Name : Md. Sohag Hossain

ID : IT-17060

Lab report no : 2

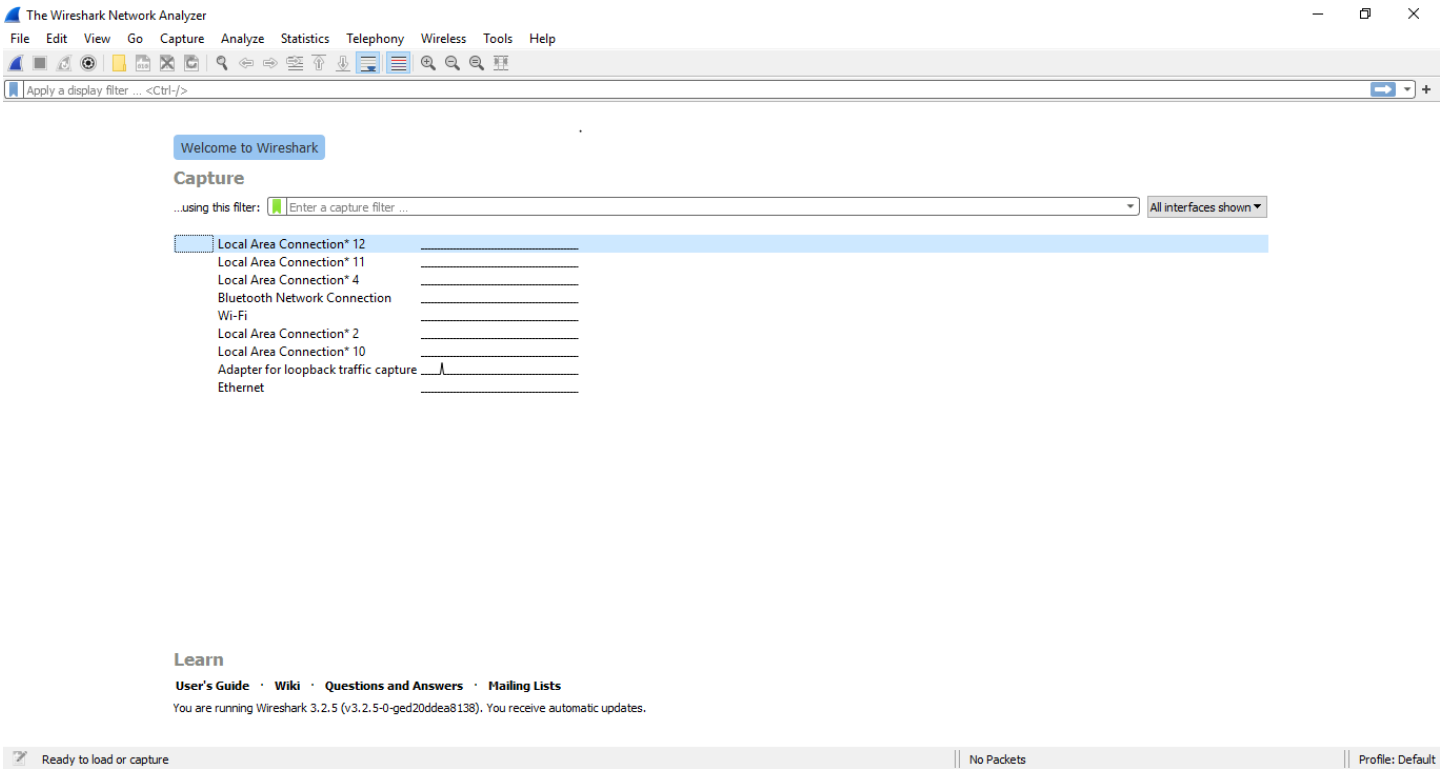
Name of the lab report : Wireshark display

Objectives : To learn basic packet analysis using Wireshark

Theory:

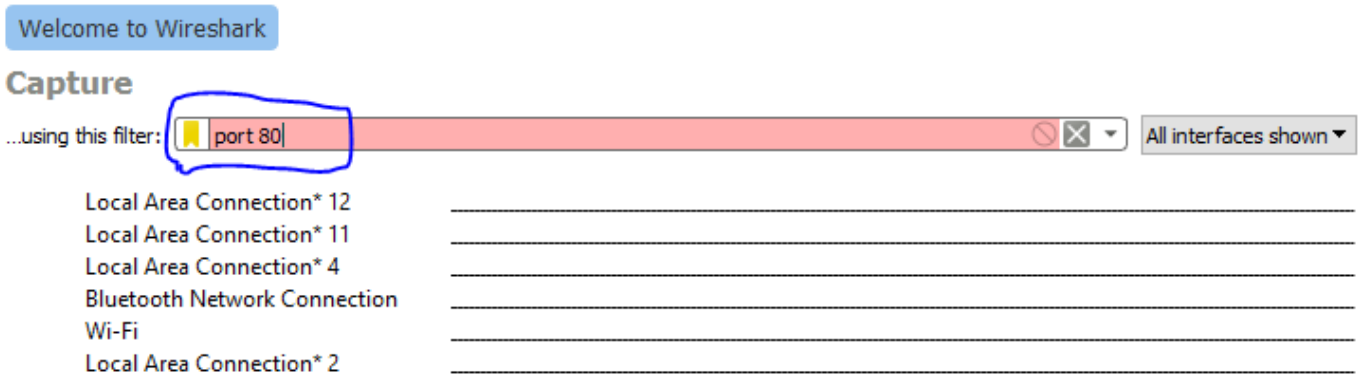
Wireshark is the world's leading network traffic analyzer, and an essential tool for any security professional or systems administrator. This free software lets you analyze network traffic in real time, and is often the best tool for troubleshooting issues on your network.

Opening display of Wireshark:

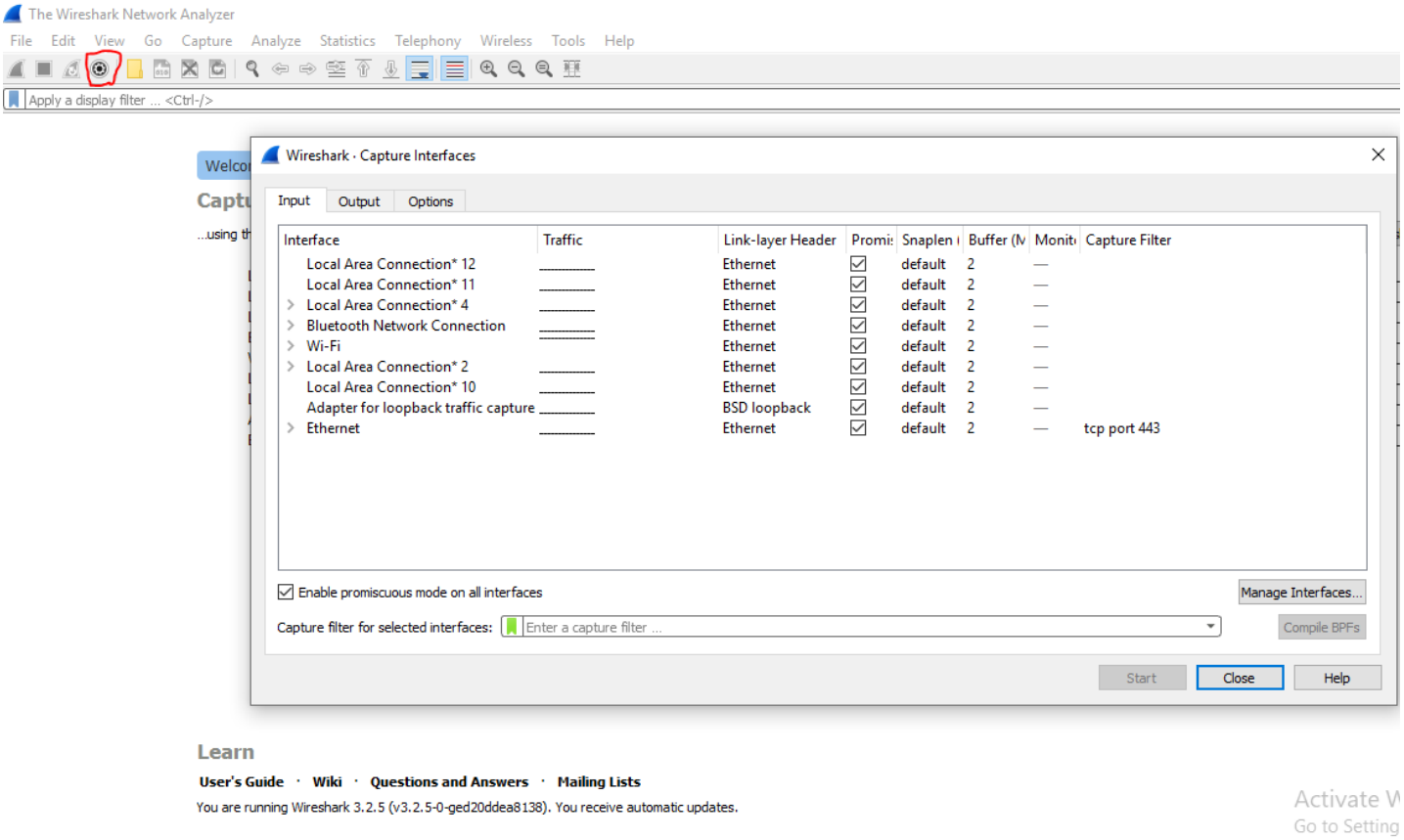


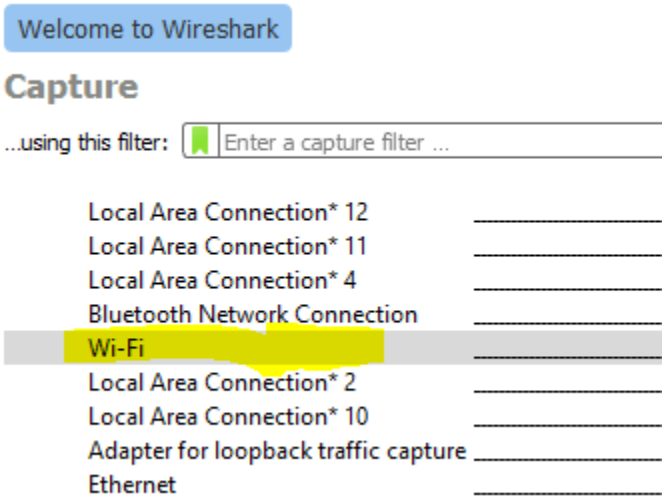
Packet Capturing:

In order to packet capturing we need click capture bar and write any packet name such as port 80, tcp port 443, tcp port http and many others.

