

Ex No: 14 b

PACKET SNIFFING USING WIRESHARK

Date : 14.8.2024


AIM:

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

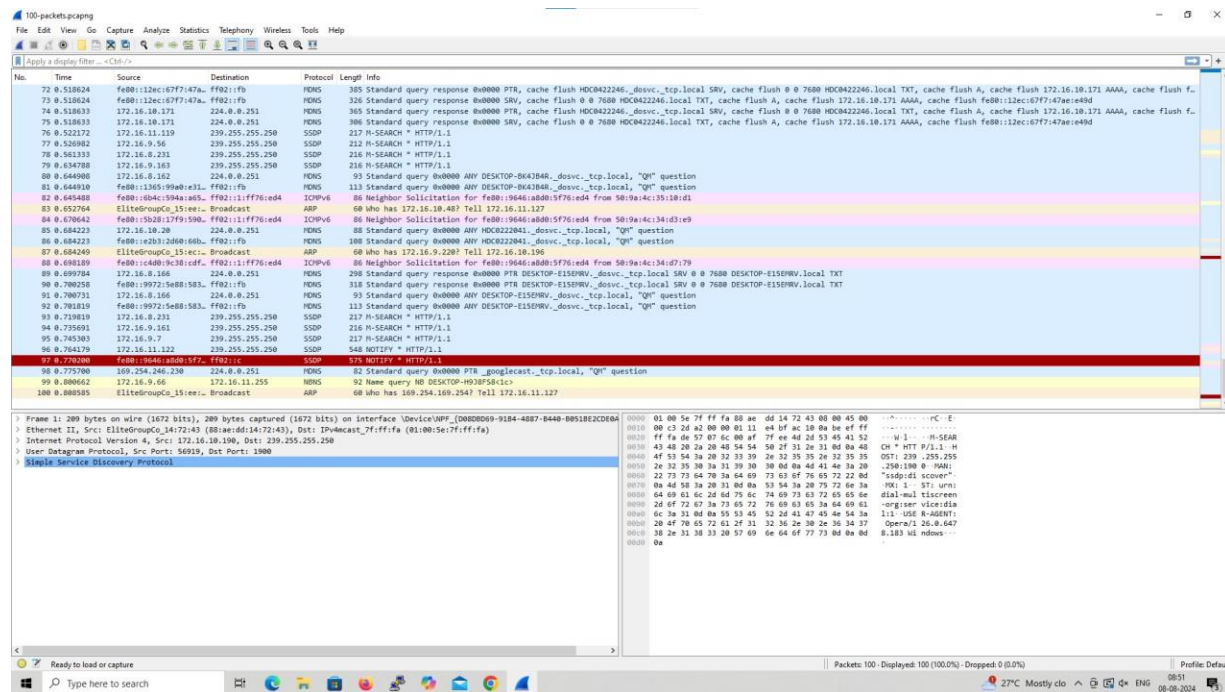
Exercises

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



100-packets.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter... 

