**Lab Exercise – UDP & TCP**

**UDP:**

**Capture a UDP Trace:**

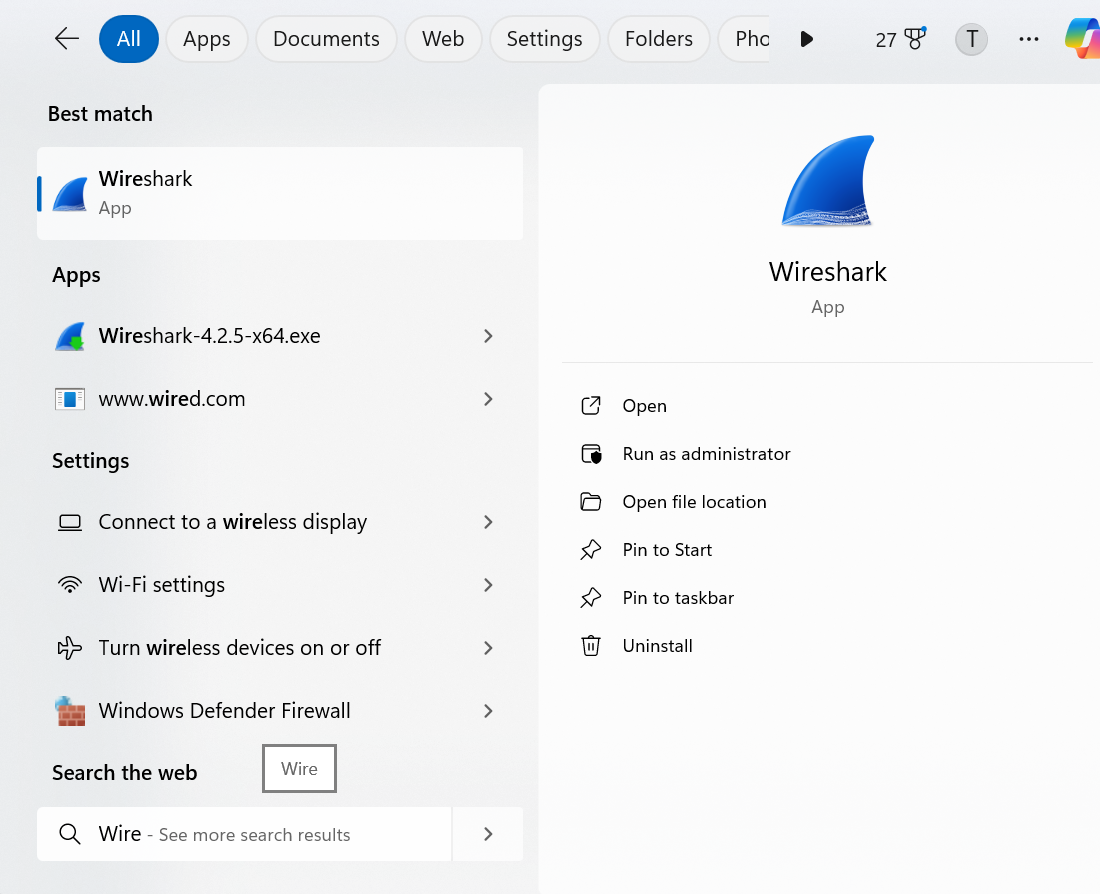
****

Figure 1: Starting Wireshark

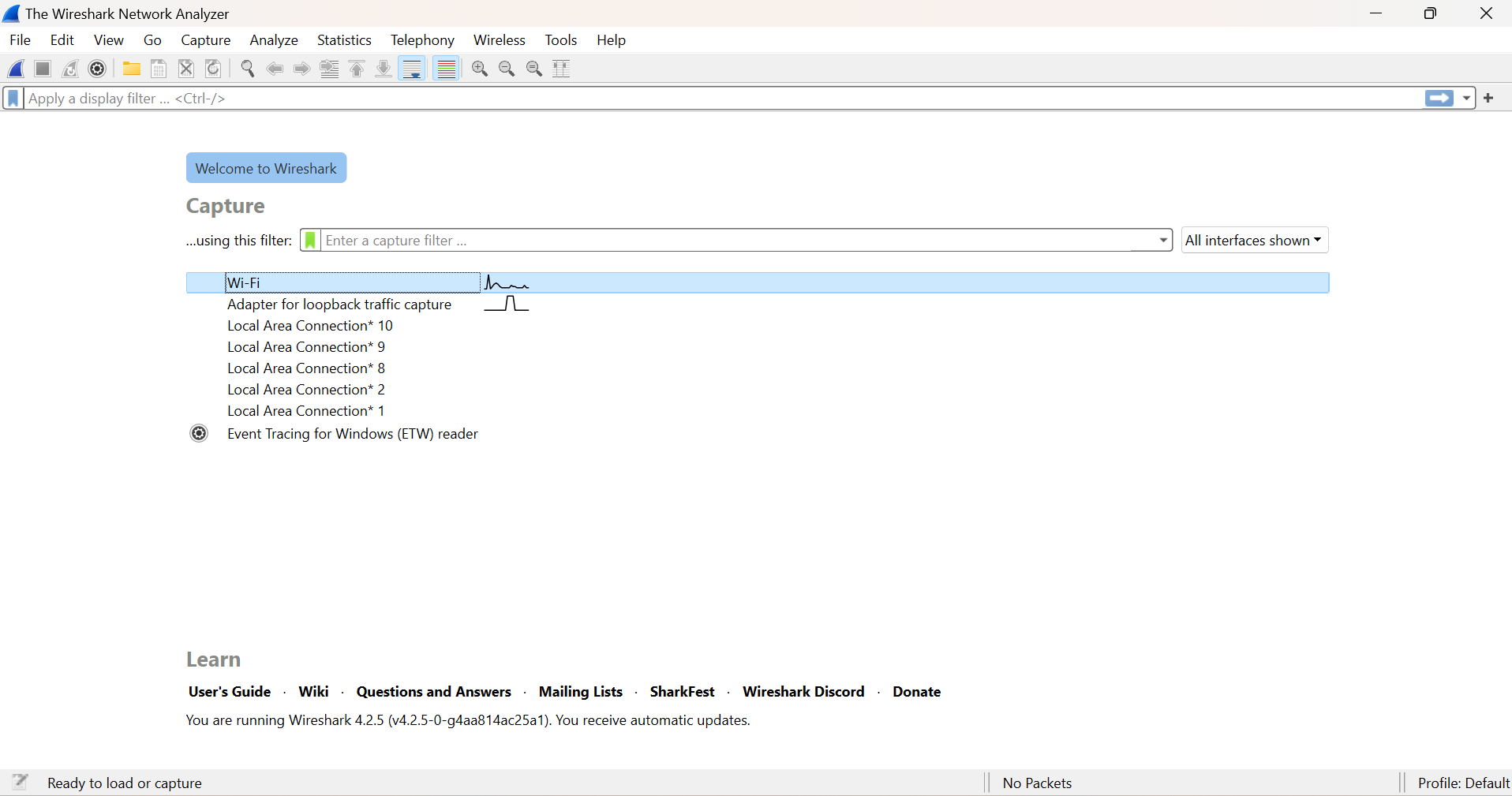
****

Figure 2: Selecting the Ethernet Interface

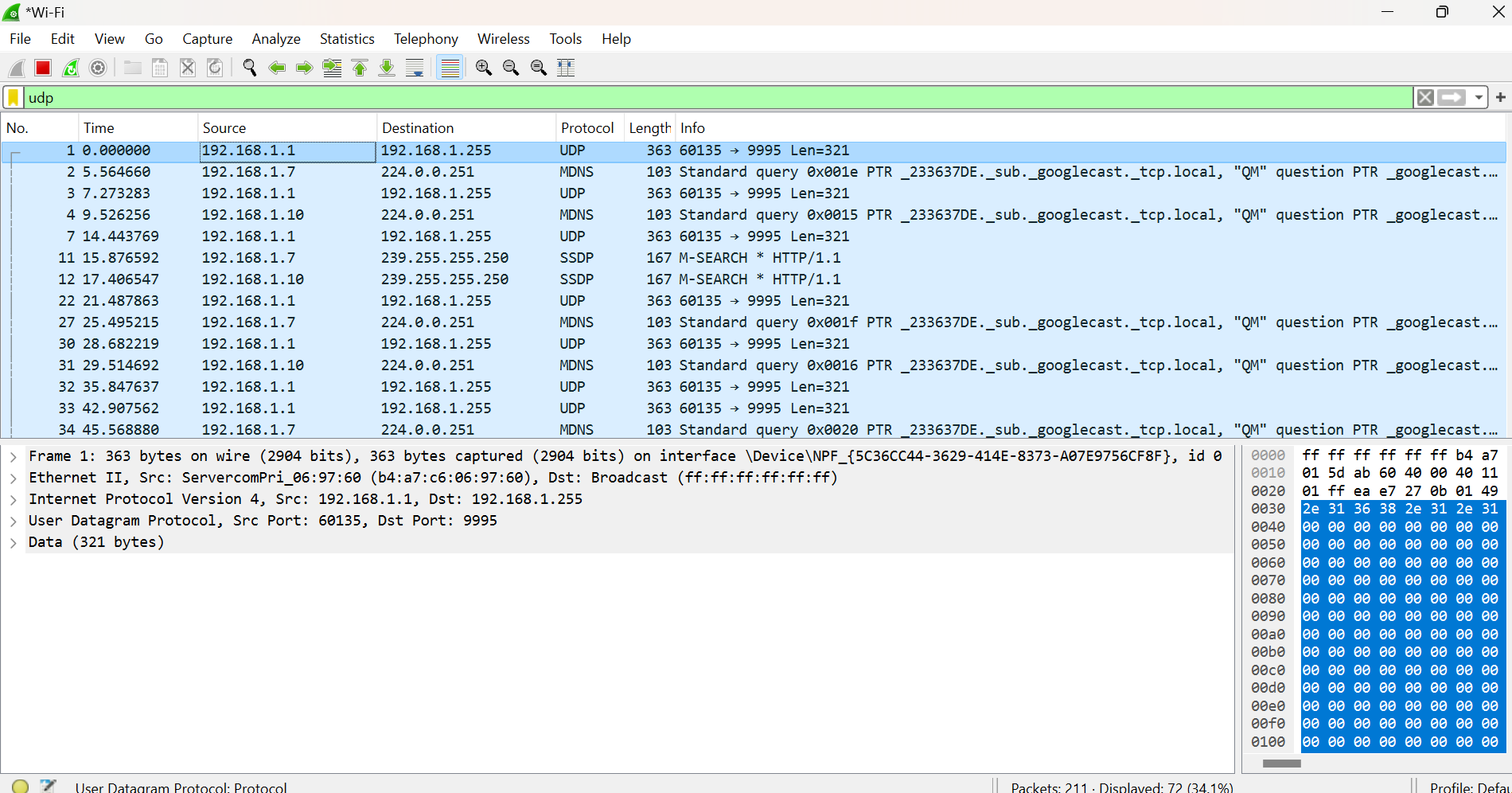
****

Figure 3: Setting up the capture options

When the capture is started, it will collect UDP traffic automatically

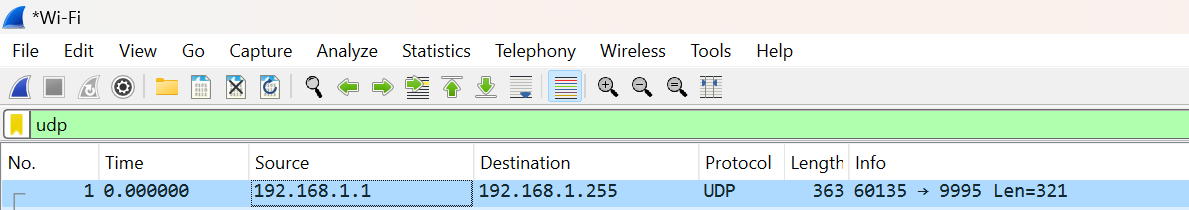


Figure 4: Stopping the capture

**TCP:**

**Open the Trace:**

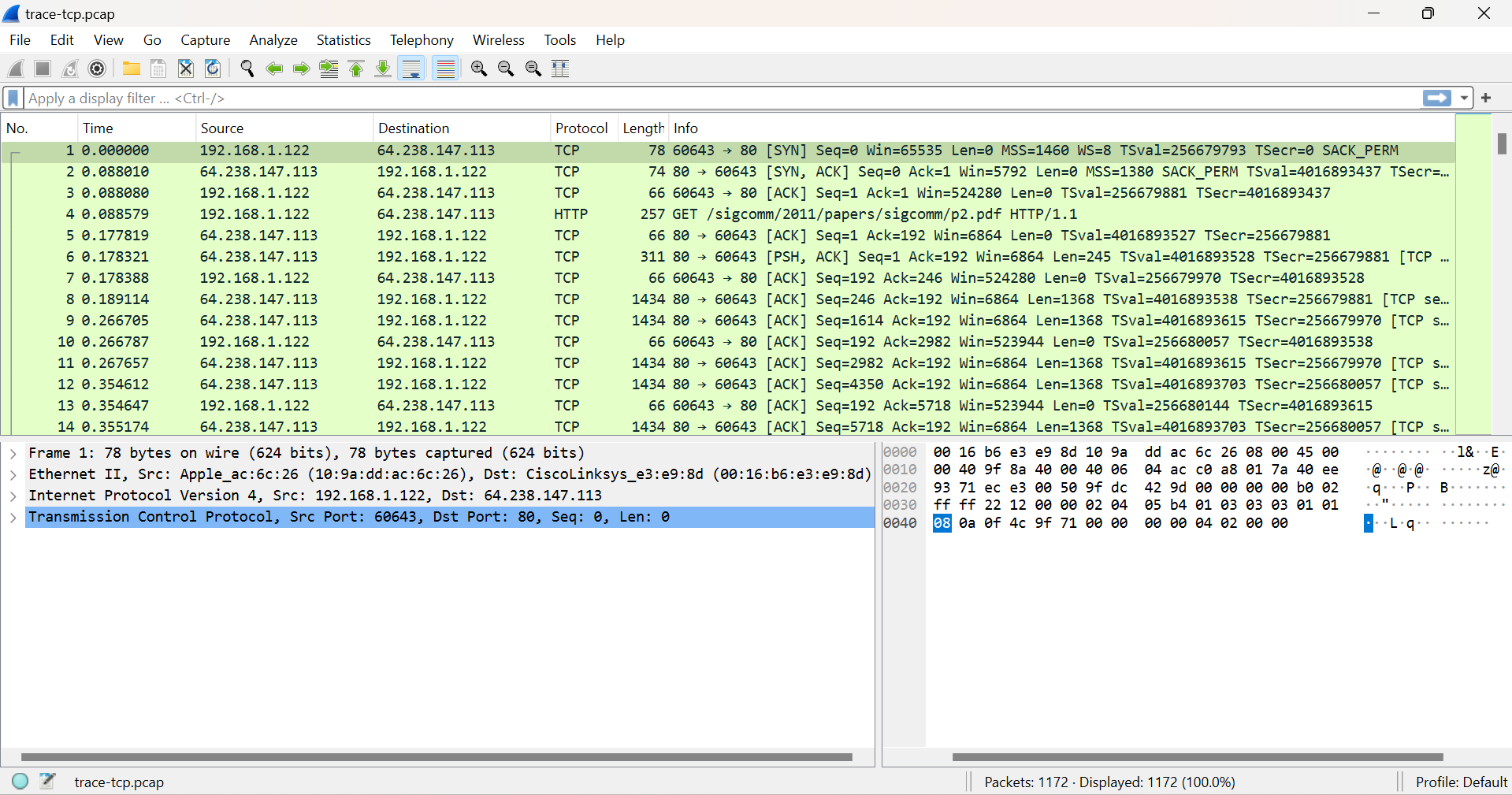
****

Figure 5: Selecting the Ethernet Interface

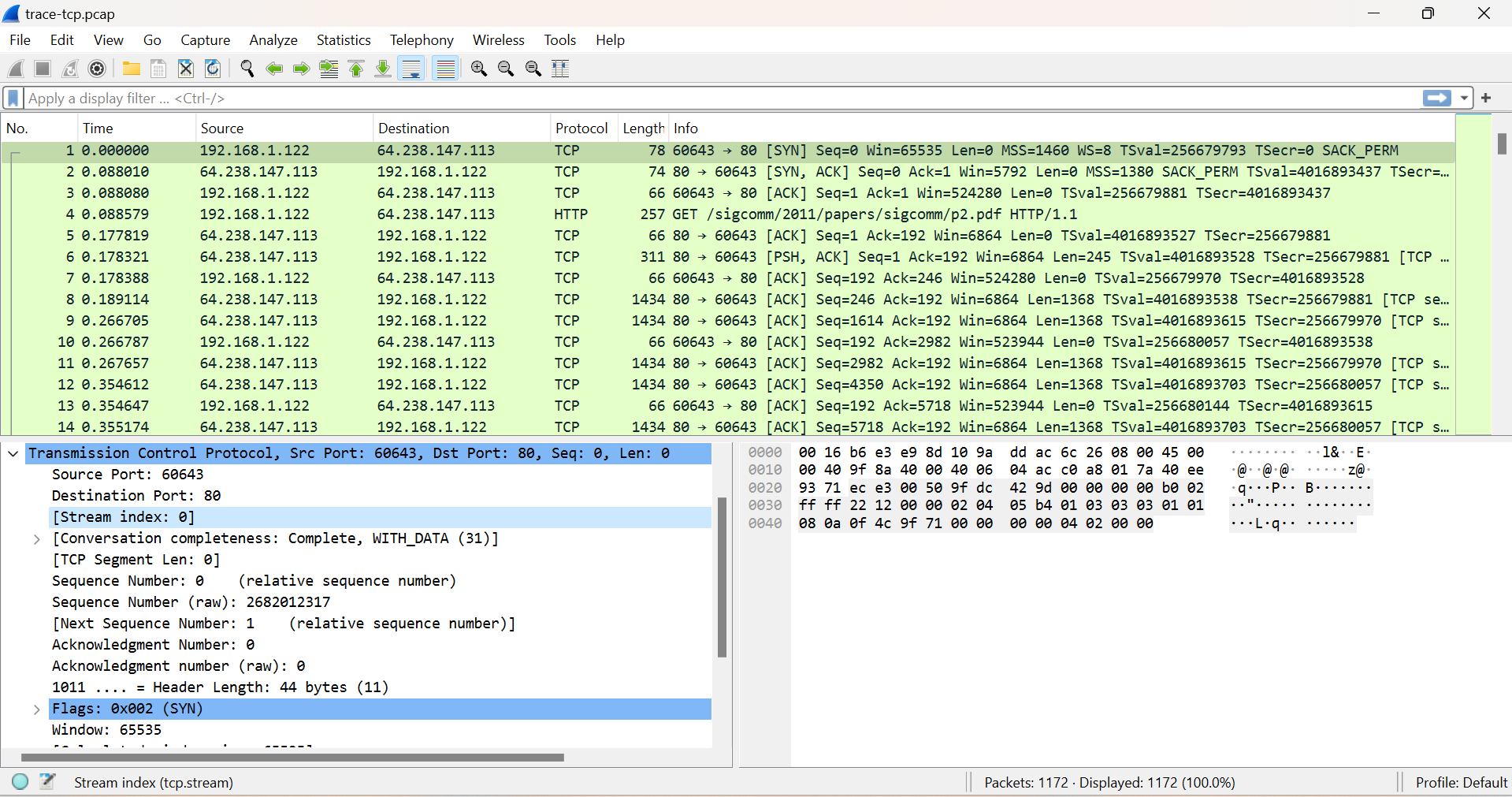


Figure 6: Examining the size of segments

**TCP Connection Setup/Teardown:**

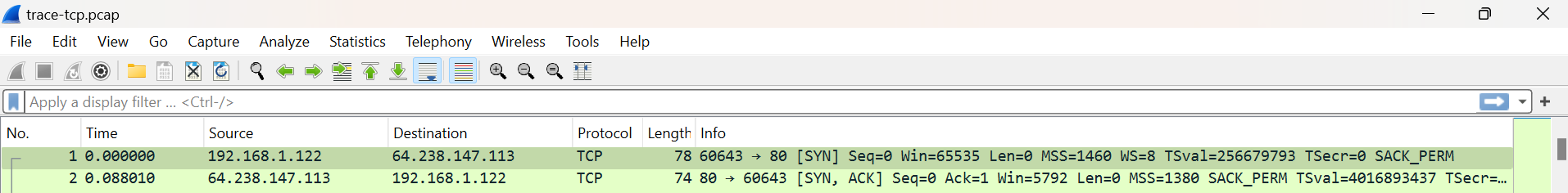
****

Figure 9: Selecting a TCP segment with SYN flag

The SYN flag is noted in the Info column. You can also search for packets with the SYN flag on using the filter expression “tcp.flags.syn==1”. (See below)

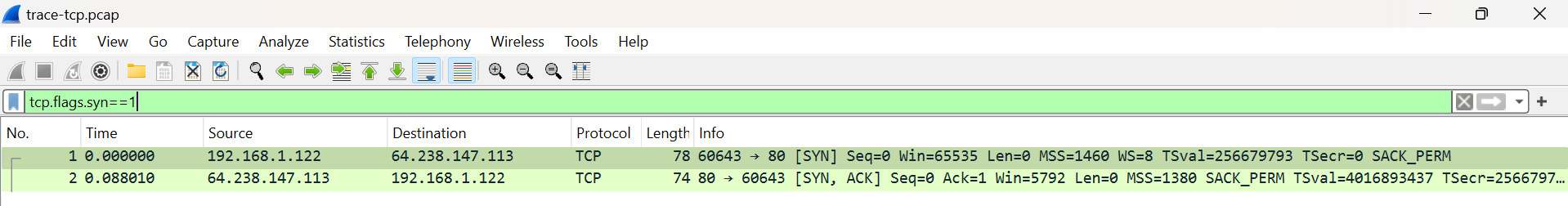
****

Figure 7: Selecting a TCP segment with SYN flag on

**TCP Connection Setup/Teardown:**

Next, we wish to clear the display filter tcp.flags.syn==1 so that we can once again see all the packets in our original trace. Do this by clearing the display filter as shown below.

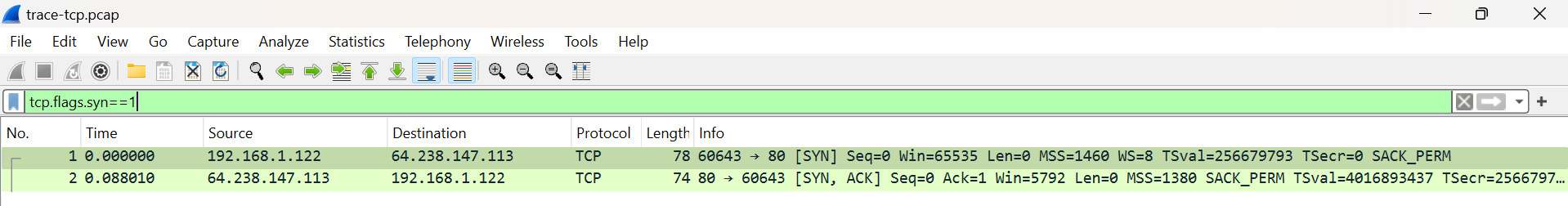
****

Figure 8: Clearing the display filter TCP segment with SYN flag on

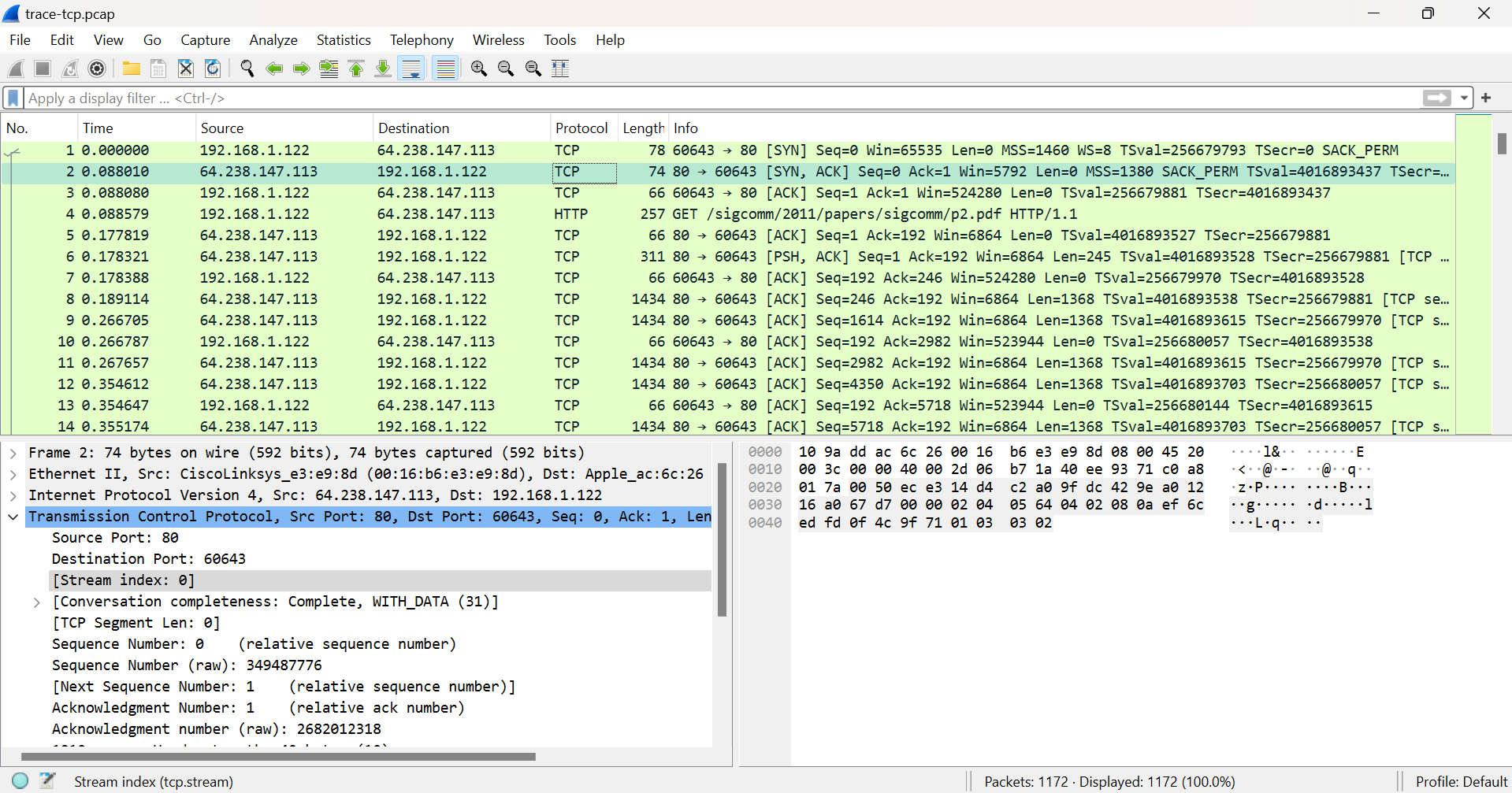
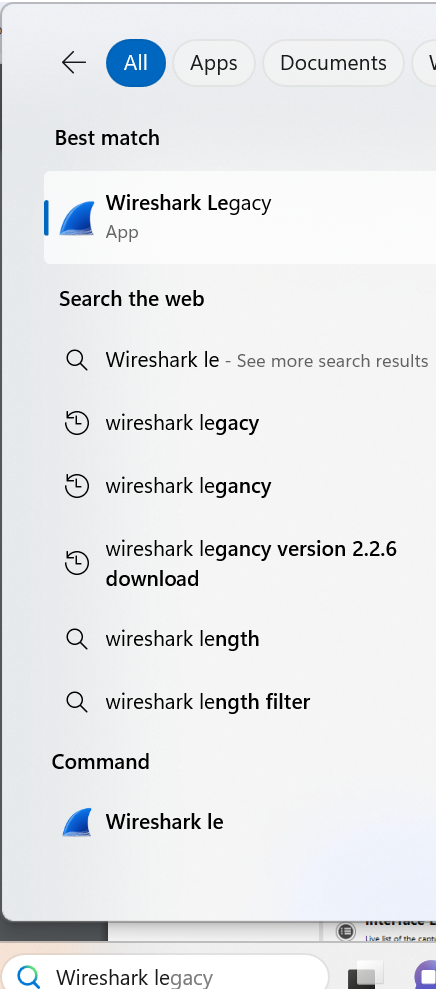
****

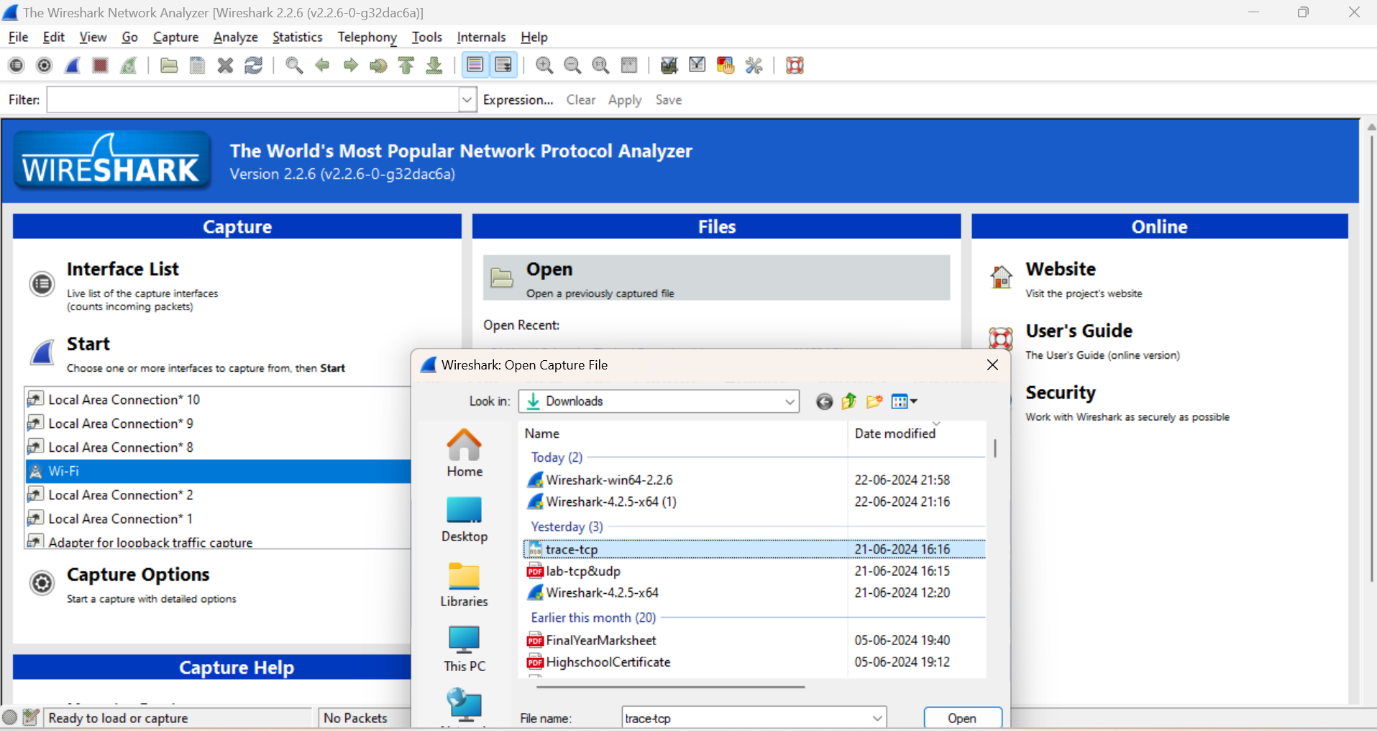
Figure 9: Viewing the complete trace

**TCP Data Transfer:**

For this part, we are going to launch an older version of Wireshark called Wireshark legacy. You do this by selecting the Wireshark legacy application as follows.

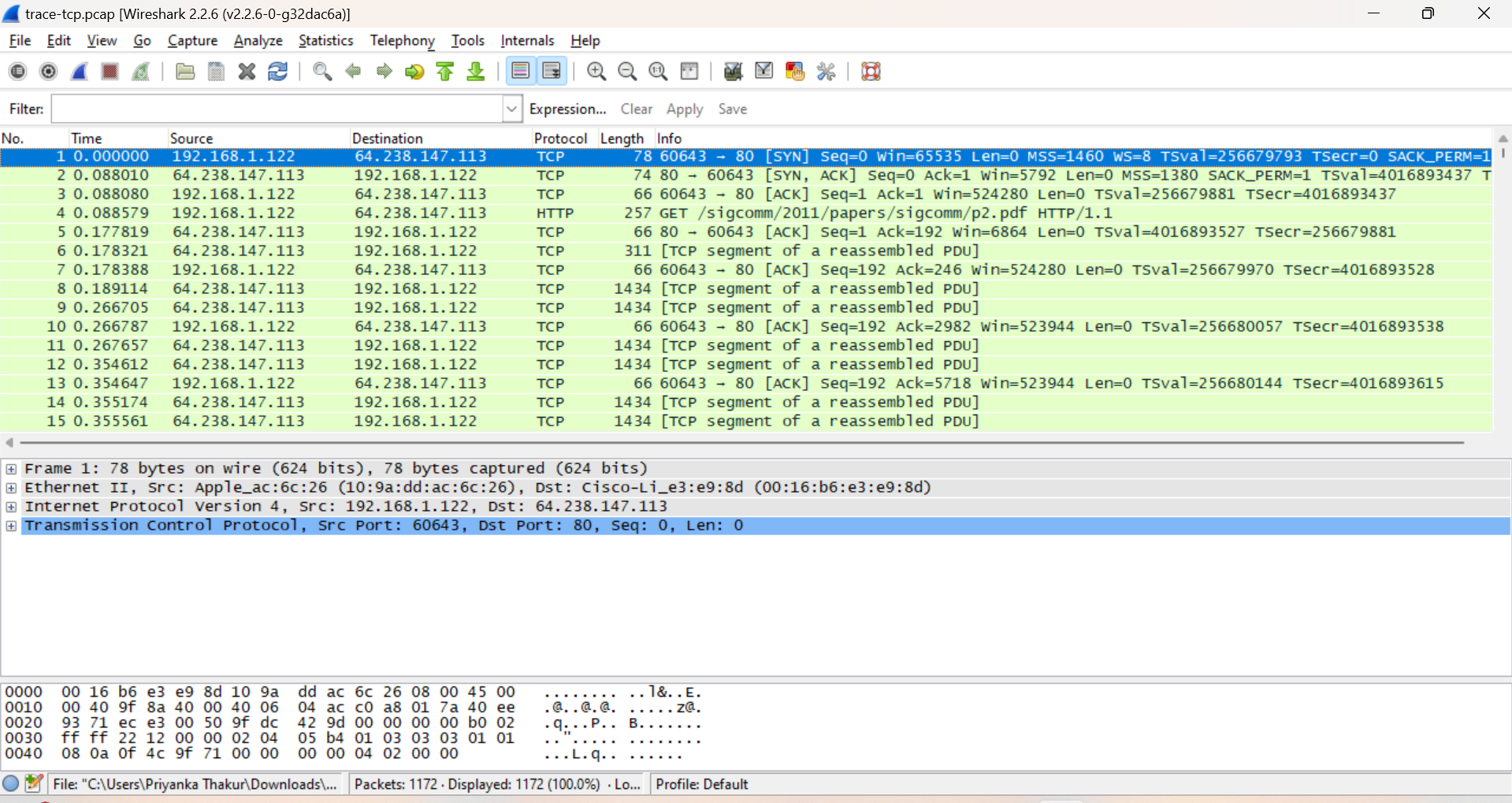
****

When it launches, you should open the trace-tcp file which is in your downloads folder from earlier.





You should then be presented with the same trace-tcp as used previously in this exercise



The middle portion of the TCP connection is the data transfer, or download, in our trace. This is the main event. To get an overall sense of it, we will first look at the download rate over time.

Under the Statistics menu select an “IO Graph” (as shown below).

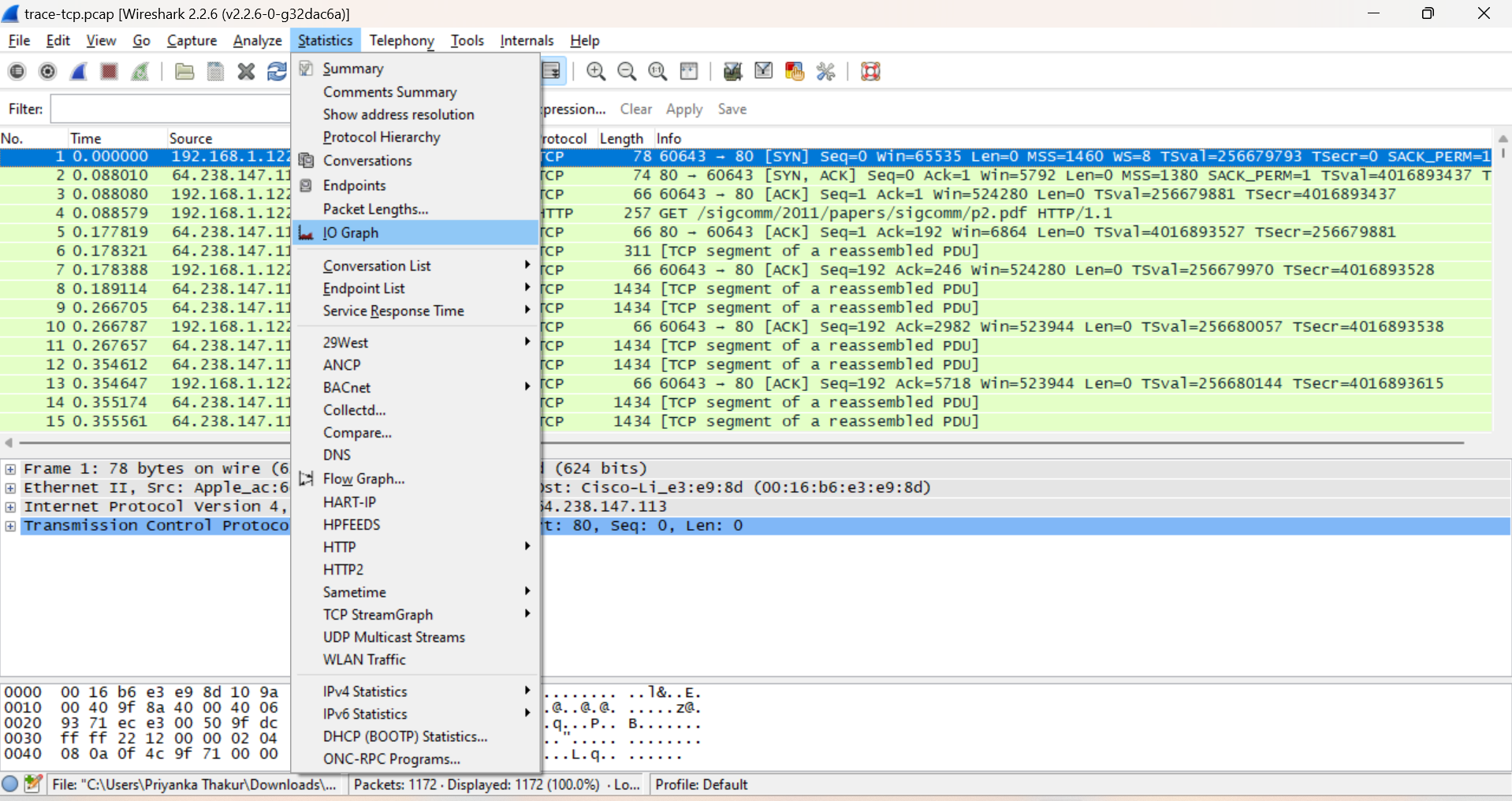


Figure 13: Opening an IO graph

You should end up with a graph like below. By default, this graph shows the rate of packets over time. You might be tempted to use the “TCP Stream Graph” tools under the Statistics menu instead. However, these tools are not useful for our case because they assume the trace is taken near the computer sending the data; our trace is taken near the computer receiving the data.

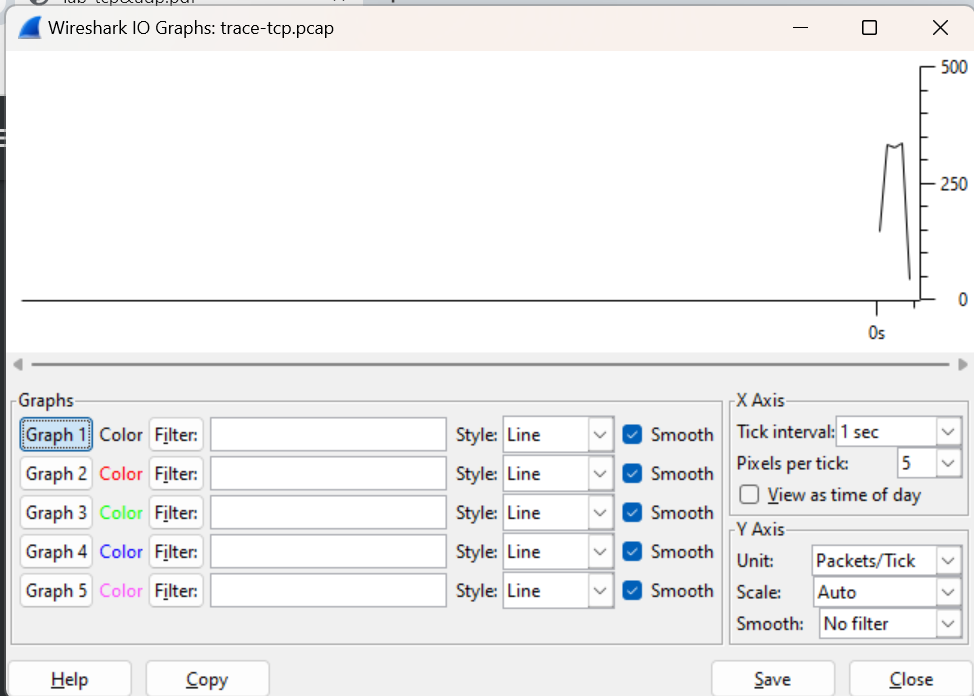
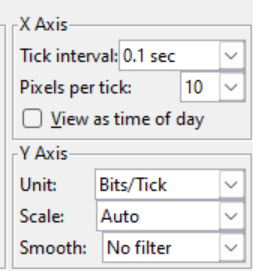
****

Figure 14: The IO graph

Now we will tweak it to show the download rate with the changes given below

****

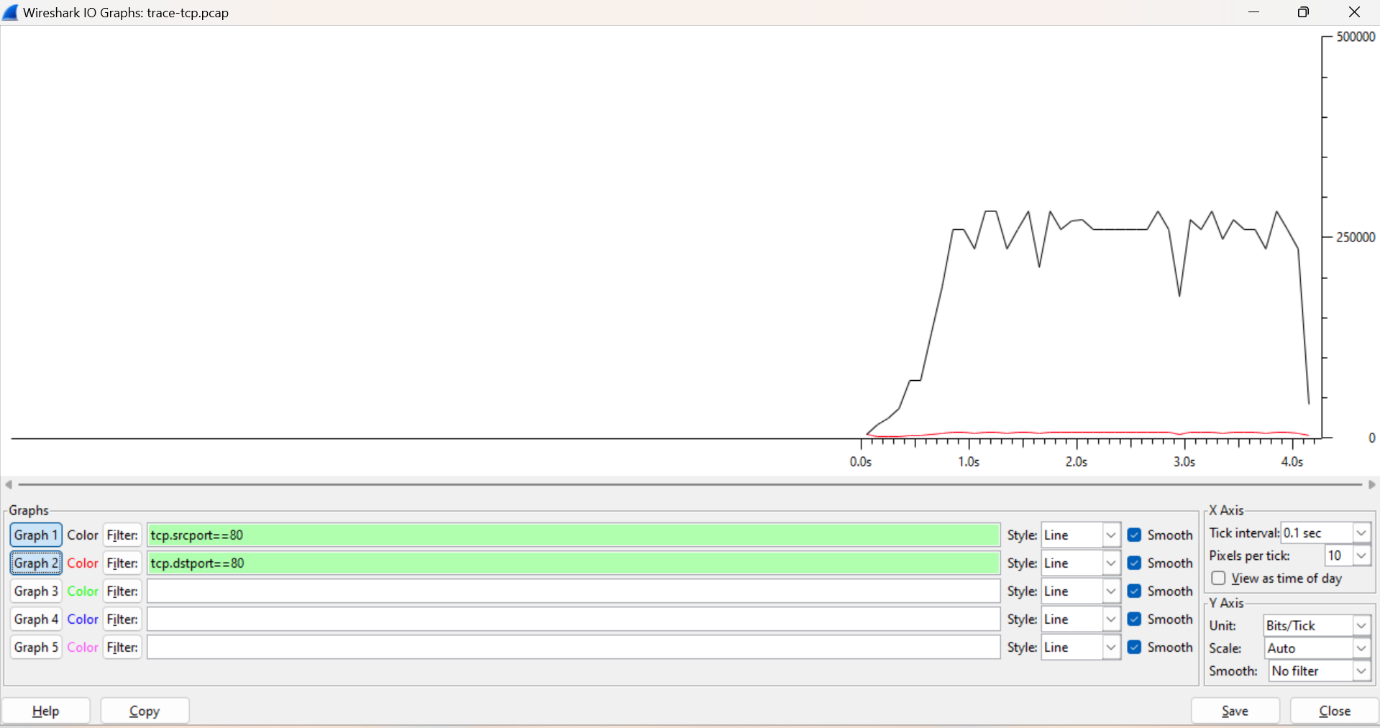
****

Figure 16: TCP download rate over time via an IO graph