231901015 JAYGANESH KANNAN Date: 13.8.24

Ex No: 4a STUDY OF WIRESHARK TOOL FOR PACKET SNIFFING

AIM:

To study packet sniffing concepts using Wireshark Tool.

DESCRIPTION:

Wireshark, a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format. Wireshark includes filters, color coding, and other features that let you dig deep into network traffic and inspect individual packets. You can use Wireshark to inspect a suspicious program's network traffic, analyze the traffic flow on your network, or troubleshoot network problems.

What we can do with Wireshark:

- Capture network traffic
- Decode packet protocols using dissectors
- Define filters – capture and display
- Watch smart statistics
- Analyze problems
- Interactively browse that traffic

Wireshark used for:

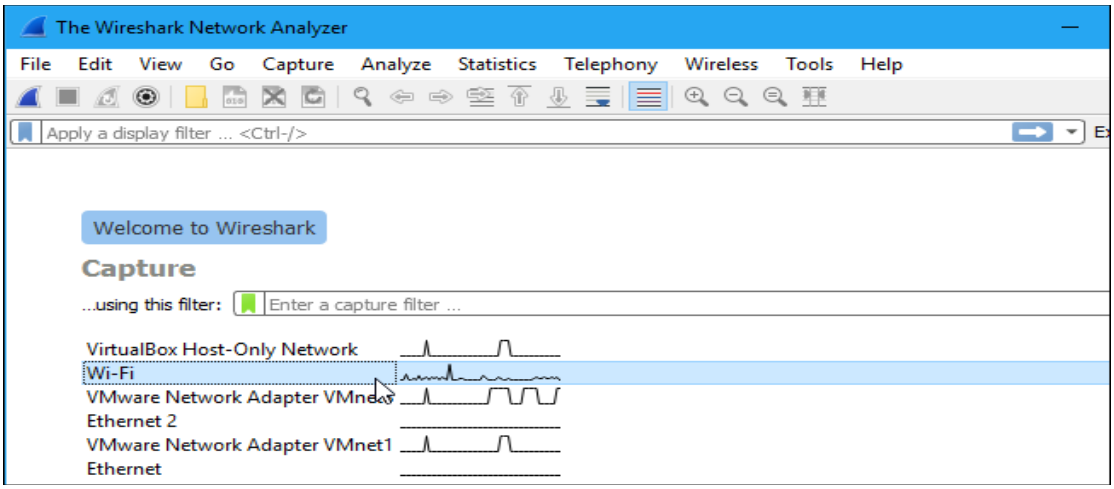
- Network administrators: troubleshoot network problems
- Network security engineers: examine security problems
- Developers: debug protocol implementations
- People: learn **network protocol internals**

Getting Wireshark

Wireshark can be downloaded for Windows or macOS from its official website. For Linux or another UNIX-like system, Wireshark will be found in its package repositories. For Ubuntu, Wireshark will be found in the Ubuntu Software Center.

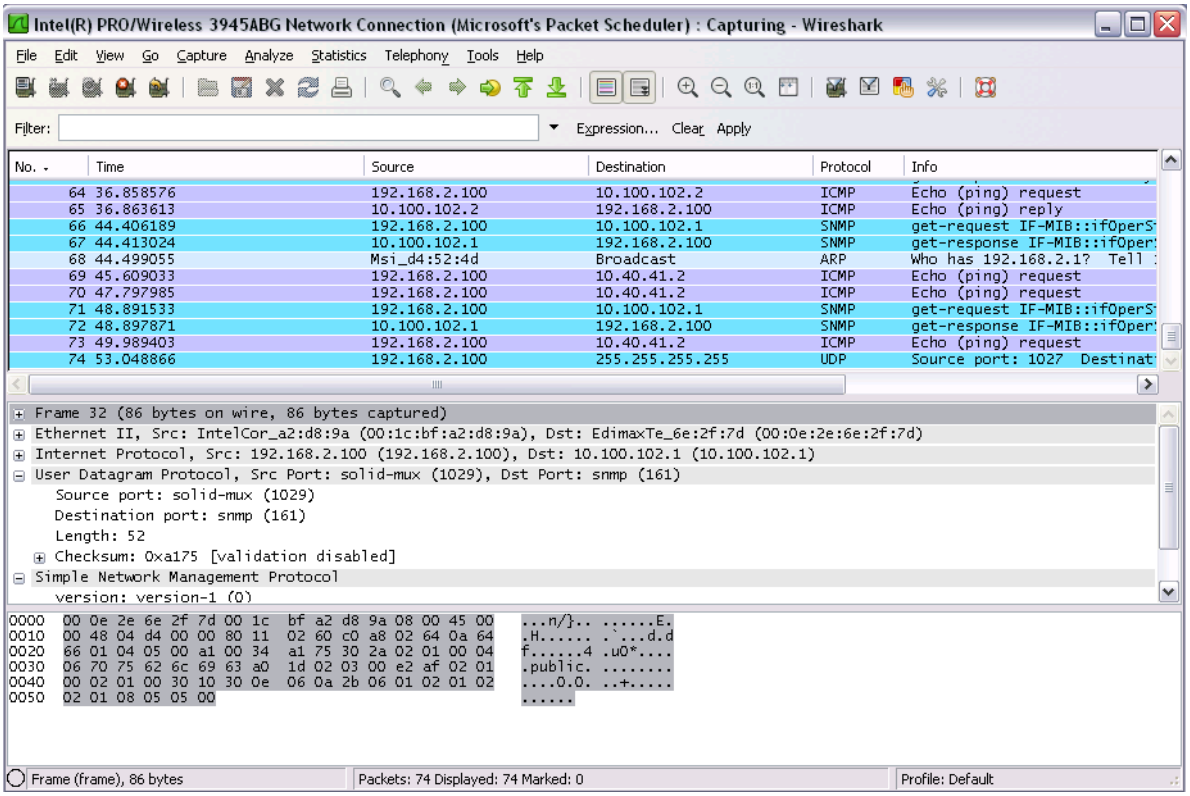
Capturing Packets

After downloading and installing Wireshark, launch it and double-click the name of a network interface under Capture to start capturing packets on that interface



As soon as you click the interface's name, you'll see the packets start to appear in real time. Wireshark captures each packet sent to or from your system.

If you have promiscuous mode enabled—it's enabled by default—you'll also see all the other packets on the network instead of only packets addressed to your network adapter. To check if promiscuous mode is enabled, click Capture > Options and verify the "Enable promiscuous mode on all interfaces" checkbox is activated at the bottom of this window.



Click the red “Stop” button near the top left corner of the window when you want to stop capturing traffic.

The “Packet List” Pane

The packet list pane displays all the packets in the current capture file. The “Packet List” pane Each line in the packet list corresponds to one packet in the capture file. If you select a line in this pane, more details will be displayed in the “Packet Details” and “Packet Bytes” panes.

The “Packet Details” Pane

The packet details pane shows the current packet (selected in the “Packet List” pane) in a more detailed form. This pane shows the protocols and protocol fields of the packet selected in the “Packet List” pane. The protocols and fields of the packet shown in a tree which can be expanded and collapsed.

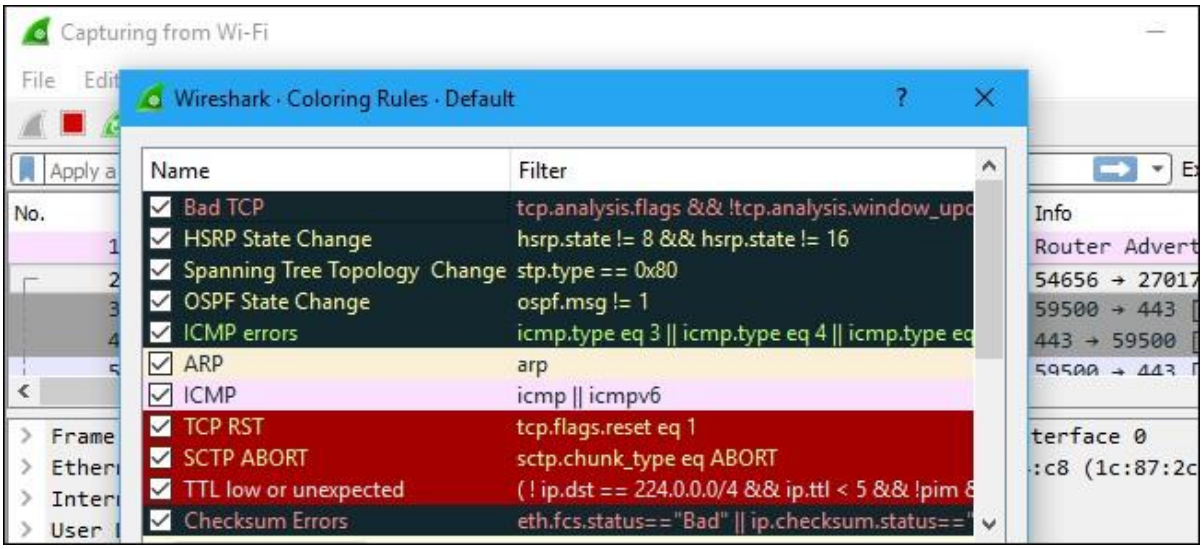
The “Packet Bytes” Pane

The packet bytes pane shows the data of the current packet (selected in the “Packet List” pane) in a hexdump style.

Color Coding

You’ll probably see packets highlighted in a variety of different colors. Wireshark uses colors to help you identify the types of traffic at a glance. By default, light purple is TCP traffic, light blue is UDP traffic, and black identifies packets with errors—for example, they could have been delivered out of order.

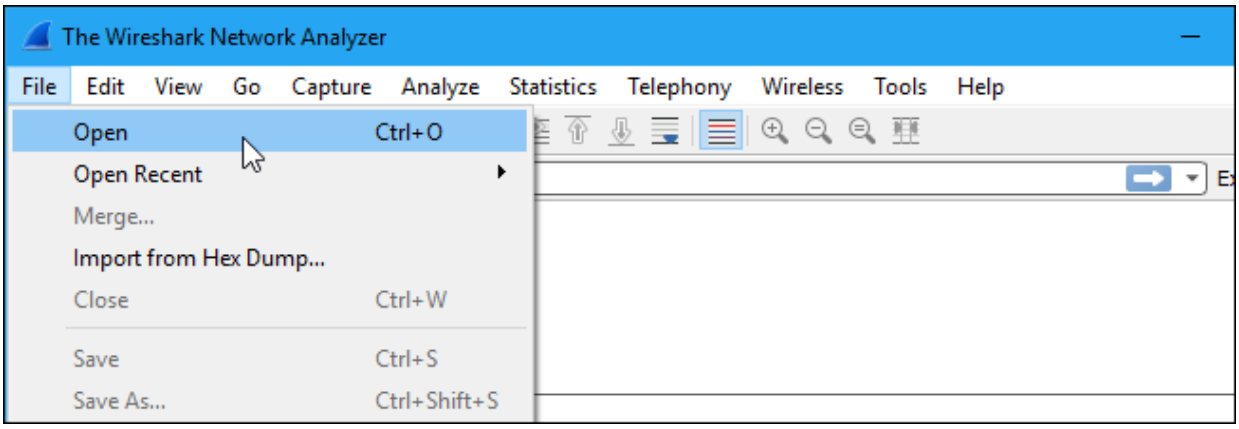
To view exactly what the color codes mean, click View > Coloring Rules. You can also customize and modify the coloring rules from here, if you like.



