

Exp.No.4

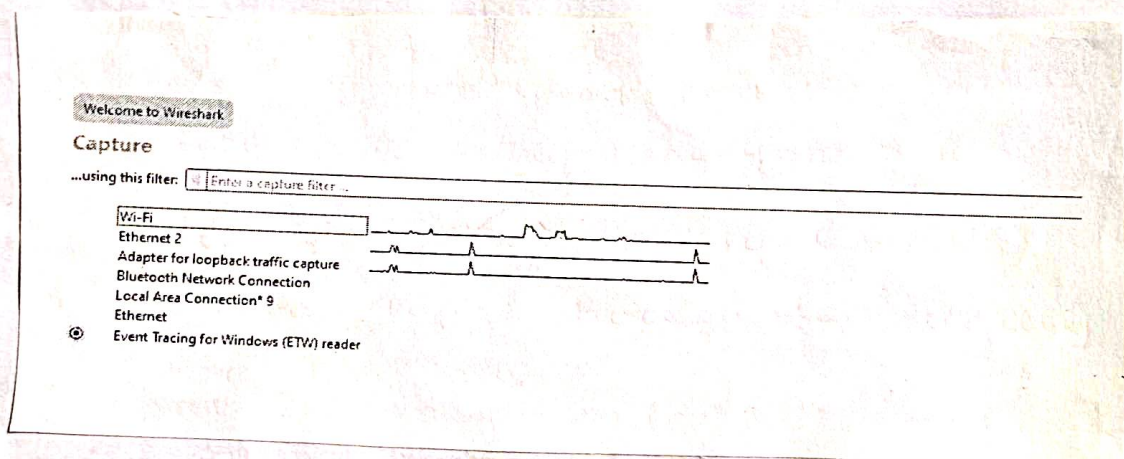
Date: 4.8.25

AIM: Experiments on Packet capture tool
- Wireshark

WIRESHARK

It is a network analysis tool formerly known as Ethereal, captures packets in real time and display them in human-readable format.

CAPTURING AND ANALYSING PACKETS USING WIRESHARK TOOL



* Create a filter to display only TCP/UDP packets, inspect the packets

- Select Local Area Connection

- Go to capture → option

- Select stop capture automatically after 100 packets

- click start capture

- search TCP packets in search bar

* create a filter to display only ARP packets and inspect the packets

- Goto capture → option
- select stop capture automatically after 100 packets
- Then click Start Capture
- Search ARP packets in search bar

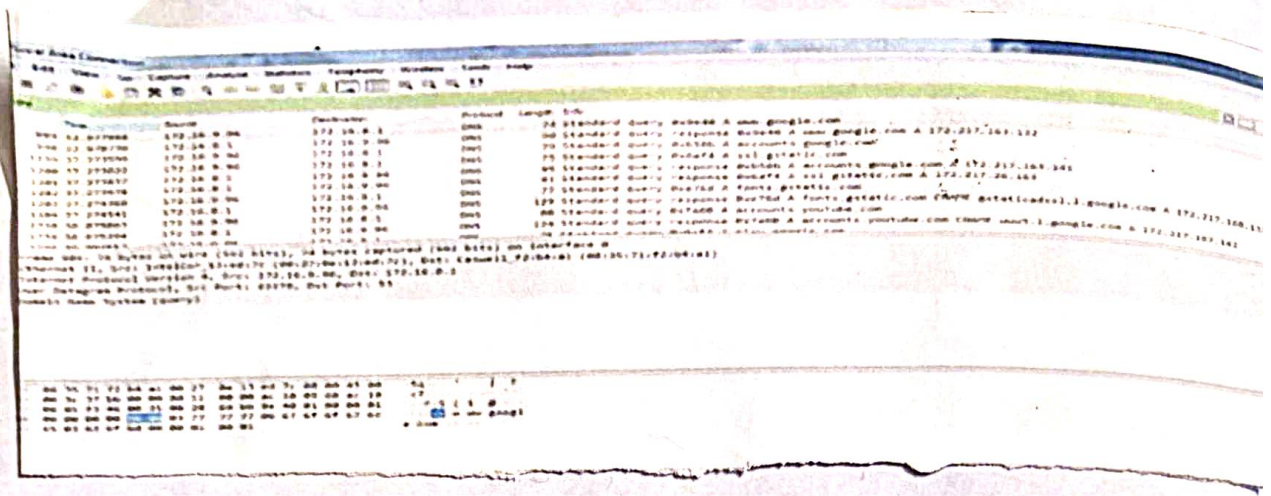
No.	Time	Source	Destination	Protocol	Length	Info
6	0.255305	Foxconn_c9:c5:f0	Broadcast	ARP	60	Who has 172.16.10.15? Tell 172.16.10.3
14	0.692936	Foxconn_d0:ac:46	Broadcast	ARP	60	Who has 172.16.8.39? Tell 172.16.10.8
19	1.418424	Foxconn_c9:c9:91	Broadcast	ARP	60	Who has 172.16.8.106? Tell 172.16.10.26
24	1.880729	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	2.509905	Giga-Byt_7c:c5:34	Broadcast	ARP	60	Who has 172.16.9.82? Tell 172.16.9.111
44	2.602358	Foxconn_c9:c8:24	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
60	3.237061	Giga-Byt_7c:c5:34	Broadcast	ARP	60	Who has 172.16.9.82? Tell 172.16.9.111
71	3.438662	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:e0:4c:b2:60:90)
 Address Resolution Protocol (reply)

