Experiment 4:- Perform the practical sniffing tool -Wireshark and install Quad9 on Windows. (CO2)

Student Name: *Abhishek Kumar* **UID:** *20BCS3536*
Branch: *Information Security* **Section/Group:** *20BIS-1/A*
Semester: *5th semester* **Date of Performance:** *12/09/2022*
Subject Name: *Security Intelligence lab* **Subject Code:** *20CSB-343*

1. **Aim/Overview of the practical:**
   (A) Install Wireshark and Quad9.
   (B) Understand the working of Wireshark and Quad9.

2. **Task to be done:**
   Perform the practical of sniffing tool -Wireshark and install Quad9 on Windows. (CO2)

3. Theory:

Quad 9:

Quad9 is a free service that replaces your default ISP or enterprise Domain Name Server (DNS) configuration. When your computer performs any Internet transaction that uses the DNS (and most transactions do), Quad9 blocks lookups of malicious host names from an up-to-the-minute list of threats. This blocking action protects your computer, mobile device, or IoT systems against a wide range of threats such as malware, phishing, spyware, and botnets, and it can improve performance in addition to guaranteeing privacy.

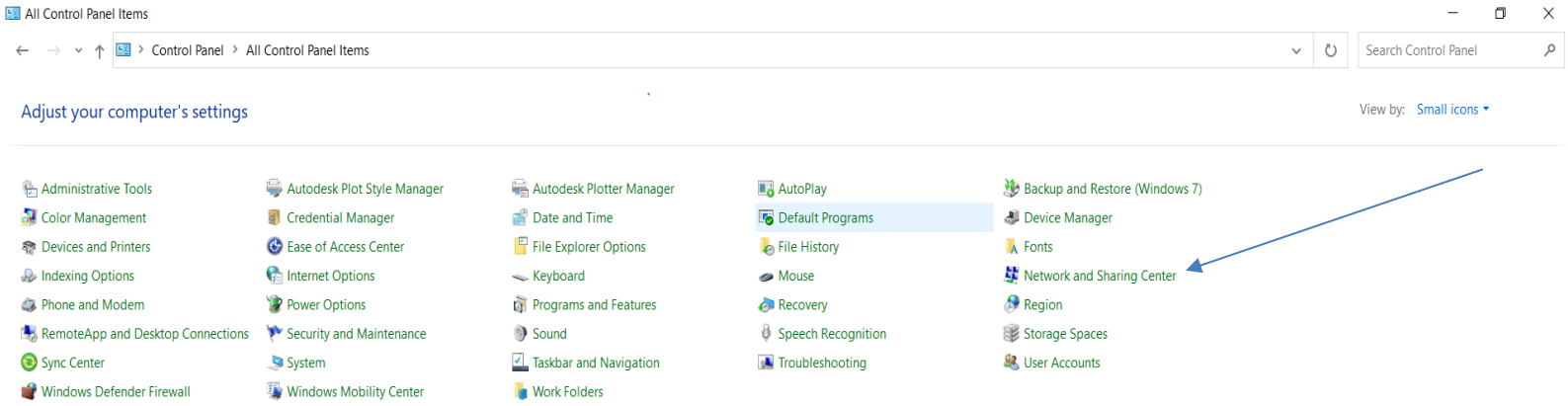
Wireshark:

Wireshark is a packet sniffer and analysis tool. It captures network traffic from ethernet, Bluetooth, wireless (IEEE.802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.

