

Ex: 04
Date:
4/8/25

PRACTICAL-5

WIRESHARK

AIM:-

To filter, capture, view, packets in Wireshark tool.

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

• 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 packet.

[illegible][illegible]

- 2) Create a Filter to display only ARP packets and inspect the packets Procedure.
- Go to capture → option
 - Select stop capture automatically after 100 packets.
 - Then click start capture.
 - Search ARP packets in search bar.
- exp:-

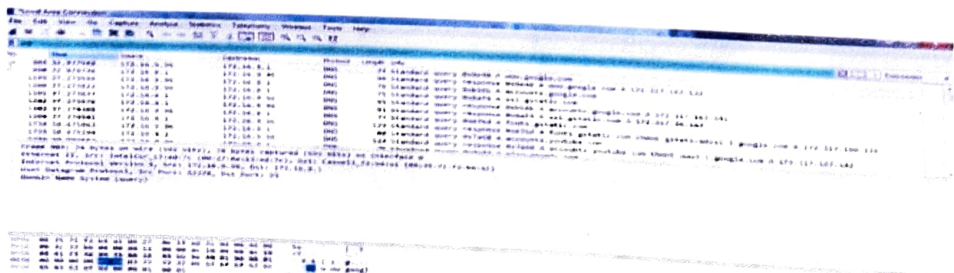
No.	Time	Source	Destination	Protocol	Length	Info
6	0.255305	Foxconn_c9:c5:f0	Broadcast	ARP	60	Who has 172.16.10.15? Tell 172.16.10.3
14	0.692936	Foxconn_d0:ac:46	Broadcast	ARP	60	Who has 172.16.8.39? Tell 172.16.10.8
19	1.418424	Foxconn_c9:c9:91	Broadcast	ARP	60	Who has 172.16.8.106? Tell 172.16.10.26
24	1.888729	Foxconn_d0:ac:46	Broadcast	ARP	60	Who has 172.16.8.40? Tell 172.16.10.8
27	2.029517	Giga-Byt_92:d2:ef	Broadcast	ARP	60	Who has 172.16.10.33? Tell 172.16.10.1
41	2.509085	Giga-Byt_7c:c5:34	Broadcast	ARP	60	Who has 172.16.9.82? Tell 172.16.9.111
44	2.602358	Foxconn_c9:c8:74	Broadcast	ARP	60	Who has 172.16.8.139? Tell 172.16.10.22
46	2.743021	Dell_35:11:11	Broadcast	ARP	60	Who has 172.16.8.118? Tell 172.16.10.195
56	3.201822	Giga-Byt_92:d2:ef	Broadcast	ARP	60	Who has 172.16.10.34? Tell 172.16.10.1
63	3.237061	Giga-Byt_7c:c5:34	Broadcast	ARP	60	Who has 172.16.9.82? Tell 172.16.9.111
71	3.430623	Dell_35:11:11	Broadcast	ARP	60	Who has 172.16.8.118? Tell 172.16.10.195

Frame 119: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
 Ethernet II, Src: IntelCor_13:ed:7c (00:27:0e:13:ed:7c), Dst: Realtek5_b2:60:90 (00:0e:4c:b2:60:90)
 Address Resolution Protocol (reply)

```
0000 00 e0 4c b2 60 90 00 27 0e 13 ed 7c 08 06 00 01
0010 08 00 06 04 00 02 00 27 0e 13 ed 7c 0c 10 09 06
0020 00 e0 4c b2 60 90 ac 10 09 6a
```

3. Create a filter to display only DNS packets and provide the flow graph procedure.

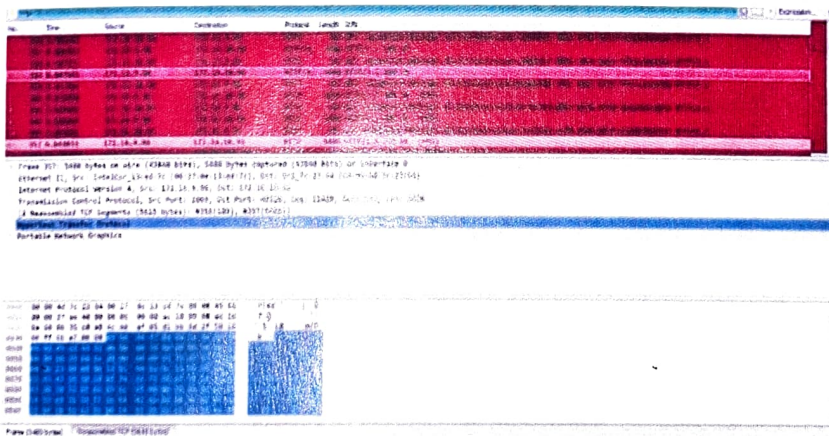
- Go to capture → option
 - Select stop capture automatically after 100 packets.
 - Then click start capture.
 - Search DNS packets in search bar.
 - To see flow graph click Statistics → Flow graph.
 - Save the packets.
- elp:-



4. Create a filter to display only HTTP 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 search bar.
- Save the packets.

o/p:-



5. Create a ~~filter~~ and inspect the packets to display only IP/ICMP 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.

OLP:-

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.18.82	255.255.255.255	DHCP	240	Standard query (0) 172.16.18.82
2	0.000000	172.16.18.82	172.16.18.82	DHCP	240	Standard query response (1) 172.16.18.82
3	0.000000	172.16.18.82	255.255.255.255	DHCP	240	Standard query (0) 172.16.18.82
4	0.000000	172.16.18.82	172.16.18.82	DHCP	240	Standard query response (1) 172.16.18.82
5	0.000000	172.16.18.82	255.255.255.255	DHCP	240	Standard query (0) 172.16.18.82
6	0.000000	172.16.18.82	172.16.18.82	DHCP	240	Standard query response (1) 172.16.18.82
7	0.000000	172.16.18.82	255.255.255.255	DHCP	240	Standard query (0) 172.16.18.82
8	0.000000	172.16.18.82	172.16.18.82	DHCP	240	Standard query response (1) 172.16.18.82
9	0.000000	172.16.18.82	255.255.255.255	DHCP	240	Standard query (0) 172.16.18.82
10	0.000000	172.16.18.82	172.16.18.82	DHCP	240	Standard query response (1) 172.16.18.82

6. 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.

OLP:-

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
2	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)
3	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
4	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)
5	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
6	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)
7	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
8	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)
9	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
10	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)

No.	Time	Source	Destination	Protocol	Length	Info
11	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
12	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)
13	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
14	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)
15	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
16	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)
17	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
18	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)
19	0.000000	192.168.1.100	192.168.1.1	DHCP	240	192.168.1.100:67 → 192.168.1.1:68 [Relay Agent] (12)
20	0.000000	192.168.1.1	192.168.1.100	DHCP	240	192.168.1.1:68 → 192.168.1.100:67 [Relay Agent] (12)

Student Observation:-

1) What is promiscuous mode?

It is a network interface mode in which a network card (NIC) captures all network packets that pass through it, regardless of the destination MAC address.

2) Does ARP packets have a transport layer header? Explain.

No, ARP packets do not have a transport layer header.

- ARP works the Data Link layer (layer 2) of the OSI model, and in TCP/IP terms, it's part of the link layer.

- Its purpose is to map an IP address to a MAC address.

3) Which transport layer protocol is used by DNS?

DNS can use both UDP and TCP at the transport layer.

4) What is the port number used by HTTP protocol?

HTTP uses port number 80 by default.

- HTTPS uses port number 443.

5) What is a broadcast IP address?

A broadcast IP address is an address used to send data to all hosts on a network segment at once.

RESULT:-

Successfully simulated and analyzed the
experiment on Packet capture tool :
Wireshark.

Dr
18/9/20