Experiment 08

Study of packet sniffer tools Wireshark - a. Observer performance in promiscuous and non-promiscuous modes. b. Show the packets can be traced based on different filters.

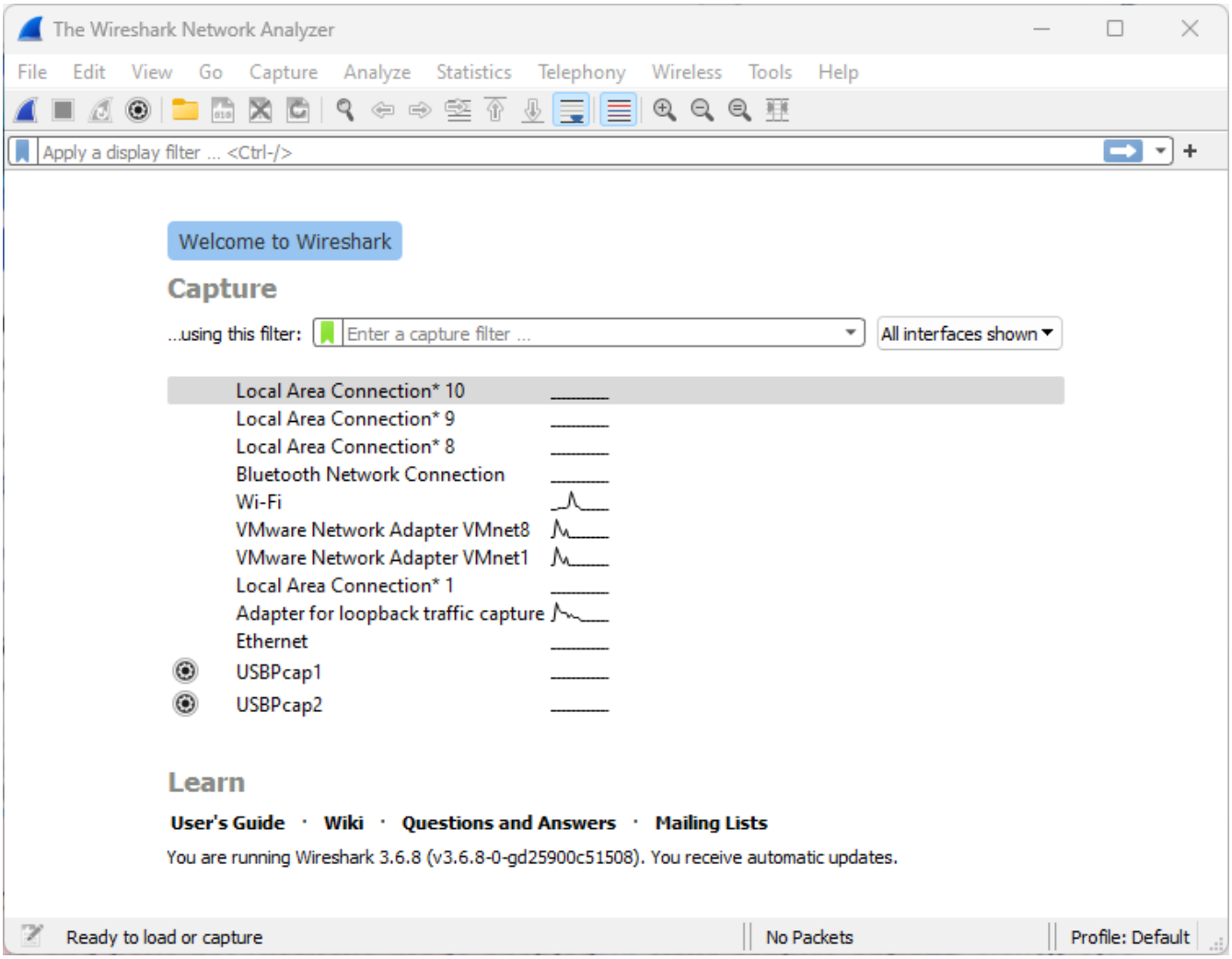
Roll No.	37
Name	Mikil Lalwani
Class	D15-B
Subject	Security Lab
LO Mapped	LO3: Explore the different network reconnaissance tools to gather information about networks

Aim:

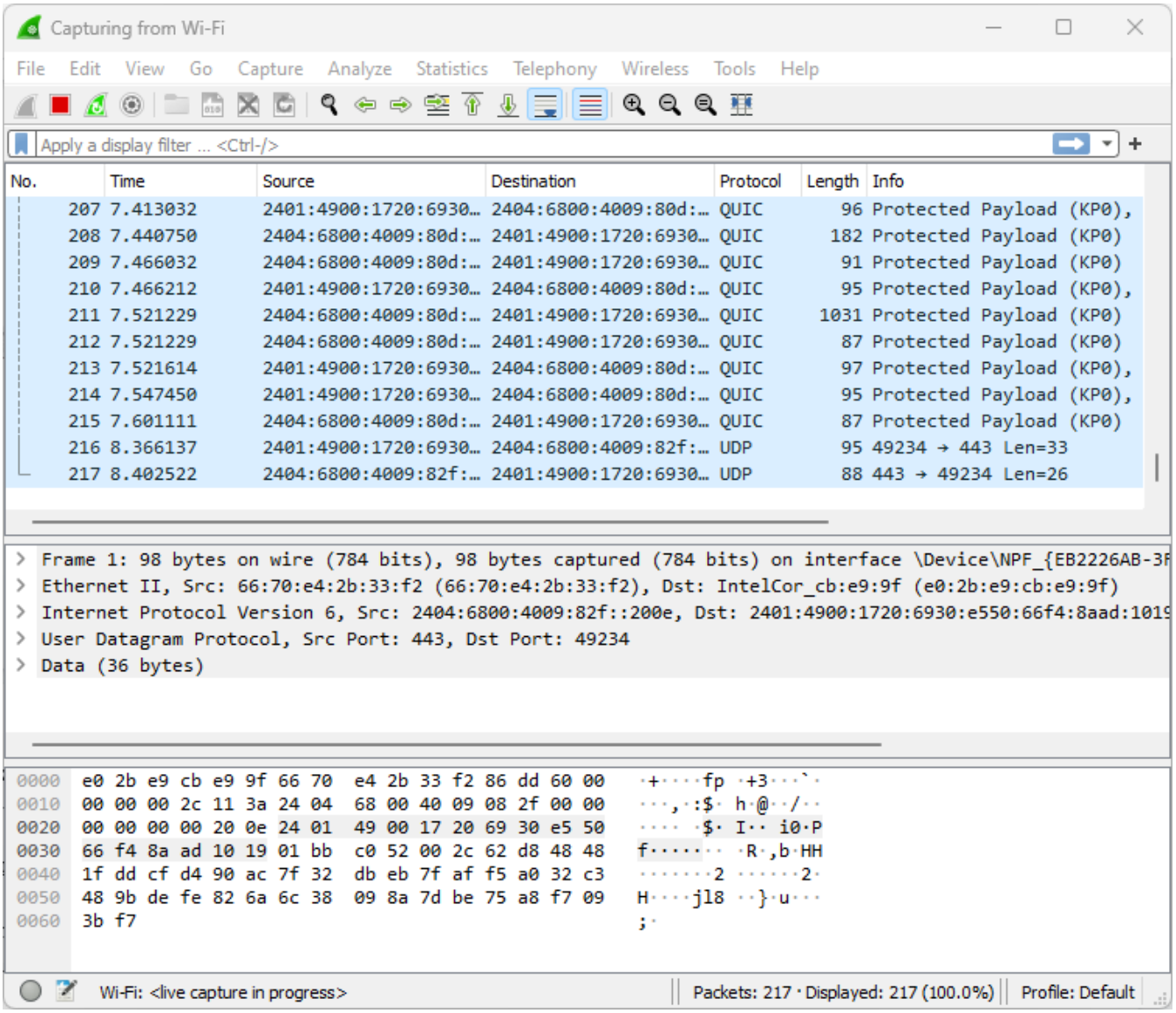
Study of packet sniffer tools Wireshark: -
a. Observer performance in promiscuous as well as non-promiscuous mode.
b. Show the packets can be traced based on different filters.

Methods:

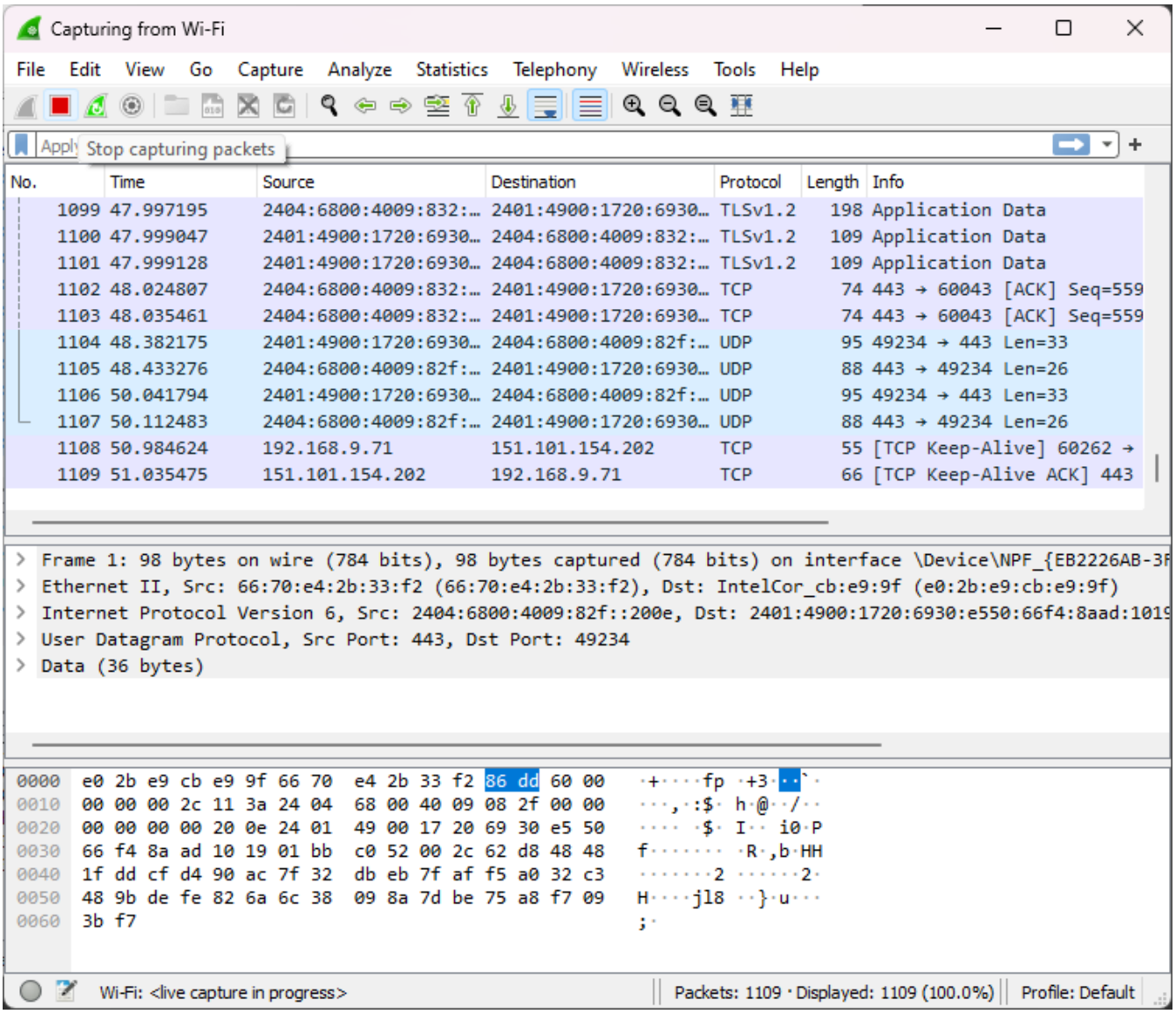
1. After downloading and installing Wireshark, you launch it and click the name of an interface under the interface list to start capturing packets on that interface. For example, if you want to capture traffic on the wireless network, you click your wireless interface. You can configure advanced features by clicking capture options.



