PRACTICAL: 10

# AIM:

Approach to study Wireshark.

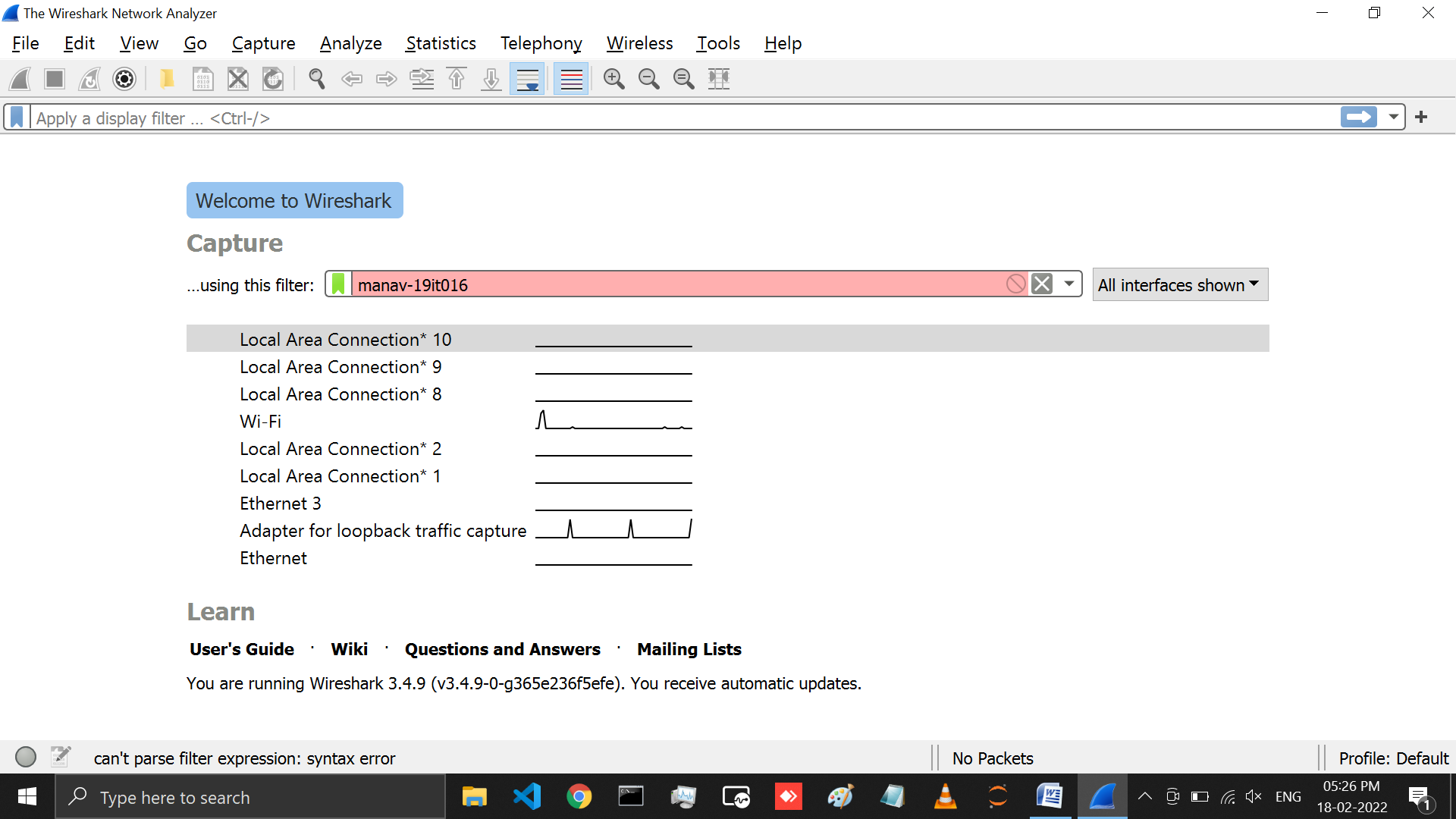
# THEORY:

Wireshark is the world’s foremost and widely-used network protocol analyzer. It lets you see what’s happening on your network at a microscopic level and is the de facto (and often danger) standard across many commercial and non-profit enterprises, government agencies, and educational institutions. Wireshark development thrives thanks to the volunteer contributions of networking experts around the globe and is the continuation of a project started by Gerald Combs in 1998.

