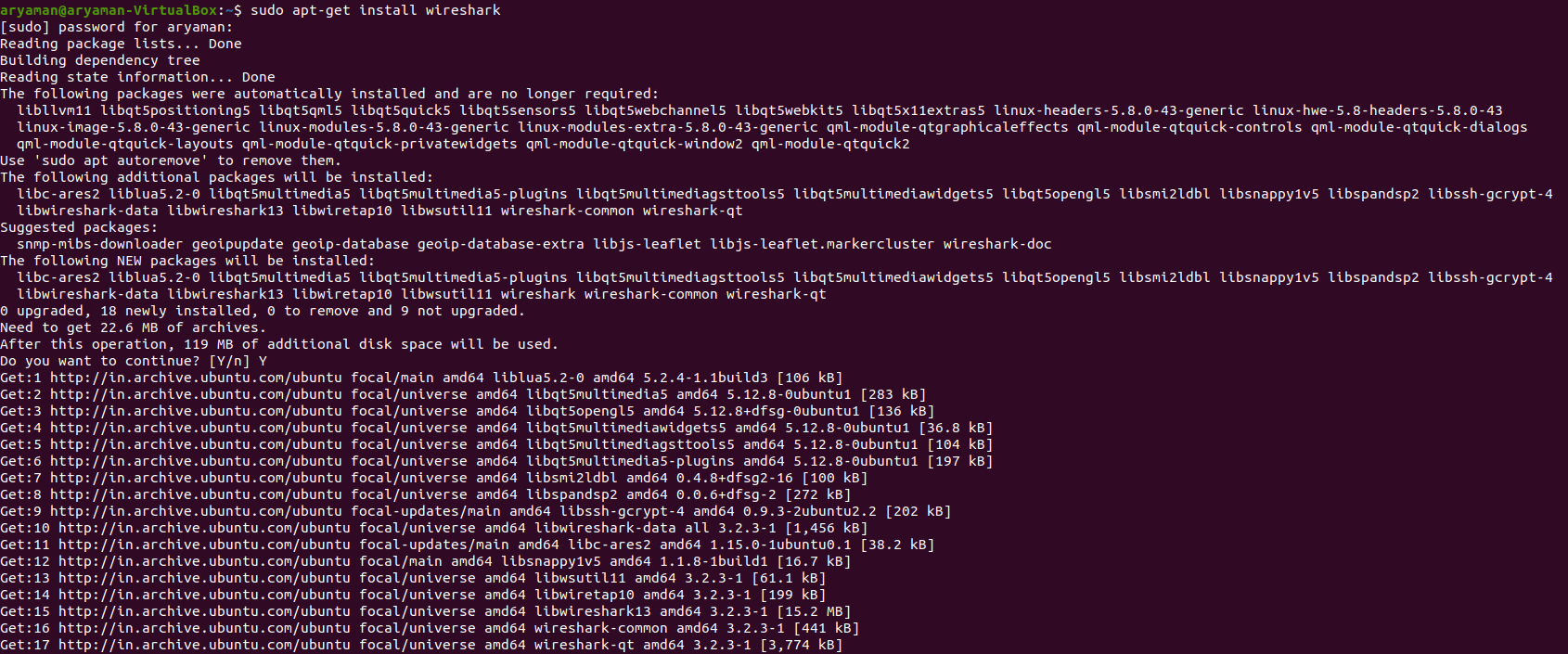
**ARYAMAN MISHRA**

**19BCE1027**

**LAB 3**

**INSTALLATION GUIDE FOR LINUX OS**

I’ll be using Wireshark to monitor incoming traffic in networks and we will use sudo to download it via terminal.

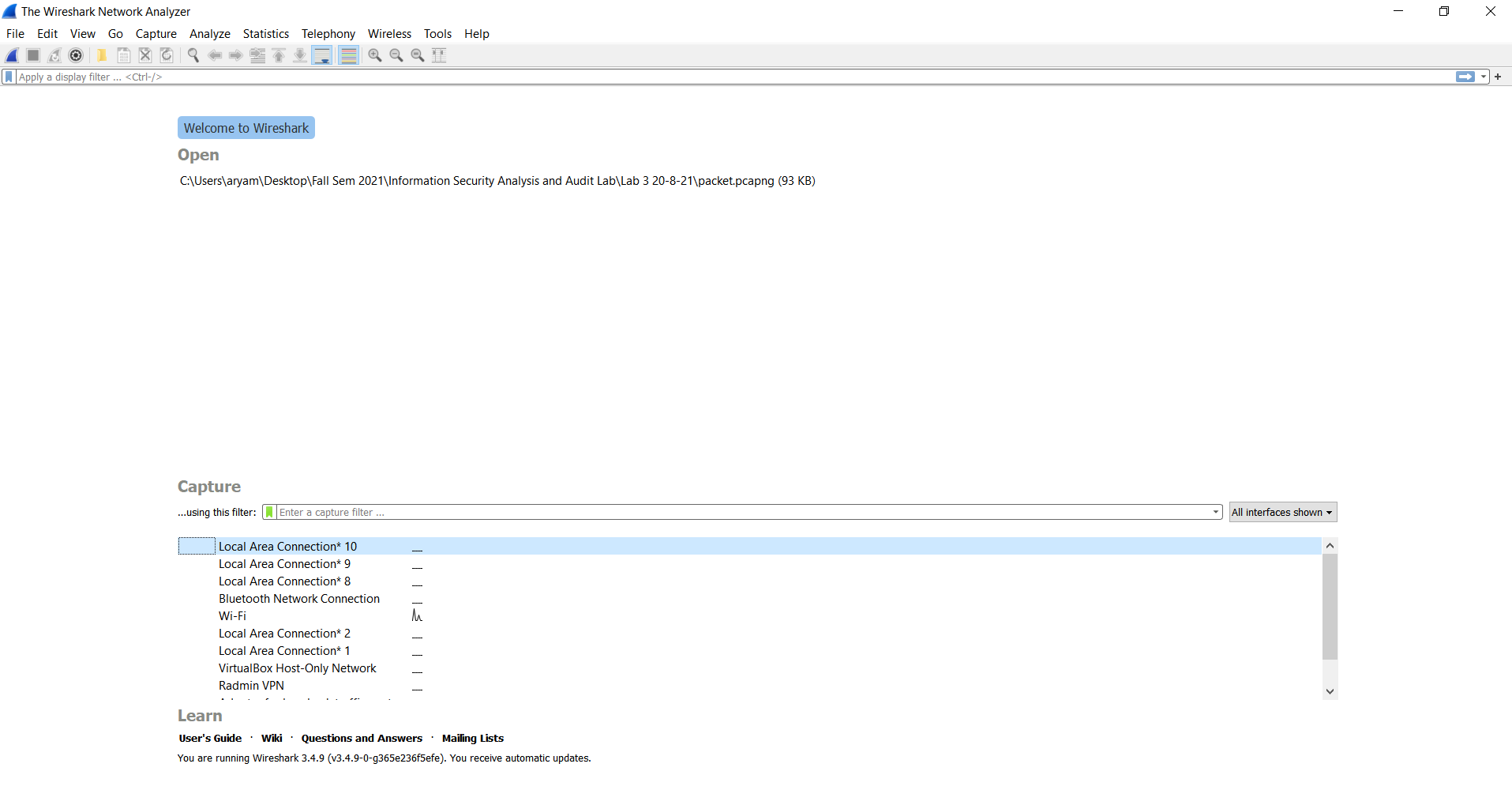


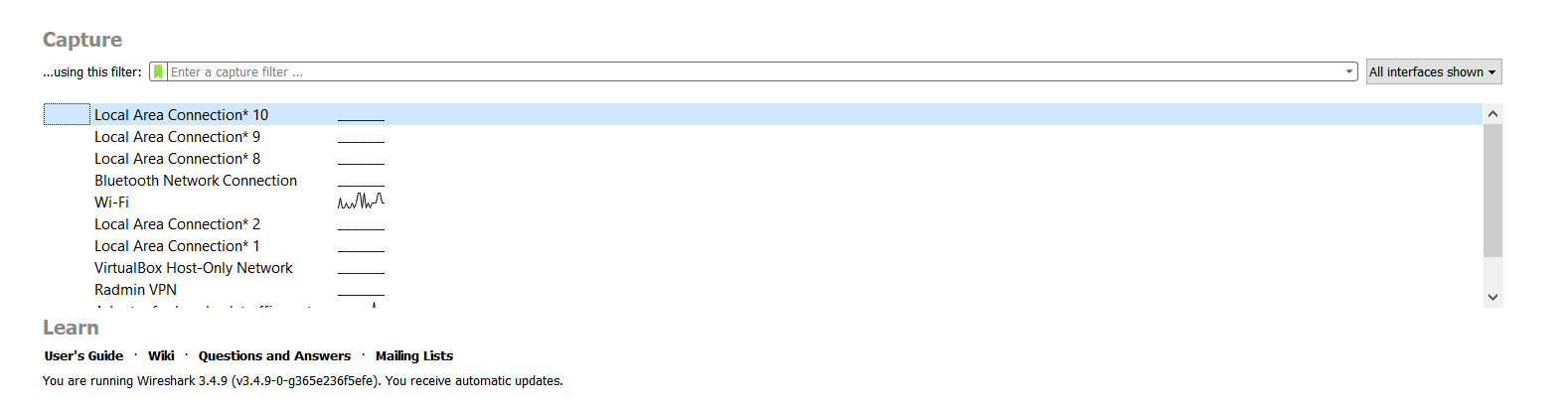
We will then launch Wireshark:



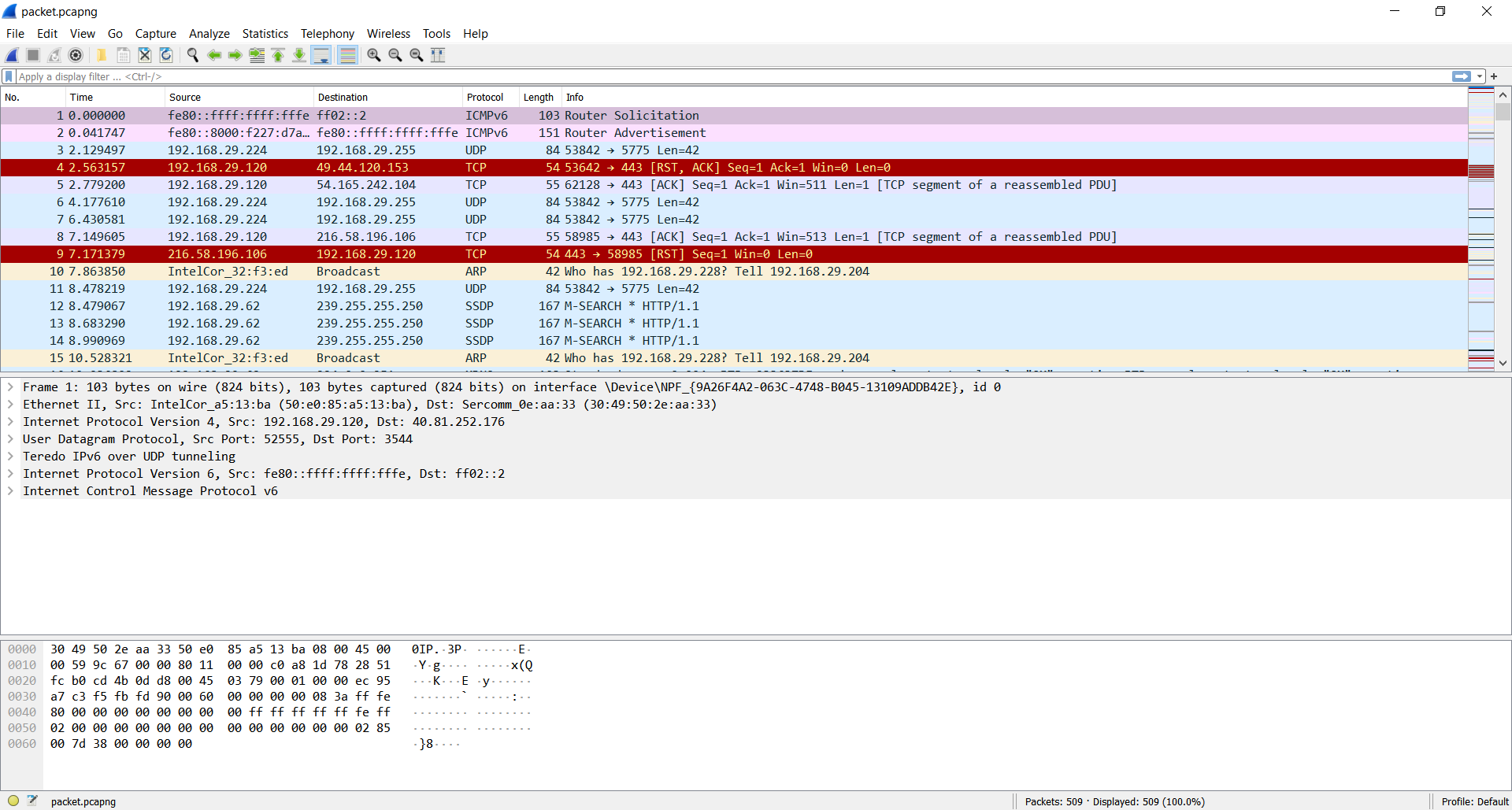
**FUNCTIONALITIES:**

**1)Launch Wireshark**

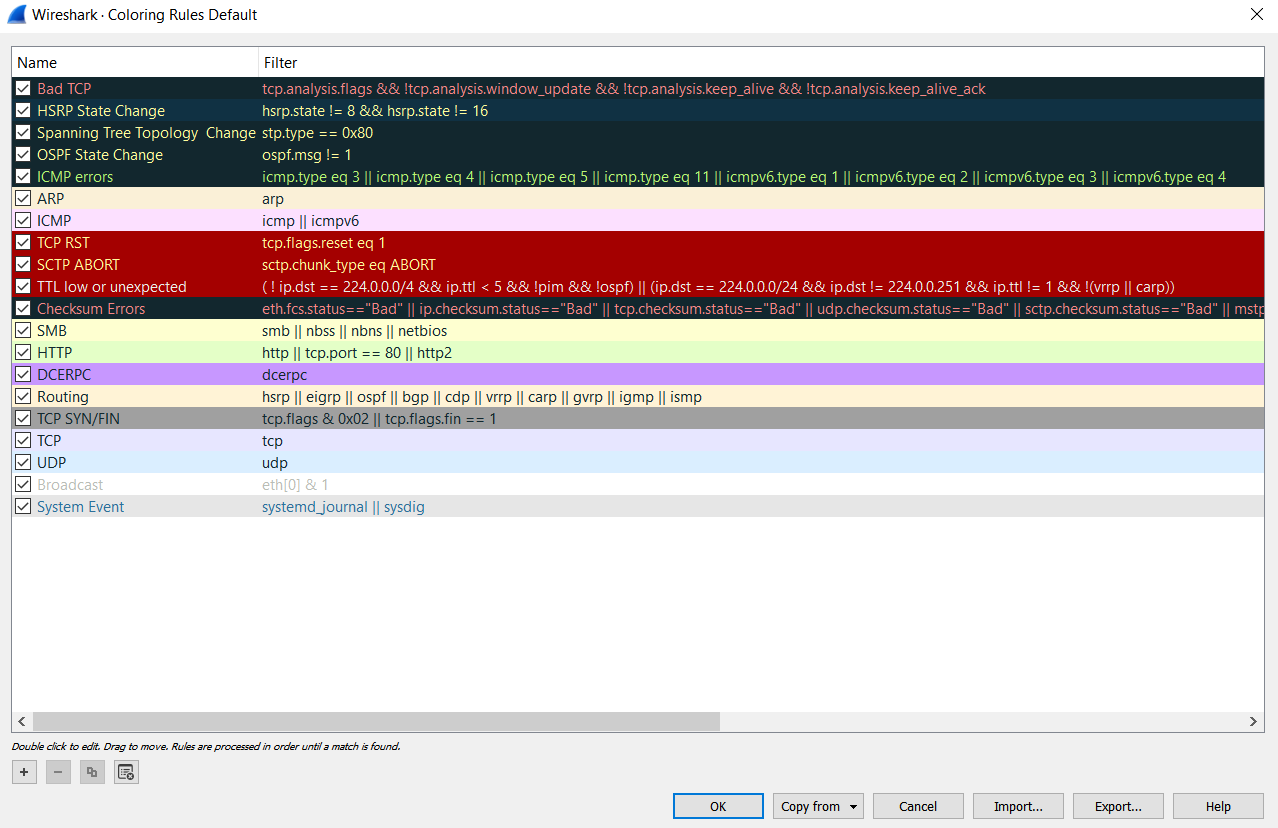


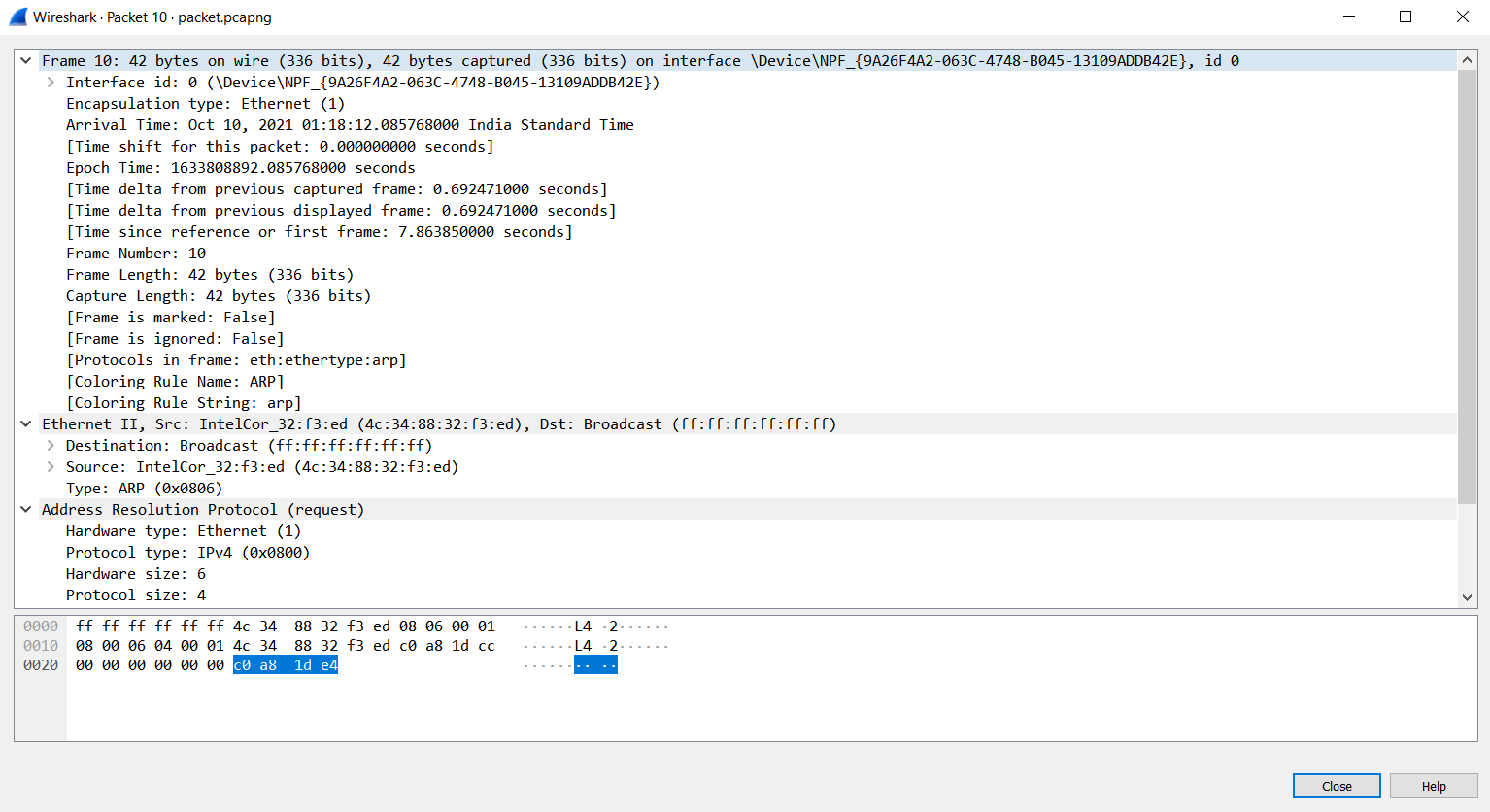


2)START CAPTURING PACKETS.

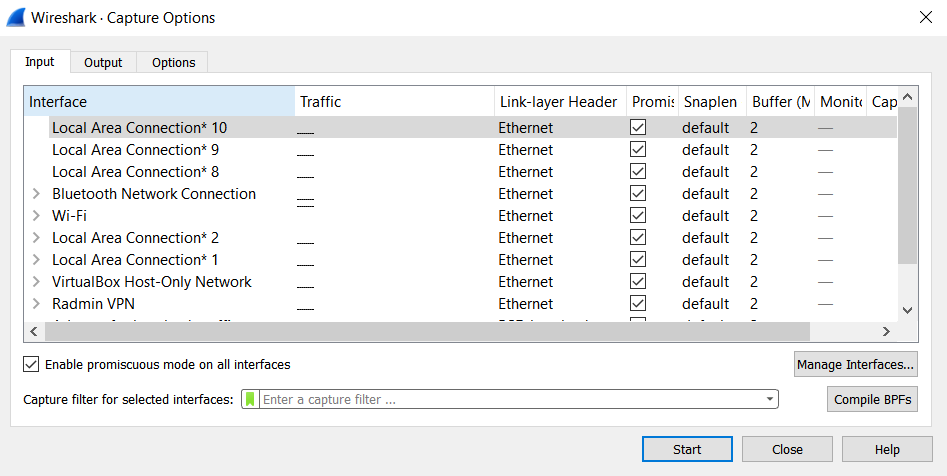


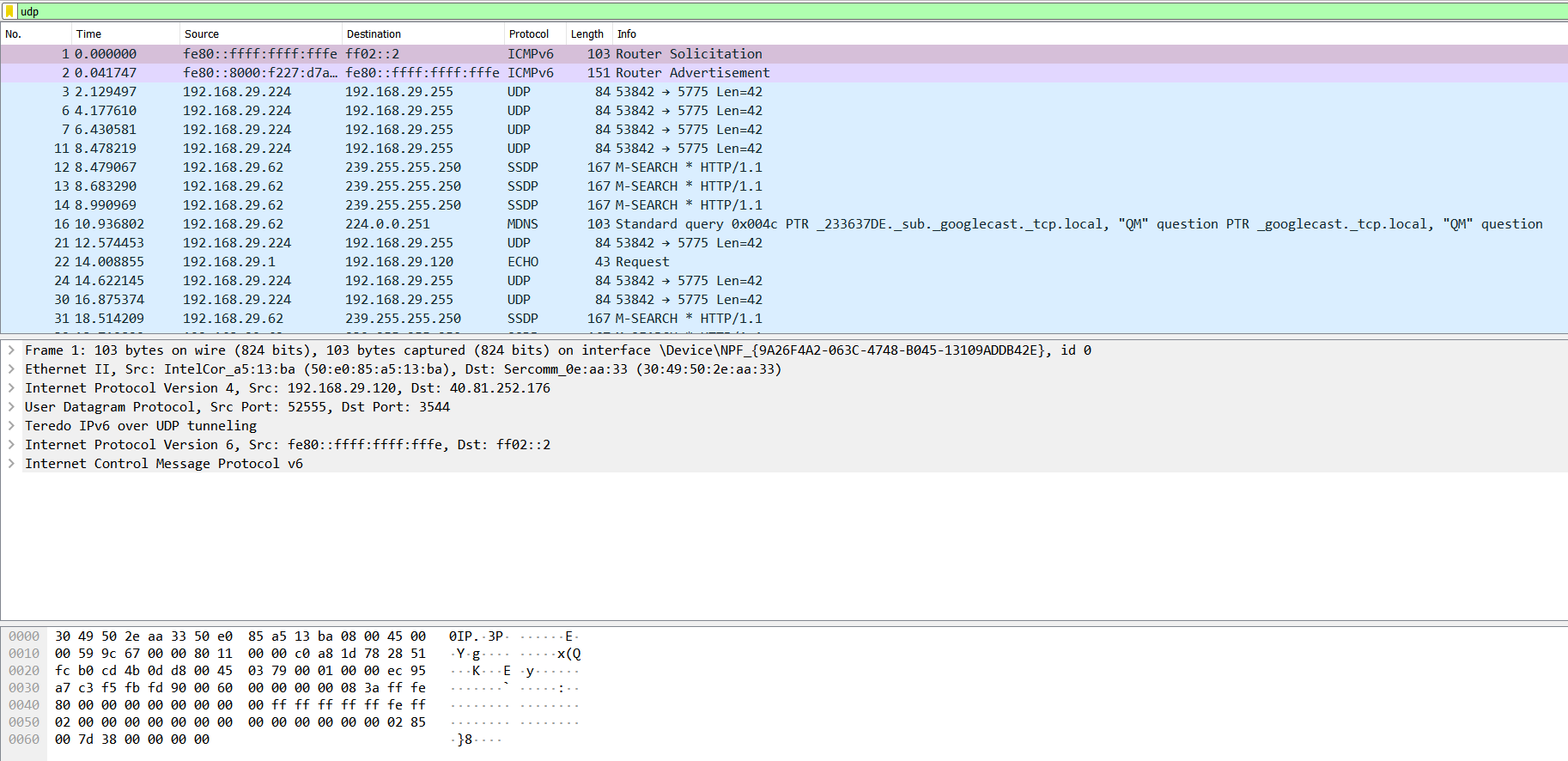
3)You can apply/change color schemes for packets of different protocols from the View->Change Color Menu.

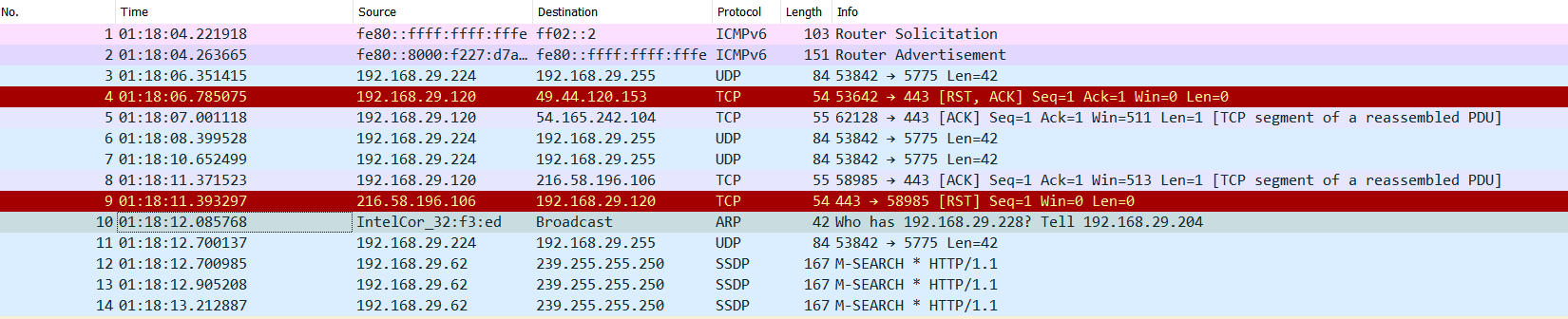


4)You can select any particular packet to study about it in another window by double clicking on it.

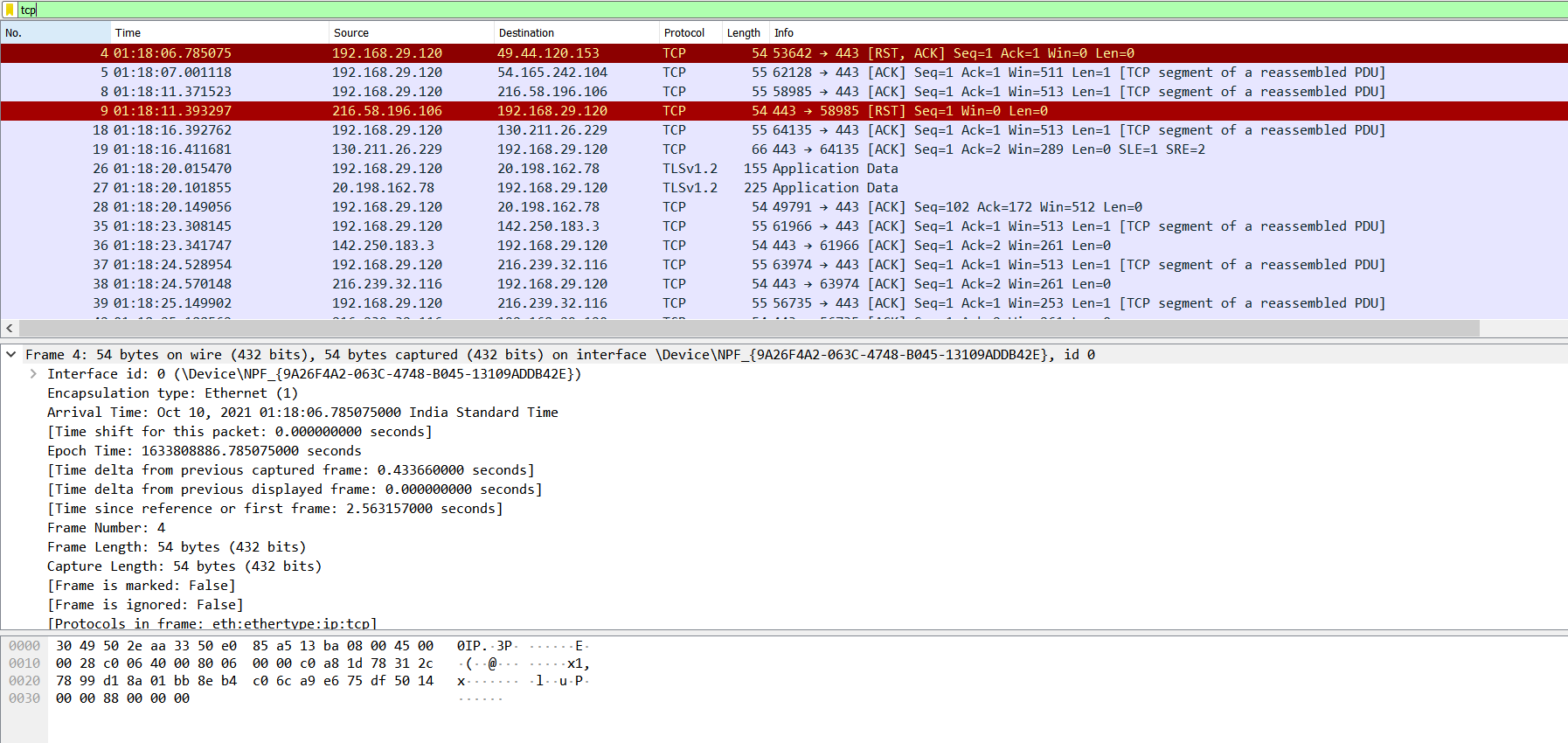
5)We can monitor the network devices and any devices connected to our network.We can enable/disable any device we want to connect to.



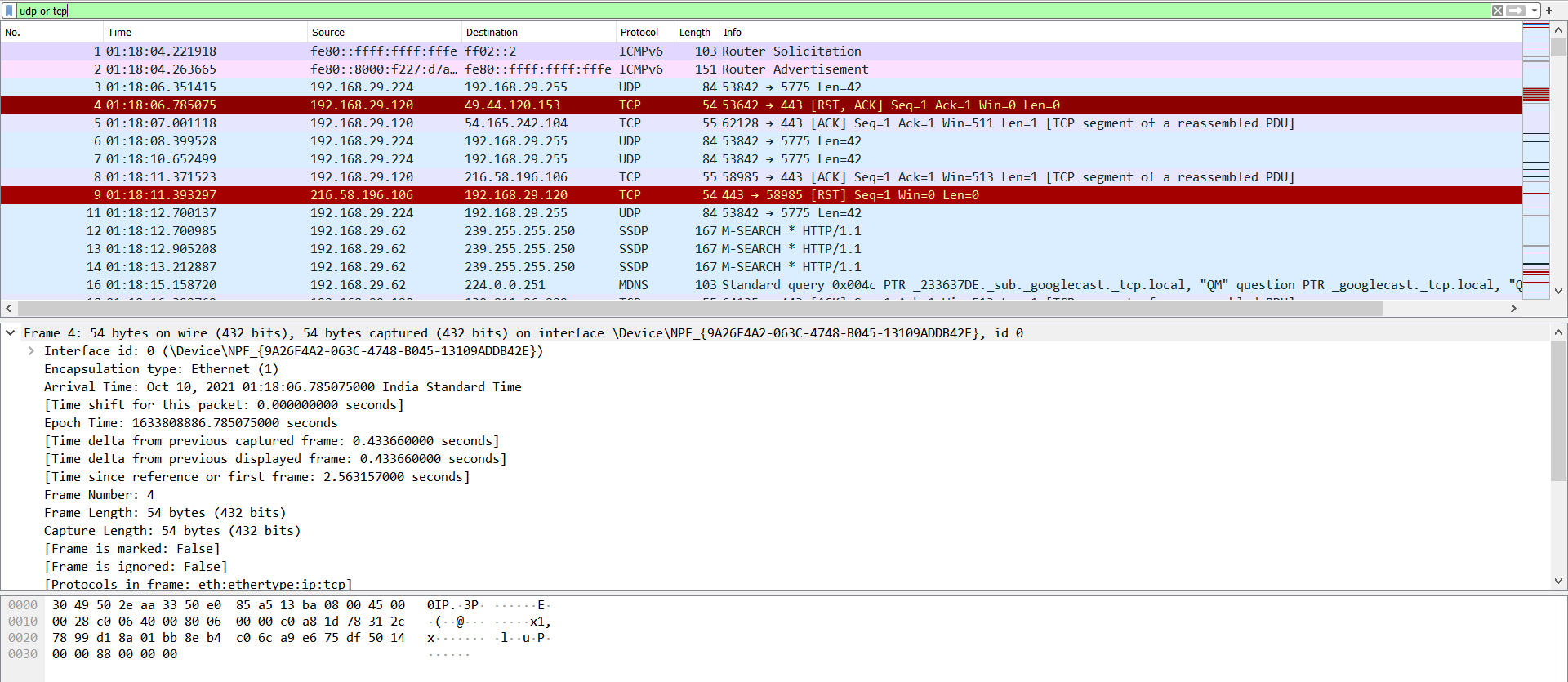


6) We can search for any particular packet using Capture Filter.

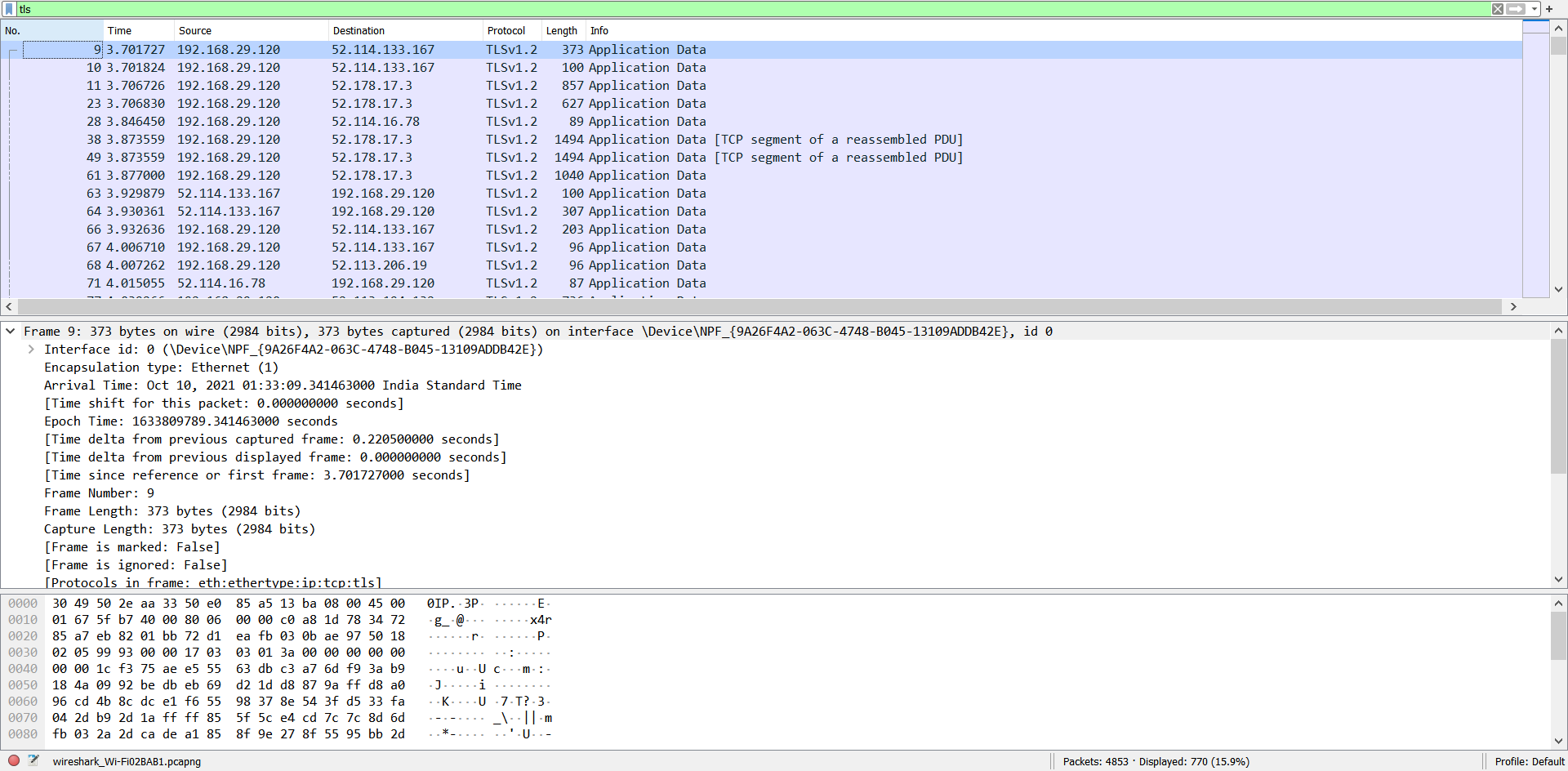
7)Capture only TCP Packets.



8)Capture only TCP or UDP packets using capture filter.



If we want to search for **https**,we have to put **tls** in the capture filter.

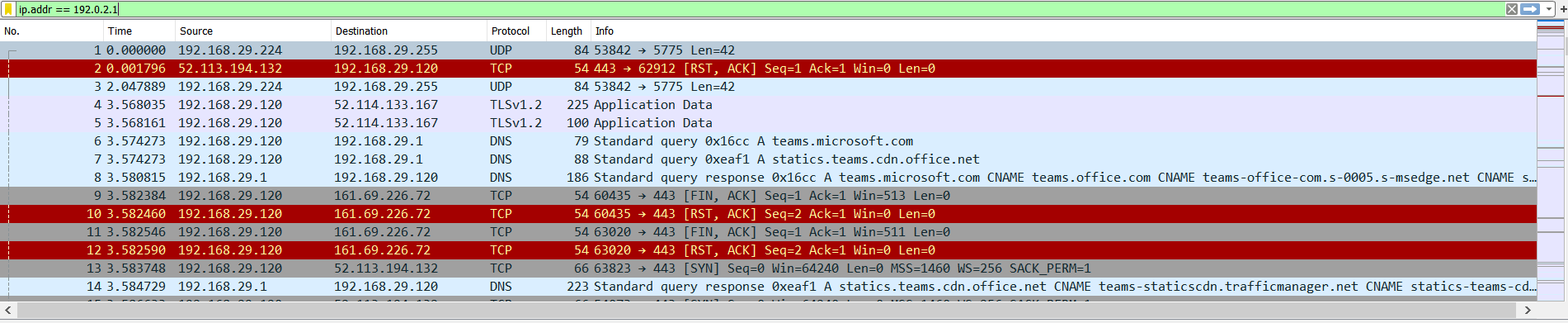


Black colored packets either mean as mad TCP or it indicates checksum error.

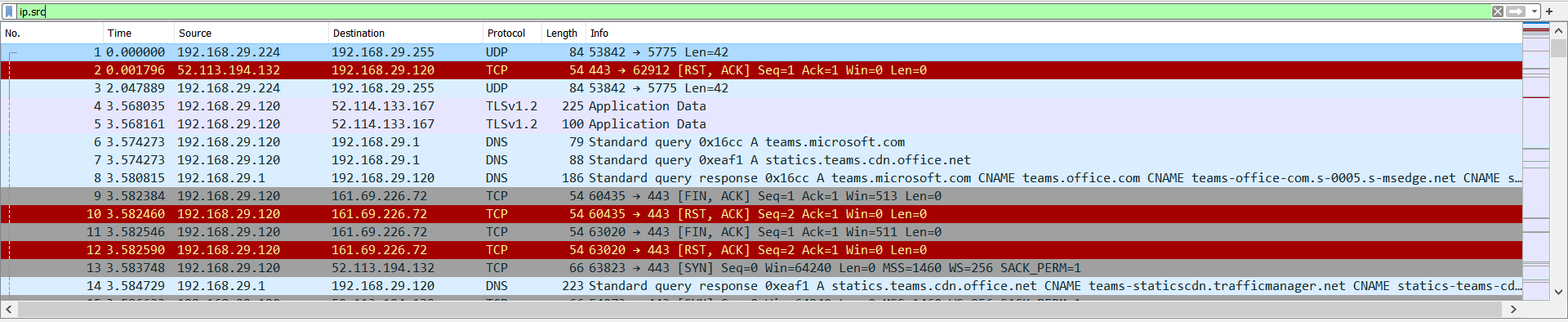
To view only HTTP traffic, type http (lower case) in the Filter box and press Enter. Select the first HTTP packet labeled GET /. Observe the destination IP address.

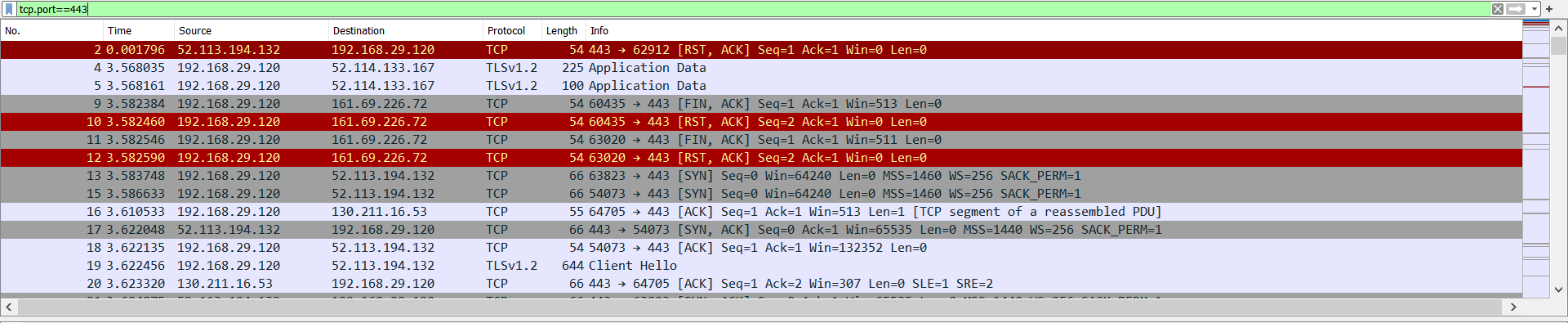
UDP is much faster. TCP is slow as it requires 3-way handshake. The load on DNS servers is also an important factor. DNS servers (since they use UDP) don’t have to keep connections. DNS requests are generally very small and fit well within UDP segments. UDP is not reliable, but reliability can added on application layer. An application can use UDP and can be reliable by using a timeout and resend at the application layer. Differentiate http and https traffic. HTTPS is HTTP with encryption. The only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses. As a result, HTTPS is far more secure than HTTP.

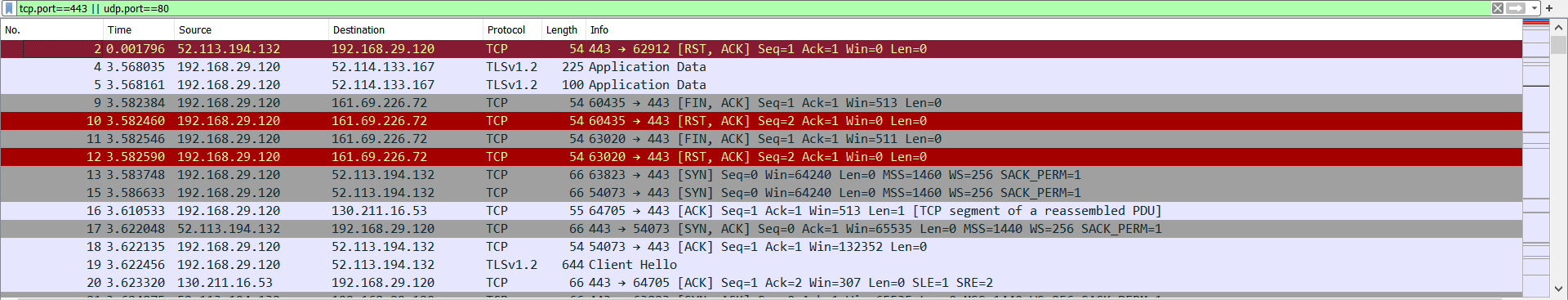
9)Capture packets for any IP Address.

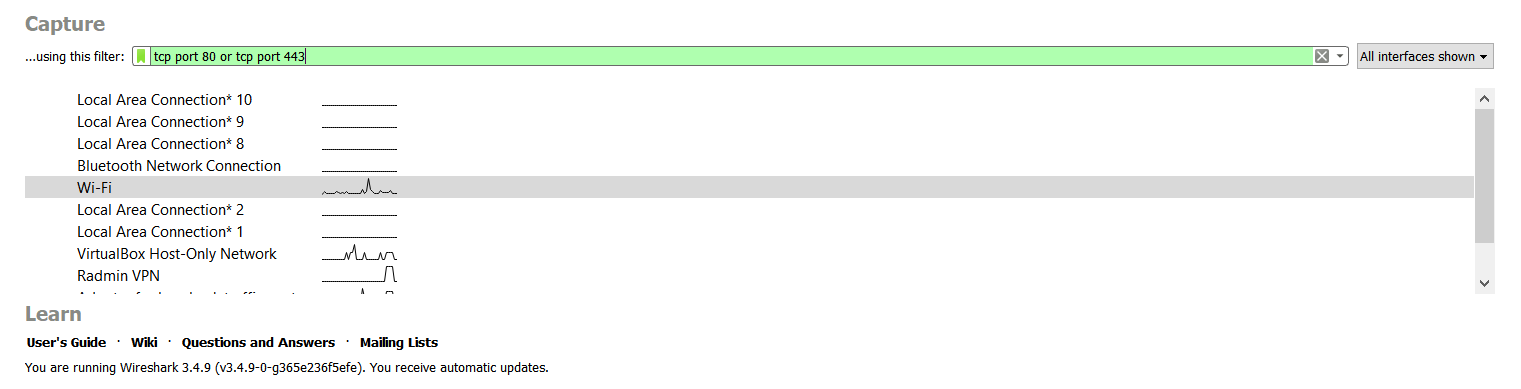
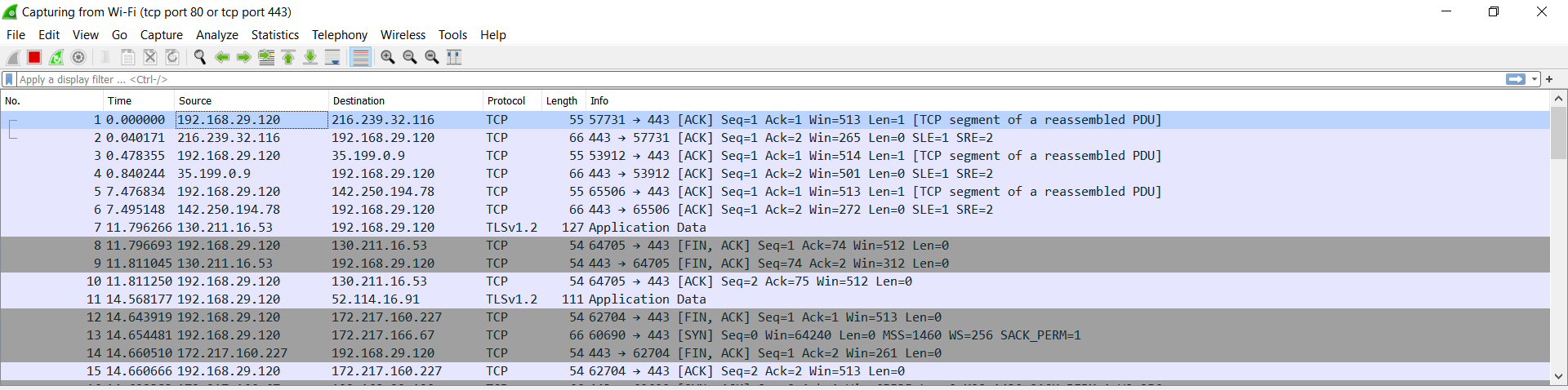


10)Capture packets from source IP.

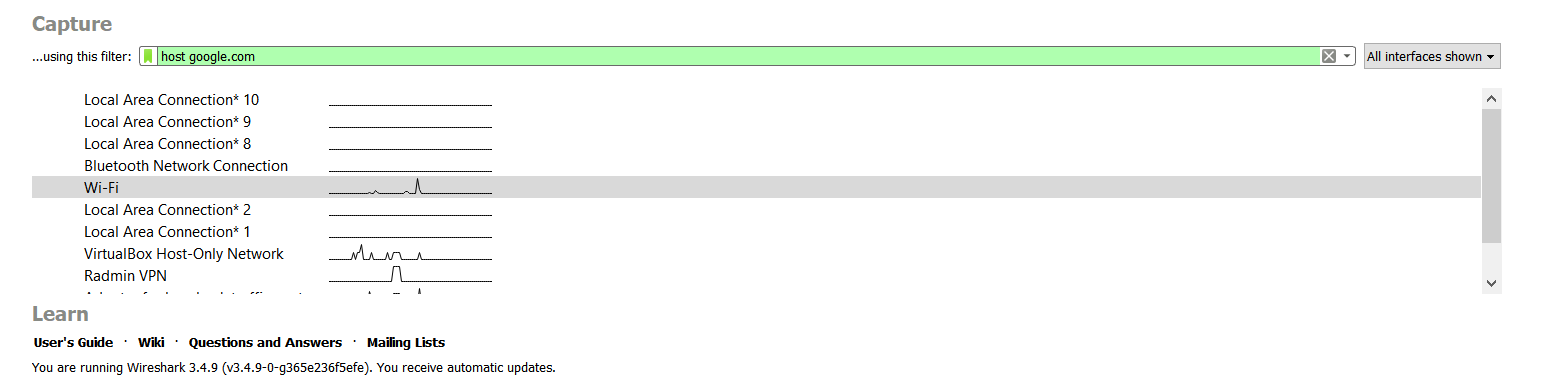


11)Capture packets for any specified TCP port.

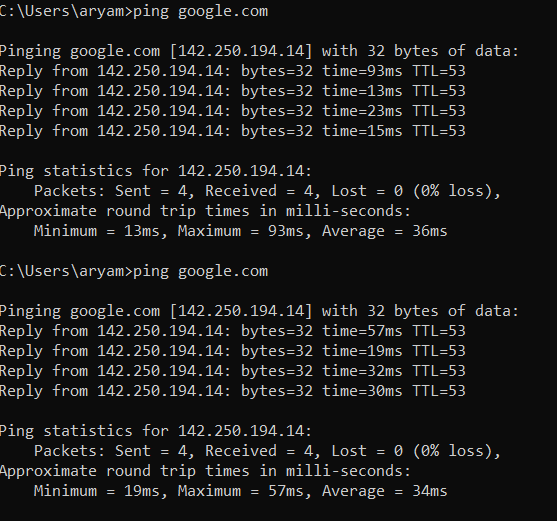
12) Capture packets for any specified TCP or UDP port. 

13)You can also use the Capture Filter from the main menu and select your desired interface you want to capture packets on. 

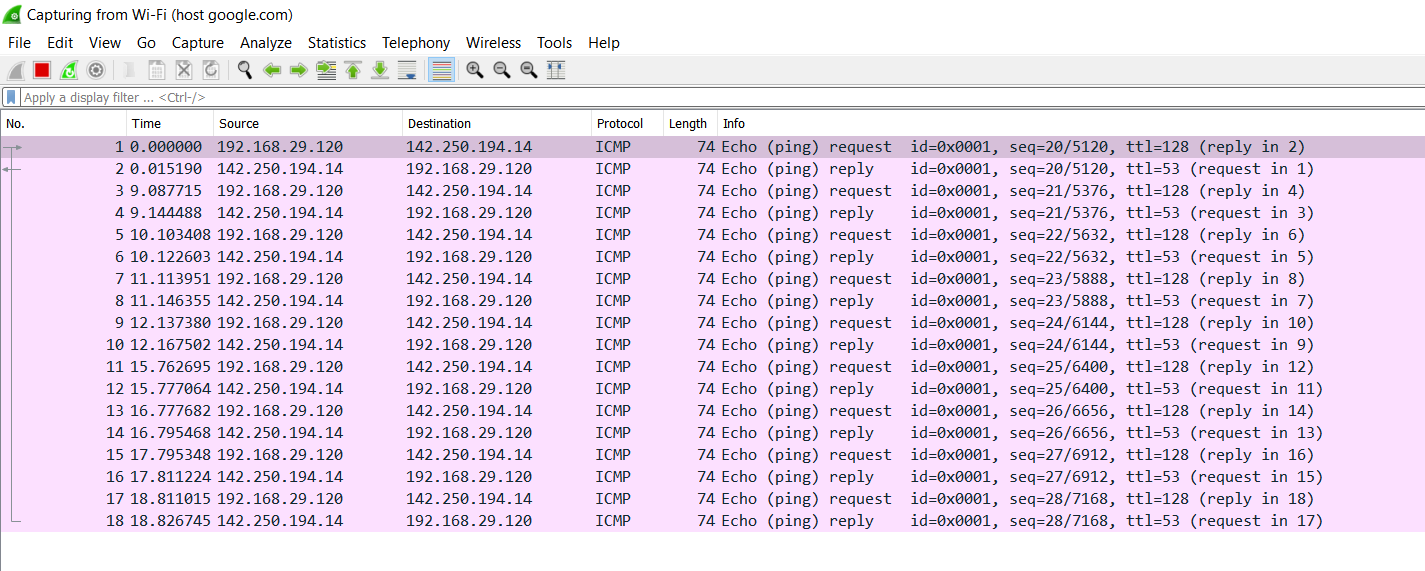
14)Ping from cmd and capture packets on Wireshark.

Write host google.com on the filter bar.

Open Command Prompt on your device and ping google.com.When pinging starts,start the capture process on Wireshark.



You can view the ICMP packets captured during the ping on Wireshark.



Conclusion:The Installation and functionalities of Wireshark were noted successfully.