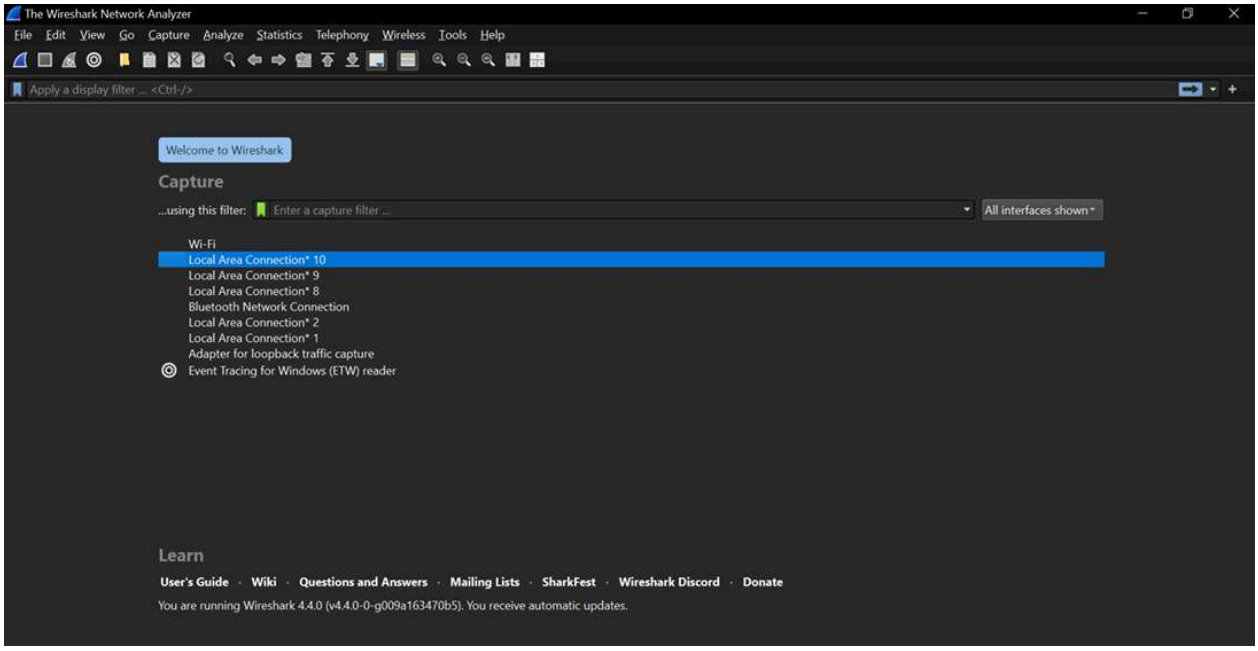
Name: Atharva Patil Div: D15C Roll No: 39

CNS Lab Experiment 8

AIM: Study of packet sniffer tools Wireshark
Theory:
Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible. You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable.
In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

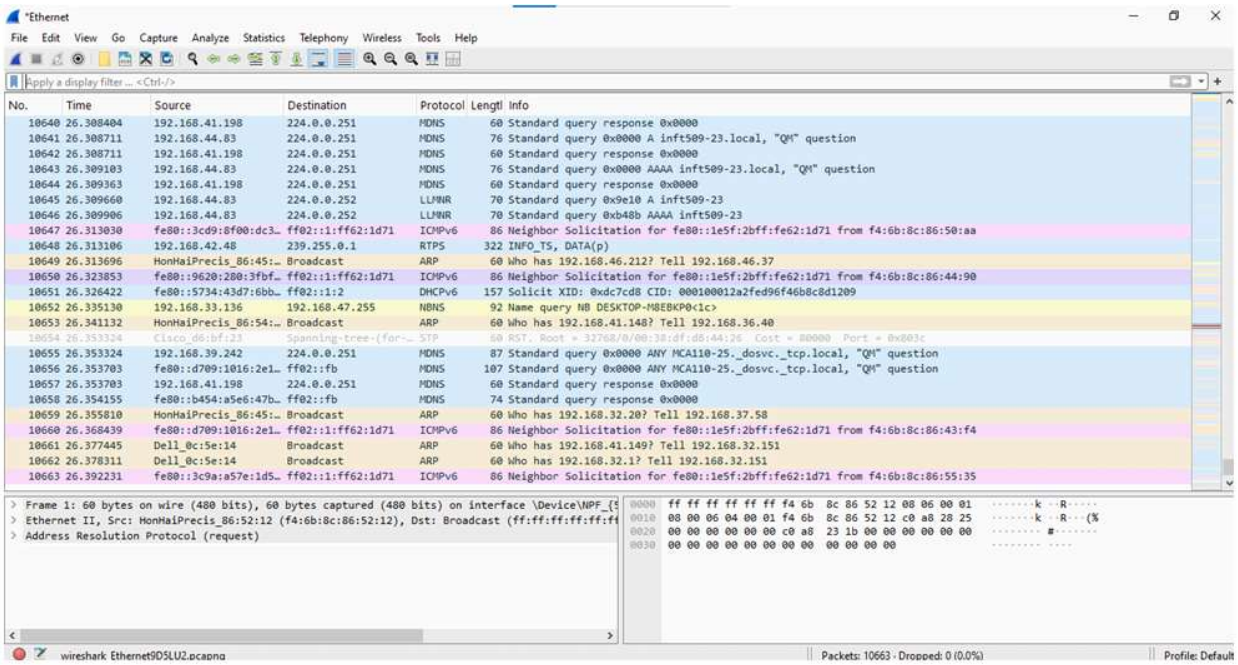
Applications of wireshark :
- Network administrators use it to troubleshoot network problems
- Network security engineers use it to examine security problems
- QA engineers use it to verify network applications
- Developers use it to debu g protocol implementations
- People use it to learn network protocol internals