No.	Time	Source	Destination	Protocol	Length	Info
72	0.518624	fe80::12ec:e77f:47a...:ff02::fb	ff02::fb	RDNS	365	Standard query response 0x0000 PTR, cache flush HDCM22246..._dosvc_tcp.local SRV, cache flush 0 0 7680 HDCM22246.local TXT, cache flush 172.16.10.171 AAAA, cache flush f...
73	0.518624	fe80::12ec:e77f:47a...:ff02::fb	ff02::fb	RDNS	326	Standard query response 0x0000 PTR, cache flush 0 0 7680 HDCM22246.local TXT, cache flush 172.16.10.171 AAAA, cache flush fe80::12ec:e77f:47a:e49d
74	0.518633	172.16.10.171	224.0.0.251	RDNS	365	Standard query response 0x0000 PTR, cache flush HDCM22246..._dosvc_tcp.local SRV, cache flush 0 0 7680 HDCM22246.local TXT, cache flush 172.16.10.171 AAAA, cache flush f...
75	0.518633	172.16.10.171	224.0.0.251	RDNS	386	Standard query response 0x0000 SRV, cache flush 0 0 7680 HDCM22246.local TXT, cache flush A, cache flush 172.16.10.171 AAAA, cache flush fe80::12ec:e77f:47a:e49d
76	0.520172	172.16.11.119	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
77	0.520182	172.16.9.56	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
78	0.561333	172.16.8.231	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
79	0.634780	172.16.9.163	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
80	0.644980	172.16.9.162	224.0.0.251	RDNS	93	Standard query 0x0000 ANY DESKTOP-0643B48..._dosvc_tcp.local, "Q" question
81	0.644918	fe80::1365:99a8:e31...:ff02::fb	ff02::fb	RDNS	113	Standard query 0x0000 ANY DESKTOP-0643B48..._dosvc_tcp.local, "Q" question
82	0.645480	fe80::0b4c:59a4:a65...:ff02::1:ff76::ed4	ff02::1:ff76::ed4	ICMPv6	86	Neighbor Solicitation for fe80::9646:ad88:5f76::ed4 from 58:9a:4c:35:18:d1
83	0.652764	ff1fe900c0:35:ee::	Broadcast	ARP	68	Who has 172.16.10.40? Tell 172.16.11.127
84	0.670642	fe80::9b20:1379:590...:ff02::1:ff76::ed4	ff02::1:ff76::ed4	ICMPv6	86	Neighbor Solicitation for fe80::9646:ad88:5f76::ed4 from 58:9a:4c:34:d3:e9
85	0.684223	172.16.10.20	224.0.0.251	RDNS	88	Standard query 0x0000 ANY HCR222841..._dosvc_tcp.local, "Q" question
86	0.684223	fe80::c203:2060:660...:ff02::fb	ff02::fb	RDNS	188	Standard query 0x0000 ANY HCR222841..._dosvc_tcp.local, "Q" question
87	0.684249	ff1fe900c0:35:ee::	Broadcast	ARP	68	Who has 172.16.9.220? Tell 172.16.10.196
88	0.690189	fe80::c400:0c3b:cdf...:ff02::1:ff76::ed4	ff02::1:ff76::ed4	ICMPv6	86	Neighbor Solicitation for fe80::9646:ad88:5f76::ed4 from 58:9a:4c:34:d7:79
89	0.699784	172.16.8.166	224.0.0.251	RDNS	290	Standard query response 0x0000 PTR DESKTOP-E150RW..._dosvc_tcp.local SRV 0 0 7680 DESKTOP-E150RW.local TXT
90	0.700258	fe80::9972:5e88:583...:ff02::fb	ff02::fb	RDNS	318	Standard query response 0x0000 PTR DESKTOP-E150RW..._dosvc_tcp.local SRV 0 0 7680 DESKTOP-E150RW.local TXT
91	0.700731	172.16.8.166	224.0.0.251	RDNS	93	Standard query 0x0000 ANY DESKTOP-E150RW..._dosvc_tcp.local, "Q" question
92	0.701819	fe80::9972:5e88:583...:ff02::fb	ff02::fb	RDNS	113	Standard query 0x0000 ANY DESKTOP-E150RW..._dosvc_tcp.local, "Q" question
93	0.725819	172.16.8.231	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
94	0.735991	172.16.9.161	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
95	0.745303	172.16.9.7	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
96	0.764376	172.16.11.122	239.255.255.250	SSDP	540	NOTIFY * HTTP/1.1
97	0.776104	fe80::9646:ad88:5f7...:ff02::1	ff02::1	SSDP	575	NOTIFY * HTTP/1.1
98	0.775790	169.254.246.238	224.0.0.251	RDNS	82	Standard query 0x0000 PTR _googlecast_tcp.local, "Q" question
99	0.800662	172.16.9.66	172.16.11.255	RDNS	92	Name query NO DESKTOP-H9JF58:io
100	0.800585	ff1fe900c0:35:ee::	Broadcast	ARP	68	Who has 169.254.169.254? Tell 172.16.11.127

Frame 1: 289 bytes on wire (1672 bits), 289 bytes captured (1672 bits) on Interface \Device\NPF_{D080D09-9104-4887-B440-80518E2C2D04} (0:00:00:00:00:00:00:00)

Ethernet II, Src: ElliteGroupC_35:ee:: (88:ae:8d:14:72:43), Dst: Dpbcast7f:ff:fa (01:00:5e:7f:ff:fa)

Internet Protocol Version 4, Src: 172.16.10.196, Dst: 239.255.255.250

User Datagram Protocol, Src Port: 56919, Dst Port: 1900

Simple Service Discovery Protocol

0000 01 00 5e 7f ff fa 08 ae d4 72 43 00 00 45 00 ... PC-E

0001 00 c3 26 a2 00 00 02 11 e4 0f ac 10 0a be ef ff ... W-1 ... M-SEAR

0002 ff fa d4 57 07 0c 00 af 7f ee 4d 28 53 45 41 52 ... M-ATT P/1.1 R

0003 43 40 20 2a 20 40 54 54 50 2f 31 2e 31 0d 0a 40 ... CH * HTTP/1.1 R

0004 4f 53 54 3a 20 32 33 39 2e 32 35 26 32 35 35 ... OST: 239.255.255

0005 2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20 ... 250:1900 0 -RAN:

0006 22 73 4a 70 3a 64 69 73 63 0f 76 65 72 22 bd ... "ndp:d4:accon"

0007 0a 4d 50 3a 20 31 0d 0a 53 54 3a 20 75 72 6a 3a ... PK: 1 - ST: urn:

0008 04 69 61 6c 20 6d 75 6c 74 69 73 63 72 65 65 6e ... dial-mul tiscrem

0009 2d 6f 72 63 3a 73 65 72 76 69 63 65 3a 64 69 63 ... -org: user vici:da

000a 0c 3a 31 0d 0a 55 53 45 52 2d 41 47 45 4e 54 3a ... lit: USE R-AGENT:

000b 20 4f 70 65 72 61 2f 31 32 36 2e 30 2e 36 34 37 ... Operat: 126.0.647

000c 38 2e 31 38 33 20 57 69 6e 64 6f 77 73 0d 0a bd ... 8.183 ki ndous:

000d 0a



Packets: 100 - Displayed: 100 (100.0%) - Dropped: 0 (0.0%)

Profile: Default

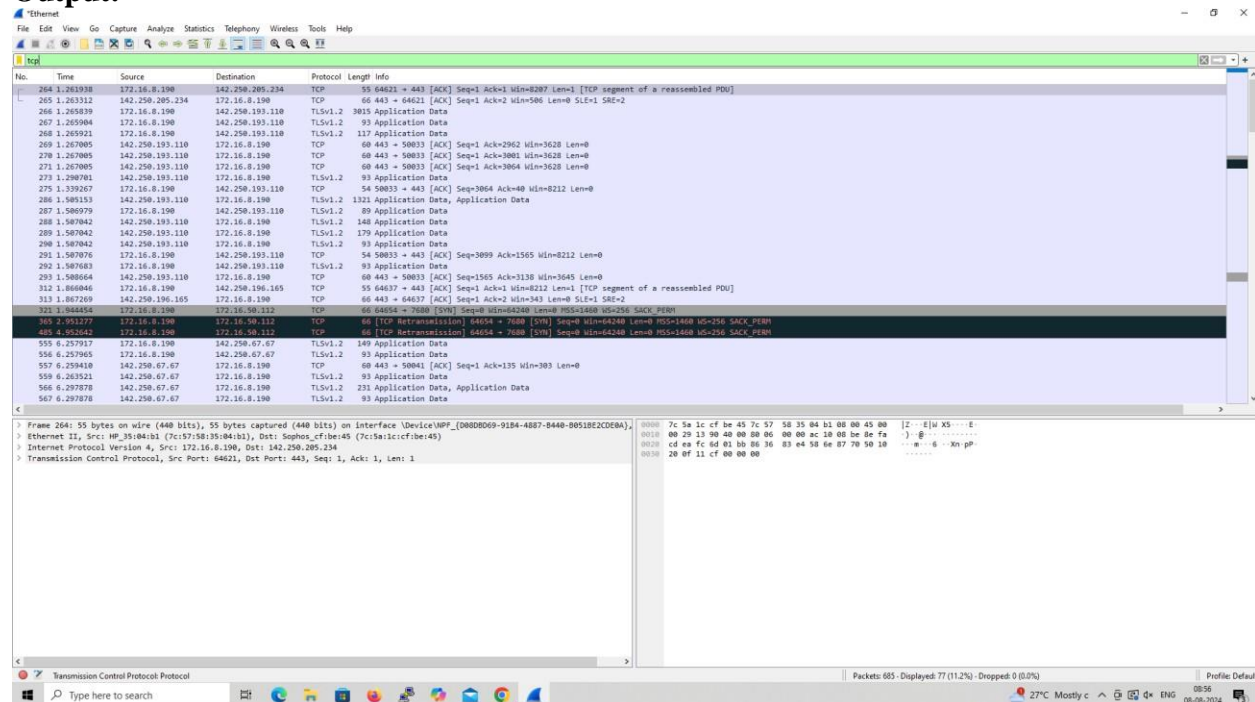
27°C Mostly clo ENG 08:51 08-08-2024

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 network capture. The packet list on the left shows several TCP segments. The packet details pane on the right shows the structure of a selected TCP segment, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Packet List (Selected Packet 65):