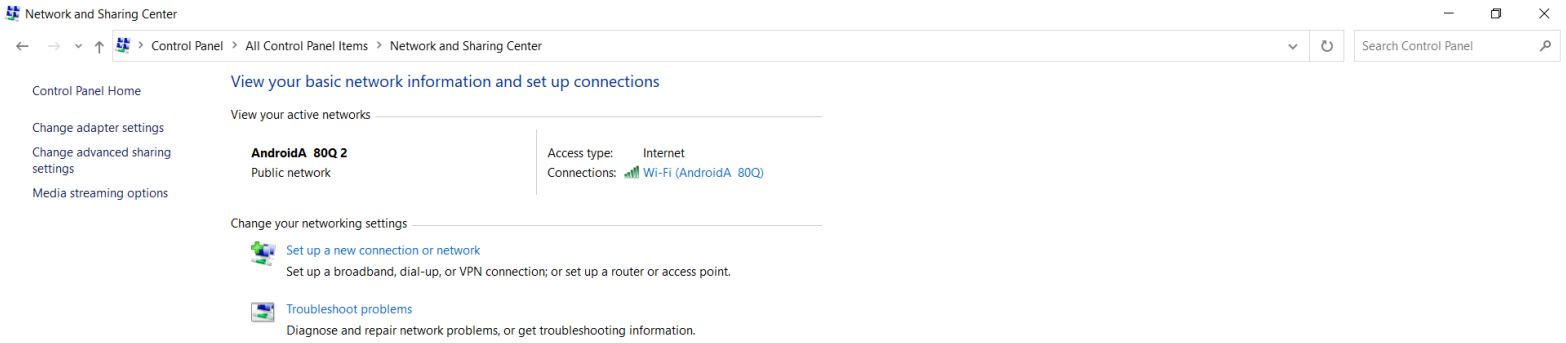
4. Steps and Results:

a. Install Quad 9 on the system:

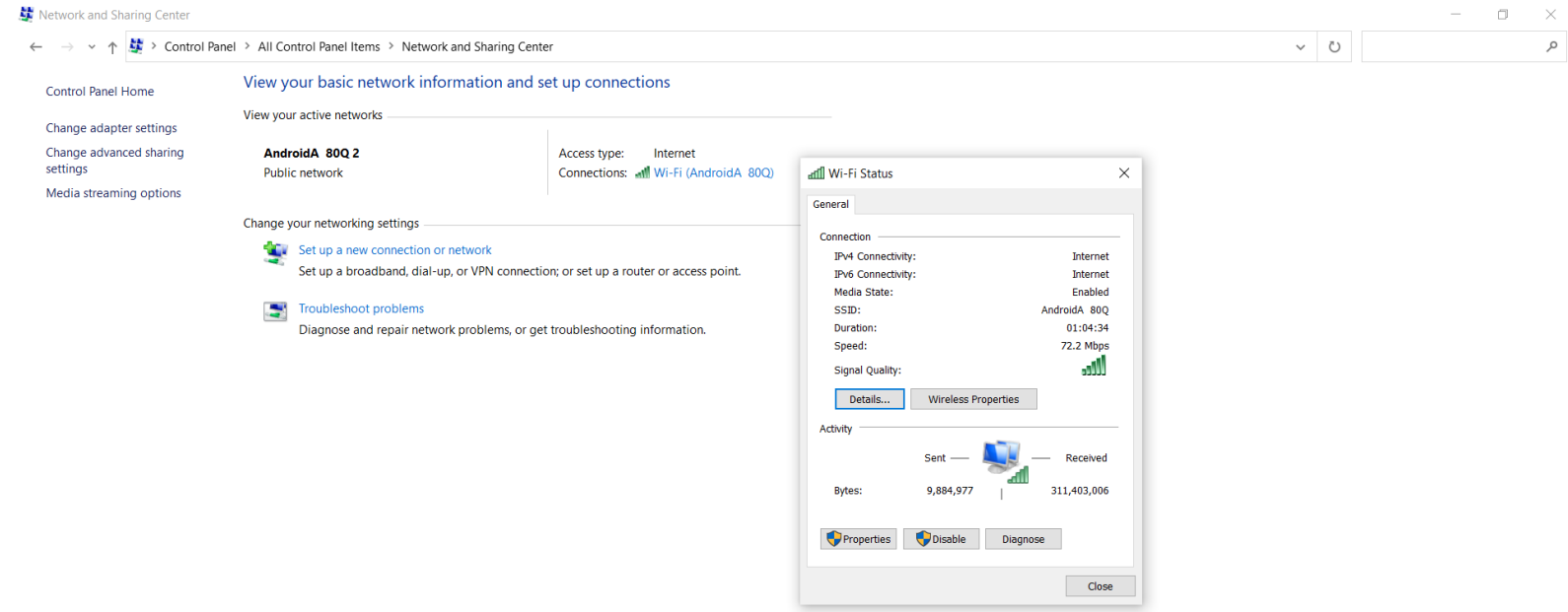
i.) Search **'Control Panel'** on search bar. Open it and click on the **'Network and Sharing centre'.**