a. Observe performance in promiscuous as well as non-promiscuous mode.

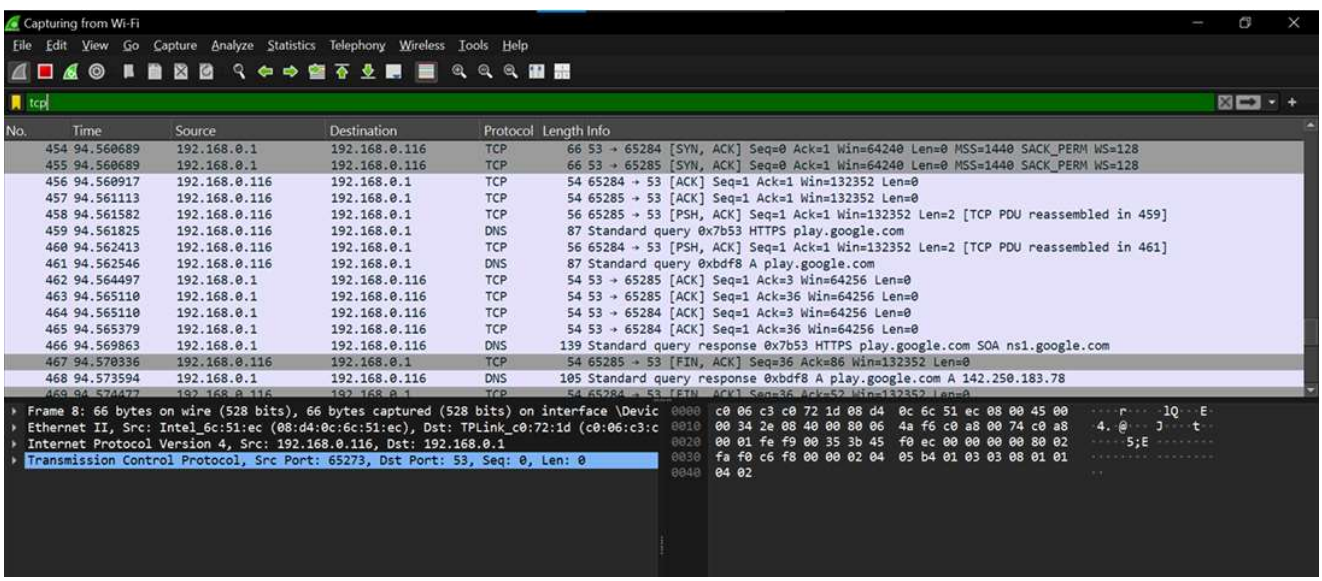
Name: Atharva Patil Div: D15C Roll No: 39

