Aditya Lalwani D15C 30 2024-25

Aim: Study of packet sniffer tools Wireshark: -

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

b. Show the packets can be traced based on different filters

Theory:

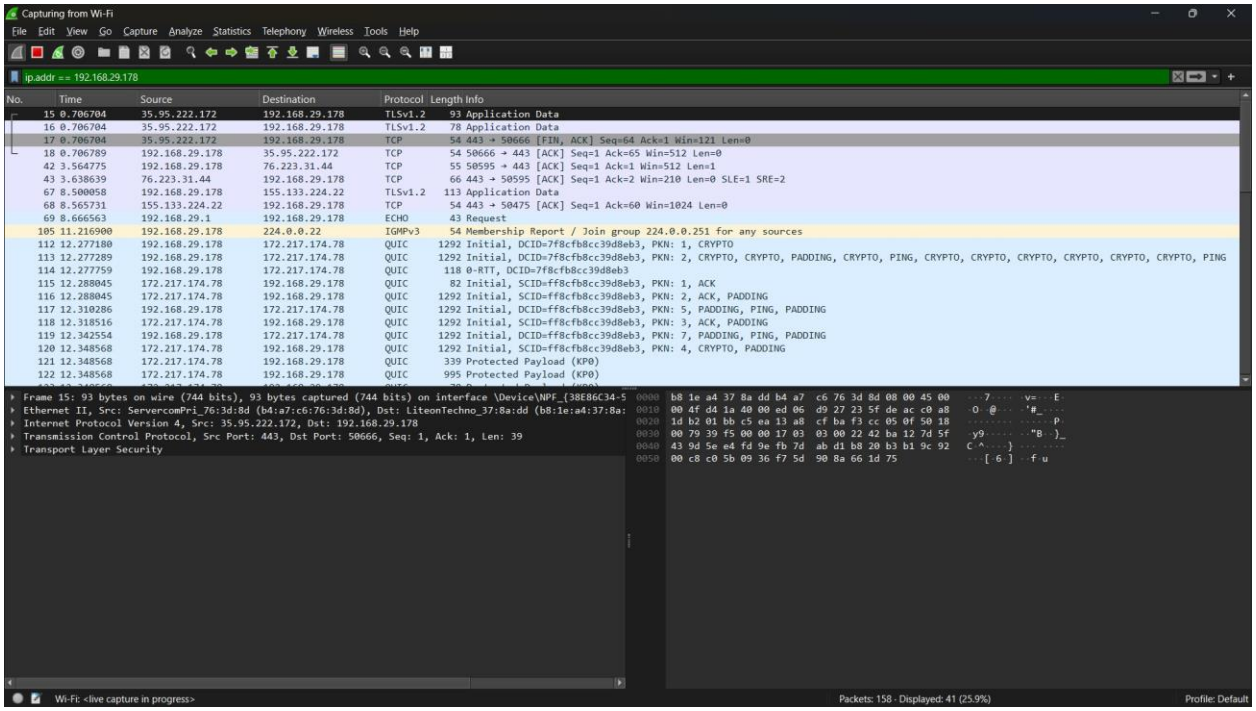
Wireshark is a powerful network packet analyzer that provides detailed insights into captured packet data. Think of it as a diagnostic tool for networks, similar to how an electrician uses a voltmeter to analyze electrical cables—only Wireshark operates at a higher level within network traffic.

Historically, such tools were expensive and proprietary, but Wireshark has transformed the landscape. It is open-source, free to use, and widely regarded as one of the best packet analyzers available today.

Applications of Wireshark:

- Network administrators troubleshoot network issues.
- Network security engineers analyze security concerns.
- QA engineers validate network applications.
- Developers debug protocol implementations.
- Learners study network protocol internals.

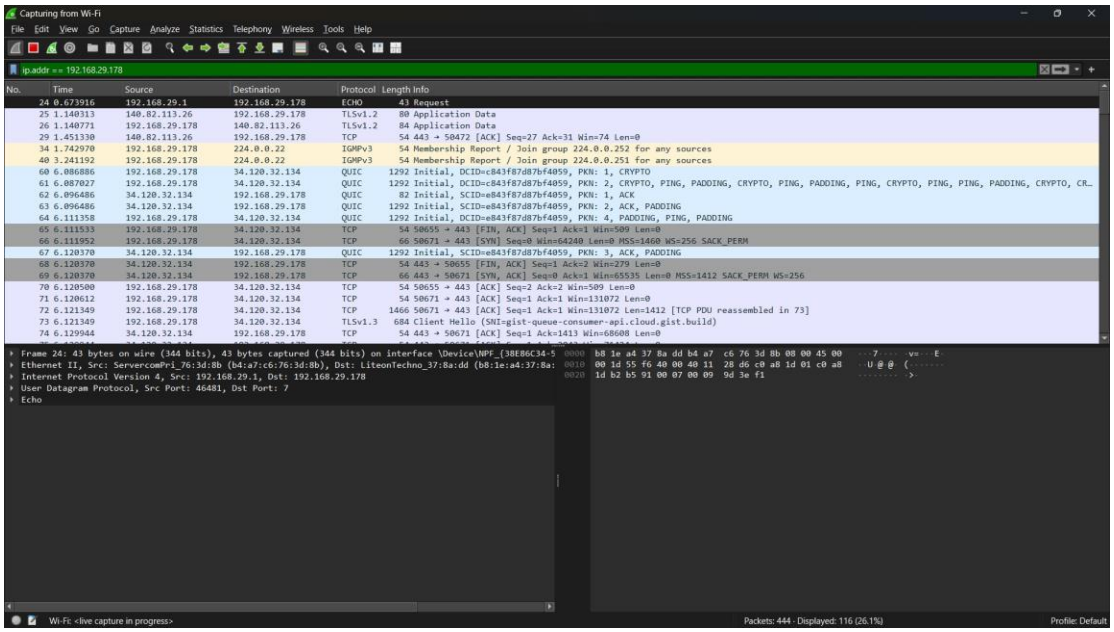
Output:



Aditya Lalwani D15C 30 2024-25

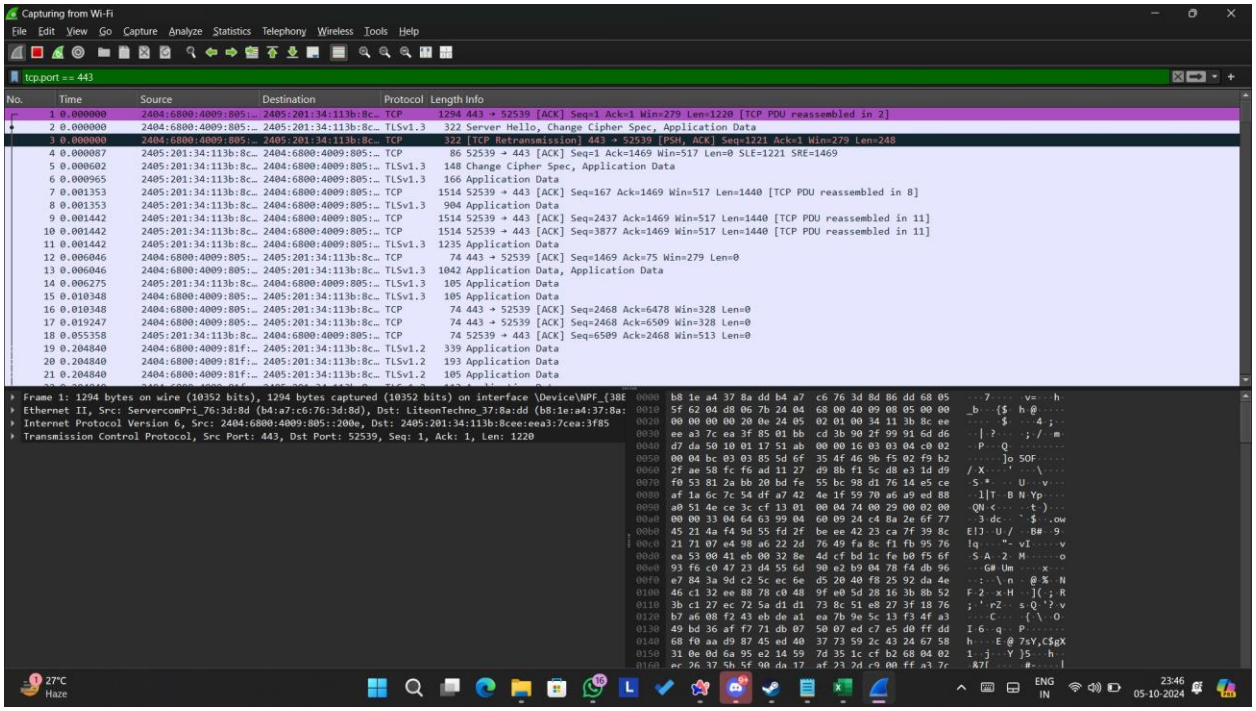
1) Filter: IP Address

- Promiscuous off
- Promiscuous on

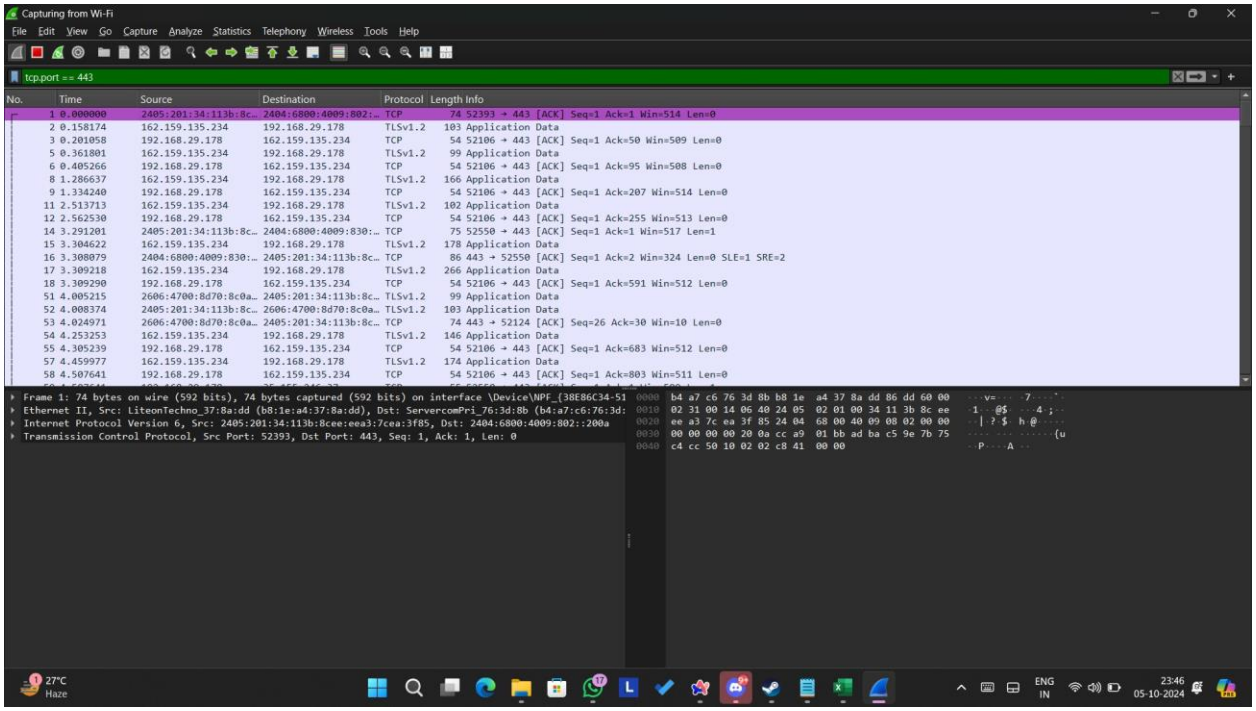


2) Filter: Port number

- Promiscuous off



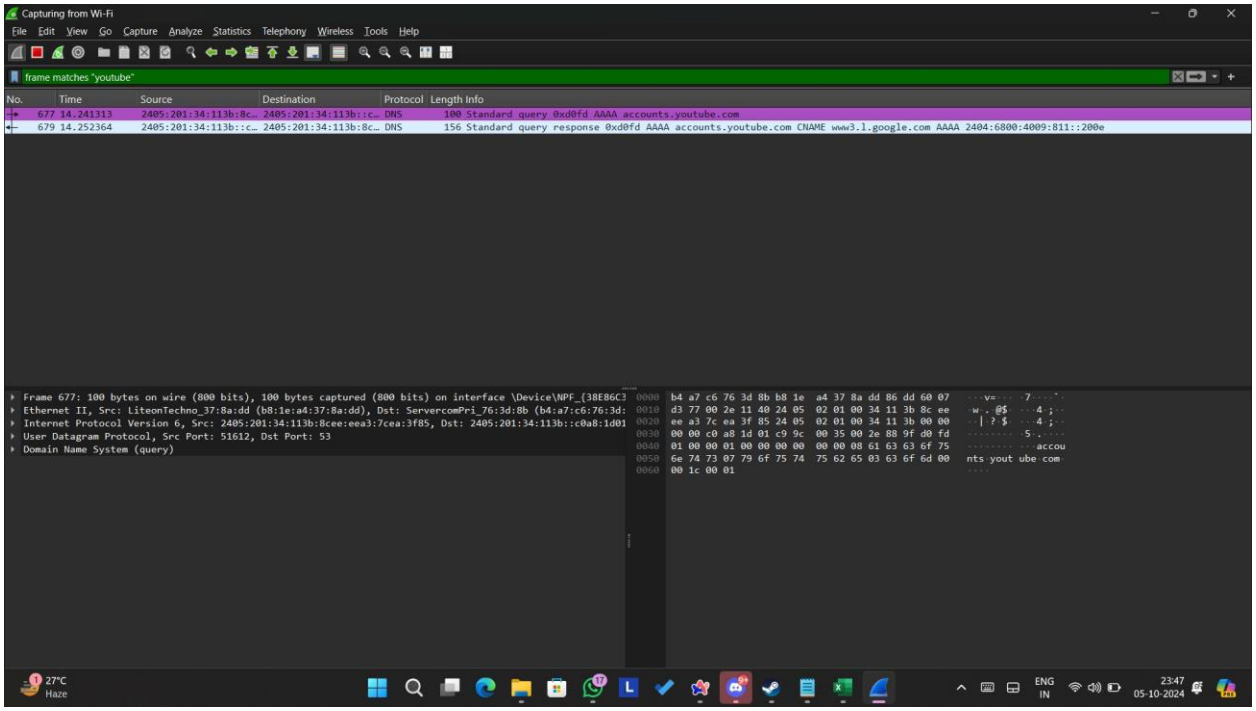
- Promiscuous on



3) Filter: String matching

- Promiscuous off

Aditya Lalwani D15C 30 2024-25



- Promiscuous on