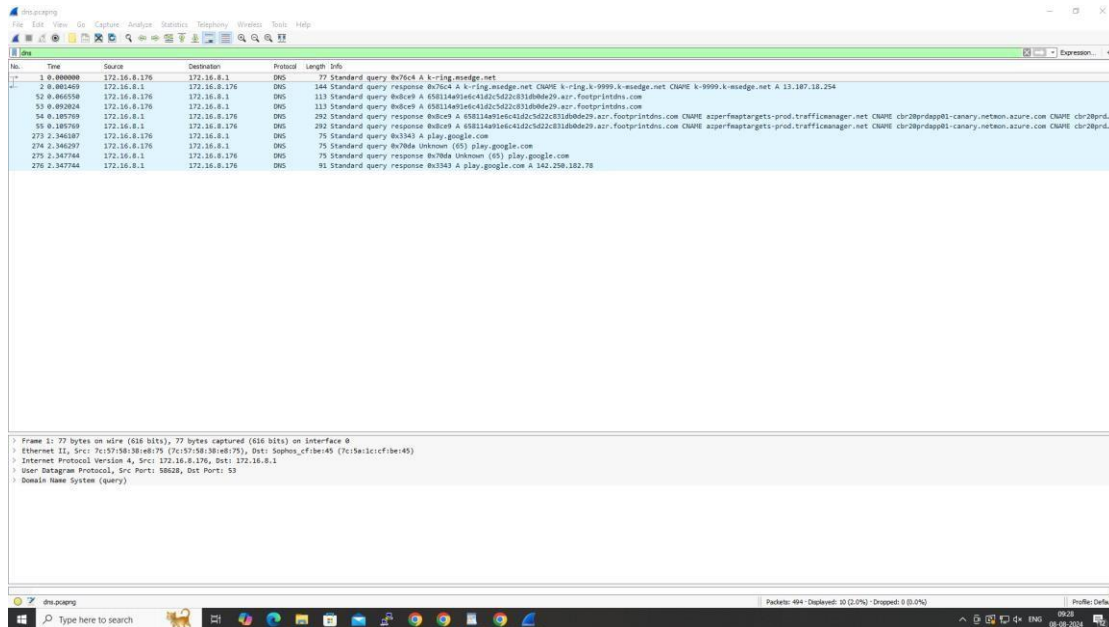


### 4.Create a Filter to display only DNS packets and provide the flow graph.

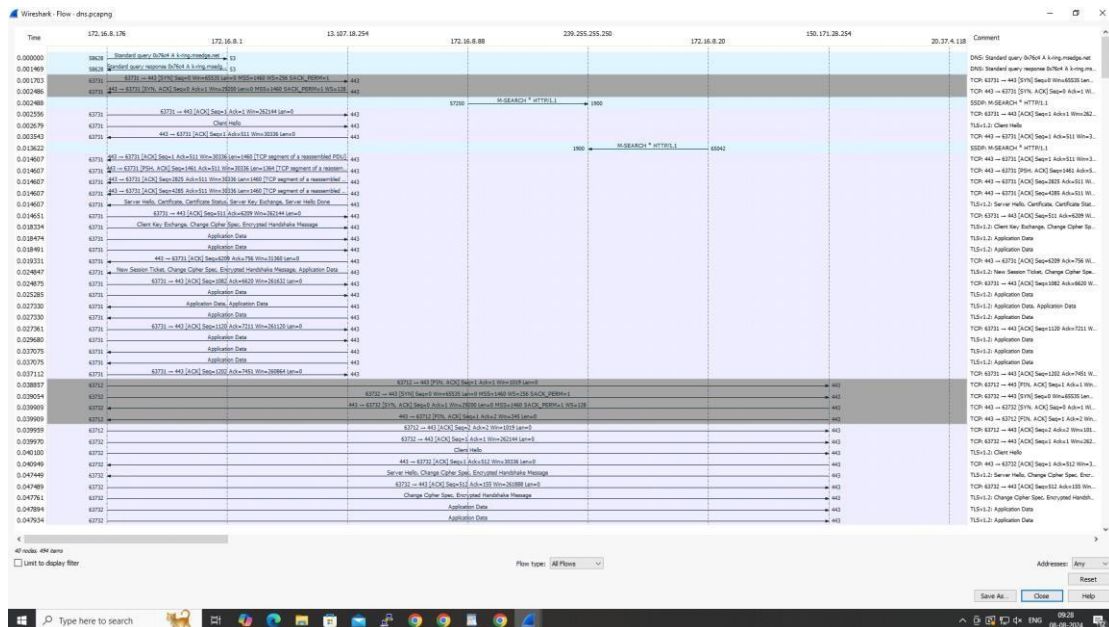
#### Procedure

- 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



## Flow Graph output



## 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:

The screenshot displays the Wireshark network protocol analyzer interface. The main window shows a packet capture of an HTTP GET request. The packet list on the left shows a single packet (No. 1) of type HTTP. The packet details pane on the right shows the structure of the HTTP packet, including Ethernet II, Internet Protocol Version 4, Transmission Control Protocol, and Hypertext Transfer Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.


## Flow Graph output:

The screenshot displays the Wireshark Flow Graph output. The graph shows a sequence of network events, including a broadcast, a request, and a response. The nodes are labeled with IP addresses and port numbers. The edges represent the flow of data between these nodes. The graph shows a sequence of events including a broadcast, a request, and a response.

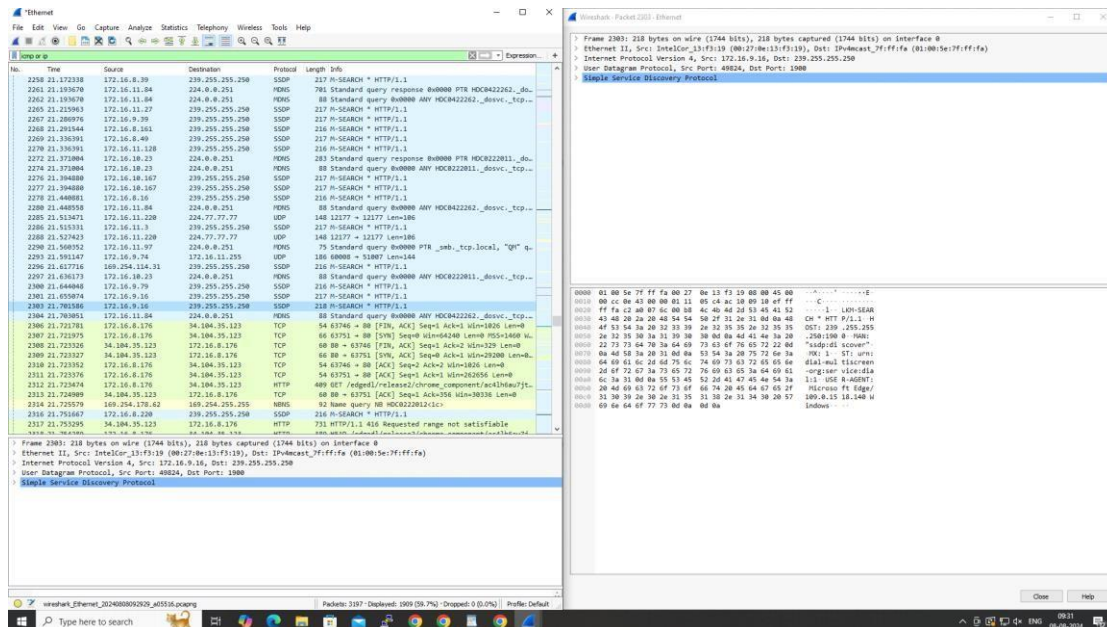


## 6. Create a Filter to display only IP/ICMP packets and inspect the packets.

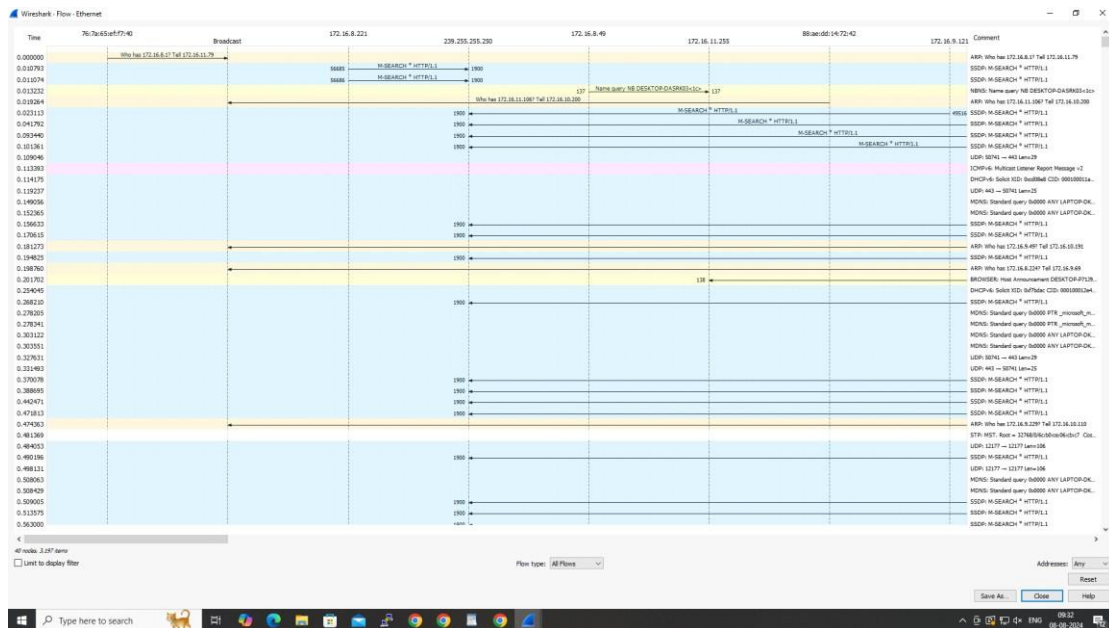
### Procedure

- 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:




### Flow Graph output:



## 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:

Wireshark Packet 173: Ethernet

Frame 173: 378 bytes on wire (3060 bits), 378 bytes captured (3060 bits) on Interface 0

Ethernet II, Src: 28:c1:9b:8e:3f:e1 (28:c1:9b:8e:3f:e1), 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)

No.	Time	Source	Destination	Protocol	Length	Info
172	2.447280	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 8a4d59c8e
173	2.447287	0.0.0.0	255.255.255.255	DHCP	378	DHCP Request - Transaction ID 8a4d59c8e
238	3.181724	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 8a7821321
356	4.239145	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 8a1eff81c
483	5.248145	0.0.0.0	255.255.255.255	DHCP	378	DHCP Request - Transaction ID 8a1eff81c

Frame 173: 378 bytes on wire (3060 bits), 378 bytes captured (3060 bits) on Interface 0

Ethernet II, Src: 28:c1:9b:8e:3f:e1 (28:c1:9b:8e:3f:e1), 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 20 c1 9b 8e 3f e1 00 00 45 00 .....?..E

0010 01 64 ba c5 00 00 00 11 7e c3 00 00 00 ff ff ..d.w.....

0020 ff ff 00 44 00 41 01 58 30 20 01 01 00 00 4d 05 ..CP+..M

0030 5c ce 00 00 00 00 00 00 00 00 00 00 00 00 00 ..Scce.....

0040 00 00 00 00 00 20 c1 9b 8e 3f e1 00 00 00 00 .....?..E

0050 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 .....  
0070 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 .....  
0090 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 .....  
00b0 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 .....  
00d0 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 .....  
00f0 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 .....  
0110 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....  
0120 20 c1 9b 8e 3f e1 32 04 ac 10 00 c0 36 04 ac 10 ..?..E

0130 00 01 0c 0f 44 45 53 00 54 4f 54 2f 53 40 44 00 ..DESKTOP-SAGE

0140 48 47 4e 51 12 00 00 00 44 45 53 40 54 4f 50 20 ..HMQZ..DESKTOP

0150 53 40 44 40 47 4e 2c 60 40 52 40 54 20 55 26 ..SAGEHMQZ..HQP1 S-

0160 30 37 04 01 03 00 0f 1f 21 20 2c 20 2f 77 70 70 ..?..?..?..?..?

0170 fc ff ..

No. 173: Time 2.447287 Source 0.0.0.0 Destination 255.255.255.255 Protocol DHCP Length 378 Info DHCP Request - Transaction ID 8a4d59c8e