## Graph High TCP Delta Time (TCP-Based Application)

Some TCP-based applications (such as HTTP and SMB) have a delta time tracking function in Wireshark. If the application does not have the delta time tracking function built into the dissector, you can still graph high delta times using **`tcp.time_delta`**.

We will practice graphing high TCP delta times in this lab.

### Wireshark Lab 89: Graph and Analyze High TCP Delta Times

This trace file contains a single encrypted TCP conversation. We will need to use Wireshark's **`tcp.time_delta`** function because we do not have an application delta time function available to us.

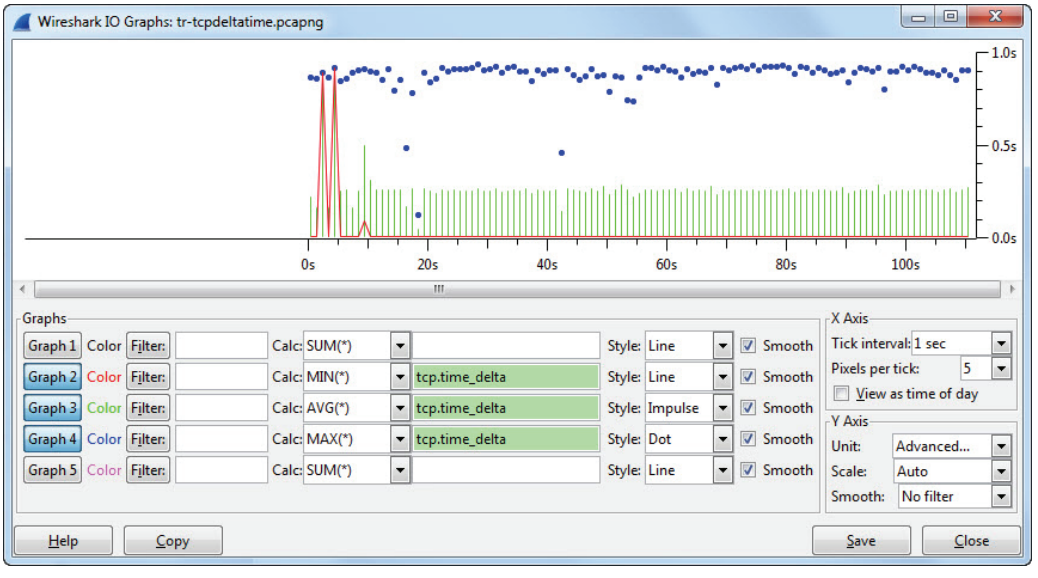
Step 1: Open **tr-tcpdeltatime.pcapng**.

Step 2: Select **Statistics | IO Graph**. In the Y Axis Unit area, select **Advanced…**

Step 3: In the Graph 2 Calc area, select **MIN(*)** and enter **`tcp.time_delta`**. Click the **Graph 2** button to enable this graph.

Step 4: In the Graph 3 Calc area, select **AVG(*)** and enter **`tcp.time_delta`**. Set the Style to **Impulse** and click the **Graph 3** button to enable this graph.

Step 5: In the Graph 4 Calc area, select **MAX(*)** and enter **`tcp.time_delta`**. Set the Style to **Dot** and click the **Graph 4** button to enable this graph.




The graph clearly shows that the average response time in the trace file is slightly less than 300 ms and there are higher TCP response times in the beginning of the trace file.