No.	Time	Source	Destination	Protocol	Length	Info
264	1.265938	172.16.8.190	142.250.205.234	TCP	55	64621 → 443 [ACK] Seq=1 Ack=1 Win=8287 Len=0 [TCP segment of a reassembled PDU]
265	1.265938	142.250.205.234	172.16.8.190	TCP	66	443 → 64621 [ACK] Seq=1 Ack=2 Win=586 Len=0 SLE=1 SRE=2
266	1.265939	172.16.8.190	142.250.193.110	TLSv1.2	3815	Application Data
267	1.265940	172.16.8.190	142.250.193.110	TLSv1.2	93	Application Data
268	1.265921	172.16.8.190	142.250.193.110	TLSv1.2	127	Application Data
269	1.267005	142.250.193.110	172.16.8.190	TCP	60	443 → 50033 [ACK] Seq=1 Ack=2962 Win=3628 Len=0
270	1.267005	142.250.193.110	172.16.8.190	TCP	60	443 → 50033 [ACK] Seq=1 Ack=3062 Win=3628 Len=0
271	1.267005	142.250.193.110	172.16.8.190	TCP	60	443 → 50033 [ACK] Seq=1 Ack=3064 Win=3628 Len=0
273	1.290761	142.250.193.110	172.16.8.190	TLSv1.2	93	Application Data
275	1.339267	172.16.8.190	142.250.193.110	TCP	54	50033 → 443 [ACK] Seq=3064 Ack=40 Win=8212 Len=0
286	1.580153	142.250.193.110	172.16.8.190	TLSv1.2	1321	Application Data, Application Data
287	1.580979	172.16.8.190	142.250.193.110	TLSv1.2	89	Application Data
288	1.580942	142.250.193.110	172.16.8.190	TLSv1.2	148	Application Data
289	1.580942	142.250.193.110	172.16.8.190	TLSv1.2	179	Application Data
290	1.580942	142.250.193.110	172.16.8.190	TLSv1.2	93	Application Data
291	1.580976	172.16.8.190	142.250.193.110	TCP	54	50033 → 443 [ACK] Seq=3099 Ack=1565 Win=8212 Len=0
292	1.580983	172.16.8.190	142.250.193.110	TLSv1.2	93	Application Data
293	1.580964	142.250.193.110	172.16.8.190	TCP	60	443 → 50033 [ACK] Seq=1565 Ack=3138 Win=3645 Len=0
312	1.860846	172.16.8.190	142.250.196.165	TCP	55	64637 → 443 [ACK] Seq=1 Ack=1 Win=8212 Len=0 [TCP segment of a reassembled PDU]
313	1.087269	142.250.196.165	172.16.8.190	TCP	66	443 → 64637 [ACK] Seq=1 Ack=2 Win=345 Len=0 SLE=1 SRE=2
315	1.584656	172.16.8.190	172.16.50.132	TCP	66	64654 → 7080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM
365	9.951277	172.16.8.190	172.16.50.132	TCP	66	[TCP Retransmission] 64654 → 7080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM
43	6.485242	172.16.8.190	172.16.50.132	TCP	66	[TCP Retransmission] 64654 → 7080 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 S=256 SACK_PERM
555	6.257917	172.16.8.190	142.250.67.67	TLSv1.2	140	Application Data
556	6.257965	172.16.8.190	142.250.67.67	TLSv1.2	93	Application Data
557	6.259410	142.250.67.67	172.16.8.190	TCP	60	443 → 50041 [ACK] Seq=1 Ack=135 Win=363 Len=0
558	6.261521	142.250.67.67	172.16.8.190	TLSv1.2	93	Application Data
566	6.297878	142.250.67.67	172.16.8.190	TLSv1.2	231	Application Data, Application Data
567	6.297878	142.250.67.67	172.16.8.190	TLSv1.2	93	Application Data

Packet Details (Selected Packet 65):

- Ethernet II, Src: HP_35:84:b1 (7c:57:58:35:84:b1), Dst: Sophos_fiber45 (7c:5a:1c:cf:be:45)
- Internet Protocol Version 4, Src: 172.16.8.190, Dst: 142.250.205.234
- Transmission Control Protocol, Src Port: 64621, Dst Port: 443, Seq: 1, Len: 1

Packet Bytes (Selected Packet 65):

