

Experiment: 4B

Date: 19.8.24

ANALYZE NETWORK TRAFFIC USING WIRESHARK TOOL

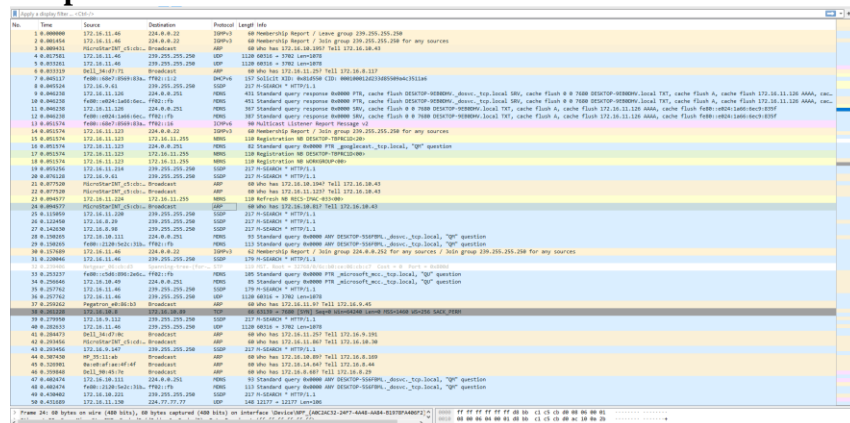
AIM:

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

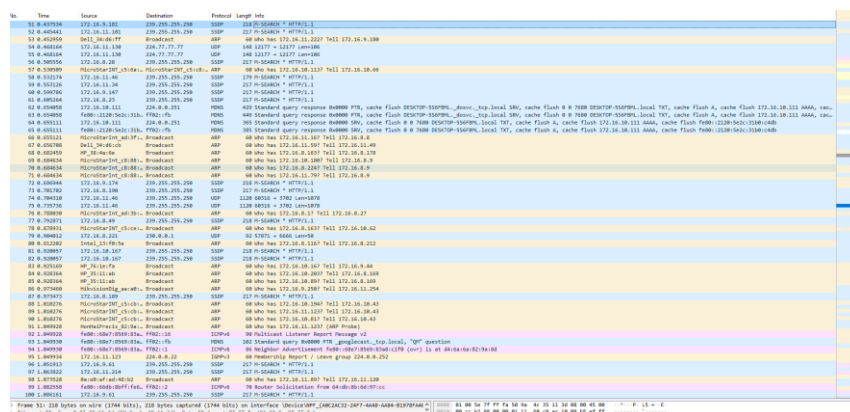
1. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it. Procedure

- 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



The image shows a Wireshark packet capture window with a list of 58 captured packets. The packets are filtered by 'eth 0' and show a variety of protocols including ICMP (ping requests and replies), DHCP (discovery, offer, request, and acknowledgment), and HTTP (GET requests for various resources). The packet list includes columns for No., Time, Source, Destination, Protocol, and Length. The packet details pane on the right shows the structure of the selected packet (No. 58, an HTTP GET request).



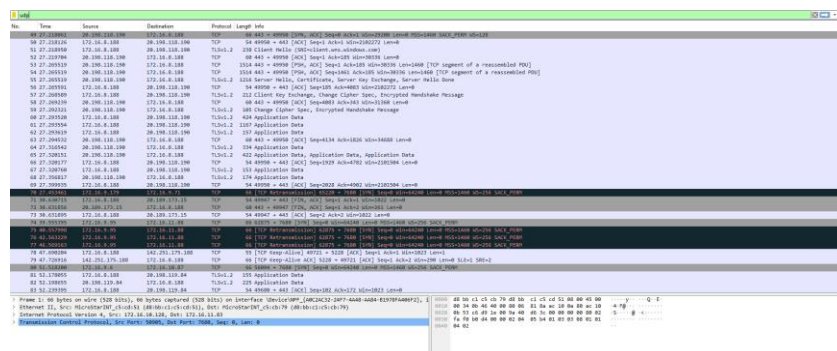
This image shows another Wireshark packet capture window, displaying a list of 58 packets. The packets are filtered by 'eth 0' and show a variety of protocols including ICMP, DHCP, and HTTP. The packet list includes columns for No., Time, Source, Destination, Protocol, and Length. The packet details pane on the right shows the structure of the selected packet (No. 58, an HTTP GET request).

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

Procedure

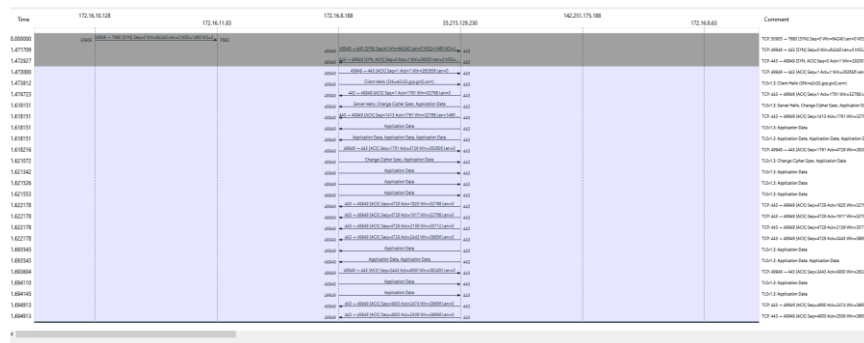
- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search TCP packets in search bar.
- To see flow graph click Statistics ☐ Flow graph.
- Save the packets.

Output:



The screenshot shows a Wireshark packet capture with columns for No., Time, Source, Destination, Protocol, Length, and Info. The packet list shows various network traffic, including TCP, UDP, and ICMP packets. The packet details pane shows the structure of the selected packet, and the packet bytes pane shows the raw data in hexadecimal and ASCII.

Flow Graph output



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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	WP_30-00-3d	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
2	0.001012	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.240? 172.16.18.172
3	0.001094	0x11,35:11:0b	Broadcast	ARP	60	Who has 172.16.18.180? 172.16.18.172
4	0.001096	0x11,35:11:0b	Broadcast	ARP	60	Who has 172.16.18.24? 172.16.18.172
5	0.001426	0x01:00:00:00:00:00	Broadcast	ARP	60	Who has 172.16.18.17? 172.16.18.172
6	0.001426	WP_30-00-3d	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
7	0.001786	0x01:00:00:00:00:00	Broadcast	ARP	60	Who has 172.16.18.160? 172.16.18.172
8	0.001788	0x01:00:00:00:00:00	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
9	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
10	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
11	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
12	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
13	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
14	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
15	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
16	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
17	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
18	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
19	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
20	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
21	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
22	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
23	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
24	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
25	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
26	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
27	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
28	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
29	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
30	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
31	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
32	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
33	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
34	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172
35	0.002027	0x11,35:11:07	Broadcast	ARP	60	Who has 172.16.18.80? 172.16.18.172

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

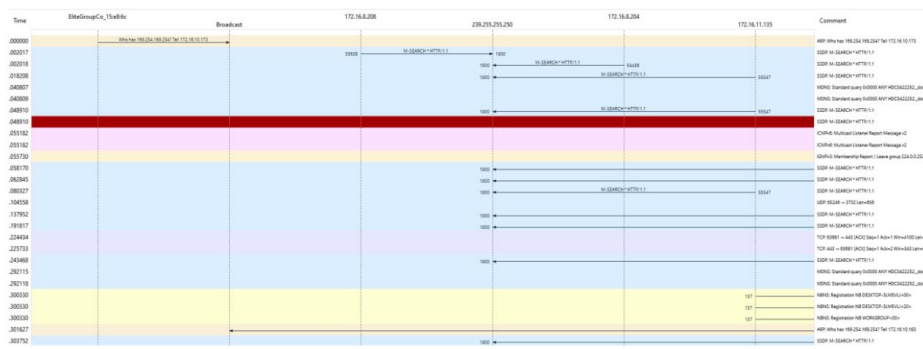
- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics ☐ Flow graph.
- Save the packets.

Output

No.	Time	Source	Destination	Protocol	Length	Info
9	0.000518	172.16.18.179	172.16.18.1	DNS	88	Standard query 0x0194 A t-ring-fallback2.msedge.net
162	2.000949	172.16.18.179	172.16.18.1	DNS	88	Standard query 0x0194 A t-ring-fallback2.msedge.net
307	4.000171	172.16.18.179	172.16.18.1	DNS	81	Standard query 0x0404 A static-cust.llnwd.net
368	4.000555	172.16.18.1	172.16.18.179	DNS	136	Standard query response 0x0404 A static-cust.llnwd.net CHAVE cs1404.upc.epsiloncdn.net A 152.199.43.62
517	6.101578	172.16.18.179	172.16.18.1	DNS	88	Standard query 0x0194 A t-ring-fallback2.msedge.net
746	10.110311	172.16.18.179	172.16.18.1	DNS	88	Standard query 0x0194 A t-ring-fallback2.msedge.net
746	10.110311	172.16.18.179	172.16.18.1	DNS	88	Standard query 0x0194 A t-ring-fallback2.msedge.net
861	11.155000	172.16.18.179	172.16.18.1	DNS	88	Standard query 0x020c A t-ring-fallback2.msedge.net

Frame 11: 88 bytes on wire (704 bits), 88 bytes captured (704 bits) on interface 0x0000000000000000 (eth0) on interface 0x0000000000000000 (eth0) [Ethernet II, Src: WP_30-00-3d (7c:57:58:35:00:3d), Dst: Sophoscfbe45 (7c:5a:1c:cf:be:45)]	0000 7c 5a 1c cf be 45 7c 57 58 35 05 05 00 00 00 00 [2] [N X5 ...]
Internet Protocol Version 4, Src: 172.16.18.179, Dst: 172.16.18.1	0010 00 4a f9 02 00 00 00 00 00 00 00 00 00 00 00 [3] [N X5 ...]
User Datagram Protocol, Src Port: 54158, Dst Port: 53	0020 00 00 00 00 00 00 11 74 2f 72 05 0a 67 5d 66 61 [4] [N X5 ...]
Domain Name System (query)	0030 0c 6c 62 61 63 60 73 32 86 6d 73 65 64 67 65 03 [5] [N X5 ...]
	0040 0c 65 74 00 00 01 00 01 [6] [N X5 ...]

Flow Graph output

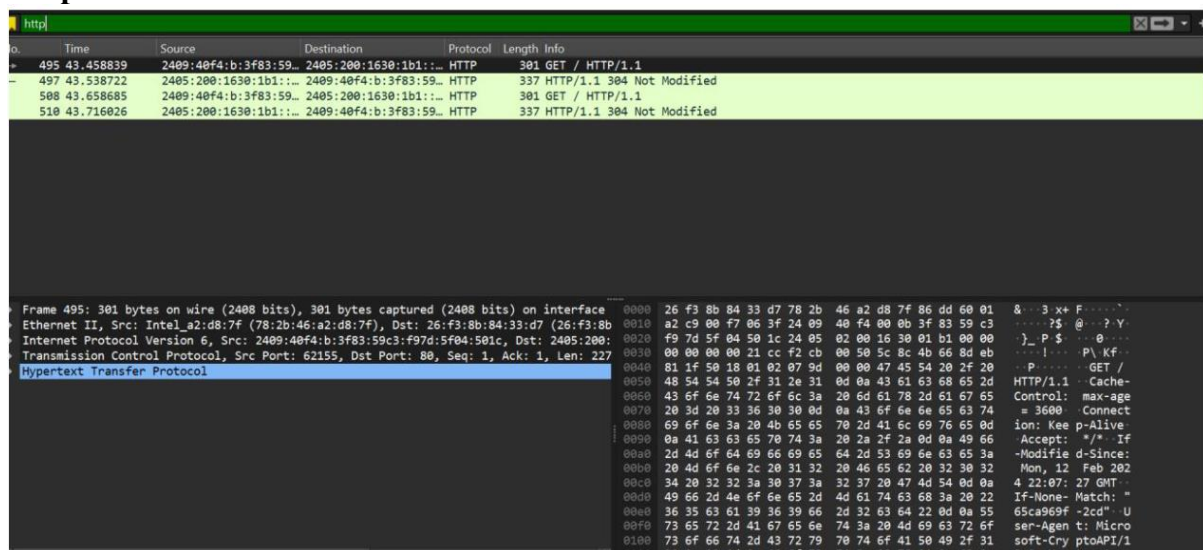


5.Create a Filter to display only HTTP packets and inspect the packets

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



Flow Graph output

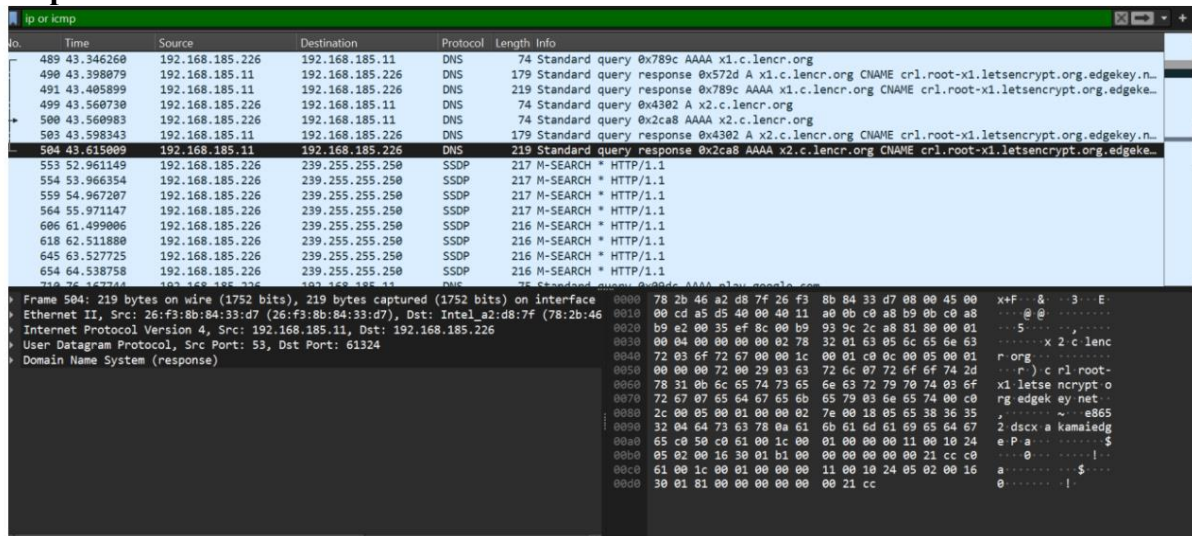


6. Create a Filter to display only IP/ICMP packets and inspect the packets.

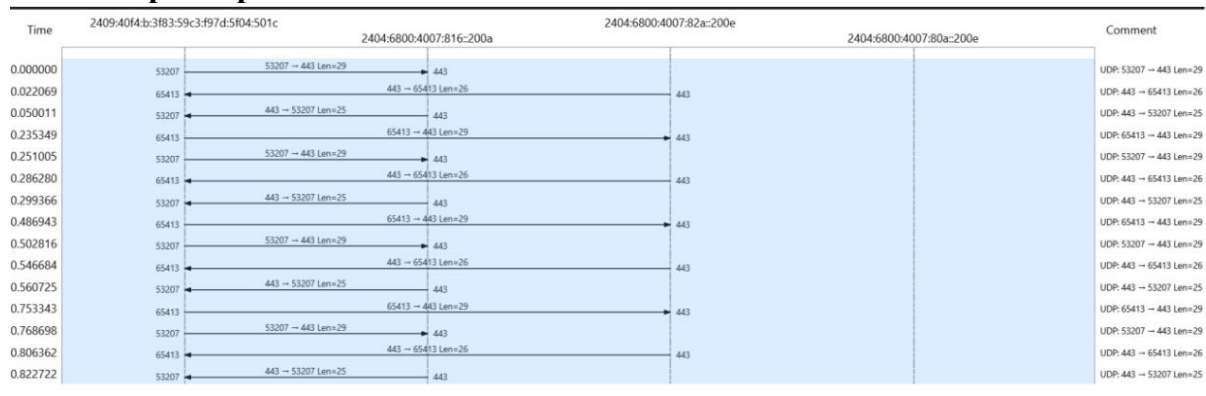
Procedure

- 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

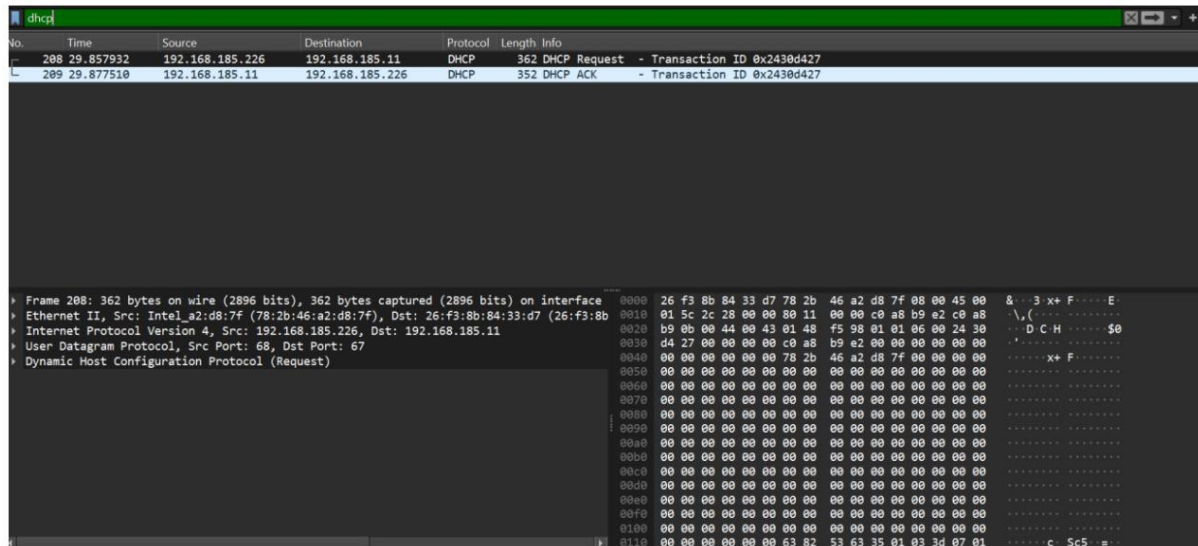


7. Create a Filter to display only DHCP packets and inspect the packets.

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



RESULT:

Hence,analyzing network traffic using Wireshark Tool is studied