Wireshark Customization – From Scratch

A foundational guide to installing and customizing Wireshark for packet analysis

A hands-on network analysis project focused on customizing Wireshark for efficient packet inspection and analysis.

Introduction

Wireshark is one of the most powerful and widely used network protocol analyzers in the world. Whether you're troubleshooting networks, analyzing performance, or learning cybersecurity, Wireshark is a must-have tool for anyone dealing with packets.

This project is **Part One** of my deep dive into Wireshark. The focus is on starting completely from scratch — installing the tool, understanding its interface, and customizing the layout and features for a more efficient analysis experience.

💡 *The goal of this phase is to lay the groundwork for future packet analysis labs by creating a clean and analyst-friendly environment inside Wireshark.*

Sirjan Pun Magar

Installing Wireshark

For windows:

- Downloaded the installer from: https://www.wireshark.org

- Installed WinPcap/Npcap as the packet capture interface
- Verified working installation by listing available network interfaces

Installing Wireshark is a simple and straightforward process suitable for users across all major platforms including Windows, macOS, and Linux.
Since the installation process is widely documented and intuitive, I have not included detailed screenshots or step-by-step instructions in this project. Wireshark's official website provides a user-friendly installer and clear prompts that guide users through the setup process without any complexity.

📌 **Note:** During installation on Windows, you may be prompted to install additional components like **WinPcap** or **Npcap**, which are essential for packet capturing. It's recommended to accept these defaults for full functionality.

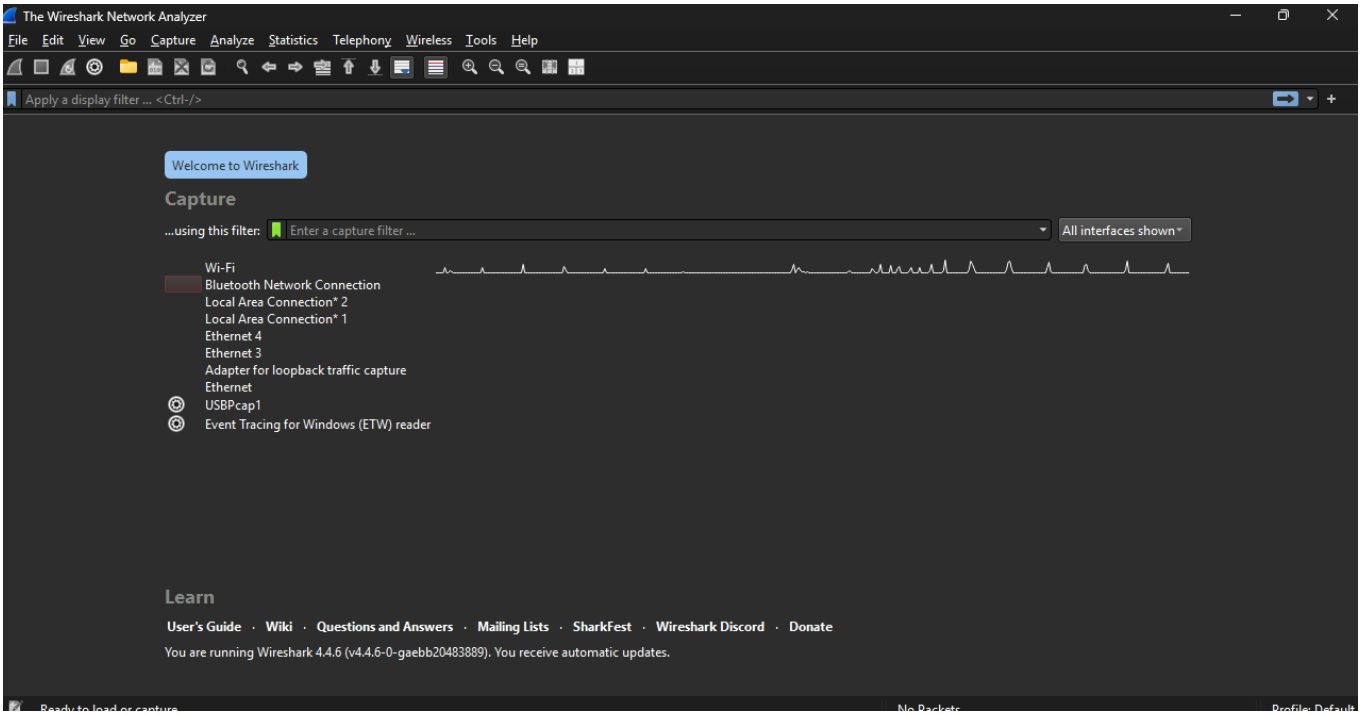
Once installed, Wireshark is ready to be launched and used for capturing and analyzing network traffic.

1. Understanding the Wireshark Interface.

Before jumping into customization, it's essential to get familiar with the core interface of Wireshark. Here's a quick overview of the default layout and its main components:

- Interface List (Home Screen)

Upon launching Wireshark, you're presented with a list of all available network interfaces. You can select any interface to begin capturing packets in real-time.



The Main Toolbar

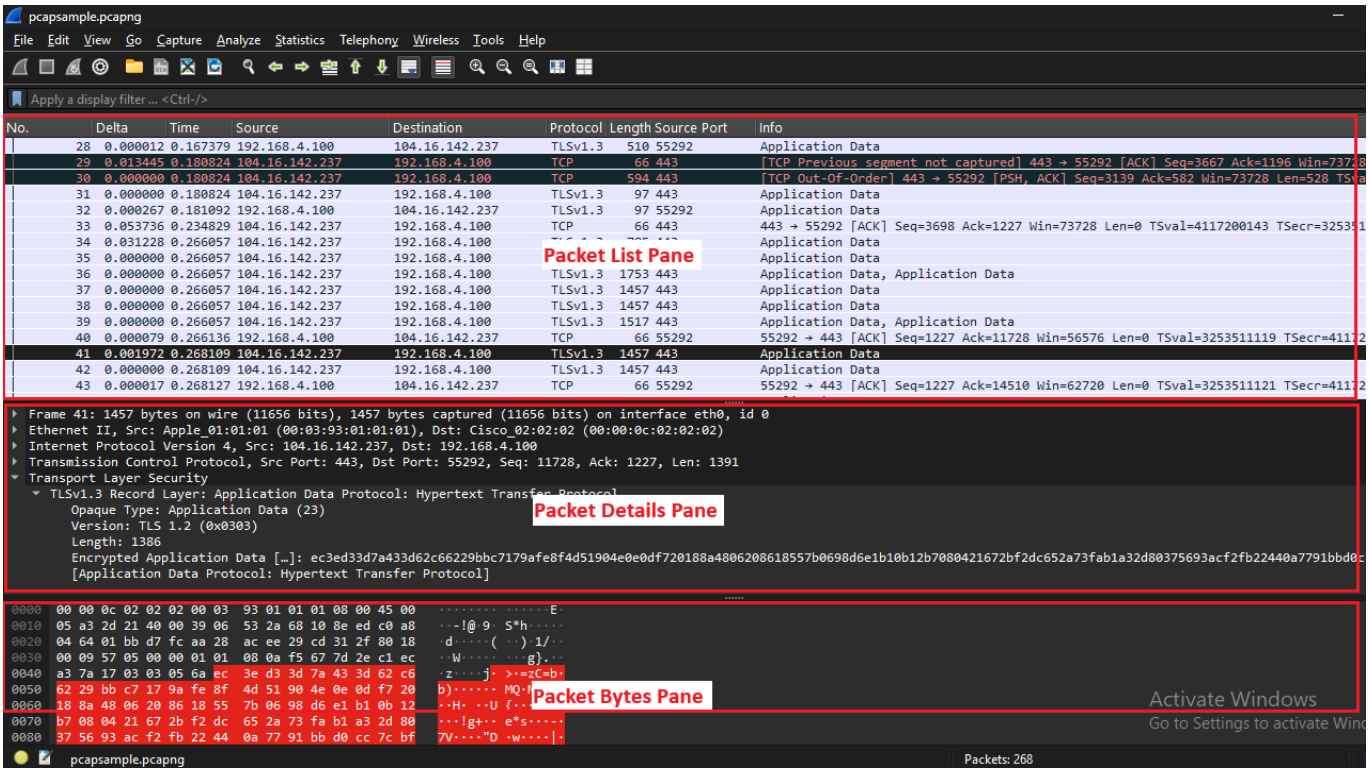
1. Start — Starts capturing packets with the same options as the last capture.
2. Stop — Stops the currently running capture.
3. Restart — Restarts the current capture session.
4. Option — Opens the "Capture Options" dialog box.
5. Open — Opens the file open dialog box, which allows you to load a capture file for viewing.
6. Save As — Save the current capture file to whatever file you would like. If you currently have a temporary capture file open the "Save" icon will be
7. shown instead.
8. Close — Closes the current capture. If you have not saved the capture, you will be asked to save it first.

Sirjan Pun Magar

9. Reload — Reloads the current capture file.
10. Find Packet — Find a packet based on different criteria.
11. Go Back — Jump back in packet history. Hold down the Alt key (Option on macOS) to go back in the selection history.
12. Go Forward — Jump forward in the packet history. Hold down the Alt key (Option on macOS) to go forward in the selection history.
13. Go to Packet — Go to a specific packet.
14. Go To First Packet — Jump to the first packet of the capture file.
15. Go To Last Packet — Jump to the last packet of the capture file.
16. Auto Scroll in Live — Capture Auto scroll packet list while doing a live capture (or not).
17. Colorize — Colorize the packet list (or not).
18. Zoom In — Zoom into the packet data (increase the font size).
19. Zoom Out — Zoom out of the packet data (decrease the font size).
20. Normal Size — Set zoom level back to 100%.
21. Resize Columns — Resize columns, so the content fits into them.

2. Panes in Wireshark

Wireshark's main window is divided into three primary panes, each serving a specific purpose for analyzing network traffic. Understanding these panes is essential for efficient packet inspection.



Packet List Pane:

Displays all captured packets with summary details for quick scanning.

Packet Details Pane:

Break down the selected packet into its protocol layers for detailed analysis.

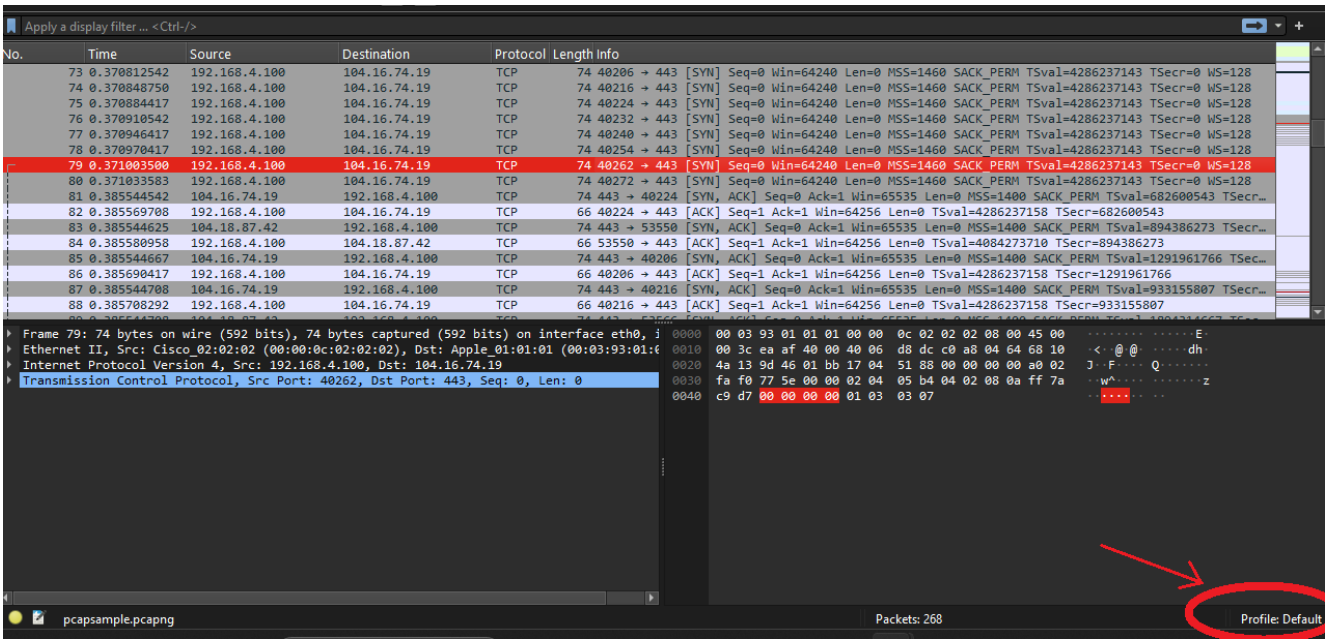
Packet Bytes Pane:

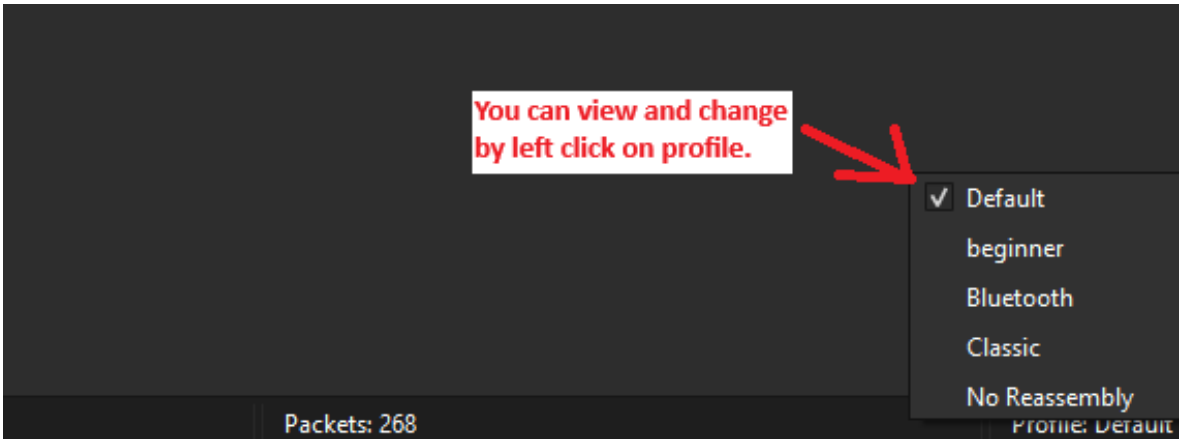
Shows the raw hex and ASCII data of the selected packet for byte-level inspection.

3. Profiles in Wireshark

In Wireshark, profiles are personalized environments that store your specific display settings, filters, coloring rules, column layouts, and other preferences.

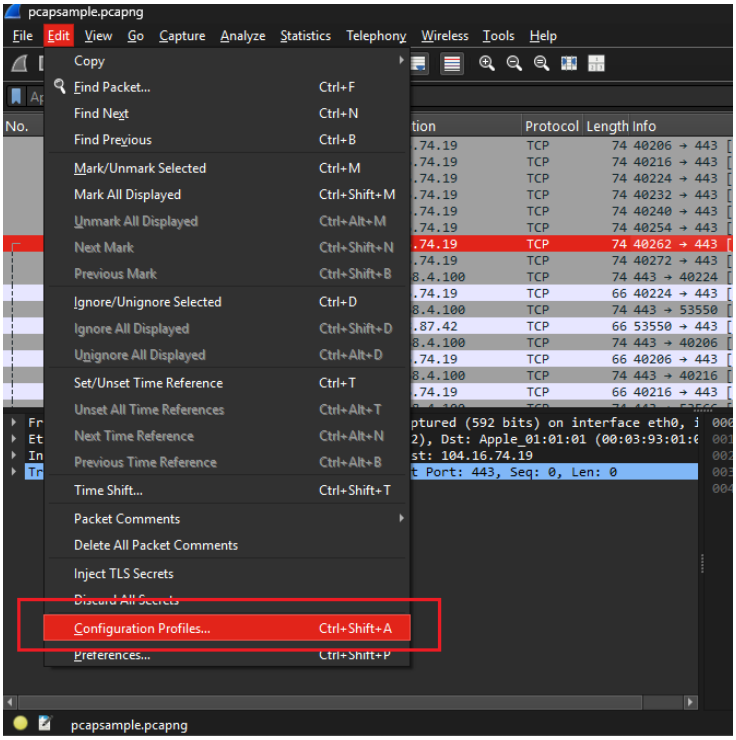
Each profile acts like a separate workspace, allowing users to quickly switch between different setups depending on the task.



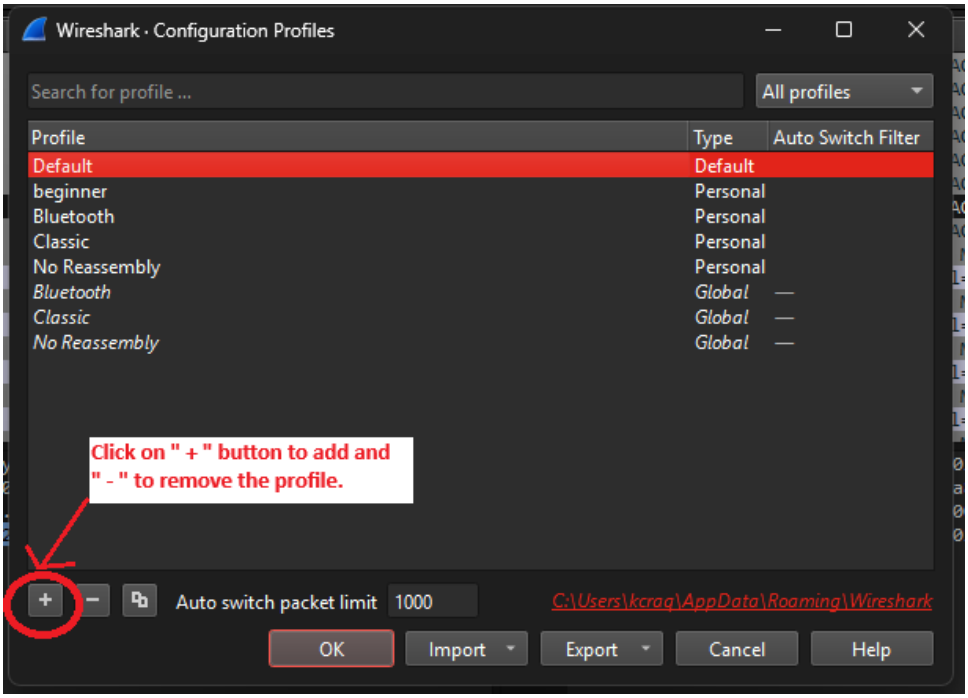


How to Create a New Profile in Wireshark

1. Go to: Edit → Configuration Profiles...



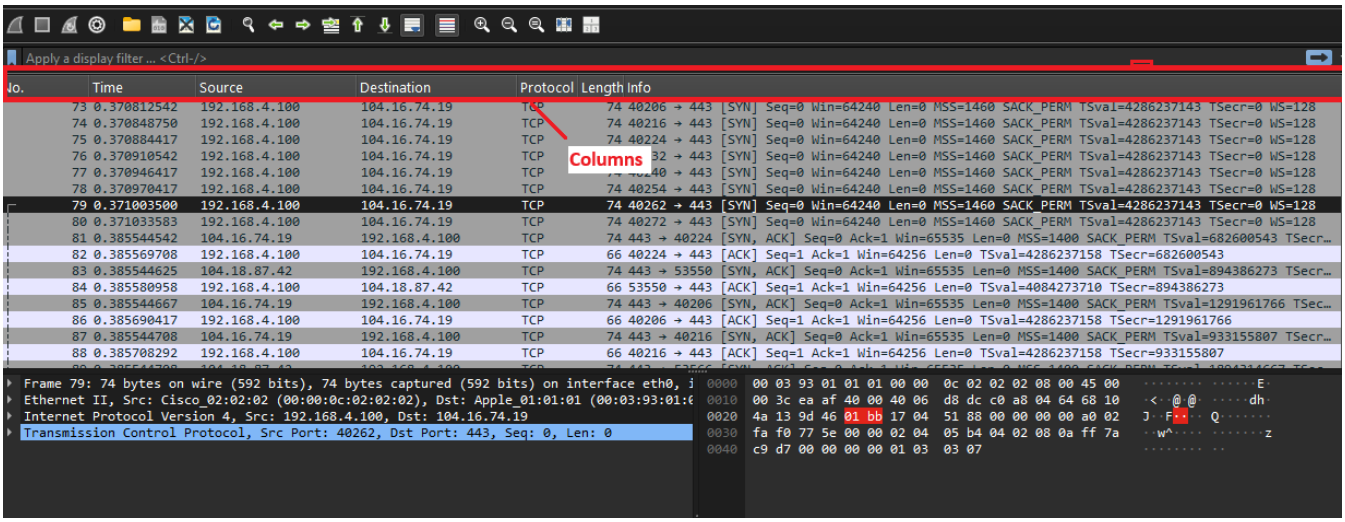
2. Click: “+” New to create a new profile.
3. Name your Profile: Enter a descriptive name (e.g., "Cybersecurity Lab Profile").
4. Switch Profiles Easily: You can switch between profiles anytime from the main toolbar or the Edit → Configuration Profiles menu.



Sirjan Pun Magar

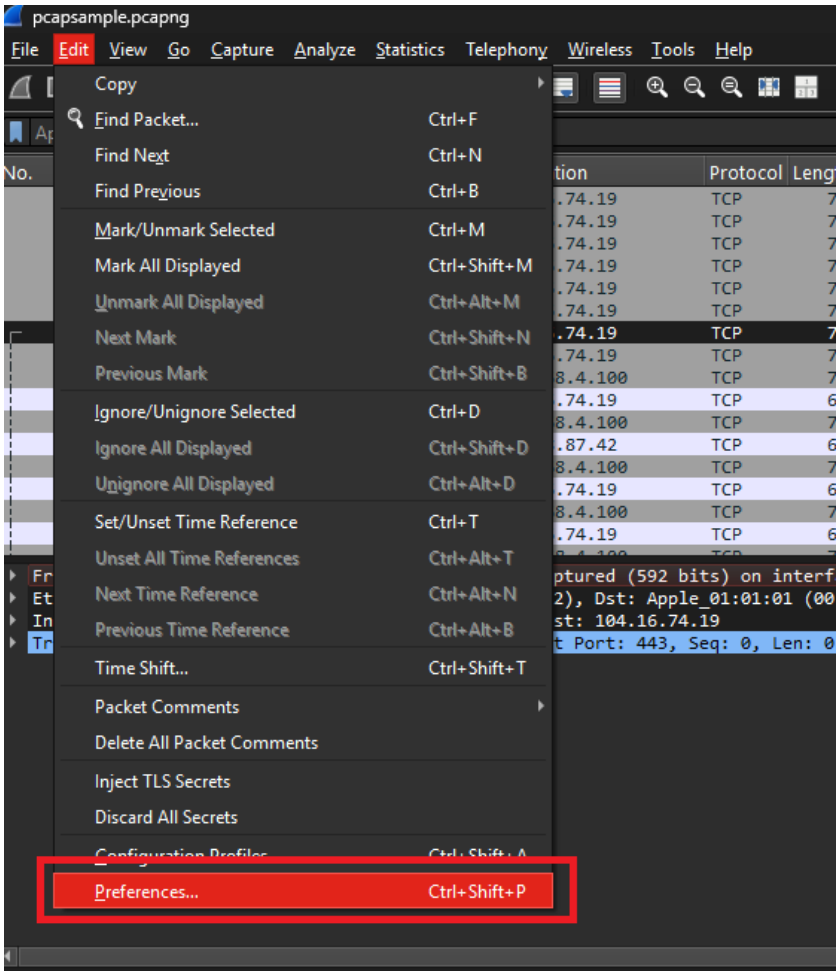
4. Columns in Wireshark

Columns in Wireshark display important fields from captured packets in an organized, readable table. By default, Wireshark shows basic columns like Time, Source, Destination, Protocol, and Info — but you can customize and add more columns based on what information you need most during analysis.

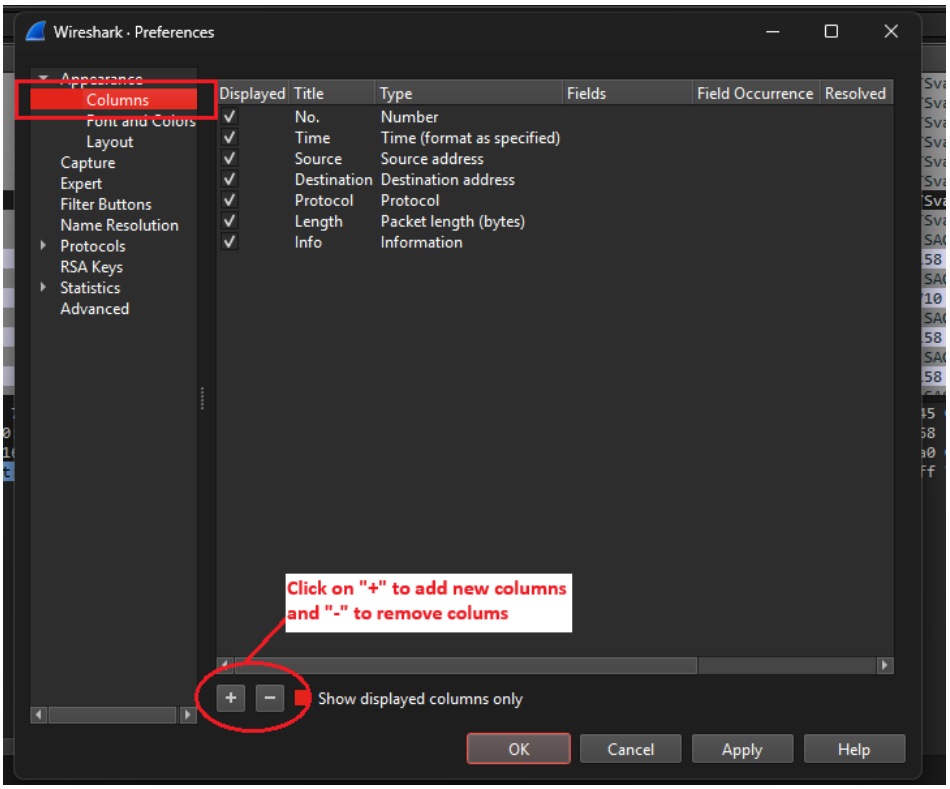


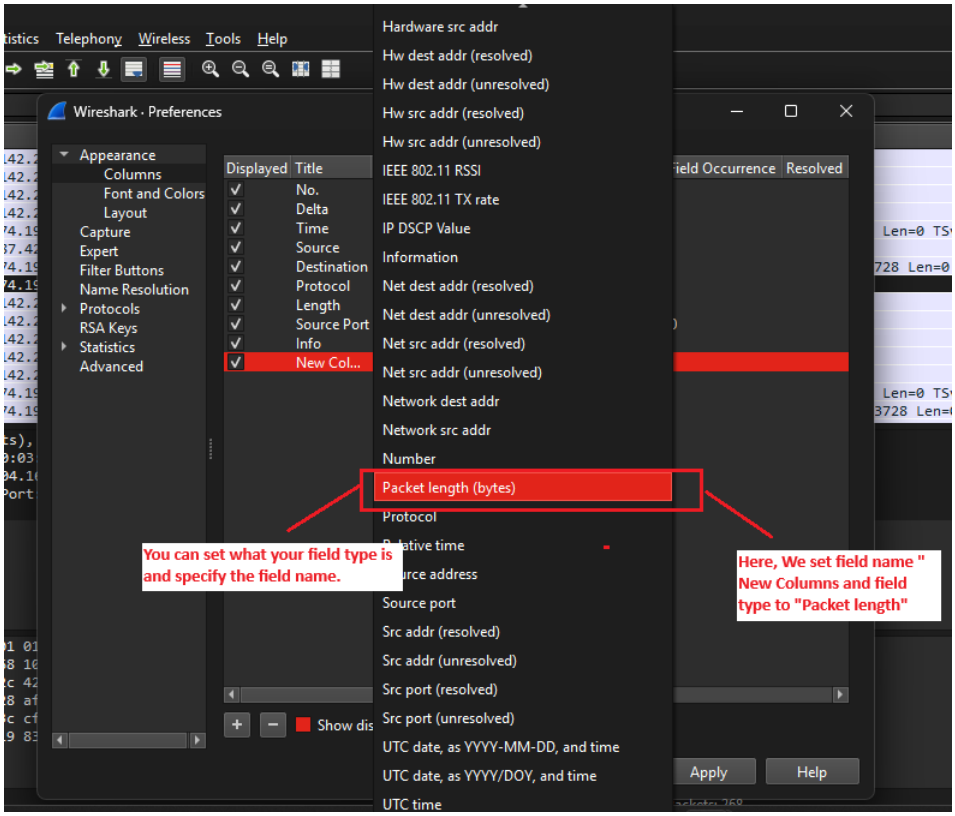
How to Add a Custom Column in Wireshark

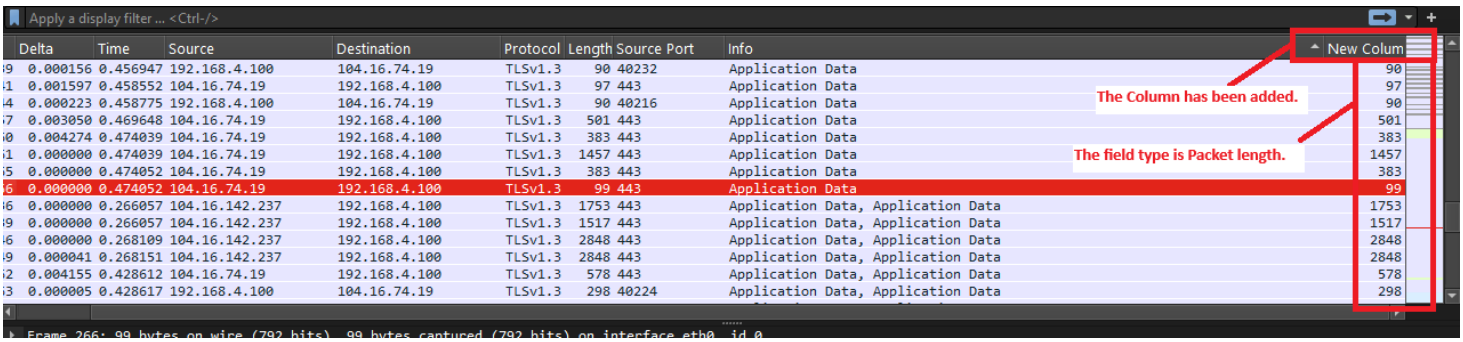
1. Right-click any existing column header → Select Column Preferences,
2. or go to Edit → Preferences → Appearance → Columns.
3. Click + (Add) to create a new column.
4. Enter a Title for the column (e.g., "HTTP Host").
5. Set the Field Type to "New Column" and specify the Field Name (e.g., Packet length).
6. Apply/Save your changes — the new column will appear instantly!



Sirjan Pun Magar


Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Displayed
Title
Type
Fields
Field Occurrence
Resolved
No. Number
Time Time (format as specified)
Source Source address
Destination Destination address
Protocol Protocol
Length Packet length (bytes)
Info Information
Click on "+" to add new columns and "-" to remove colums
Show displayed columns only
OK
Cancel
Apply
Help


Wireshark · Preferences
Appearance
Columns
Font and Colors
Layout
Capture
Expert
Filter Buttons
Name Resolution
Protocols
RSA Keys
Statistics
Advanced
Displayed
Title
No.
Delta
Time
Source
Destination
Protocol
Length
Source Port
Info
New Col...
Hardware src addr
Hw dest addr (resolved)
Hw dest addr (unresolved)
Hw src addr (resolved)
Hw src addr (unresolved)
IEEE 802.11 RSSI
IEEE 802.11 TX rate
IP DSCP Value
Information
Net dest addr (resolved)
Net dest addr (unresolved)
Net src addr (resolved)
Net src addr (unresolved)
Network dest addr
Network src addr
Number
Packet length (bytes)
Protocol
Source port
Src addr (resolved)
Src addr (unresolved)
Src port (resolved)
Src port (unresolved)
UTC date, as YYYY-MM-DD, and time
UTC date, as YYYY/DOY, and time
UTC time
You can set what your field type is and specify the field name.
Here, We set field name " New Columns and field type to "Packet length"
Apply
Help

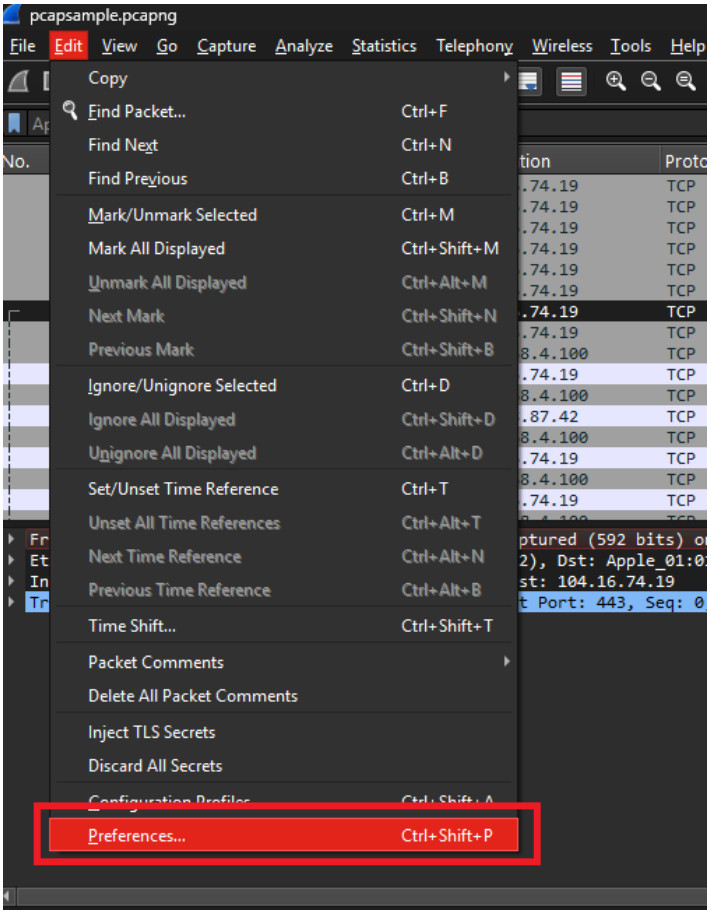

Apply a display filter ... <Ctrl-/>
Delta
Time
Source
Destination
Protocol
Length
Source Port
Info
New Colum
The Column has been added.
The field type is Packet length.

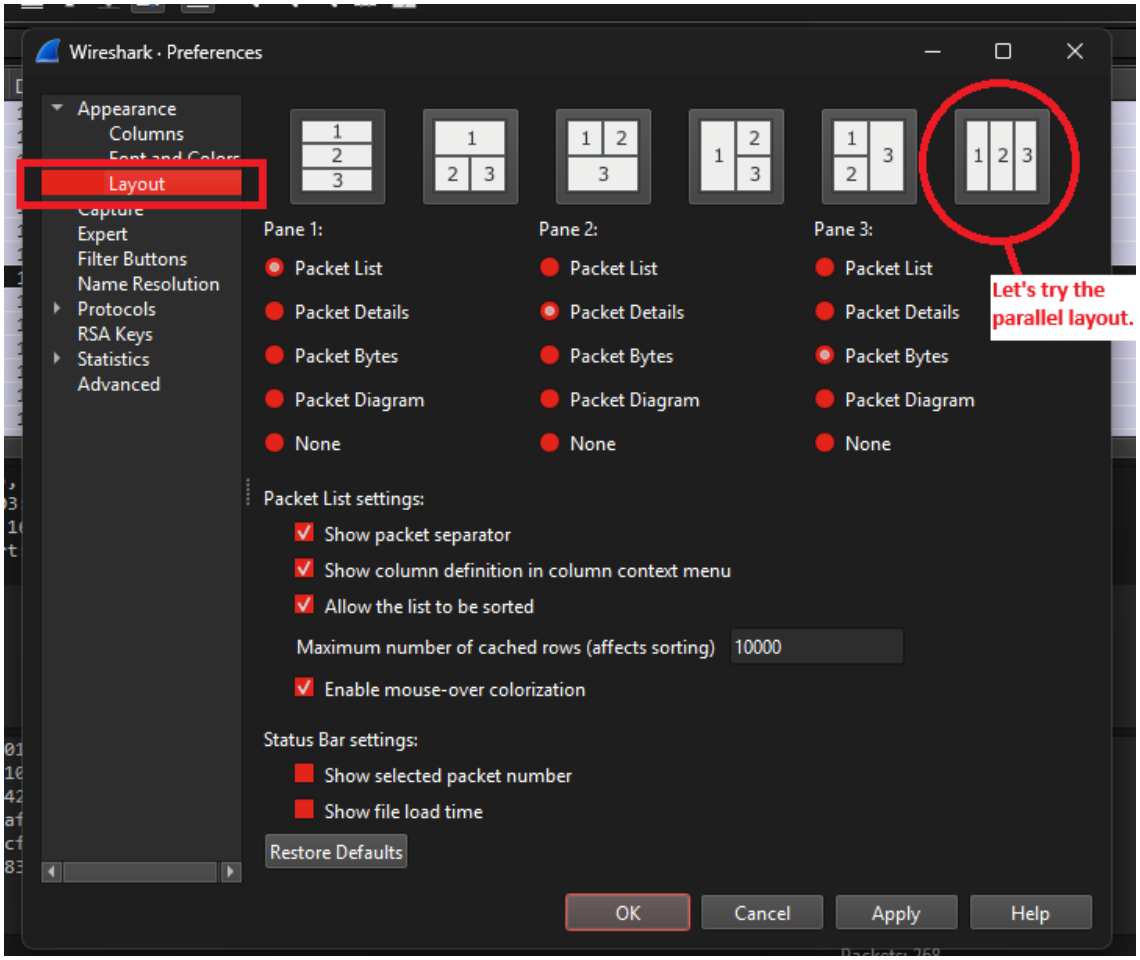
5. Layout in Wireshark.

The layout in Wireshark defines how the main panes (Packet List, Packet Details, and Packet Bytes) are arranged on your screen.
You can customize the position, size, and orientation of these panes to match your personal workflow and screen size.

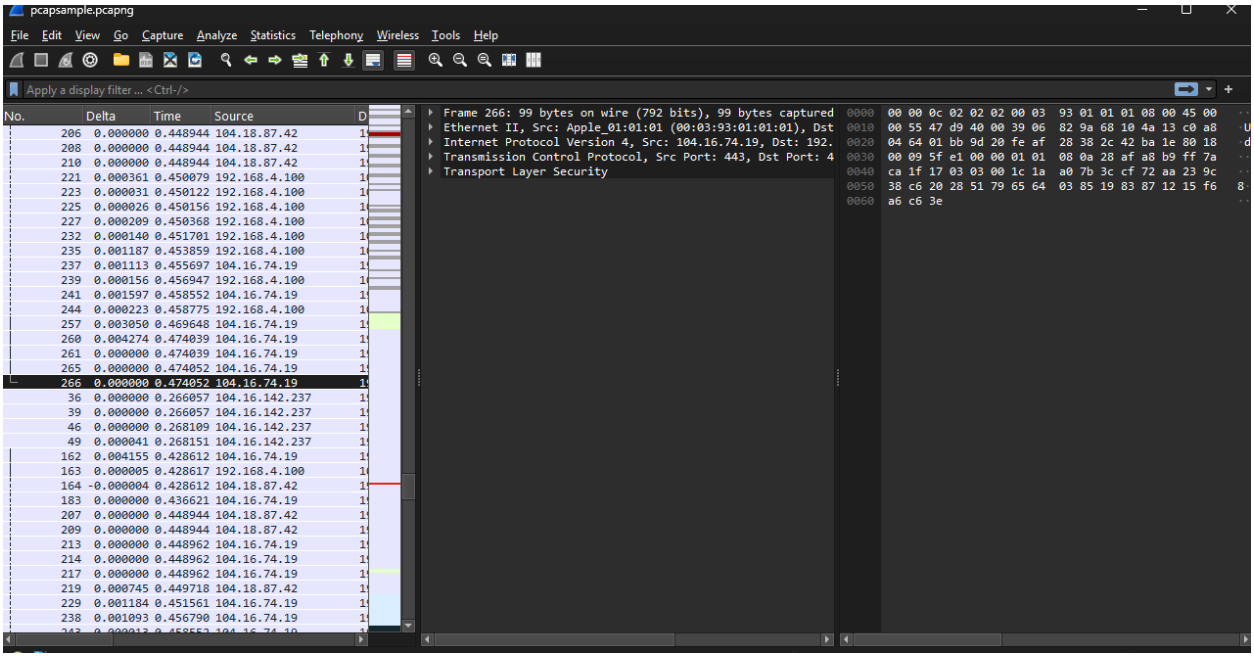
How to Adjust the Layout in Wireshark

1. Go to: Edit → Preferences → Appearance → Layout.
2. Choose Layout Style: Select from built-in options like "Classic three-pane", "Packet List on top," or "Packet List on the left."
3. Customize Pane Sizes: Drag the borders between panes manually to adjust their size.
4. Apply Changes: Your new layout will be saved automatically within your active profile.





The parallel layout has been applied.



Sirjan Pun Magar

6. Coloring in Wireshark

Coloring in Wireshark highlights packets based on certain rules, making it easier to quickly spot important or abnormal traffic.

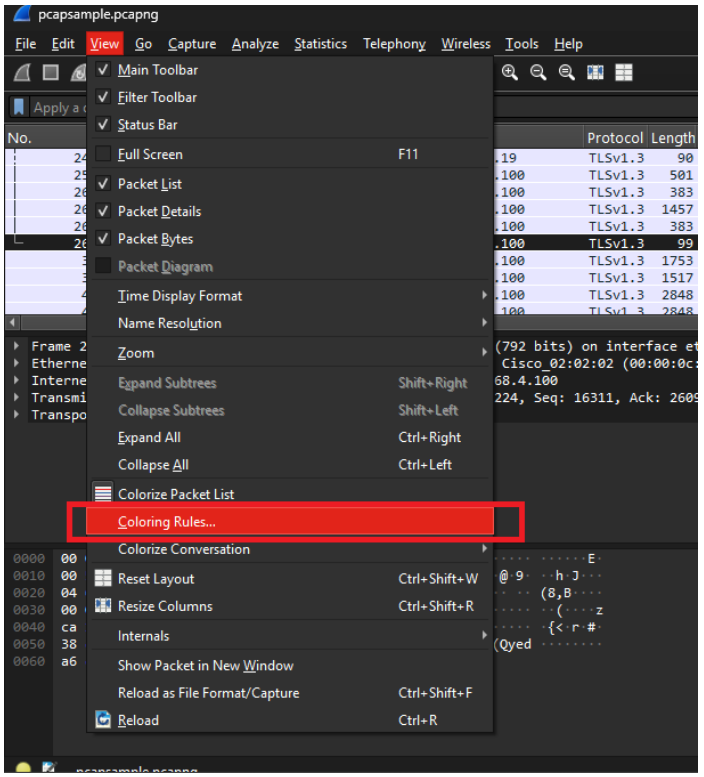
Each coloring rule matches packet fields or protocols and applies a background and/or foreground color to the packet in the Packet List Pane.

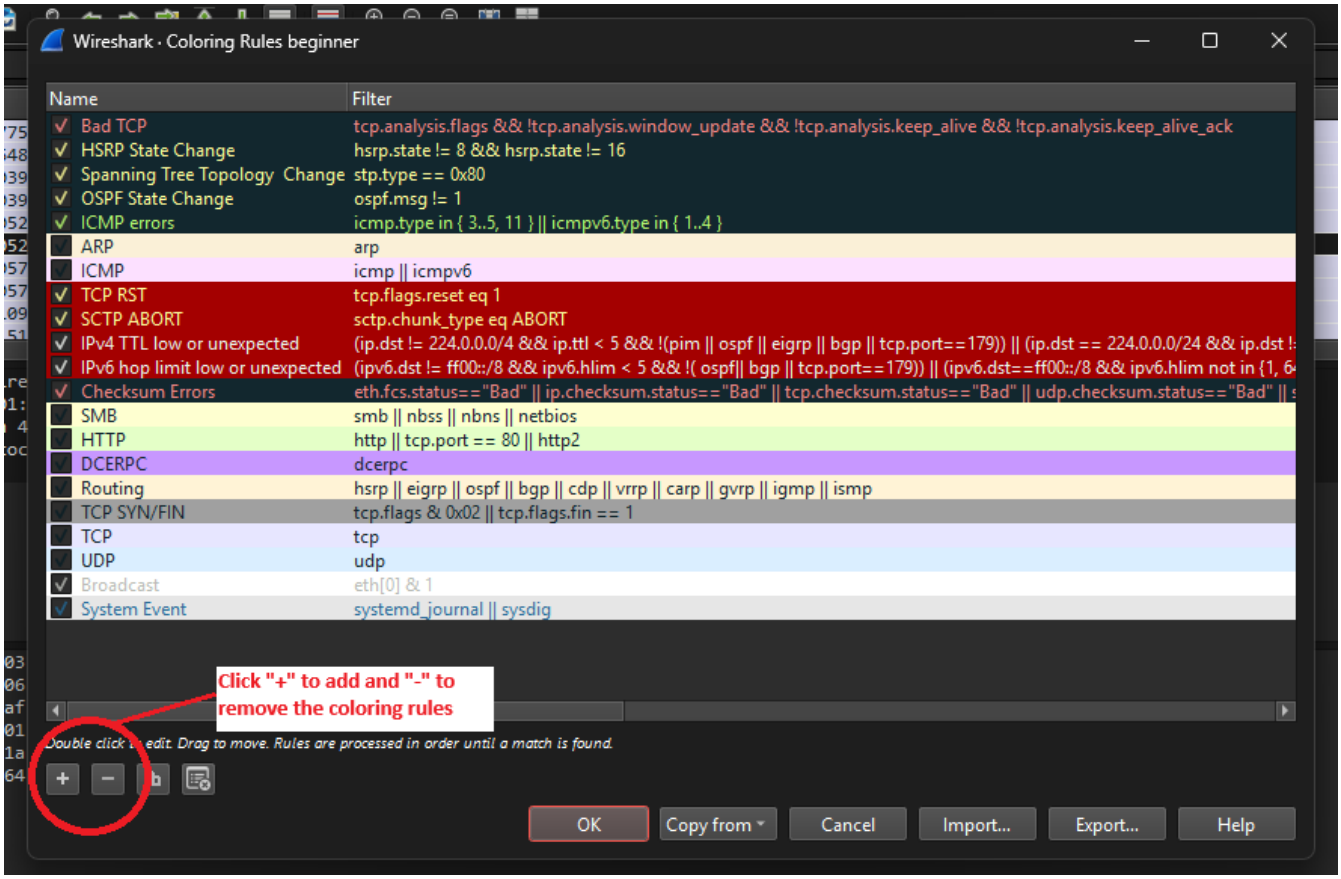
Why Coloring is Important

- Instant Pattern Recognition: Quickly identify traffic types (e.g., TCP retransmissions, DNS queries, HTTP requests) at a glance.
- Highlight Suspicious Activity: Easily spot anomalies, errors, or suspicious packets without inspecting each one manually.
- Customized Focus: You can modify existing rules or create new ones tailored to your specific analysis needs.
- Improve Workflow: Reduces the mental load during packet analysis by visually grouping similar packet types together.

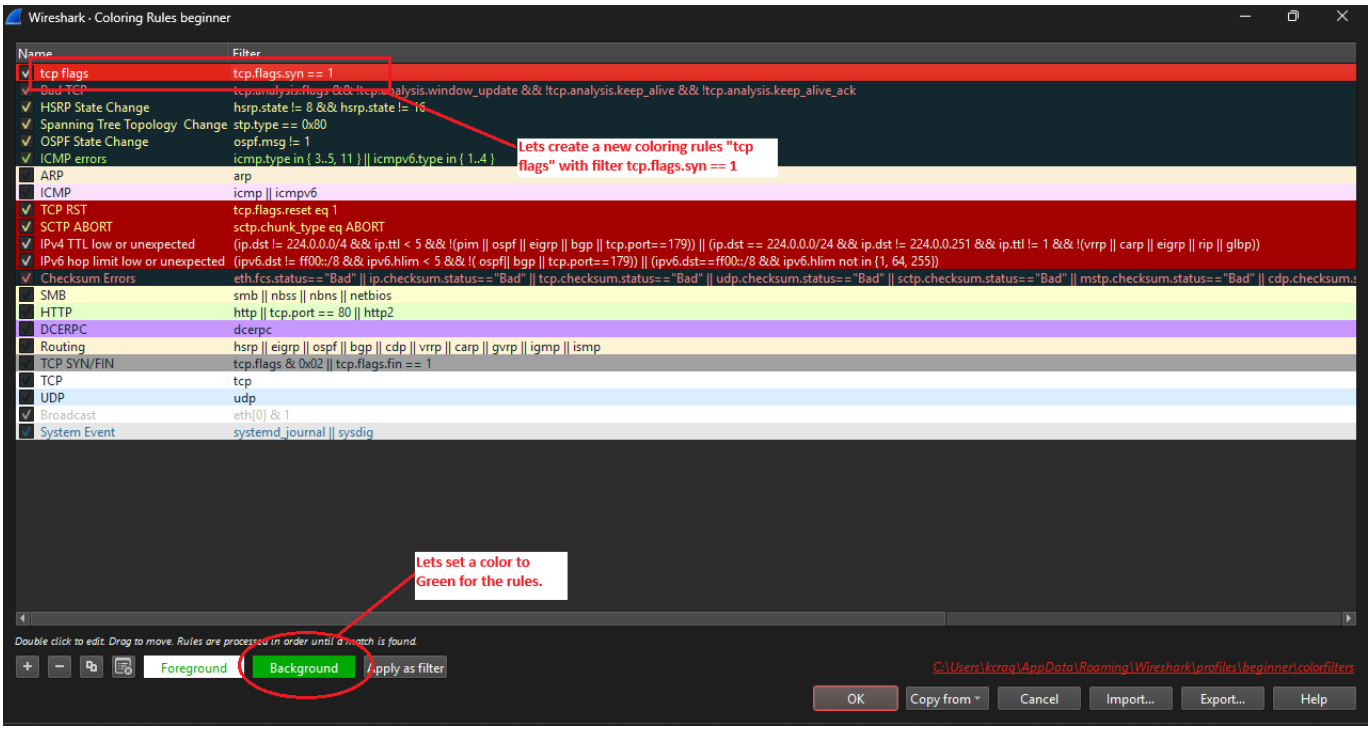
How to Manage Coloring Rules in Wireshark

1. Open Coloring Rules: View → Coloring Rules...
2. Edit Existing Rules: You can double-click any rule to modify its filter expression or colors.
3. Add New Rule: Click + to add a new rule. Specify a display filter (e.g., tcp.flags.syn == 1) and assign colors.
4. Remove Rule: Select a rule and click - if it's no longer needed.
5. Apply and Save: Coloring changes apply immediately and are saved to the active profile.



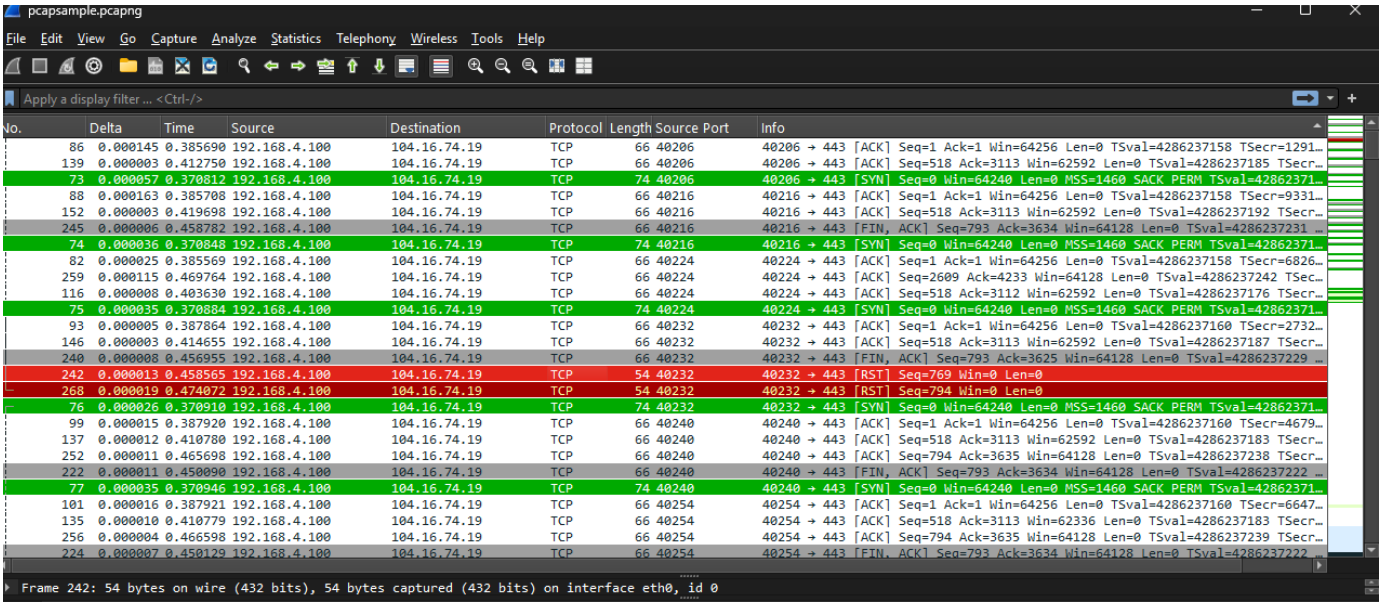


Add New Rule: Click + to add a new rule. Specify a display filter (e.g., tcp.flags.syn == 1) and assign colors here "Green"



Sirjan Pun Magar

The coloring rule can be seen in the green coloring pattern.



Sirjan Pun Magar

7. Filters in Wireshark

Filters in Wireshark allow you to narrow down the vast amount of captured data, helping you focus only on the packets you care about.

There are two main types of filters:

- Capture Filters — applied before capturing traffic.
- Display Filters — applied after capturing, to view only specific packets.

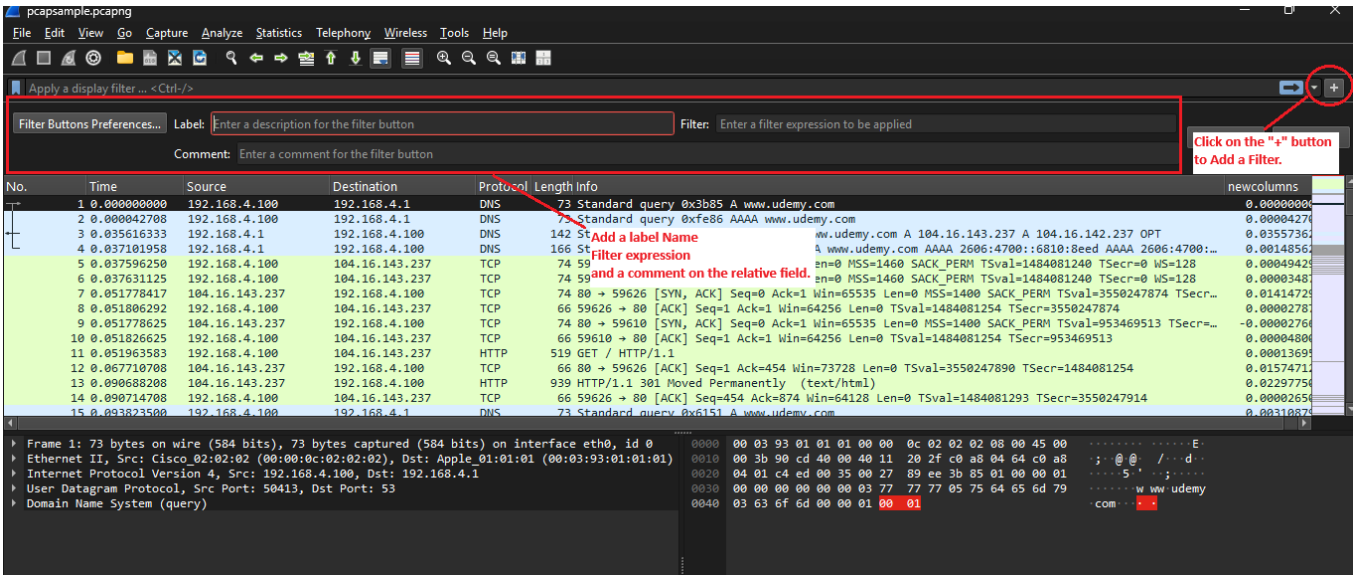
In this project, we focus mainly on Display Filters because they are essential during packet analysis.

Why Filters are Important

- Focus on Relevant Data: Quickly isolate interesting or suspicious packets.
- Speed Up Analysis: Avoid being overwhelmed by thousands of irrelevant packets.
- Troubleshoot Faster: Target specific conversations (like HTTP traffic, DNS queries, TCP issues) immediately.
- Precision Investigation: Apply complex filter expressions to find exactly what you need.

How to Add a Filter Button in Wireshark

1. Apply a Display Filter: Type a filter in the top filter bar (e.g., http or ip.addr == 192.168.1.1) and hit Enter.
2. Save as Filter Button: Click the small + icon next to the filter bar after applying your filter.
3. Name Your Filter Button: Enter a short, descriptive name (e.g., "HTTP Traffic").
4. Use Filters Quickly: Your new filter button will appear below the filter bar for one-click access in the future.



Sirjan Pun Magar

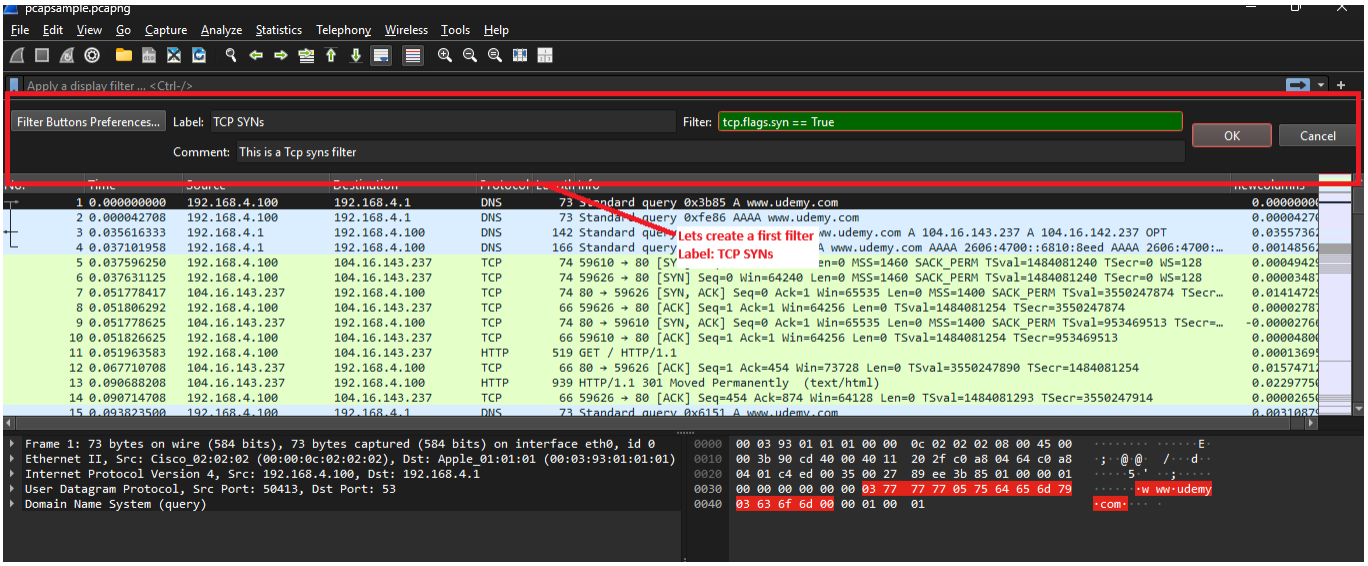
Example 1:

Click on the “+” button.

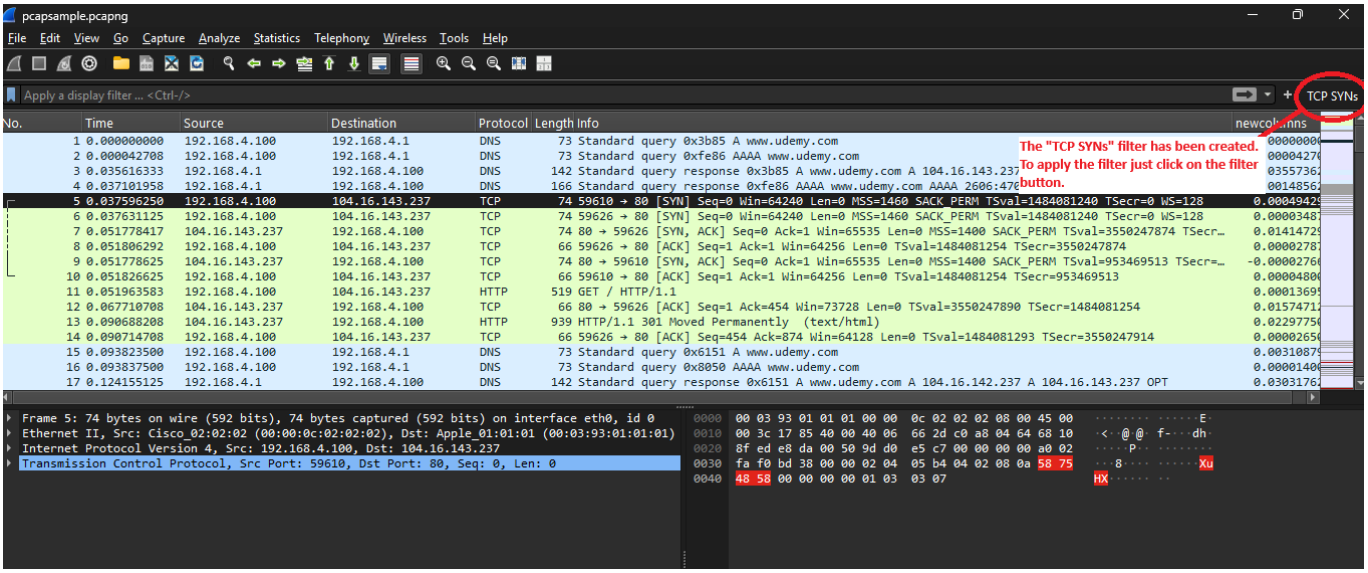
Now let’s name a Label : TCP SYNs

Filter: tcp.flags.syn == true

Comment: This is a Tcp syns filter.

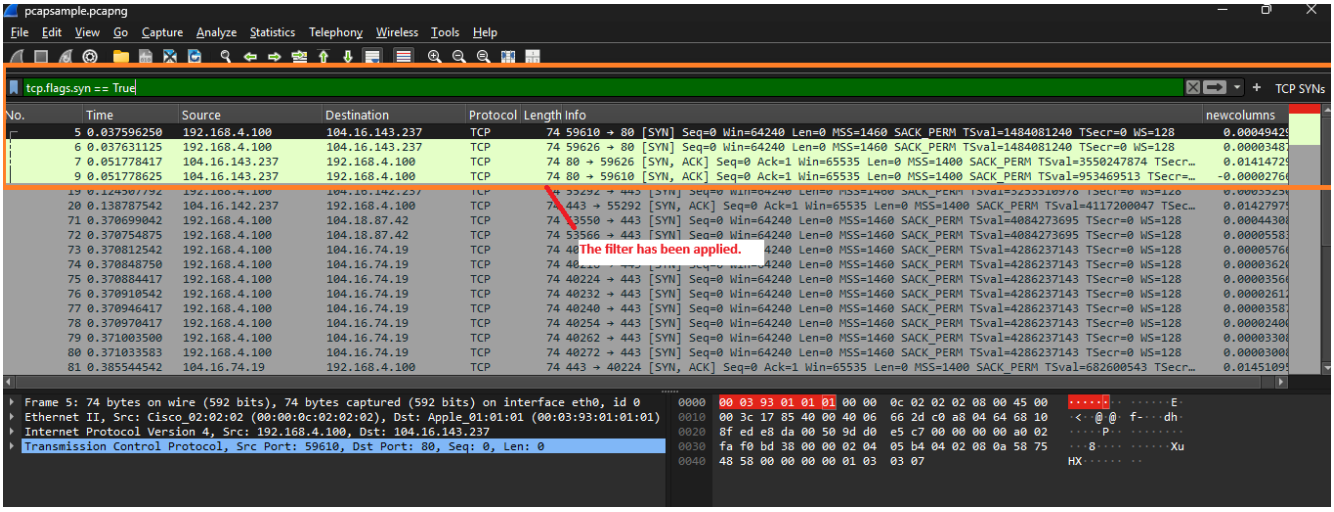


After the creation we can see the TCP SYNs button on the corner of the filter box.



Sirjan Pun Magar

Click on the Filter button to apply.



Sirjan Pun Magar

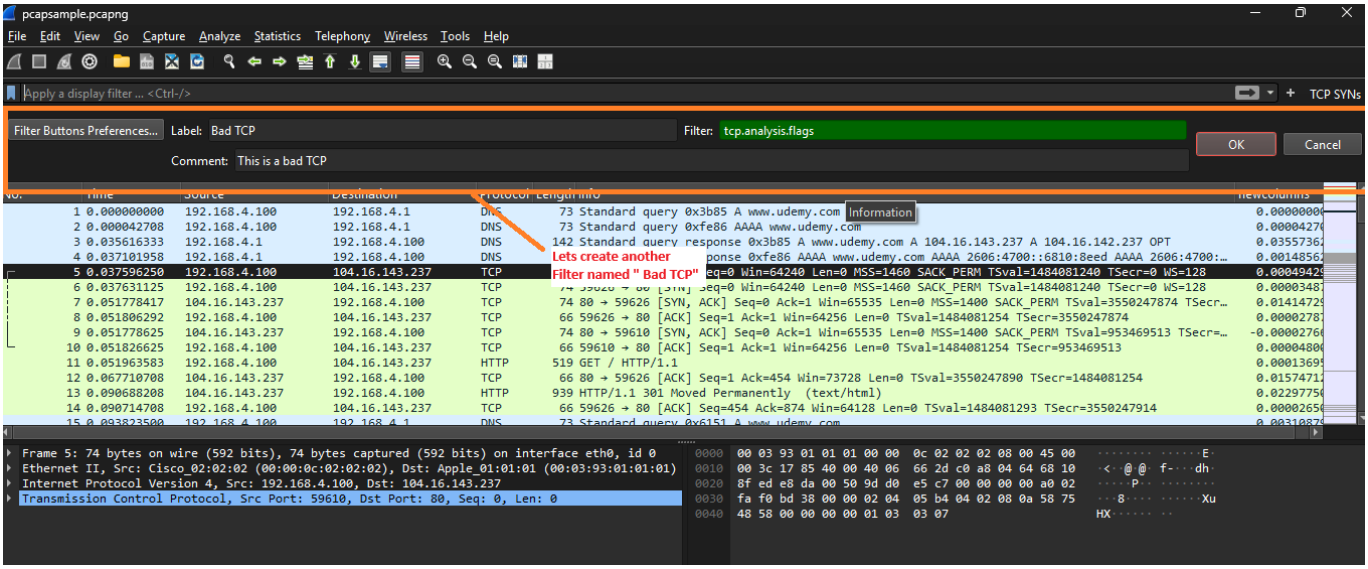
Example 2:

Click on the “+” button.

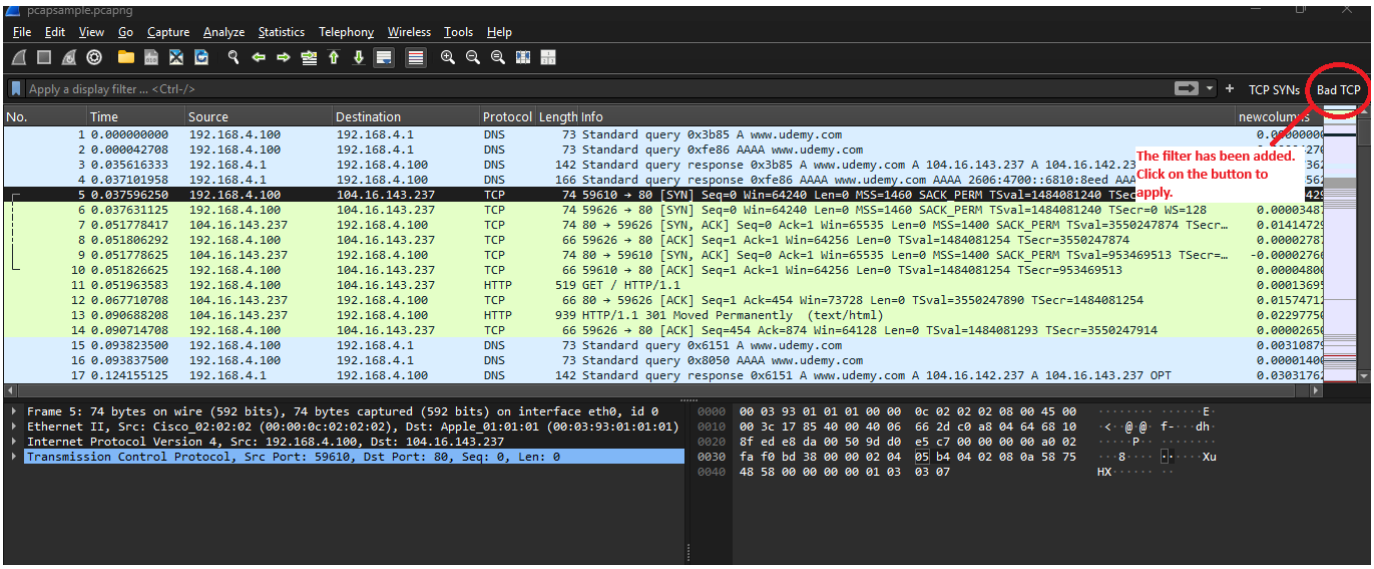
Now let’s name a Label : Bad TCP

Filter: tcp.analysis.flags

Comment: This is a bad TCP

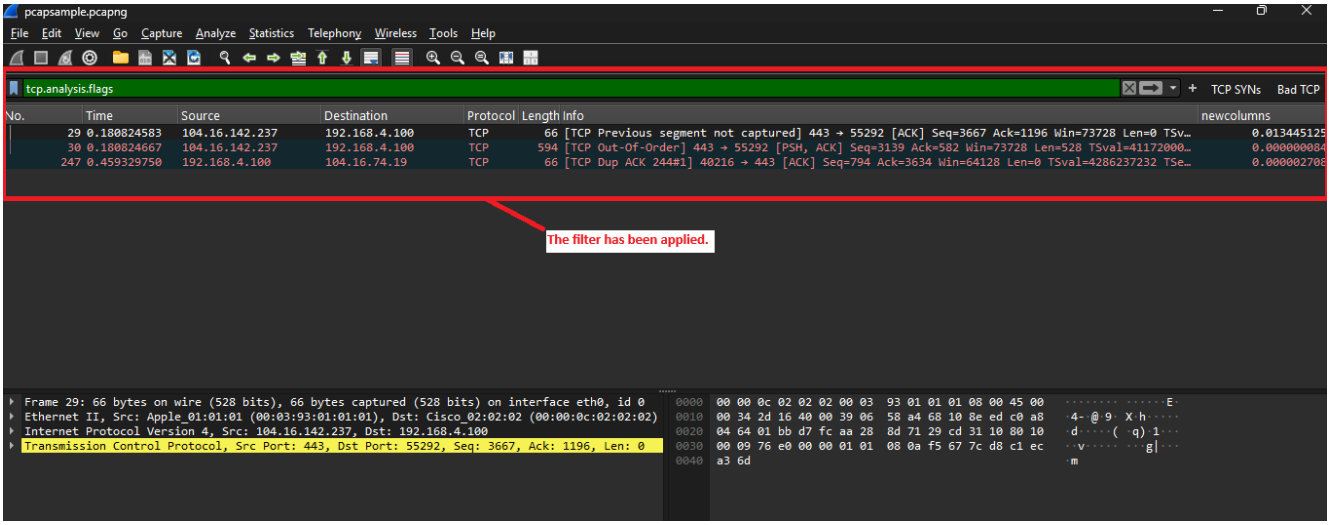


After the creation we can see the Bad TCP button on the corner of the filter box.



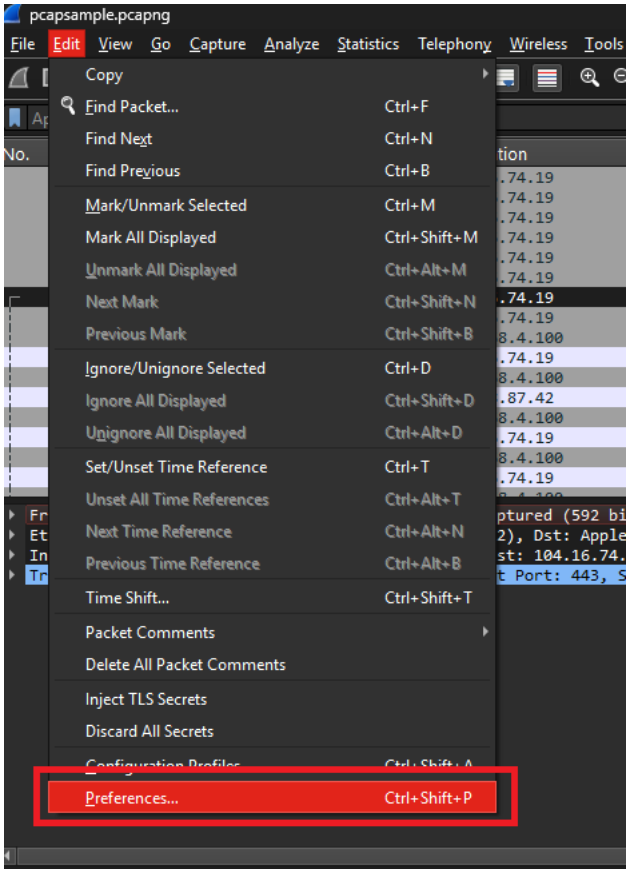
Sirjan Pun Magar

The Bad TCP filter has been applied.



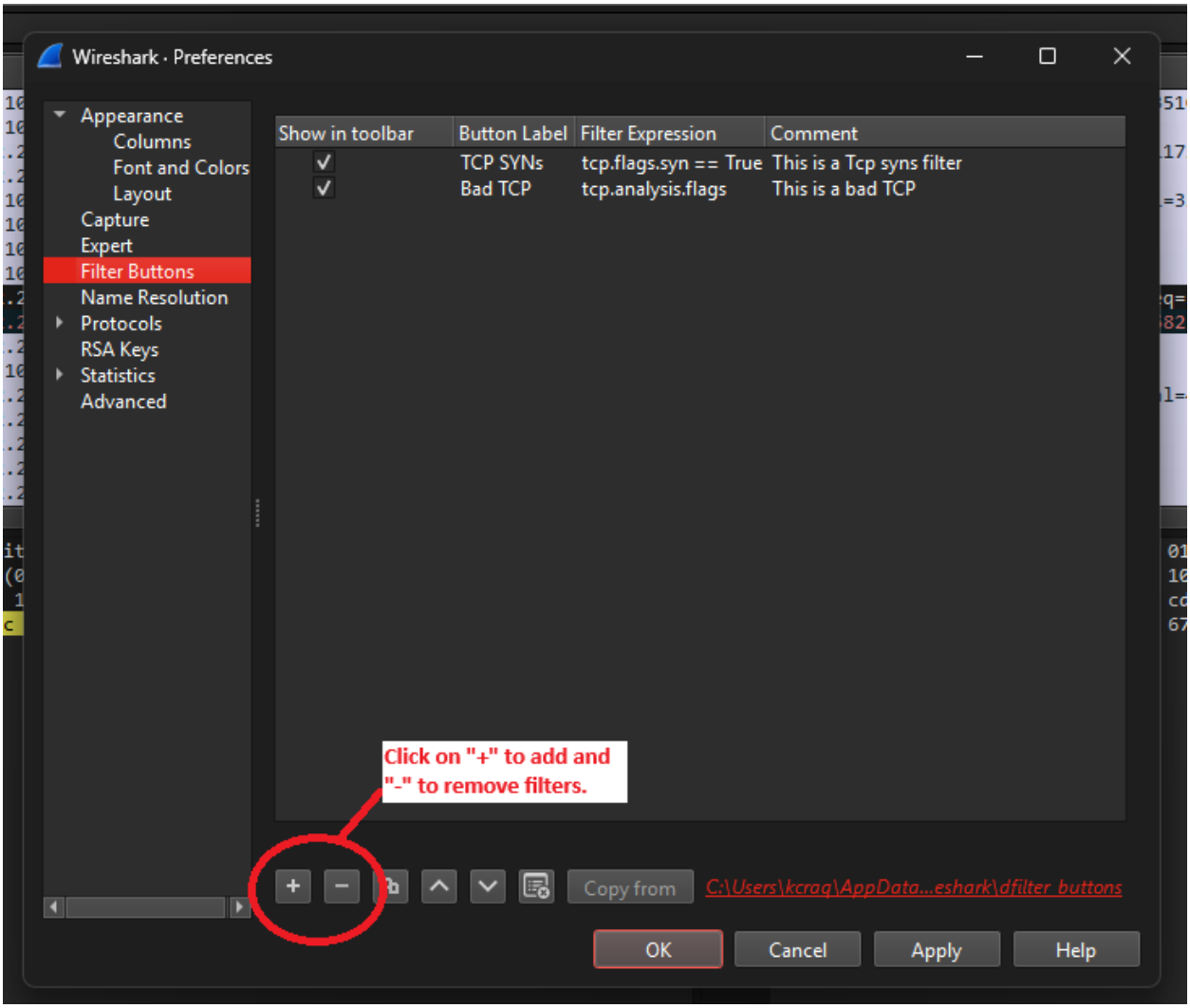
You can also view, add or remove filter by:

1. Go to Edit -> Preferences.
2. Click on Filter Buttons
3. Add / Remove the filters.



Sirjan Pun Magar

You can view/edit/add/remove the filters.



Sirjan Pun Magar