* create a filter to display only DNS packets

- Goto capture → option
- select stop capture automatically after 100 packets

- Then click start capture
- search DNS packets in search bar



* create a filter to display only HTTP packets and inspect the packets

- Select Local Area Connection in Wireshark
- Goto capture → option
- select stop capture automatically after 100 packets
- click start capture
- search HTTP packets in search bar
- save the packets.

No.	Time	Source	Destination	Protocol	Length	Info
324	9.487865	172.16.9.96	172.16.10.96	HTTP/X	4408	HTTP/1.1 200 OK
357	9.843033	172.16.9.96	172.16.10.96	HTTP	5480	HTTP/1.1 200 OK (PNG)

Frame 357: 5480 bytes on wire (43840 bits), 5480 bytes captured (43840 bits) on Interface 0
 Ethernet II, Src: IntelCon_13:ed:7c (00:27:0e:13:ed:7c), Dst: Dcl_7c:23:64 (00:00:4d:7c:23:64)
 Internet Protocol Version 4, Src: 172.16.9.96, Dst: 172.16.10.96
 Transmission Control Protocol, Src Port: 2869, Dst Port: 49320, Seq: 11420, Ack: 574, Len: 5426
 [2 Reassembled TCP Segments (5615 bytes): #356(189), #357(5426)]
 Hypertext Transfer Protocol
 Portable Network Graphics

```

0000 00 00 4d 7c 23 64 00 27 0e 13 ed 7c 08 00 45 00  M|d. . . . E
0010 00 00 37 ae 40 00 80 06 00 00 ac 10 09 60 ac 10  7 @ . . . .
0020 0a 60 0b 35 c0 a8 4c 40 af 05 d1 bb 6d 2f 50 18  S LB . . . . /P
0030 00 ff 6b e7 00 00 59 50 4e 47 00 9a 3a 0a 00 00  k . P R . . . .
0040 00 0d 49 48 44 52 00 00 00 70 00 00 00 30 08 02  XON . . . .
0050 00 00 00 d8 00 00 00 00 00 00 09 70 43 59 73 00  . . . . phys
0060 00 00 13 00 00 00 13 01 00 8a 9c 18 00 00 0a 4f  . . . . ID
0070 00 02 03 00 00 00 00 00 00 00 00 00 00 00 00  . . . . ID
0080 43 20 70 72 6f 66 69 6c 65 00 00 78 da 9d 53 67  C profil e . . . S
0090 54 53 e9 16 3d 77 de f4 42 4b 88 80 94 4b 6f 52  TS . . . . K
00a0 15 08 20 52 42 8b 80 14 91 26 20 21 00 10 4a 80  R . . . . J
  
```

* create a filter to display only DHCP packets and inspect the packets

- Select Local Area connection
- Goto → capture → option
- Select stop capture after 100 packets
- Search DHCP packets in search bar
- Save the packets.

No.	Time	Source	Destination	Protocol	Length	Info
3	0.209593	fe80::5cda:e1f4:d07...	ff02::1:2	DHCPv6	150	Solicit XID: 0x3634f7 CID: 000100010d2a7d1000004d7cd3e
4	0.310897	fe80::d40:4448:5018...	ff02::1:2	DHCPv6	150	Solicit XID: 0x8084a1 CID: 0001000103c2673c00004c552cb0
7	0.323092	fe80::5147:5612:a48...	ff02::1:2	DHCPv6	150	Solicit XID: 0xa70c07 CID: 00010001215e5349d43d7ec807b2
11	0.524560	fe80::f021:1889:190...	ff02::1:2	DHCPv6	150	Solicit XID: 0x0df0a3 CID: 000100012153c05f00270e13fed9
51	1.215571	fe80::5cda:e1f4:d07...	ff02::1:2	DHCPv6	150	Solicit XID: 0x3634f7 CID: 000100010d2a7d1000004d7cd3e
85	3.228007	fe80::5cda:e1f4:d07...	ff02::1:2	DHCPv6	150	Solicit XID: 0x3634f7 CID: 000100010d2a7d1000004d7cd3e
96	5.649034	fe80::c159:d7a6:a74...	ff02::1:2	DHCPv6	150	Solicit XID: 0x0236e0 CID: 00010001210226a5001fd0e2a391
109	4.096915	fe80::c4b5:5e2c:922...	ff02::1:2	DHCPv6	150	Solicit XID: 0x002548 CID: 0001000121d5ad5200270e13ec4
118	4.311356	fe80::d40:4448:5018...	ff02::1:2	DHCPv6	150	Solicit XID: 0x8084a1 CID: 0001000103c2673c00004c552cb0
211	7.240392	fe80::5cda:e1f4:d07...	ff02::1:2	DHCPv6	150	Solicit XID: 0x3634f7 CID: 000100010d2a7d1000004d7cd3e

Frame 3: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on Interface 0
 Ethernet II, Src: Giga-Byt_7c:cd:3e (00:1a:4d:7c:cd:3e), Dst: IPv6cast_01:00:02 (33:33:00:01:00:02)
 Internet Protocol Version 6, Src: fe80::5cda:e1f4:d07e:7544, Dst: ff02::1:2
 User Datagram Protocol, Src Port: 346, Dst Port: 547
 DHCPv6

```

0000 33 33 00 01 00 02 00 1a 4d 7c cd 3e 00 00 00 00  33 . . . . M
0010 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00 . . . .
0020 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00 . . . .
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  00 . . . .
0040 34 f7 00 00 00 00 00 00 00 01 00 00 00 00 01  4 . . . .
0050 00 2a 7d 38 00 00 4d 7c cd 3e 00 03 00 0c 0e 00  0 . . . .
0060 00 4d 00 00 00 00 00 00 00 00 00 27 00 0a 00 00  0 . . . .
0070 41 64 6d 69 6e 23 50 43 00 10 00 0e 00 00 01 37  a d e i n - P C
0080 00 00 4d 53 46 54 20 35 2e 10 00 0e 00 00 00 18  . . . . M S T
0090 00 17 00 11 00 27  . . . .
  
```


STUDENT OBSERVATION

1. What is promiscuous mode?

A) It is a networking setting that allows a network adapter to capture all data packets on a network.

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

A) NO, ARP packets do not have TLH because ARP operates at data link layer.

3. Which transport layer protocol is used by DNS?

A) Uses UDP for speed port 53. TCP for larger data transfer.

4. What is the port no. used by HTTP protocols

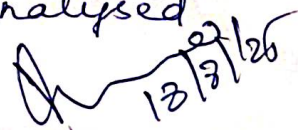
A) Standard port is port '80'.

5. What is a broadcast IP address.

A) A special address used to send a single message to all devices on a specific network simultaneously.

RESULT:

Hence the experiments conducted in Wireshark was successful and packets were captured and analysed

 12/3/26