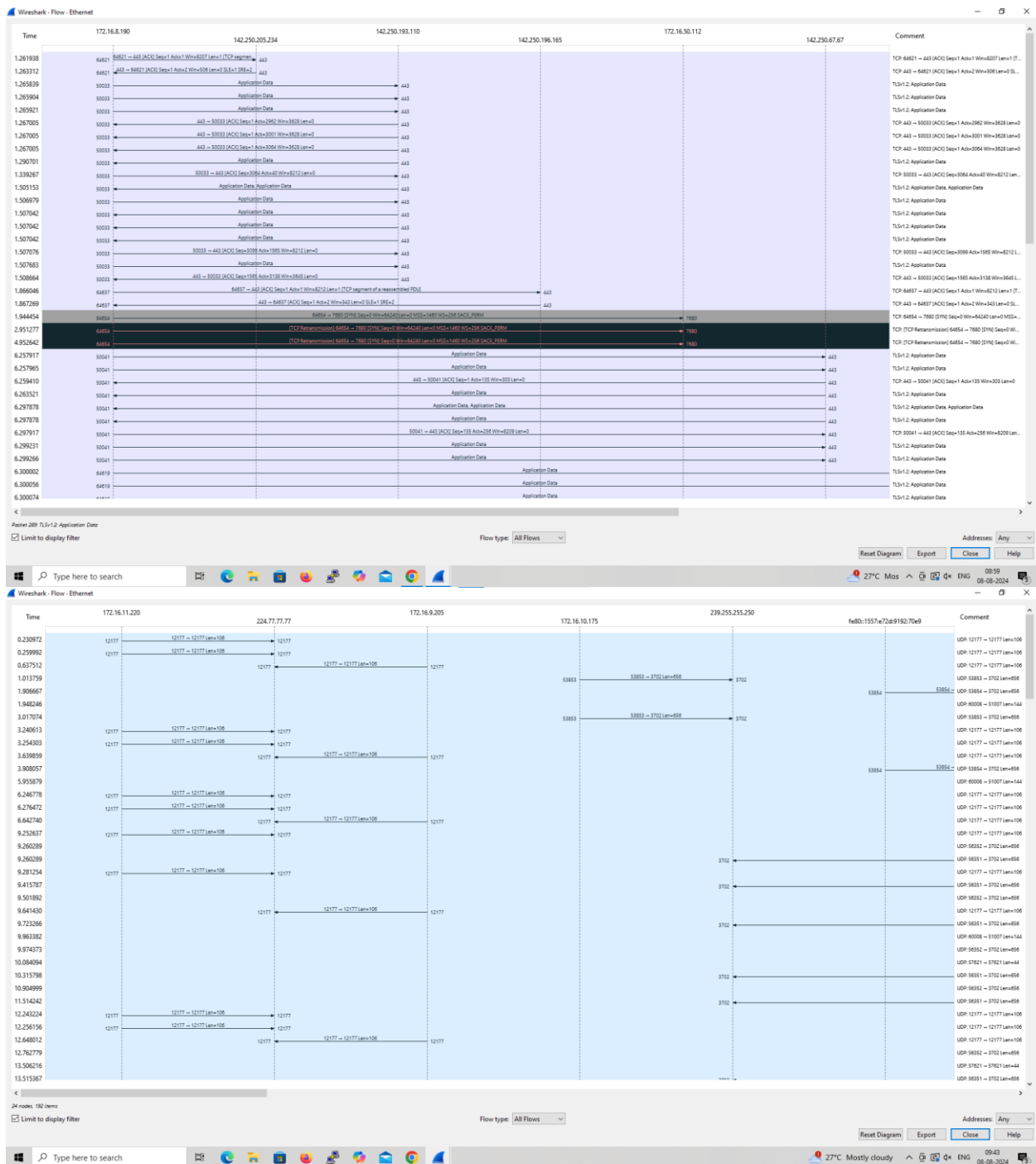
```

0000  7c 5a 1c cf be 45 7c 57 58 35 84 b1 08 00 45 00  |Z...E|X5...8
0010  00 29 13 99 40 00 00 06 00 00 ac 10 08 0e be fa  |...9...99...00
0020  cd ea fc 6d 81 30 88 36 83 e4 58 6e 87 70 50 18  |...d...f...6...Xn p
0030  20 ff 11 cf 00 00 00                                |...0...0...0...
  
```

Wireshark packet capture showing UDP traffic. The packet list on the left shows a series of UDP packets from 172.16.11.220 to 224.77.77.77. The packet details pane on the right shows the structure of a UDP packet, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.


Wireshark packet capture showing Ethernet traffic. The packet list on the left shows a series of Ethernet packets from 172.16.9.74 to 172.16.11.255. The packet details pane on the right shows the structure of an Ethernet packet, including Ethernet II, Internet Protocol Version 4, and User Datagram Protocol. The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII.

