Experiment: 1

Student Name: Yash Kumar
UID: 20BCS9256
Branch: BE-CSE
Section/Group: 616 'B'

Web and Mobile Security

Aim: Open any website on computer system and identify http packets on monitoring tool like wireshark

Objective: To analyse http traffic.

Software/Hardware Requirements: Window 7 and above version

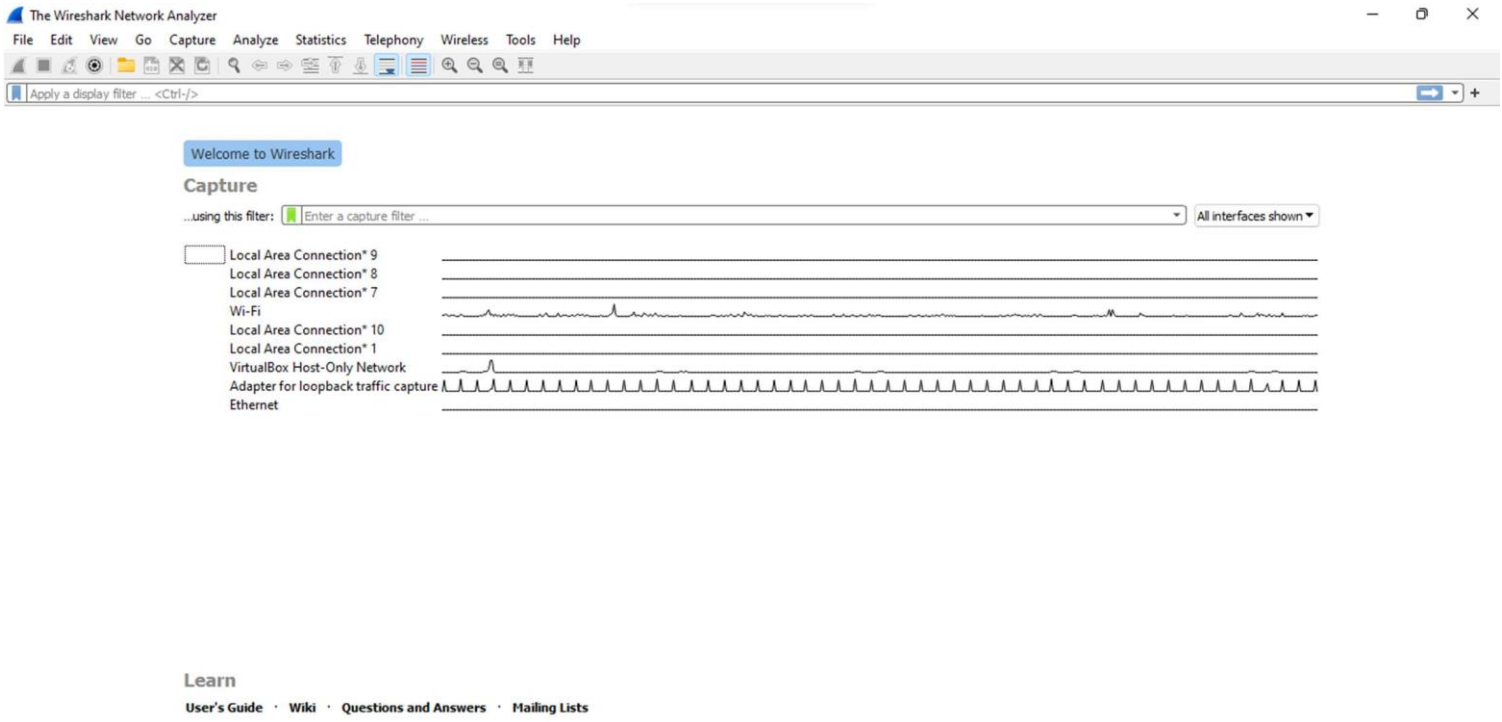
Tools Used:

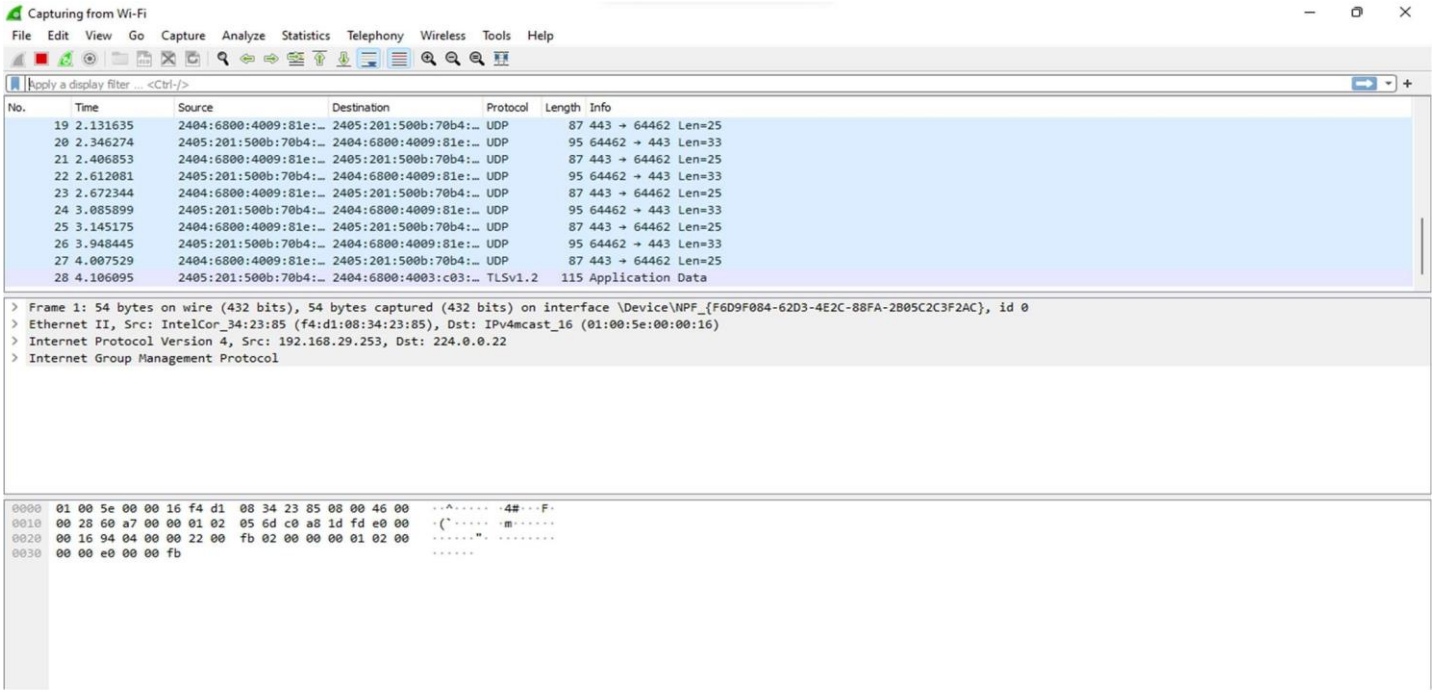
1. Wireshark Packet sniffer and Packet Capture Library.
2. Microsoft word.