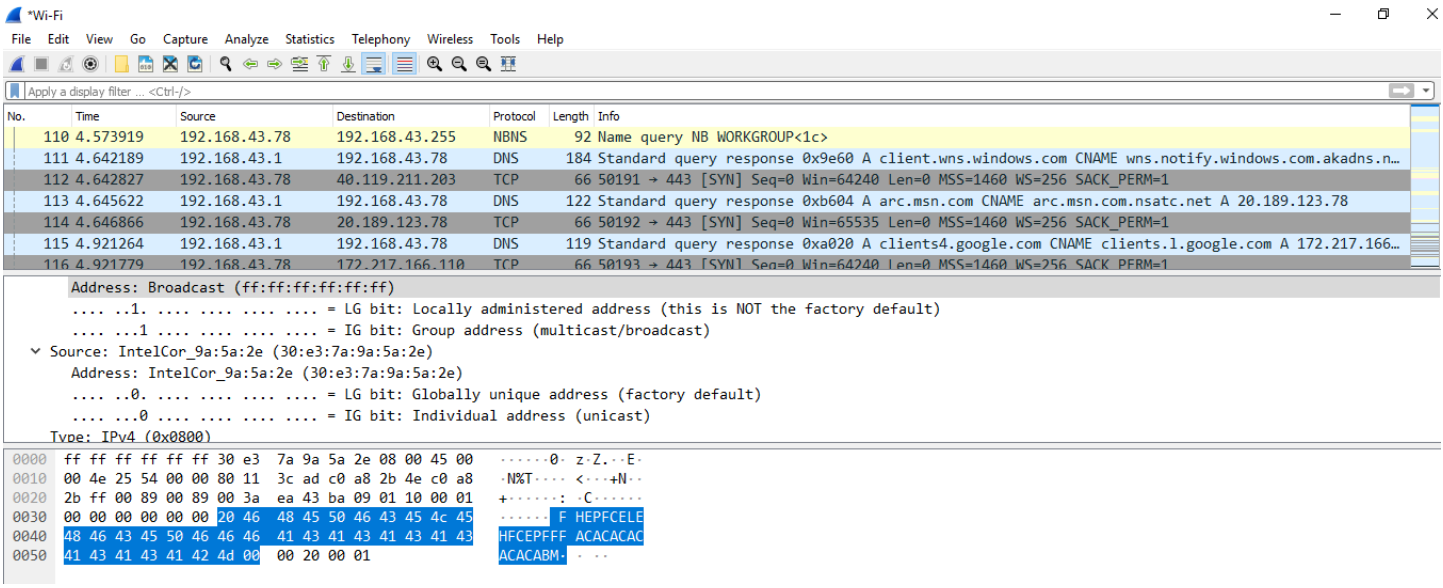


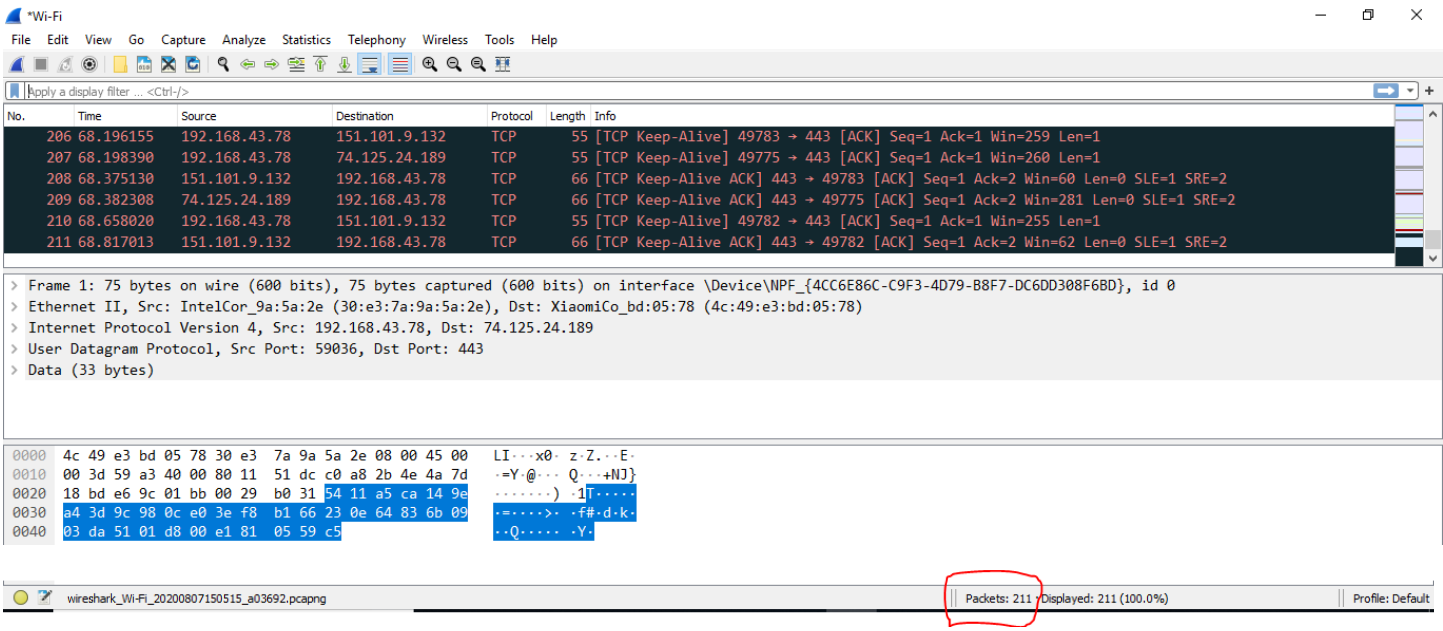
If we click the red marked option we will see the Capture Interface





