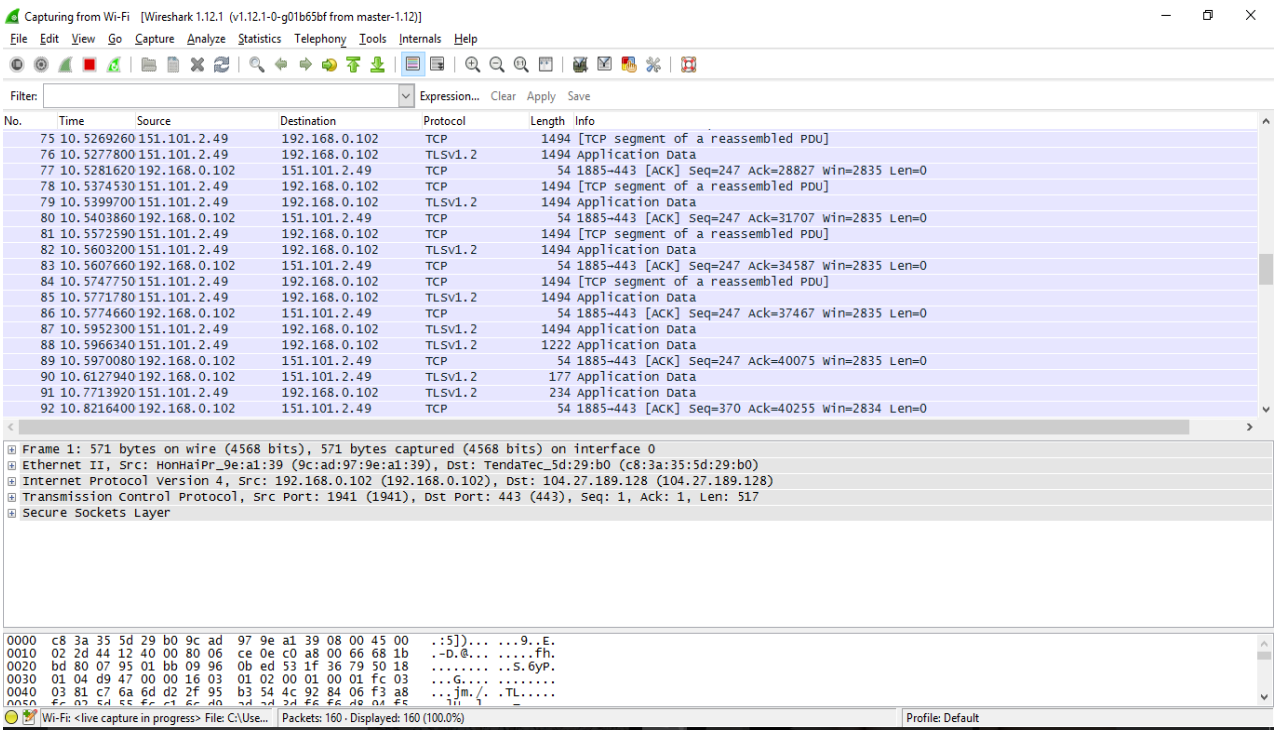
Practical - 4

Aim: - Packet capturing and network scanning using Wireshark.

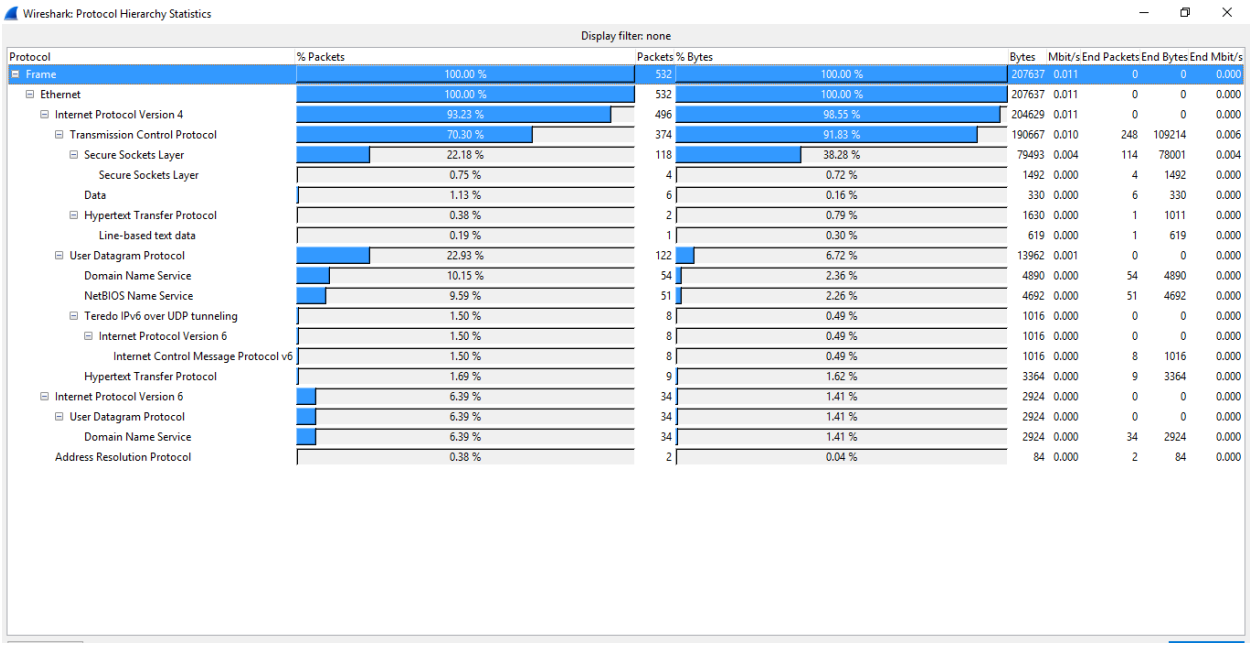
Wireshark: -

- Wireshark is a free and open source packet analyzer.
- It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- Wireshark is cross-platform, using the Qt widget toolkit in current releases to implement its user interface, and using pcap to capture packets; it runs on Linux, macOS, BSD, Solaris, some other Unix-like operating systems, and Microsoft Windows.
- There is also a terminal-based (non-GUI) version called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Capturing Packets: -

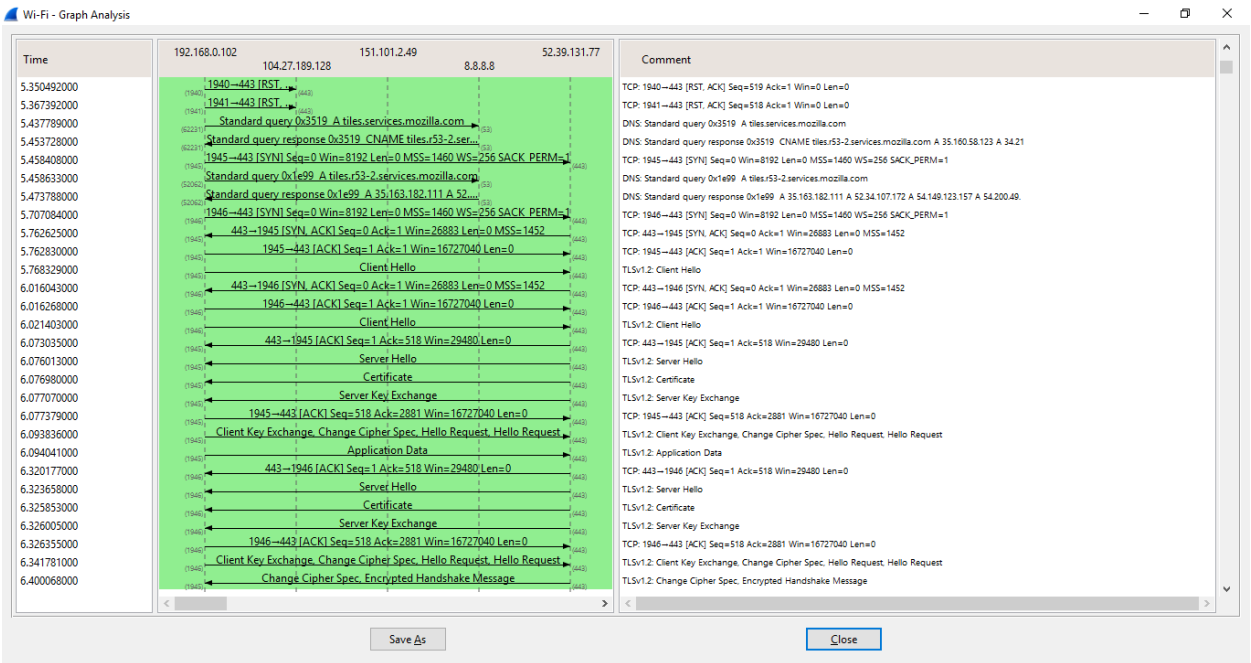


Protocol Hierarchy: -

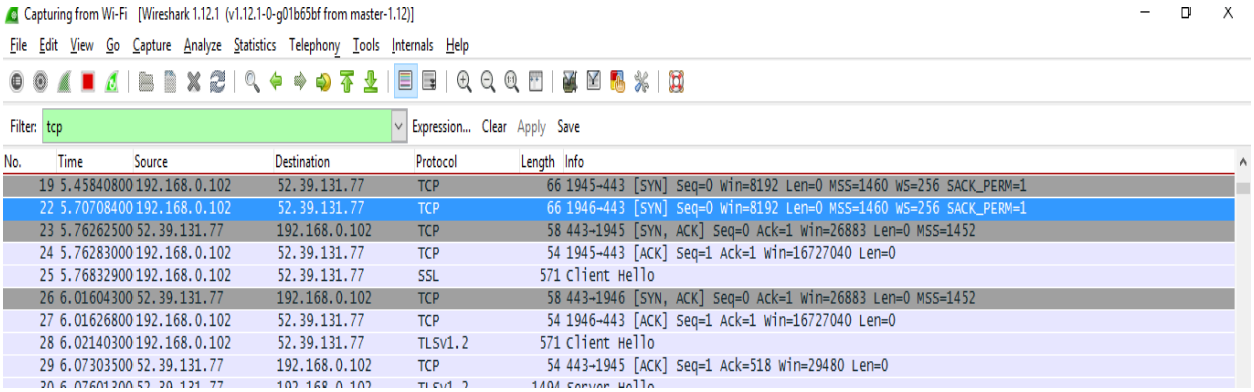


Protocol	% Packets	Packets	% Bytes	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	532	100.00 %	207637	0.011	0	0	0.000
Ethernet	100.00 %	532	100.00 %	207637	0.011	0	0	0.000
Internet Protocol Version 4	93.23 %	496	98.55 %	204629	0.011	0	0	0.000
Transmission Control Protocol	70.30 %	374	91.83 %	190667	0.010	248	109214	0.006
Secure Sockets Layer	22.18 %	118	38.28 %	79493	0.004	114	78001	0.004
Secure Sockets Layer	0.75 %	4	0.72 %	1492	0.000	4	1492	0.000
Data	1.13 %	6	0.16 %	330	0.000	6	330	0.000
Hypertext Transfer Protocol	0.38 %	2	0.79 %	1630	0.000	1	1011	0.000
Line-based text data	0.19 %	1	0.30 %	619	0.000	1	619	0.000
User Datagram Protocol	22.93 %	122	6.72 %	13962	0.001	0	0	0.000
Domain Name Service	10.15 %	54	2.36 %	4890	0.000	54	4890	0.000
NetBIOS Name Service	9.59 %	51	2.26 %	4692	0.000	51	4692	0.000
Teredo IPv6 over UDP tunneling	1.50 %	8	0.49 %	1016	0.000	0	0	0.000
Internet Protocol Version 6	1.50 %	8	0.49 %	1016	0.000	0	0	0.000
Internet Control Message Protocol v6	1.50 %	8	0.49 %	1016	0.000	8	1016	0.000
Hypertext Transfer Protocol	1.69 %	9	1.62 %	3364	0.000	9	3364	0.000
Internet Protocol Version 6	6.39 %	34	1.41 %	2924	0.000	0	0	0.000
User Datagram Protocol	6.39 %	34	1.41 %	2924	0.000	0	0	0.000
Domain Name Service	6.39 %	34	1.41 %	2924	0.000	34	2924	0.000
Address Resolution Protocol	0.38 %	2	0.04 %	84	0.000	2	84	0.000

Flow Graph: -



TCP Handshaking: -



Follow TCP Stream: -