Support Guide: Wireshark Collection

# Collecting network traffic with Wireshark

***Collecting network traffic with Wireshark to troubleshoot connectivity issues***

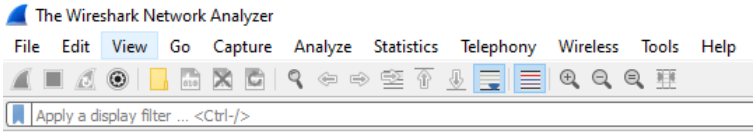
**Important Note**

*This guide assumes you have downloaded and installed the freeware Wireshark package from www.wireshark.org.*
*Wireshark is a 3rd party product useful for collecting network traffic. Wireshark is not supported by F-Response, nor will F-Response assume any responsibilities for its actions. You elect to install and run Wireshark on your own accord.*

## Step 1: Download and install Wireshark from Wireshark.org.

Download and install Wireshark from www.wireshark.org. When prompted, be sure to install the additional packet capture driver necessary to collect live traffic on one or more network interfaces.

## Step 2: Start and configure Wireshark to collect specific traffic.

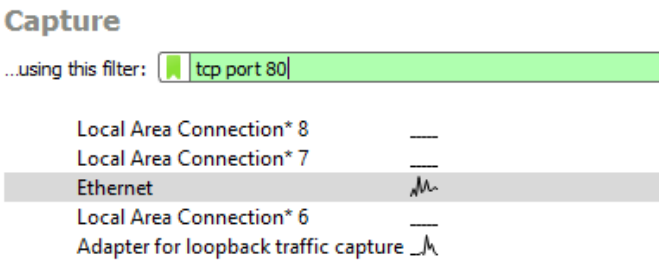



Open Wireshark by right clicking on the icon and running “as administrator”. Wireshark must be run with administrative rights to collect network traffic.

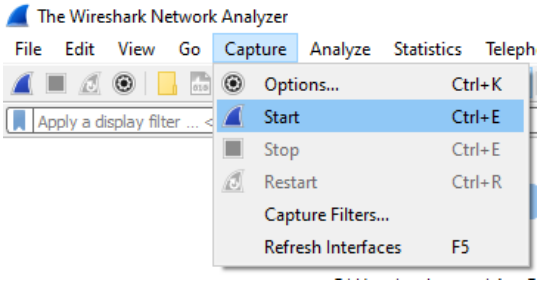
F-Response support will provide a capture string specific to what they need to evaluate. You will want to enter this string in the initial start-up screen.

An example of this is included below.

“tcp port 80”




Once configured you should get a green bar as shown on the right. Now select the interface with traffic, in most cases this is “Ethernet”.




Lastly go to Capture->Start to begin the network capture.

## Step 3: Execute the action(s) as requested.

Execute the action(s) in F-Response that are failing to complete, i.e. connecting, deploying, etc. Make sure you are doing this as the collection is taking place.

## Step 4: Stop capturing.

Once you have received the anticipated error state, stop the Wireshark capture, save the file, and send the resulting pcap to support via email.