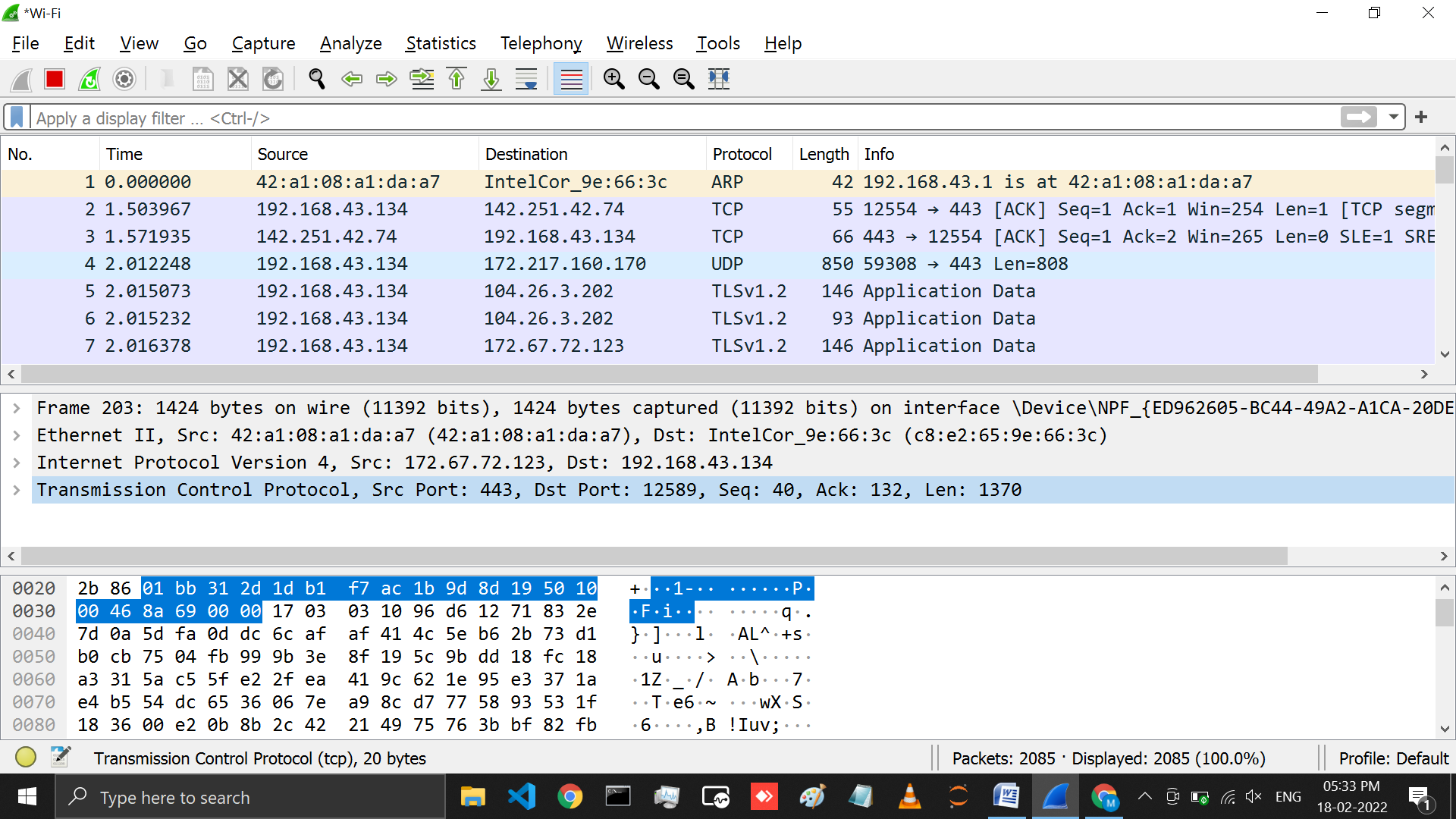
Wireshark is the most often-used packet sniffer in the world. Like any other packet sniffer, Wireshark does three things:

1. **Packet Capture:** Wireshark listens to a network connection in real time and then grabs entire streams of traffic – quite possibly tens of thousands of packets at a time.
2. **Filtering:** Wireshark is capable of slicing and dicing all of this random live data using filters. By applying a filter, you can obtain just the information you need to see.
3. **Visualization:** Wireshark, like any good packet sniffer, allows you to dive right into the very middle of a network packet. It also allows you to visualize entire conversations and network streams.