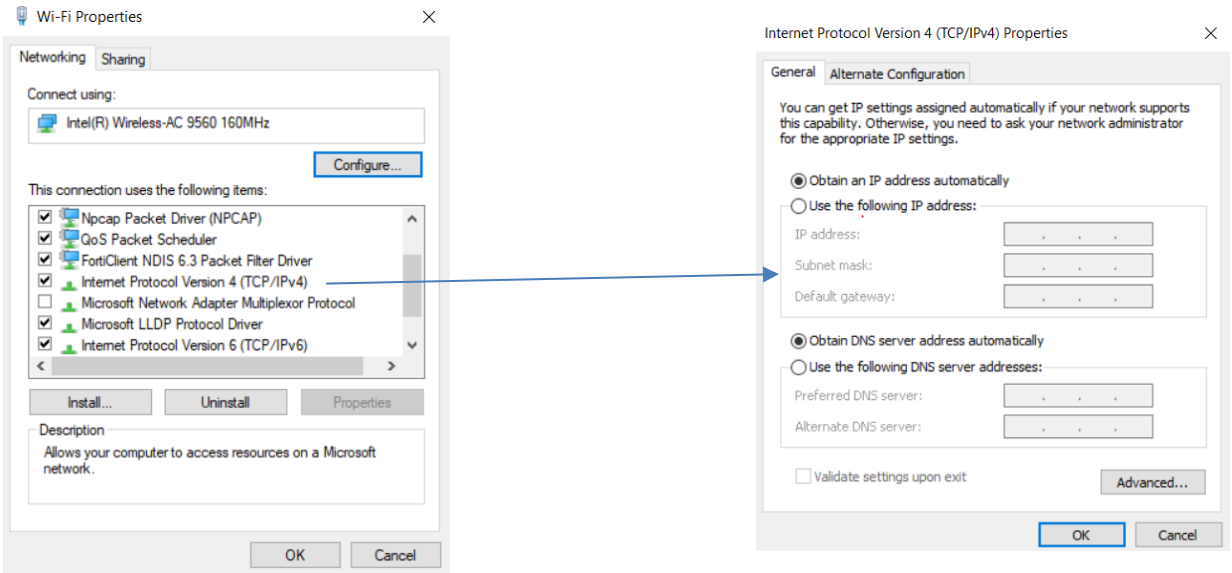
ii.) A new window will open where your basic network information and set up connections will be displayed.



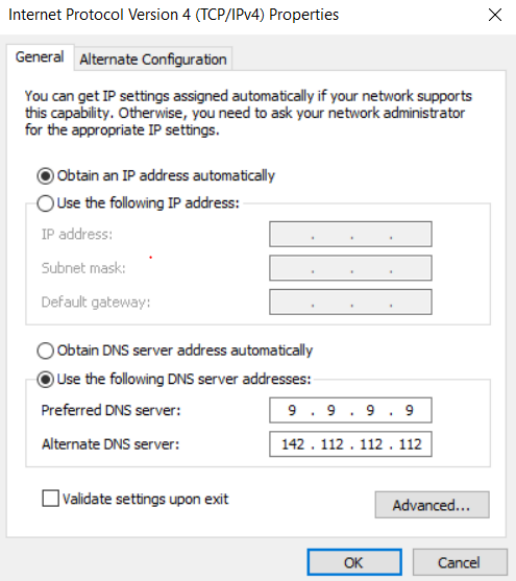
iii.) Now to setup quad 9 in your windows you have to right click on the connections under the view your active networks. After right clicking a new pop window will open.



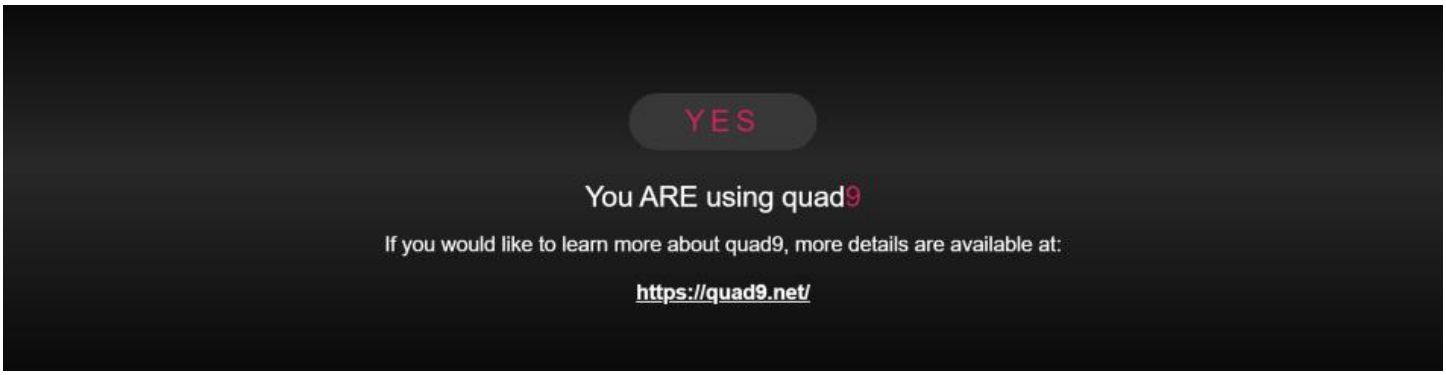
iv.) Now click on properties. Click on IPv4 if you are using IPv4 otherwise click on IPv6. A dialog box will open. Click on the check box 'Use the following DNS server addresses.'



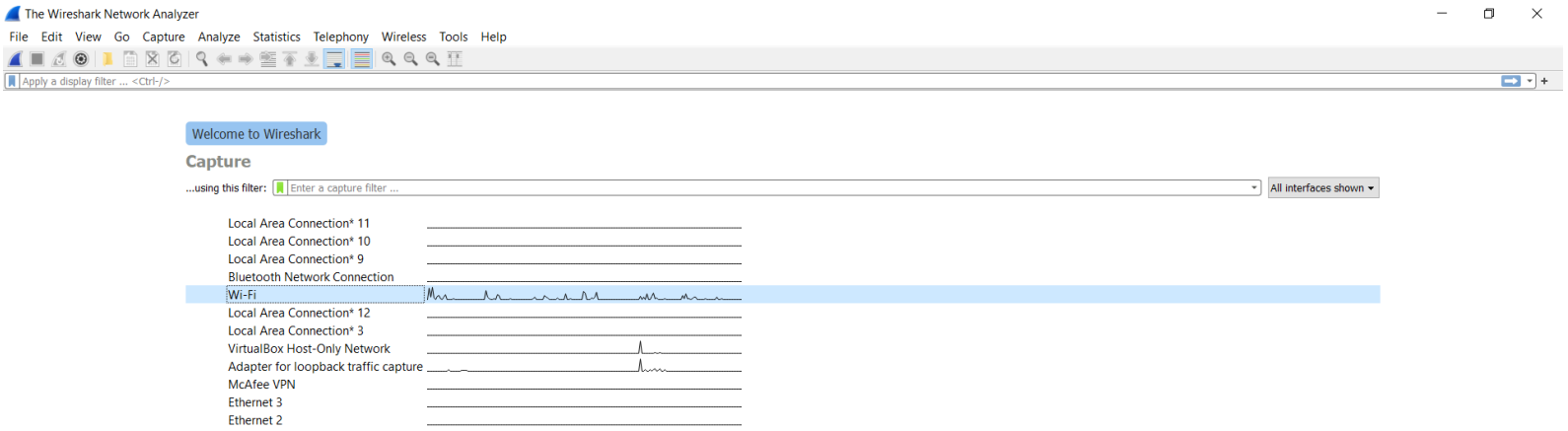
v.) Use preferred DNS server as **'9.9.9.9'** and alternate DNS server as **'149.112.112.112'**. Now Click on OK.



