

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

- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Save the packets.

[illegible][illegible]

CSE-CYBER SECURITY-2ND YEAR

- 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.

[illegible][illegible]

- 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.

CSE-CYBER SECURITY-2ND YEAR

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	WP_30-00-3d	Broadcast	ARP	00	who has 172.16.18.80? 172.16.18.172
2	0.001012	0x11:35:01:07	Broadcast	ARP	00	who has 172.16.18.240? 172.16.18.11,17
3	0.001094	0x11:35:01:0b	Broadcast	ARP	00	who has 172.16.18.180? 172.16.18.4
4	0.001096	0x11:35:01:0b	Broadcast	ARP	00	who has 172.16.18.24? 172.16.18.4
5	0.001426	0x11:35:01:07:04	Broadcast	ARP	00	who has 172.16.18.17? 172.16.18.11,184
6	0.002023	WP_30-00-3d	Broadcast	ARP	00	who has 172.16.18.81? 172.16.18.100
7	0.002786	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.16? 172.16.18.11,200
8	0.002798	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.87? 172.16.18.11,200
9	0.002827	0x11:35:01:07	Broadcast	ARP	00	who has 172.16.18.83? 172.16.18.100
10	0.002927	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.81? 172.16.18.114
11	0.003070	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.80? 172.16.18.1
12	0.003170	0x11:35:01:0b	Broadcast	ARP	00	who has 172.16.18.180? 172.16.18.212
13	0.003621	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.240? 172.16.18.1,204
14	0.003638	0x11:34:00:73	Broadcast	ARP	00	who has 172.16.18.110? 172.16.18.96
15	0.003637	0x11:34:00:73	Broadcast	ARP	00	who has 172.16.18.200? 172.16.18.1,47
16	0.003638	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.80? 172.16.18.62
17	0.003638	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.200? 172.16.18.62
18	0.003639	WP_30-00-3d	Broadcast	ARP	00	who has 172.16.18.80? 172.16.18.1,172
19	0.003639	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.70? 172.16.18.100
20	0.003647	WP_30-00-3d	Broadcast	ARP	00	who has 168.254.149.107? 172.16.18.1,176
21	0.003651	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.81? 172.16.18.114
22	0.003700	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.16? 172.16.18.200
23	0.003700	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.16? 172.16.18.200
24	0.003893	0x11:35:01:07	Broadcast	ARP	00	who has 172.16.18.83? 172.16.18.100
25	0.003959	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.180? 172.16.18.42
26	0.003961	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.80? 172.16.18.31
27	0.003970	0x11:34:00:73	Broadcast	ARP	00	who has 172.16.18.180? 172.16.18.96
28	0.003970	0x11:34:00:73	Broadcast	ARP	00	who has 172.16.18.200? 172.16.18.1,204
29	0.003970	0x11:34:00:73	Broadcast	ARP	00	who has 172.16.18.180? 172.16.18.96
30	0.003970	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.180? 172.16.18.96
31	0.003970	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.180? 172.16.18.212
32	0.003970	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.180? 172.16.18.1
33	0.003970	WP_30-00-3d	Broadcast	ARP	00	who has 168.254.149.107? 172.16.18.1,176
34	0.003970	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.16? 172.16.18.200
35	0.003970	0x01:00:0c:00:00:00:00:00	Broadcast	ARP	00	who has 172.16.18.16? 172.16.18.1,176

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

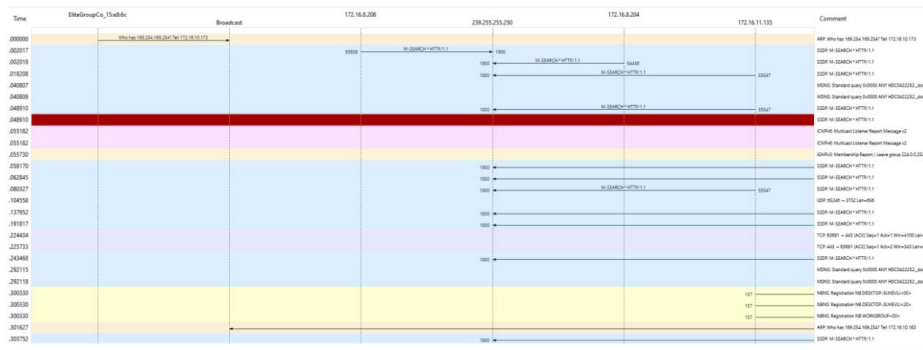
- Select Local Area Connection in Wireshark.
- Go to capture ☐ option
- Select stop capture automatically after 100 packets.
- Then click Start capture.
- Search DNS packets in search bar.
- To see flow graph click Statistics ☐ Flow graph.
- Save the packets.

