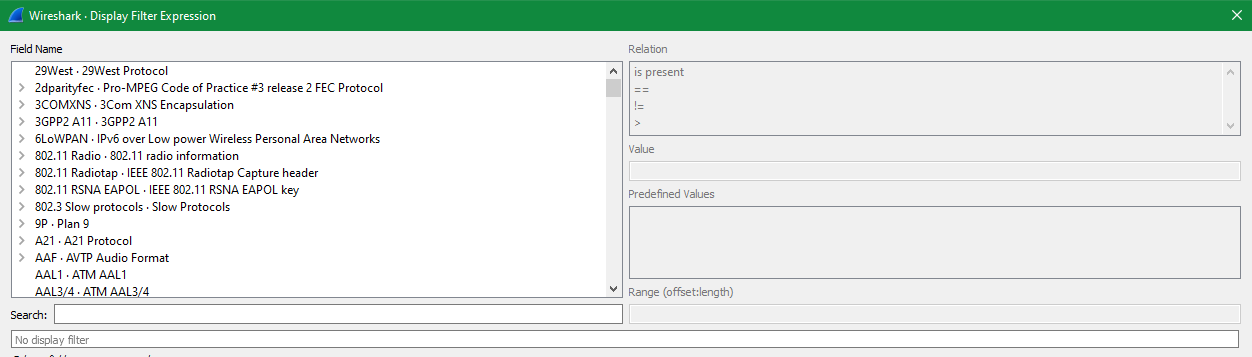
**LAB­­­­­ 8**

**WIRESHARK FILTERING (for Ethernet)**

In this lab you learn how to use filters for Ethernet in Wireshark.

1. Download the file **Capture1.pcapng** (PCAPNG = Packet Capture Next Generation) from Leho (module Wireshark-files) and open it by double clicking.
2. Please enter appropriate filters to answer the following questions. **Also, don't forget to write down the used filter expression for each question.** Each time you move on to a next question, you can clear the filter expression of the previous question unless otherwise mentioned.

Hint 1: When setting up, you can use the built-in “Display Filter Expression” by right-clicking in the filter box and selecting “Display Filter Expression”.



Hint 2: Use the built-in Wireshark manual pages (via Menu Help > Manual Pages > Wireshark Filter) for additional explanations and examples of filters.

1. Can ‘Ethernet II’ frames and ‘Ethernet 802.3’ frames be used on the same network? How many ‘Ethernet 802.3’ frames are in the capture file?

Hint: There is a specific protocol of a data link sublayer that is always used together with Ethernet 802.3 (see lecture slides). You can filter on that protocol

1. How many frames were sent from a device with MAC address 78:45:c4:42:26:71?

eth.src==78:45:c4:42:26:71

3549 packets

1. How many frames were exchanged between the devices with MAC addresses 78:45:c4:42:26:71 and 00:8e:73:88:a8:c8?

eth.addr==78:45:c4:42:26:71 and eth.addr == 00:8e:73:88:a8:c8

19002 packets

Hint: you can check this answer by studying statistical data from the capture via the menu Statistics > Conversations.

1. How many broadcast frames were sent?

eth.addr== ff:ff:ff:ff:ff:ff

10 frames

1. What is the packet number of the last multicast frame containing an IPv4 multicast packet?

Hint: See lecture slides about Ethernet for the form of such a multicast address.

ip.addr >= 224.0.0.0

packet number 13100

1. How many frames were sent from a Cisco device?

Hint: use the OUI and Wireshark built in OUI resolving to manufacturers!

eth.src.oui\_resolved contains "Cisco"

15487 frames

1. How many IPv6 packets were sent?

Hint: use the type field (cfr lecture slides about Ethernet for the value of this field).

Ipv6

19 packets

Hint: you can also check this answer by looking at statistical data about this capture!