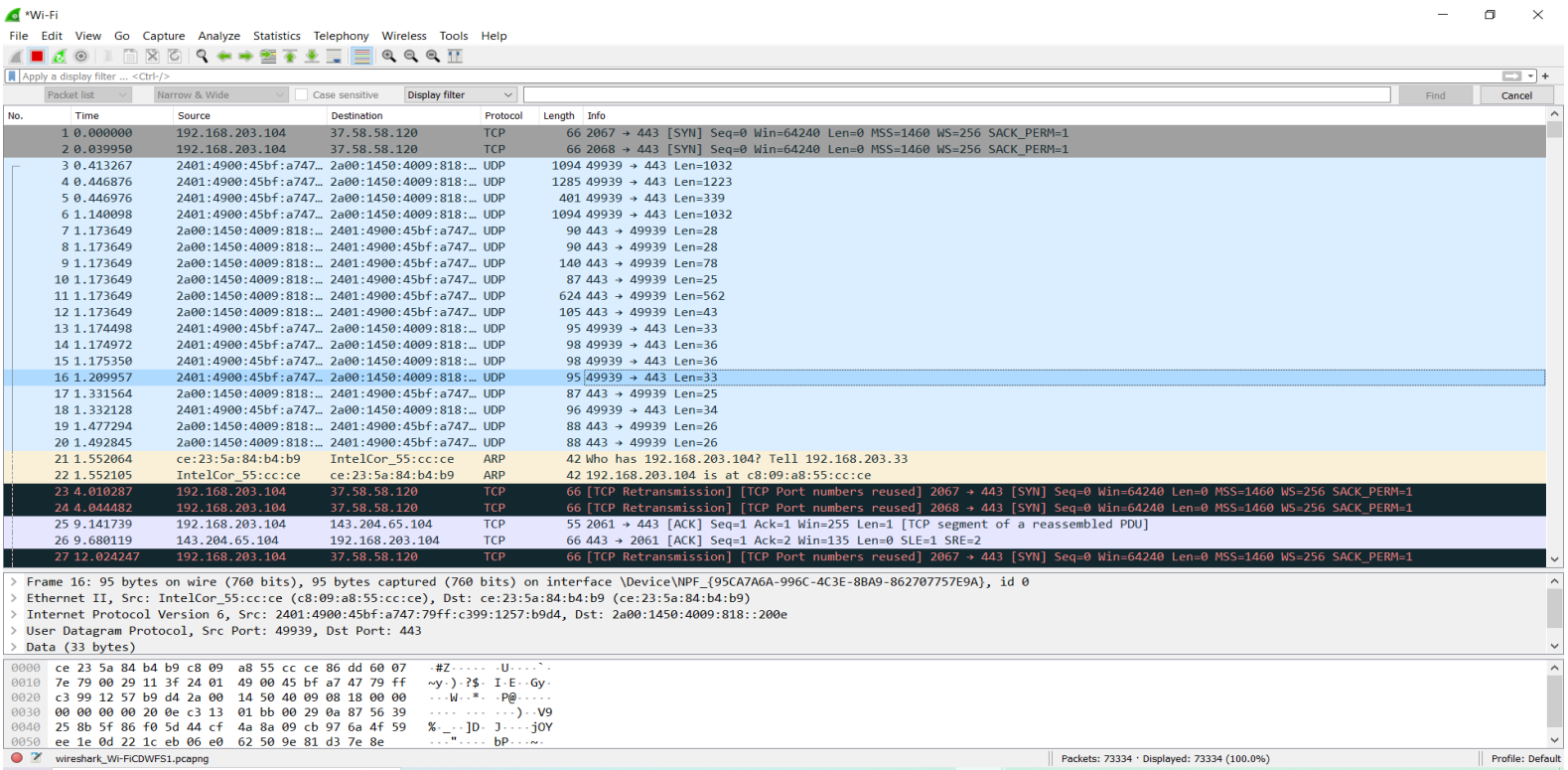
vi.) Now to check that Quad 9 setup is working successfully on your system you have to open https://on.quad9.net/ on your system if it is working fine than it shows 'Yes' otherwise 'No'.



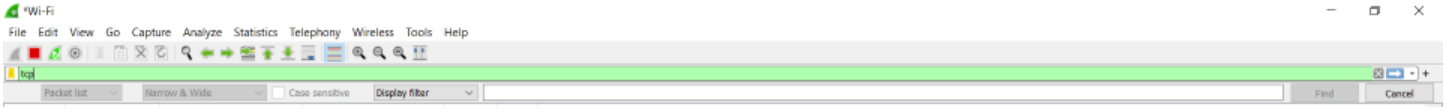
Wireshark: Open Wireshark. Click on Wi-Fi. Now you can able to capture all packets on Wi-Fi.



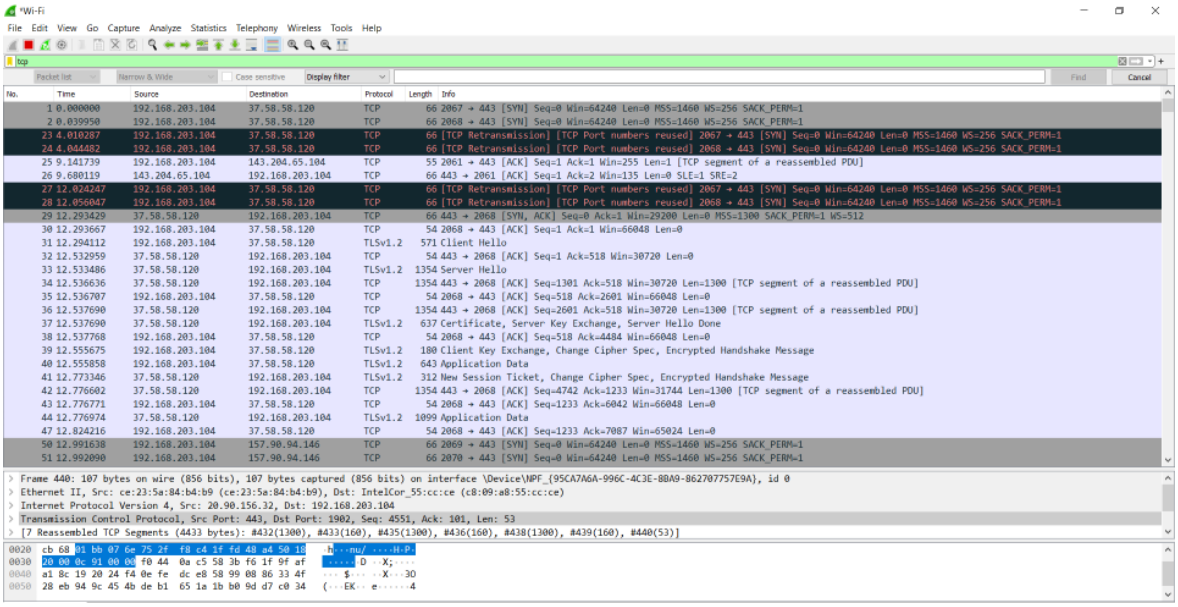
ii.) Now new window will open on the screen with detailed information about captured packets (i.e.- length of packet, protocol type of the packet and source and destination IP addresses).



iii.) You can use filter to get particular information from the captured packets.