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.epsloncdn.net A 152.199.43.62
517	6.1001578	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:57:58:35:00:00), Dst: Sophoscfbe45 (7c:5a:1c:cf:be:45)]	0000	Tc 5a 1c cf be 45 7c 57 58 35 05 05 00 00 00 00	[2] [N X5 ...]
Ethernet II, Src: WP_30-00-3d (7c:57:58:35:00:00), Dst: Sophoscfbe45 (7c:5a:1c:cf:be:45)	0010	00 4a f9 02 00 00 00 11 00 00 ac 10 00 03 ac 10	3
User Datagram Protocol, Src Port: 54158, Dst Port: 53	0020	00 01 03 0e 00 00 35 00 36 03 1c 01 04 01 00 00 015 4 1
Domain Name System (query)	0030	00 00 00 00 00 00 11 74 2f 72 05 0a 67 1d 66 01t-ring-fa
	0040	0c 6c 62 61 63 60 73 32 06 6d 73 65 64 67 65 03	llbacks2 msedge
	0050	0c 65 74 00 00 01 00 01	net

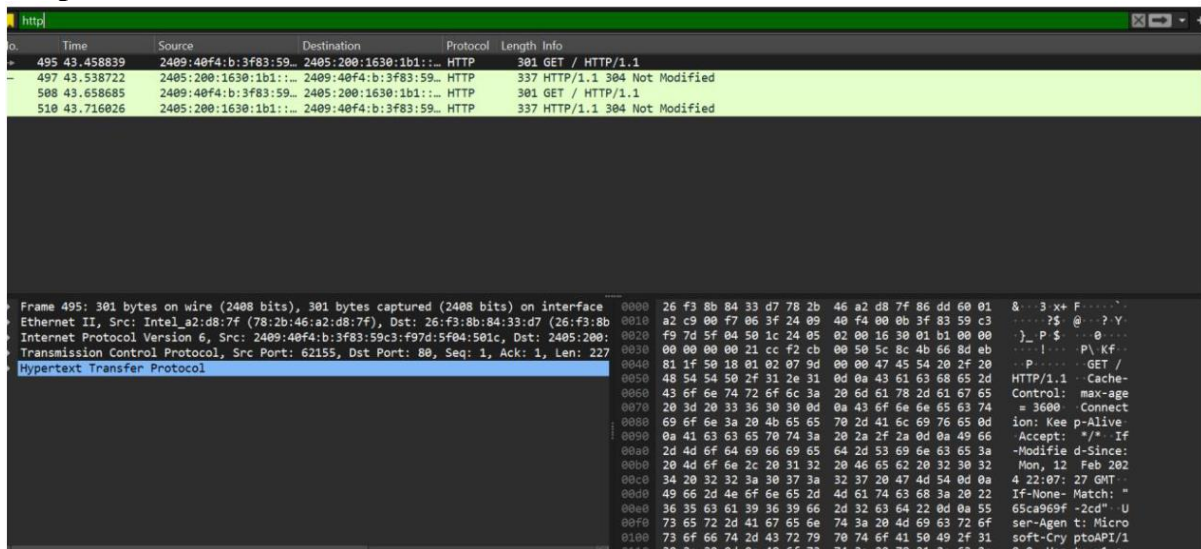
Flow Graph output



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



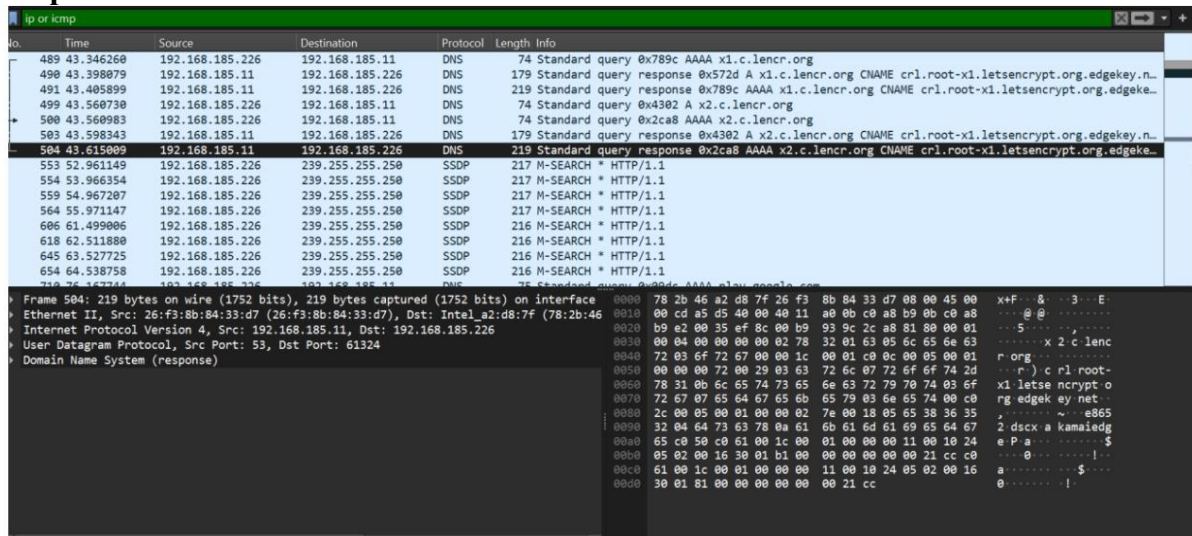
Flow Graph output



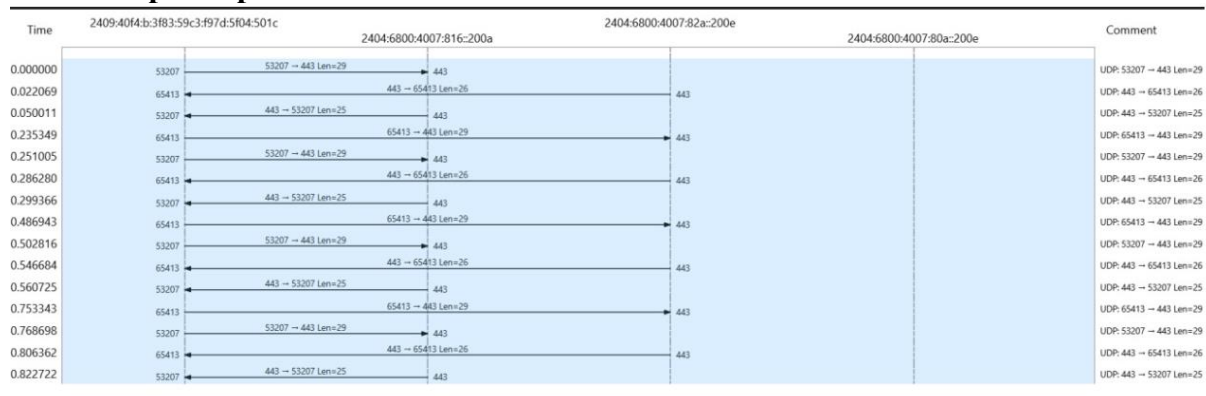
6. Create a Filter to display only IP/ICMP packets and inspect the packets. Procedure

- 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



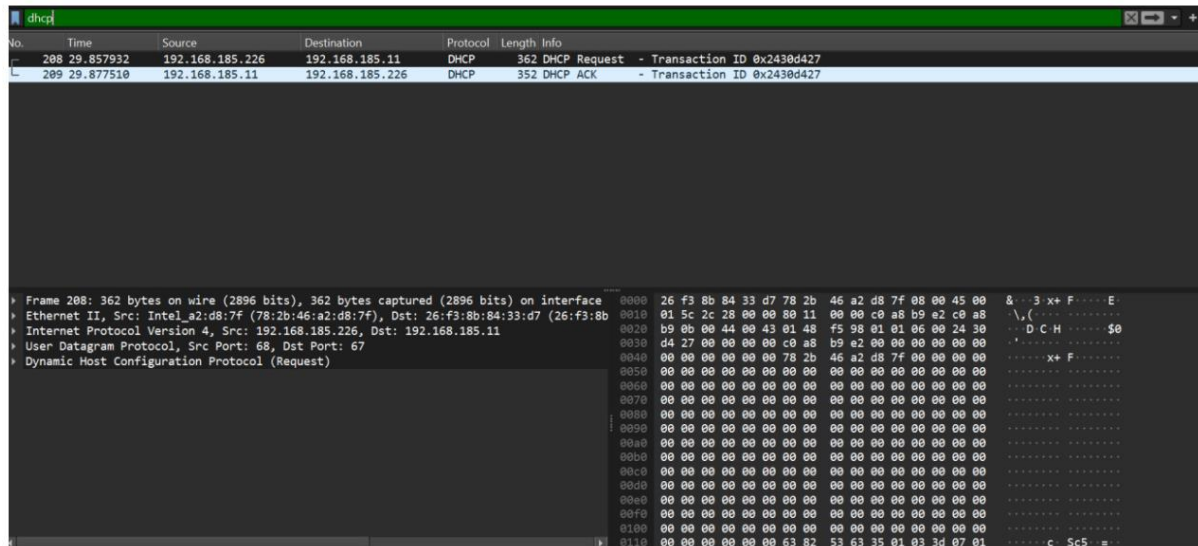
Flow Graph output



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