Flow Graph output

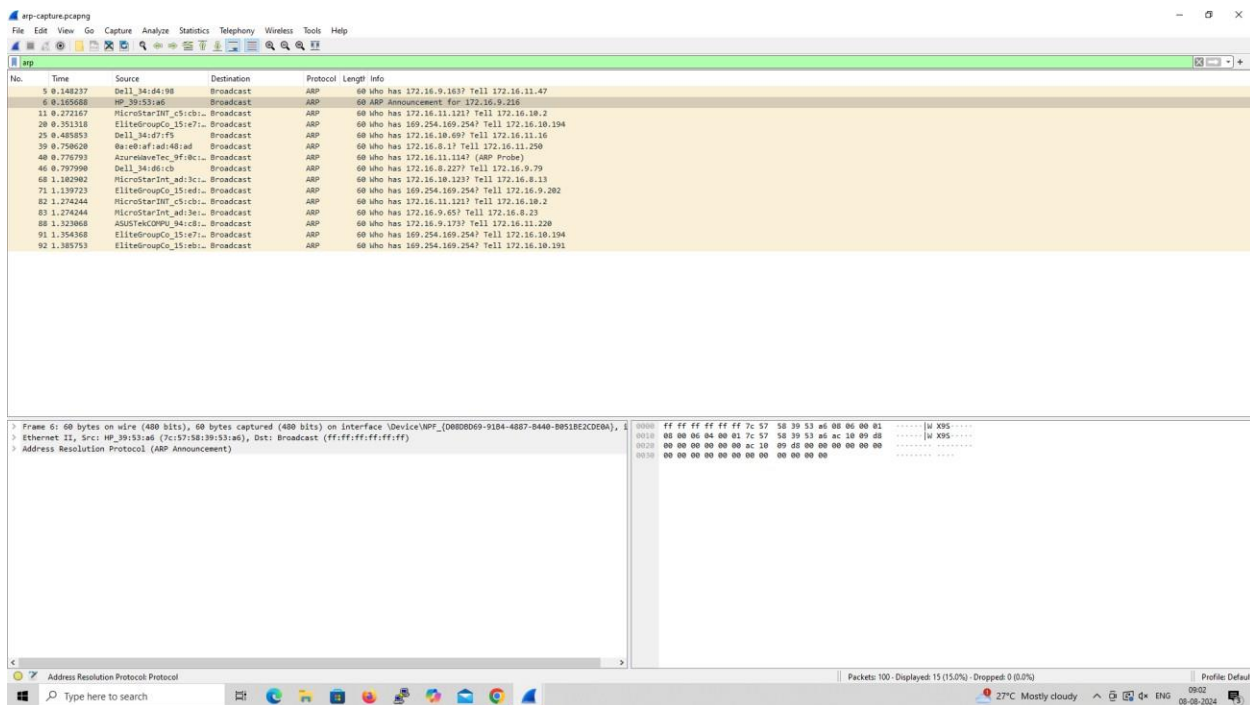


3. Create a Filter to display only ARP packets and inspect the packets.

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

