Collecting network traffic with Wireshark



Collecting network traffic with Wireshark to troubleshoot connectivity issues



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 <u>www.wireshark.org</u>. 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.

🚄 The Wireshark Network Analyzer									
File Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
	۲	010	XC	۹ 🗢 🖻	- <u>E</u> 7	& ⊒ ≡	⊕, ⊖, (₹.	
Apply a display filter <ctrl-></ctrl->									

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".

apture

using this filter: 📙 tcp port 80	
Local Area Connection* 8 Local Area Connection* 7	
Ethernet	M
Local Area Connection* 6 Adapter for loopback traffic capture	M

🚄 The Wireshark Network Analyzer Edit View Go Capture Analyze Statistics Teleph File 🚄 🔳 🙋 💽 📴 🔚 🛞 Options... Ctrl+K Ctrl+E Start Apply a display filter $\boldsymbol{\Lambda}$ Stop Ctrl+E Ctrl+R C) Restart Capture Filters... **Refresh Interfaces** F5

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.

Capturing from Ethernet (tcp port 80) File Edit Go Capture Analyze View Statistics Telepho ۲ 010 ۲ Options... Ctrl+K Æ. Δ Start Ctrl+E Apply a display filter Ctrl+E Stop No. Time đ Restart Ctrl+R Capture Filters... Refresh Interfaces F5