Sample Captures

If there's nothing interesting on your own network to inspect, Wireshark's wiki has you covered. The wiki contains a page of sample capture files that you can load and inspect. Click File > Open in Wireshark and browse for your downloaded file to open one.

You can also save your own captures in Wireshark and open them later. Click File > Save to save your captured packets.

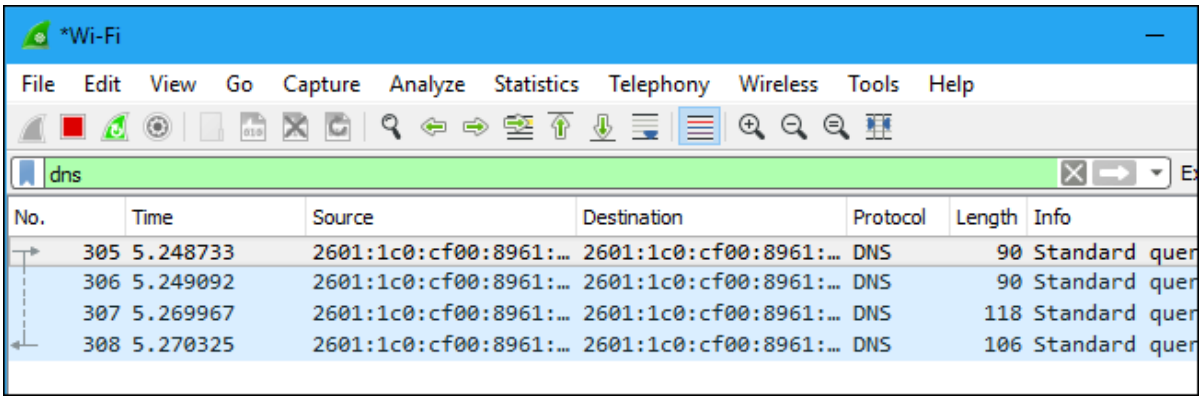


Filtering Packets

If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the

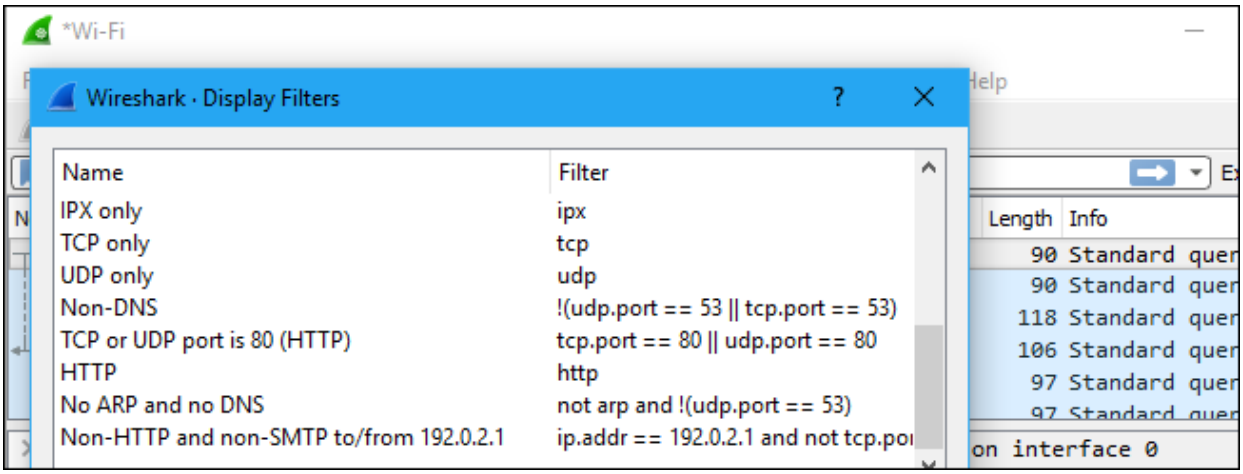
traffic. Still, you'll likely have a large amount of packets to sift through. That's where Wireshark's filters come in.

The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "dns" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.



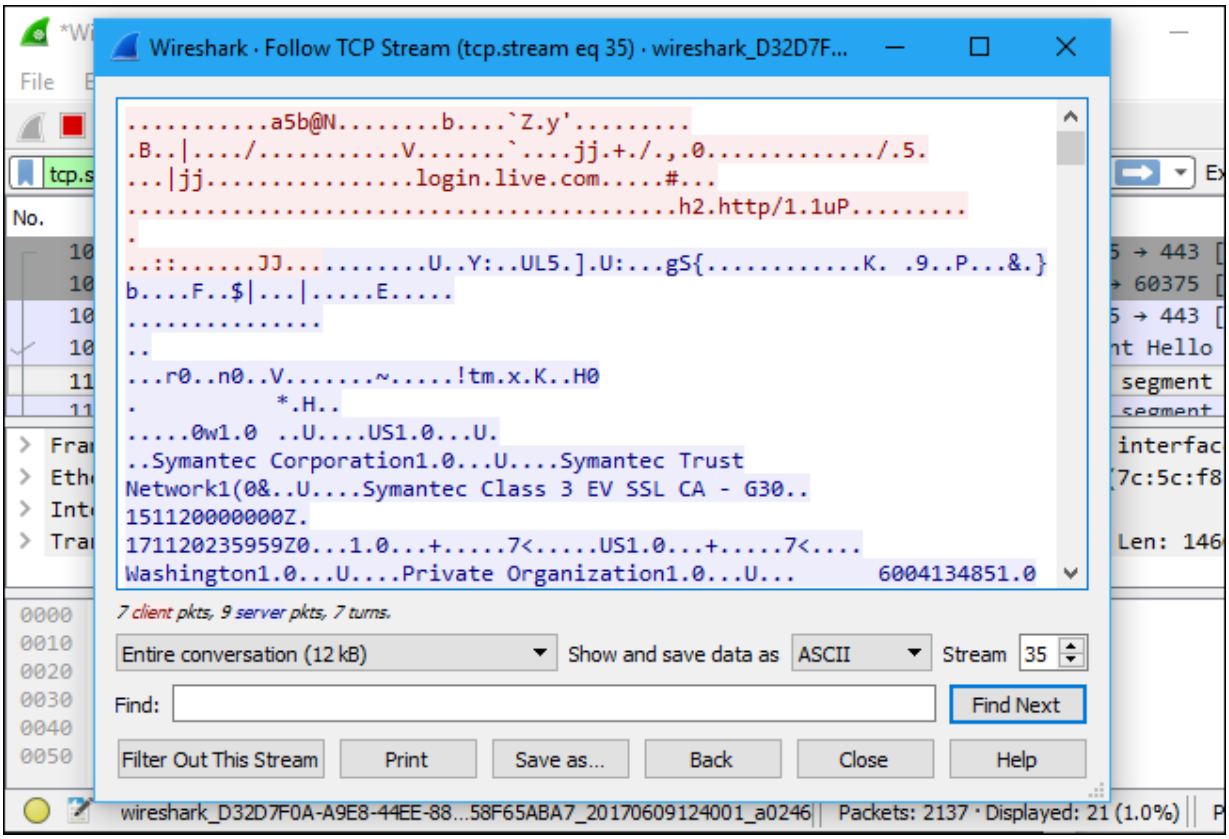
You can also click Analyze > Display Filters to choose a filter from among the default filters included in Wireshark. From here, you can add your own custom filters and save them to easily access them in the future.

For more information on Wireshark's display filtering language, read the Building display filter expressions page in the official Wireshark documentation.

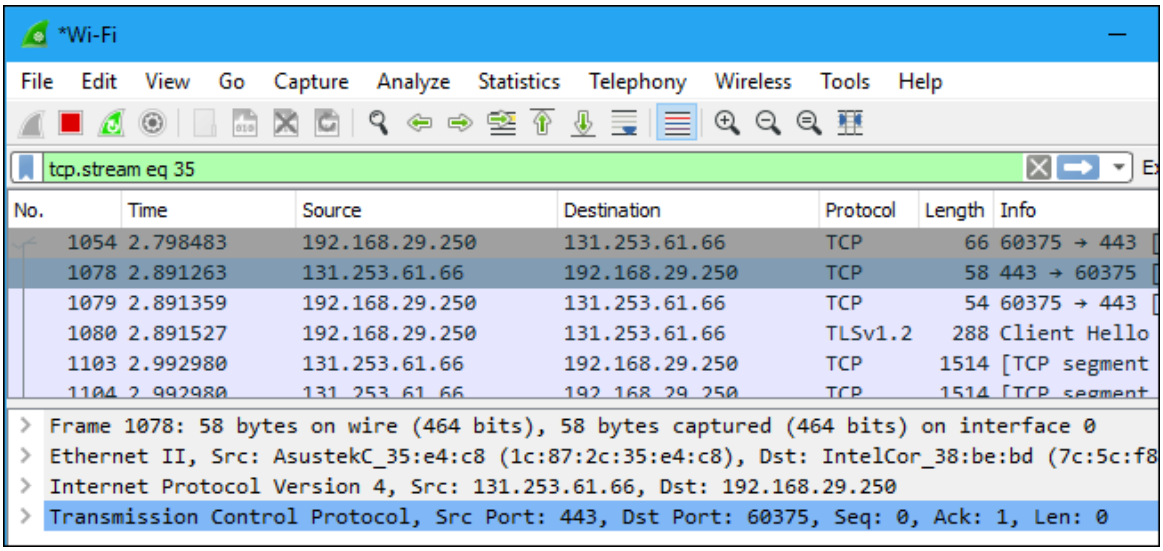


Another interesting thing you can do is right-click a packet and select Follow > TCP Stream.