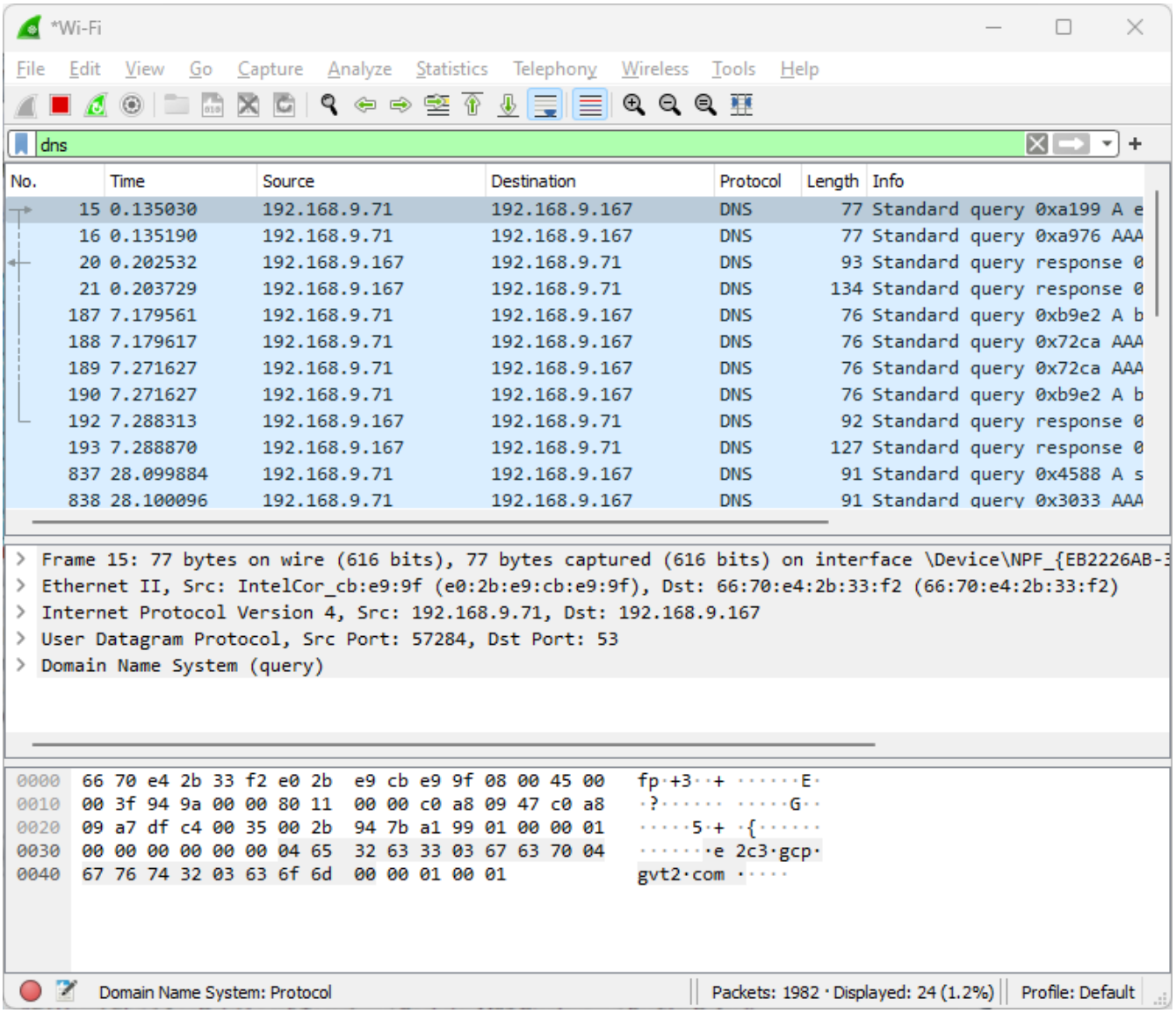
2. As soon as you click the interface's name, you'll see the packets start to appear in real-time. Wireshark captures each packet sent to or from your system. If you're capturing on a wireless interface and have promiscuous mode enabled in your capture options, you'll also see other packets on the network.



3. Click the stop capture button near the top left comer of the window when you want to stop capturing traffic.

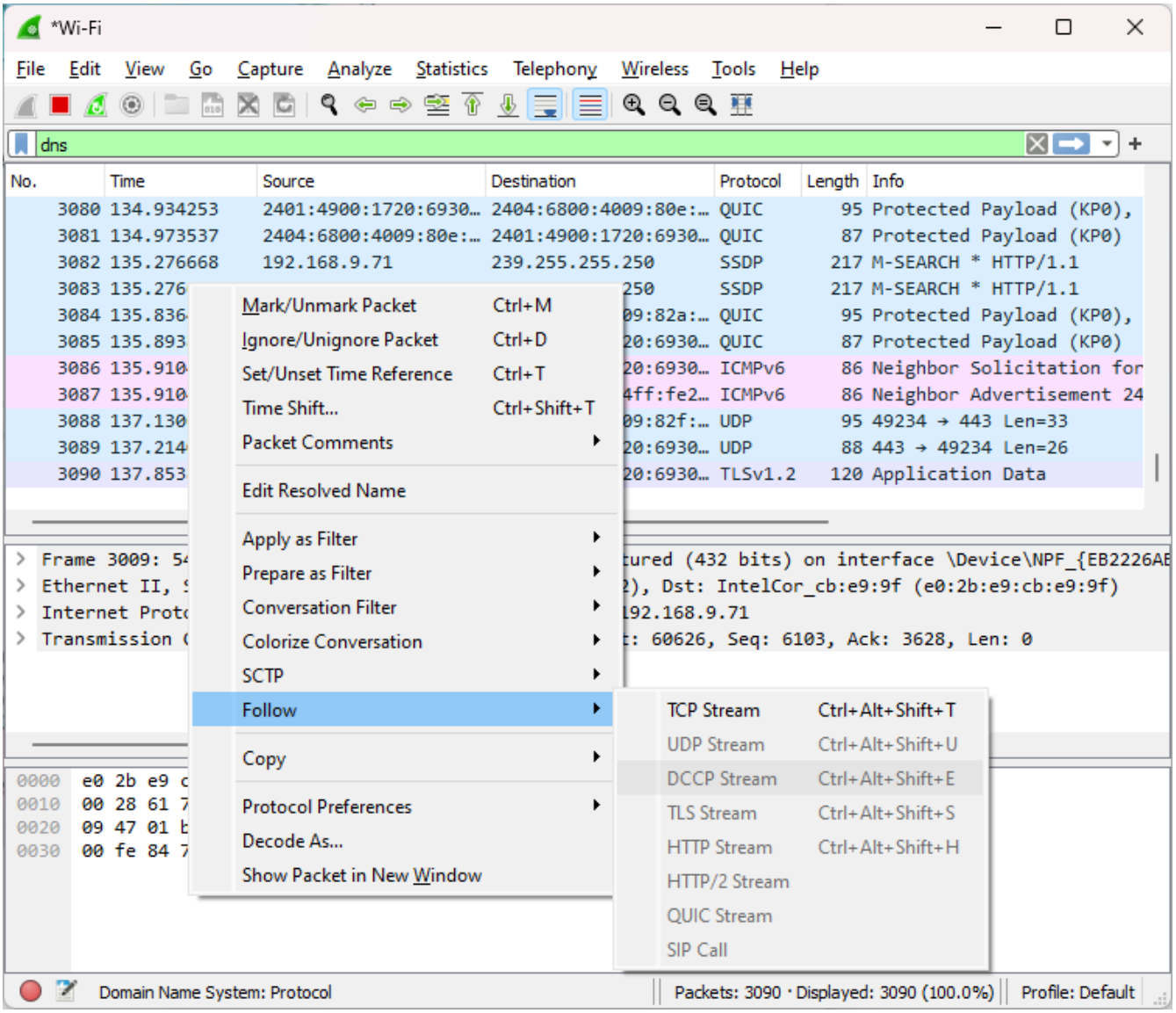


4. Wireshark uses colors to help you identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order.



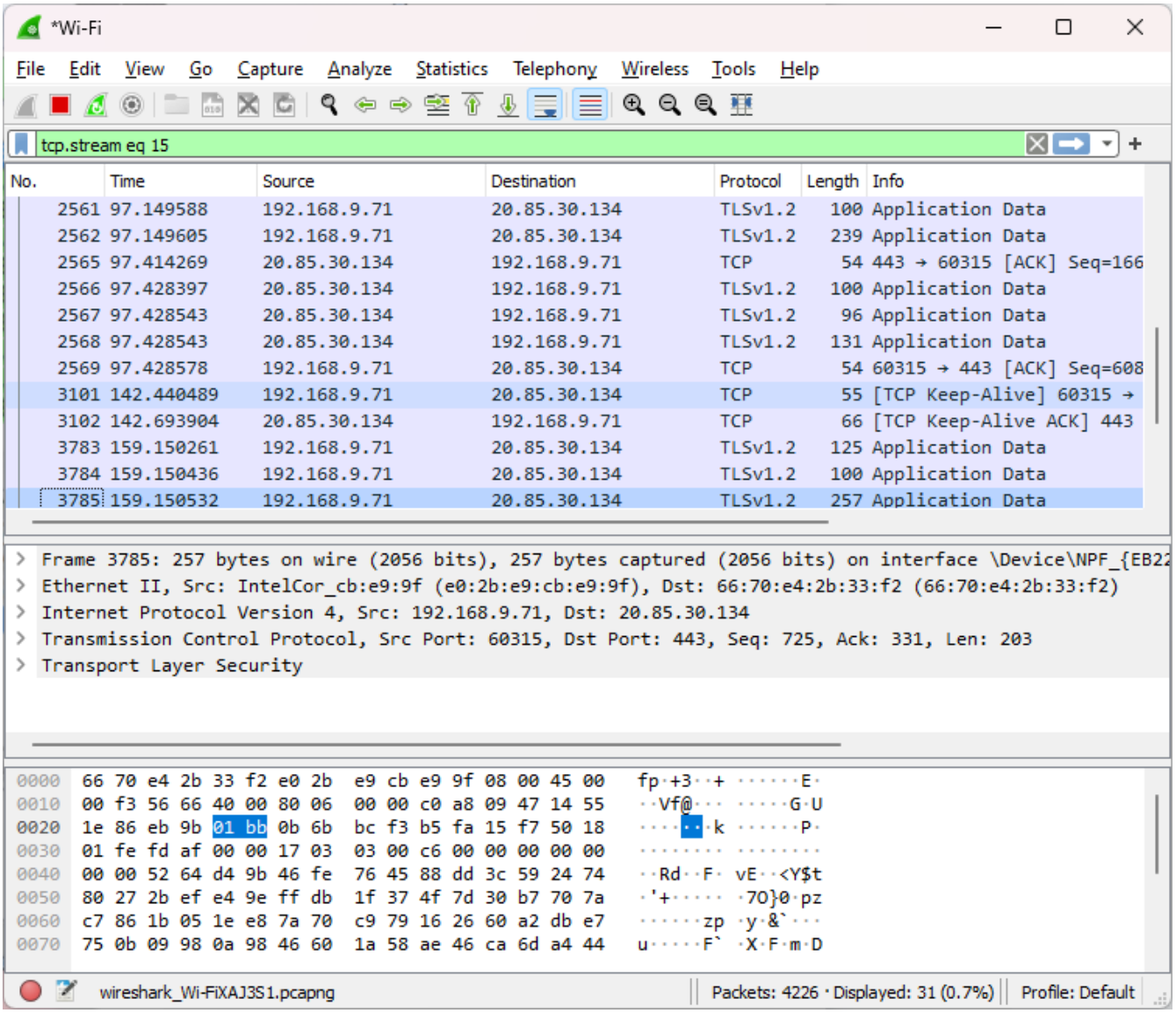
5. Filtering Packets If you're trying to inspect something specific, such as the traffic a program sends when phoning home, it helps to close down all other applications using the network so you can narrow down the traffic. Still, you'll likely have a large number of packets to sift through. That's where Wireshark's filters come in.
   The most basic way to apply a filter is by typing it into the filter box at the top of the window and clicking Apply (or pressing Enter). For example, type "DNS" and you'll see only DNS packets. When you start typing, Wireshark will help you autocomplete your filter.\

6. Another interesting thing you can do is right-click a packet and click on Follow TCP Stream.



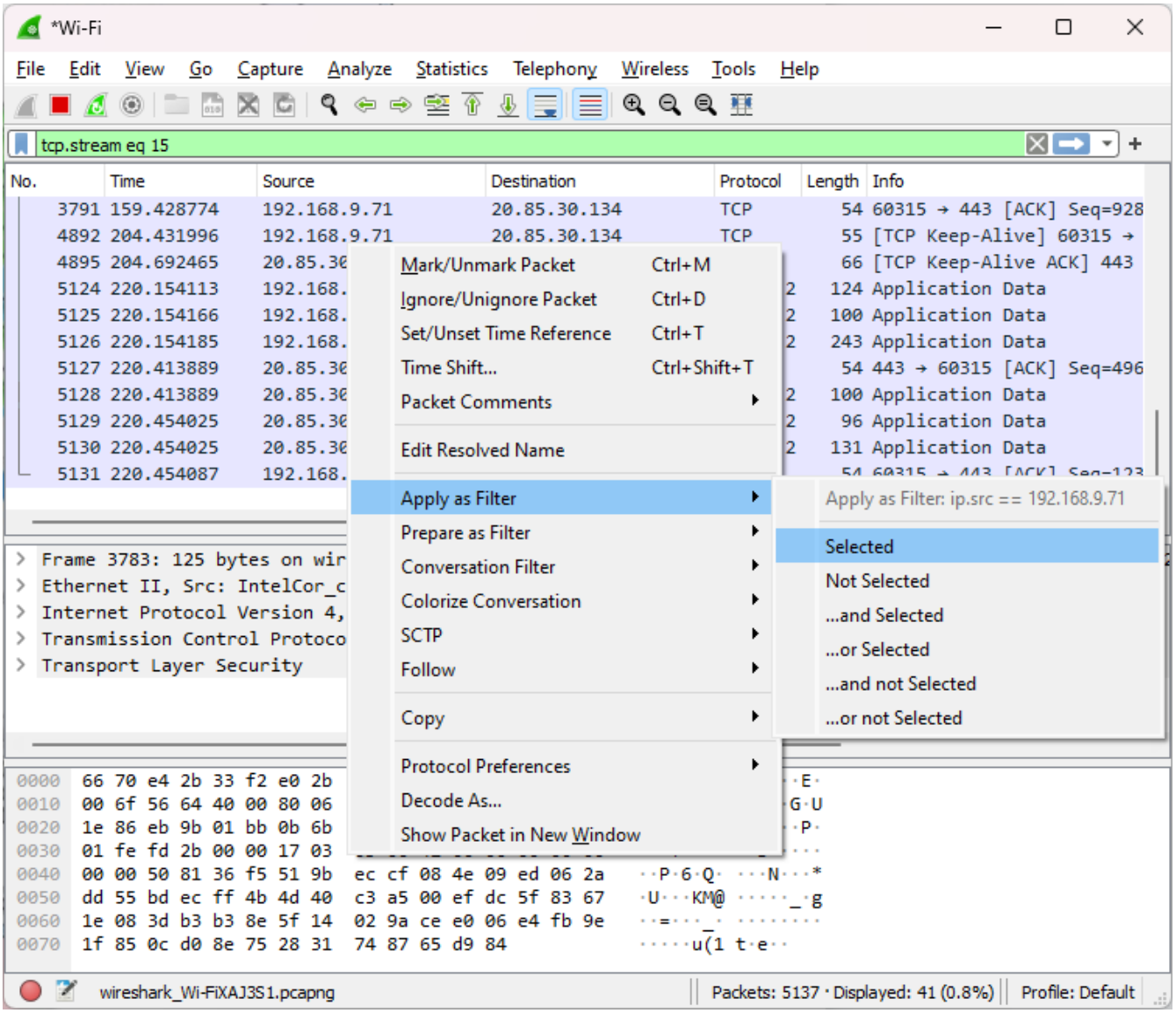
7. You can see full conversion between client and server.

8. Close the window and you can see a filter has been applied automatically. Wireshark is showing you the packets that make up the conversation.



9. Inspecting Packets

Click a packet to select it and you can dig down to view its details.



10. Wireshark is an extremely powerful tool, and this tutorial is just scratching the surface of what you can do with it. Professionals use it to debug network protocol implementations, examine security problems and inspect network protocol internals.

Conclusion:

In this experiment, we analyze various packet sniffing tools that monitor network traffic transmitted between legitimate users or in the network. The packet sniffer is a network monitoring tool. It has opted for network monitoring, traffic analysis, troubleshooting, Packet gripping, message, protocol analysis, penetration testing, and many other purposes.