- Promiscuous mode



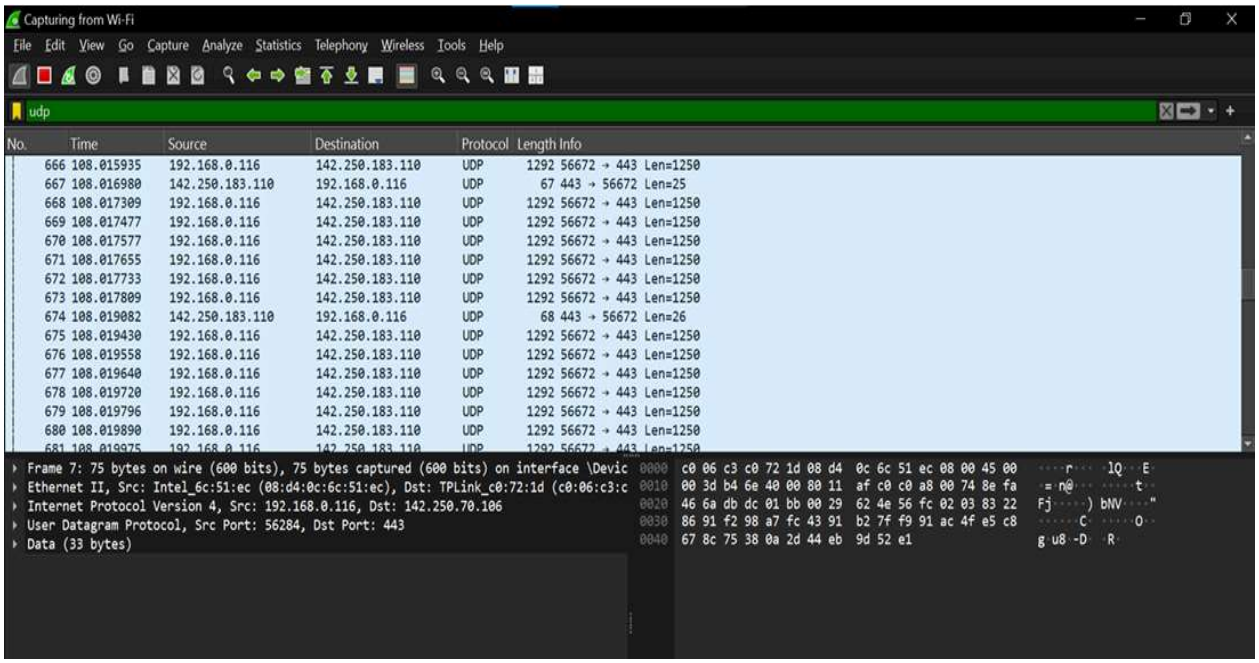
Applying filters in promiscuous mode:

- TCP

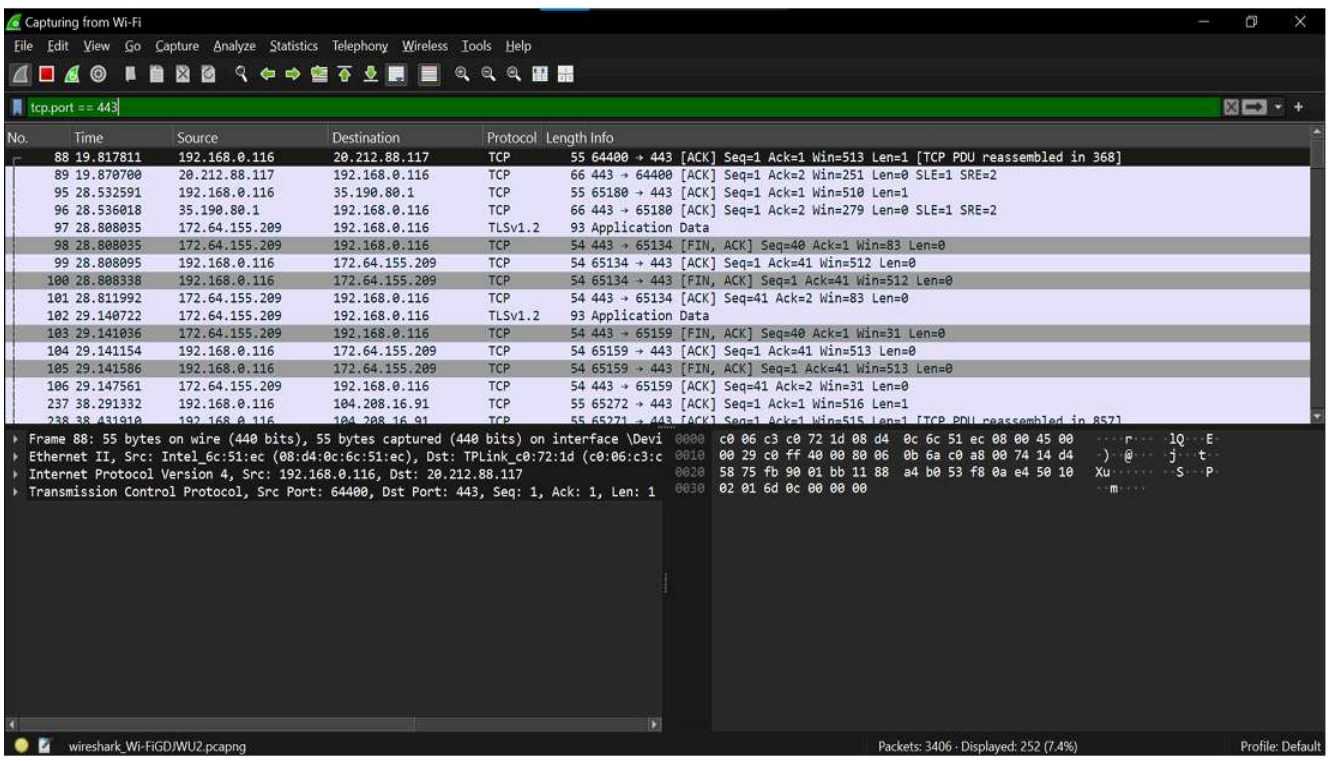


Name: Atharva Patil Div: D15C Roll No: 39

- UDP

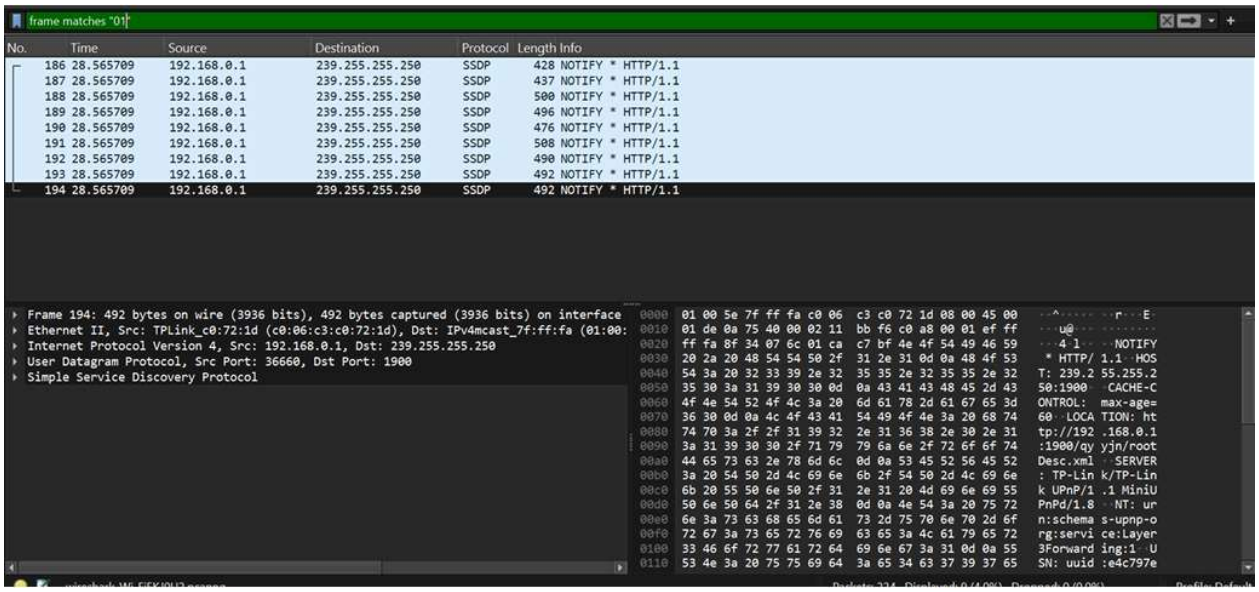


- Port

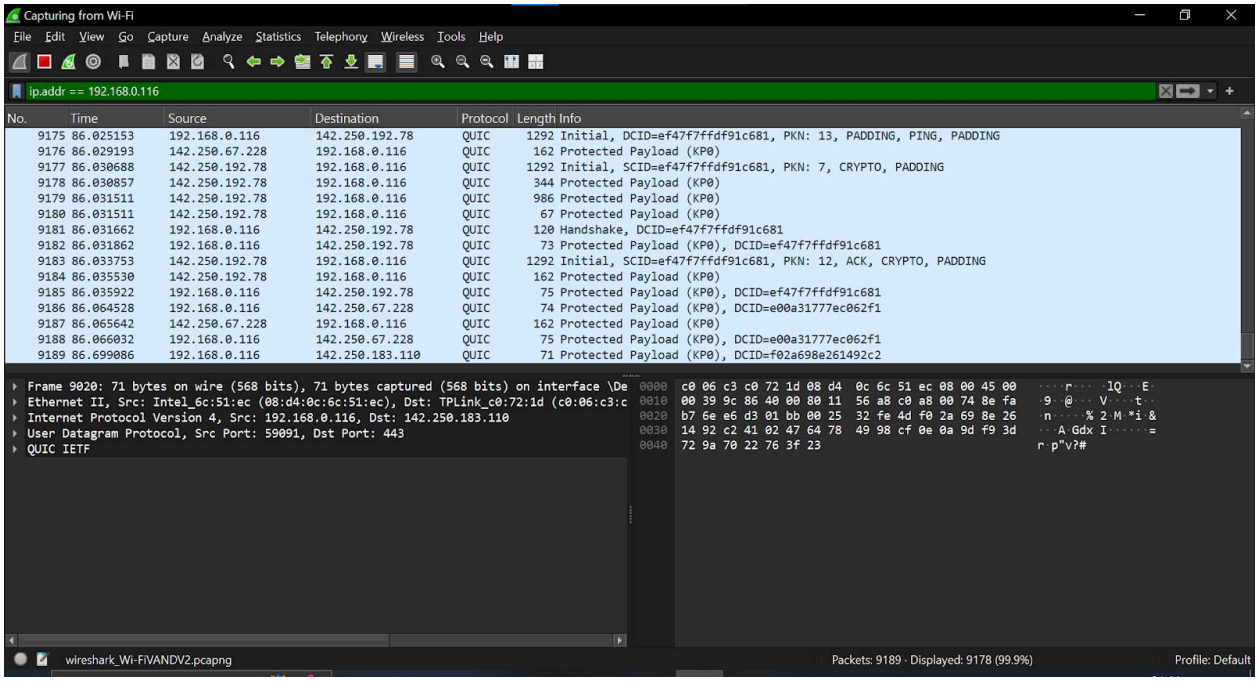


Name: Atharva Patil Div: D15C Roll No: 39

- Frame Matches

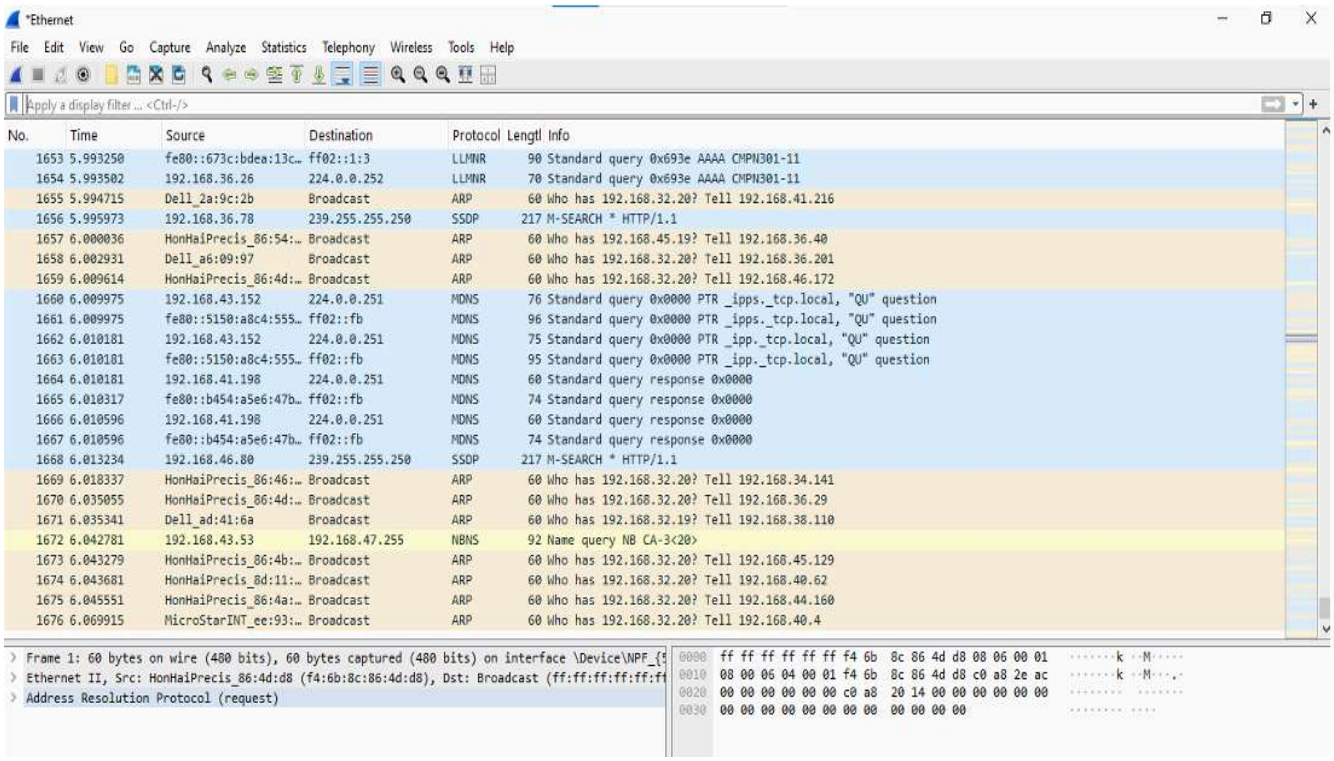


Filter: ip.addr == 192.168.0.4



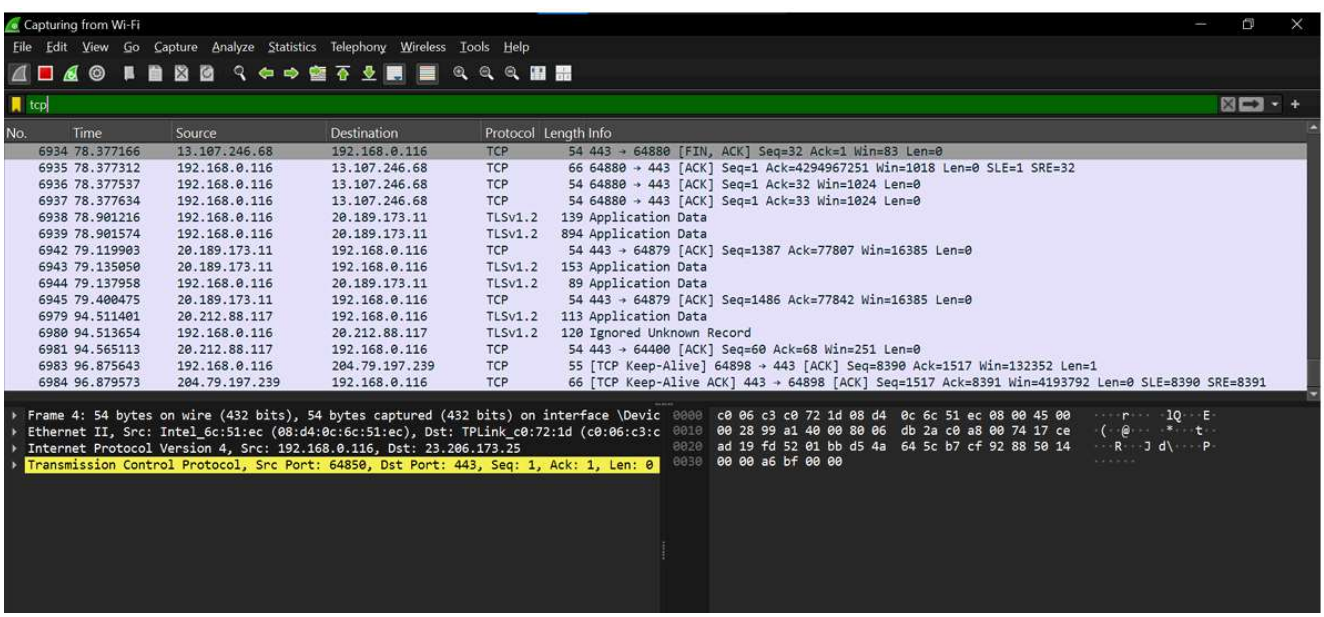
Name: Atharva Patil Div: D15C Roll No: 39

- Non-Promiscuous mode



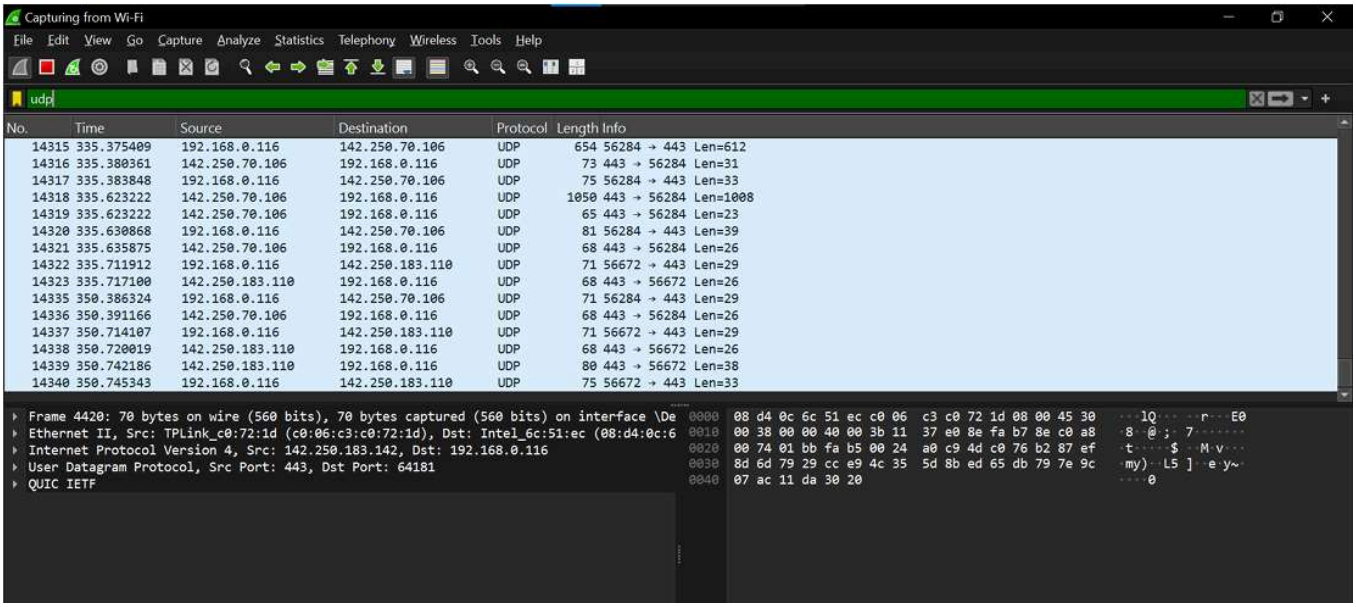
Applying filters in non promiscuous mode:

- TCP

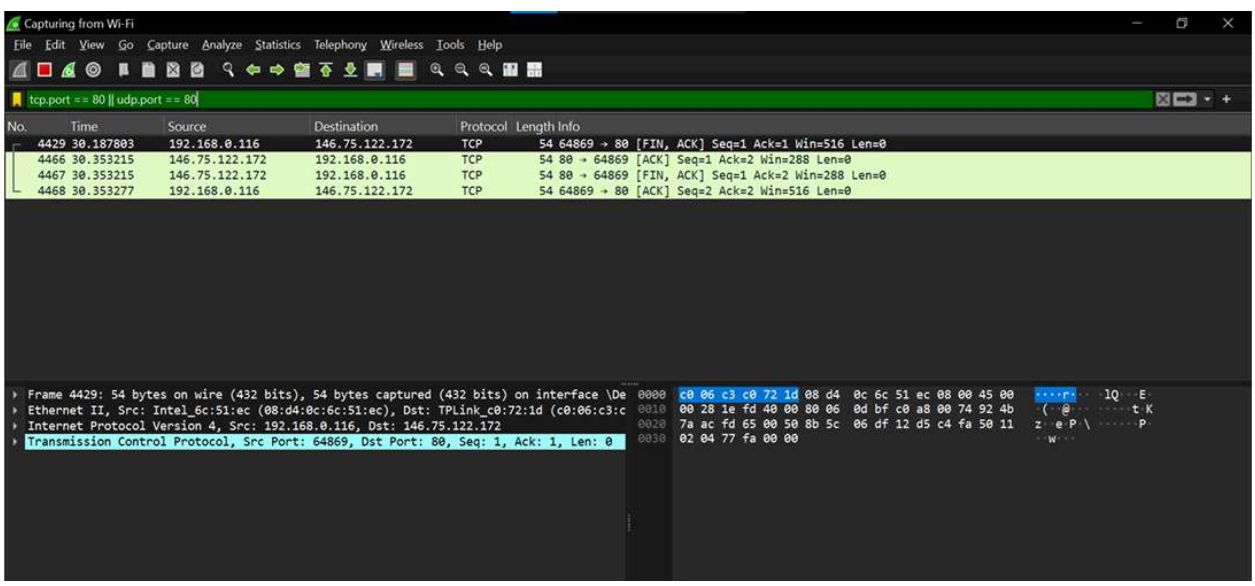


Name: Atharva Patil Div: D15C Roll No: 39

- UDP

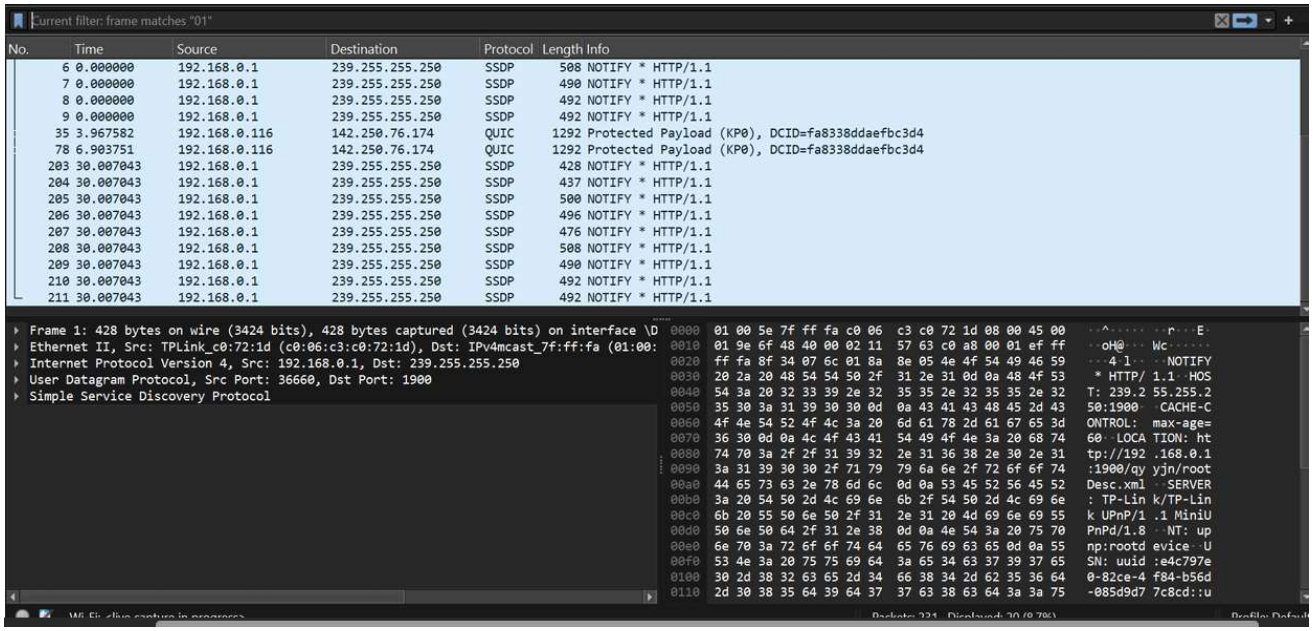


- Port

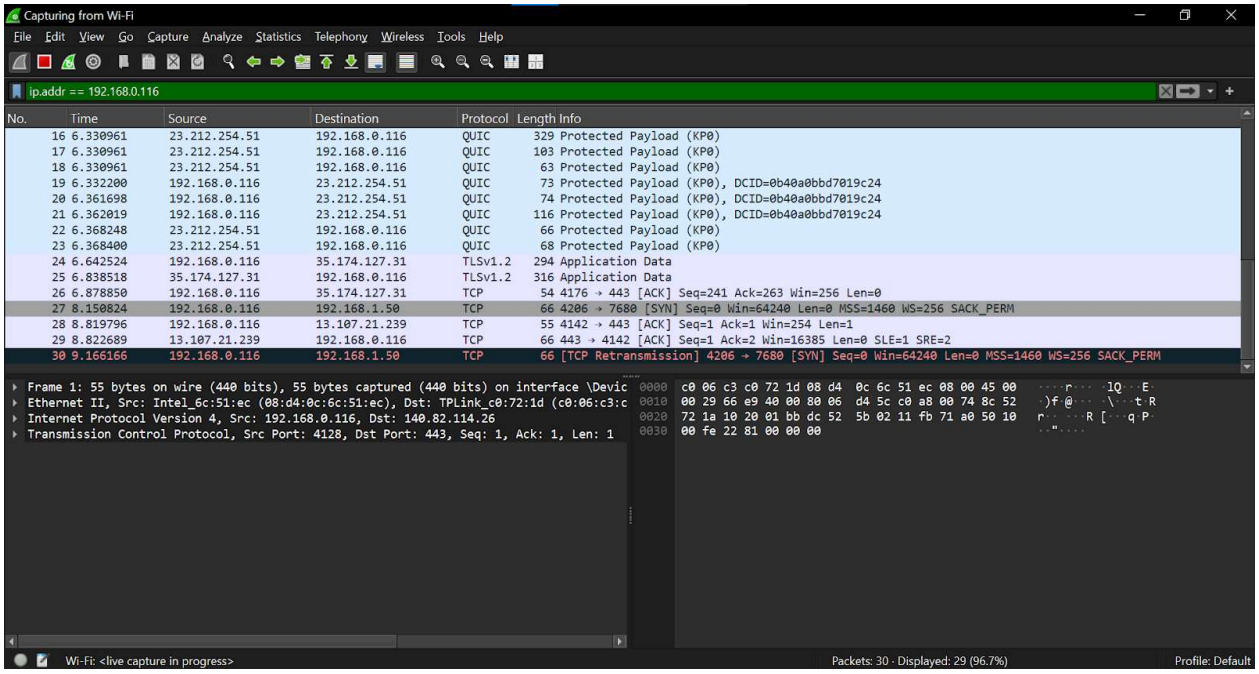


Name: Atharva Patil Div: D15C Roll No: 39

- Frame Matches



Filter: ip.addr == 192.168.0.4



Conclusion: Thus, by performing this experiment, we have studied and implemented packet sniffing tool Wireshark