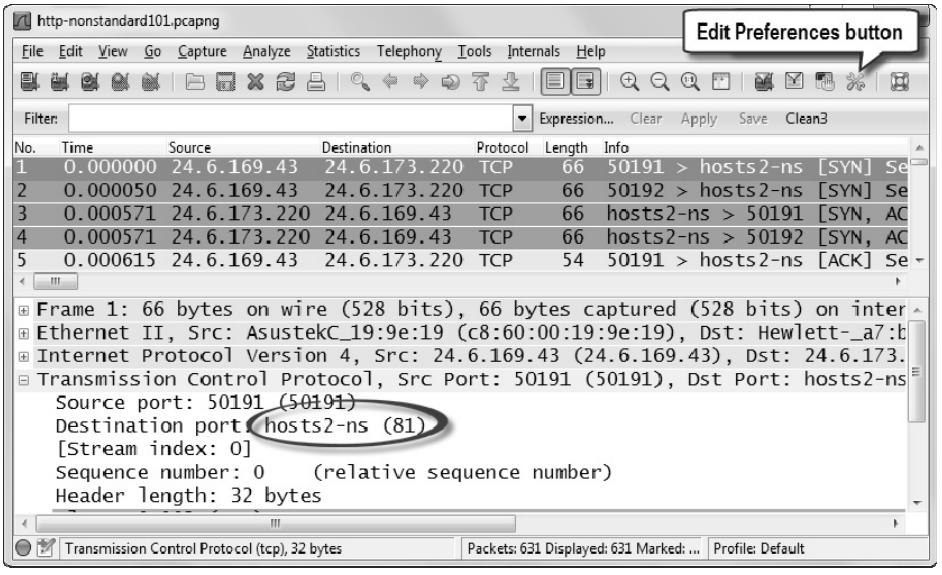
Lab 5: Configure Wireshark to Dissect Port 81 Traffic as HTTP

You have been given a trace file that contains an HTTP session, but your customer uses port 81 instead of port 80 on their HTTP server. In this lab you will get a chance to enhance Wireshark's HTTP dissection capability to include an extra port number.

***Note**: All frames from 24.6.173.220 will appear with a black background and red foreground if Wireshark is set to validate IP header checksums. You will disable this feature in Lab 6.*

Step 1: Open ***http-nonstandard101.pcapng*** and examine the Packet List pane. This does not look like HTTP traffic. The **Protocol** column simply lists TCP for all the packets. Wireshark indicates that traffic is being sent from the client ports 50191 through 50197 to port 81 (which is recognized as *hosts2-ns* by Wireshark's *services* file). We will discuss Wireshark's *services* file in the next section.



Step 2: Click on the **Edit Preferences**  button on the main toolbar.

Step 3: Expand the **Protocols** section and type **HTTP** to quickly jump to that configuration area. Add **81** to the port number list and click **OK**.

Step 4: Scroll through the trace file. Your traffic is now dissected as TCP (TCP handshakes and ACKs) and HTTP.

Step 5: Lab Clean-up Since you likely do not have HTTP traffic running over port 81, return to the HTTP port preference setting, and remove **81**. Click **OK** to save your new setting.

Scroll through the protocols listed in the Preferences area. There are many applications that allow setting ports in this manner. This is an easy way to change Wireshark's dissection methods.