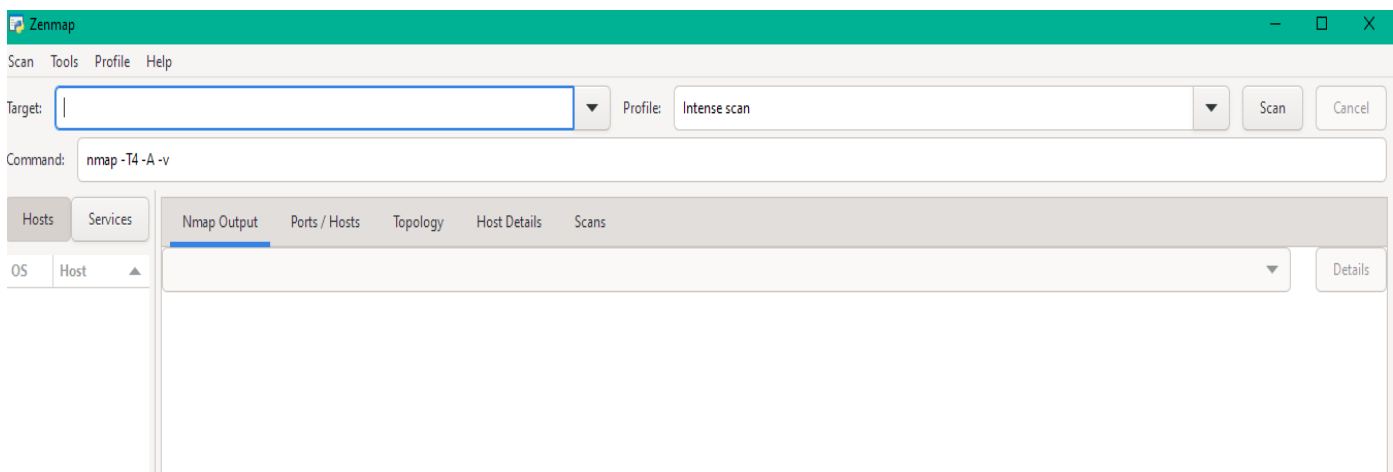


Nmap Port scanning:

Initially Nmap was used to see the network ports whether they are open/closed.

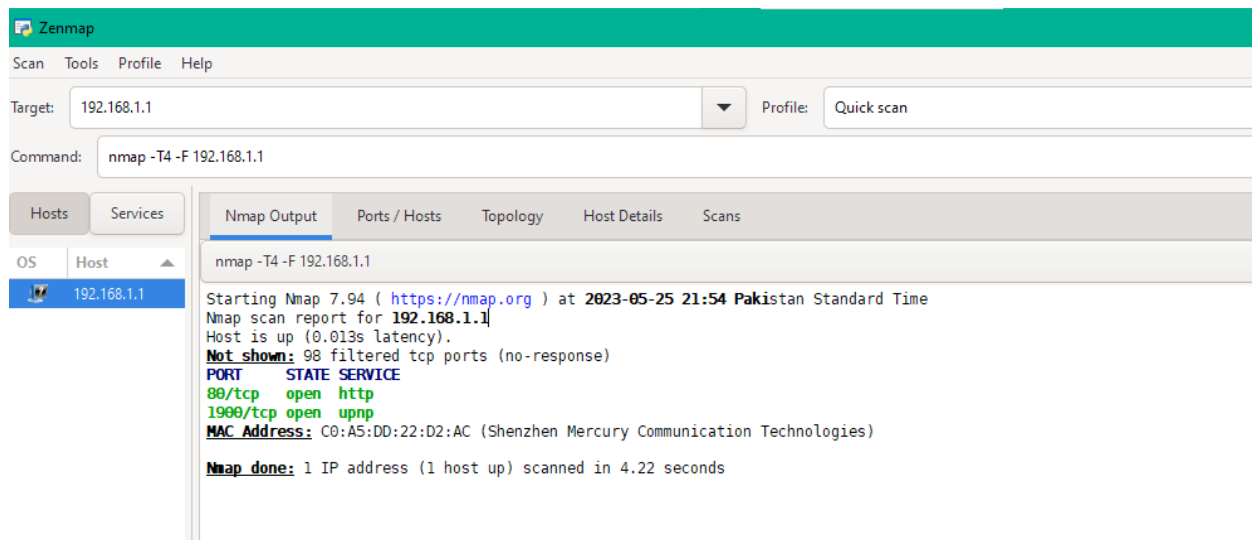
1. Scan for service and version detection:

In addition to checking whether network ports are open or closed, Nmap can also identify the services running on those ports and provide information about the version of the service. This can be useful in understanding the specific software or application running on each port and its associated vulnerabilities.



