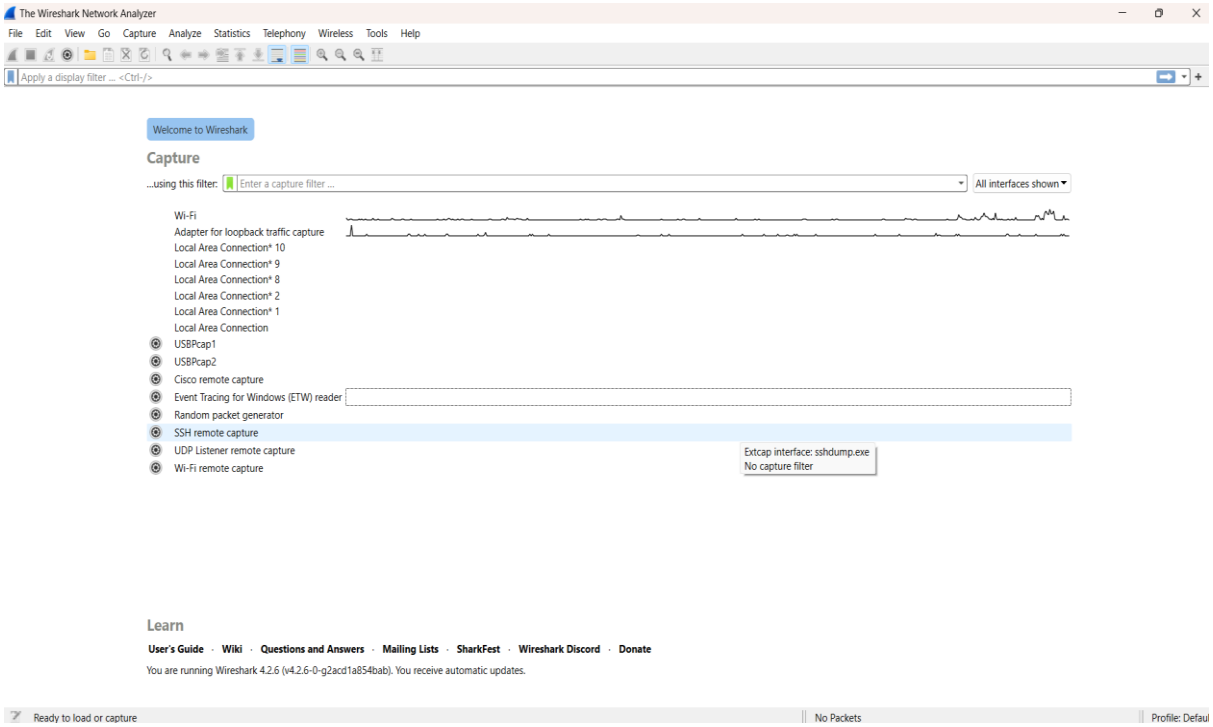
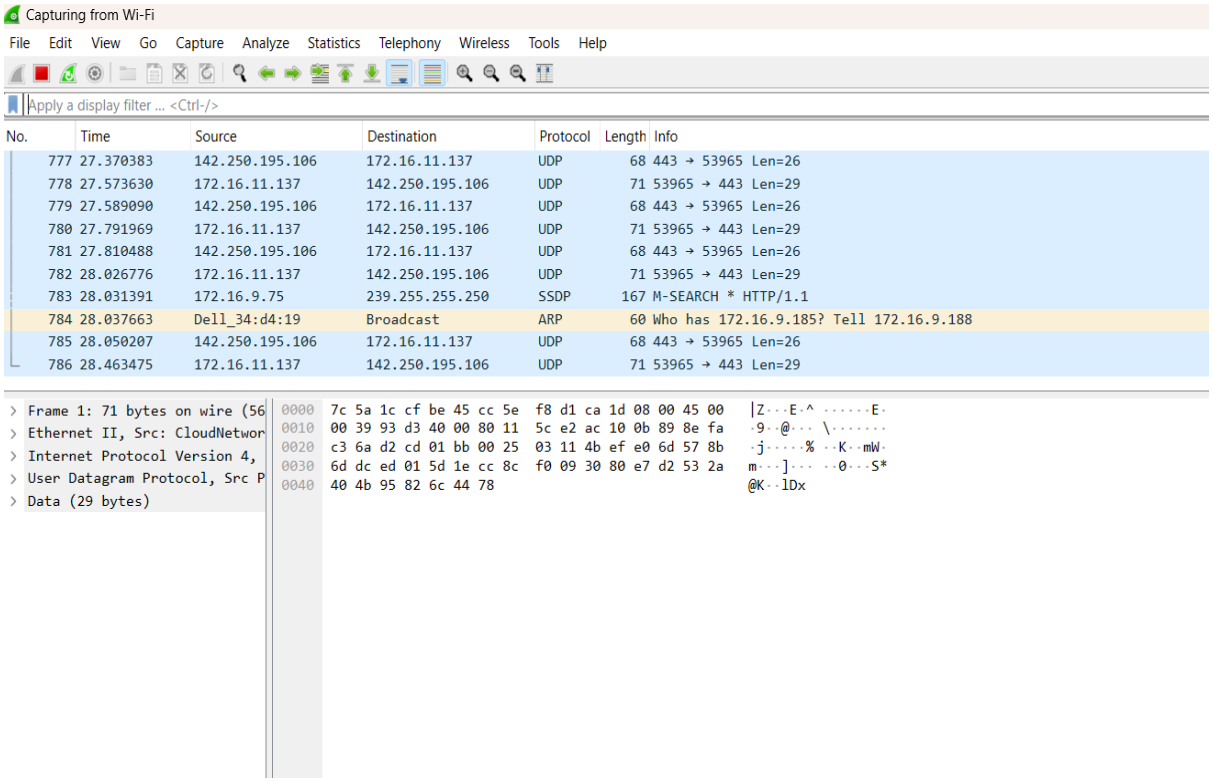
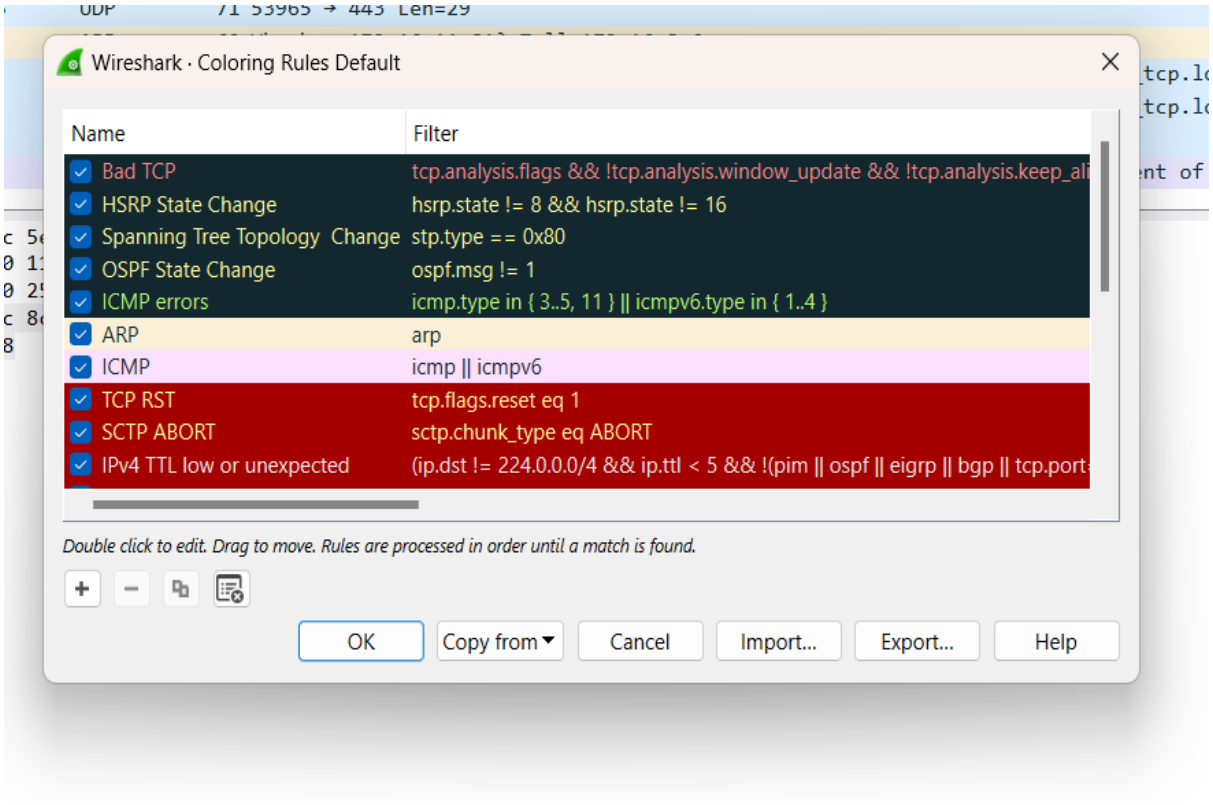
Capturing Packets:

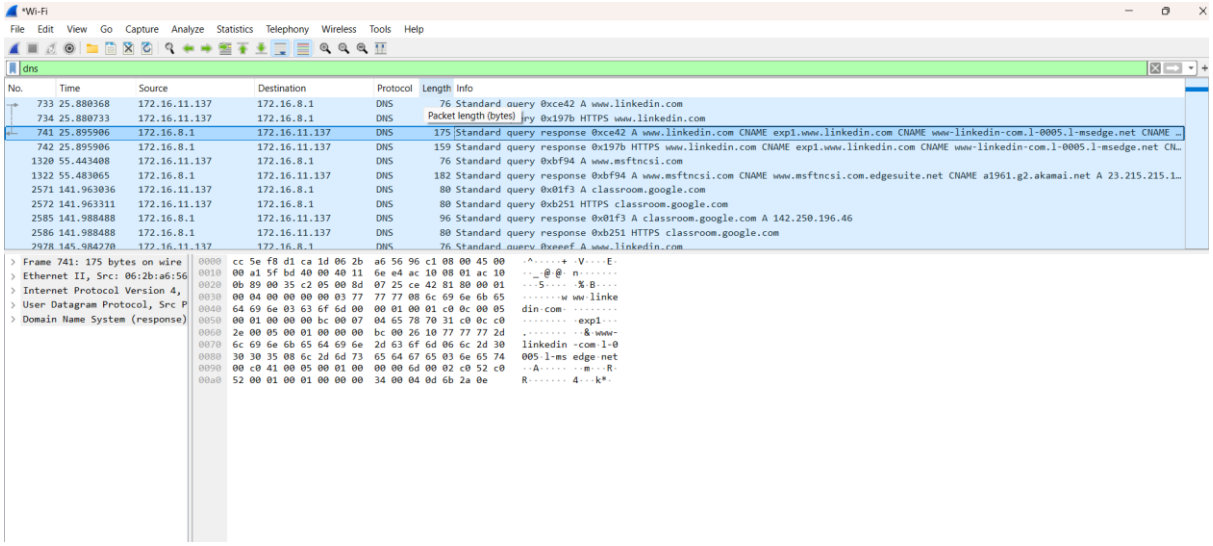




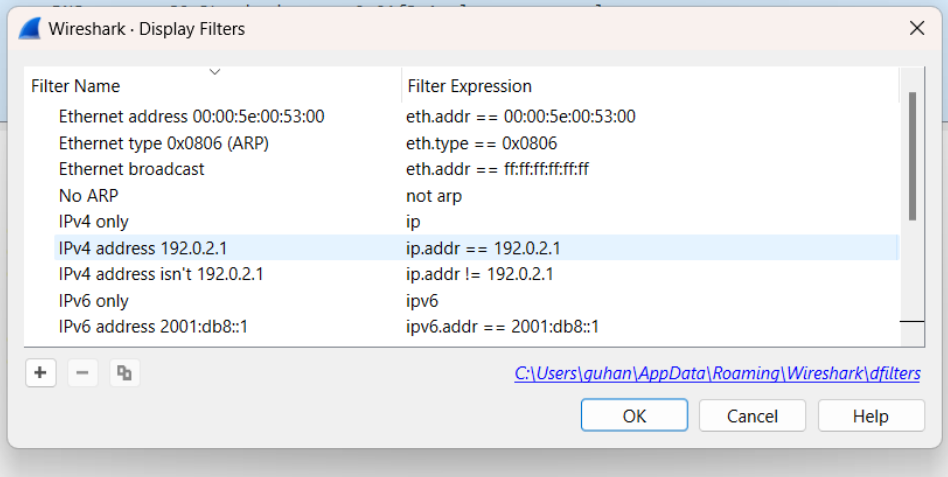
Color Coding:

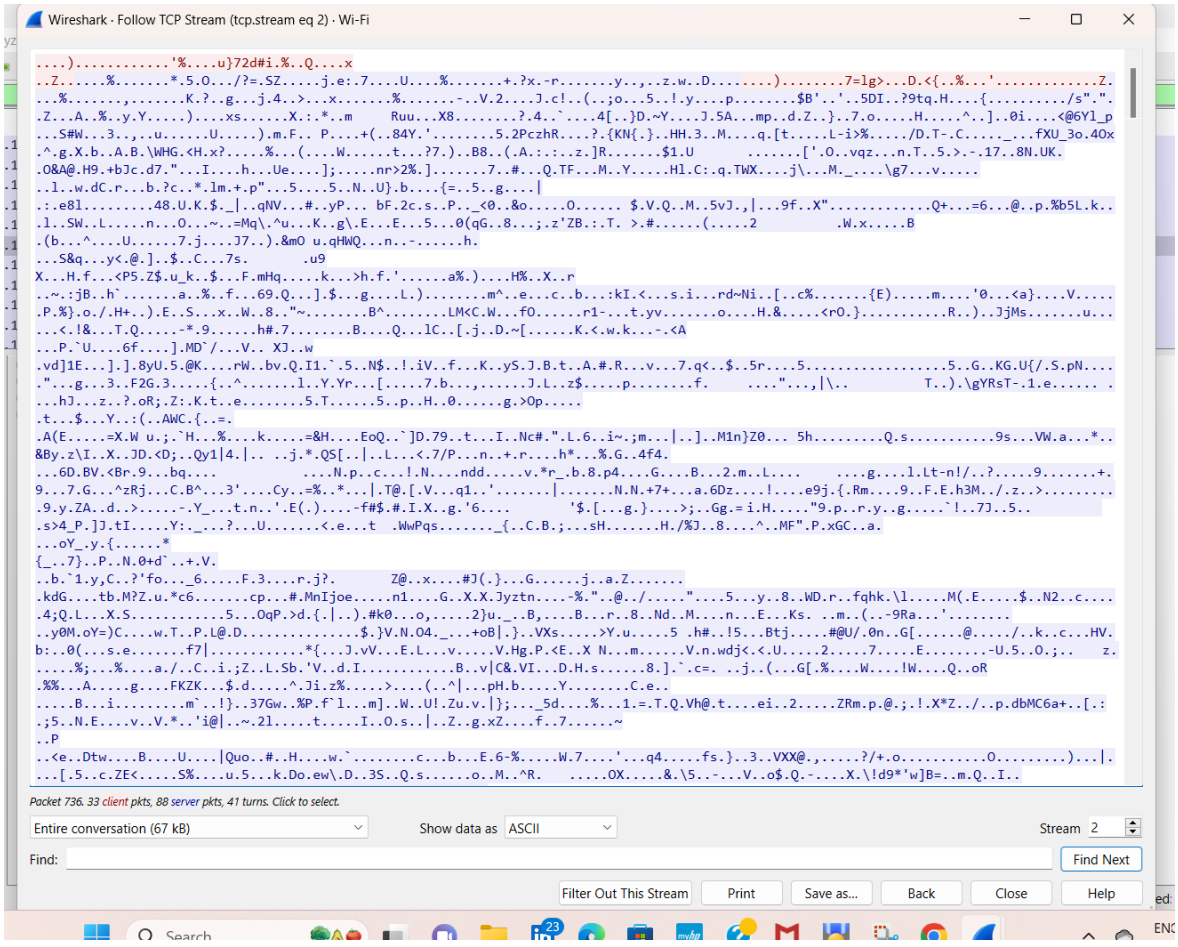


Filtering packets

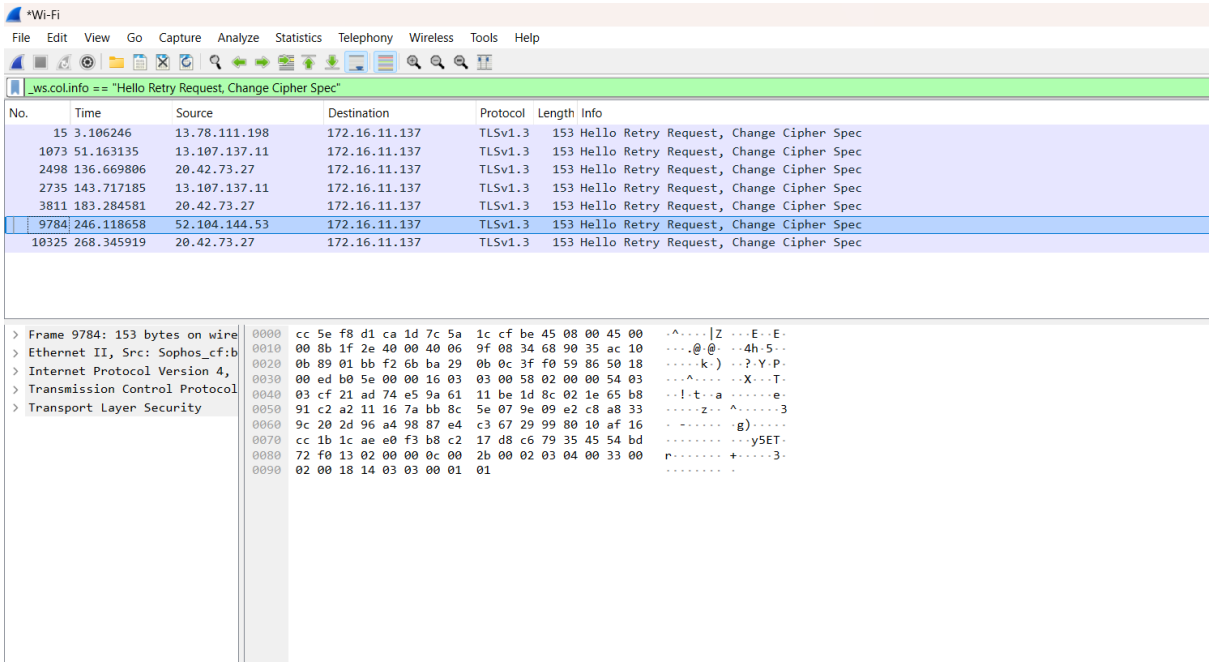


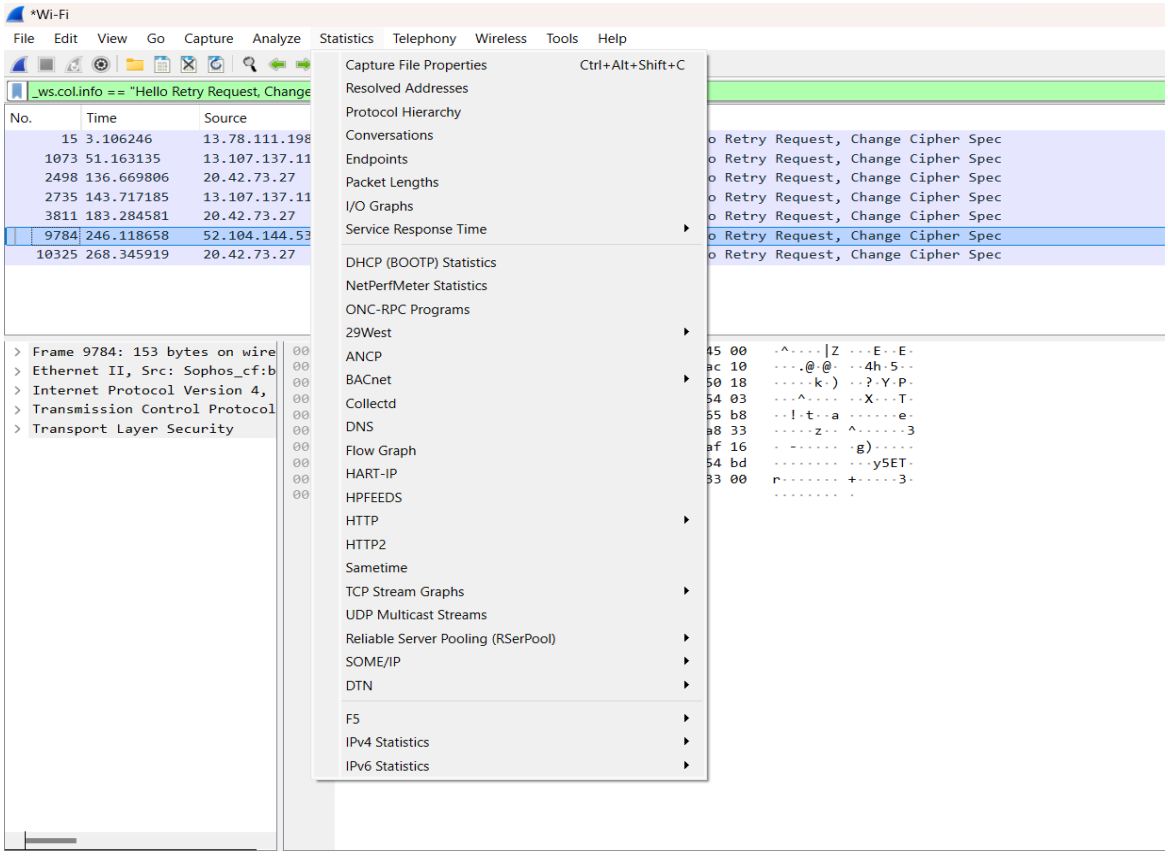

2.16.11.137 DNS 175 Standard query response 0xce42 A www.linkedin.com CNAME exp1.www.linkedin.com CNAME
2.16.11.137 DNS 159 Standard query response 0x197b HTTPS www.linkedin.com CNAME exp1.www.linkedin.com C
2.16.8.1 DNS 76 Standard query 0xbf94 A www.msftncsi.com
2.16.11.137 DNS 182 Standard query response 0xbf94 A www.msftncsi.com CNAME www.msftncsi.com.edgesuite.


Wireshark · Display Filters
Filter Name
Filter Expression
Ethernet address 00:00:5e:00:53:00
eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)
eth.type == 0x0806
Ethernet broadcast
eth.addr == ff:ff:ff:ff:ff:ff
No ARP
not arp
IPv4 only
ip
IPv4 address 192.0.2.1
ip.addr == 192.0.2.1
IPv4 address isn't 192.0.2.1
ip.addr != 192.0.2.1
IPv6 only
ipv6
IPv6 address 2001:db8::1
ipv6.addr == 2001:db8::1
C:\Users\guhan\AppData\Roaming\Wireshark\dfilters
OK
Cancel
Help


Wireshark · Follow TCP Stream (tcp.stream eq 2) · Wi-Fi
Packet 736. 33 client pkts, 88 server pkts, 41 turns. Click to select.
Entire conversation (67 kB)
Show data as ASCII
Stream 2
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

Inspecting Packets:





Graph Analysis: