
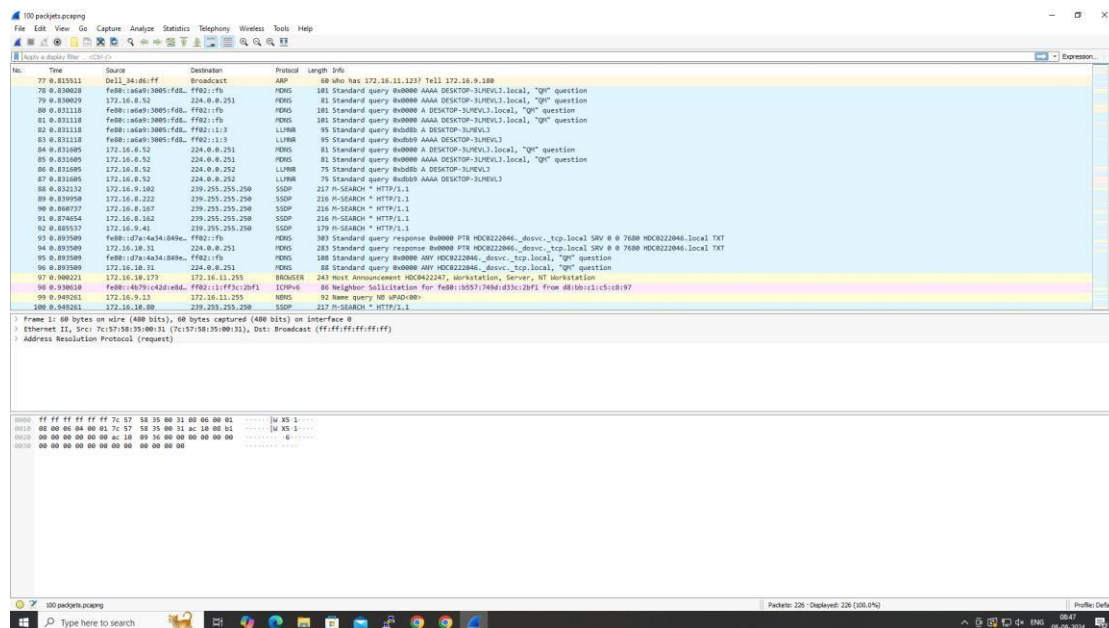


**Ex No: 4 b    PACKET SNIFFING USING WIRESHARK****DATE:19.8.24****AIM:**

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 screenshot shows the Wireshark interface with a packet capture on the left pane. The packet list shows various protocols including HTTP, DNS, and User Datagram Protocol (UDP). The right pane displays the details of a selected packet (Frame 17), showing the raw data and its hexadecimal representation.

## Flow Graph output:

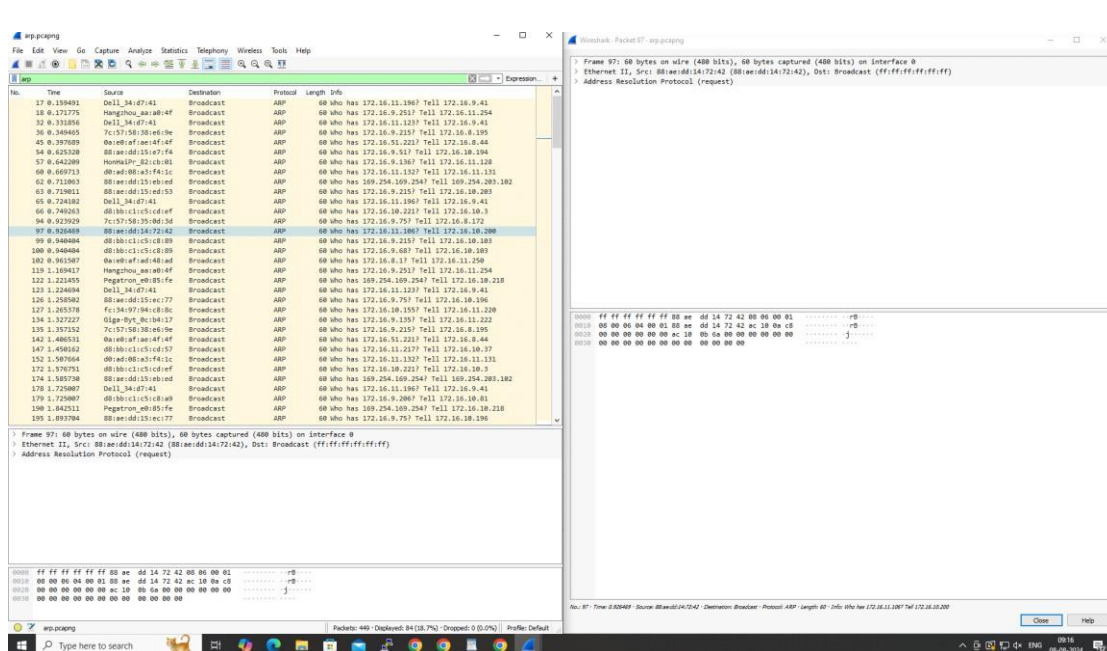
The screenshot shows the Wireshark Flow Graph output, displaying a sequence of packets and their relationships. The graph shows the flow of data between different hosts and ports, with packets numbered and color-coded to represent different flows.

### 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

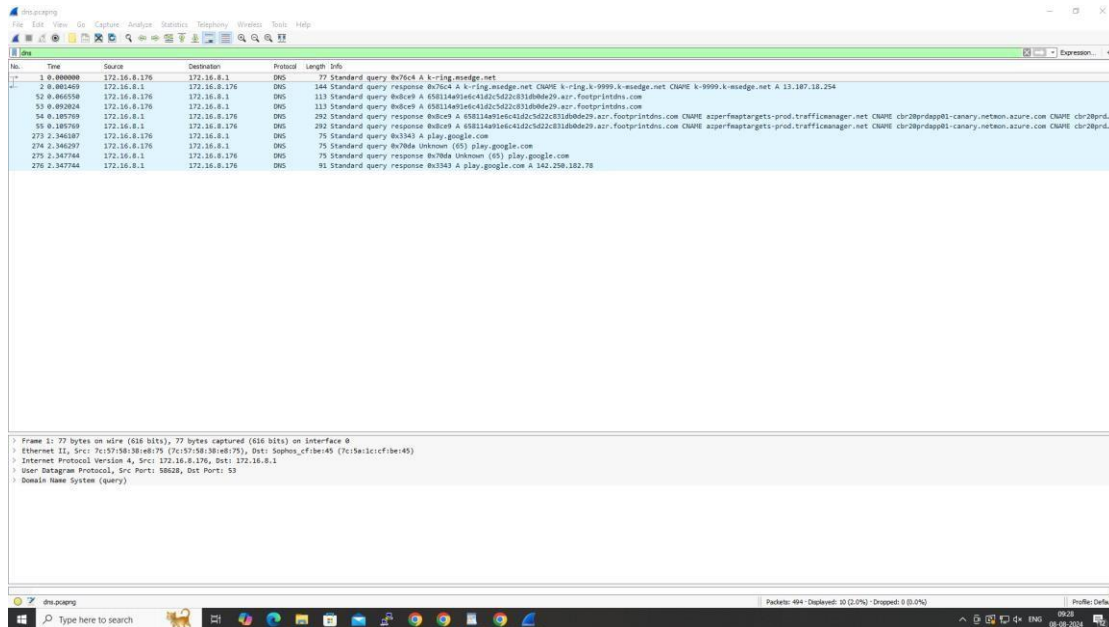


### 4.Create a Filter to display only DNS packets and provide the flow graph.

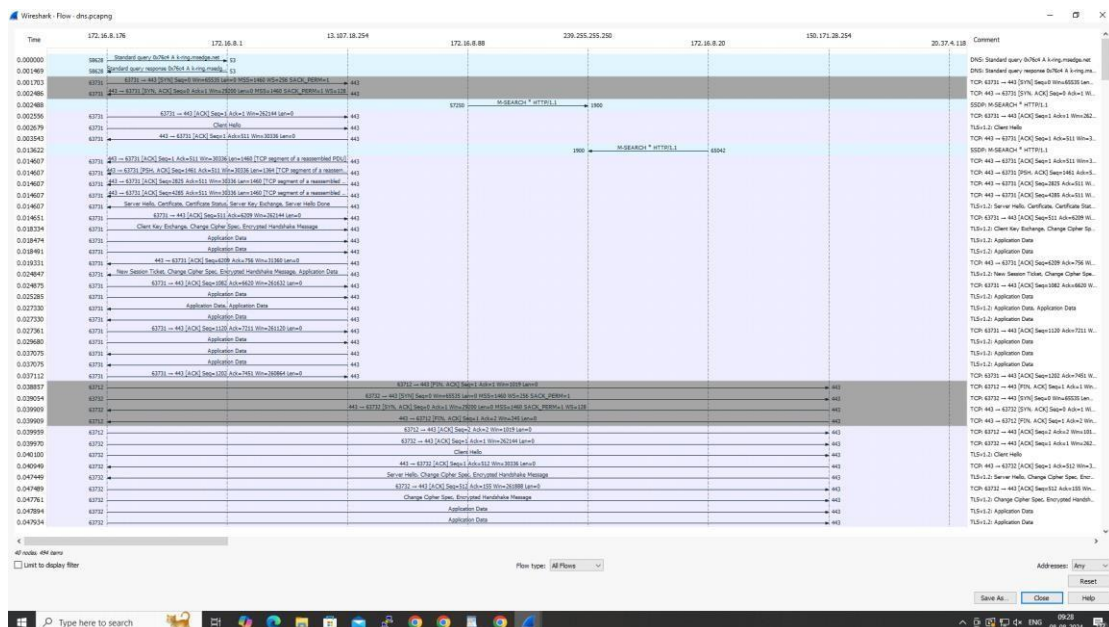
#### Procedure

- 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 packet 731 selected. The packet details pane on the right shows the structure of the HTTP GET request, including the status line '200 OK' and various headers. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.