You'll see the full TCP conversation between the client and the server. You can also click other protocols in the Follow menu to see the full conversations for other protocols, if applicable.

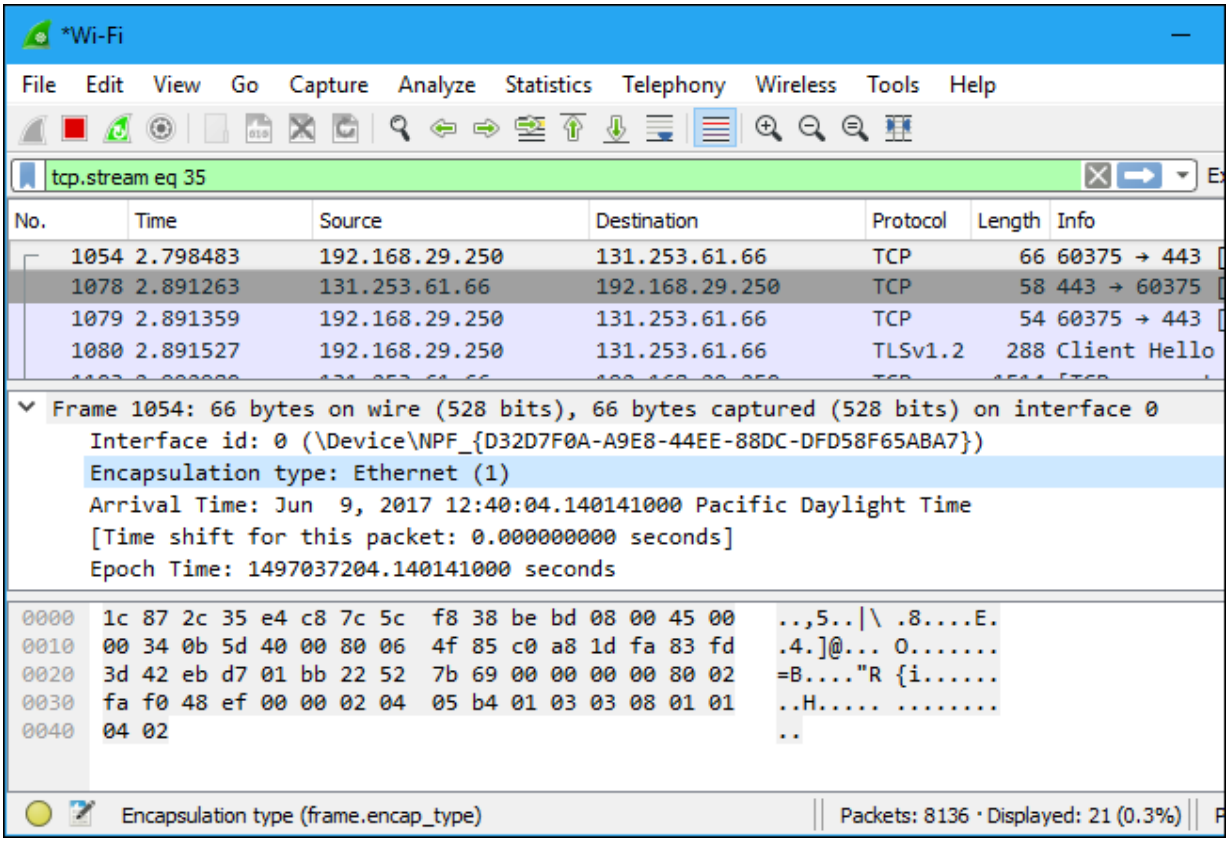


Close the window and you'll find a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.

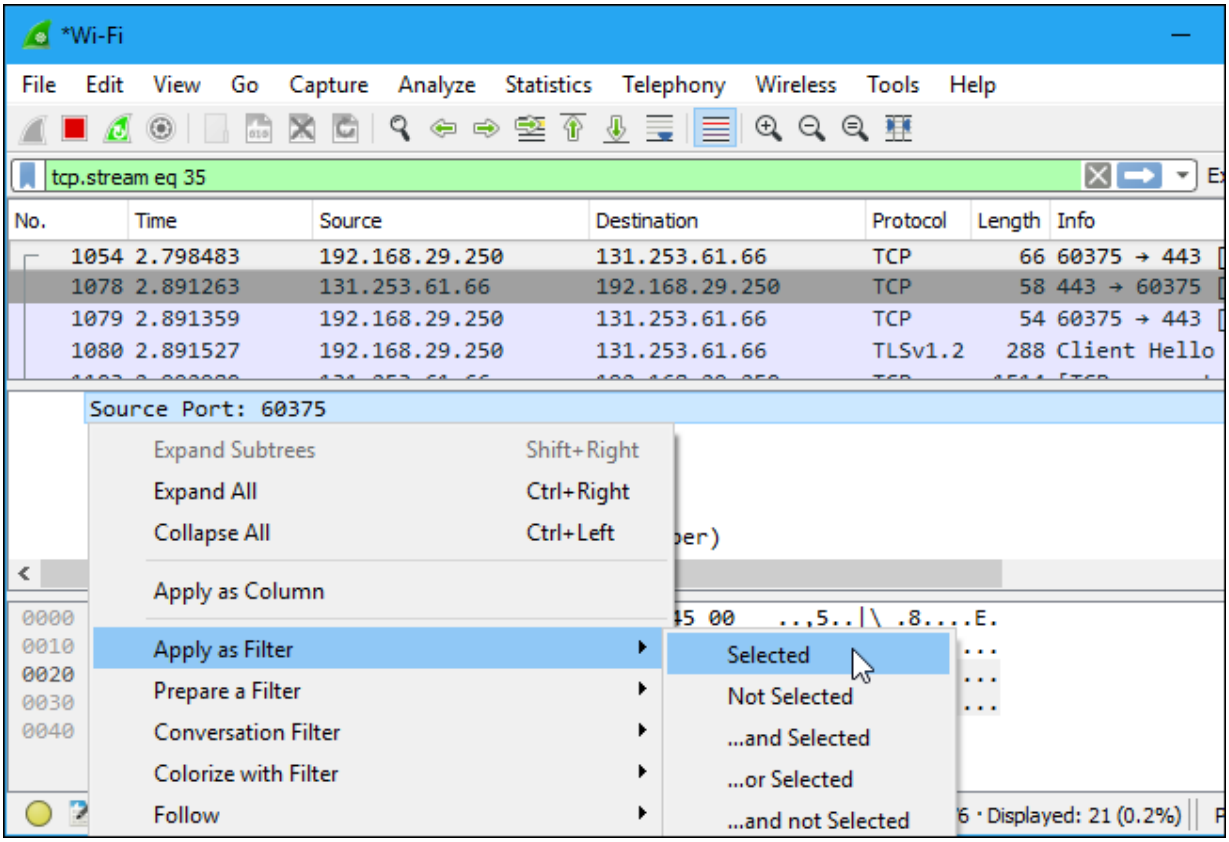


Inspecting Packets

Click a packet to select it and you can dig down to view its details.

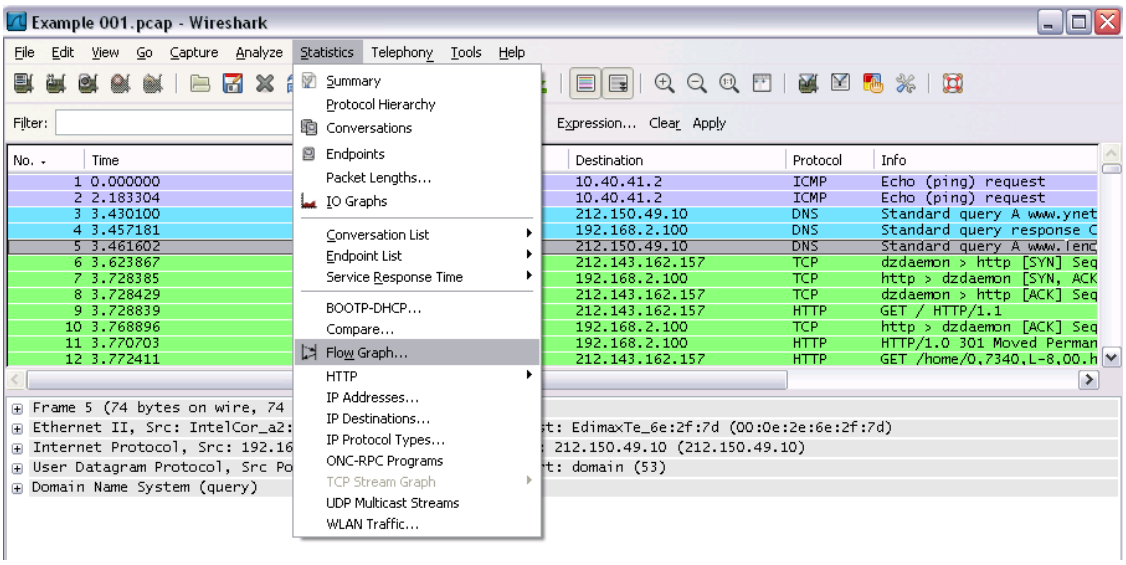


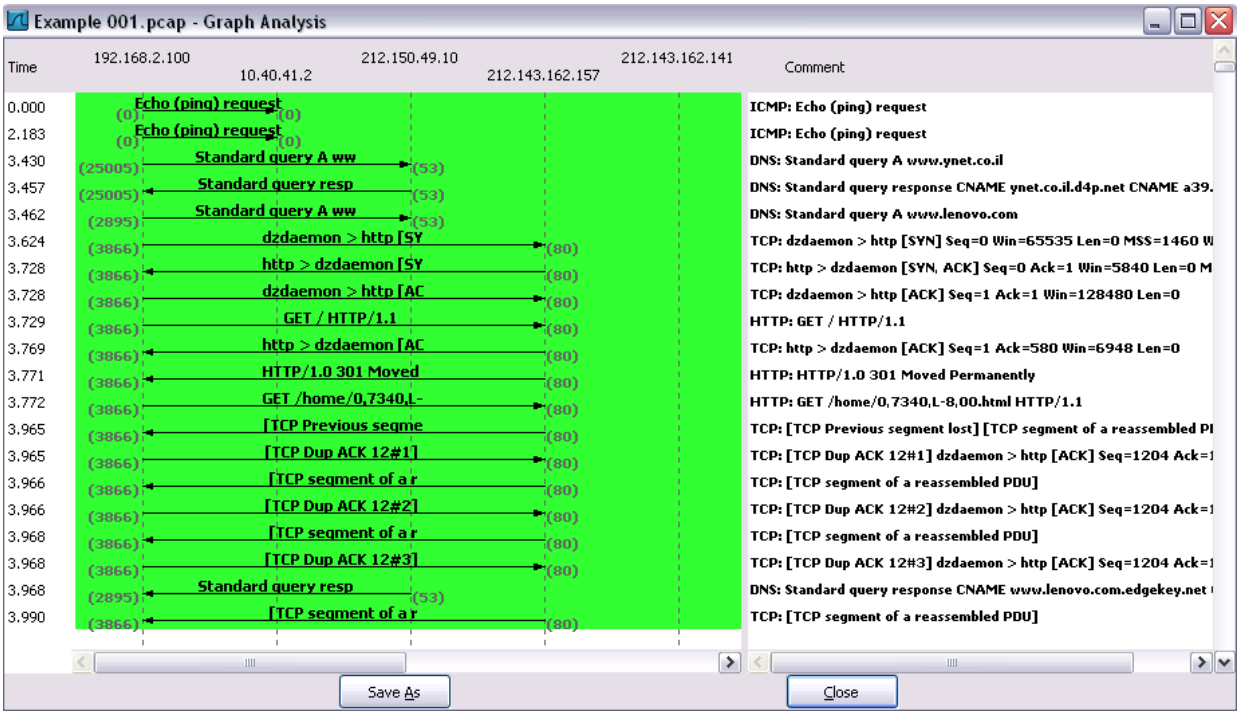
You can also create filters from here — just right-click one of the details and use the Apply as Filter submenu to create a filter based on it.



Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

Flow Graph: Gives a better understanding of what we see.


Example 001.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Summary
Protocol Hierarchy
Conversations
Endpoints
Packet Lengths...
IO Graphs
Conversation List
Endpoint List
Service Response Time
BOOTP-DHCP...
Compare...
Flow Graph...
HTTP
IP Addresses...
IP Destinations...
IP Protocol Types...
ONC-RPC Programs
TCP Stream Graph
UDP Multicast Streams
WLAN Traffic...
Filter:
Expression... Clear Apply
No. Time Destination Protocol Info
1 0.000000 10.40.41.2 ICMP Echo (ping) request
2 2.183304 10.40.41.2 ICMP Echo (ping) request
3 3.430100 212.150.49.10 DNS Standard query A www.ynet
4 3.457181 192.168.2.100 DNS Standard query response C
5 3.461602 212.150.49.10 DNS Standard query A www.lenc
6 3.623867 212.143.162.157 TCP dzdaemon > http [SYN] Seq
7 3.728385 192.168.2.100 TCP http > dzdaemon [SYN, ACK
8 3.728429 212.143.162.157 TCP dzdaemon > http [ACK] Seq
9 3.728839 212.143.162.157 HTTP GET / HTTP/1.1
10 3.768896 192.168.2.100 TCP http > dzdaemon [ACK] Seq
11 3.770703 192.168.2.100 HTTP HTTP/1.0 301 Moved Perman
12 3.772411 212.143.162.157 HTTP GET /home/0,7340,L-8,00.h
Frame 5 (74 bytes on wire, 74
Ethernet II, Src: IntelCor_a2:
Internet Protocol, Src: 192.16
User Datagram Protocol, Src Po
Domain Name System (query)
t: EdimaxTe_6e:2f:7d (00:0e:2e:6e:2f:7d)
212.150.49.10 (212.150.49.10)
t: domain (53)


Example 001.pcap - Graph Analysis
Time
192.168.2.100
10.40.41.2
212.150.49.10
212.143.162.157
212.143.162.141
Comment
0.000 Echo (ping) request (0) (0) ICMP: Echo (ping) request
2.183 Echo (ping) request (0) (0) ICMP: Echo (ping) request
3.430 Standard query A ww (25005) (53) DNS: Standard query A www.ynet.co.il
3.457 Standard query resp (25005) (53) DNS: Standard query response CNAME ynet.co.il.d4p.net CNAME a39.
3.462 Standard query A ww (2895) (53) DNS: Standard query A www.lenovo.com
3.624 dzdaemon > http [SY (3866) (80) TCP: dzdaemon > http [SYN] Seq=0 Win=65535 Len=0 MSS=1460 W
3.728 http > dzdaemon [SY (3866) (80) TCP: http > dzdaemon [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 M
3.728 dzdaemon > http [AC (3866) (80) TCP: dzdaemon > http [ACK] Seq=1 Ack=1 Win=128480 Len=0
3.729 GET / HTTP/1.1 (3866) (80) HTTP: GET / HTTP/1.1
3.769 http > dzdaemon [AC (3866) (80) TCP: http > dzdaemon [ACK] Seq=1 Ack=580 Win=6948 Len=0
3.771 HTTP/1.0 301 Moved (3866) (80) HTTP: HTTP/1.0 301 Moved Permanently
3.772 GET /home/0,7340,L- (3866) (80) HTTP: GET /home/0,7340,L-8,00.html HTTP/1.1
3.965 [TCP Previous segme (3866) (80) TCP: [TCP Previous segment lost] [TCP segment of a reassembled PI
3.965 [TCP Dup ACK 12#1] (3866) (80) TCP: [TCP Dup ACK 12#1] dzdaemon > http [ACK] Seq=1204 Ack=1
3.966 [TCP segment of a r (3866) (80) TCP: [TCP segment of a reassembled PDU]
3.966 [TCP Dup ACK 12#2] (3866) (80) TCP: [TCP Dup ACK 12#2] dzdaemon > http [ACK] Seq=1204 Ack=1
3.968 [TCP segment of a r (3866) (80) TCP: [TCP segment of a reassembled PDU]
3.968 [TCP Dup ACK 12#3] (3866) (80) TCP: [TCP Dup ACK 12#3] dzdaemon > http [ACK] Seq=1204 Ack=1
3.968 Standard query resp (2895) (53) DNS: Standard query response CNAME www.lenovo.com.edgekey.net
3.990 [TCP segment of a r (3866) (80) TCP: [TCP segment of a reassembled PDU]
Save As
Close

Date : 19.8.24

Ex No: 4 b **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

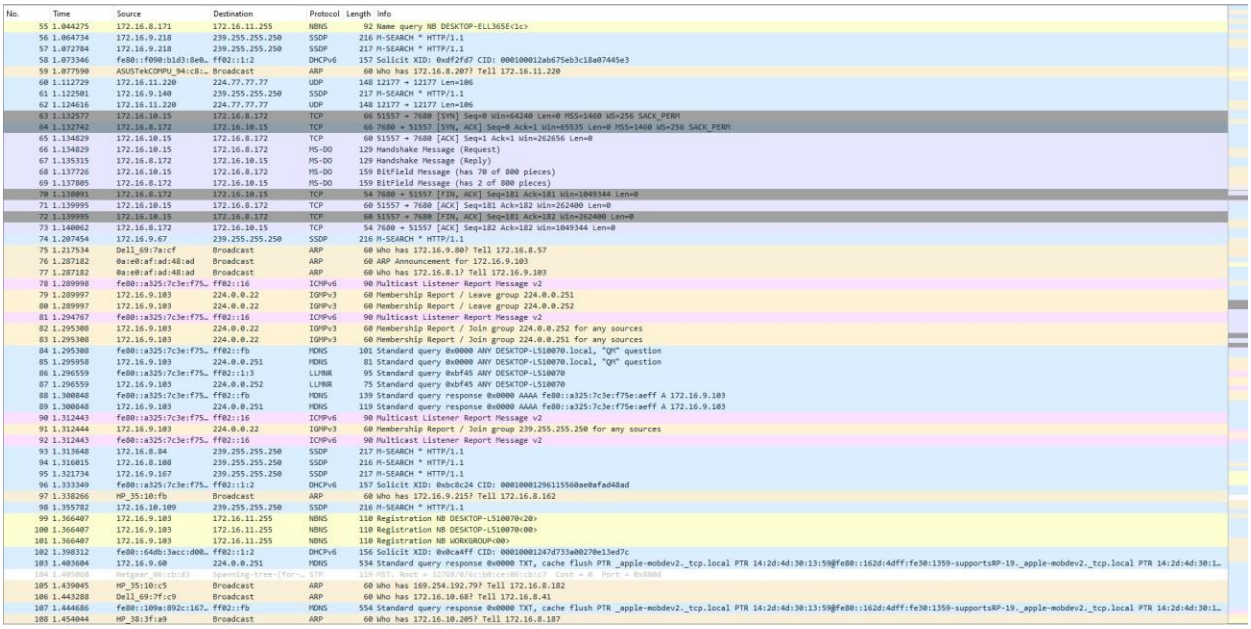
1. Capture 100 packets from the Ethernet: IEEE 802.3 LAN Interface and save it.

