Creating Network Captures with Wireshark

To troubleshoot network problems it sometimes becomes necessary to make a packet capture demonstrating the problem. Follow the directions in this note to create a network capture that you can submit to FacetCorp support for analysis.

Wireshark is a useful utility for capturing network data packets between two or more systems. Wireshark Download

Once you have Wireshark running, select the interface that you will be capturing through if you have multiple interfaces displayed.
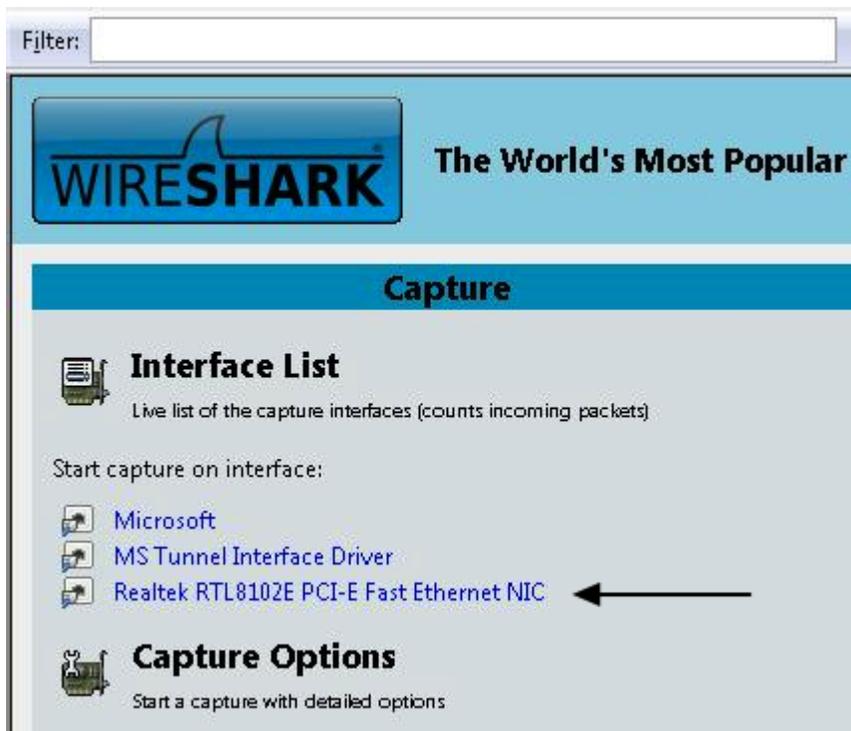
Once the interface is selected, Wireshark will begin to capture data packets via that interface. At this point re-create your network problem so that the event can be captured. Watch the packet count at the bottom of the Wireshark display page. The count should increase as data packets are displayed and captured:
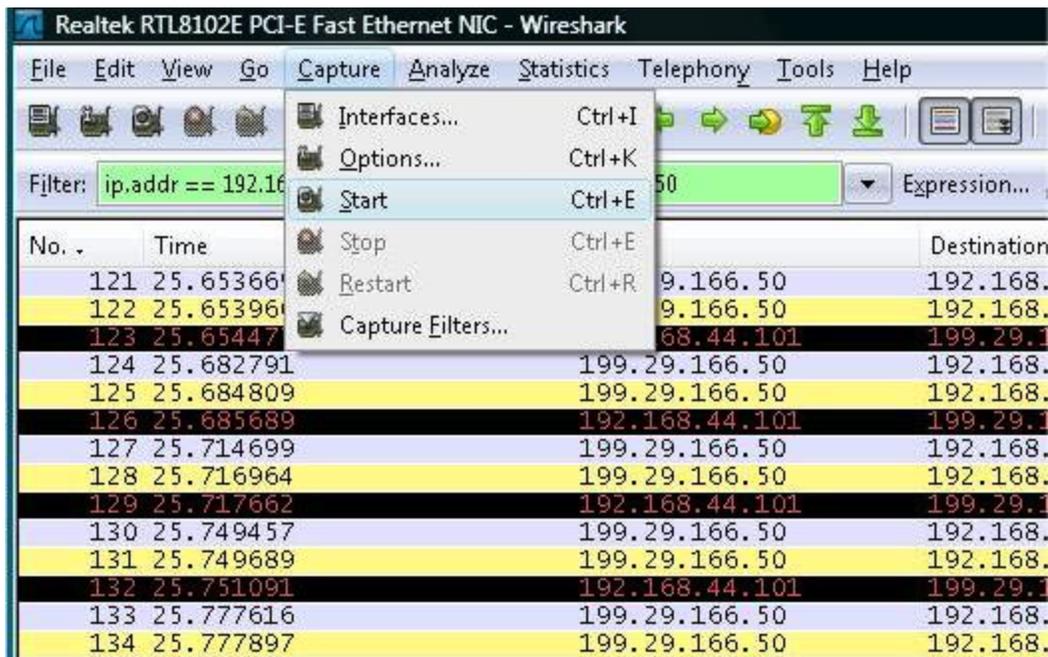
When the problem has been captured you can save the capture session to a file that can be emailed to FacetCorp.

Use the Capture menu option dropdown box to select Stop capture. When you exit the program you will be asked if you want to save the captured data. Save it to a file on your system and give it an extension of "cap". You can also use the File menu option and select Save As.

Along with the capture, send us the following information:

1. The partnumber of the FacetCorp product being captured

2. Your server OS information (uname -a, uname -X or oslevel)

3. Entries generated in "syslog" or "messages" during the capture

4. The IP addresses that should be examined in the capture (client and server)

5. A brief description of the problem being reported.

6. Send us all these items via email to: support@facetcorp.com

Your capture file will be submitted to the FacetCorp development team for review. A technical support agent will contactyou with information regarding your reported problem after it has been analyzed.