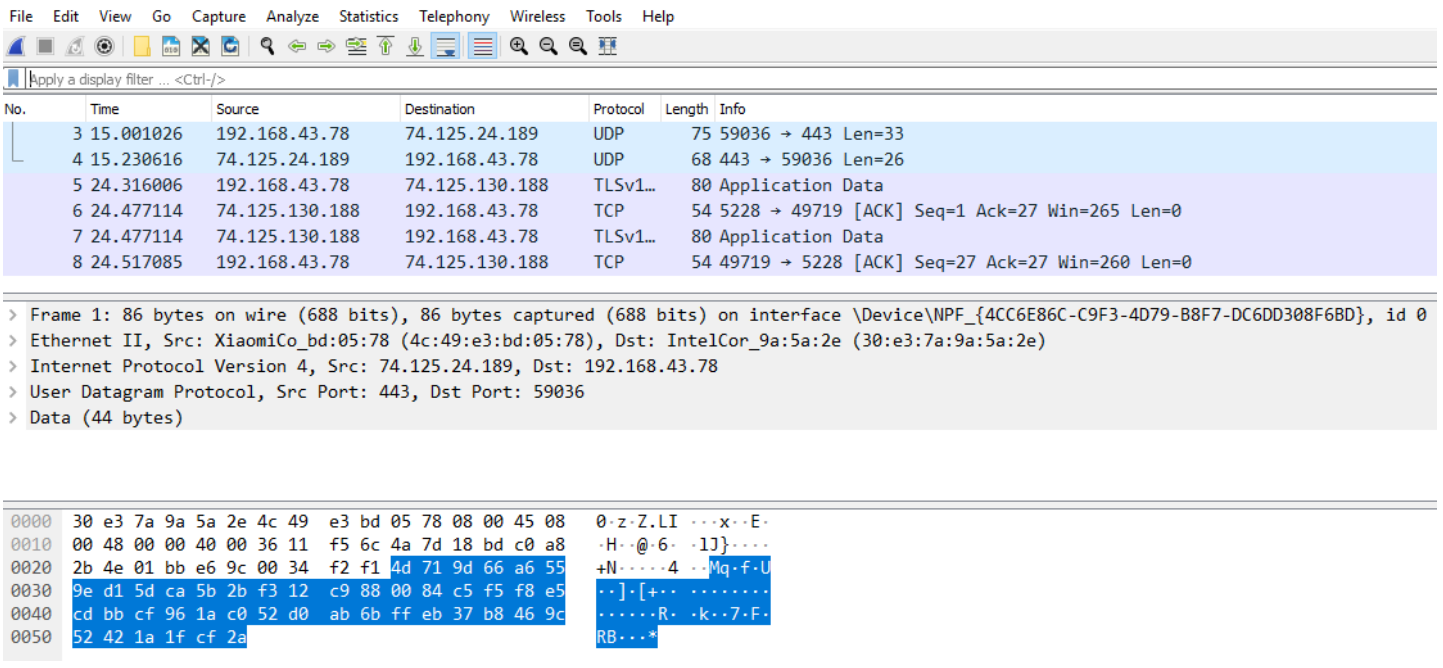
If we click the yellow highlighted portion(Wi-Fi) then we will see the below figure.



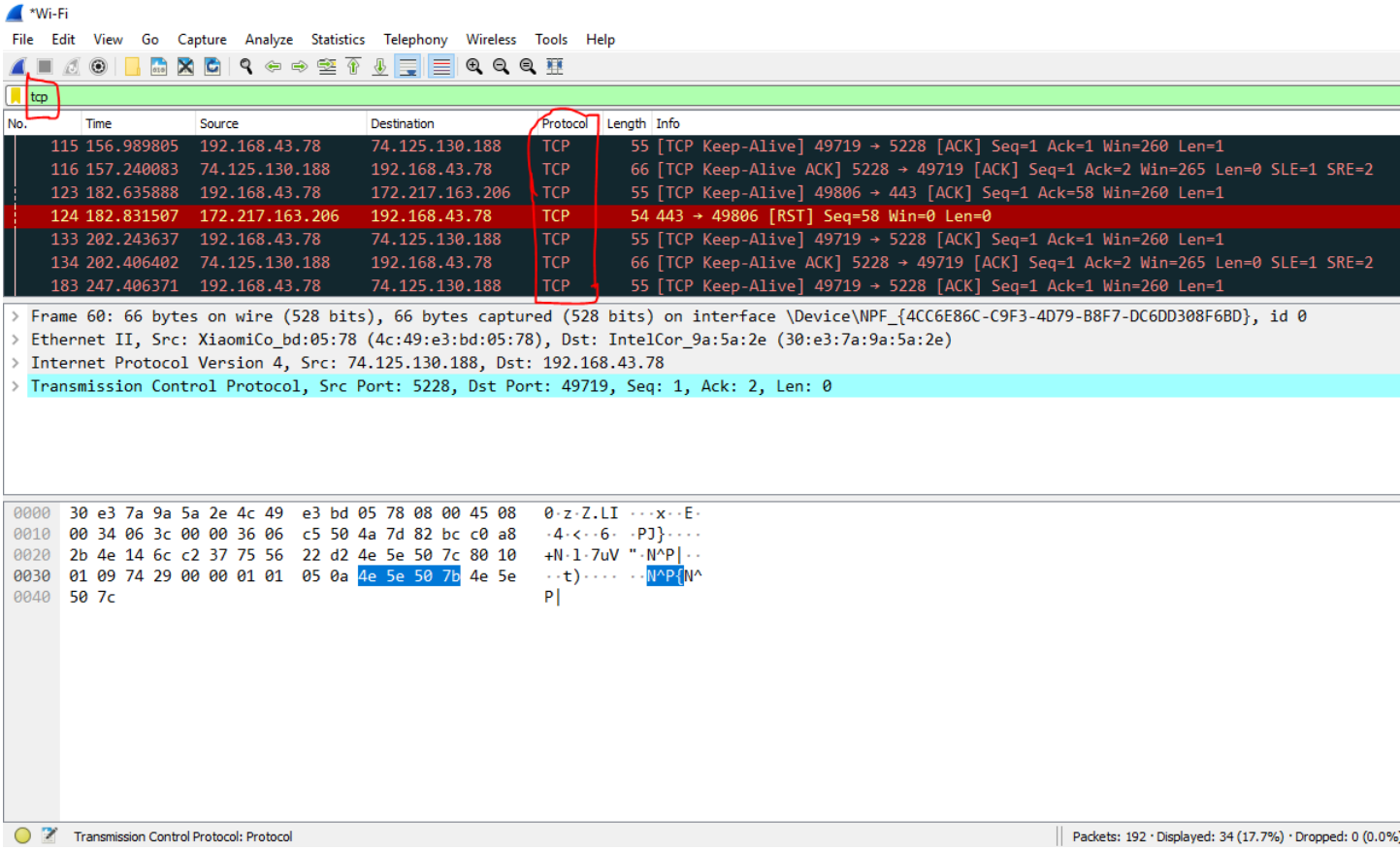


Here the total number of packets is 211.