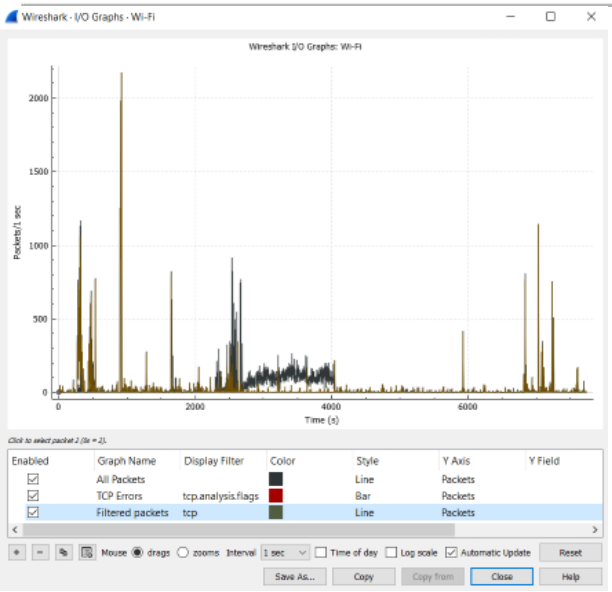


Result after using filter option.



If we want to create a graph on the result which we get after capturing the packets. We have to follow the following steps:

1. Click on the Statistics on the menu bar. After that click on the I/O graph.



Wireshark · Capture File Properties · Wi-Fi

Details

File

Name:	C:\Users\Abhishek\AppData\Local\Temp\wireshark_Wi-FiCDWFS1.pcapng
Length:	62 MB
Hash (SHA256):	cfe517e814b643ad2c28eaa067cfb2de433893022788365a84f2cc9645cac9d7
Hash (RIPEMD160):	2135374ee6339e7075b0b580b9c06b1ae76c7802
Hash (SHA1):	0daba5903c609ce8f24c8442eab338e111bf094e
Format:	Wireshark/... - pcapng
Encapsulation:	Ethernet

Time

First packet:	2022-09-23 13:28:56
Last packet:	2022-09-23 14:04:27
Elapsed:	00:35:30

Capture

Hardware:	Intel(R) Core(TM) i5-10210U CPU @ 1.60GHz (with SSE4.2)
OS:	64-bit Windows 10 (21H2), build 19044
Application:	Dumpcap (Wireshark) 3.6.8 (v3.6.8-0-gd25900c51508)

Interfaces

Interface	Dropped packets	Capture filter	Link type	Packet size limit (snaplen)
Wi-Fi	Unknown	none	Ethernet	262144 bytes

Statistics

Measurement	Captured	Displayed	Marked
Packets	87104	71081 (81.6%)	—
Time span, s	2130.837	2127.663	—
Average pps	40.9	33.4	—
Average packet size, B	688	702	—
Bytes	59907036	49921784 (83.3%)	0
Average bytes/s	28 k	23 k	—
Average bits/s	224 k	187 k	—

Capture file comments

Refresh | Save Comments | Close | Copy To Clipboard | Help

Learning outcomes (What I have learnt):

1. Basics of Quad9.

2. Basics of Wireshark.

3. Working and installation of Wireshark.

4. Working and installation of Quad 9.

Evaluation Grid (To be created as per the SOP and Assessment guidelines by the faculty):

Sr. No.	Parameters	Marks Obtained	Maximum Marks
1.			
2.			
3.			