

Name: Alok Bhawankar

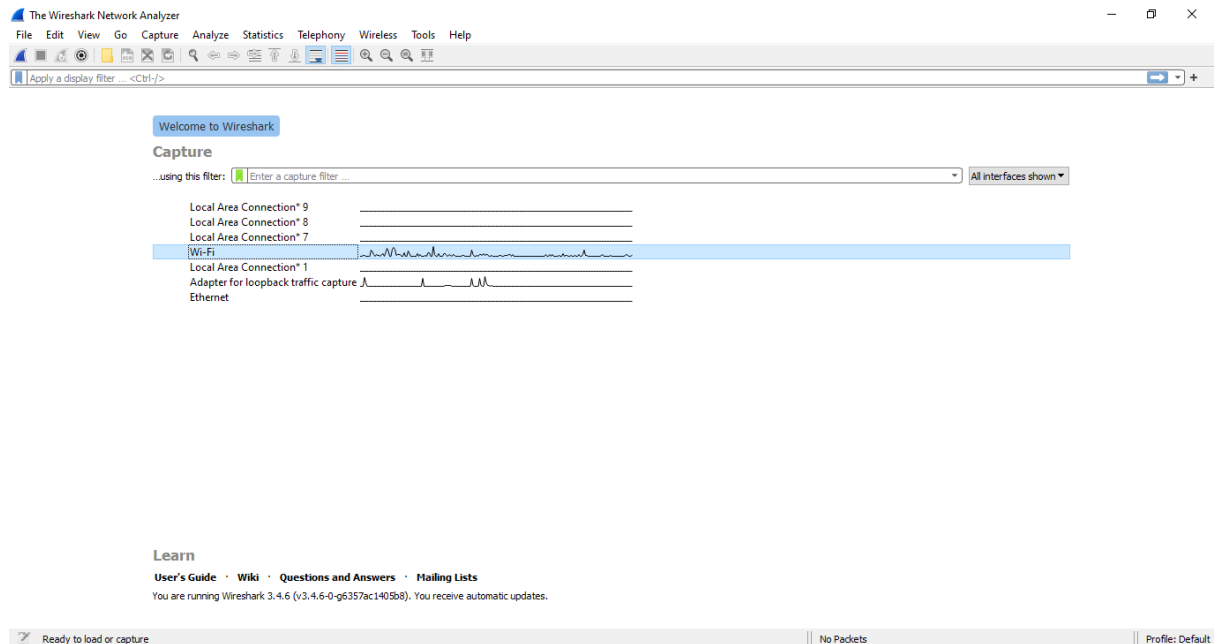
Roll No: CSE-37

PRN: 1032170126

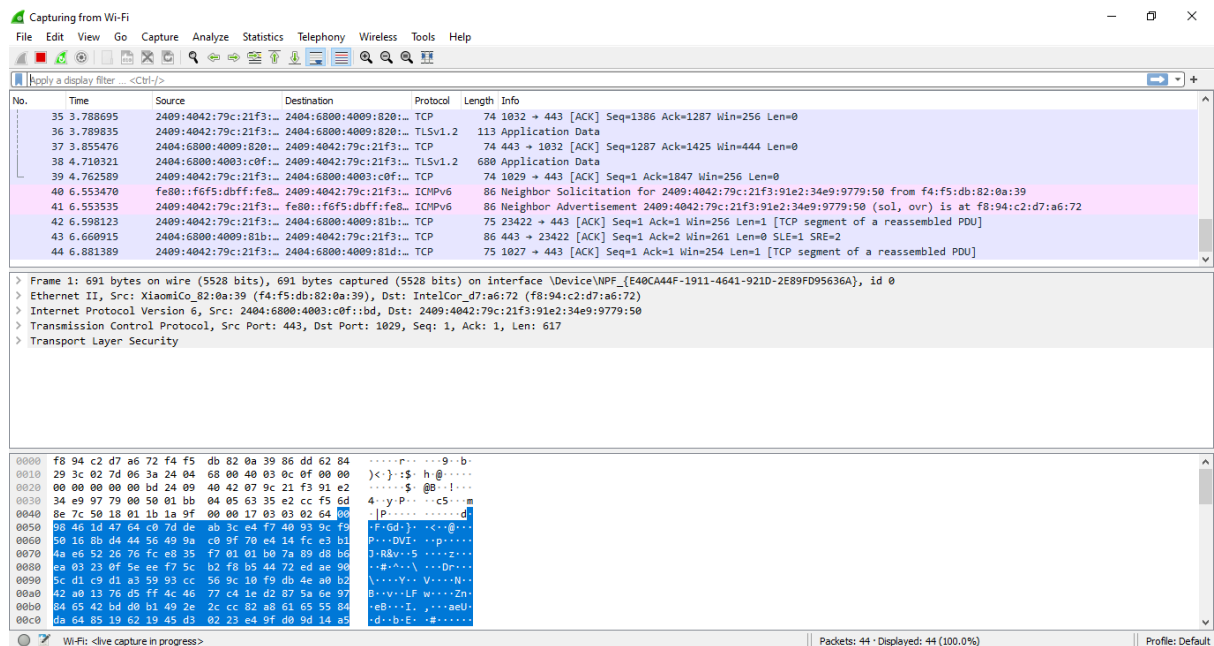
Lab Assignment 2

Wireshark

1) List of Interfaces



2) Capturing packets



3) Exploring TCP Packet

Capturing from Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp

No.	Time	Source	Destination	Protocol	Length	Info
1413	56.892727	XiaomiCo_82:0a:39	IntelCor_d7:a6:72	ARP	42	who has 192.168.43.61? Tell 192.168.43.162
1414	56.892742	IntelCor_d7:a6:72	XiaomiCo_82:0a:39	ARP	42	192.168.43.61 is at f8:94:c2:d7:a6:72
1415	57.036255	2404:6800:4009:80a::	2409:4042:79c:21f3::	TCP	86	[TCP Keep-Alive ACK] 443 → 21372 [ACK] Seq=1 Ack=2 Win=261 Len=0 SLE=1 SRE=2
1416	57.958180	2404:6800:4003:c0f::	2409:4042:79c:21f3::	TLSv1.2	697	Application Data
1417	58.011625	2409:4042:79c:21f3::	2404:6800:4003:c0f::	TCP	74	1029 → 443 [ACK] Seq=1 Ack=25928 Win=254 Len=0
1418	58.982253	2404:6800:4003:c0f::	2409:4042:79c:21f3::	TLSv1.2	680	Application Data
1419	58.982253	2404:6800:4003:c0f::	2409:4042:79c:21f3::	TLSv1.2	691	Application Data
1420	58.982325	2409:4042:79c:21f3::	2404:6800:4003:c0f::	TCP	74	1029 → 443 [ACK] Seq=1 Ack=27151 Win=256 Len=0
1421	59.596586	2404:6800:4003:c0f::	2409:4042:79c:21f3::	TLSv1.2	691	Application Data
1422	59.643444	2409:4042:79c:21f3::	2404:6800:4003:c0f::	TCP	74	1029 → 443 [ACK] Seq=1 Ack=27768 Win=254 Len=0

▼ Frame 1353: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{E40CA44F-1911-4641-921D-2E89FD95636A}, id 0

Interface id: 0 (\Device\NPF_{E40CA44F-1911-4641-921D-2E89FD95636A})

Encapsulation type: Ethernet (1)

Arrival Time: Jun 9, 2021 00:58:05.274960000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1623180365.274960000 seconds

[Time delta from previous captured frame: 0.050499000 seconds]

[Time delta from previous displayed frame: 0.050499000 seconds]

[Time since reference or first frame: 49.407124000 seconds]

Frame Number: 1353

Frame Length: 74 bytes (592 bits)

Capture Length: 74 bytes (592 bits)

```

0000 f4 f5 db 82 0a 39 f8 94 c2 d7 a6 72 86 dd 68 00 .....9...p...
0010 f8 3d 00 14 06 ff 24 09 40 42 07 9c 21 f3 91 e2 .....$.h@!...
0020 34 e9 97 79 00 50 24 04 68 00 40 09 0c 0f 00 00 4..yP$.h@!...
0030 00 00 00 00 00 00 04 05 01 bb f5 6d 8e 7c 63 36 .....m[c6
0040 45 a4 50 10 01 00 b7 0c 00 00 .....E-P....

```

Transmission Control Protocol: Protocol

Packets: 1422 · Displayed: 1422 (100.0%)

Profile: Default

4) Using Filters

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 80 || udp.port == 80

No.	Time	Source	Destination	Protocol	Length	Info
32259	176.504504	2404:6800:4009:820::	2409:4042:79c:21f3::	QUIC	87	Protected Payload (KP0)
32278	176.525036	2409:4042:79c:21f3::	2404:6800:4009:820::	QUIC	95	Protected Payload (KP0), DCID=33ac1lad1c6b02ed
32376	176.706749	2409:4042:79c:21f3::	2404:6800:4009:820::	QUIC	95	Protected Payload (KP0), DCID=33ac1lad1c6b02ed
32409	176.968493	2404:6800:4009:820::	2409:4042:79c:21f3::	QUIC	183	Protected Payload (KP0)
32500	176.968493	2404:6800:4009:820::	2409:4042:79c:21f3::	QUIC	1120	Protected Payload (KP0)
32501	176.968493	2404:6800:4009:820::	2409:4042:79c:21f3::	QUIC	318	Protected Payload (KP0)
32504	176.969213	2409:4042:79c:21f3::	2404:6800:4009:820::	QUIC	97	Protected Payload (KP0), DCID=33ac1lad1c6b02ed
32505	176.969397	2409:4042:79c:21f3::	2404:6800:4009:820::	QUIC	95	Protected Payload (KP0), DCID=33ac1lad1c6b02ed
32533	177.021094	2404:6800:4009:820::	2409:4042:79c:21f3::	QUIC	87	Protected Payload (KP0)
32638	177.215459	2404:6800:4009:820::	2409:4042:79c:21f3::	QUIC	87	Protected Payload (KP0)

▼ Frame 23427: 121 bytes on wire (968 bits), 121 bytes captured (968 bits) on interface \Device\NPF_{E40CA44F-1911-4641-921D-2E89FD95636A}, id 0

Interface id: 0 (\Device\NPF_{E40CA44F-1911-4641-921D-2E89FD95636A})

Encapsulation type: Ethernet (1)

Arrival Time: Jun 9, 2021 00:58:00.137368000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1623180480.137368000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 164.269532000 seconds]

Frame Number: 23427

Frame Length: 121 bytes (968 bits)

Capture Length: 121 bytes (968 bits)

```

0000 f8 94 c2 d7 a6 72 f4 f5 db 82 0a 39 86 dd 68 00 .....9...h.
0010 00 00 00 43 11 3b 24 04 68 00 40 09 08 20 00 00 ...C;$.h@!...
0020 00 00 00 00 20 0e 24 09 40 42 07 9c 21 f3 91 e2 .....$.h@!...
0030 34 e9 97 79 00 50 01 bb f3 cf 00 43 90 8a 4e 0c 4..yP$.h@!...
0040 00 27 00 3e 15 17 e0 4c ed 34 f7 68 74 9f 03 58 .....CGL-4ht...
0050 08 19 25 7c 95 12 bb 9f 52 32 3f 86 ea 45 90 9d ...%|....R2?..E.
0060 40 d4 f4 62 22 9a 5c e6 c3 ae 74 a4 db 30 0f 0b 0..b".\..t..0..
0070 82 98 62 61 08 40 da 87 c3 .....ba@...

```

"t" is neither a field nor a protocol name.

Packets: 33208 · Displayed: 1092 (3.3%)

Profile: Default

5) Filtering packets using TCP and IP address

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp and ip.addr==192.168.43.61

No.	Time	Source	Destination	Protocol	Length	Info
18	2.252748	91.108.56.186	192.168.43.61	SSL	674	Continuation Data
20	2.307598	192.168.43.61	91.108.56.186	TCP	54	18274 → 443 [ACK] Seq=1 Ack=621 Win=256 Len=0
48	7.795194	192.168.43.61	142.250.183.74	TCP	55	16184 → 443 [ACK] Seq=1 Ack=1 Win=256 Len=1 [TCP segment of a reassembled PDU]
49	7.883167	142.250.183.74	192.168.43.61	TCP	66	443 → 16184 [ACK] Seq=1 Ack=2 Win=266 Len=0 SLE=1 SRE=2
62	12.240549	192.168.43.61	91.108.56.186	SSL	207	Continuation Data
63	12.492408	91.108.56.186	192.168.43.61	TCP	54	443 → 18274 [ACK] Seq=621 Ack=154 Win=18796 Len=0
64	12.492408	91.108.56.186	192.168.43.61	SSL	143	Continuation Data
65	12.537428	192.168.43.61	91.108.56.186	TCP	54	18274 → 443 [ACK] Seq=154 Ack=710 Win=256 Len=0
507	22.118721	91.108.56.186	192.168.43.61	TCP	674	443 → 18274 [PSH, ACK] Seq=710 Ack=154 Win=18796 Len=620 [TCP segment of a reassembled PDU]
509	22.118721	91.108.56.186	192.168.43.61	TCP	159	443 → 18274 [PSH, ACK] Seq=1330 Ack=154 Win=18796 Len=105 [TCP segment of a reassembled PDU]

Frame 18: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits) on interface \Device\NPF_{E40CA44F-1911-4641-921D-2E89FD95636A}, id 0

Interface id: 0 (\Device\NPF_{E40CA44F-1911-4641-921D-2E89FD95636A})

Encapsulation type: Ethernet (1)

Arrival Time: Jun 9, 2021 00:55:18.120584000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1623180318.120584000 seconds

[Time delta from previous captured frame: 0.744101000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 2.252748000 seconds]

Frame Number: 18

Frame Length: 674 bytes (5392 bits)

Capture Length: 674 bytes (5392 bits)

0000 f8 94 c2 d7 a6 72 f4 f5 db 82 0a 39 08 00 45 289...E(
0010 02 94 6a b4 40 00 30 06 5d 7c 5b 6c 38 ba c0 a8 ...j @ 0:][[18...
0020 2b 3d 01 bb 47 62 1f 62 1b 2a af c1 17 cb 50 18 +=Gb b- *...P
0030 48 60 a7 0c 00 00 12 34 3a 33 8d 5b 9a e2 23 f0 H...4 3: [+*#
0040 11 8a b5 f9 33 02 66 2f 29 2b ac bc 67 04 90 ec ...3-f/ }+g...
0050 e5 7c f2 62 1a dd f3 4c 73 a6 6f 17 e2 e3 90 6d [-b...L s-o...l
0060 01 fc 94 4c 40 25 e8 ad 2d 93 71 31 80 ac b1 7d ...LHk...-q1...
0070 7d 17 18 fd ee f4 21 1c 6c 2d 6d 41 94 d8 a0 d2 }...1: 1-mA...
0080 43 6f 98 35 6c 10 b5 38 79 f9 e7 f8 52 90 80 73 Co-Sl-8 y--R-+s
0090 5e 43 90 63 79 83 f3 49 84 51 65 0a 0d 45 b6 6a ^Ccy:1 ^Qe:Etj
00a0 86 ea 97 4d 4a 9a 72 61 7f e0 a5 7c 05 fd c1 69 ...HJ-ra ...-1...
00b0 5a c0 a0 8a f7 85 a7 a1 eb 39 8c f2 4a 2d b5 64 Z.....9-1-+d
00c0 c8 cd 7e 81 09 ce 6a d4 80 a1 18 e5 ab bc 99 53j.....S

Packets: 93824 · Displayed: 564 (0.6%) Profile: Default

6) TCP flag ACK Filter

Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.ack

No.	Time	Source	Destination	Protocol	Length	Info
1688..	346.521625	2600:9000:21fe:4a00..	2409:4042:79c:21f3:..	TCP	11054	443 → 1050 [PSH, ACK] Seq=189138015 Ack=5076 Win=71680 Len=10980 [TCP segment of a reassembled PDU]
1688..	346.521676	2409:4042:79c:21f3:..	2600:9000:21fe:4a00..	TCP	74	1050 → 443 [ACK] Seq=5076 Ack=189148995 Win=3181568 Len=0
1688..	346.523422	2600:9000:21fe:4a00..	2409:4042:79c:21f3:..	TLSv1.3	11054	Application Data [TCP segment of a reassembled PDU]
1688..	346.523473	2409:4042:79c:21f3:..	2600:9000:21fe:4a00..	TCP	74	1050 → 443 [ACK] Seq=5076 Ack=189159975 Win=3181568 Len=0
1688..	346.524261	2600:9000:21fe:4a00..	2409:4042:79c:21f3:..	TLSv1.3	9834	Application Data [TCP segment of a reassembled PDU]
1688..	346.524303	2409:4042:79c:21f3:..	2600:9000:21fe:4a00..	TCP	74	1050 → 443 [ACK] Seq=5076 Ack=189169735 Win=3181568 Len=0
1688..	346.528290	2600:9000:21fe:4a00..	2409:4042:79c:21f3:..	TCP	1294	443 → 1050 [ACK] Seq=189169735 Ack=5076 Win=71680 Len=1220 [TCP segment of a reassembled PDU]
1688..	346.528988	2600:9000:21fe:4a00..	2409:4042:79c:21f3:..	TCP	4954	443 → 1050 [PSH, ACK] Seq=189170955 Ack=5076 Win=71680 Len=4880 [TCP segment of a reassembled PDU]
1688..	346.529037	2409:4042:79c:21f3:..	2600:9000:21fe:4a00..	TCP	74	1050 → 443 [ACK] Seq=5076 Ack=189175835 Win=3181568 Len=0
1688..	346.531190	2600:9000:21fe:4a00..	2409:4042:79c:21f3:..	TCP	1294	443 → 1050 [PSH, ACK] Seq=189175835 Ack=5076 Win=71680 Len=1220 [TCP segment of a reassembled PDU]

Frame 18: 674 bytes on wire (5392 bits), 674 bytes captured (5392 bits) on interface \Device\NPF_{E40CA44F-1911-4641-921D-2E89FD95636A}, id 0

Interface id: 0 (\Device\NPF_{E40CA44F-1911-4641-921D-2E89FD95636A})

Encapsulation type: Ethernet (1)

Arrival Time: Jun 9, 2021 00:55:18.120584000 India Standard Time

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1623180318.120584000 seconds

[Time delta from previous captured frame: 0.744101000 seconds]

[Time delta from previous displayed frame: 0.744101000 seconds]

[Time since reference or first frame: 2.252748000 seconds]

Frame Number: 18

Frame Length: 674 bytes (5392 bits)

Capture Length: 674 bytes (5392 bits)

0000 f8 94 c2 d7 a6 72 f4 f5 db 82 0a 39 08 00 45 289...E(
0010 02 94 6a b4 40 00 30 06 5d 7c 5b 6c 38 ba c0 a8 ...j @ 0:][[18...
0020 2b 3d 01 bb 47 62 1f 62 1b 2a af c1 17 cb 50 18 +=Gb b- *...P
0030 48 60 a7 0c 00 00 12 34 3a 33 8d 5b 9a e2 23 f0 H...4 3: [+*#
0040 11 8a b5 f9 33 02 66 2f 29 2b ac bc 67 04 90 ec ...3-f/ }+g...
0050 e5 7c f2 62 1a dd f3 4c 73 a6 6f 17 e2 e3 90 6d [-b...L s-o...l
0060 01 fc 94 4c 40 25 e8 ad 2d 93 71 31 80 ac b1 7d ...LHk...-q1...
0070 7d 17 18 fd ee f4 21 1c 6c 2d 6d 41 94 d8 a0 d2 }...1: 1-mA...
0080 43 6f 98 35 6c 10 b5 38 79 f9 e7 f8 52 90 80 73 Co-Sl-8 y--R-+s
0090 5e 43 90 63 79 83 f3 49 84 51 65 0a 0d 45 b6 6a ^Ccy:1 ^Qe:Etj
00a0 86 ea 97 4d 4a 9a 72 61 7f e0 a5 7c 05 fd c1 69 ...HJ-ra ...-1...
00b0 5a c0 a0 8a f7 85 a7 a1 eb 39 8c f2 4a 2d b5 64 Z.....9-1-+d
00c0 c8 cd 7e 81 09 ce 6a d4 80 a1 18 e5 ab bc 99 53j.....S

Packets: 168825 · Displayed: 166598 (98.7%) Profile: Default