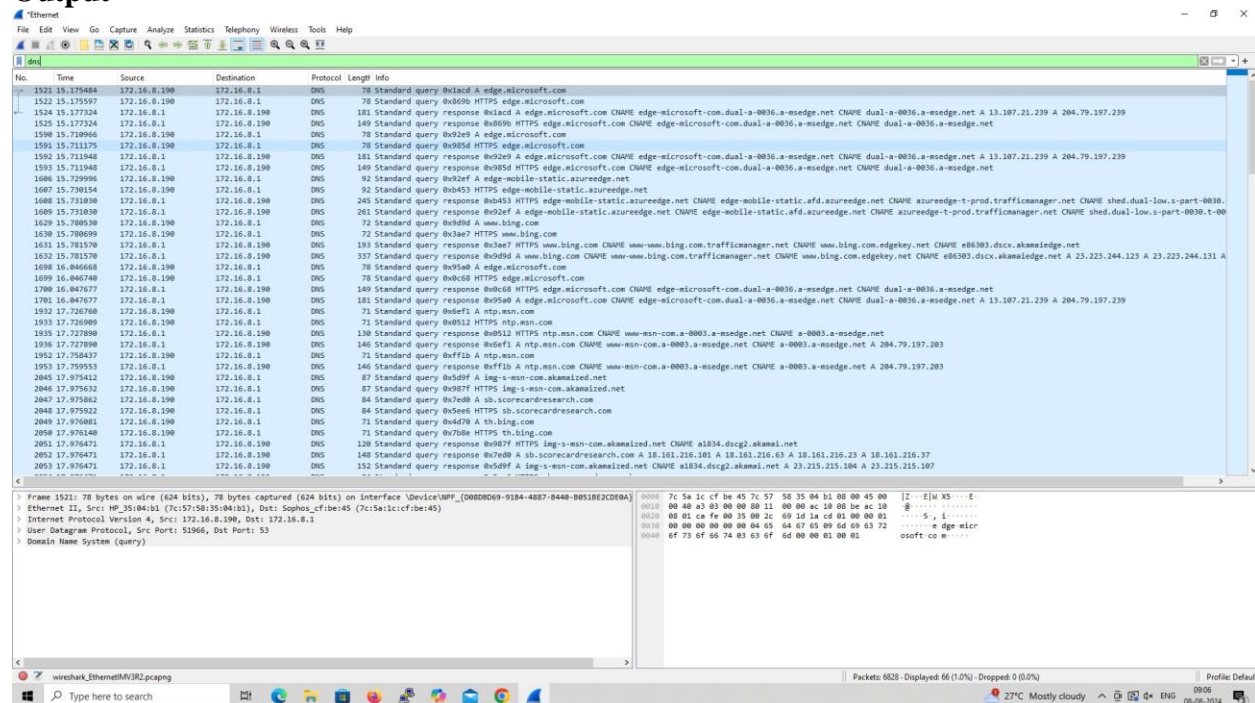


4. Create a Filter to display only DNS packets and provide the flow graph.

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



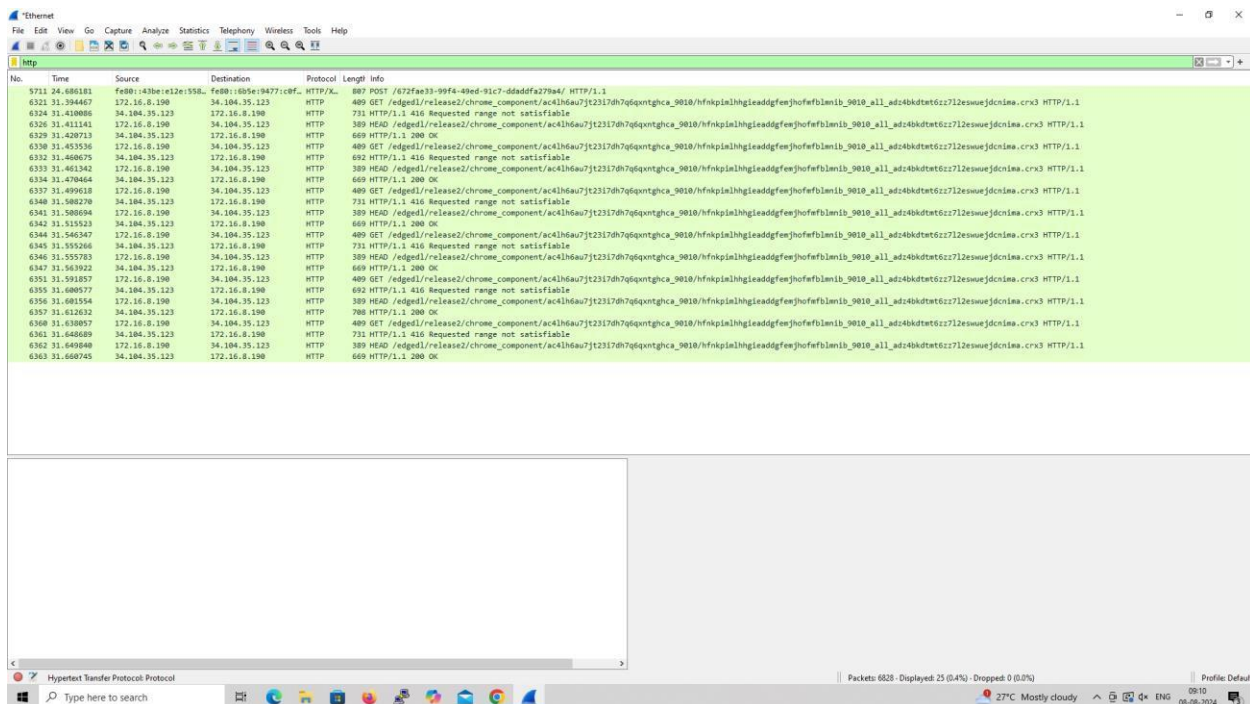
[illegible]

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

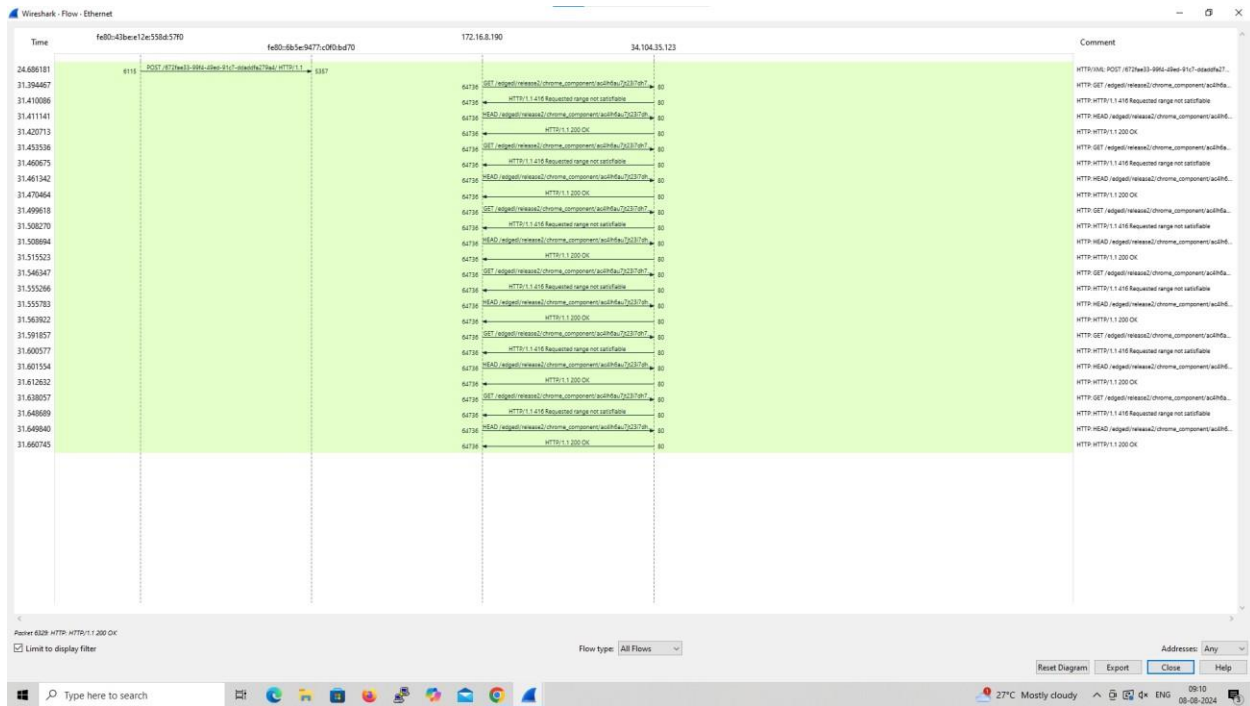
Procedure

- 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

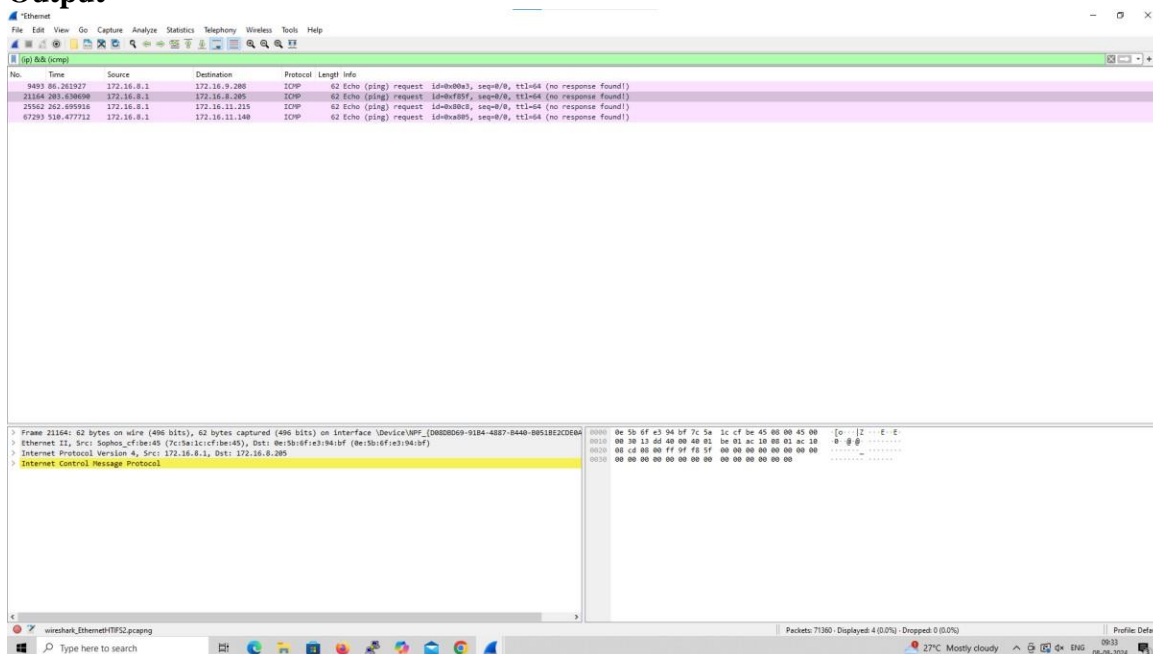


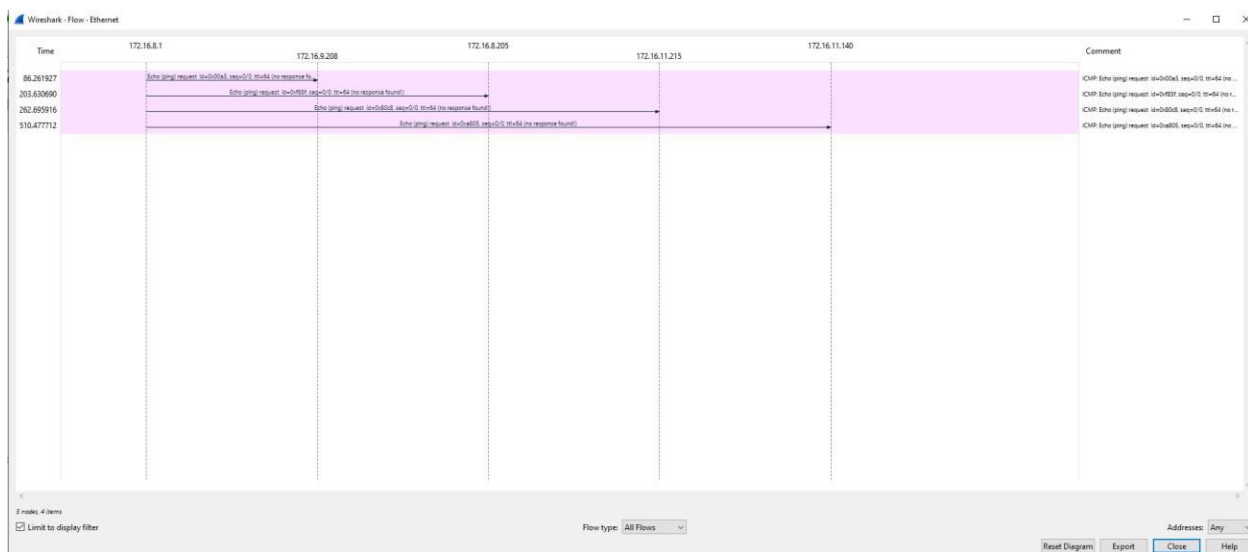
6. Create a Filter to display only IP/ICMP packets and inspect the packets.

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







CSE(Cybersecurity) 2nd year