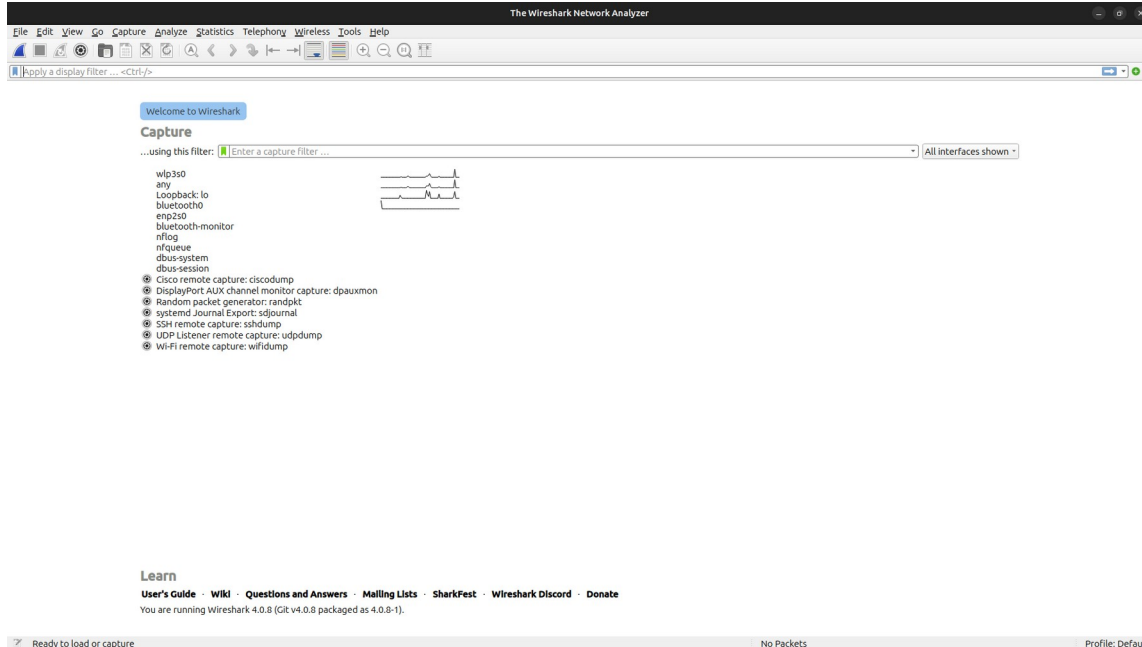


7.NETWORK TRAFFIC ANALYZES USING WIRE-SHARK...

Lab Procedure:

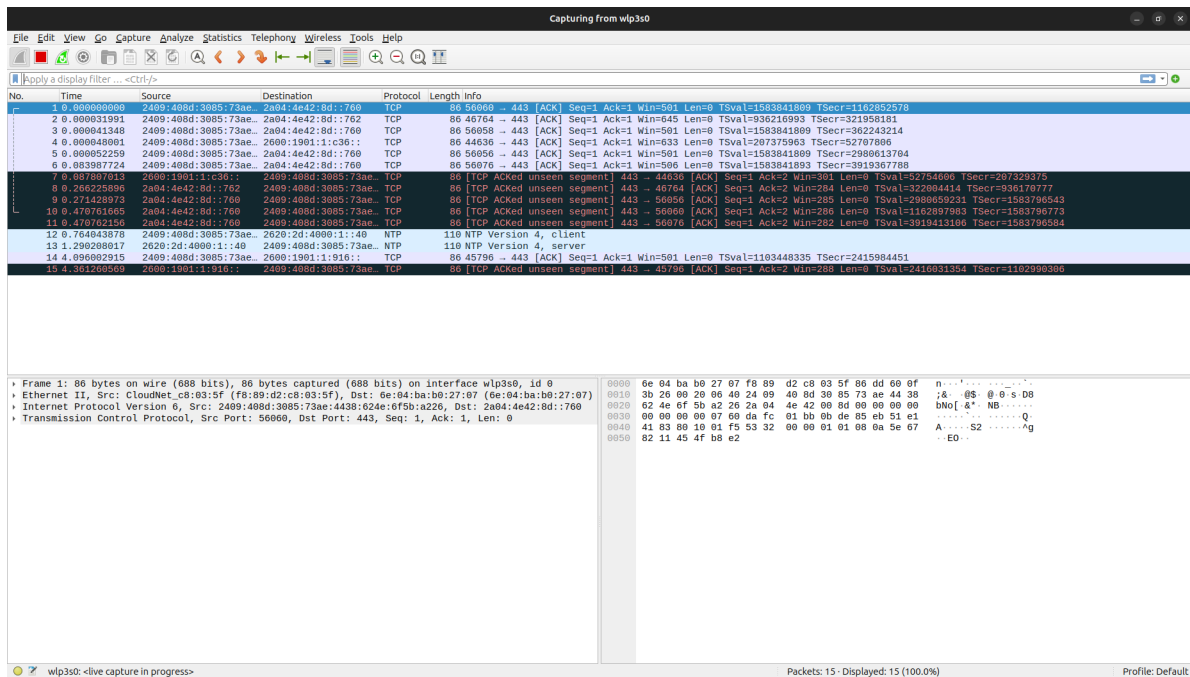
1. Open Wireshark:

- Start Wireshark on your computer.



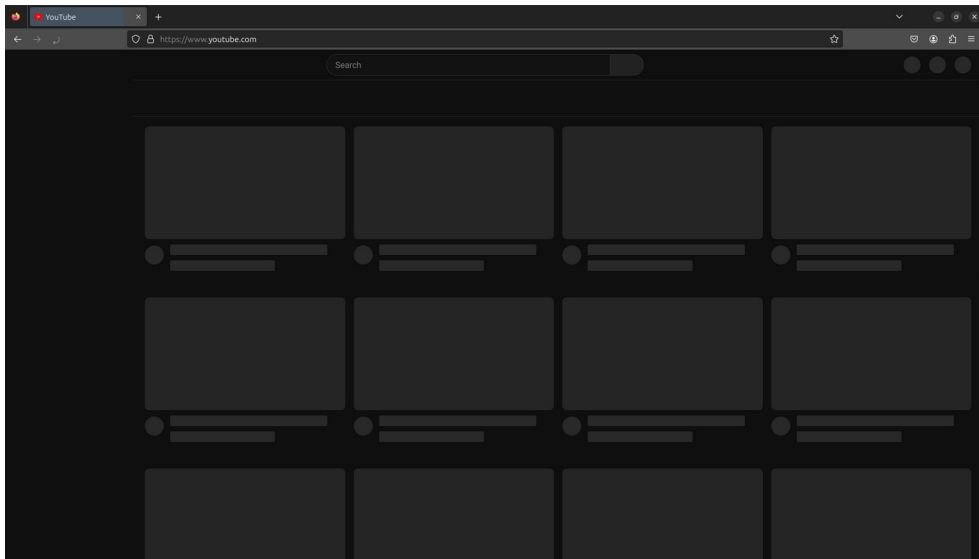
2. Capture Traffic:

- Select the network interface.
- Begin capturing packets.

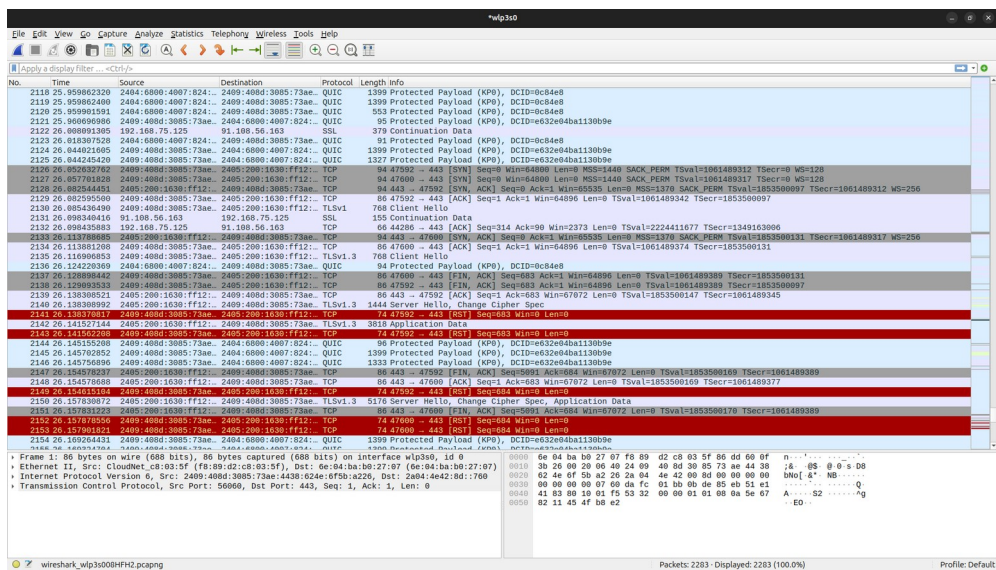


3. Analyze Packets:

- open a sample website eg: (www.youtube.com)

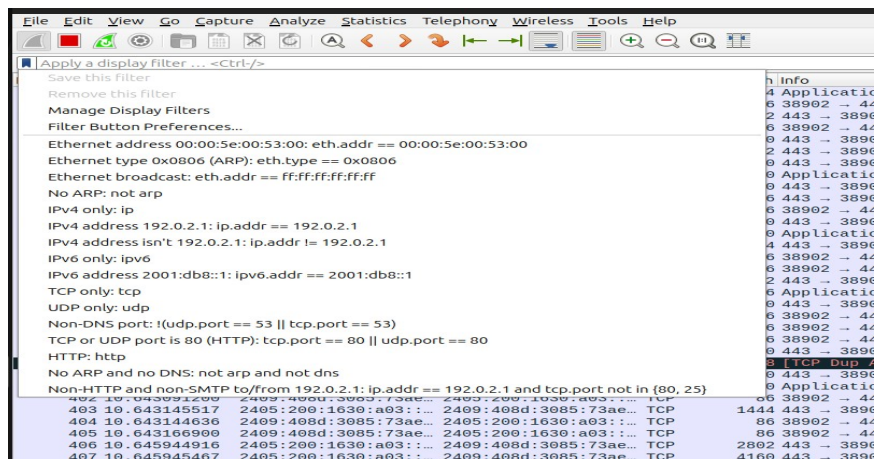


- Stop the capture after a brief duration.
- Review and analyze captured packets.



4.Filtering:

- Introduce basic display filters.

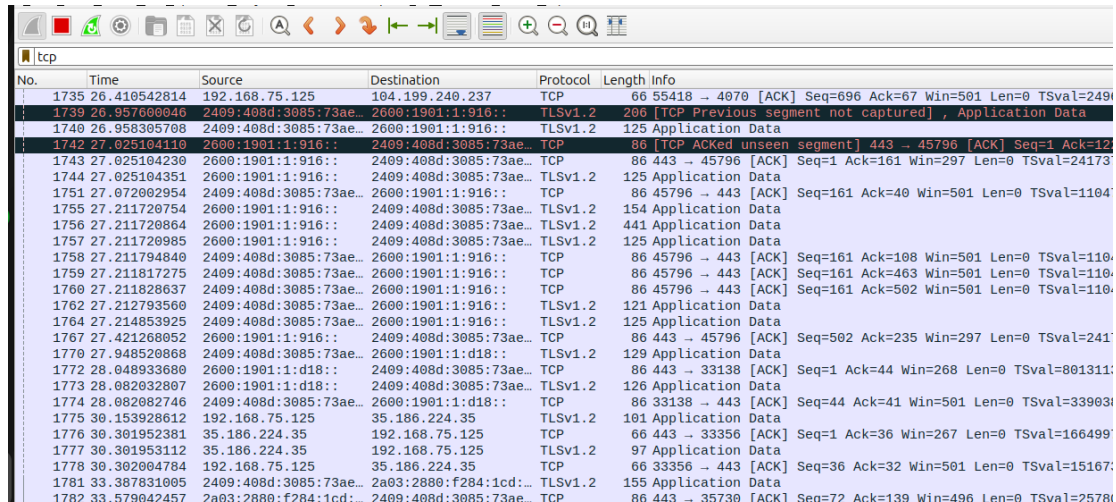


5. Packet Details:

- Examine details of selected packets.

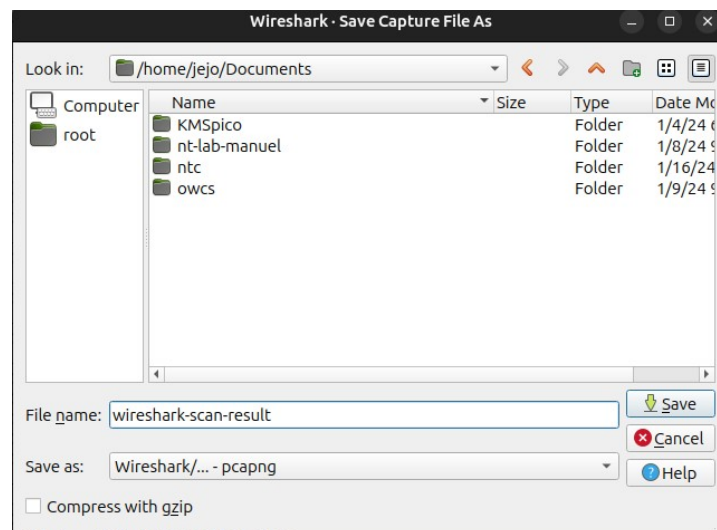
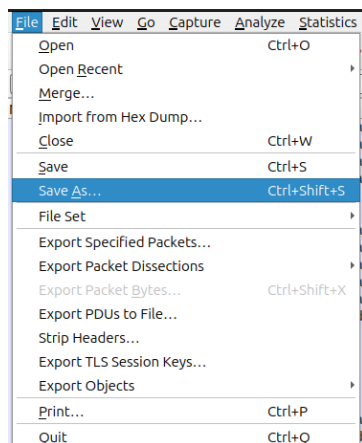
6. Follow TCP Stream:

- Analyze entire TCP conversations.



No.	Time	Source	Destination	Protocol	Length	Info
1735	26.410542814	192.168.75.125	104.199.240.237	TCP	66	55418 → 4070 [ACK] Seq=696 Ack=67 Win=501 Len=0 TSval=249
1739	26.957600046	2409:408d:3085:73ae...	2600:1901:1:916::	TLSv1.2	206	[TCP Previous segment not captured], Application Data
1740	26.958305708	2409:408d:3085:73ae...	2600:1901:1:916::	TLSv1.2	125	Application Data
1742	27.025104110	2600:1901:1:916::	2409:408d:3085:73ae...	TCP	86	[TCP ACKed unseen segment] 443 → 45796 [ACK] Seq=1 Ack=12
1743	27.025104230	2600:1901:1:916::	2409:408d:3085:73ae...	TCP	86	443 → 45796 [ACK] Seq=1 Ack=161 Win=297 Len=0 TSval=24173
1744	27.025104351	2600:1901:1:916::	2409:408d:3085:73ae...	TLSv1.2	125	Application Data
1751	27.072002954	2409:408d:3085:73ae...	2600:1901:1:916::	TCP	86	45796 → 443 [ACK] Seq=161 Ack=40 Win=501 Len=0 TSval=1104
1755	27.211720754	2600:1901:1:916::	2409:408d:3085:73ae...	TLSv1.2	154	Application Data
1756	27.211720864	2600:1901:1:916::	2409:408d:3085:73ae...	TLSv1.2	441	Application Data
1757	27.211720985	2600:1901:1:916::	2409:408d:3085:73ae...	TLSv1.2	125	Application Data
1758	27.211794840	2409:408d:3085:73ae...	2600:1901:1:916::	TCP	86	45796 → 443 [ACK] Seq=161 Ack=108 Win=501 Len=0 TSval=110
1759	27.211817275	2409:408d:3085:73ae...	2600:1901:1:916::	TCP	86	45796 → 443 [ACK] Seq=161 Ack=463 Win=501 Len=0 TSval=110
1760	27.211828637	2409:408d:3085:73ae...	2600:1901:1:916::	TCP	86	45796 → 443 [ACK] Seq=161 Ack=502 Win=501 Len=0 TSval=110
1762	27.212793560	2409:408d:3085:73ae...	2600:1901:1:916::	TLSv1.2	121	Application Data
1764	27.214853925	2409:408d:3085:73ae...	2600:1901:1:916::	TLSv1.2	125	Application Data
1767	27.421268052	2600:1901:1:916::	2409:408d:3085:73ae...	TCP	86	443 → 45796 [ACK] Seq=502 Ack=235 Win=297 Len=0 TSval=241
1770	27.948520868	2409:408d:3085:73ae...	2600:1901:1:d18::	TLSv1.2	129	Application Data
1772	28.048933680	2600:1901:1:d18::	2409:408d:3085:73ae...	TCP	86	443 → 33138 [ACK] Seq=1 Ack=44 Win=268 Len=0 TSval=801311
1773	28.082032807	2600:1901:1:d18::	2409:408d:3085:73ae...	TLSv1.2	126	Application Data
1774	28.082082746	2409:408d:3085:73ae...	2600:1901:1:d18::	TCP	86	33138 → 443 [ACK] Seq=44 Ack=41 Win=501 Len=0 TSval=33903
1775	30.153928612	192.168.75.125	35.186.224.35	TLSv1.2	101	Application Data
1776	30.301952381	35.186.224.35	192.168.75.125	TCP	66	443 → 33356 [ACK] Seq=1 Ack=36 Win=267 Len=0 TSval=166499
1777	30.301953112	35.186.224.35	192.168.75.125	TLSv1.2	97	Application Data
1778	30.302004784	192.168.75.125	35.186.224.35	TCP	66	33356 → 443 [ACK] Seq=36 Ack=32 Win=501 Len=0 TSval=15167
1781	33.387831005	2409:408d:3085:73ae...	2a03:2880:f284:1cd::	TLSv1.2	155	Application Data
1782	33.579042457	2a03:2880:f284:1cd::	2409:408d:3085:73ae...	TCP	86	443 → 35730 [ACK] Seq=72 Ack=139 Win=496 Len=0 TSval=2578

7. saving the scan output:



*our output will be saved in the /documents/wireshark-scan-result.pcapng form...

