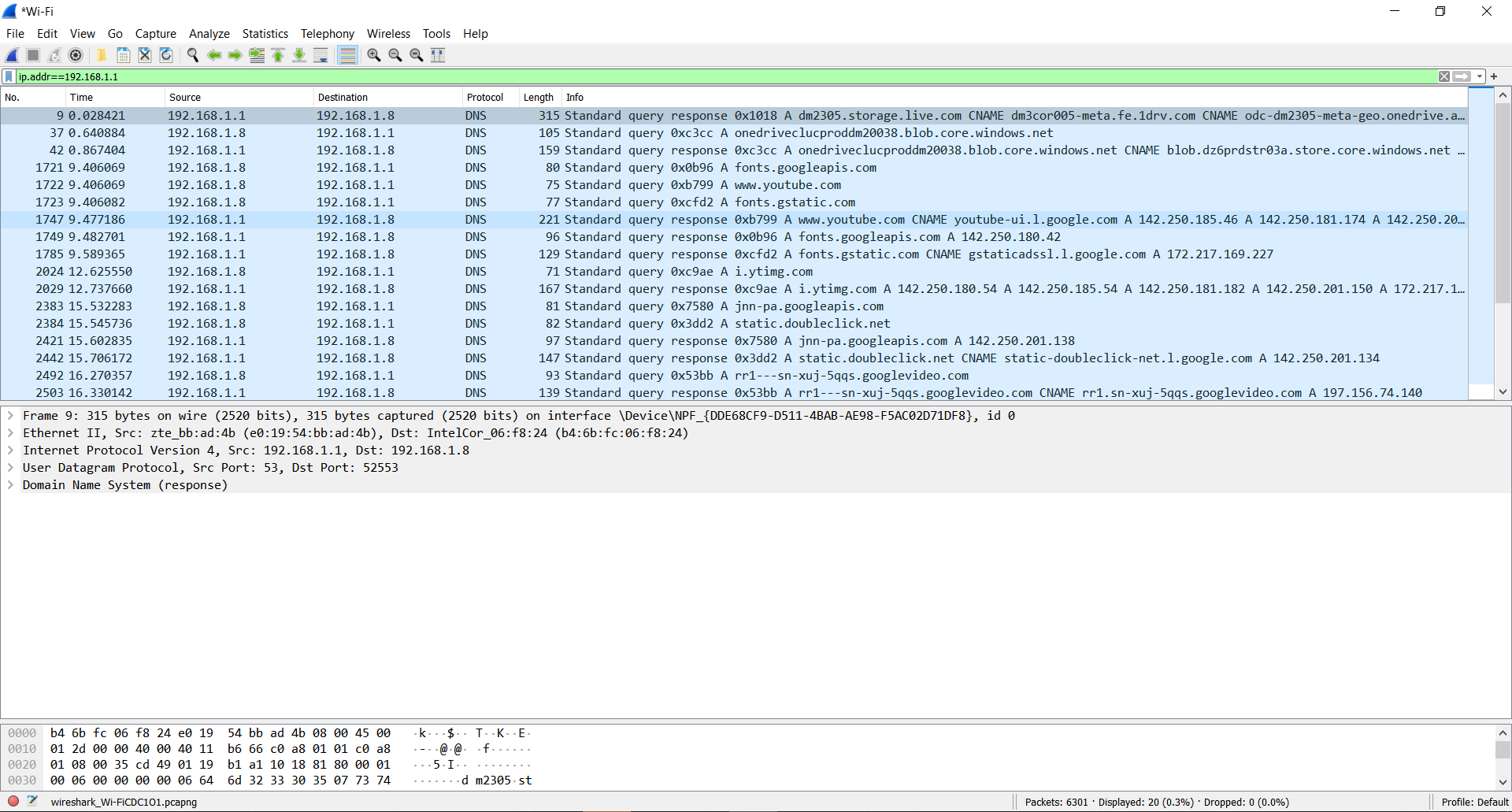
**Task 1. Capture packets when “pinging” another computer. Understand how ping**

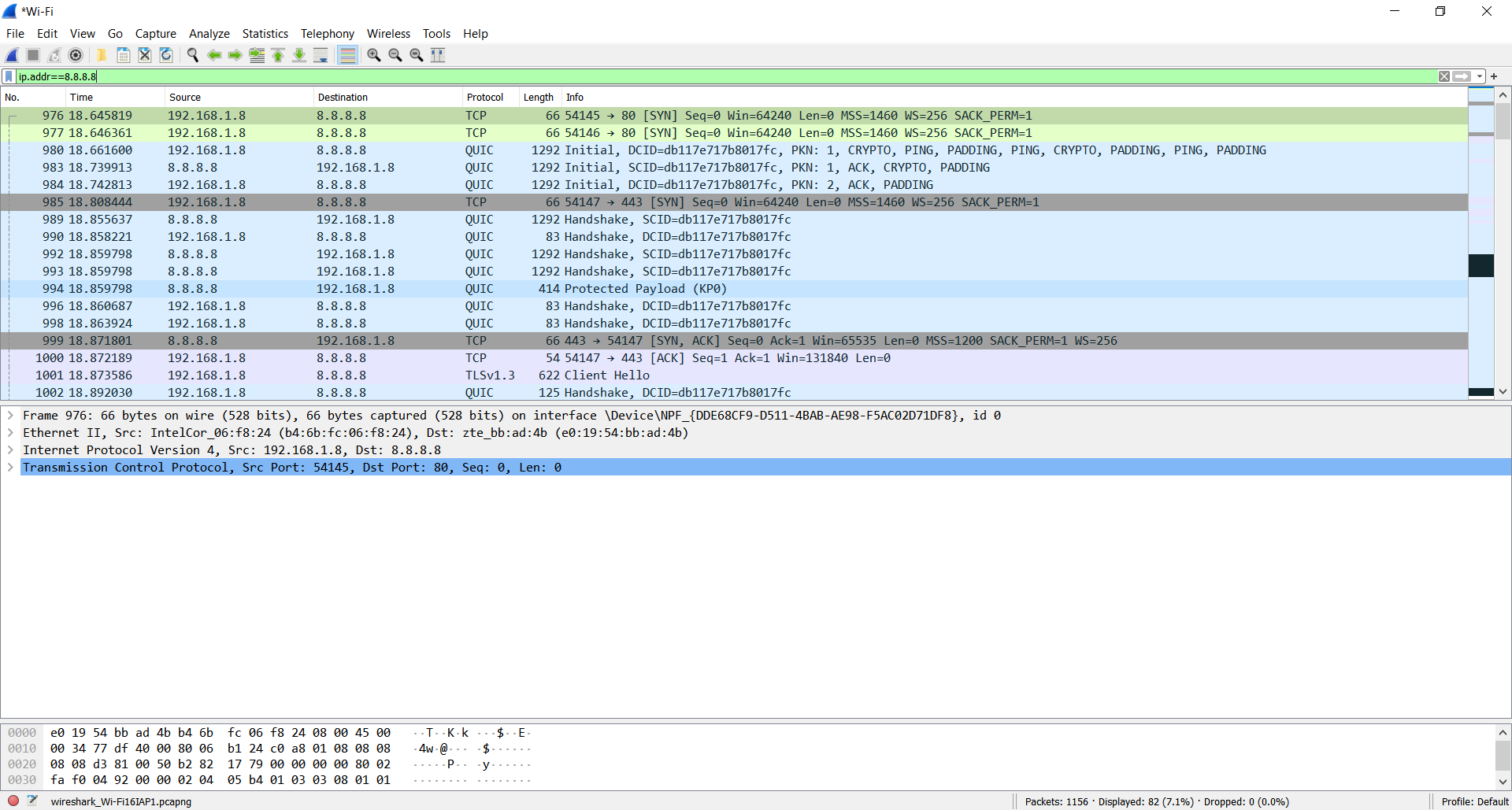
**works from the packet capture.**



**Task 2. Capture packets transferred while browsing a selected website (e.g. a page from**

**the course website, a search engine home page). Investigate the protocols used in each**

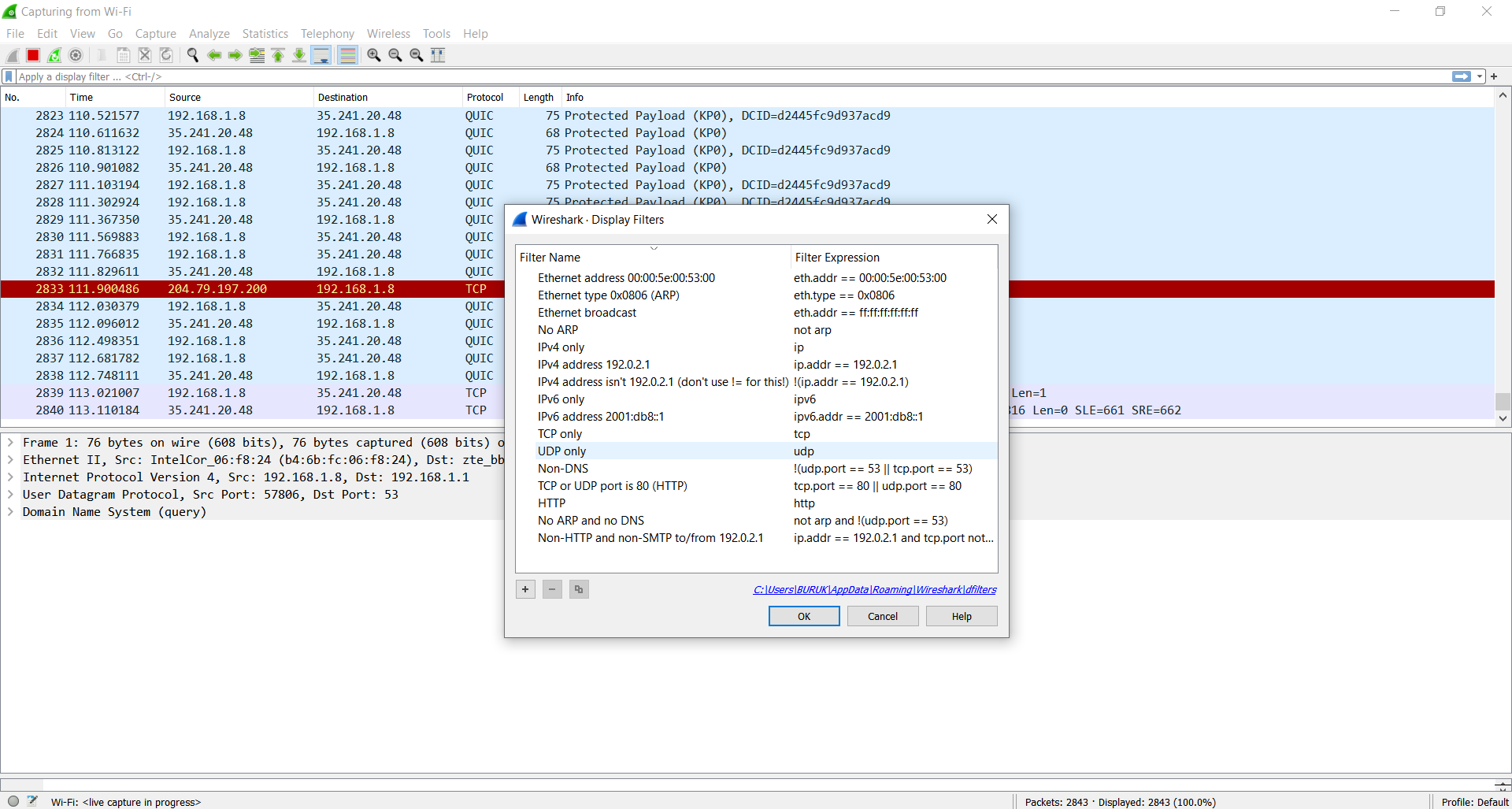
**packet, the values of the header fields and the packet sizes.**



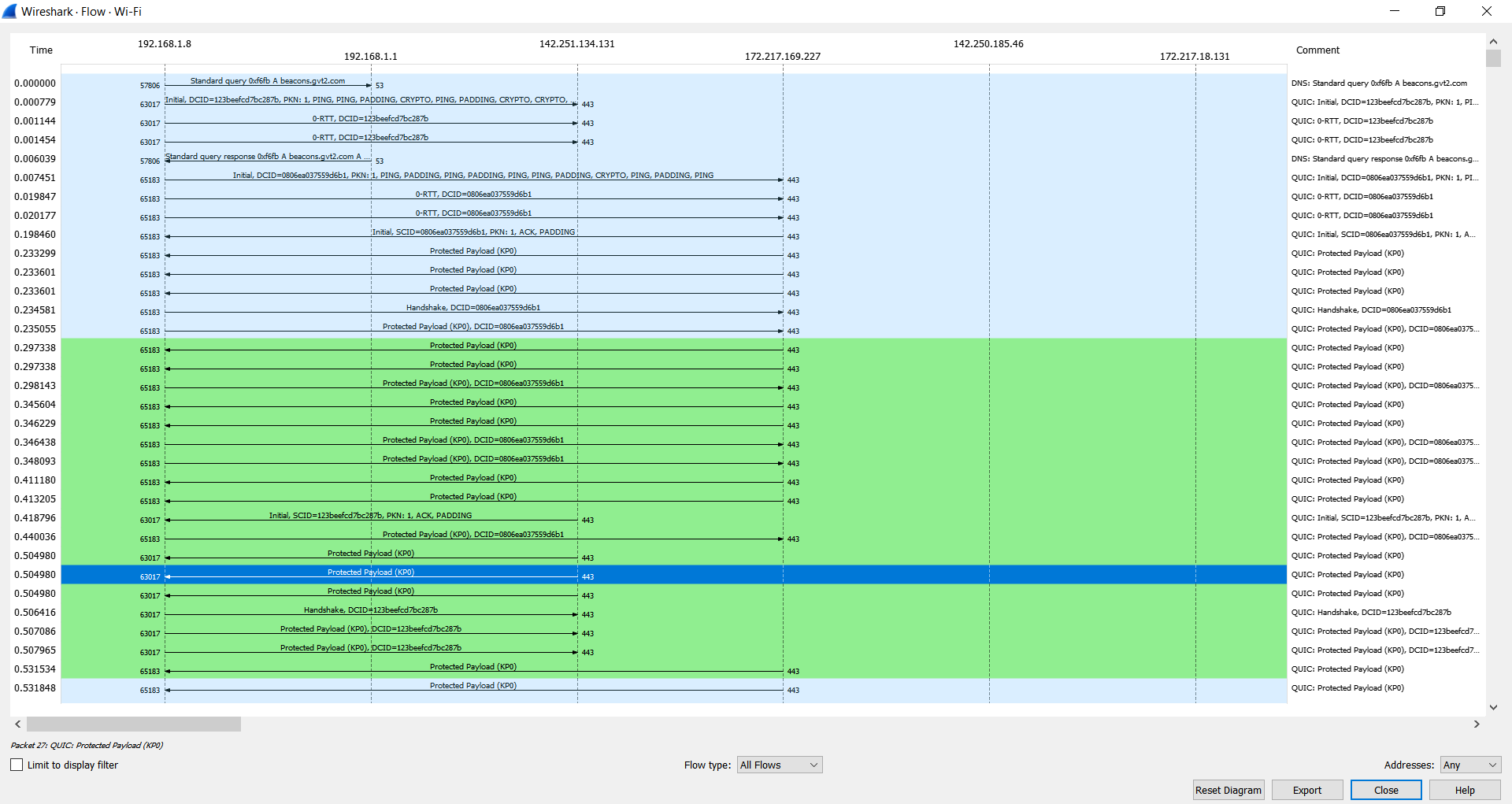
**Task 3. Explore at least the following features of Wireshark: filters, Flow Graphs**

**(TCP), statistics, protocol hierarchies.**

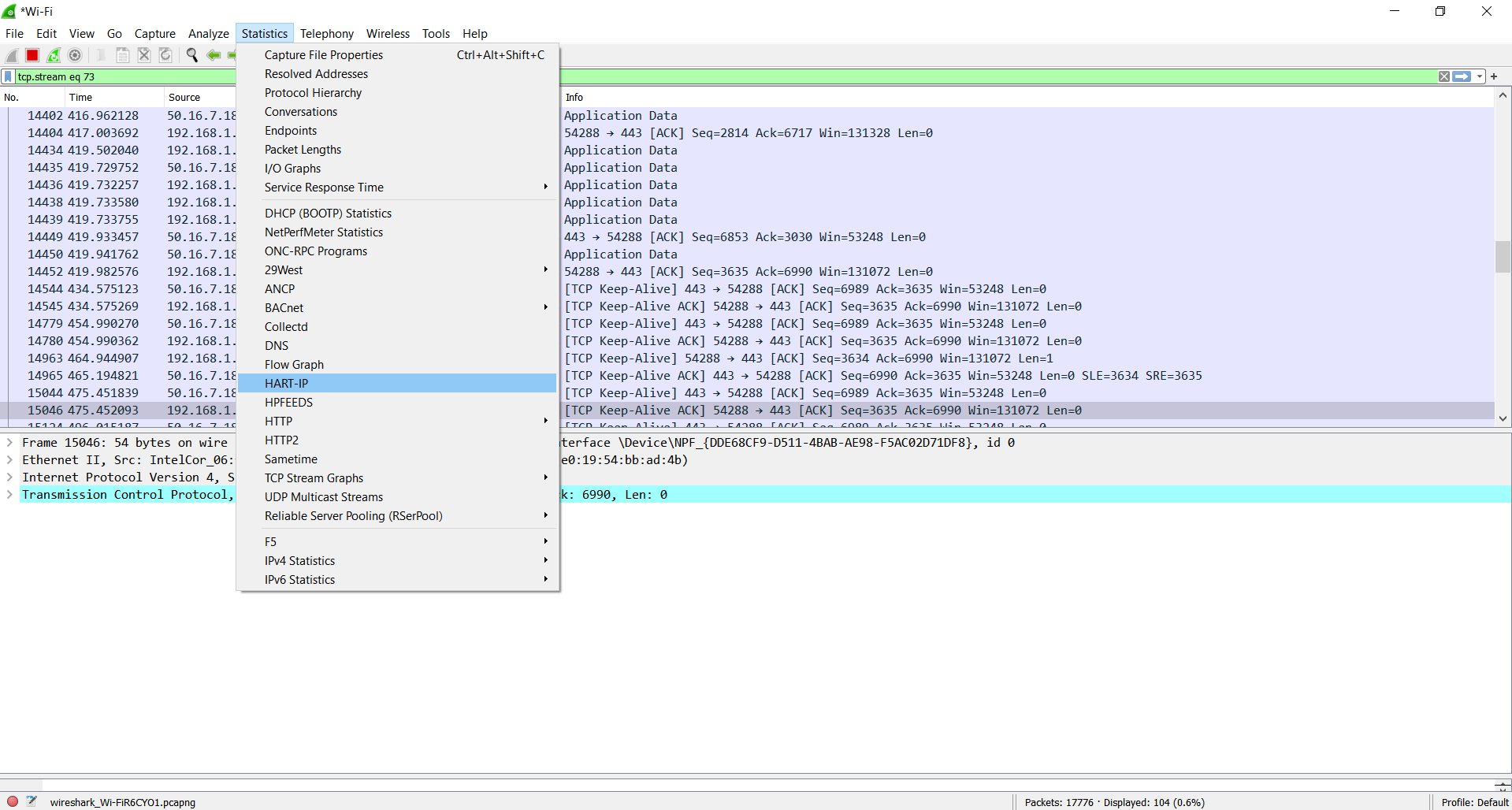
**Filters - Wireshark provides a display filter language that enables you to precisely control which packets are displayed. They can be used to check for the presence of a protocol or field, the value of a field, or even compare two fields to each other.**



**Flow Graphs -**  shows connections between hosts. It displays the packet time, direction, ports and comments for each captured connection. You can filter all connections by ICMP Flows, ICMPv6 Flows, UIM Flows and TCP Flows. Flow Graph window is used for showing multiple different topics. Based on it, it offers different controls.



**Statistics - Wireshark provides a wide range of network statistics. These statistics range from general information about the loaded capture file (like the number of captured packets), to statistics about specific protocols (e.g. statistics about the number of HTTP requests and responses captured).**



**Protocol hierarchies - The protocol hierarchy of the captured packets. This is a tree of all the protocols in the capture. Each row contains the statistical values of one protocol. Two of the columns (Percent Packets and Percent Bytes) serve double duty as bar graphs.**