## Flow Graph output:

The screenshot displays the Wireshark Flow Editor interface, showing a flow graph for the selected HTTP GET request. The graph illustrates the sequence of events, including the arrival of the packet, the search for the destination IP, and the subsequent actions taken by the network stack.

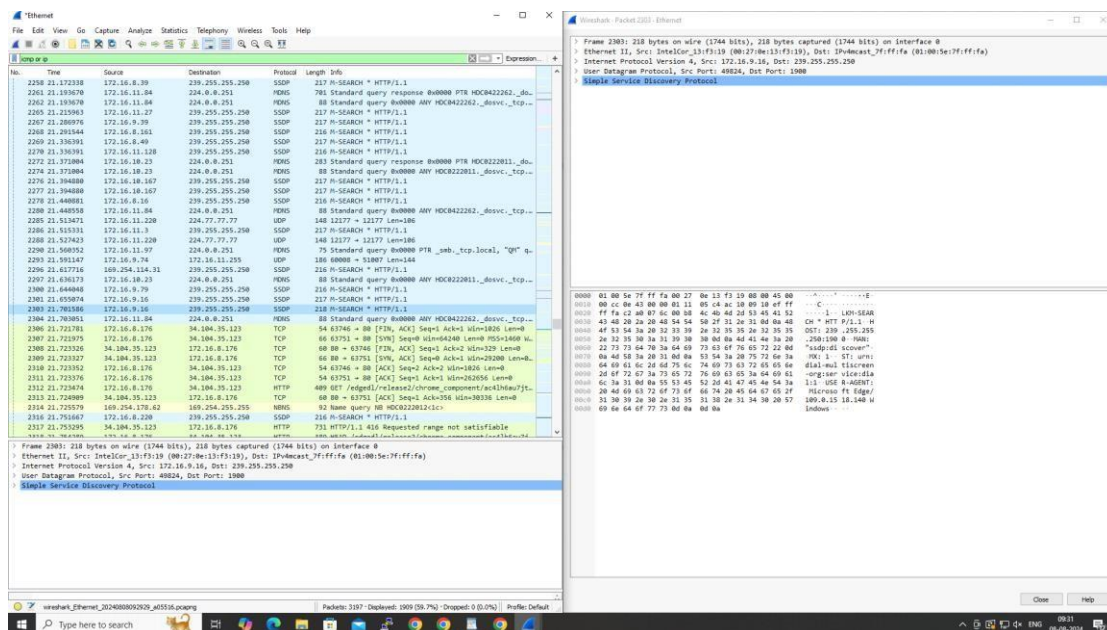


## 6.Create a Filter to display only IP/ICMP packets and inspect the packets.

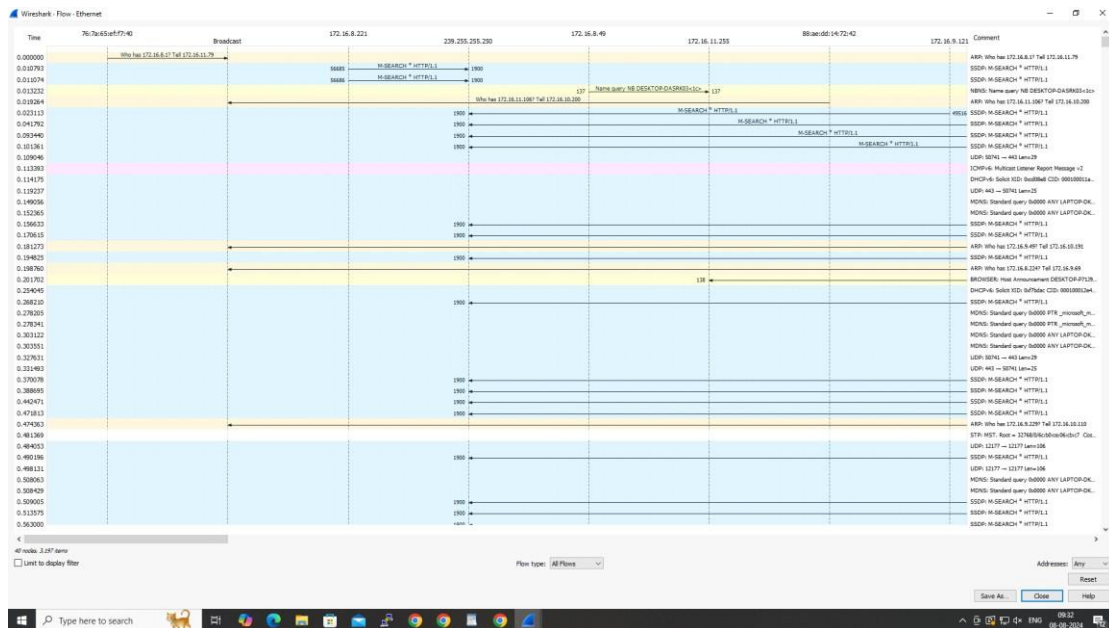
### Procedure

- 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:

