

Ex NO: 5

EXPERIMENT ON PACKET CAPTURE

DATE: 14.08.2025 TOOL: WIRESHARK

AIM:

to capture and analyze network packets using Wireshark and apply filters to display specific protocols.

PACKET SNIFFER:

→ Sniffs messages being sent/received from/by your computer.

→ store and display the contents of the various protocol fields in the message.

Description:

Wireshark, a network analysis tool formerly known as Ethereal, captures packet in real time and display them in human-readable format. Wireshark includes filters, color coding and other features that let you dig deeper into network traffic and inspect individual packets.

capturing and analysing packets using
Wireshark tool :

=> to filter, capture, view packets in
Wireshark tool.

=> 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

Procedure :

→ select local Area connection in
Wireshark

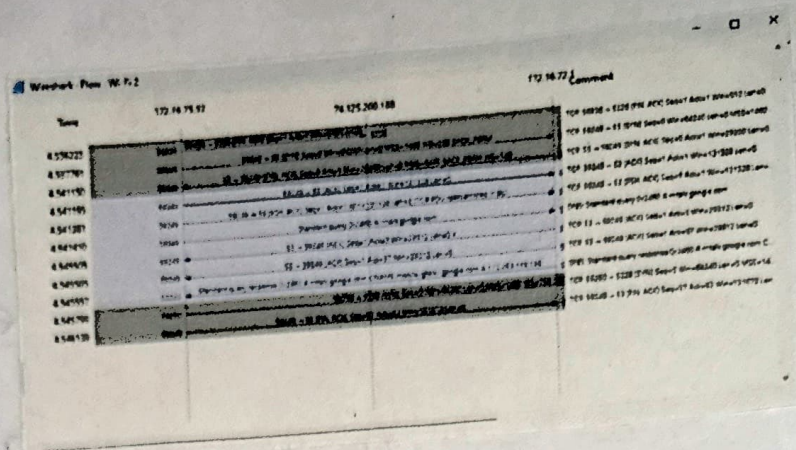
→ go to capture → option

→ select stop capture automatically
after 100 packets.

→ then click start capture

→ save the packets.

output: packet list



- 1) Create a filter to display only TCP and UDP packets the packets and provide the flow graph.

Procedure:

- ⇒ Select LAN in Wireshark
- ⇒ go to capture → option
- ⇒ select stop capture
- ⇒ search TCP packets in search bar.
- ⇒ to see flow graph click statistics → flow graph
- save the packets.

Flow graph:

No.	Time	Source	Destination	Protocol	Length	Info
79	0.000113	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
80	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
81	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
82	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
83	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
84	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
85	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
86	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
87	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
88	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
89	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
90	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
91	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
92	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
93	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
94	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
95	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
96	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
97	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
98	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
99	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000
100	0.000180	192.16.75.53	192.16.75.53	ICMP	56	Standard query response 0x0000 P.D. 0x0000 0x0000 0x0000

2) Create a filter to display only ARP packets and inspect the packets.

Procedure:

- search ARP packets in search bar
- save the packets.

Output:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	CloudNetwork_77:ff:bf	Broadcast	ARP	42	Who has 172.16.75.53? (ARP Probe)
23	0.940875	CloudNetwork_77:ff:bf	Broadcast	ARP	42	Who has 172.16.75.53? (ARP Probe)
49	1.997894	CloudNetwork_77:ff:bf	Broadcast	ARP	42	ARP Announcement for 172.16.75.53
81	3.996581	CloudNetwork_77:ff:bf	Broadcast	ARP	42	ARP Announcement for 172.16.75.53

3) create a filter to display only DNS packets and provide the flow graph.

Procedure:

- search DNS packets in search bar.
- to see flow graph click statistics
- flow graph.
- save the packets.

output :

Time	172.16.75.53	172.16.72.1	Comment
4.541810	172.16.75.53 → 172.16.72.1		DHCP Standard query response 0x0000 PTR DELL:DESKTOP-C
4.545557	172.16.72.1 → 172.16.75.53		DHCP Standard query response 0x0000 PTR DELL:DESKTOP-C

4) create a filter to display any IP/ICMP

Packets and inspect the packets

Procedure :

→ Search IP packets in search bar

→ save the packets

Output

No.	Time	Source	Destination	Protocol	Length	Info
2	0.001651	172.16.75.151	224.0.0.251	IGMP	1317	Standard query response 0x0000 PTR DELL:DESKTOP-C
5	0.003064	172.16.75.151	224.0.0.251	IGMP	848	Standard query response 0x0000 PTR DELL:DESKTOP-C
6	0.003064	172.16.75.151	224.0.0.251	IGMP	306	Standard query response 0x0000 PTR DELL:DESKTOP-C
7	0.005073	172.16.75.53	142.251.228.110	UDP	71	57362 → 443 Len=29
8	0.226622	172.16.75.53	142.251.228.110	UDP	71	57362 → 443 Len=29
9	0.226622	142.251.228.110	172.16.75.53	UDP	72	443 → 57362 Len=30
10	0.285830	142.251.228.110	172.16.75.53	UDP	73	443 → 57362 Len=31
11	0.547071	172.16.75.53	22.59.71.10	TCP	54	59222 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
12	0.548036	172.16.75.53	104.79.107.222	TCP	54	59222 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
13	0.548036	172.16.75.53	71.201.251.21	TCP	54	59222 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
14	0.548112	172.16.75.53	20.507.281.100	TCP	54	59222 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
15	0.548112	172.16.75.53	82.207.246.50	TCP	54	59222 → 443 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
16	0.620316	172.16.79.251	239.0.0.0	UDP	1070	59726 → 51721 Len=1036
17	0.620316	172.16.79.248	239.0.0.1	UDP	92	63458 → 6666 Len=50
18	0.622462	172.16.79.248	239.0.0.0	UDP	1076	54274 → 51721 Len=1036
19	0.622462	172.16.79.246	239.0.0.8	UDP	1078	40626 → 51721 Len=1036
20	0.622462	172.16.79.46	255.255.255.255	IGMP	92	Name query 0x00000000000000000000000000000000
21	0.622793	172.16.75.53	172.16.79.46	IGMP	128	Name query response, Requested name does not exist
22	0.626057	172.16.79.245	239.0.0.8	UDP	1078	35893 → 51721 Len=1036
23	0.641350	172.16.79.46	172.16.79.55	IGMP	92	Name query 0x00000000000000000000000000000000

5) create a filter to display only DHCP packets and the packets

Procedure:

→ search DHCP packets in search bar.

→ save the packets.

output:

No.	Time	Source	Destination	Protocol	Length	Info
13273	264.000754	0.0.0.0	255.255.255.255	DHCP	346	DHCP Discover - Transaction ID 0x526403c5
13678	278.398004	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x79e7c50f
15137	329.289935	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xc4b405cf
29218	433.428083	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request - Transaction ID 0x16d306c8
30438	464.148857	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xc2c0990b
31218	482.582826	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x15ad16d0
31859	501.217956	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xf355796f
33455	538.908519	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x56dfcb82
34081	582.214991	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request - Transaction ID 0x9c22a40b
36462	622.867521	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xfda38add
42871	810.467653	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x59b3f05d
47976	813.535985	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x59b3f05d
48562	826.892230	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x1b8f62
49185	848.978214	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xb792e0cf
49366	854.393085	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x7af16a96
49934	861.460416	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0xe8d6b47b
50294	875.695584	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x13890bc3
51344	904.977436	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x76a370ec

Student observation:

1) What is promiscuous mode?

Ans: Promiscuous mode is a setting for a network interface card (NIC) that allows it to capture all network packets passing through it, regardless of the destination MAC address.

2. Does ARP packets has transport layer header? Explain.

Ans: NO, ARP packets do not have a transport layer header. it sits between the network and data link layer - there is no TCP or UDP involved,

so no transport layer header exists.

3. which transport layer protocol is used by DNS?

Ans: It uses UDP for normal queries and TCP for large responses/zones transfer

4. what is the port number used by HTTP protocol?

Ans: It uses Port 80 by default.

5) what is broadcast IP address?

Ans: Address to reach all hosts in a network (192.168.1.255/24)

RESULT:

thus the experiment on packet capture tool: Wireshark has been done successfully.

✓
26/9/23