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.8.111	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
2	0.003427	MicroStarINT_c5:cb:…	Broadcast	ARP	60	Who has 169.254.192.79? Tell 172.16.10.43
3	0.004362	172.16.9.25	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
4	0.078130	ASUSTekCOMPU_94:c8:…	Broadcast	ARP	60	Who has 172.16.8.207? Tell 172.16.11.220
5	0.078670	fe80::c37:8625:8e42…	ff02::c	SSDP	208	M-SEARCH * HTTP/1.1
6	0.081610	MicroStarINT_c5:cd:…	Broadcast	ARP	60	Who has 172.16.9.70? Tell 172.16.10.115
7	0.107846	172.16.9.140	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
8	0.127703	EliteGroupCo_15:eb:…	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.16.10.191
9	0.152017	36:d2:b3:cc:d1:03	HewlettPacka_be:e5:…	ARP	60	Gratuitous ARP for 172.16.9.65 (Reply)
10	0.204490	172.16.9.67	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
11	0.205056	172.16.8.58	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
12	0.214772	172.16.8.212	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
13	0.232079	172.16.9.43	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
14	0.235331	Dell_35:12:64	Broadcast	ARP	60	Who has 172.16.10.198? Tell 172.16.11.217
15	0.284300	172.16.8.171	172.16.11.255	NBNS	92	Name query NB DESKTOP-ELL365E<1c>
16	0.299901	0a:e0:af:ad:48:ad	Broadcast	ARP	60	Who has 172.16.9.103? (ARP Probe)
17	0.302304	172.16.9.47	239.255.255.250	SSDP	179	M-SEARCH * HTTP/1.1
18	0.303862	172.16.8.108	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
19	0.317549	172.16.9.167	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
20	0.349598	172.16.10.109	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
21	0.380882	Dell_35:0f:98	Broadcast	ARP	60	Who has 172.16.52.146? Tell 172.16.8.108
22	0.380882	Dell_35:0f:98	Broadcast	ARP	60	Who has 172.16.11.121? Tell 172.16.8.108
23	0.400441	fe80::64db:3acc:d00…	ff02::1:2	DHCPv6	156	Solicit XID: 0x0ca4ff CID: 00010001247d733a00270e13ed7c
24	0.426873	172.16.8.190	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
25	0.446664	HP_38:3f:a9	Broadcast	ARP	60	Who has 172.16.10.205? Tell 172.16.8.187
26	0.456672	172.16.11.239	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
27	0.467909	172.16.8.32	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
28	0.504511	172.16.8.226	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
29	0.516629	172.16.8.8	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
30	0.544987	172.16.8.176	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
31	0.559107	MicroStarINT_c5:cd:…	Broadcast	ARP	60	Who has 172.16.9.206? Tell 172.16.10.39
32	0.578334	ASUSTekCOMPU_94:c8:…	Broadcast	ARP	60	Who has 172.16.10.145? Tell 172.16.11.220
33	0.604482	172.16.10.179	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
34	0.635011	fe80::f02d:ea8d:69a…	ff02::1:2	DHCPv6	157	Solicit XID: 0x309115 CID: 000100012bb8532a509a4c34d873
35	0.640760	Dell_34:d6:ff	Broadcast	ARP	60	Who has 172.16.10.93? Tell 172.16.9.180
36	0.655012	Dell_69:7a:cf	Broadcast	ARP	60	Who has 172.16.9.80? Tell 172.16.8.57
37	0.678211	Dell_69:7f:c9	Broadcast	ARP	60	Who has 172.16.10.68? Tell 172.16.8.41
38	0.737070	RealtekSemic_42:be:…	Broadcast	ARP	60	Who has 172.16.8.1? Tell 172.16.11.126
39	0.821935	172.16.10.3	172.16.8.172	TCP	60	56015 → 7680 [FIN, ACK] Seq=1 Ack=2 Win=4100 Len=0
40	0.821935	172.16.8.172	172.16.10.3	TCP	54	7680 → 56015 [ACK] Seq=1 Ack=2 Win=4100 Len=0
41	0.822104	172.16.8.172	172.16.10.3	TCP	54	7680 → 56015 [FIN, ACK] Seq=1 Ack=2 Win=4100 Len=0
42	0.823092	172.16.10.3	172.16.8.172	TCP	60	56015 → 7680 [ACK] Seq=2 Ack=2 Win=4100 Len=0
43	0.852075	172.16.10.91	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
44	0.875465	172.16.8.225	224.0.0.251	MDNS	85	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
45	0.875465	fe80::caa4:cdb:e680…	ff02::fb	MDNS	105	Standard query 0x0000 PTR _microsoft_mcc._tcp.local, "QM" question
46	0.923861	MicroStarINT_c5:cb:…	Broadcast	ARP	60	Who has 172.16.10.48? Tell 172.16.10.52
47	0.925190	HP_35:00:31	Broadcast	ARP	60	Who has 172.16.11.211? Tell 172.16.8.177
48	0.974410	172.16.10.203	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
49	0.986778	172.16.9.227	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
50	0.988176	ASUSTekCOMPU_94:c8:…	Broadcast	ARP	60	Who has 172.16.11.223? Tell 172.16.11.220
51	0.988176	ASUSTekCOMPU_94:c8:…	Broadcast	ARP	60	Who has 172.16.8.112? Tell 172.16.11.220
52	0.988176	ASUSTekCOMPU_94:c8:…	Broadcast	ARP	60	Who has 172.16.9.78? Tell 172.16.11.220
53	1.011735	EliteGroupCo_15:eb:…	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.16.10.191
54	1.012781	172.16.8.111	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1



No.	Time	Source	Destination	Protocol	Length	Info
55	1.044275	172.16.8.171	172.16.11.255	NBNS	92	Name query NB DESKTOP-ELL365E<1c>
56	1.064734	172.16.9.218	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
57	1.072784	172.16.9.218	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
58	1.073346	fe80::f090:b1d3:8e0…	ff02::1:2	DHCPv6	157	Solicit XID: 0xdf2fd7 CID: 000100012ab675eb3c18a07445e3
59	1.077590	ASUSTekCOMPU_94:c8:…	Broadcast	ARP	60	Who has 172.16.8.207? Tell 172.16.11.220
60	1.112729	172.16.11.220	224.77.77.77	UDP	148	12177 → 12177 Len=106
61	1.122501	172.16.9.140	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
62	1.124616	172.16.11.220	224.77.77.77	UDP	148	12177 → 12177 Len=106
63	1.132577	172.16.10.15	172.16.8.172	TCP	66	51557 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
64	1.132742	172.16.8.172	172.16.10.15	TCP	66	7680 → 51557 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
65	1.134829	172.16.10.15	172.16.8.172	TCP	60	51557 → 7680 [ACK] Seq=1 Ack=1 Win=262656 Len=0
66	1.134829	172.16.10.15	172.16.8.172	MS-DO	129	Handshake Message (Request)
67	1.135315	172.16.8.172	172.16.10.15	MS-DO	129	Handshake Message (Reply)
68	1.137726	172.16.10.15	172.16.8.172	MS-DO	159	BitField Message (has 70 of 800 pieces)
69	1.137805	172.16.8.172	172.16.10.15	MS-DO	159	BitField Message (has 2 of 800 pieces)
70	1.138091	172.16.8.172	172.16.10.15	TCP	54	7680 → 51557 [FIN, ACK] Seq=181 Ack=181 Win=1049344 Len=0
71	1.139995	172.16.10.15	172.16.8.172	TCP	60	51557 → 7680 [ACK] Seq=181 Ack=182 Win=262400 Len=0
72	1.139995	172.16.10.15	172.16.8.172	TCP	60	51557 → 7680 [FIN, ACK] Seq=181 Ack=182 Win=262400 Len=0
73	1.140062	172.16.8.172	172.16.10.15	TCP	54	7680 → 51557 [ACK] Seq=182 Ack=182 Win=1049344 Len=0
74	1.207454	172.16.9.67	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
75	1.217534	Dell_69:7a:cf	Broadcast	ARP	60	Who has 172.16.9.80? Tell 172.16.8.57
76	1.287182	0a:e0:af:ad:48:ad	Broadcast	ARP	60	ARP Announcement for 172.16.9.103
77	1.287182	0a:e0:af:ad:48:ad	Broadcast	ARP	60	Who has 172.16.8.17 Tell 172.16.9.103
78	1.289998	fe80::a325:7c3e:f75…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
79	1.289997	172.16.9.103	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.251
80	1.289997	172.16.9.103	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
81	1.294767	fe80::a325:7c3e:f75…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
82	1.295308	172.16.9.103	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
83	1.295308	172.16.9.103	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.251 for any sources
84	1.295308	fe80::a325:7c3e:f75…	ff02::fb	MDNS	101	Standard query 0x0000 ANY DESKTOP-L510070.local, "QM" question
85	1.295958	172.16.9.103	224.0.0.251	MDNS	81	Standard query 0x0000 ANY DESKTOP-L510070.local, "QM" question
86	1.296559	fe80::a325:7c3e:f75…	ff02::1:3	LLMNR	95	Standard query 0xbf45 ANY DESKTOP-L510070
87	1.296559	172.16.9.103	224.0.0.252	LLMNR	75	Standard query 0xbf45 ANY DESKTOP-L510070
88	1.300848	fe80::a325:7c3e:f75…	ff02::fb	MDNS	139	Standard query response 0x0000 AAAA fe80::a325:7c3e:f75e:aeff A 172.16.9.103
89	1.300848	172.16.9.103	224.0.0.251	MDNS	119	Standard query response 0x0000 AAAA fe80::a325:7c3e:f75e:aeff A 172.16.9.103
90	1.312443	fe80::a325:7c3e:f75…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
91	1.312444	172.16.9.103	224.0.0.22	IGMPv3	60	Membership Report / Join group 239.255.255.250 for any sources
92	1.312443	fe80::a325:7c3e:f75…	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
93	1.313648	172.16.8.84	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
94	1.316015	172.16.8.108	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
95	1.321734	172.16.9.167	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
96	1.333349	fe80::a325:7c3e:f75…	ff02::1:2	DHCPv6	157	Solicit XID: 0xbc8c24 CID: 000100012961155 60ae0afad48ad
97	1.338266	HP_35:10:fb	Broadcast	ARP	60	Who has 172.16.9.215? Tell 172.16.8.162
98	1.355782	172.16.10.109	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
99	1.366407	172.16.9.103	172.16.11.255	NBNS	110	Registration NB DESKTOP-L510070<20>
100	1.366407	172.16.9.103	172.16.11.255	NBNS	110	Registration NB DESKTOP-L510070<00>
101	1.366407	172.16.9.103	172.16.11.255	NBNS	110	Registration NB WORKGROUP<00>
102	1.398312	fe80::64db:3acc:d00…	ff02::1:2	DHCPv6	156	Solicit XID: 0xdca4ff CID: 00010001247d733a00270e13ed7c
103	1.403604	172.16.9.60	224.0.0.251	MDNS	534	Standard query response 0x0000 TXT, cache flush PTR _apple-mobdev2._tcp.local PTR 14:2d:4d:30:13:59@fe80::162d:4dff:fe30:1359-supportsRP-19._apple-mobdev2._tcp.local PTR 14:2d:4d:30:1…
104	1.405060	Netgear_06:cb:d3	Spanning-tree-(for-…	STP	119	MST. Root = 32768/0/6c:b0:ce:06:cb:c7 Cost = 0 Port = 0x800d
105	1.439045	HP_35:10:c5	Broadcast	ARP	60	Who has 169.254.192.79? Tell 172.16.8.182
106	1.443288	Dell_69:7f:c9	Broadcast	ARP	60	Who has 172.16.10.68? Tell 172.16.8.41
107	1.444686	fe80::109a:892c:167…	ff02::fb	MDNS	554	Standard query response 0x0000 TXT, cache flush PTR _apple-mobdev2._tcp.local PTR 14:2d:4d:30:13:59@fe80::162d:4dff:fe30:1359-supportsRP-19._apple-mobdev2._tcp.local PTR 14:2d:4d:30:1…
108	1.454044	HP_38:3f:a9	Broadcast	ARP	60	Who has 172.16.10.205? Tell 172.16.8.187

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

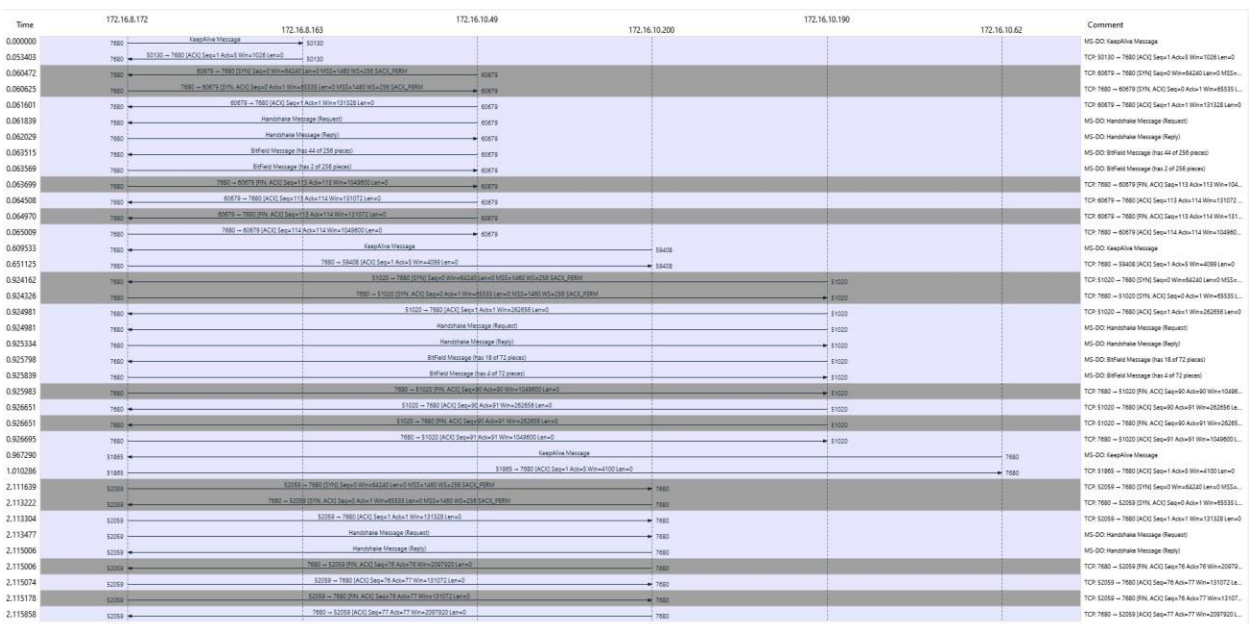
Procedure

- 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:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.8.172	172.16.8.163	MS-DO	58	KeepAlive Message
14	0.053403	172.16.8.163	172.16.8.172	TCP	60	50130 → 7680 [ACK] Seq=1 Ack=5 Win=1026 Len=0
16	0.060472	172.16.10.49	172.16.8.172	TCP	66	60679 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
17	0.060625	172.16.8.172	172.16.10.49	TCP	66	7680 → 60679 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
19	0.061601	172.16.10.49	172.16.8.172	TCP	60	60679 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
20	0.061839	172.16.10.49	172.16.8.172	MS-DO	129	Handshake Message (Request)
21	0.062029	172.16.8.172	172.16.10.49	MS-DO	129	Handshake Message (Reply)
23	0.063515	172.16.10.49	172.16.8.172	MS-DO	91	BitField Message (has 44 of 256 pieces)
24	0.063569	172.16.8.172	172.16.10.49	MS-DO	91	BitField Message (has 2 of 256 pieces)
25	0.063699	172.16.8.172	172.16.10.49	TCP	54	7680 → 60679 [FIN, ACK] Seq=113 Ack=113 Win=1049600 Len=0
26	0.064508	172.16.10.49	172.16.8.172	TCP	60	60679 → 7680 [ACK] Seq=113 Ack=114 Win=131072 Len=0
28	0.064970	172.16.10.49	172.16.8.172	TCP	60	60679 → 7680 [FIN, ACK] Seq=113 Ack=114 Win=131072 Len=0
29	0.065009	172.16.8.172	172.16.10.49	TCP	54	7680 → 60679 [ACK] Seq=114 Ack=114 Win=1049600 Len=0
56	0.609533	172.16.10.200	172.16.8.172	MS-DO	60	KeepAlive Message
62	0.651125	172.16.8.172	172.16.10.200	TCP	54	7680 → 59408 [ACK] Seq=1 Ack=5 Win=4099 Len=0
80	0.924162	172.16.10.190	172.16.8.172	TCP	66	51020 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
81	0.924326	172.16.8.172	172.16.10.190	TCP	66	7680 → 51020 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
82	0.924981	172.16.10.190	172.16.8.172	TCP	60	51020 → 7680 [ACK] Seq=1 Ack=1 Win=262656 Len=0
83	0.924981	172.16.10.190	172.16.8.172	MS-DO	129	Handshake Message (Request)
84	0.925334	172.16.8.172	172.16.10.190	MS-DO	129	Handshake Message (Reply)
85	0.925798	172.16.10.190	172.16.8.172	MS-DO	68	BitField Message (has 18 of 72 pieces)
86	0.925839	172.16.8.172	172.16.10.190	MS-DO	68	BitField Message (has 4 of 72 pieces)
87	0.925983	172.16.8.172	172.16.10.190	TCP	54	7680 → 51020 [FIN, ACK] Seq=90 Ack=90 Win=1049600 Len=0
88	0.926651	172.16.10.190	172.16.8.172	TCP	60	51020 → 7680 [ACK] Seq=90 Ack=91 Win=262656 Len=0
89	0.926651	172.16.10.190	172.16.8.172	TCP	60	51020 → 7680 [FIN, ACK] Seq=90 Ack=91 Win=262656 Len=0
90	0.926695	172.16.8.172	172.16.10.190	TCP	54	7680 → 51020 [ACK] Seq=91 Ack=91 Win=1049600 Len=0
91	0.967290	172.16.10.62	172.16.8.172	MS-DO	60	KeepAlive Message
97	1.010286	172.16.8.172	172.16.10.62	TCP	54	51865 → 7680 [ACK] Seq=1 Ack=5 Win=4100 Len=0
192	2.111639	172.16.8.172	172.16.10.200	TCP	66	52059 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
193	2.113222	172.16.10.200	172.16.8.172	TCP	66	7680 → 52059 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
194	2.113304	172.16.8.172	172.16.10.200	TCP	54	52059 → 7680 [ACK] Seq=1 Ack=1 Win=131328 Len=0
195	2.113477	172.16.8.172	172.16.10.200	MS-DO	129	Handshake Message (Request)
196	2.115006	172.16.10.200	172.16.8.172	MS-DO	129	Handshake Message (Reply)
197	2.115006	172.16.10.200	172.16.8.172	TCP	60	7680 → 52059 [FIN, ACK] Seq=76 Ack=76 Win=2097920 Len=0
198	2.115074	172.16.8.172	172.16.10.200	TCP	54	52059 → 7680 [ACK] Seq=76 Ack=77 Win=131072 Len=0
199	2.115178	172.16.8.172	172.16.10.200	TCP	54	52059 → 7680 [FIN, ACK] Seq=76 Ack=77 Win=131072 Len=0
200	2.115858	172.16.10.200	172.16.8.172	TCP	60	7680 → 52059 [ACK] Seq=77 Ack=77 Win=2097920 Len=0

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
15	0.065677	0a:e0:af:f1:0d:1f	Broadcast	ARP	60	Who has 172.16.8.164? Tell 172.16.8.234
16	0.077547	0a:e0:af:b3:03:76	Broadcast	ARP	60	Who has 172.16.8.91? Tell 172.16.8.55
17	0.093423	Dell_34:d4:f5	Broadcast	ARP	60	Who has 169.254.114.31? (ARP Probe)
21	0.106485	MicroStarInt_ad:3b:…	Broadcast	ARP	60	Who has 172.16.9.135? Tell 172.16.8.27
29	0.166240	0a:e0:af:b3:03:76	Broadcast	ARP	60	Who has 172.16.10.72? Tell 172.16.8.55
49	0.462514	EliteGroupCo_15:e7:…	Broadcast	ARP	60	Who has 172.16.8.230? Tell 172.16.10.194
52	0.496368	Dell_34:d3:d8	Broadcast	ARP	60	Who has 172.16.11.141? Tell 172.16.9.70
69	0.535712	HonHaiPrecis_82:6d:…	Broadcast	ARP	60	Who has 172.16.8.228? (ARP Probe)
78	0.564074	HonHaiPrecis_82:6d:…	Broadcast	ARP	60	Who has 172.16.8.1? Tell 172.16.8.228
79	0.564074	HonHaiPrecis_82:6d:…	Broadcast	ARP	60	Who has 172.16.8.174? Tell 172.16.8.228
88	0.564303	HonHaiPrecis_82:6d:…	Broadcast	ARP	60	Who has 172.16.8.228? (ARP Probe)
89	0.564303	HonHaiPrecis_82:6d:…	Broadcast	ARP	60	Who has 172.16.8.174? Tell 172.16.8.228
110	0.727860	Dell_34:d4:f5	Broadcast	ARP	60	Who has 169.254.49.49? Tell 169.254.114.31
111	0.728166	Dell_34:d4:f5	Broadcast	ARP	60	Who has 169.254.181.116? Tell 169.254.114.31
115	0.836101	EliteGroupCo_14:72:…	Broadcast	ARP	60	Who has 172.16.9.56? Tell 172.16.10.200
116	0.867534	EliteGroupCo_14:83:…	Broadcast	ARP	60	Who has 172.16.10.191? Tell 172.16.10.171
117	0.879128	MicroStarINT_c5:ca:…	Broadcast	ARP	60	Who has 172.16.9.206? Tell 172.16.10.110
121	0.932642	0a:e0:af:ad:48:ad	Broadcast	ARP	60	Who has 172.16.8.1? Tell 172.16.11.250
124	0.982647	Dell_34:d7:0c	Broadcast	ARP	60	Who has 172.16.11.121? Tell 172.16.9.191
125	1.001803	ASUSTekCOMPU_94:c8:…	Broadcast	ARP	60	Who has 172.16.8.165? Tell 172.16.11.220
130	1.092009	Dell_34:d4:f5	Broadcast	ARP	60	Who has 169.254.114.31? (ARP Probe)
133	1.125080	RealtekSemic_42:be:…	Broadcast	ARP	60	Who has 172.16.8.1? Tell 172.16.11.126
136	1.239714	MicroStarINT_c5:cd:…	Broadcast	ARP	60	Who has 172.16.8.94? Tell 172.16.8.208
153	1.458611	Dell_35:11:44	Broadcast	ARP	60	Who has 172.16.8.208? Tell 172.16.8.107
155	1.467944	EliteGroupCo_15:e7:…	Broadcast	ARP	60	Who has 172.16.8.230? Tell 172.16.10.194
156	1.477482	Pegatron_e0:78:08	Broadcast	ARP	60	Who has 172.16.10.229? Tell 172.16.9.134
159	1.500563	Dell_34:d3:d8	Broadcast	ARP	60	Who has 172.16.11.141? Tell 172.16.9.70
169	1.654706	ASUSTekCOMPU_94:c8:…	Broadcast	ARP	60	Who has 172.16.8.165? Tell 172.16.11.220
172	1.694843	Dell_69:7a:cf	Broadcast	ARP	60	Who has 172.16.11.85? Tell 172.16.8.57
173	1.699449	Dell_90:45:97	Broadcast	ARP	60	Who has 172.16.8.117? Tell 172.16.8.63
179	1.781615	EliteGroupCo_14:83:…	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.16.10.171
180	1.802211	Dell_34:d7:0c	Broadcast	ARP	60	Who has 172.16.11.121? Tell 172.16.9.191
181	1.812859	Dell_35:11:6e	Broadcast	ARP	60	Who has 172.16.11.96? Tell 172.16.9.174
182	1.834082	EliteGroupCo_14:72:…	Broadcast	ARP	60	Who has 172.16.9.56? Tell 172.16.10.200
183	1.852789	0a:e0:af:ad:48:ad	Broadcast	ARP	60	Who has 172.16.8.1? Tell 172.16.11.250
188	1.951037	Sophos_cf:be:45	Broadcast	ARP	60	Who has 172.16.9.48? Tell 172.16.8.1
196	2.006005	MicroStarInt_ad:3c:…	Broadcast	ARP	60	Who has 172.16.10.72? Tell 172.16.11.228
202	2.060422	Dell_df:06:80	Broadcast	ARP	60	Who has 169.254.169.254? Tell 172.16.9.66
204	2.091797	Dell_34:d4:f5	Broadcast	ARP	60	ARP Announcement for 169.254.114.31
218	2.168545	Pegatron_e0:78:08	Broadcast	ARP	60	Who has 172.16.10.229? Tell 172.16.9.134
223	2.272385	Dell_69:7a:cf	Broadcast	ARP	60	Who has 172.16.11.85? Tell 172.16.8.57

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

Procedure

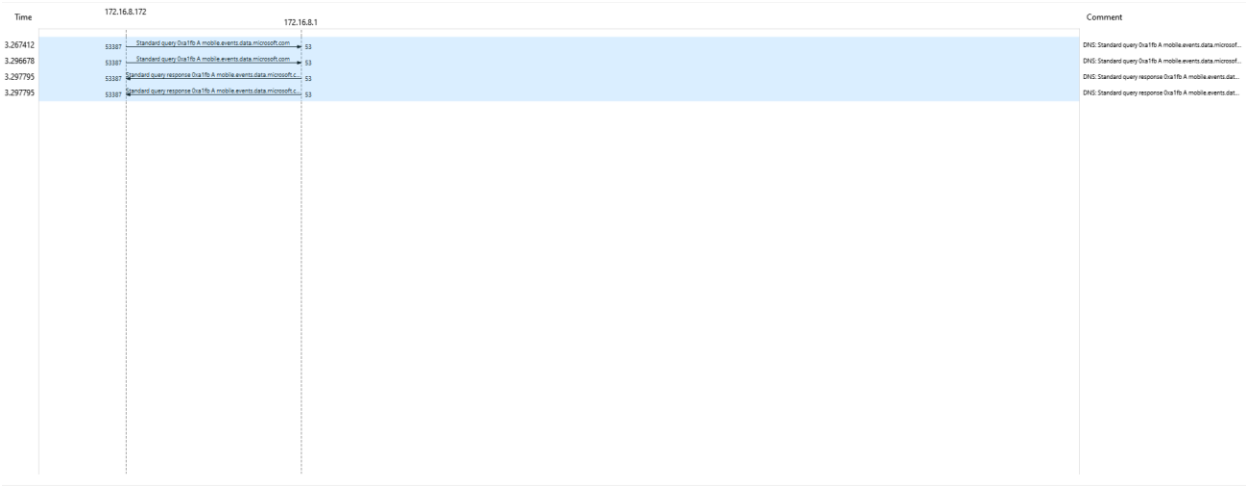
- Select Local Area Connection in Wireshark.
- Go to capture option
- Select stop capture automatically after 100 packets.
- Then click Start capture.

- Search DNS packets in search bar.
- To see flow graph click Statistics➇Flow graph.
- Save the packets.

Output

No.	Time	Source	Destination	Protocol	Length	Info
286	3.267412	172.16.8.172	172.16.8.1	DNS	92	Standard query 0xa1fb A mobile.events.data.microsoft.com
287	3.296678	172.16.8.172	172.16.8.1	DNS	92	Standard query 0xa1fb A mobile.events.data.microsoft.com
288	3.297795	172.16.8.1	172.16.8.172	DNS	212	Standard query response 0xa1fb A mobile.events.data.microsoft.com CNAME mobile.events.data.trafficmanager.net CNAME onedscolprdeus17.eastus.cloudapp.azure.com A 20.42.65.91
289	3.297795	172.16.8.1	172.16.8.172	DNS	212	Standard query response 0xa1fb A mobile.events.data.microsoft.com CNAME mobile.events.data.trafficmanager.net CNAME onedscolprdeus17.eastus.cloudapp.azure.com A 20.42.65.91

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

No.	Time	Source	Destination	Protocol	Length	Info
1871	17.243800	172.16.8.172	23.47.228.163	HTTP	281	GET / HTTP/1.1
1880	17.319132	23.47.228.163	172.16.8.172	HTTP	375	HTTP/1.1 304 Not Modified
1888	17.329963	172.16.8.172	142.250.77.131	HTTP	256	GET /r/gsr1.crl HTTP/1.1
1890	17.337672	142.250.77.131	172.16.8.172	HTTP	359	HTTP/1.1 304 Not Modified
1896	17.347600	172.16.8.172	199.232.210.172	HTTP	335	GET /msdownload/update/v3/static/trustedr/en/authrootstl.cab?debc25c894cfffdc HTTP/1.1
1935	17.794679	199.232.210.172	172.16.8.172	HTTP	290	HTTP/1.1 304 Not Modified
1936	17.802014	172.16.8.172	142.250.77.131	HTTP	254	GET /r/r4.crl HTTP/1.1
1938	17.808053	142.250.77.131	172.16.8.172	HTTP	359	HTTP/1.1 304 Not Modified
1939	17.811345	172.16.8.172	199.232.210.172	HTTP	340	GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?1be63c969d897ed0 HTTP/1.1
1961	18.034082	199.232.210.172	172.16.8.172	HTTP	289	HTTP/1.1 304 Not Modified

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

ICMP:

No.	Time	Source	Destination	Protocol	Length	Info
3378	33.142360	172.16.8.1	172.16.9.208	ICMP	62	Echo (ping) request id=0x00a3, seq=0/0, ttl=64 (no response found!)
14526	158.511703	172.16.8.1	172.16.8.205	ICMP	62	Echo (ping) request id=0xf85f, seq=0/0, ttl=64 (no response found!)
18707	209.577475	172.16.8.1	172.16.11.215	ICMP	62	Echo (ping) request id=0x80c8, seq=0/0, ttl=64 (no response found!)

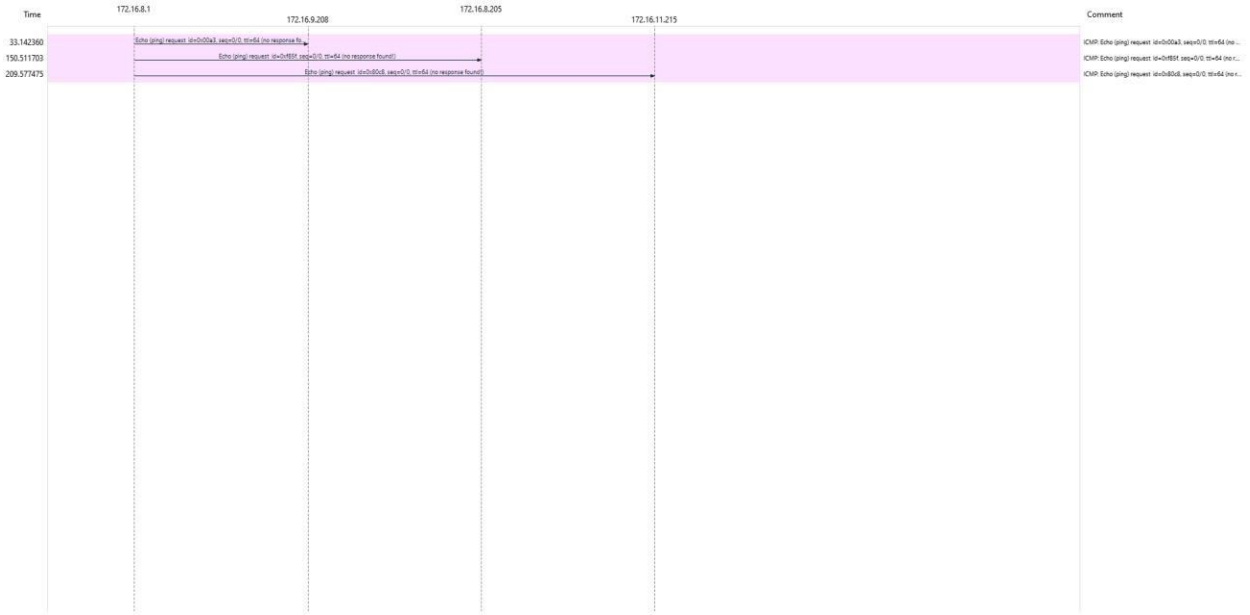
IP:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.030020	172.16.10.63	172.16.11.255	NBNS	92	Name query NB DESKTOP-NB2JA59<1c>
3	0.041874	172.16.10.24	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
4	0.093595	172.16.9.173	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
5	0.130420	172.16.9.230	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
7	0.141319	172.16.11.138	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
8	0.180541	172.16.10.152	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
9	0.210249	169.254.89.232	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
10	0.212427	172.16.9.66	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
11	0.251462	172.16.9.188	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
12	0.268566	172.16.8.57	172.16.9.213	TCP	66	58489 → 7680 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
13	0.350849	172.16.10.44	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
14	0.362364	172.16.11.117	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
16	0.362707	172.16.11.117	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
18	0.388553	172.16.10.9	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
19	0.394398	172.16.11.117	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
21	0.394677	172.16.11.117	224.0.0.251	MDNS	82	Standard query 0x0000 PTR _googlecast._tcp.local, "QM" question
23	0.465410	13.89.179.13	172.16.8.172	TLSv1.3	153	Hello Retry Request, Change Cipher Spec
24	0.467244	172.16.8.172	13.89.179.13	TLSv1.3	805	Change Cipher Spec, Client Hello (SNI=functional.events.data.microsoft.com)
25	0.467644	13.89.179.13	172.16.8.172	TCP	60	443 → 52385 [ACK] Seq=100 Ack=752 Win=297 Len=0
30	0.492527	172.16.9.144	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
33	0.596323	172.16.10.161	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
34	0.600243	172.16.9.221	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
38	0.681889	172.16.9.204	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
39	0.689846	172.16.10.47	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
40	0.690759	172.16.10.164	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
41	0.699069	172.16.10.164	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
43	0.726386	13.89.179.13	172.16.8.172	TLSv1.3	1514	Server Hello
44	0.726386	13.89.179.13	172.16.8.172	TCP	1514	443 → 52385 [ACK] Seq=1560 Ack=752 Win=297 Len=1460 [TCP segment of a reassembled PDU]
45	0.726386	13.89.179.13	172.16.8.172	TCP	1514	443 → 52385 [ACK] Seq=3020 Ack=752 Win=297 Len=1460 [TCP segment of a reassembled PDU]
46	0.726486	172.16.8.172	13.89.179.13	TCP	54	52385 → 443 [ACK] Seq=752 Ack=4480 Win=513 Len=0
47	0.726601	13.89.179.13	172.16.8.172	TCP	1514	443 → 52385 [ACK] Seq=4480 Ack=752 Win=297 Len=1460 [TCP segment of a reassembled PDU]
48	0.726601	13.89.179.13	172.16.8.172	TLSv1.3	544	Application Data
49	0.726634	172.16.8.172	13.89.179.13	TCP	54	52385 → 443 [ACK] Seq=752 Ack=6430 Win=513 Len=0
50	0.731627	172.16.8.172	13.89.179.13	TLSv1.3	128	Application Data
51	0.731700	172.16.8.172	13.89.179.13	TLSv1.3	146	Application Data
52	0.731779	172.16.8.172	13.89.179.13	TLSv1.3	494	Application Data
53	0.731794	13.89.179.13	172.16.8.172	TCP	60	443 → 52385 [ACK] Seq=6430 Ack=826 Win=297 Len=0
54	0.731799	172.16.8.172	13.89.179.13	TLSv1.3	870	Application Data
55	0.731869	13.89.179.13	172.16.8.172	TCP	60	443 → 52385 [ACK] Seq=6430 Ack=918 Win=297 Len=0
56	0.732046	13.89.179.13	172.16.8.172	TCP	60	443 → 52385 [ACK] Seq=6430 Ack=1358 Win=320 Len=0
57	0.732046	13.89.179.13	172.16.8.172	TCP	60	443 → 52385 [ACK] Seq=6430 Ack=2174 Win=343 Len=0
58	0.740132	172.16.11.219	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
59	0.743349	172.16.9.30	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
61	0.790631	172.16.10.63	172.16.11.255	NBNS	92	Name query NB DESKTOP-NB2JA59<1c>
62	0.797895	172.16.8.203	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
63	0.807064	172.16.11.75	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
64	0.807064	172.16.11.75	239.255.255.250	SSDP	218	M-SEARCH * HTTP/1.1
65	0.829977	172.16.11.9	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
67	0.873233	172.16.9.228	224.0.0.251	MDNS	279	Standard query 0x0000 PTR _companion-link._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question PTR lb._dns-sd._udp.local, "QM" question PTR _sleep-proxy._udp.local, "QM" qu…
69	0.881946	172.16.8.174	239.255.255.250	SSDP	217	M-SEARCH * HTTP/1.1
70	0.919960	172.16.8.91	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
71	0.965944	172.16.9.78	224.0.0.251	MDNS	460	Standard query response 0x0000 PTR Aswin's MacBook Pro._companion-link._tcp.local TXT TXT, cache flush AAAA, cache flush fe80::1cca:1209:5de9:16f1 A, cache flush 172.16.9.78 SRV, cach…
75	1.005507	13.89.179.13	172.16.8.172	TLSv1.3	157	Application Data
77	1.024965	13.89.179.13	172.16.8.172	TLSv1.3	116	Application Data

Flow Graph output:

ICMP:

IP:



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

No.	Time	Source	Destination	Protocol	Length	Info
3379	33.142360	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x66f82403
3442	34.399030	0.0.0.0	255.255.255.255	DHCP	360	DHCP Request - Transaction ID 0x66f82403
6230	65.127734	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x7d7e88f2
6231	65.127741	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x7d7e88f2
6489	67.046631	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x88bf0167
6490	67.046692	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x88bf0167
8029	85.392866	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x12bfadcc
8030	85.392927	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x12bfadcc
8398	91.378312	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xe7524bd0
8399	91.378372	0.0.0.0	255.255.255.255	DHCP	358	DHCP Request - Transaction ID 0xe7524bd0
8966	101.523138	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x9f4791c1
8967	101.523140	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x9f4791c1
9738	108.166259	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xa39d312e
9739	108.166318	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xa39d312e
14525	150.511559	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa24a6202
14601	151.512849	172.16.8.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xa24a6202
15468	160.795688	172.16.11.85	255.255.255.255	DHCP	342	DHCP Inform - Transaction ID 0x6b9927ac
15866	166.671087	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x8d1689b3
15882	166.813281	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xa24a6202
15883	166.813715	172.16.8.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xa24a6202
15962	167.793575	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xbc05f522
16652	177.323319	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xbd3d5b33
16653	177.323380	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xbd3d5b33
17847	195.377939	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x8d1689b4
18493	206.429183	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x2fed0e22
18709	209.577476	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xbe5a1e56
18752	210.190147	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xdf8cd152
18848	211.592699	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xbe5a1e56
18879	212.310088	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xdf8cd152
19411	216.562770	0.0.0.0	255.255.255.255	DHCP	352	DHCP Request - Transaction ID 0x678a4397
19457	216.938258	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x8f56a53a
20540	223.720394	0.0.0.0	255.255.255.255	DHCP	344	DHCP Request - Transaction ID 0xd4abd551
24045	241.055956	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0xee9f6ce4
24271	243.225535	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x8d1689b5
24323	243.636723	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x4dd59cce
24445	244.638332	172.16.8.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x4dd59cce
24471	244.837585	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x4dd59cce
24472	244.837644	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x4dd59cce
24649	247.539957	172.16.8.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x4dd59cce
24650	247.539958	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x4dd59cce
24713	248.285129	0.0.0.0	255.255.255.255	DHCP	364	DHCP Request - Transaction ID 0x7c021321
24827	249.331960	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1eff01c
24956	250.332981	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x1eff01c

Time	0.0.0.0	255.255.255.255	172.16.8.1	172.16.11.85	Comment
33.142360	68 →	67			DHCP: DHCP Discover - Transaction ID 0x66f82403
34.399030	68 →	67			DHCP: DHCP Request - Transaction ID 0x66f82403
65.127734	68 →	67			DHCP: DHCP Request - Transaction ID 0x7d7e88f2
65.127741		68 ←	67		DHCP: DHCP ACK - Transaction ID 0x7d7e88f2
67.046631		68 ←	67		DHCP: DHCP ACK - Transaction ID 0x88bf0167
67.046692	68 →	67			DHCP: DHCP Request - Transaction ID 0x88bf0167
85.392866		68 ←	67		DHCP: DHCP ACK - Transaction ID 0x12bfadcc
85.392927	68 →	67			DHCP: DHCP Request - Transaction ID 0x12bfadcc
91.378312		68 ←	67		DHCP: DHCP ACK - Transaction ID 0xe7524bd0
91.378372	68 →	67			DHCP: DHCP Request - Transaction ID 0xe7524bd0
101.523138		68 ←	67		DHCP: DHCP ACK - Transaction ID 0x9f4791c1
101.523140	68 →	67			DHCP: DHCP Request - Transaction ID 0x9f4791c1
108.166259		68 ←	67		DHCP: DHCP ACK - Transaction ID 0xa39d312e
108.166318	68 →	67			DHCP: DHCP Request - Transaction ID 0xa39d312e
150.511559	68 →	67			DHCP: DHCP Discover - Transaction ID 0xa24a6202
151.512849		68 ←	67		DHCP: DHCP Offer - Transaction ID 0xa24a6202
160.795688		67 ←		68	DHCP: DHCP Inform - Transaction ID 0xfbb9927ac
166.671087	68 →	67			DHCP: DHCP Request - Transaction ID 0x8d1689e3
166.813281	68 →	67			DHCP: DHCP Discover - Transaction ID 0xa24a6202
166.813715		68 ←	67		DHCP: DHCP Offer - Transaction ID 0xa24a6202
167.793575	68 →	67			DHCP: DHCP Request - Transaction ID 0xbcd55f522
177.323319		68 ←	67		DHCP: DHCP ACK - Transaction ID 0xbd3d5b33
177.323380	68 →	67			DHCP: DHCP Request - Transaction ID 0xbd3d5b33
195.377939	68 →	67			DHCP: DHCP Request - Transaction ID 0x8d1689b4
206.429183	68 →	67			DHCP: DHCP Request - Transaction ID 0x2fedbe22
209.577476	68 →	67			DHCP: DHCP Discover - Transaction ID 0xbe5a1e56
210.190147	68 →	67			DHCP: DHCP Discover - Transaction ID 0xdf8cd152
211.592699	68 →	67			DHCP: DHCP Request - Transaction ID 0xbe5a1e56
212.310088	68 →	67			DHCP: DHCP Request - Transaction ID 0xdf8cd152
216.562770	68 →	67			DHCP: DHCP Request - Transaction ID 0x678a6397
216.938258	68 →	67			DHCP: DHCP Request - Transaction ID 0x9f56a53a
223.720394	68 →	67			DHCP: DHCP Request - Transaction ID 0xb4abd551
241.055956	68 →	67			DHCP: DHCP Request - Transaction ID 0xee9f6ce4
243.225535	68 →	67			DHCP: DHCP Request - Transaction ID 0x8d1689b5
243.636723	68 →	67			DHCP: DHCP Discover - Transaction ID 0x4dd59cce
244.638332		68 ←	67		DHCP: DHCP Offer - Transaction ID 0x4dd59cce