**EXPERIMENT – 4**

**Advanced wire shark features**

**Aim of the experiment:** How we use advance wire shark features

**Learning Objective/Theory**

At the end of the experiment, we will be able to

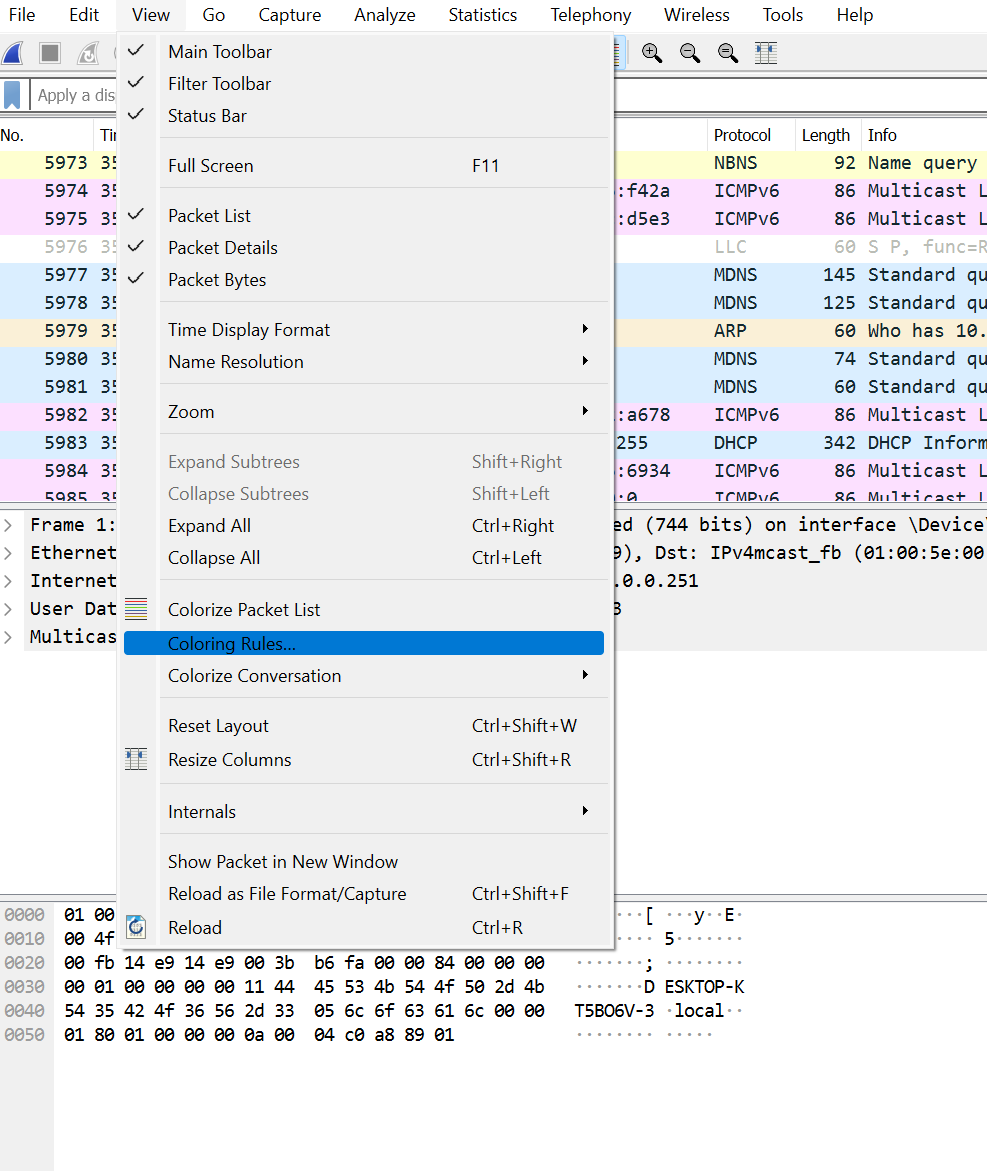
• Use one of the best packet sniffing tools i.e., “Wireshark”.

• Control upon ports, protocols and data packets.

• Quick protocol identification.

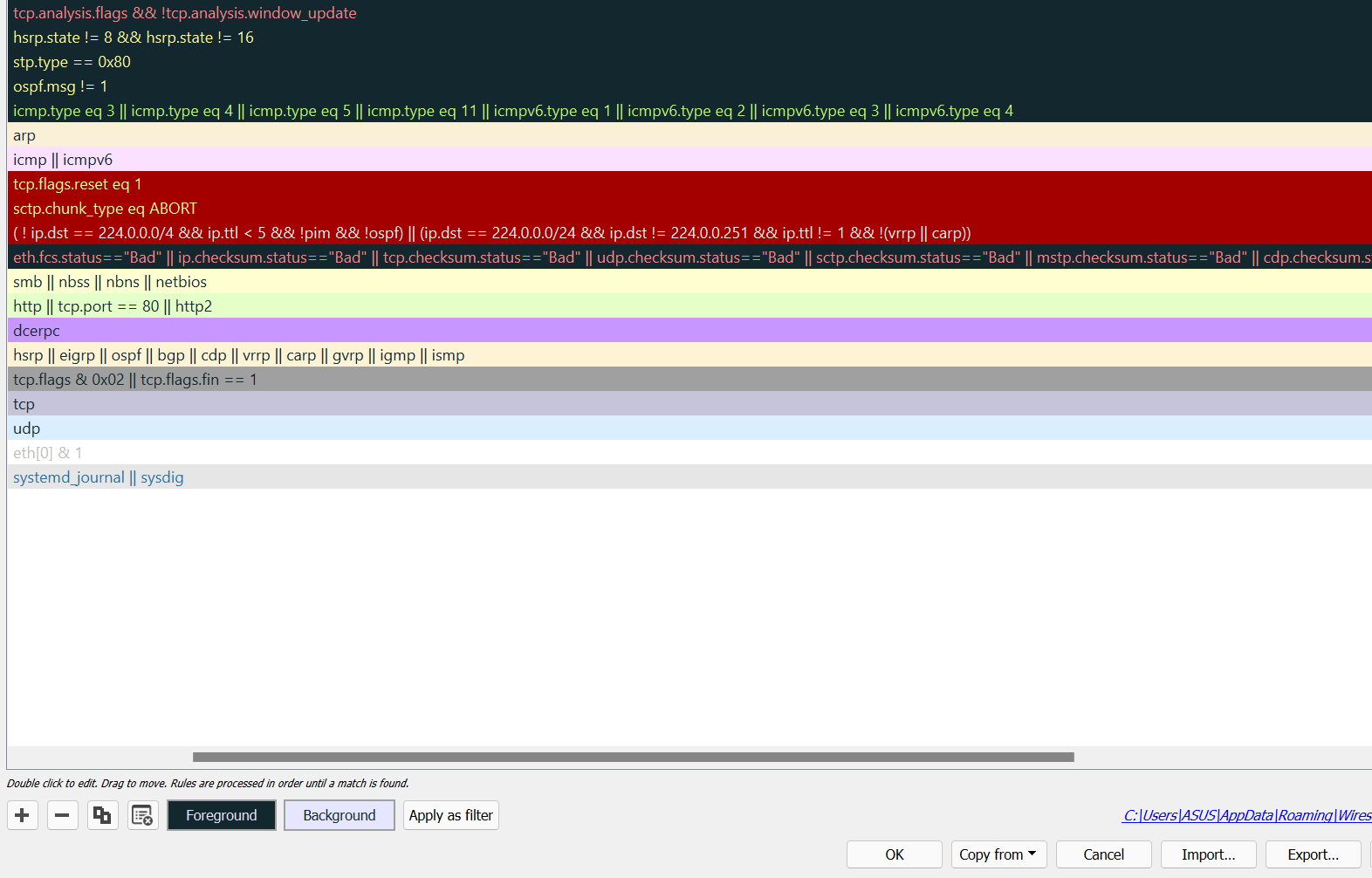
• Start capturing and analysing packets

**Step: 1**



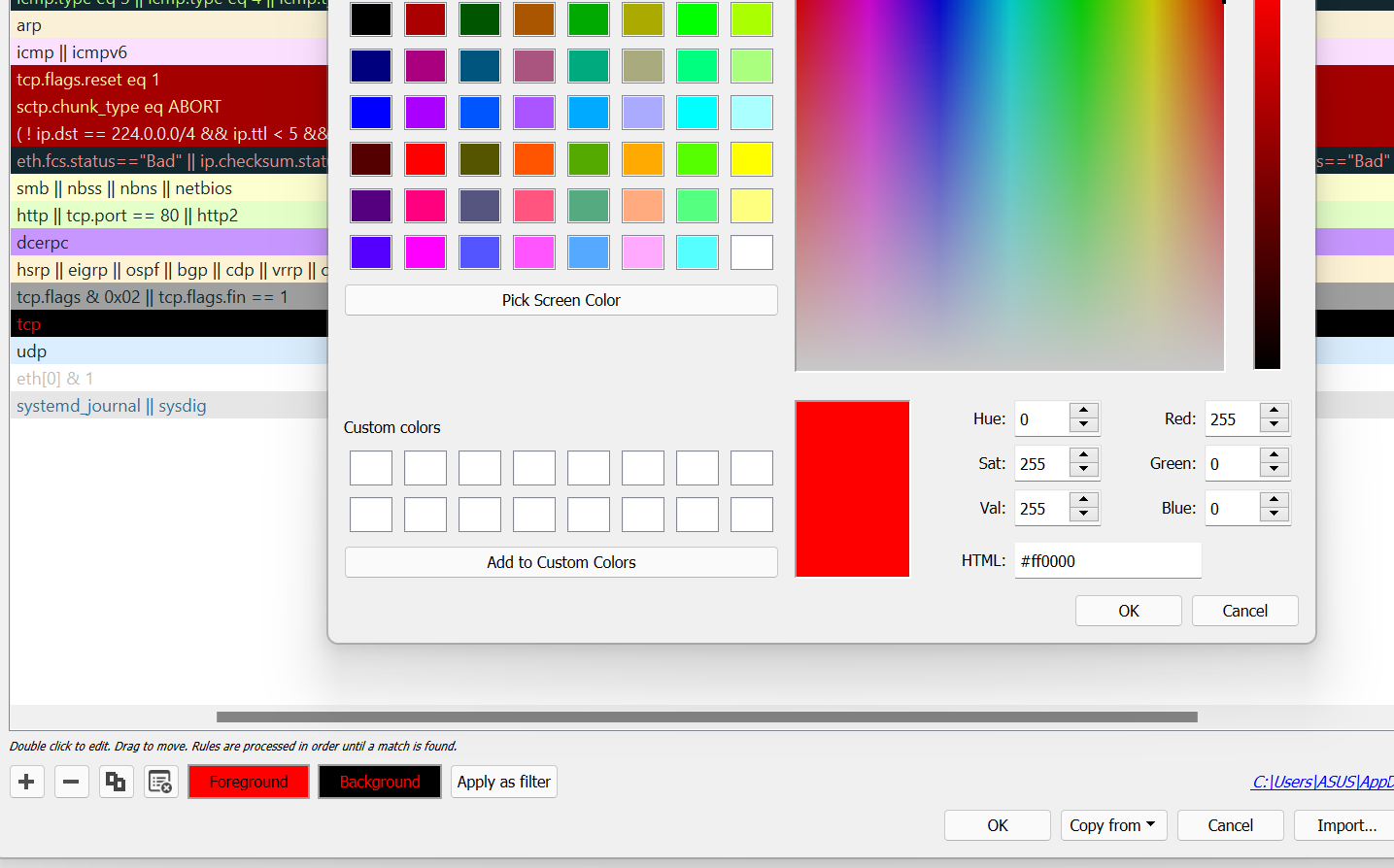
* First go to view then select coloring rules.

**Step: 2**

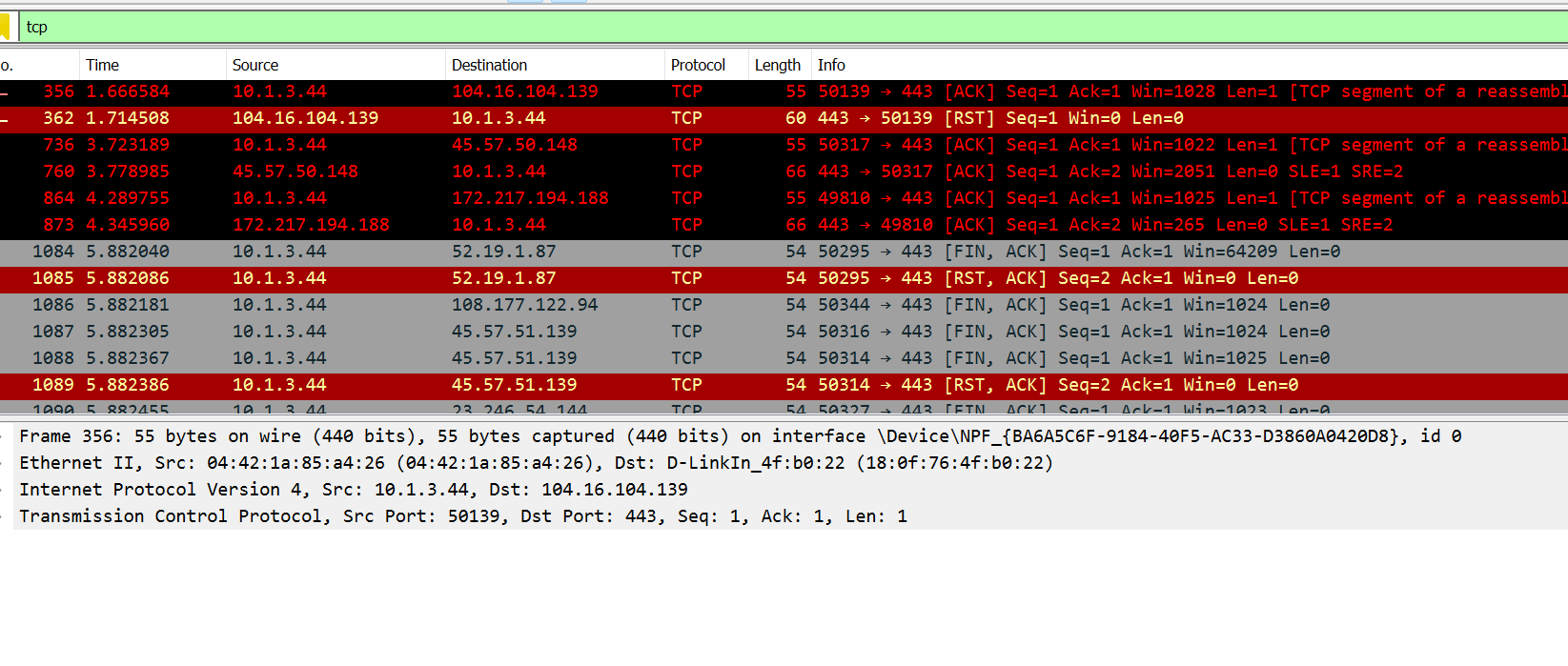


* Select any protocol to change its foreground and background colors for better analysis.

**Step: 3**



* Here we choose tcp protocol and changed its foreground color to red and background color to black.

**Step: 4** 

* In this step we found the tcp packet is colored according to the before preference that is foreground color red and background color black.

**Conclusion:** we success full coloring tcp packet