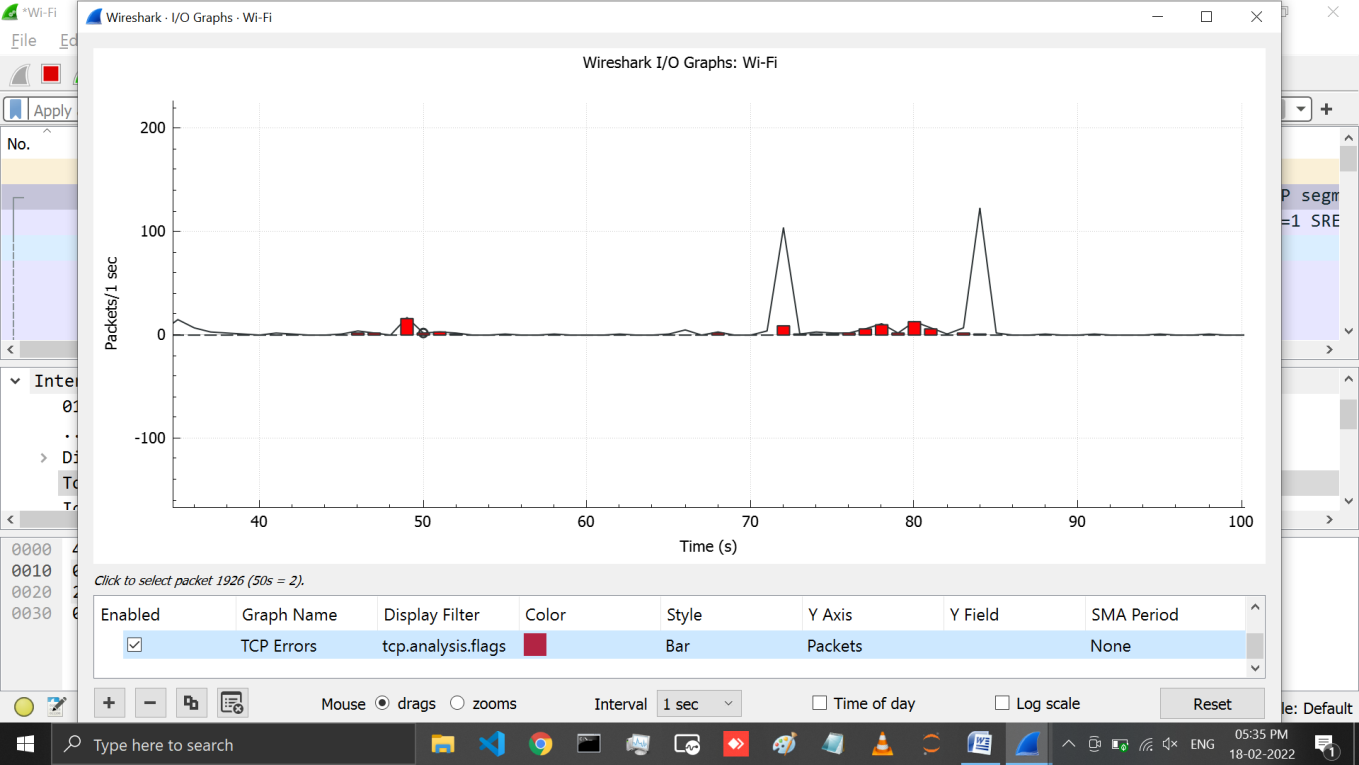
# OUTPUT:

****

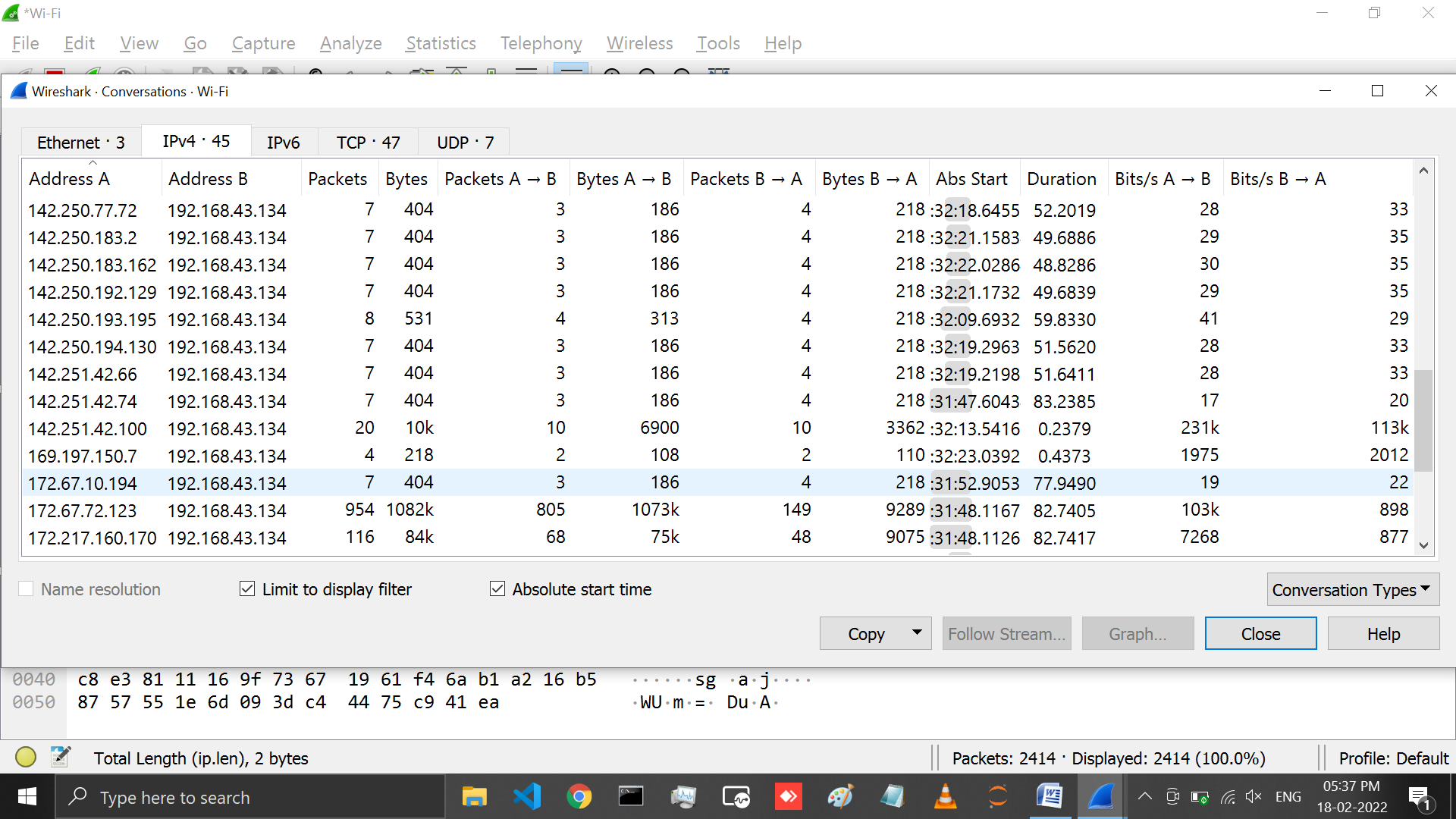
Above image represent the home page of the wireshark application on which different network interface are listed and beside them shows the graph of the activity going on (it is not sniffing). We can click on any of the network interface and can capture the traffic and start sniffing.



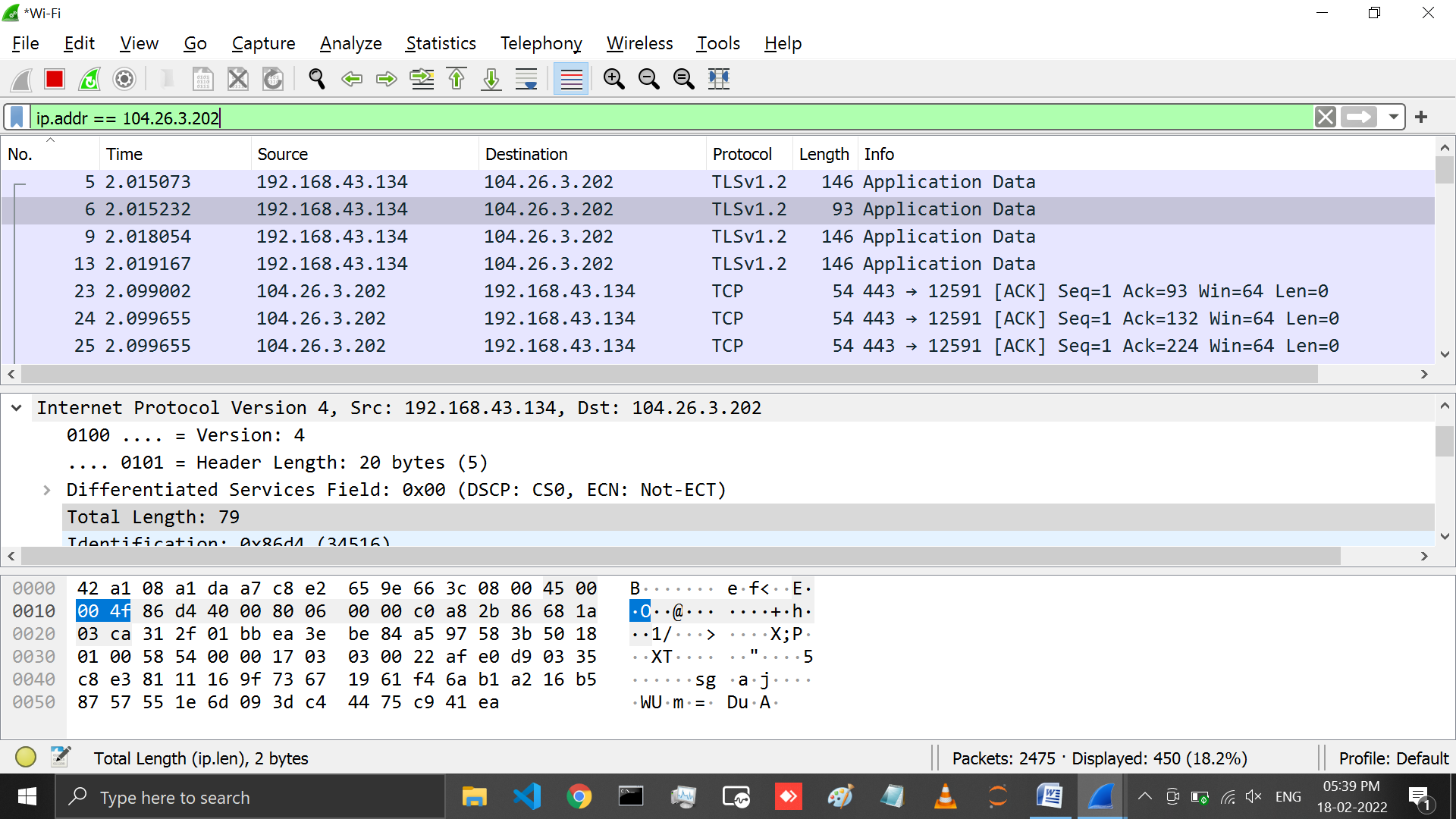
After clicking on any network interface wireshark will start capturing the packets, there are three sections in the window 1st section will show the list of the packet, 2nd section contains details such as the type of protocol used for that packet sender and receivers IP address, of the specific packet selected. And in 3rd section that the actual message that was received is shown in binary which is interpreted and shown in the 2nd section.



This particular graph is showing typical traffic generated by a laptop. The spikes in the graph are bursts of traffic. Many times, cyber security pros use Wireshark as a quick and dirty way to identify traffic bursts during attacks.

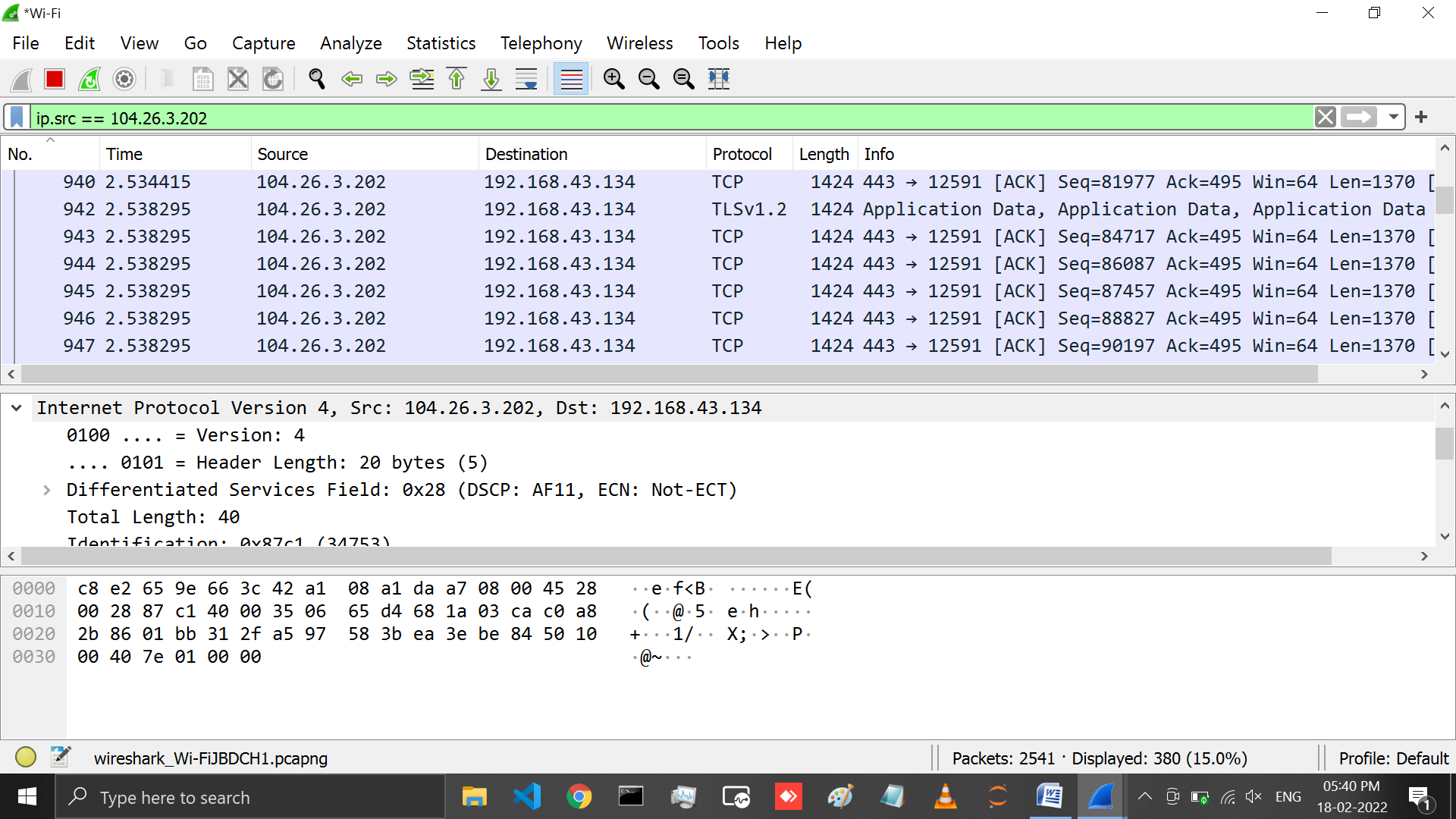


It’s also possible to capture the amount of traffic generated between one system and another. If you go to Statistics and then select Conversations, you will see a summary of conversations between end points.

