**Wireshark Lab 4 - IP**

**IT 520-A – Enterprise Infrastructure & Networks**

**Michael Weiler**

Instructions:

1. Part 1: Start up your web browser.

2. Start up the Wireshark packet sniffer, as described in the Introductory lab (but don’t yet begin packet capture). Enter “http” (just the letters, not the quotation marks) in the display-filter-specification window, so that only captured HTTP messages will be displayed later in the packet-listing window. (We’re only interested in the HTTP protocol here, and don’t want to see the clutter of all captured packets).

3. Wait a bit more than one minute (we’ll see why shortly), and then begin Wireshark packet capture.

4. Enter the following to your browser: http://gaia.cs.umass.edu/wireshark-labs/HTTP-wireshark-file1.html

5. Stop Wireshark packet capture.

Instructions:

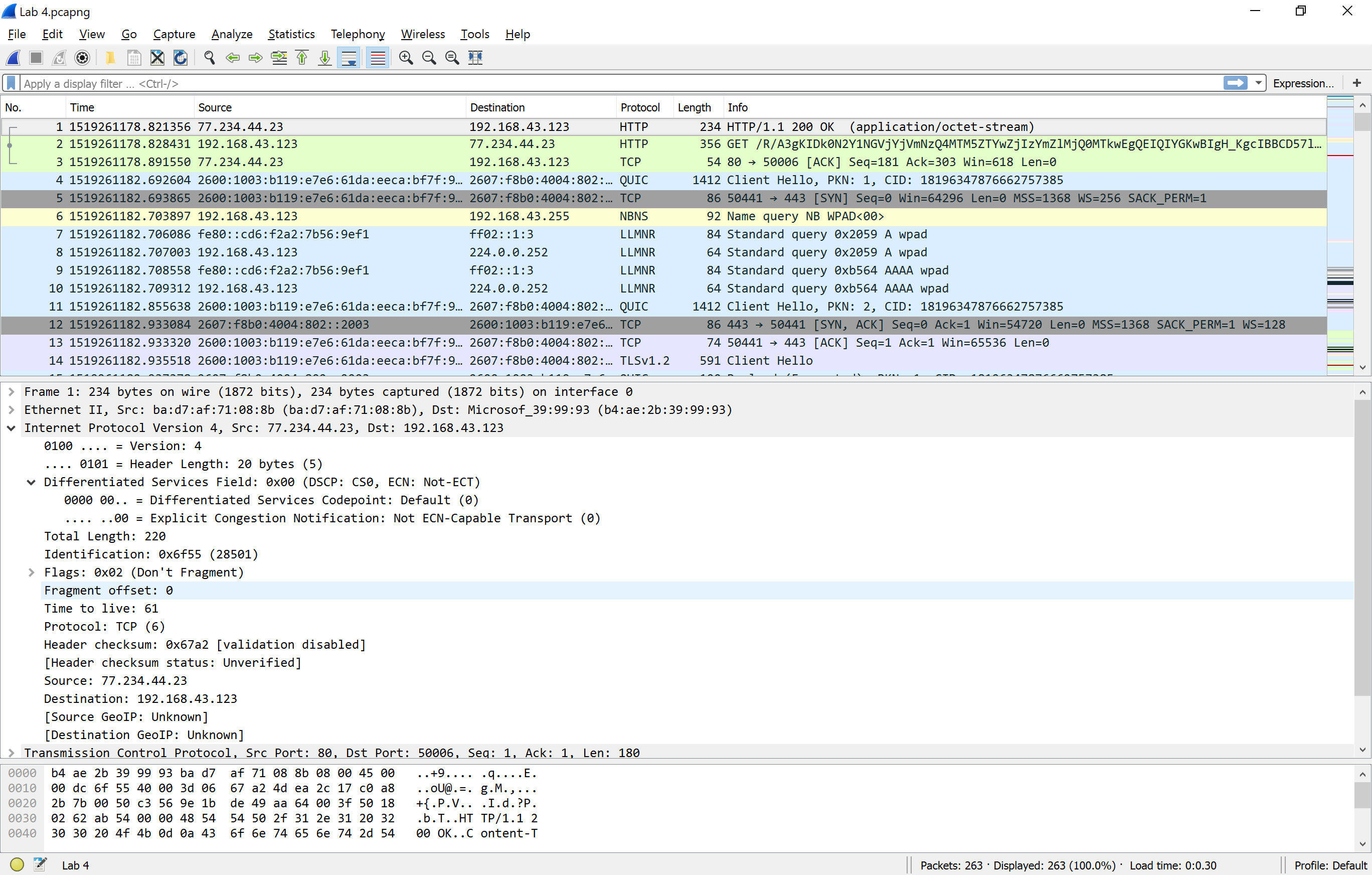
• Follow the instructions in Lab 2 and expand the IP detail section.

• **Pay attention to the text in bold. I expect you to explain?**

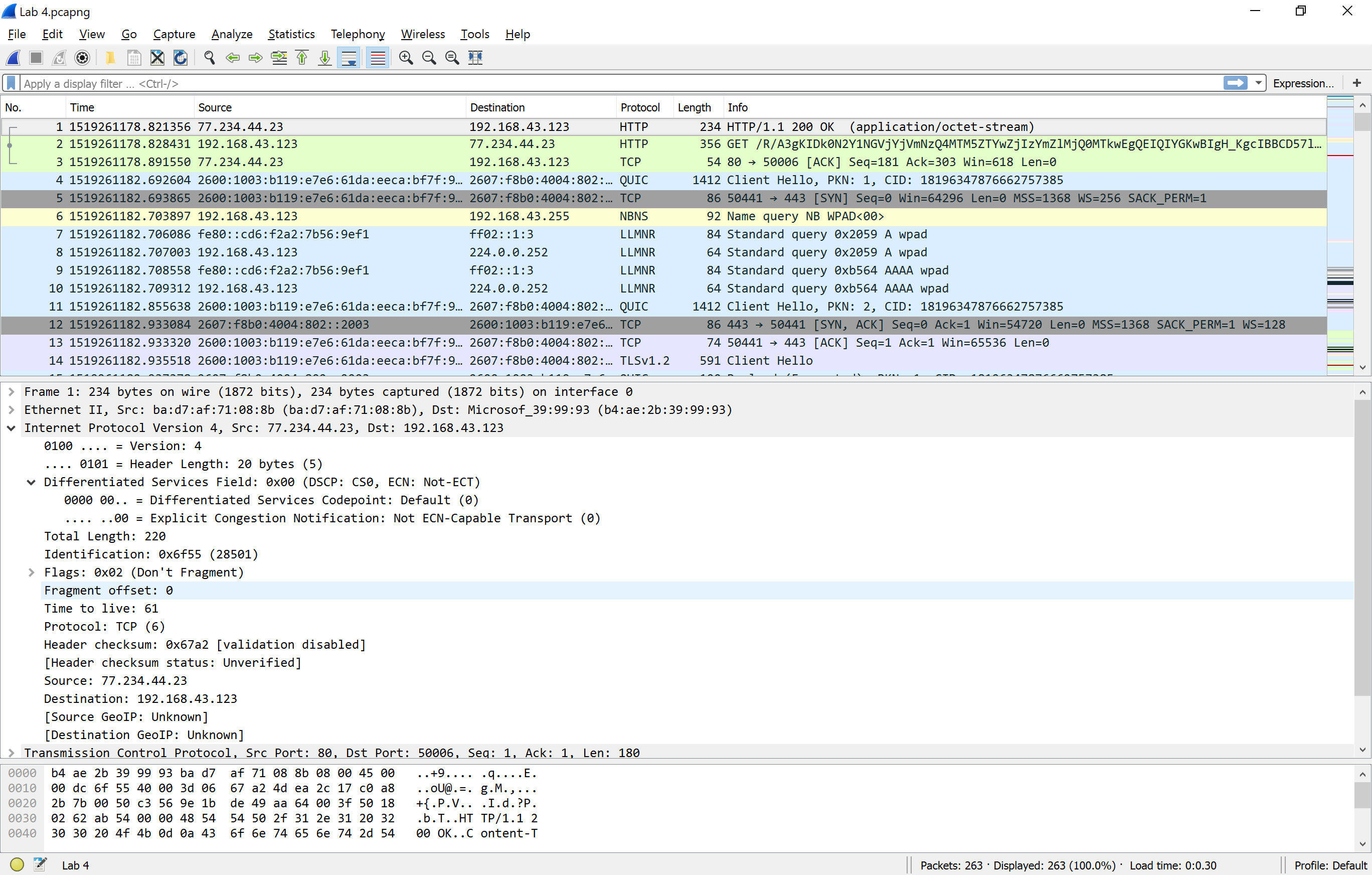
Questions:

(For each of these questions, take a screenshot of Wireshark, and attach it to your answer).

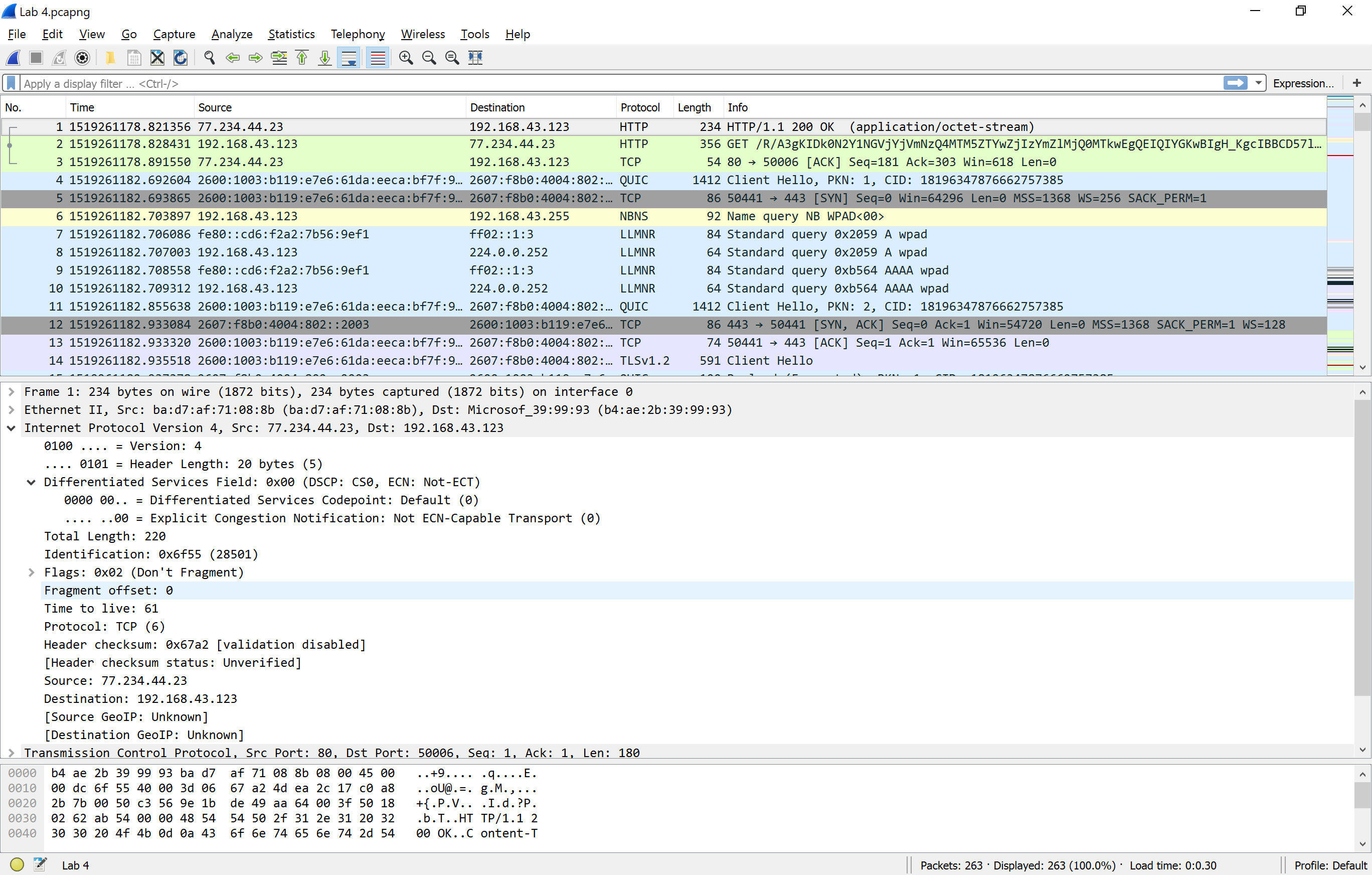
1. What is the IP address of your computer? 192.168.43.123



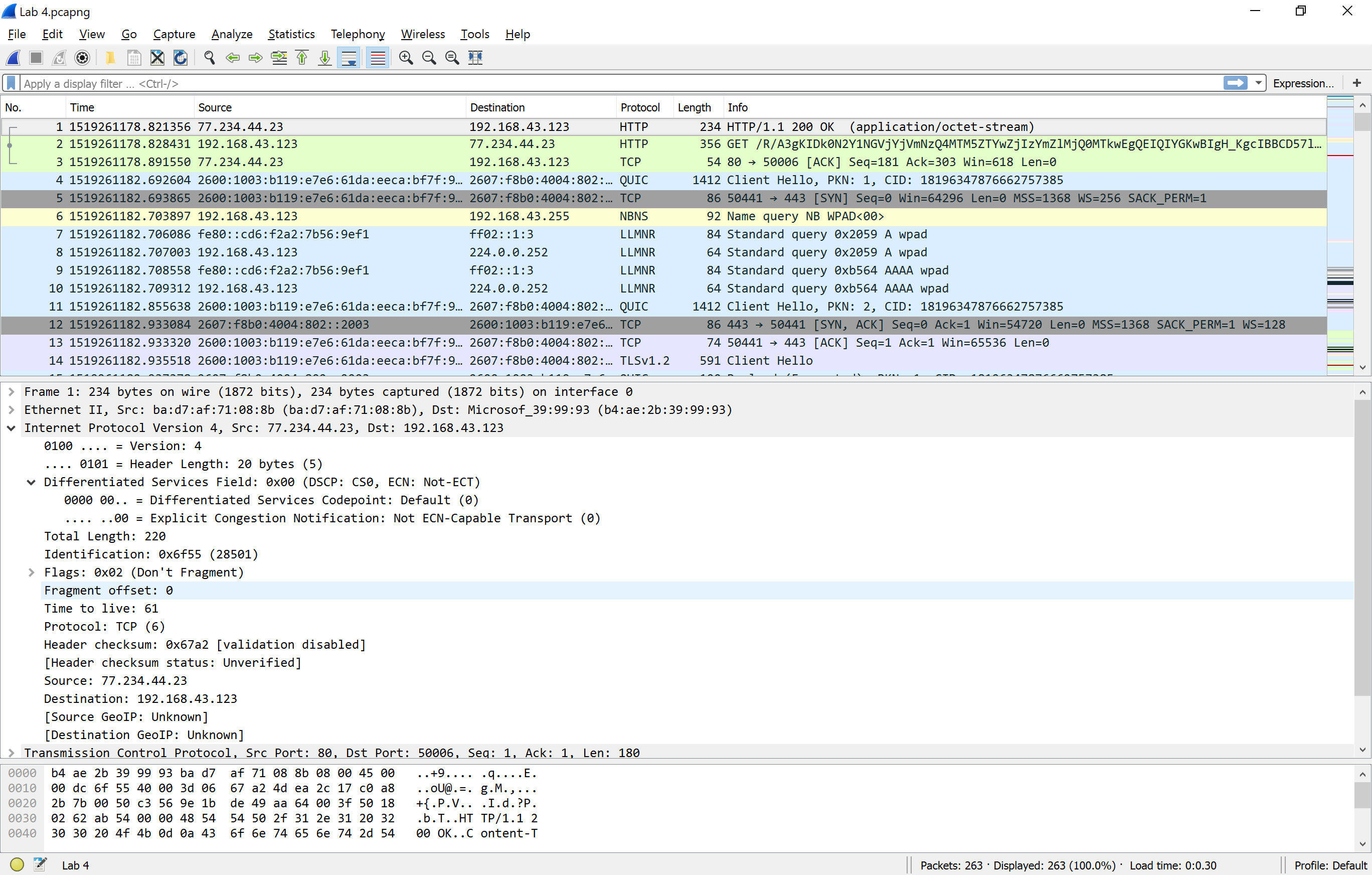
1. What is the total length of the datagram? 220



1. Has this IP datagram been fragmented? No



1. How many bytes are in the IP header? 20



1. How many bytes are in the payload of the IP datagram? Explain how you determined the number of payload bytes.

Ipheader=20

Total=220

Payload =200