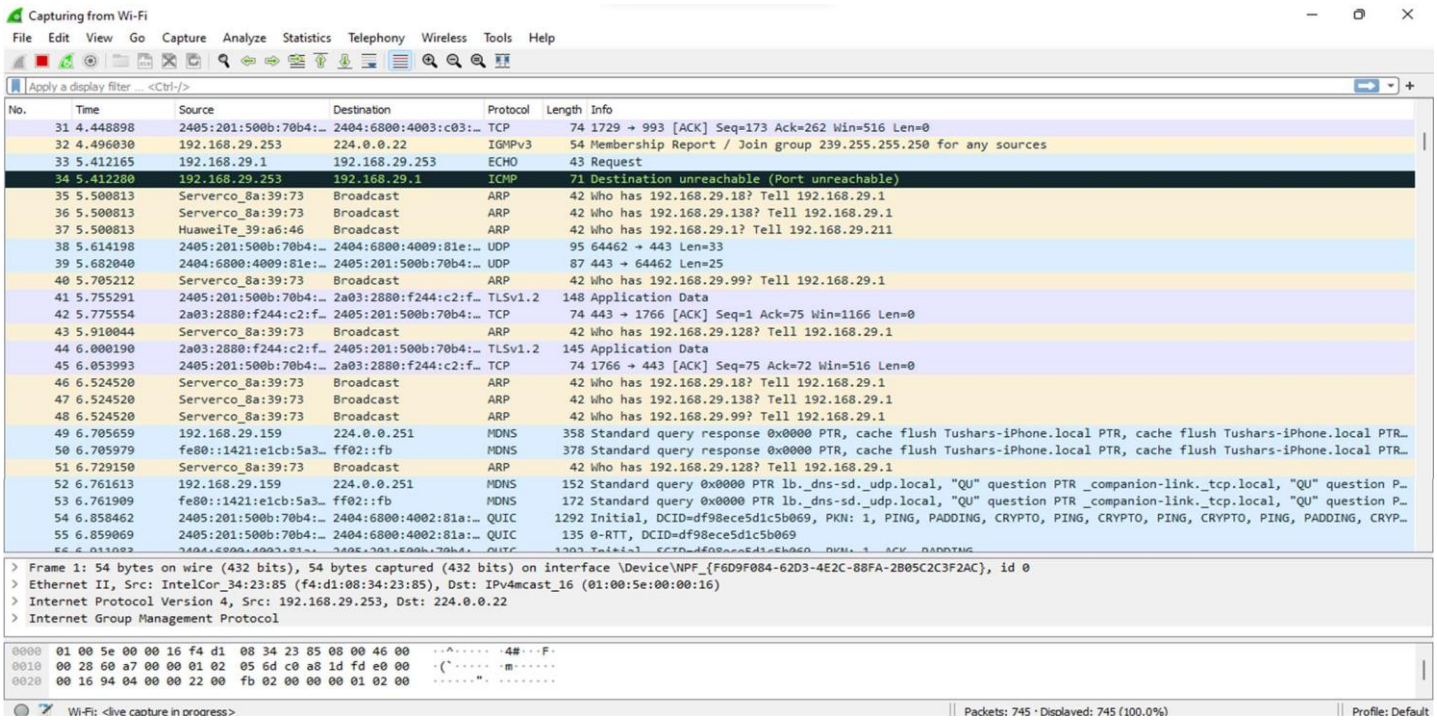
Steps/Method/Coding:

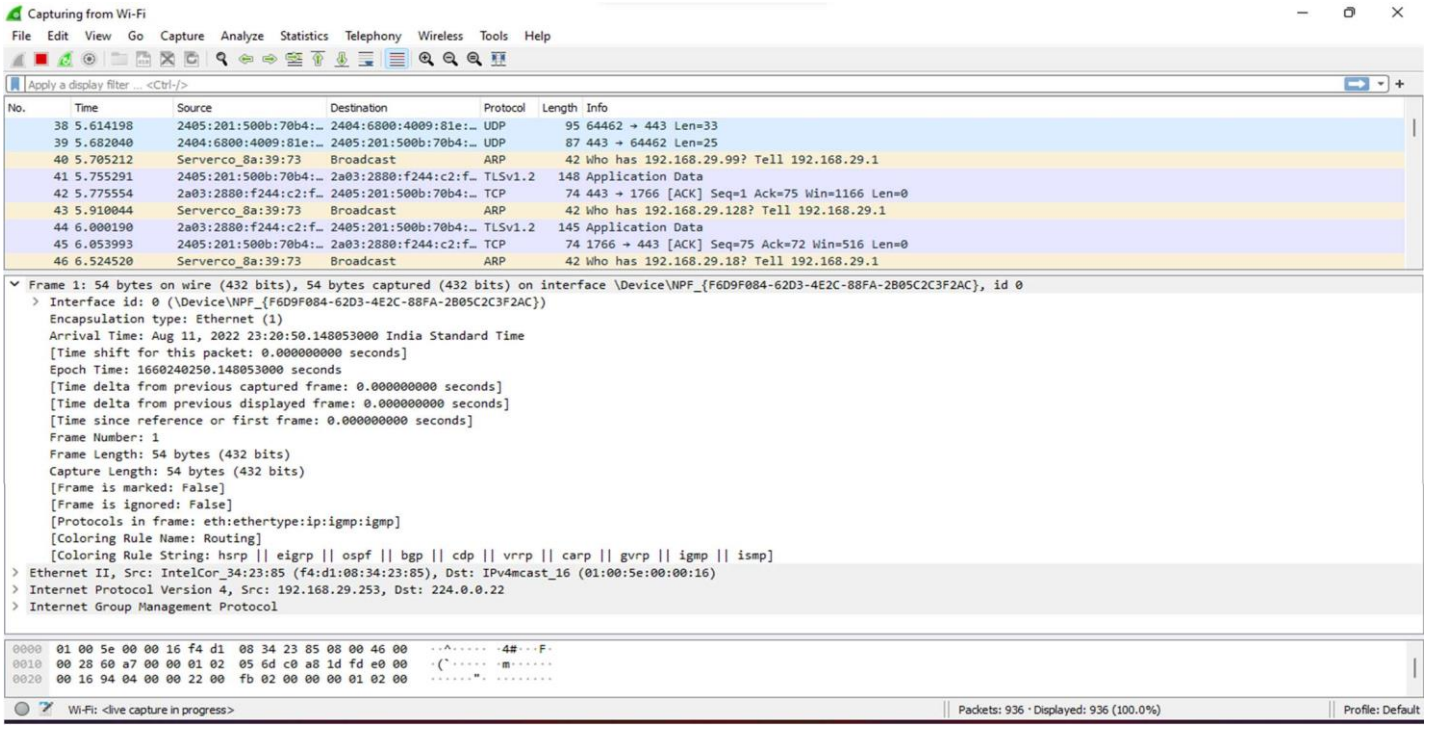
1. Install Wireshark.
2. Open your Internet browser.
3. Clear your browser cache.
4. Open Wireshark
5. Click on "Capture > Interfaces". A pop-up window will display.
6. You'll want to capture traffic that goes through your Ethernet driver. Click on the Start buttonto capture traffic via this interface.
7. Visit the URL that you wanted to capture the traffic from.
8. Go back to your Wireshark screen and press Ctrl + E to stop capturing.
9. After the traffic capture is stopped, please save the captured traffic intoa *.pcap format file and attach it to your support ticket.

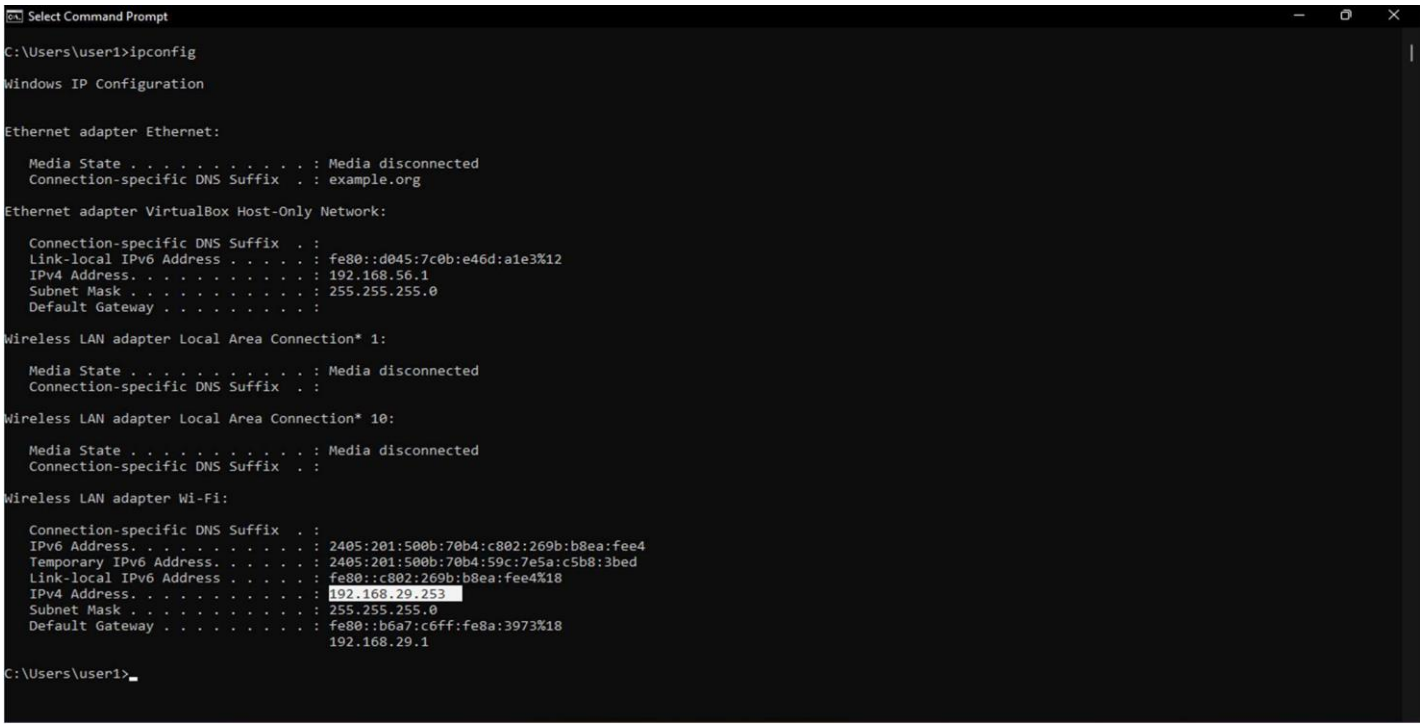
Output screenshot:

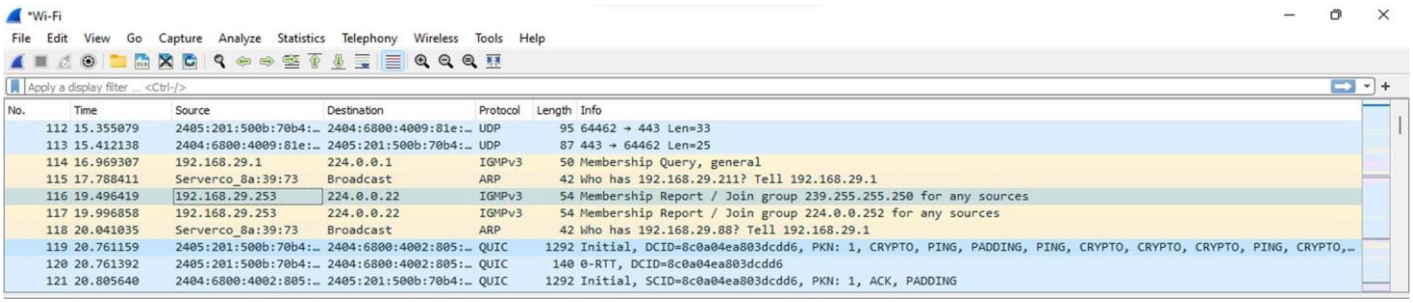





Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
31 4.448898 2405:201:500b:70b4:... 2404:6800:4003:c03:... TCP 74 1729 → 993 [ACK] Seq=173 Ack=262 Win=516 Len=0
32 4.496030 192.168.29.253 224.0.0.22 IGMPv3 54 Membership Report / Join group 239.255.255.250 for any sources
33 5.412165 192.168.29.1 192.168.29.253 ECHO 43 Request
34 5.412280 192.168.29.253 192.168.29.1 ICMP 71 Destination unreachable (Port unreachable)
35 5.500813 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.18? Tell 192.168.29.1
36 5.500813 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.138? Tell 192.168.29.1
37 5.500813 HuaweiTe_39:a6:46 Broadcast ARP 42 Who has 192.168.29.1? Tell 192.168.29.211
38 5.614198 2405:201:500b:70b4:... 2404:6800:4009:81e:... UDP 95 64462 → 443 Len=33
39 5.682040 2404:6800:4009:81e:... 2405:201:500b:70b4:... UDP 87 443 → 64462 Len=25
40 5.705212 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.99? Tell 192.168.29.1
41 5.755291 2405:201:500b:70b4:... 2a03:2880:f244:c2:f... TLSv1.2 148 Application Data
42 5.775554 2a03:2880:f244:c2:f... 2405:201:500b:70b4:... TCP 74 443 → 1766 [ACK] Seq=1 Ack=75 Win=1166 Len=0
43 5.910044 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.128? Tell 192.168.29.1
44 6.000190 2a03:2880:f244:c2:f... 2405:201:500b:70b4:... TLSv1.2 145 Application Data
45 6.053993 2405:201:500b:70b4:... 2a03:2880:f244:c2:f... TCP 74 1766 → 443 [ACK] Seq=75 Ack=72 Win=516 Len=0
46 6.524520 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.18? Tell 192.168.29.1
47 6.524520 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.138? Tell 192.168.29.1
48 6.524520 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.99? Tell 192.168.29.1
49 6.705659 192.168.29.159 224.0.0.251 MDNS 358 Standard query response 0x0000 PTR, cache flush Tushars-iPhone.local PTR, cache flush Tushars-iPhone.local PTR...
50 6.705979 fe80::1421:e1cb:5a3... ff02::fb MDNS 378 Standard query response 0x0000 PTR, cache flush Tushars-iPhone.local PTR, cache flush Tushars-iPhone.local PTR...
51 6.729150 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.128? Tell 192.168.29.1
52 6.761613 192.168.29.159 224.0.0.251 MDNS 152 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU" question PTR _companion-link._tcp.local, "QU" question P...
53 6.761909 fe80::1421:e1cb:5a3... ff02::fb MDNS 172 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QU" question PTR _companion-link._tcp.local, "QU" question P...
54 6.858462 2405:201:500b:70b4:... 2404:6800:4002:81a:... QUIC 1292 Initial, DCID=df98ece5d1c5b069, PKN: 1, PING, PADDING, CRYPTO, PING, CRYPTO, PING, CRYPTO, PING, PADDING, CRYP...
55 6.859069 2405:201:500b:70b4:... 2404:6800:4002:81a:... QUIC 135 0-RTT, DCID=df98ece5d1c5b069
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{F6D9F084-62D3-4E2C-88FA-2B05C2C3F2AC}, id 0
Ethernet II, Src: IntelCor_34:23:85 (f4:d1:08:34:23:85), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
Internet Protocol Version 4, Src: 192.168.29.253, Dst: 224.0.0.22
Internet Group Management Protocol
0000 01 00 5e 00 00 16 f4 d1 08 34 23 85 08 00 46 00
0010 00 28 60 a7 00 00 01 02 05 6d c0 a8 1d fd e0 00
0020 00 16 94 04 00 00 22 00 fb 02 00 00 00 01 02 00
Wi-Fi: <live capture in progress>
Packets: 745 · Displayed: 745 (100.0%)
Profile: Default


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
38 5.614198 2405:201:500b:70b4:... 2404:6800:4009:81e:... UDP 95 64462 → 443 Len=33
39 5.682040 2404:6800:4009:81e:... 2405:201:500b:70b4:... UDP 87 443 → 64462 Len=25
40 5.705212 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.99? Tell 192.168.29.1
41 5.755291 2405:201:500b:70b4:... 2a03:2880:f244:c2:f... TLSv1.2 148 Application Data
42 5.775554 2a03:2880:f244:c2:f... 2405:201:500b:70b4:... TCP 74 443 → 1766 [ACK] Seq=1 Ack=75 Win=1166 Len=0
43 5.910044 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.128? Tell 192.168.29.1
44 6.000190 2a03:2880:f244:c2:f... 2405:201:500b:70b4:... TLSv1.2 145 Application Data
45 6.053993 2405:201:500b:70b4:... 2a03:2880:f244:c2:f... TCP 74 1766 → 443 [ACK] Seq=75 Ack=72 Win=516 Len=0
46 6.524520 Serverco_8a:39:73 Broadcast ARP 42 Who has 192.168.29.18? Tell 192.168.29.1
Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{F6D9F084-62D3-4E2C-88FA-2B05C2C3F2AC}, id 0
Interface id: 0 (\Device\NPF_{F6D9F084-62D3-4E2C-88FA-2B05C2C3F2AC})
Encapsulation type: Ethernet (1)
Arrival Time: Aug 11, 2022 23:20:50.148053000 India Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1660240250.148053000 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: 0.000000000 seconds]
Frame Number: 1
Frame Length: 54 bytes (432 bits)
Capture Length: 54 bytes (432 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth:ethertype:ip:igmp:igmp]
[Coloring Rule Name: Routing]
[Coloring Rule String: hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp]
Ethernet II, Src: IntelCor_34:23:85 (f4:d1:08:34:23:85), Dst: IPv4mcast_16 (01:00:5e:00:00:16)
Internet Protocol Version 4, Src: 192.168.29.253, Dst: 224.0.0.22
Internet Group Management Protocol
0000 01 00 5e 00 00 16 f4 d1 08 34 23 85 08 00 46 00
0010 00 28 60 a7 00 00 01 02 05 6d c0 a8 1d fd e0 00
0020 00 16 94 04 00 00 22 00 fb 02 00 00 00 01 02 00
Wi-Fi: <live capture in progress>
Packets: 936 · Displayed: 936 (100.0%)
Profile: Default





Learning Outcomes (What I have learnt):

- Became familiar with how and when to capture the data packet appropriately.
- The aim is to help you develop and understanding of packet-sniffer placement.
- I got to know the different guidelines for Packet Sniffing in network and internet working environment.