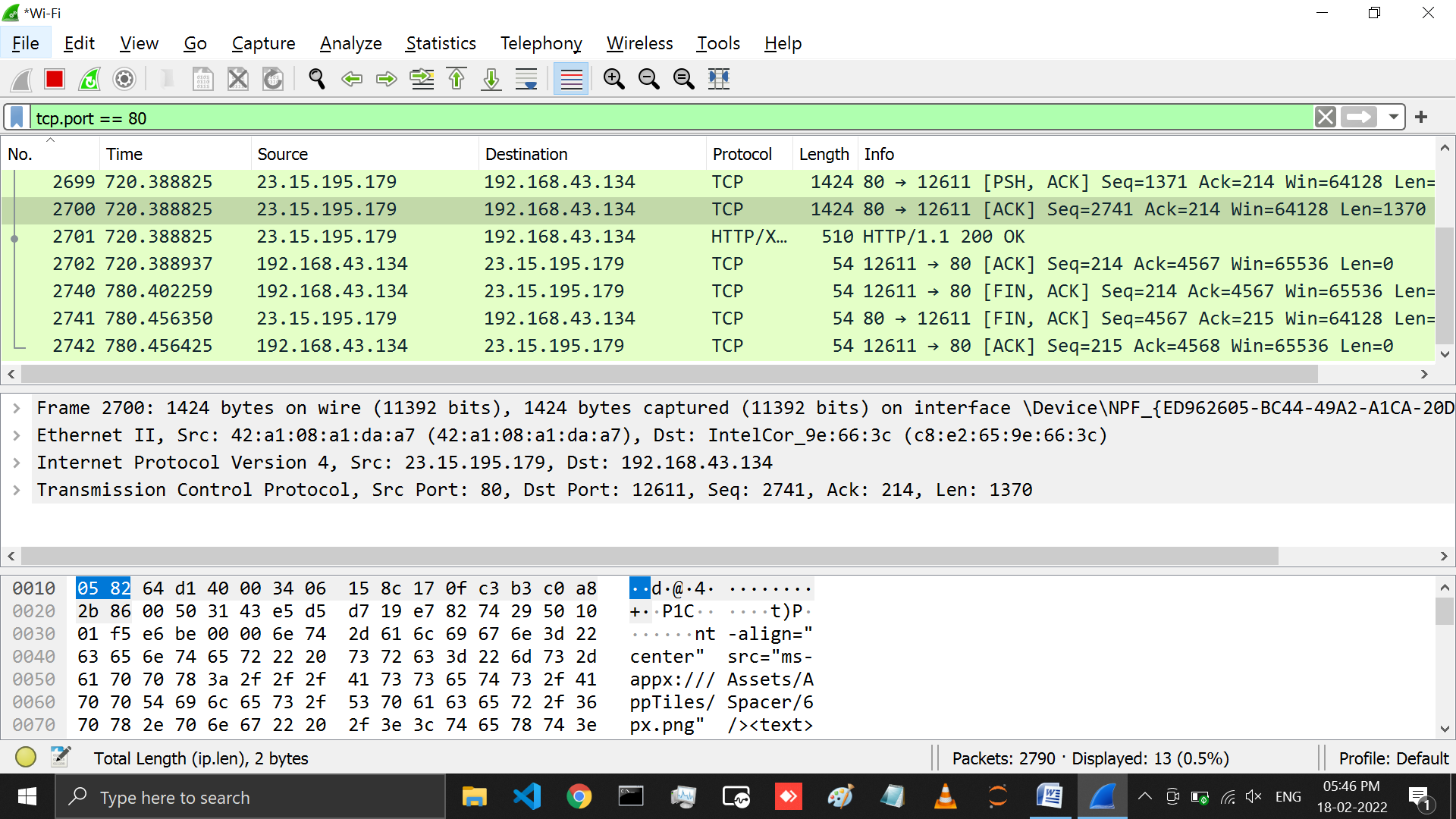


We can even filter the packets based on the IP address using the command ***“ip.addr == 104.26.3.202”***

this command will filter the packets which includes 104.26.3.202 as source or destination.



We can filter the packets based on the source destination as ***“ip.src == 104.26.3.202”*** and this will show the packets for which the source is ***104.26.3.202***



We can also filter the packets based on the TCP port number with the following command as

***“tcp.port == 80”*** which will filter the TCP port 80.

# LATEST APPLICATIONS

* Network administrators use it to troubleshoot network problems
* Network security engineers use it to examine security problems
* Developers use it to debug protocol implementations
* To learn network protocol internals
* Cybersecurity professionals often use Wireshark to trace connections, view the contents of suspect network transactions and identify bursts of network traffic.

# LEARNING OUTCOME:

with this practical learned about wireshark which is an open source tool for network traffic analyzer it is a tool which sniffs the network and gives the result as the list of packets. We can then analyze this packets and can identify if the network is behaving properly or not. This tools is also used by professionals to identify the attack in a network.

# REFERENCES:

1. [**https://www.wireshark.org/**](https://www.wireshark.org/)
2. [**https://www.wireshark.org/docs/**](https://www.wireshark.org/docs/)
3. [**https://www.wireshark.org/index.html#download**](https://www.wireshark.org/index.html#download)
4. [**https://www.youtube.com/watch?v=yC0e0bSSleo**](https://www.youtube.com/watch?v=yC0e0bSSleo)
5. [**https://www.comparitech.com/net-admin/wireshark-cheat-sheet/**](https://www.comparitech.com/net-admin/wireshark-cheat-sheet/)
6. [**https://www.stationx.net/wireshark-cheat-sheet/**](https://www.stationx.net/wireshark-cheat-sheet/)