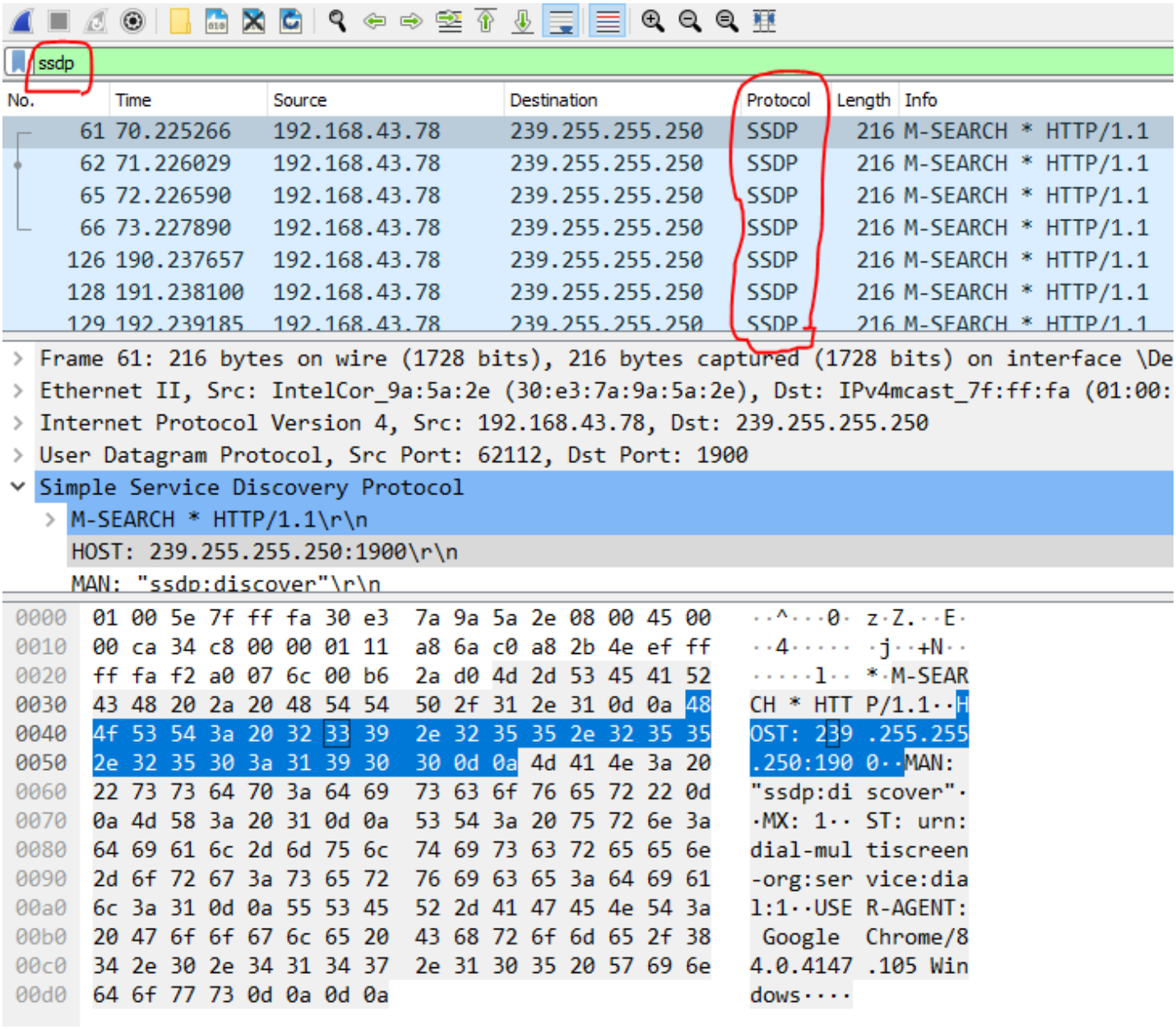
List of Captured packet:



TCP packet capture:



SSDP packet capture:



UDP packet capture: