**AIM:**

Capturing and analyzing network packets using Wireshark (Fundamentals) :

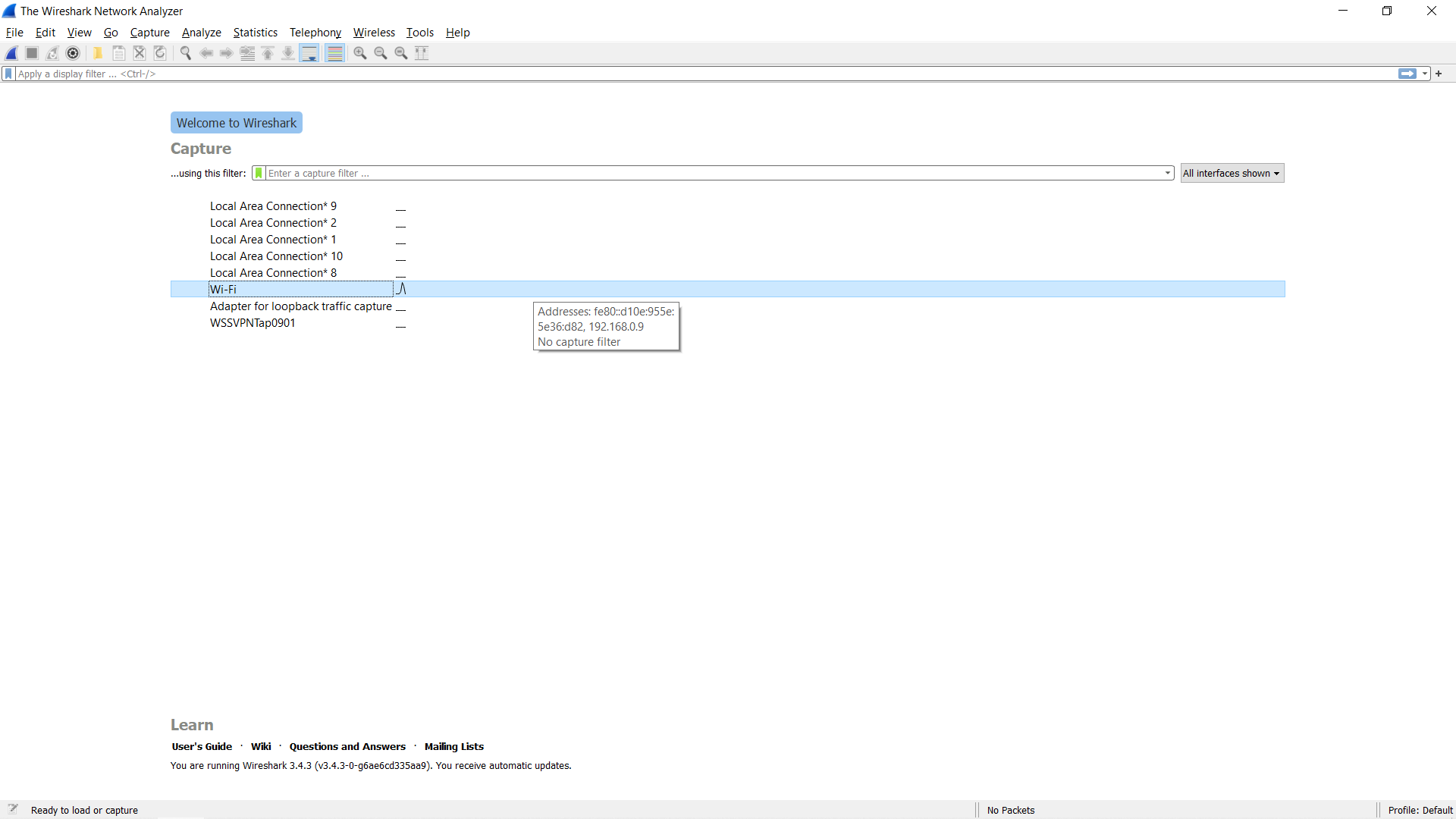
- Identification the live network

- Capture Packets

- Analyze the captured packets

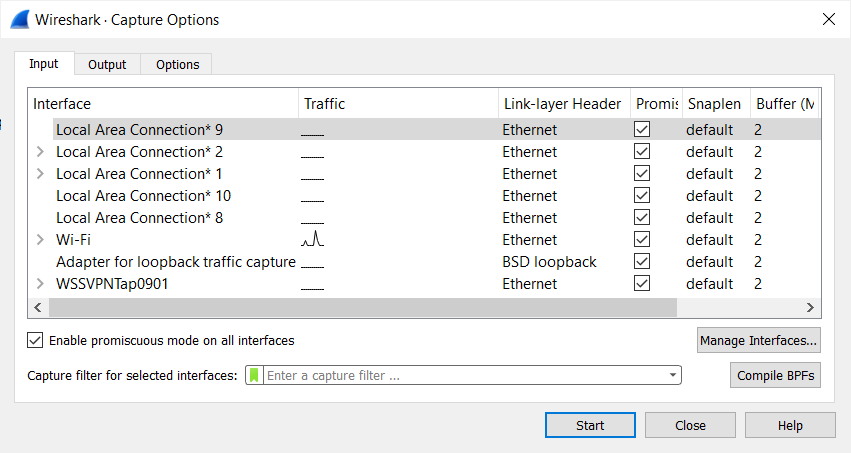
**Capturing Packets**

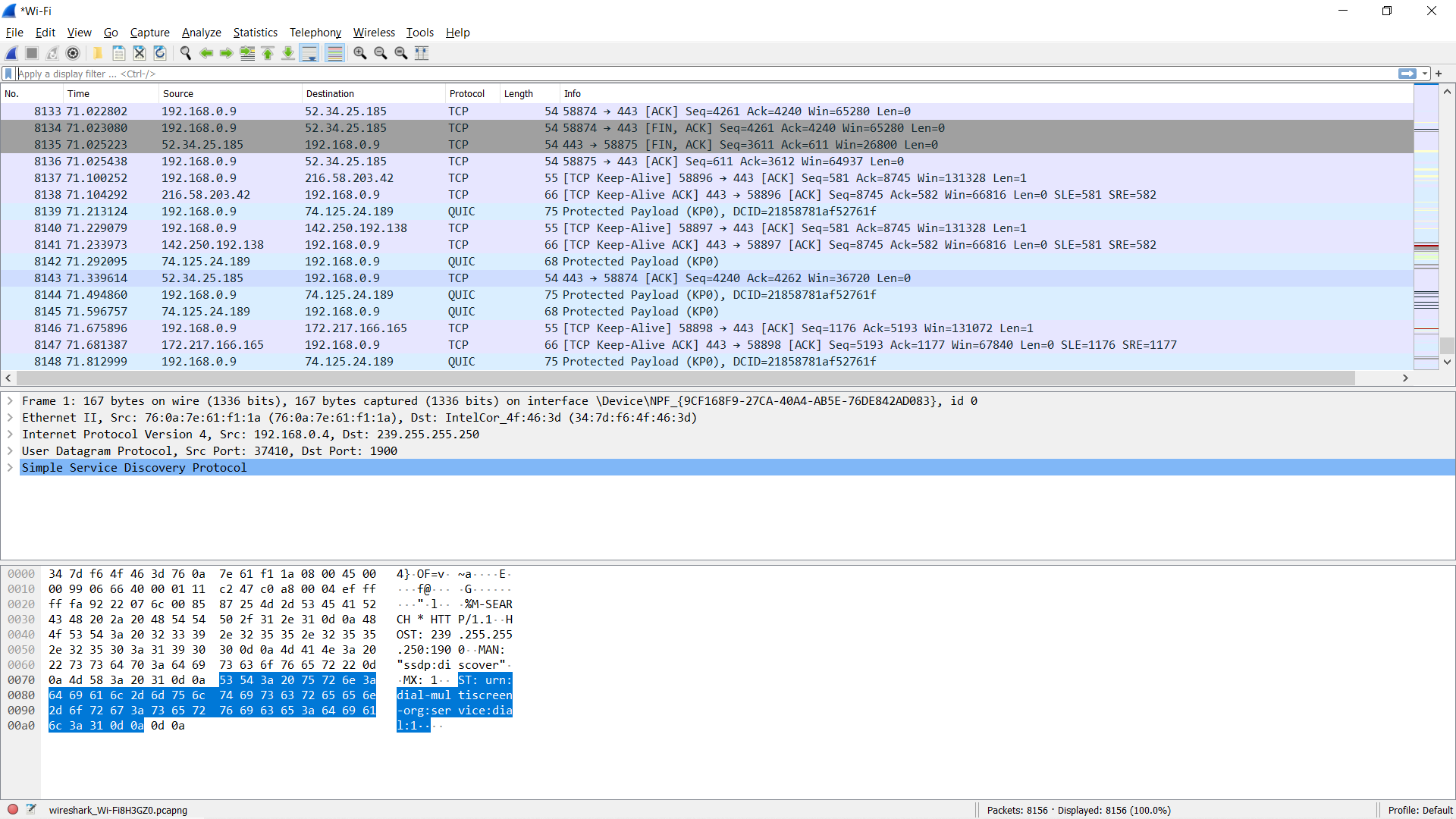
Capture traffic on your wireless network, click your wireless interface. You can configure advanced features by clicking Capture > Options, but this isn’t necessary for now.



As soon as you single-click on your network interface’s name, you can see how the packets are working in real time. Wireshark will capture all the packets going in and out of our systems.

Promiscuous mode is the mode in which you can see all the packets from other systems on the network and not only the packets send or received from your network adapter. Promiscuous mode is enabled by default. To check if this mode is enabled, go to Capture and Select Options. Under this window check, if the checkbox is selected and activated at the bottom of the window. The checkbox says “Enable promiscuous mode on all interfaces”.





The red box button **“STOP”** on the top left side of the window can be clicked to stop the capturing of traffic on the network.

**Color Coding**

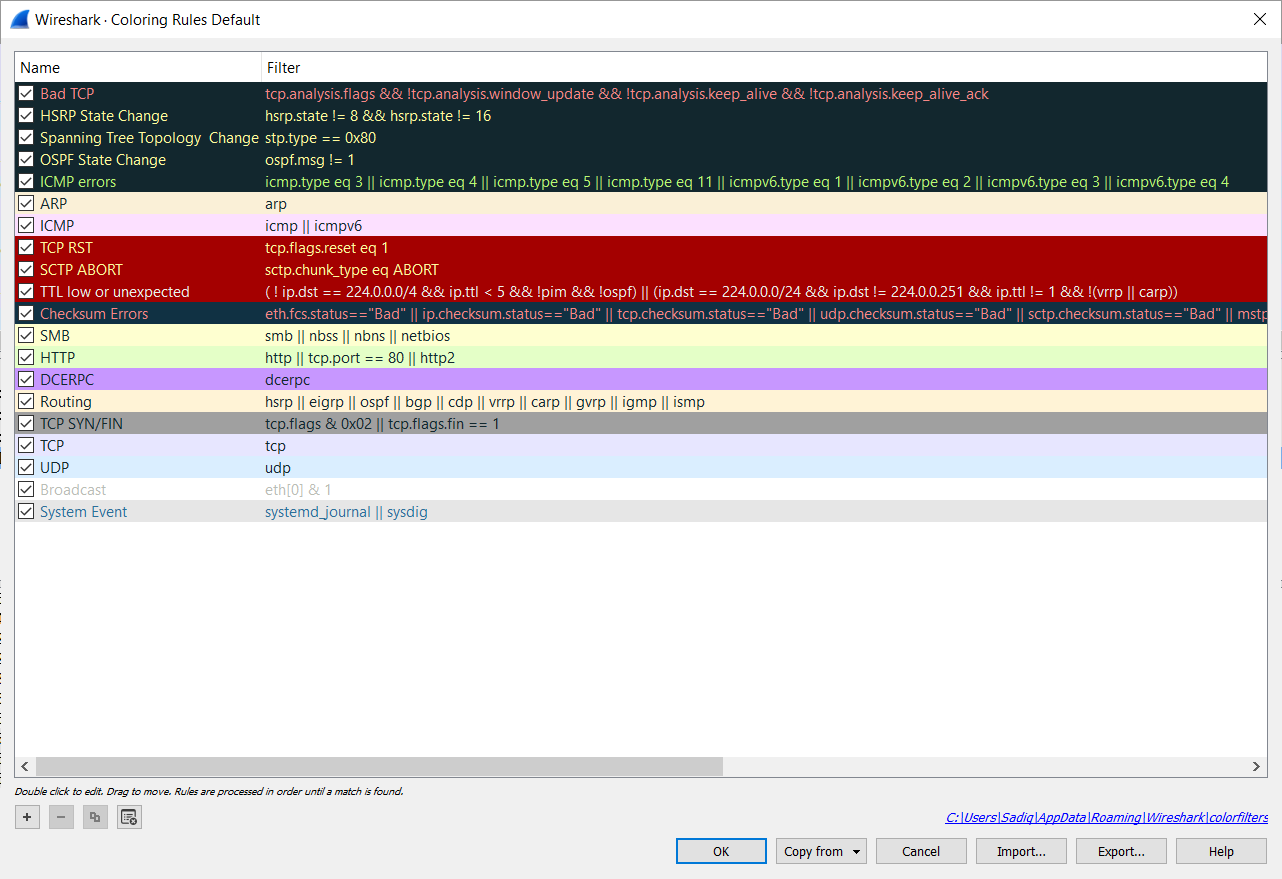
Different packets are seen highlighted in various different colors. This is Wireshark’s way of displaying traffic to help you easily identify the types of it. Default colors are:

Light Purple color for TCP traffic

Light Blue color for UDP traffic

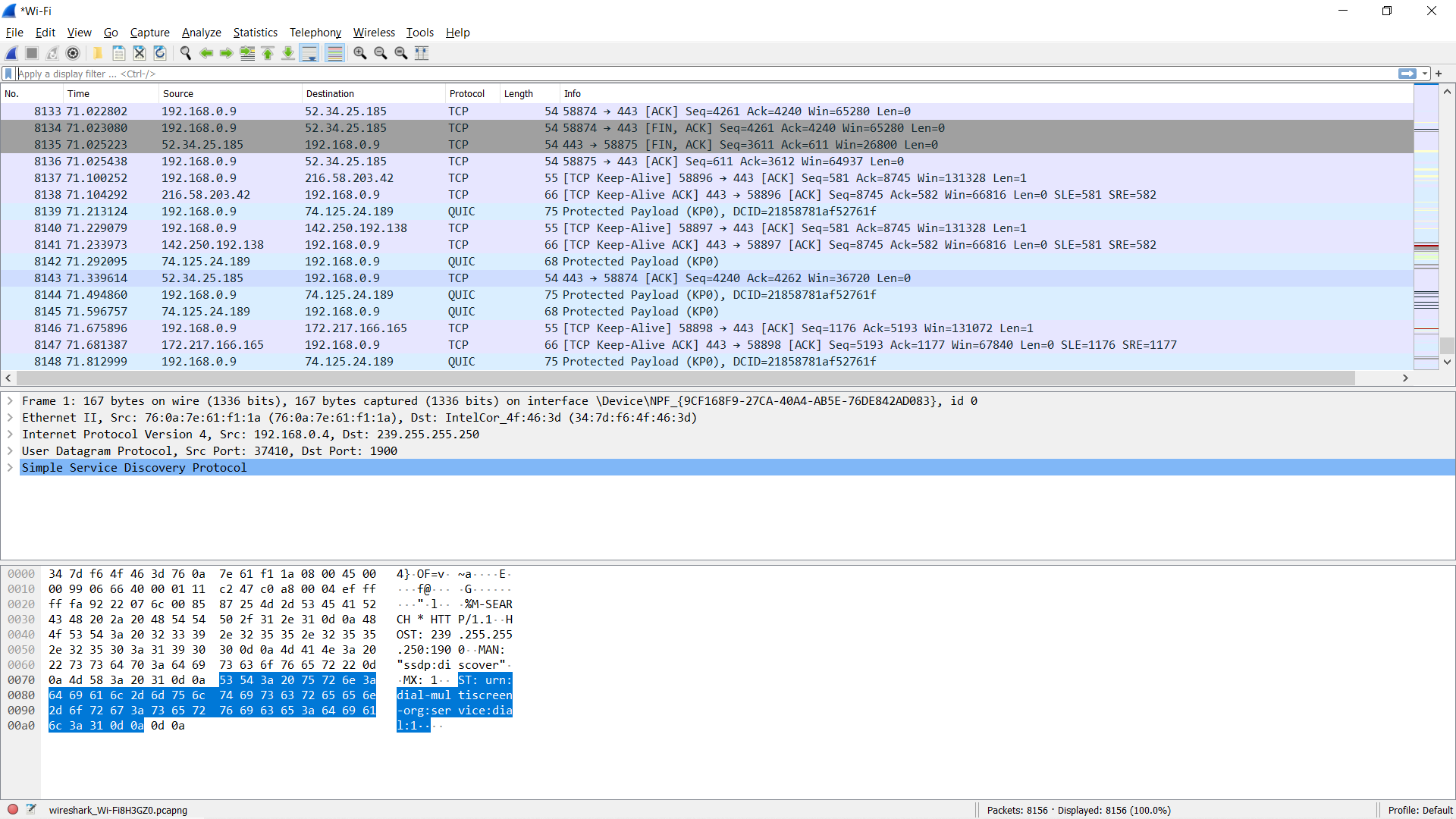
Black color identifies packets with errors – example these packets are delivered in an unordered manner.

To check the color coding rules click on View and select Coloring Rules. These color coding rules can be customized and modified to fit your needs.

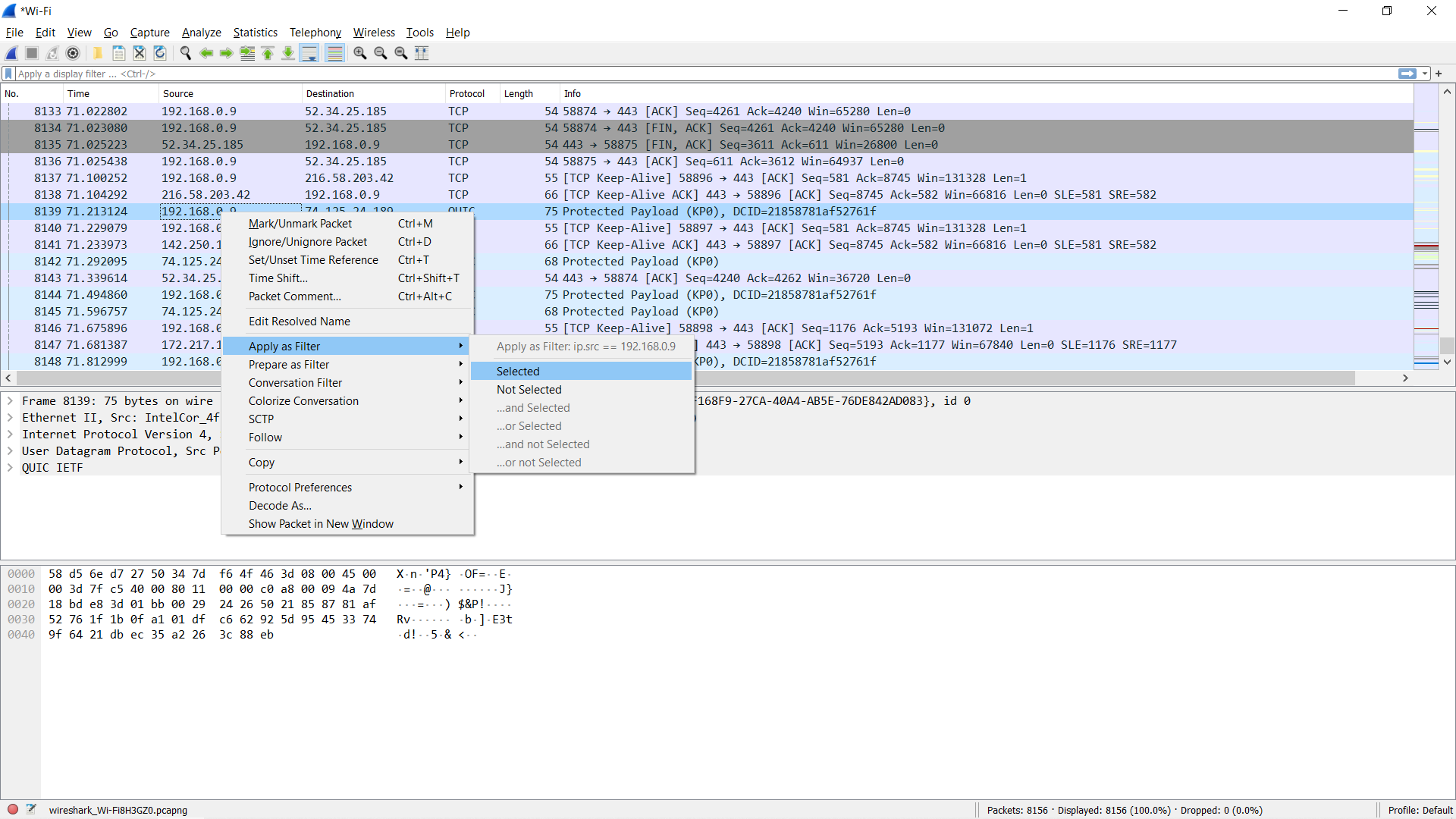


**Analyze the captured Packets:**

First of all, click on a packet and select it. Now, you can scroll down to view all its details.



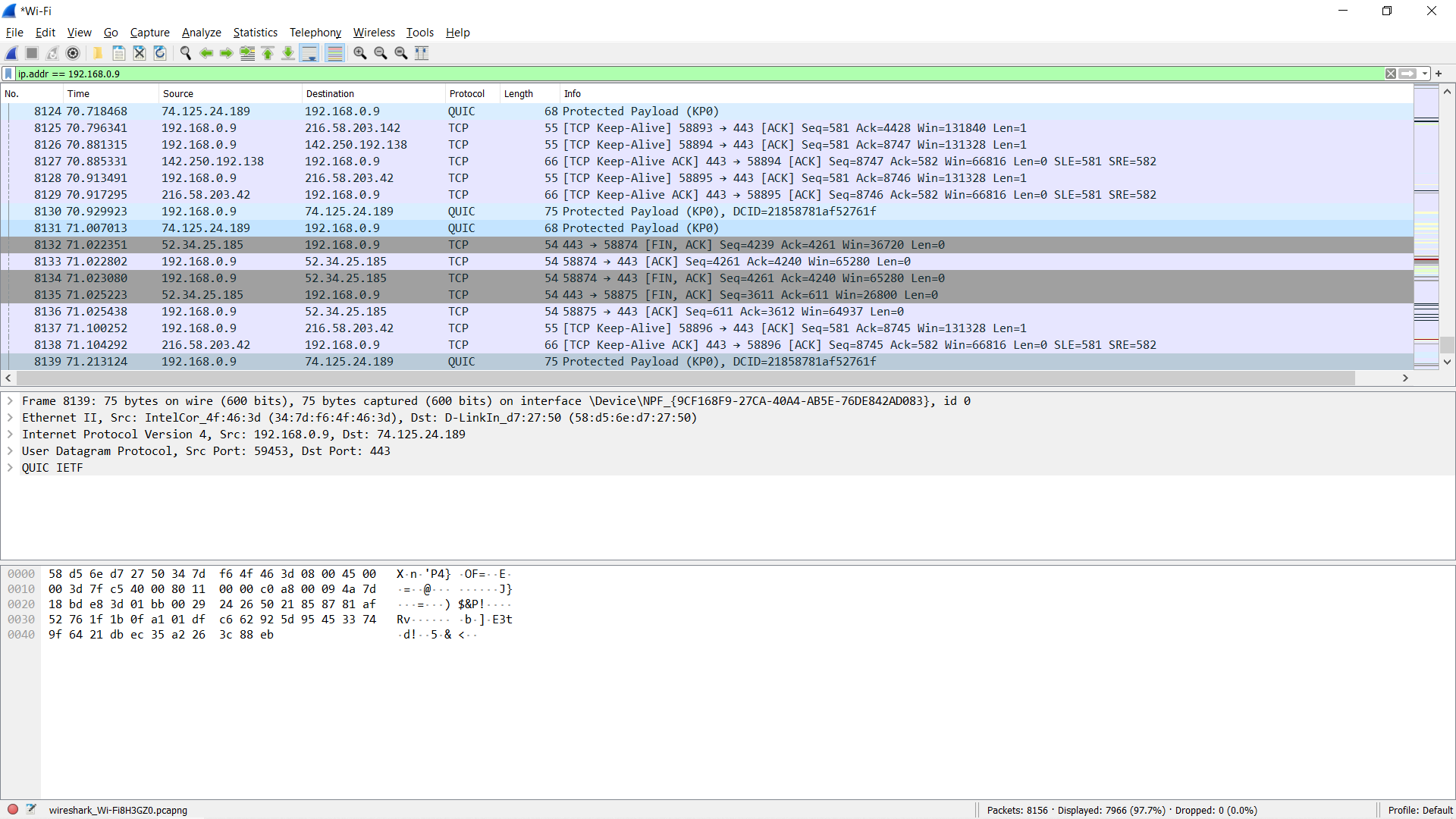
Filters can also be created from here. Right-click on one of any details. From the menu select Apply as Filter drop-down menu so filter based on it can be created.



**Display filter command –**

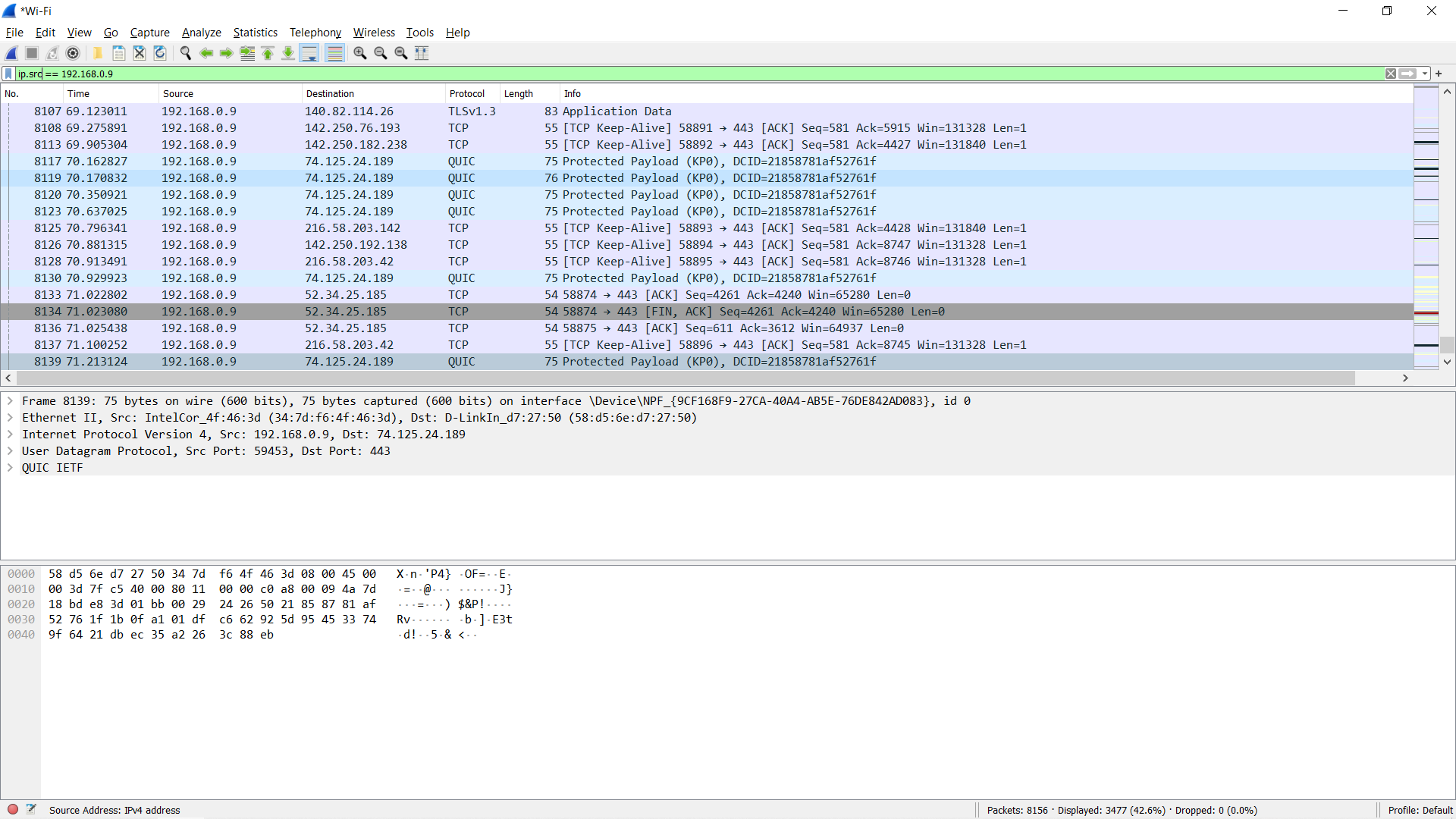
1.Display packets based on specific IP-address

* **ip.addr == 192.168.0.9**



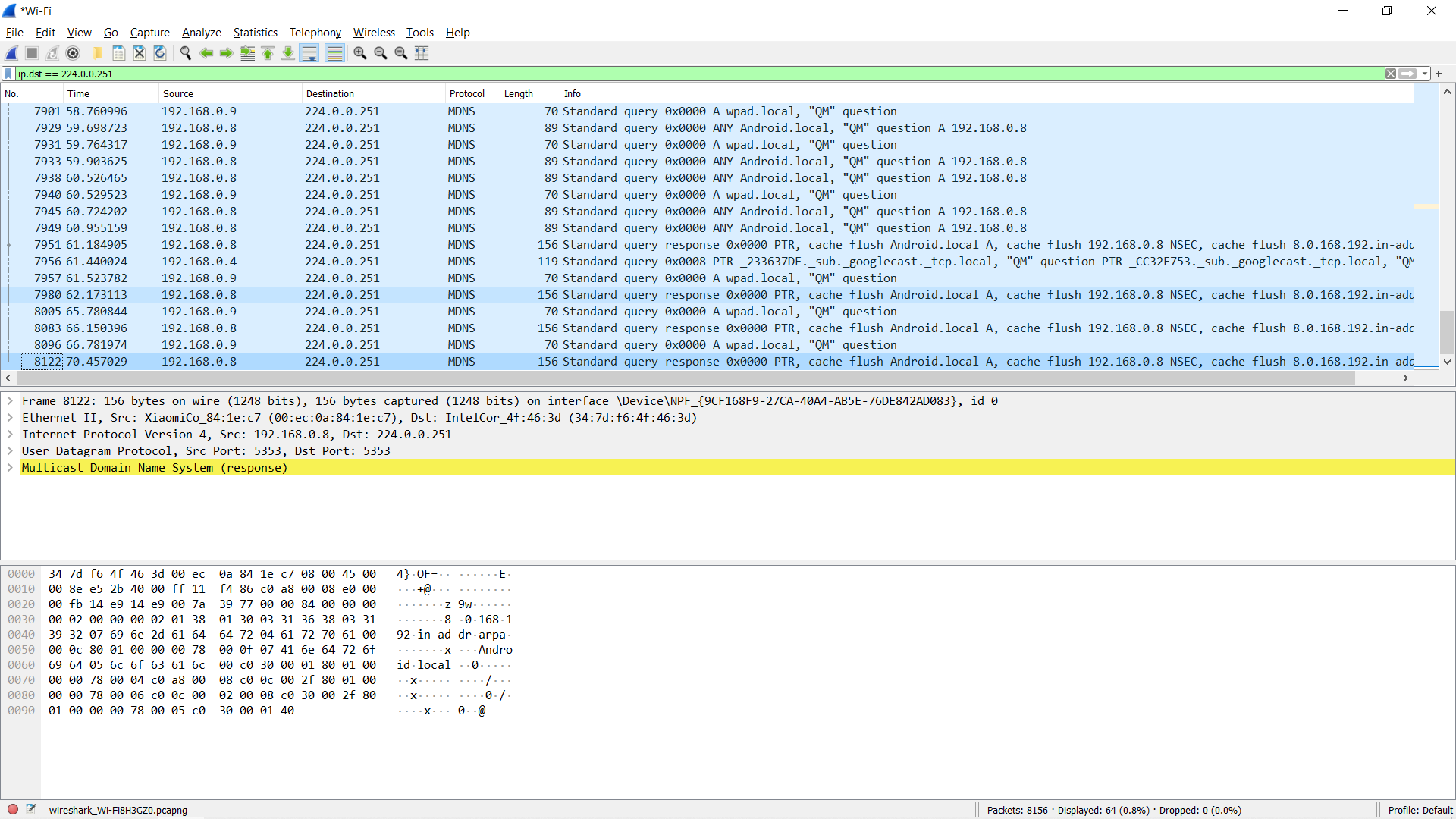
2. Display packets which are coming from specific IP-address

* **ip.src == 192.168.0.9**



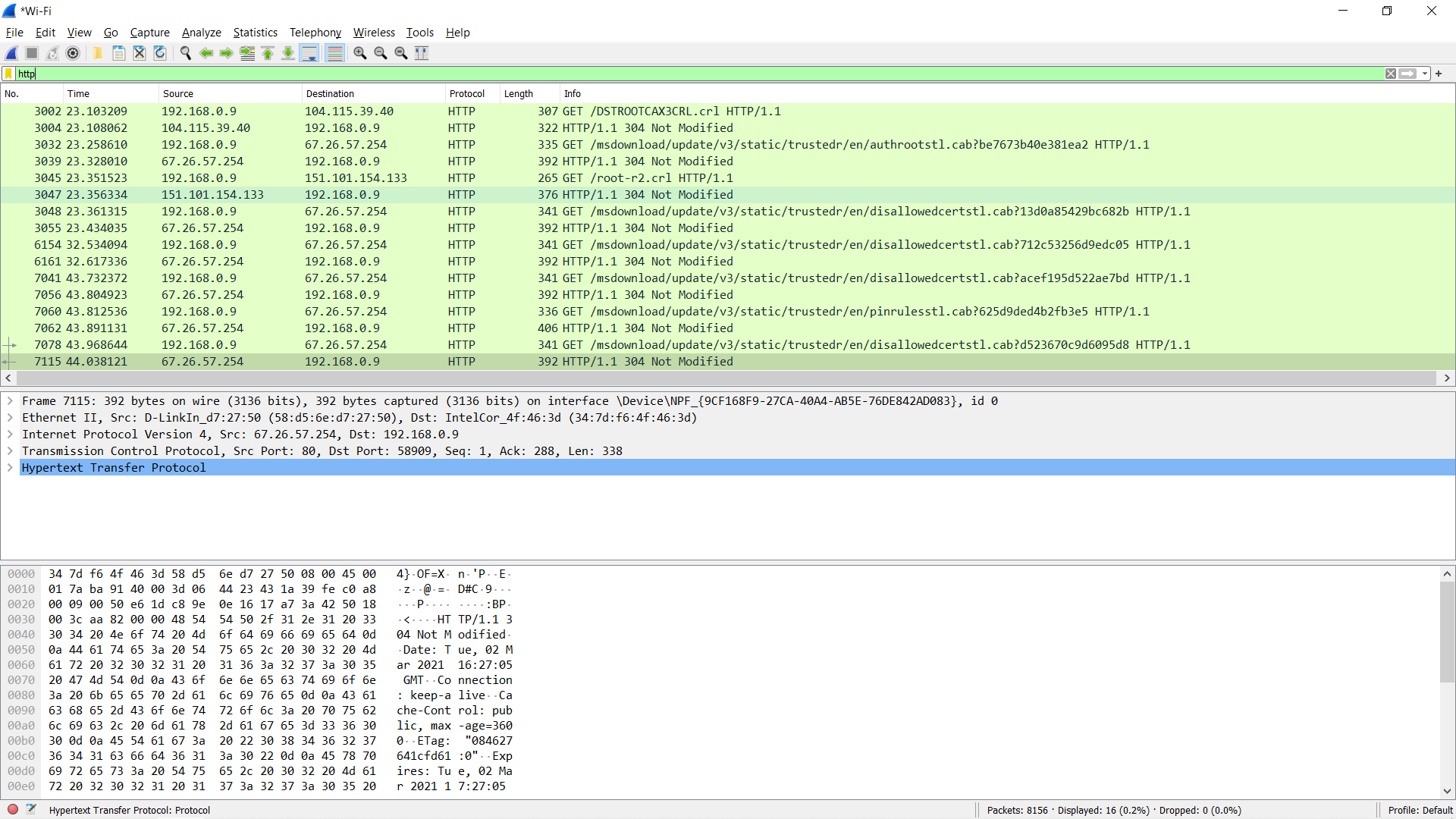
3. Display packets which are having specific IP-address destination

* **ip.dst == 224.0.0.251**



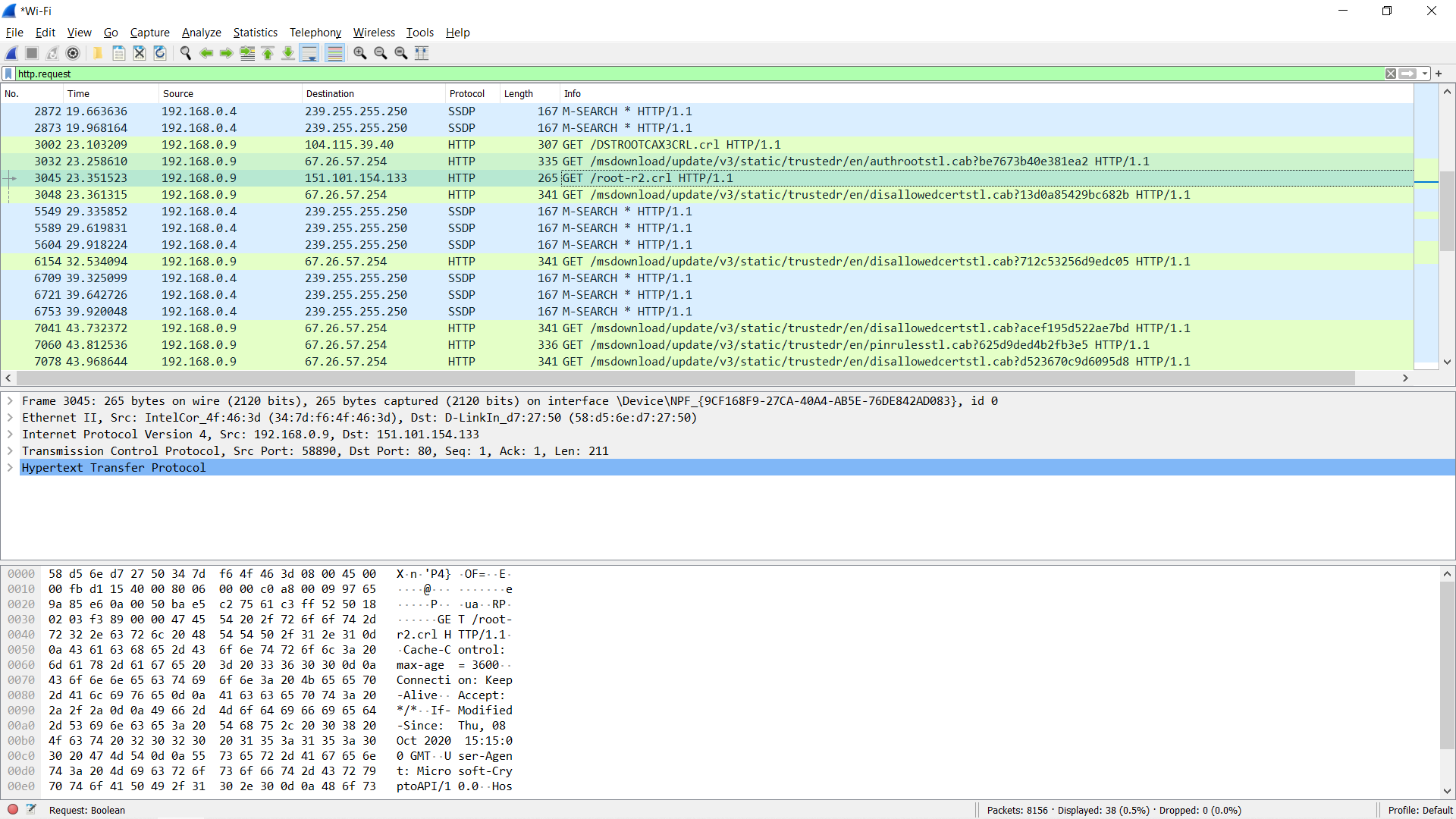
4. Display packets which are using http protocol

* **http**



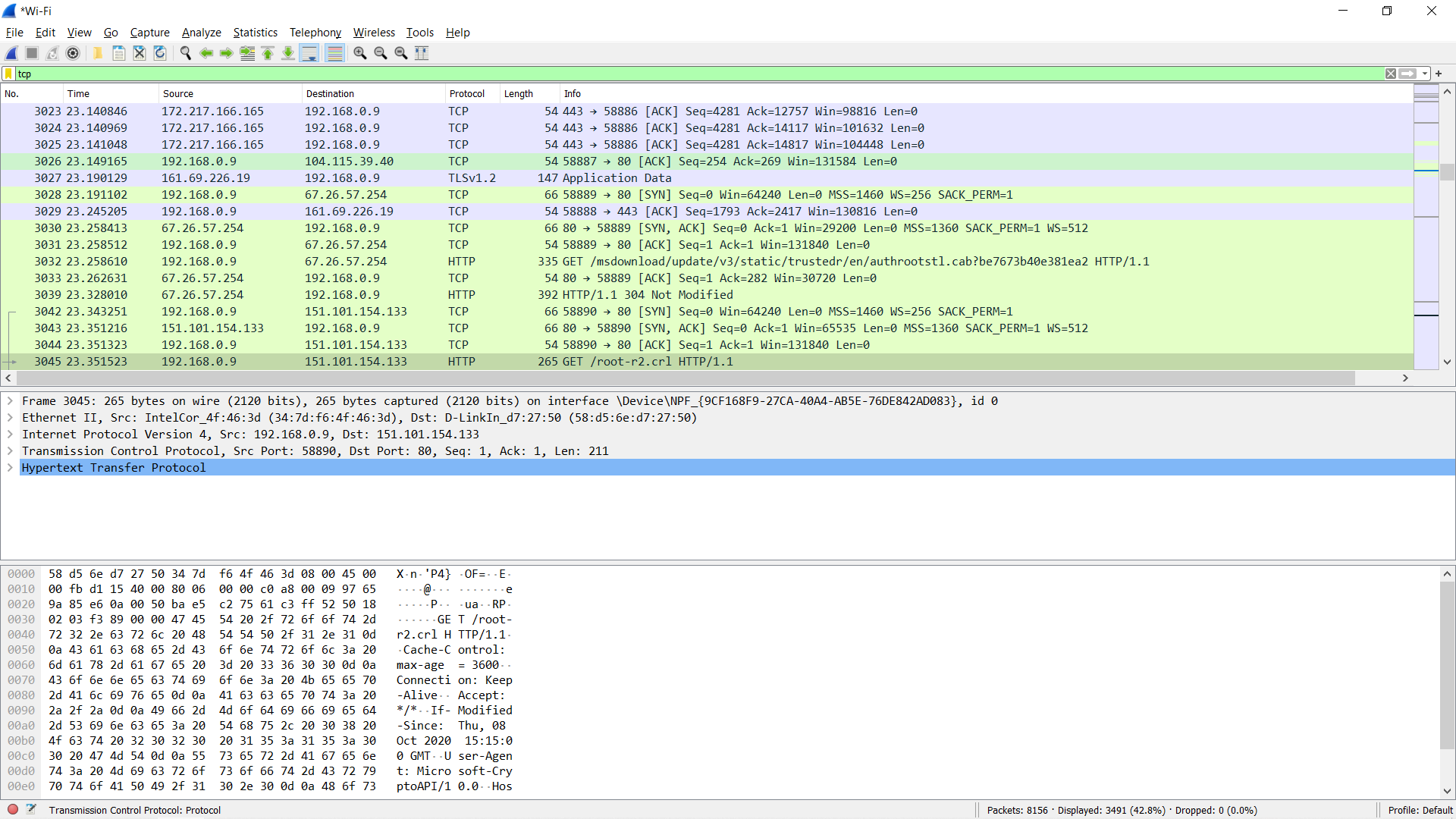
5. Display packets which are using http request

* **http.request**



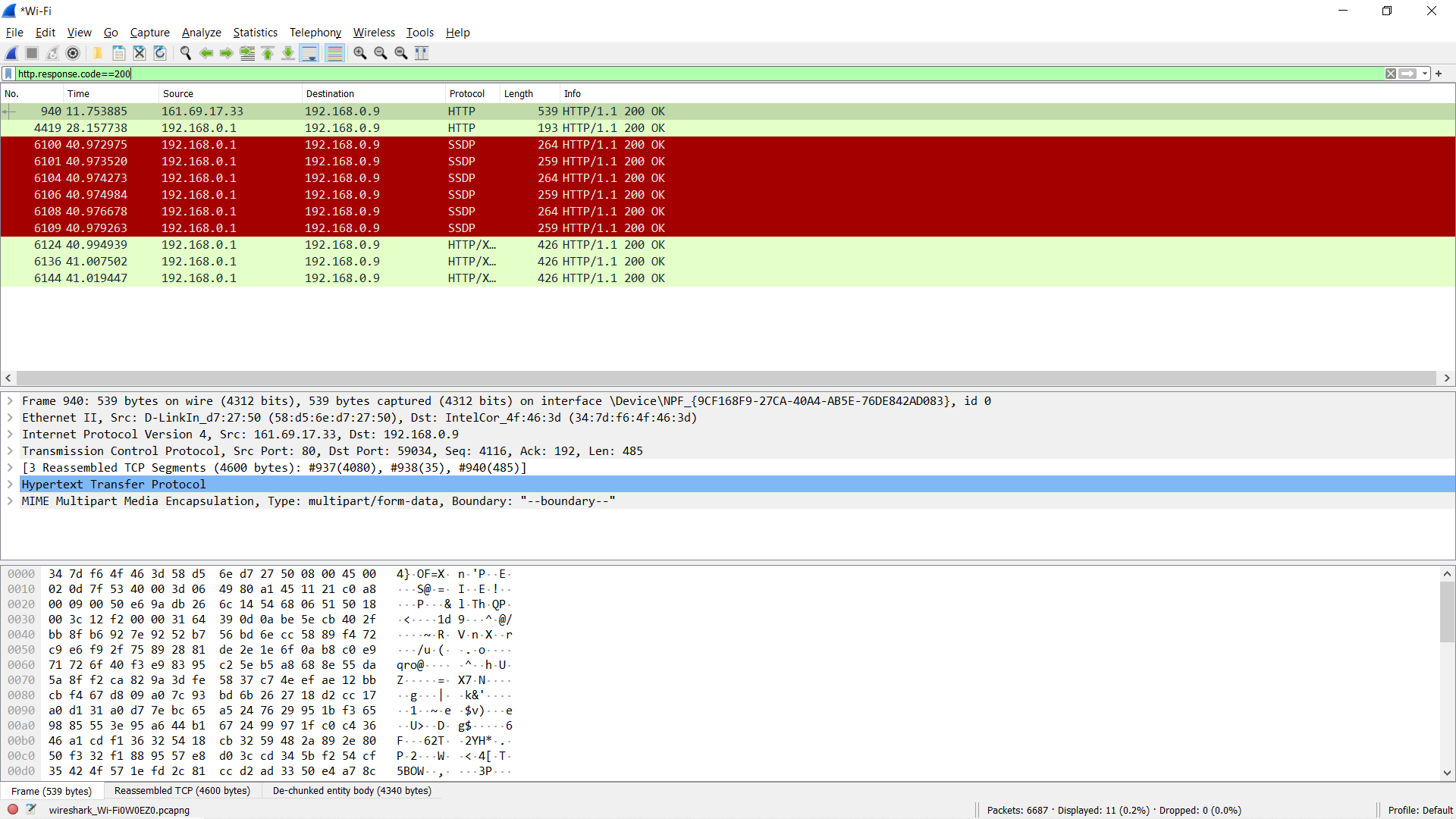
6. Display packets which are using TCP protocol

* **tcp**



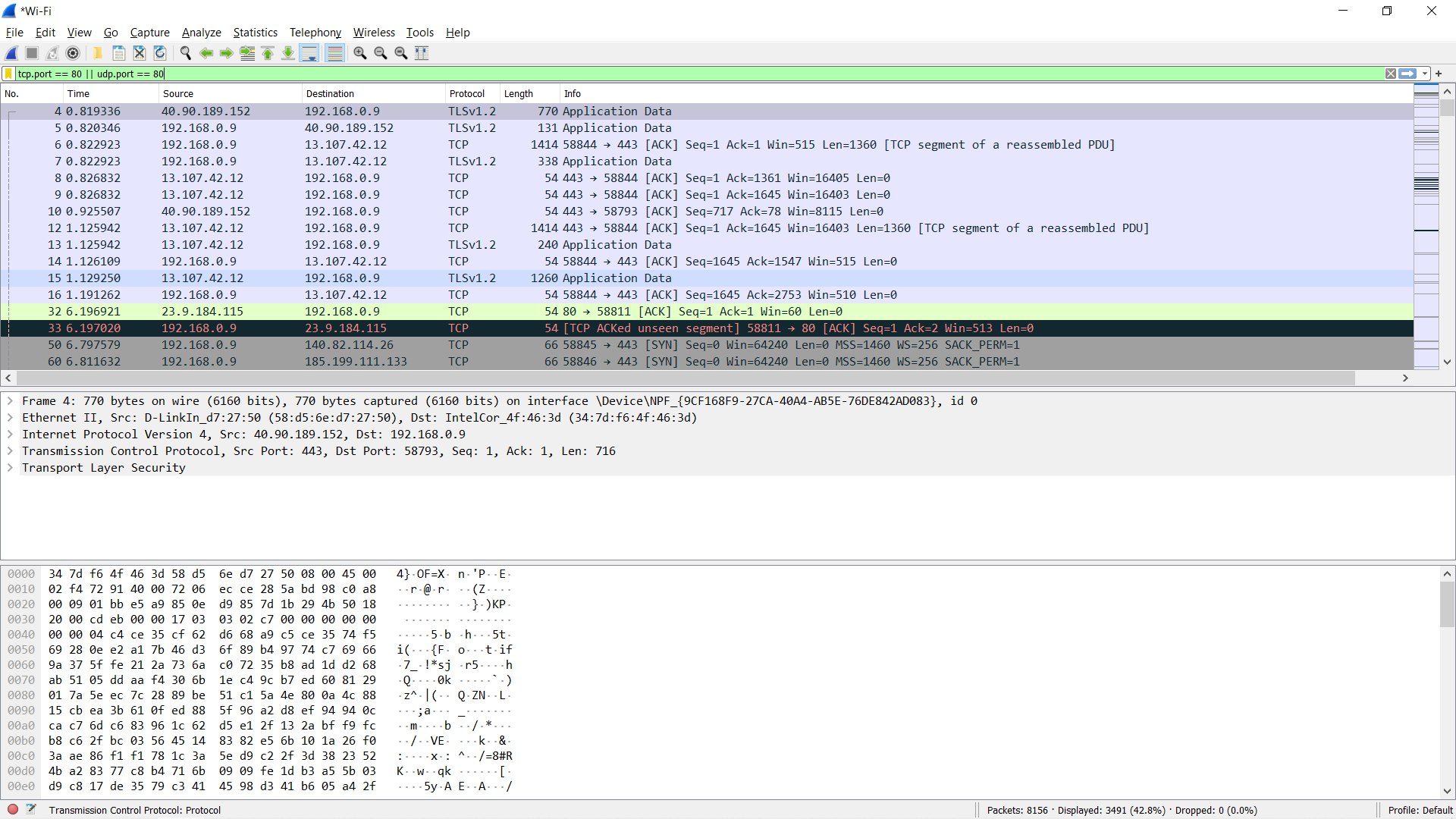
7. Display packets having no error connecting to server

* **http.response.code==200**



8. Display packets having port number 80

* **tcp.port==80 || udp.port==80**



9. Display packets which that contains keyword facebook

* **tcp contains facebook**

