

ROLL NO:231901047
SASIKUMAR.B
EXPNO: 4B

4B: PACKET SNIFFING USING WIRESHARK


AIM:

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

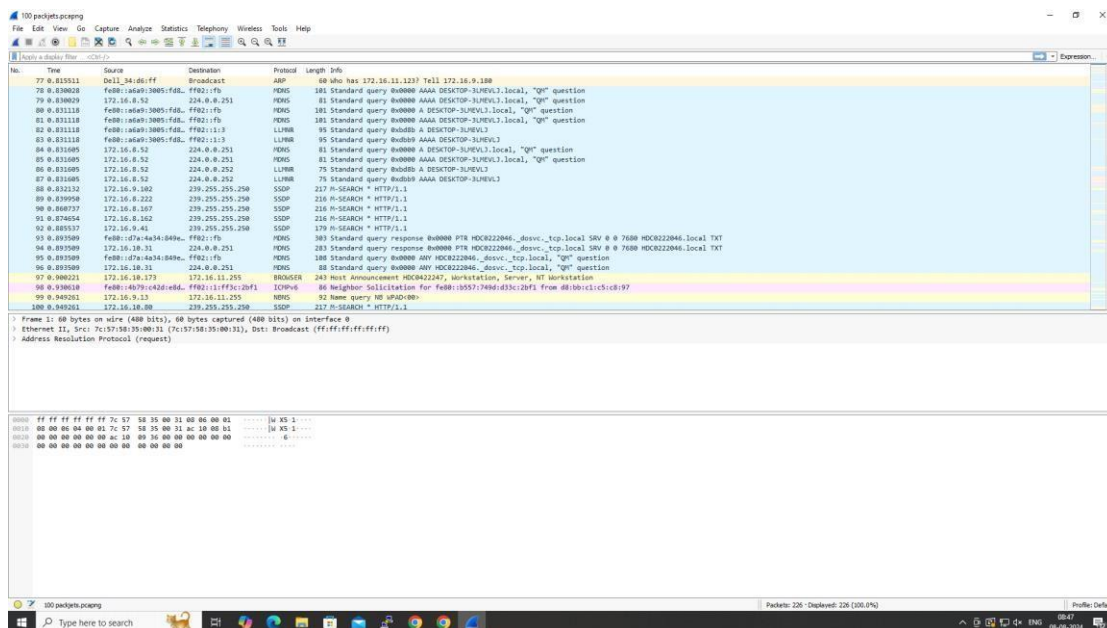
Exercises

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 displays 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 shows the details of a selected packet, specifically a frame of 256 bytes on wire (1728 bits), 256 bytes captured (1728 bits) on interface 0. The packet is an Ethernet II, Src: d81b01c1c1a18 (d81b01c1c1a18), Dst: 1p0mcast_7f:ff:fa (01:00:5e:7f:ff:fa). The packet is a User Datagram Protocol, Src Port: 51785, Dst Port: 1900. The packet is a Simple Service Discovery Protocol.

Flow Graph output:

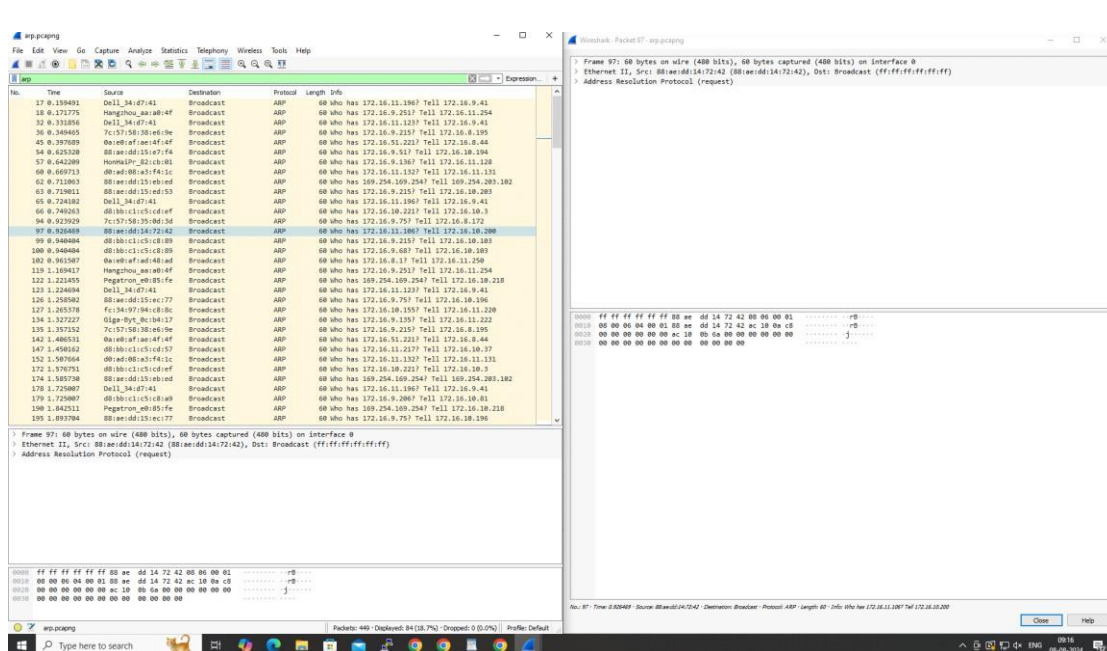
The screenshot displays the Wireshark flow graph output. The top pane shows a list of packets with their time, source, destination, protocol, length, and info. The bottom pane shows the flow graph, which is a sequence of packets connected by arrows, representing the flow of data. The flow graph shows a sequence of packets from 0.000000 to 0.455223, with various protocols and lengths. The flow graph is a sequence of packets connected by arrows, representing the flow of data.

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

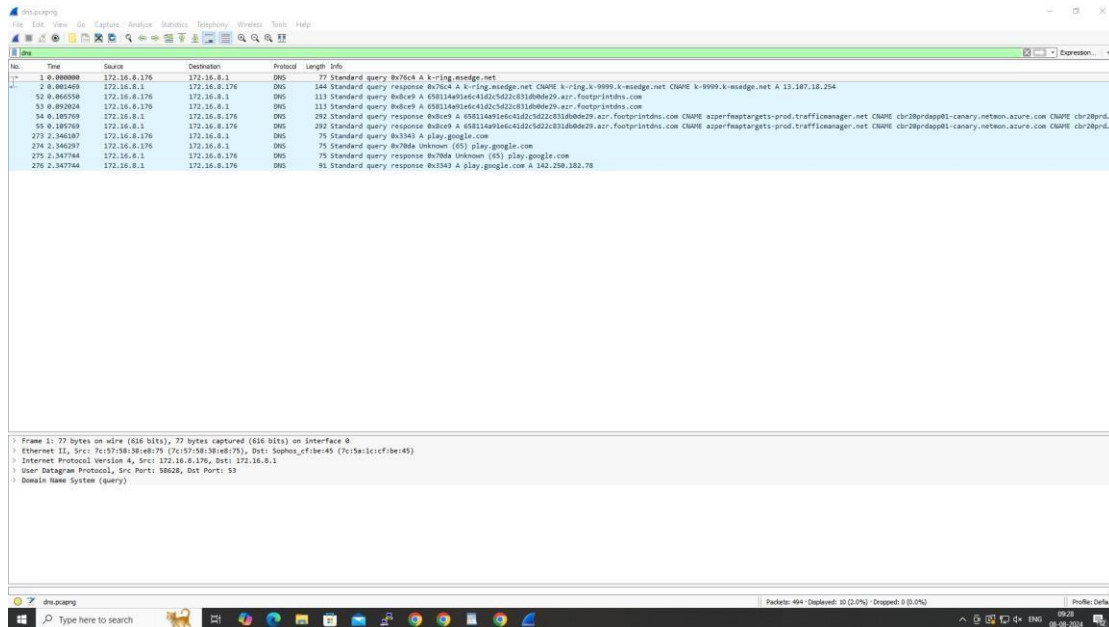


4.Create a Filter to display only DNS packets and provide the flow graph.

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 StatisticsFlow graph.
- Save the packets.

Output

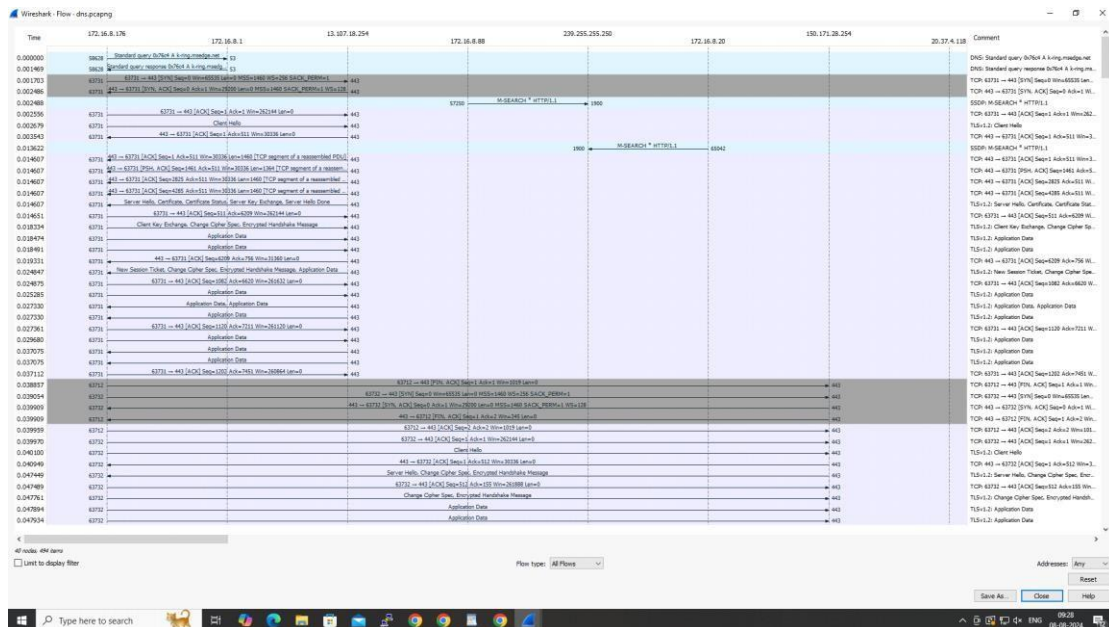


The screenshot shows the Wireshark interface with a packet capture list on the left and packet details on the right. The packet list shows several DNS queries and responses. The packet details pane shows the structure of a DNS query, including the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query) layers.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.8.176	172.16.8.1	DNS	77	Standard query 8476c4 A k-ring.msedge.net
2	0.001469	172.16.8.1	172.16.8.176	DNS	144	Standard query response 8476c4 A k-ring.msedge.net CNAME k-ring.k-9999.k-msedge.net CNAME k-9999.k-msedge.net A 13.107.18.254
52	0.000550	172.16.8.176	172.16.8.1	DNS	113	Standard query 8d0ce9 A 65811481e41d2c5d2c811dbbde29.acr-footprintdns.com
53	0.002824	172.16.8.176	172.16.8.1	DNS	113	Standard query 8d0ce9 A 65811481e41d2c5d2c811dbbde29.acr-footprintdns.com
54	0.185789	172.16.8.1	172.16.8.176	DNS	282	Standard query response 8d0ce9 A 65811481e41d2c5d2c811dbbde29.acr-footprintdns.com CNAME asperfwatargets-prod.trafficmanager.net CNAME chr28rpdag01-canary.network.azure.com CNAME chr28rpd-
55	0.185789	172.16.8.1	172.16.8.176	DNS	282	Standard query response 8d0ce9 A 65811481e41d2c5d2c811dbbde29.acr-footprintdns.com CNAME asperfwatargets-prod.trafficmanager.net CNAME chr28rpdag01-canary.network.azure.com CNAME chr28rpd-
273	2.346387	172.16.8.176	172.16.8.1	DNS	75	Standard query 8a3343 A play.google.com
274	2.346207	172.16.8.1	172.16.8.176	DNS	75	Standard query 8a78da Unknown (65) play.google.com
275	2.347744	172.16.8.1	172.16.8.176	DNS	75	Standard query response 8a78da Unknown (65) play.google.com
276	2.347744	172.16.8.1	172.16.8.176	DNS	81	Standard query response 8a3343 A play.google.com A 342.250.182.78

Frame 1: 77 bytes on wire (616 bits), 77 bytes captured (616 bits) on interface 0
Ethernet II, Src: Tc15718618014879 (Tc15718618014879), Dst: Sophos_cfb45 (Tc15718618014879)
Internet Protocol Version 4, Src: 172.16.8.176, Dst: 172.16.8.1
User Datagram Protocol, Src Port: 58628, Dst Port: 53
Domain Name System (query)

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.

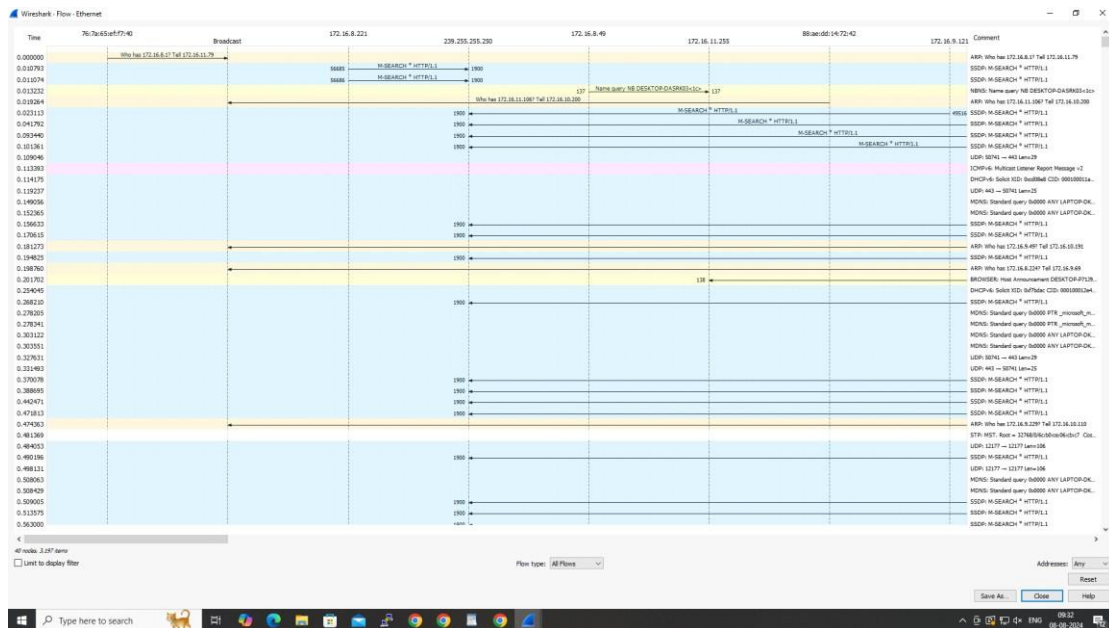
Output:

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 flow graph shows a sequence of 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 flow graph shows a sequence of events including a broadcast, a request, and a response.

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:

[illegible]