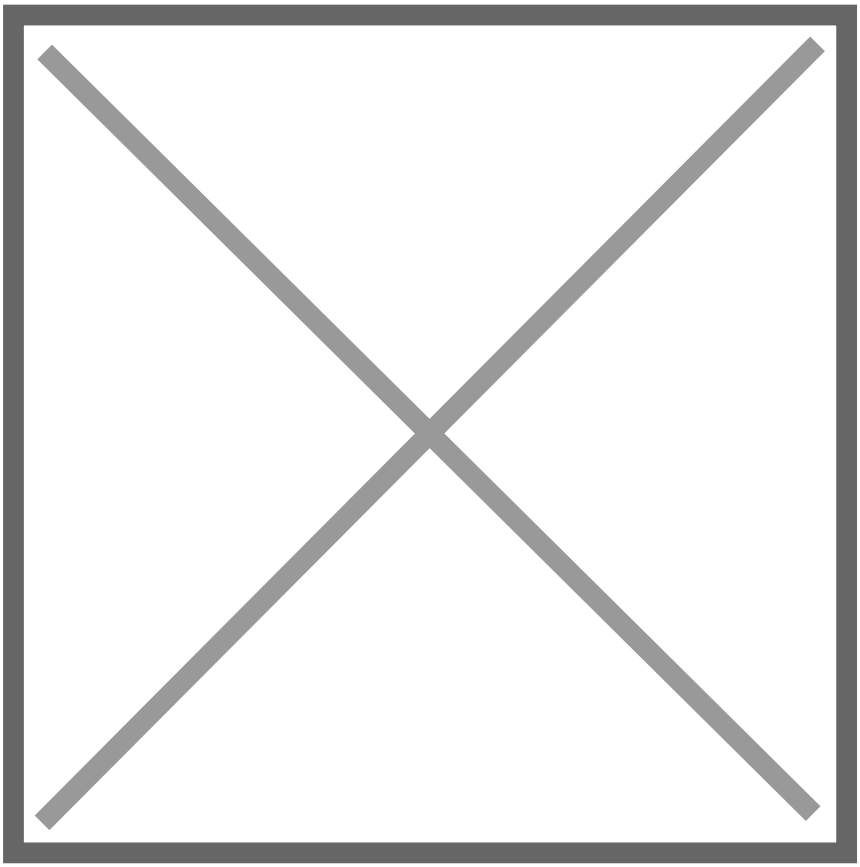
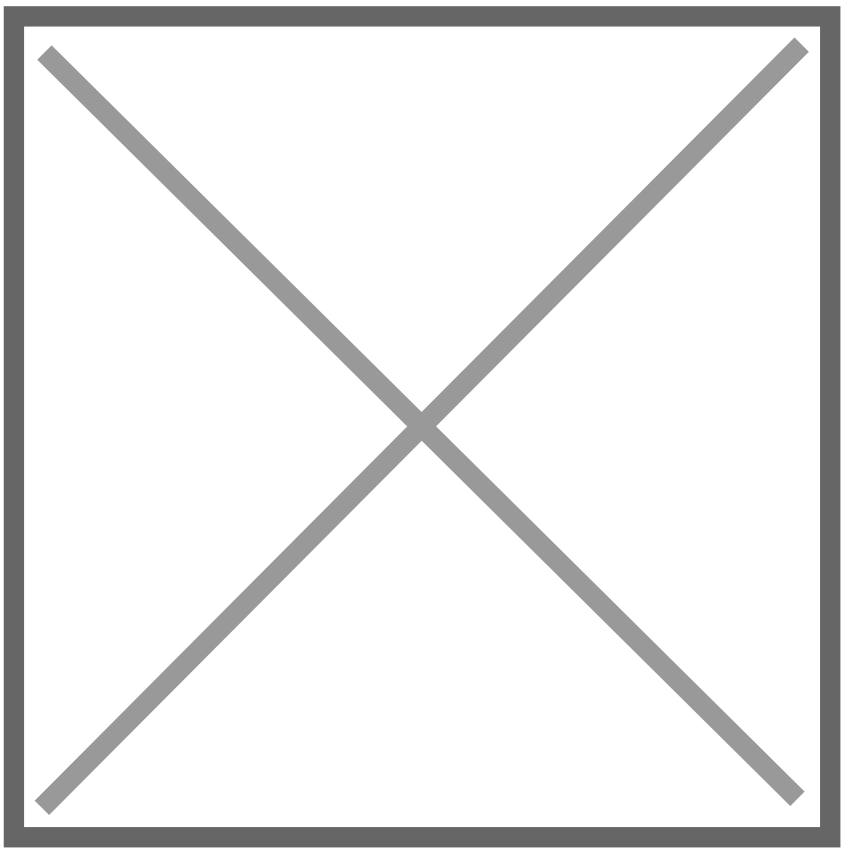
Wireshark

Wireshark is an open-source packet analyzer which is widely used for network troubleshooting and traffic analysis.

You can download it from the official website https://www.wireshark.org/#download



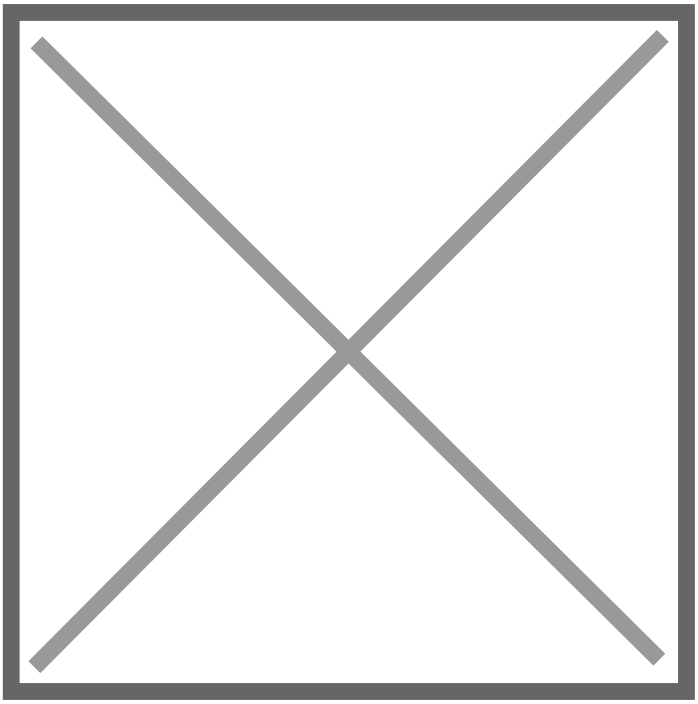
With Wireshark you can capture traffic on any of your available interfaces, you must be clear on what interface your traffic is working on.



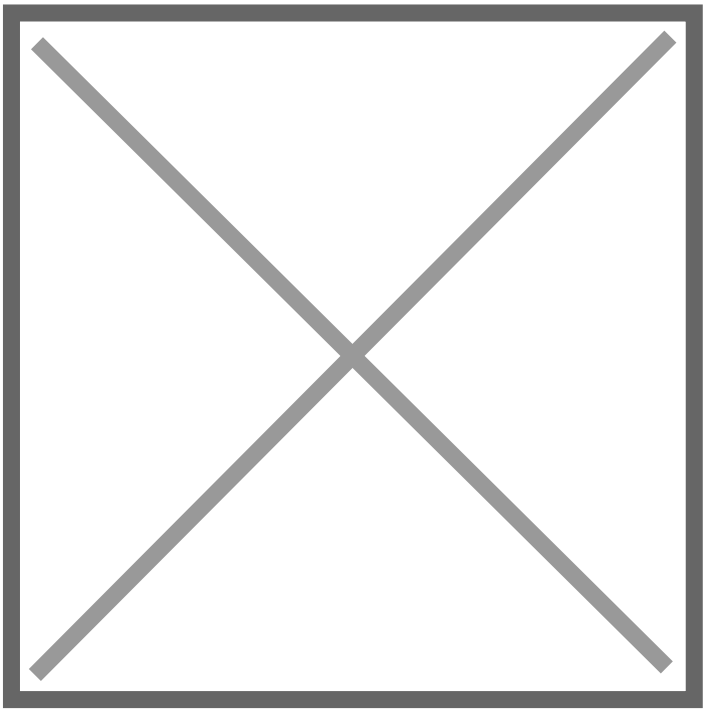
Its really recommended to apply filters to narrow down to show only the packets you are interested in.

Filters can work based on transport or application protocol, source or destination IP addresses, source or destination port, etc.

Its highly recommended that you set the view that you feel more comfortable, for example, I personally like to see the Source and Destination Port on the captures, this is easily modified right clicking on the column name and choose **Column Preferences**

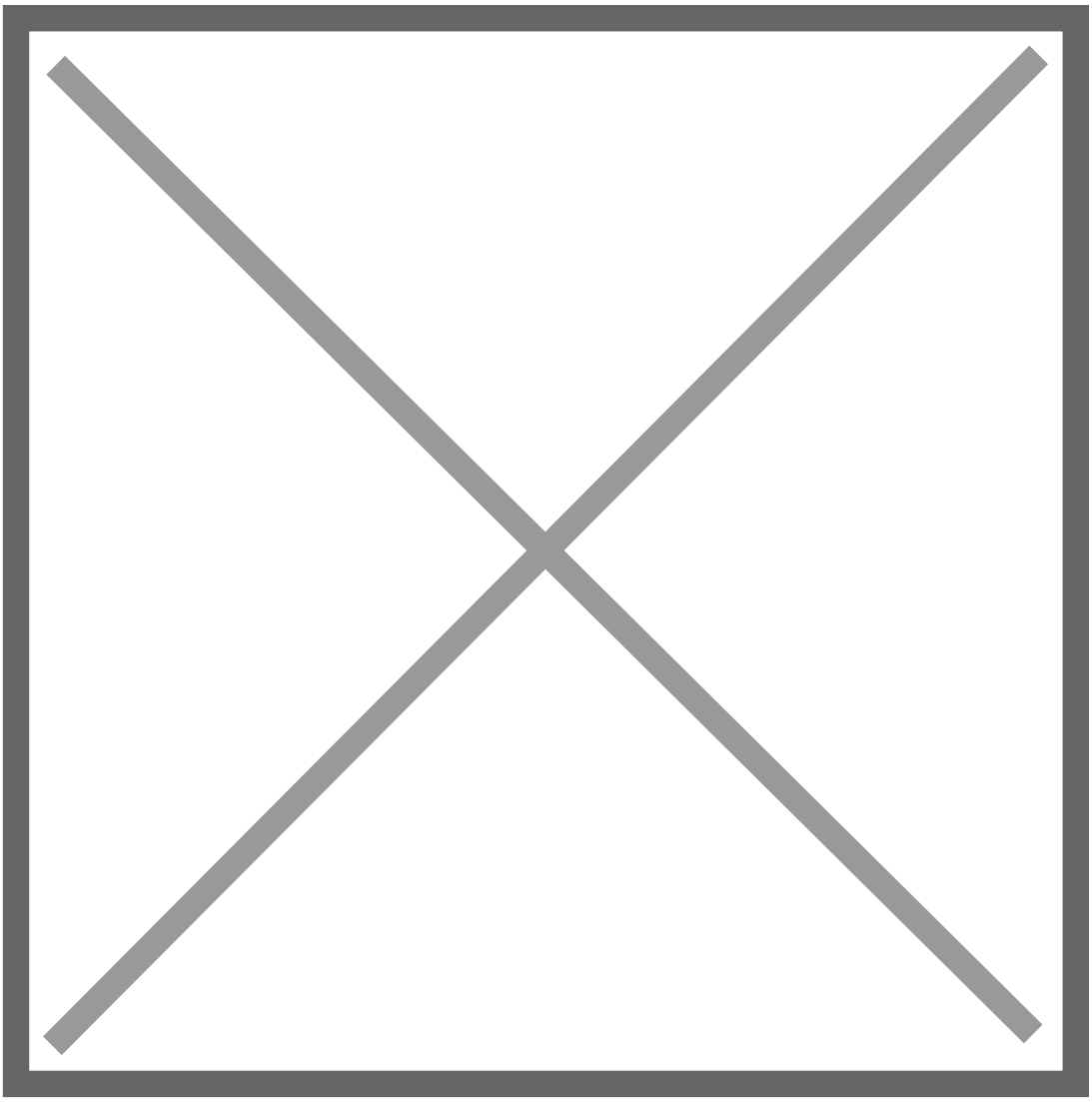


On Title set up the name you want to use to identify the column in the top and select the type to Destination port and Source port.

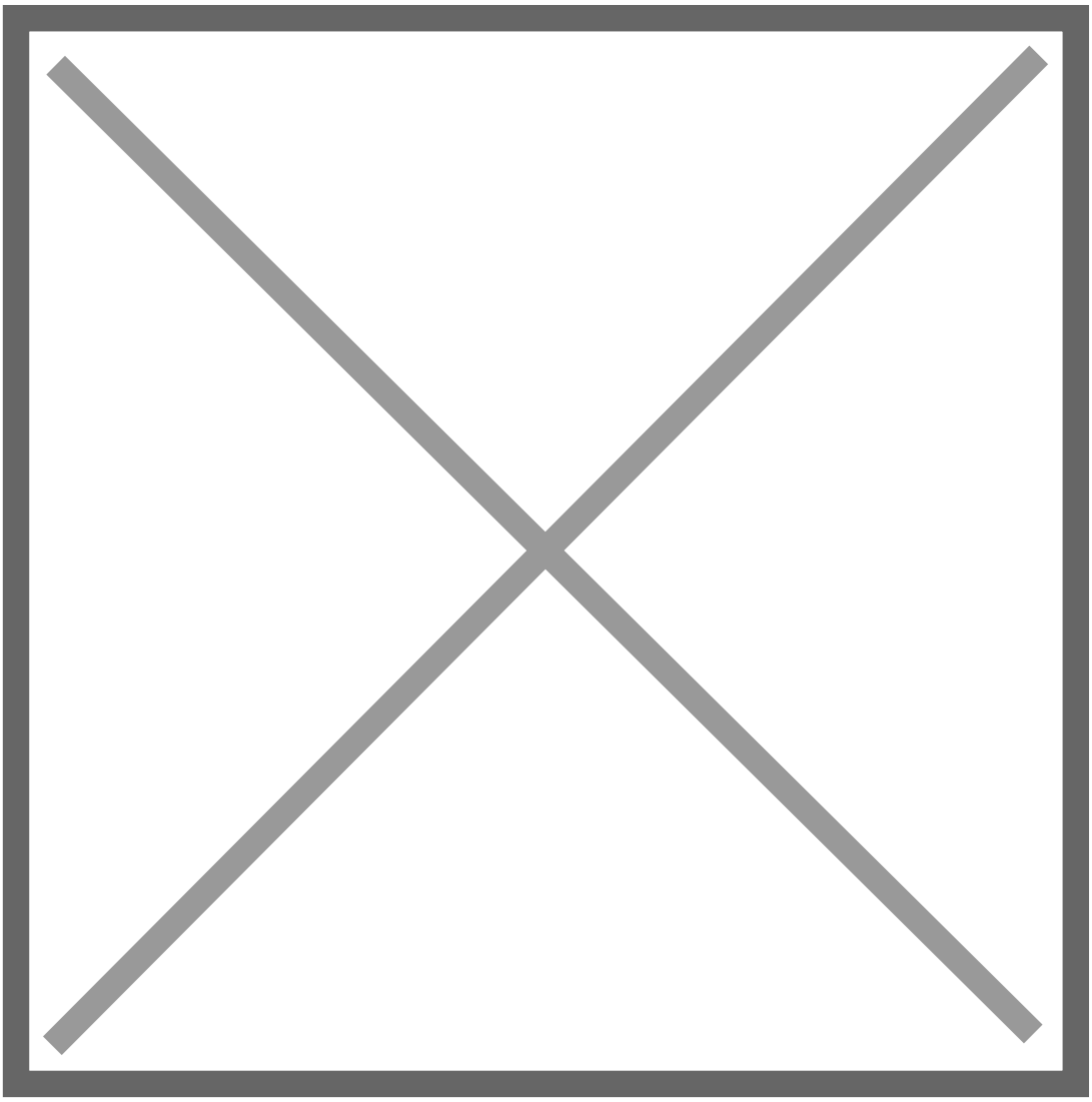


Other setting is also removing the Packet bytes in the bottom.

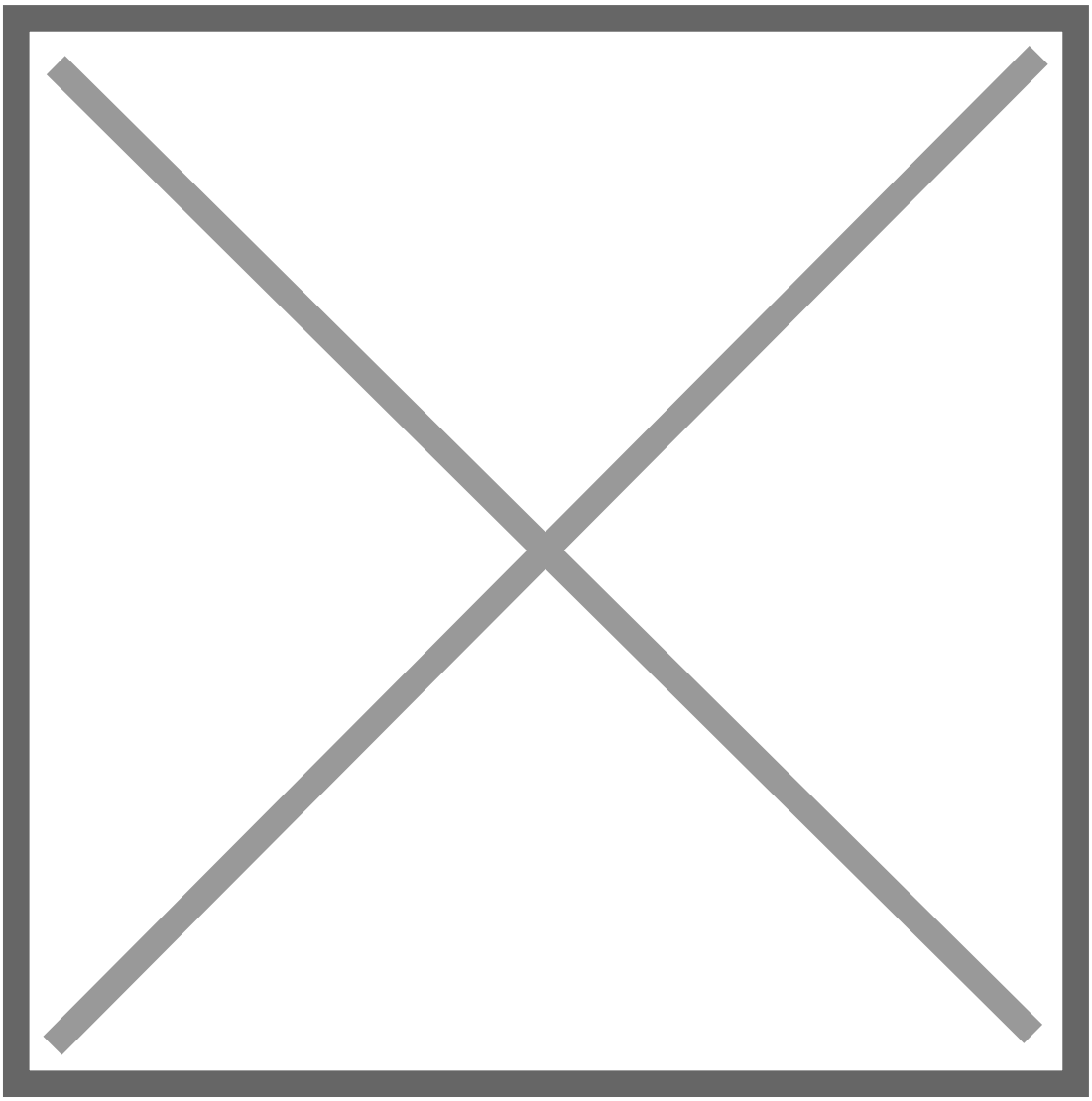
The filter toolbar lets you quickly edit and apply filters



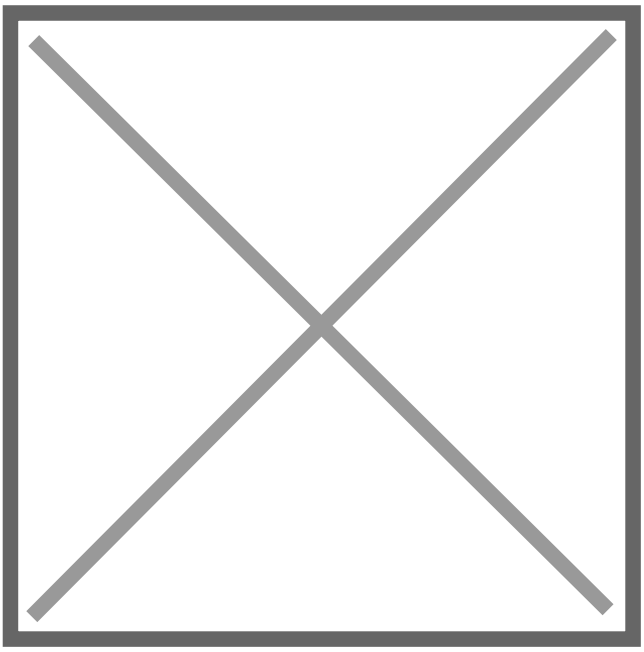
Filters can be combined and applied on the traffic for example:



Any error in the syntax of the filter will turn the background of the toolbar to red:



When saving your traffic you could choose to save only the traffic you filtered, you can use the option **Export Specified Packets** and select the **Displayed** option



Revision #1
Created 20 April 2023 16:43:55 by Cesar Gzz
Updated 2 May 2024 16:19:10 by Cesar Gzz