2. Vulnerability scanning:

Nmap has the capability to perform vulnerability scanning by using NSE (Nmap Scripting Engine) scripts. These scripts can help identify specific vulnerabilities present on the target system or network. You can utilize Nmap's extensive collection of NSE scripts to scan for common vulnerabilities, misconfigurations, or weaknesses in network services. This involves entering targets IP in the initial stage.

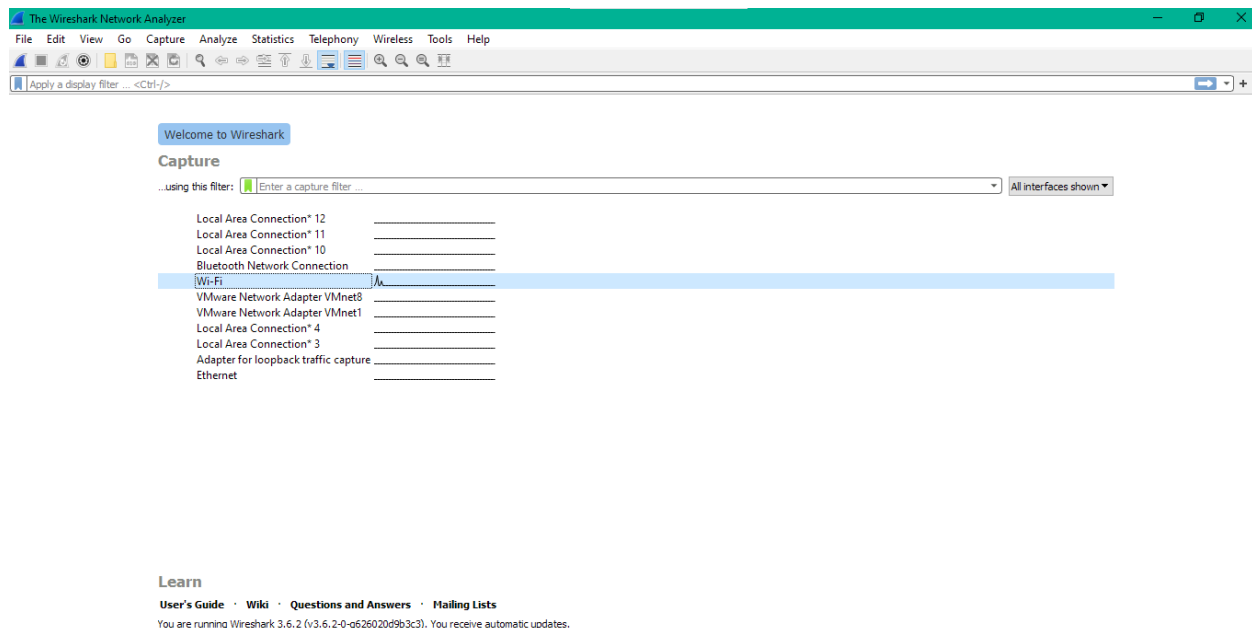


Wireshark Network sniffing:

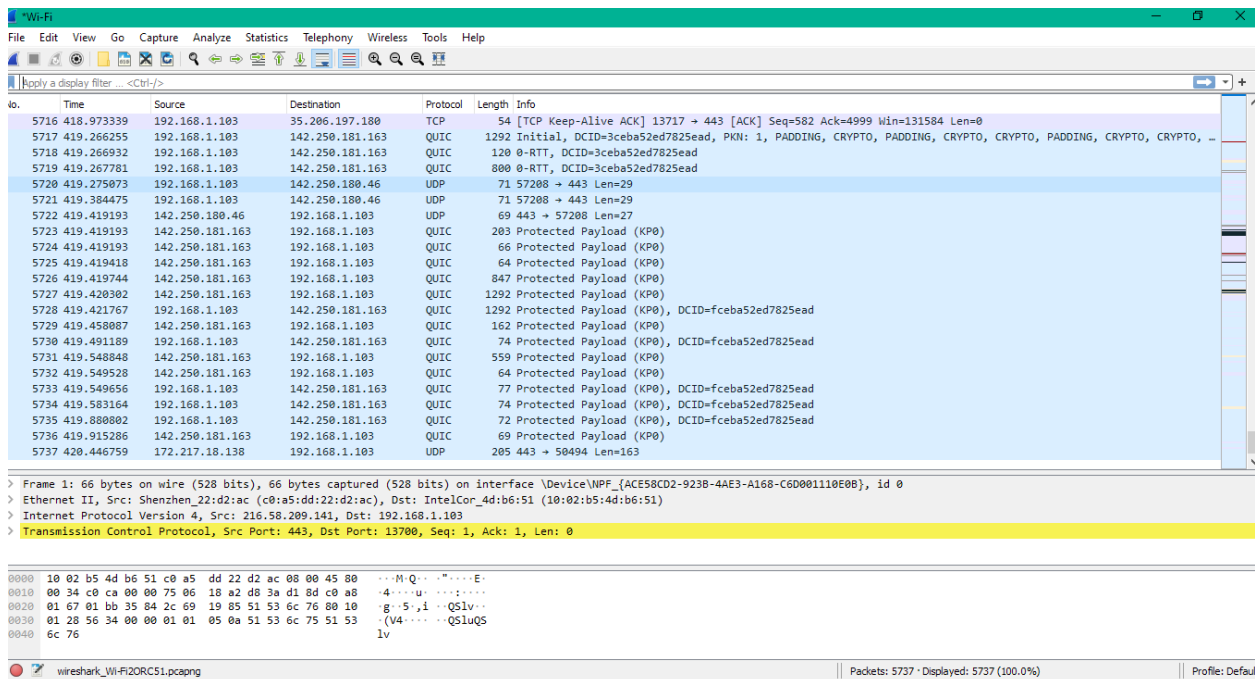
After the initial network vulnerability check using Nmap, we employed the use of a network sniffing tool (Wireshark) for capturing data packets on a network.

1. Select a specific channel:

Wi-Fi networks operate on different channels, and by selecting a specific channel in Wireshark, you can focus your packet capturing on a particular Wi-Fi channel of interest. This can help in narrowing down the analysis and capturing relevant packets from a specific channel.

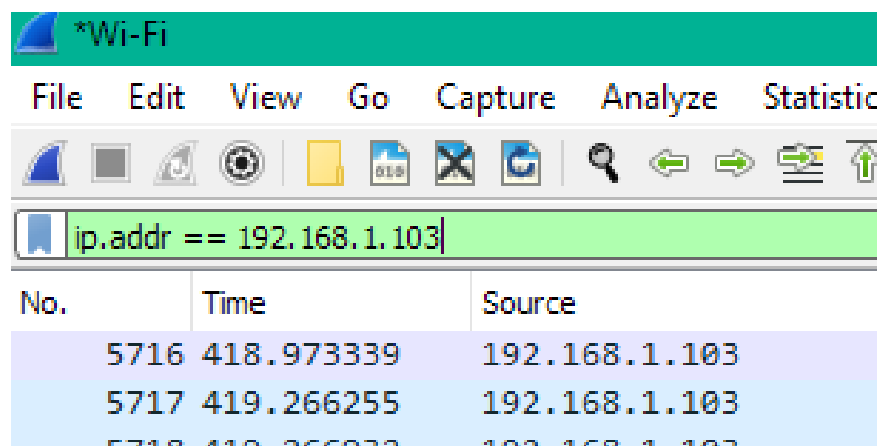


By double clicking on the selected channel, all the network traffic of that specific channel becomes visible.



2. Select a specific target:

Wireshark provides a "Filter" field where we can enter filter expressions to selectively display packets that meet specific criteria. In this case, we'll use a filter expression to match packets with the desired IP address. The filter expression `ip.addr == 192.168.1.103` is an example of a filter syntax. It uses the `ip.addr` field to filter for packets with a source or destination IP address that matches the specified IP address (192.168.0.103 in this example).



Now we can see the network traffic specific to the selected IP address.

The image shows a Wireshark capture of network traffic filtered by the IP address 192.168.1.103. The capture is displayed in a table with columns for No., Time, Source, Destination, Protocol, Length, and Info. The traffic includes QUIC, UDP, and TCP packets. The bottom of the image shows the packet details for the selected packet, including the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields.

No.	Time	Source	Destination	Protocol	Length	Info
732	114.041069	192.168.1.103	142.250.185.42	QUIC	82	Protected Payload (KP0), DCID=ceaed67ed59ce6bd
733	114.049010	142.250.185.42	192.168.1.103	QUIC	241	Protected Payload (KP0)
734	114.060278	192.168.1.103	142.250.185.42	QUIC	79	Protected Payload (KP0), DCID=ceaed67ed59ce6bd
735	114.062135	192.168.1.103	172.217.18.138	UDP	609	50494 → 443 Len=567
736	114.062967	192.168.1.103	172.217.18.138	UDP	389	50494 → 443 Len=347
737	114.100231	142.250.185.42	192.168.1.103	QUIC	68	Protected Payload (KP0)
738	114.104817	172.217.18.138	192.168.1.103	UDP	67	443 → 50494 Len=25
739	114.104817	172.217.18.138	192.168.1.103	UDP	68	443 → 50494 Len=26
740	114.105096	192.168.1.103	172.217.18.138	UDP	76	50494 → 443 Len=34
741	114.204790	172.217.18.138	192.168.1.103	UDP	68	443 → 50494 Len=26
742	114.205313	192.168.1.103	172.217.18.138	UDP	76	50494 → 443 Len=34
743	114.375943	172.217.18.138	192.168.1.103	UDP	137	443 → 50494 Len=95
744	114.375943	172.217.18.138	192.168.1.103	UDP	108	443 → 50494 Len=66
745	114.376496	192.168.1.103	172.217.18.138	UDP	83	50494 → 443 Len=41
746	114.376838	192.168.1.103	172.217.18.138	UDP	83	50494 → 443 Len=41
747	114.419464	172.217.18.138	192.168.1.103	UDP	68	443 → 50494 Len=26
748	114.834829	192.168.1.103	74.125.133.188	TCP	55	[TCP Keep-Alive] 13400 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
749	115.090626	74.125.133.188	192.168.1.103	TCP	66	[TCP Keep-Alive ACK] 5228 → 13400 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
750	116.633209	192.168.1.103	74.125.133.188	TCP	55	[TCP Keep-Alive] 13399 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
751	116.727258	192.168.1.103	104.121.8.126	TCP	54	13708 → 443 [FIN, ACK] Seq=906 Ack=9833 Win=261888 Len=0
752	116.867779	192.168.1.103	40.99.70.210	TCP	54	13704 → 443 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
753	116.868078	192.168.1.103	52.111.240.9	TCP	54	13707 → 443 [FIN, ACK] Seq=901 Ack=7145 Win=132352 Len=0
754	116.868306	192.168.1.103	52.109.44.80	TCP	54	13703 → 443 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0

> Frame 753: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{ACE58CD2-923B-4AE3-A168-C6D001110E08}, id 0
> Ethernet II, Src: IntelCor_4d:b6:51 (10:02:b5:4d:b6:51), Dst: Shenzhen_22:d2:ac (c0:a5:dd:22:d2:ac)
> Internet Protocol Version 4, Src: 192.168.1.103, Dst: 52.111.240.9
> Transmission Control Protocol, Src Port: 13707, Dst Port: 443, Seq: 901, Ack: 7145, Len: 0

0000 c0 a5 dd 22 d2 ac 10 02 b5 4d b6 51 00 00 45 00M.Q..E.
0010 00 28 d6 82 40 00 00 06 3d c5 c0 a8 01 67 34 ef :(.@...=...g4o
0020 f0 09 35 8b 01 bb 12 fb 86 06 8b cc ef 31 50 11 :.5.....IP.
0030 02 05 7c 00 00 00 ..|...

wireshark_Wi-Fi20RC51.pcapng | Packets: 5737 · Displayed: 5607 (97.7%) · Dropped: 0 (0.0%)

3. Filter packets by specific protocols:

Wireshark allows us to filter captured packets based on specific protocols. By applying protocol filters, such as HTTP, DNS, TCP, or FTP, we can focus on analyzing the traffic of protocols within the selected Wi-Fi channel. This can help us gain a deeper understanding of the specific protocols' behavior and potential security implications.

Enter the desired protocol filter expression to display packets related to a specific protocol. For example, to filter for TCP traffic, we can use the filter expression `&& tcp` after the pervious expression `ip.addr == 192.168.1.103` to filter for TCP packets

The image shows a Wireshark capture of network traffic filtered by the IP address 192.168.1.103 and the TCP protocol. The capture is displayed in a table with columns for No., Time, Source, Destination, Protocol, Length, and Info. The traffic includes TCP and TLSv1.2 packets. The bottom of the image shows the packet details for the selected packet, including the Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (TCP) fields.

No.	Time	Source	Destination	Protocol	Length	Info
637	88.689165	192.168.1.103	142.250.180.37	TCP	55	[TCP Keep-Alive]
640	90.267118	192.168.1.103	216.58.209.141	TCP	55	[TCP Keep-Alive]
641	90.531145	216.58.209.141	192.168.1.103	TCP	66	[TCP Keep-Alive]
657	98.195610	34.237.73.95	192.168.1.103	TLSv1.2	92	Application Data
658	98.237430	192.168.1.103	34.237.73.95	TCP	54	13383 → 443 [ACK]
659	99.937038	52.109.44.80	192.168.1.103	TCP	54	443 → 13702 [RST]

Wireshark packet capture showing a TCP Reset (RST) packet. The packet list shows packet 759 as a RST from 192.168.1.103 to 104.121.8.126. The packet details show it's a TCP Reset (RST) with Seq=907, Ack=9864, and Win=0. The packet bytes show the raw data.

No.	Time	Source	Destination	Protocol	Length	Info
750	116.633209	192.168.1.103	74.125.133.188	TCP	55	[TCP Keep-Alive] 13399 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
751	116.727258	192.168.1.103	104.121.8.126	TCP	54	13708 → 443 [FIN, ACK] Seq=906 Ack=9833 Win=261888 Len=0
752	116.867779	192.168.1.103	40.99.70.210	TCP	54	13704 → 443 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
753	116.868078	192.168.1.103	52.111.240.9	TCP	54	13707 → 443 [FIN, ACK] Seq=901 Ack=7145 Win=132352 Len=0
754	116.868306	192.168.1.103	52.109.44.80	TCP	54	13703 → 443 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0
755	116.868586	192.168.1.103	20.207.199.231	TCP	54	13705 → 443 [FIN, ACK] Seq=2141 Ack=1653 Win=517 Len=0
756	116.881468	74.125.133.188	192.168.1.103	TCP	66	[TCP Keep-Alive ACK] 5228 → 13399 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
757	116.884612	104.121.8.126	192.168.1.103	TLSv1.2	85	Encrypted Alert
758	116.884612	104.121.8.126	192.168.1.103	TCP	54	443 → 13708 [FIN, ACK] Seq=9864 Ack=907 Win=64128 Len=0
759	116.884757	192.168.1.103	104.121.8.126	TCP	54	13708 → 443 [RST, ACK] Seq=907 Ack=9864 Win=0 Len=0
760	116.942756	40.99.70.210	192.168.1.103	TCP	54	443 → 13704 [FIN, ACK] Seq=1 Ack=2 Win=16382 Len=0
761	116.942810	192.168.1.103	40.99.70.210	TCP	54	13704 → 443 [ACK] Seq=2 Ack=2 Win=517 Len=0
762	117.040311	20.207.199.231	192.168.1.103	TCP	54	443 → 13705 [FIN, ACK] Seq=1653 Ack=2142 Win=2053 Len=0
763	117.040361	192.168.1.103	20.207.199.231	TCP	54	13705 → 443 [ACK] Seq=2142 Ack=1654 Win=517 Len=0
764	117.242762	52.111.240.9	192.168.1.103	TCP	54	443 → 13707 [FIN, ACK] Seq=7145 Ack=902 Win=64512 Len=0
765	117.242812	192.168.1.103	52.111.240.9	TCP	54	13707 → 443 [ACK] Seq=902 Ack=7146 Win=132352 Len=0

Frame 662: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{ACE58CD2-923B-4AE3-A168-C6D001110E08}, id 0
 Ethernet II, Src: Shenzhen_22:d2:ac (c0:a5:dd:22:d2:ac), Dst: IntelCor_4d:b6:51 (10:02:b5:4d:b6:51)
 Internet Protocol Version 4, Src: 157.240.227.60, Dst: 192.168.1.103
 Transmission Control Protocol, Src Port: 443, Dst Port: 13384, Seq: 423, Ack: 355, Len: 0

0000 10 02 b5 4d b6 51 c0 a5 dd 22 d2 ac 08 00 45 00 ...M.Q...E
 0010 00 28 04 9a 40 00 52 06 e0 f9 9d f0 e3 3c c0 a8 ...@.R...<
 0020 01 67 01 bb 34 48 c8 2b 87 2e f7 82 18 38 50 10 ...g..4H+...8P
 0030 02 b4 d4 cb 00 00

4. Analyzing Packet:

On selecting a specific packet we can view the encrypted contents. Initially by right clicking on the specific packet, selecting Follow option in the menu and then click on specific protocol (TCP).

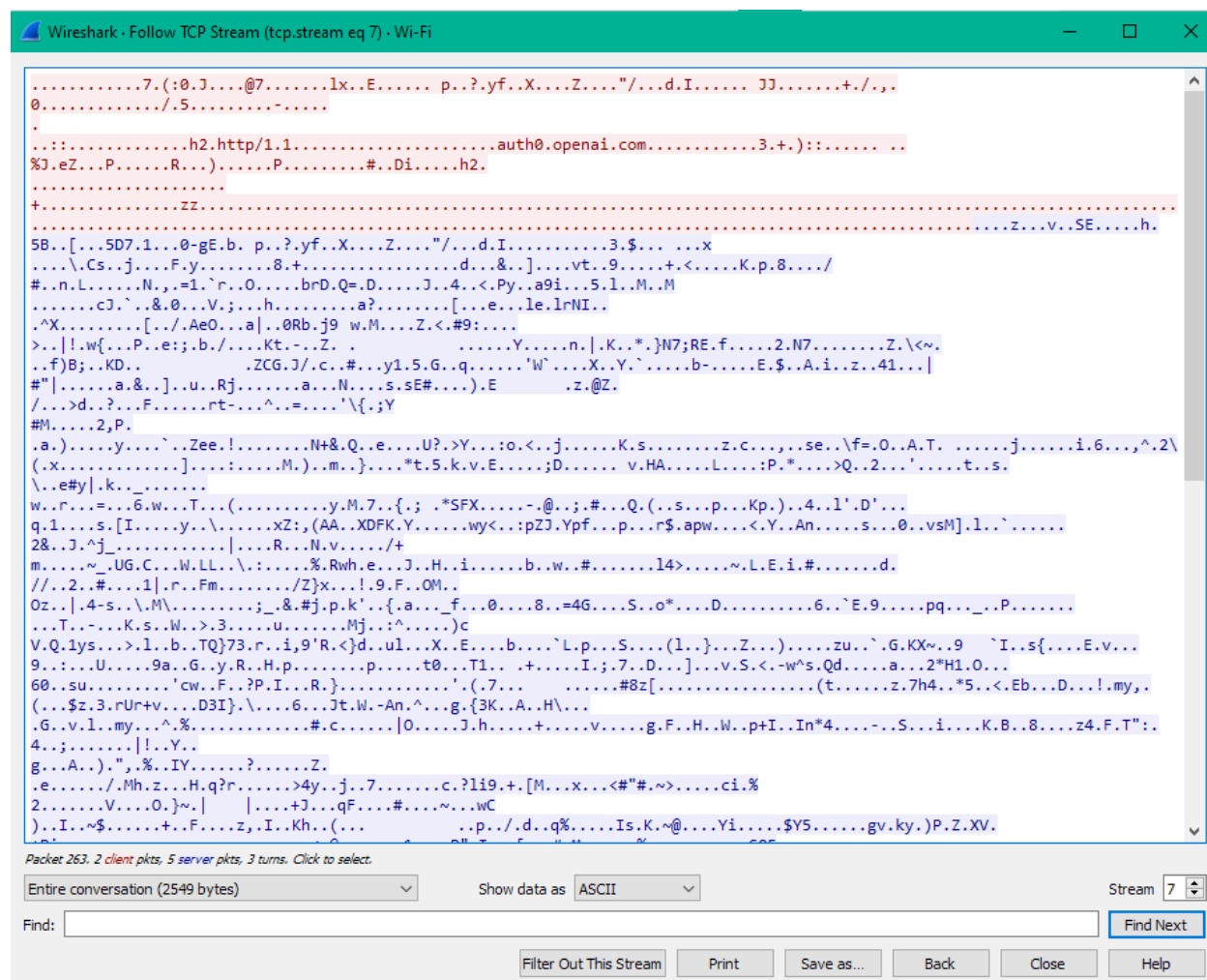
Wireshark packet capture showing a context menu for packet 759. The 'Follow' option is selected, and the 'TCP Stream' is chosen from the submenu. The packet details show it's a TCP Reset (RST) with Seq=907, Ack=9864, and Win=0.

No.	Time	Source	Destination	Protocol	Length	Info
750	116.633209	192.168.1.103	74.125.133.188	TCP	55	[TCP Keep-Alive] 13399 → 5228 [ACK] Seq=1 Ack=1 Win=509 Len=1
751	116.727258	192.168.1.103	104.121.8.126	TCP	54	13708 → 443 [FIN, ACK] Seq=906 Ack=9833 Win=261888 Len=0
752	116.867779	192.168.1.103	40.99.70.210	TCP	54	13704 → 443 [FIN, ACK] Seq=1 Ack=1 Win=517 Len=0
753	116.868078	192.168.1.103	52.111.240.9	TCP	54	13707 → 443 [FIN, ACK] Seq=901 Ack=7145 Win=132352 Len=0
754	116.868306	192.168.1.103	52.109.44.80	TCP	54	13703 → 443 [FIN, ACK] Seq=1 Ack=1 Win=509 Len=0
755	116.868586	192.168.1.103	20.207.199.231	TCP	54	13705 → 443 [FIN, ACK] Seq=2141 Ack=1653 Win=517 Len=0
756	116.881468	74.125.133.188	192.168.1.103	TCP	66	[TCP Keep-Alive ACK] 5228 → 13399 [ACK] Seq=1 Ack=2 Win=265 Len=0 SLE=1 SRE=2
757	116.884612	104.121.8.126	192.168.1.103	TLSv1.2	85	Encrypted Alert
758	116.884612	104.121.8.126	192.168.1.103	TCP	54	443 → 13708 [FIN, ACK] Seq=9864 Ack=907 Win=64128 Len=0
759	116.884757	192.168.1.103	104.121.8.126	TCP	54	13708 → 443 [RST, ACK] Seq=907 Ack=9864 Win=0 Len=0
760	116.942756	40.99.70.210	192.168.1.103	TCP	54	443 → 13704 [FIN, ACK] Seq=1 Ack=2 Win=16382 Len=0
761	116.942810	192.168.1.103	40.99.70.210	TCP	54	13704 → 443 [ACK] Seq=2 Ack=2 Win=517 Len=0
762	117.040311	20.207.199.231	192.168.1.103	TCP	54	443 → 13705 [FIN, ACK] Seq=1653 Ack=2142 Win=2053 Len=0
763	117.040361	192.168.1.103	20.207.199.231	TCP	54	13705 → 443 [ACK] Seq=2142 Ack=1654 Win=517 Len=0
764	117.242762	52.111.240.9	192.168.1.103	TCP	54	443 → 13707 [FIN, ACK] Seq=7145 Ack=902 Win=64512 Len=0
765	117.242812	192.168.1.103	52.111.240.9	TCP	54	13707 → 443 [ACK] Seq=902 Ack=7146 Win=132352 Len=0

Frame 756: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface \Device\NPF_{ACE58CD2-923B-4AE3-A168-C6D001110E08}, id 0
 Ethernet II, Src: Shenzhen_22:d2:ac (c0:a5:dd:22:d2:ac), Dst: IntelCor_4d:b6:51 (10:02:b5:4d:b6:51)
 Internet Protocol Version 4, Src: 74.125.133.188, Dst: 192.168.1.103
 Transmission Control Protocol, Src Port: 5228, Dst Port: 13399, Seq: 1, Ack: 13399, Win: 0, Len: 0

0000 10 02 b5 4d b6 51 c0 a5 dd 22 d2 ac 08 00 45 00 ...M.Q...E
 0010 00 34 ba 2a 00 00 74 06 f9 d0 4a 7d 85 bc c0 a8 ...4.*.t...<
 0020 01 67 14 6c 34 57 b3 b6 14 5b 3c 9e d8 2a 00 10 ...g..14W...[<.*<
 0030 01 09 97 3c 00 00 01 01 05 0a 3c 9e d8 29 3c 9e ...<...<...<
 0040 d8 2a

The highlighted encryption (in Red) indicates the request sent by the user, and the encryption (in Blue) indicates the reply in response to the request.



Further Analysis:

The data received from the captured packet can be decrypted to obtain information using the website www.apackets.com. Where you can upload the saved packet for decryption.