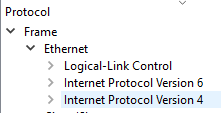
**LAB 10**

**IP PACKETS**

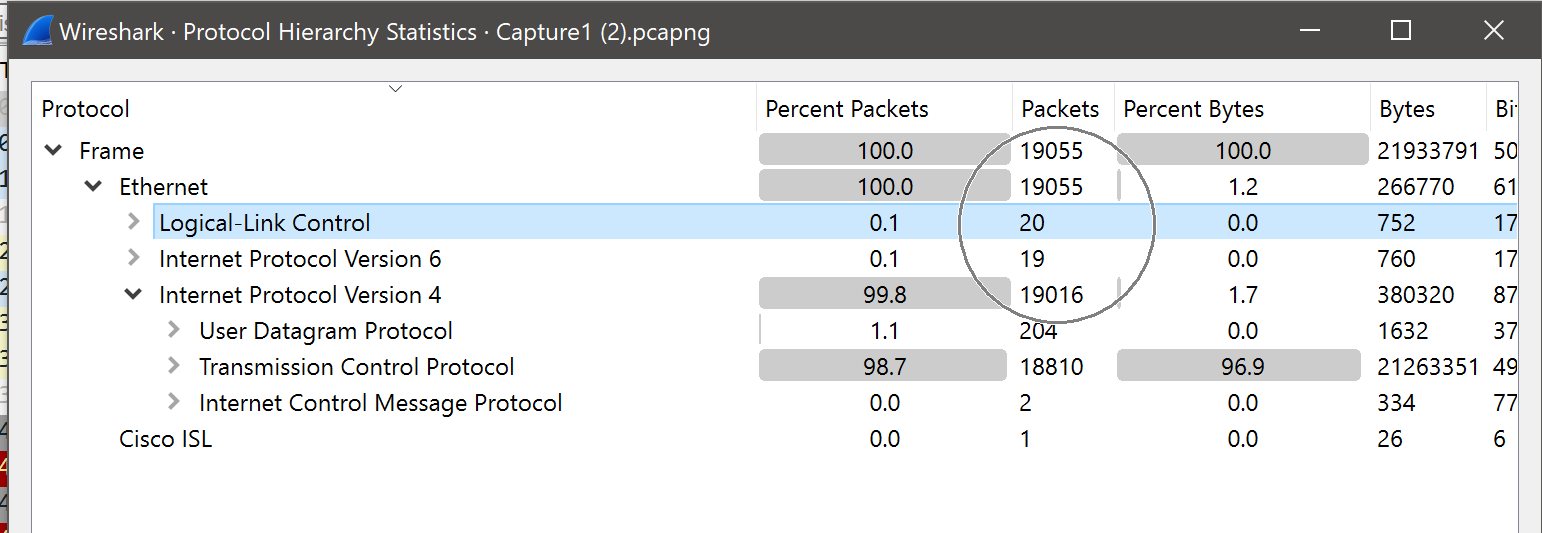
1. Download the file **Capture1.pcapng** (PCAPNG = Packet Capture Next Generation) from Leho (module Wireshark-files) and open it by double clicking.
2. Not all Ethernet packets in this capture file are IP packets. You can quickly see this by clicking on *Protocol Hierarchy* in the *Statistics* menu and then closing/collapsing the items under *Ethernet* until you get the following tree:



How many frames do not contain IP packets?

20 frames

Paste below a screenshot of the window where you found this info and mark this number.



1. Close this window and return to your capture file. Now enter a filter that allows you to display only the frames that do not contain IP packets.

not ip and not ipv6

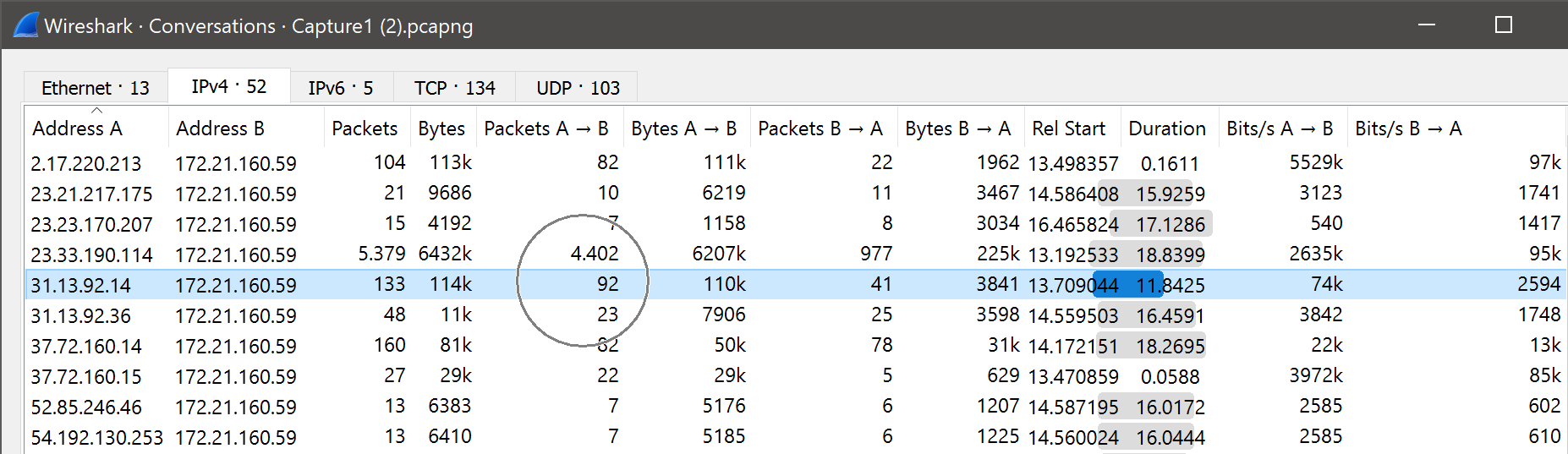
1. Which filter do you need to enter to see how many IPv4 packets were sent by the device with IPv4 address 31.13.92.14?

ip.src==31.13.92.14

So how many packets like that are there?

92 packets

You can also find this number by requesting statistical information about the capture file. Paste below a screenshot of the window where you found this info and mark this number.



1. How many routers can frame number 100 pass before it will no longer be forwarded?

128 (Time to Live)

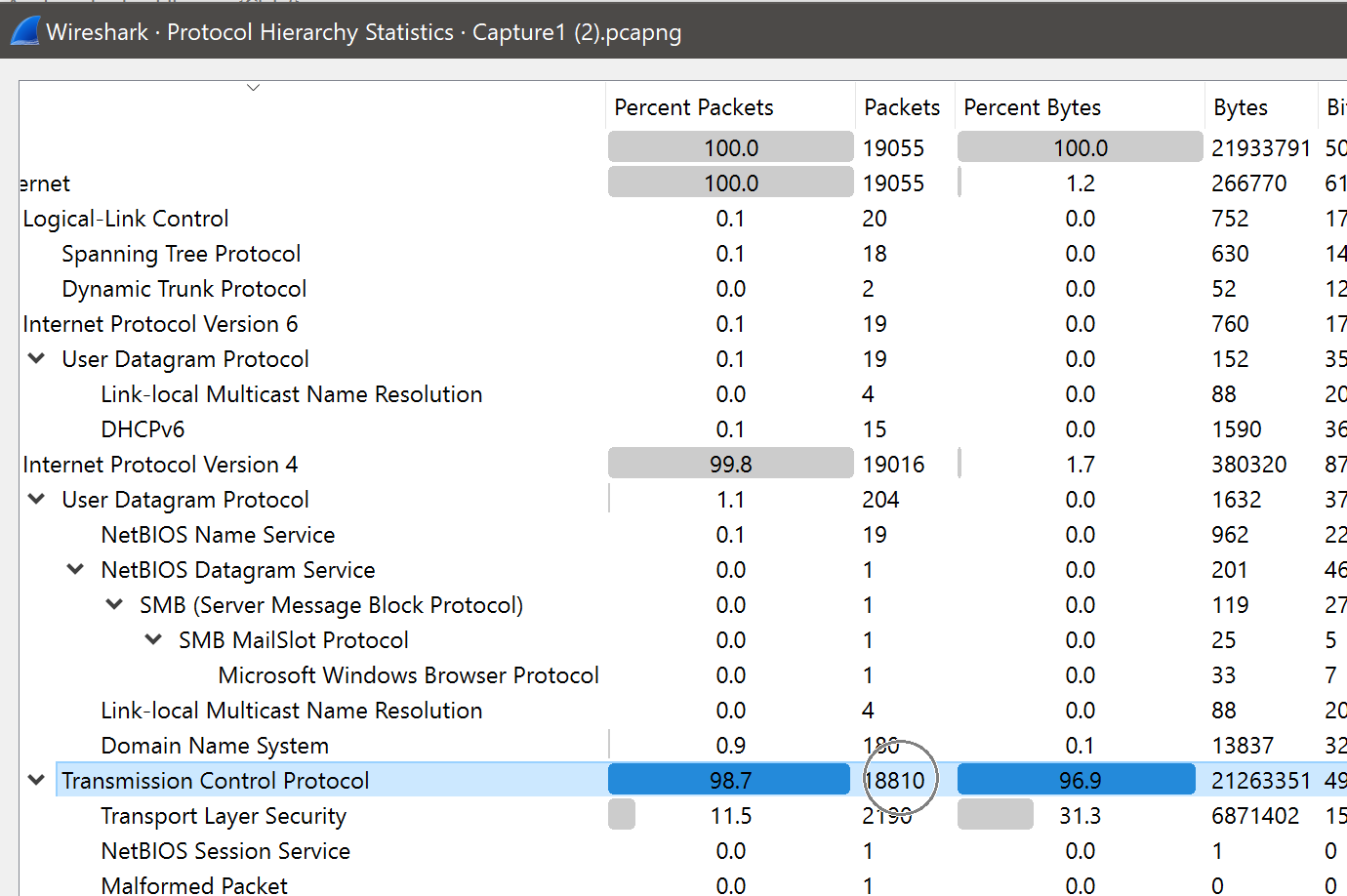
1. What filter do you need to enter to keep only the IP packets that are carrying the TCP protocol (more on TCP in another lecture)?

tcp

How many of these packets did you find?

18810

You can also find this number via statistical info. Paste below a screenshot of the window in which you found it and mark the requested number.



1. Show the UDP packets from the capture file by simply entering *UDP* as a filter expression (more on UDP in another lecture).

Check the filtered packets to determine the value of the protocol field of the UDP packets’ IP header and write down that value below.

17