

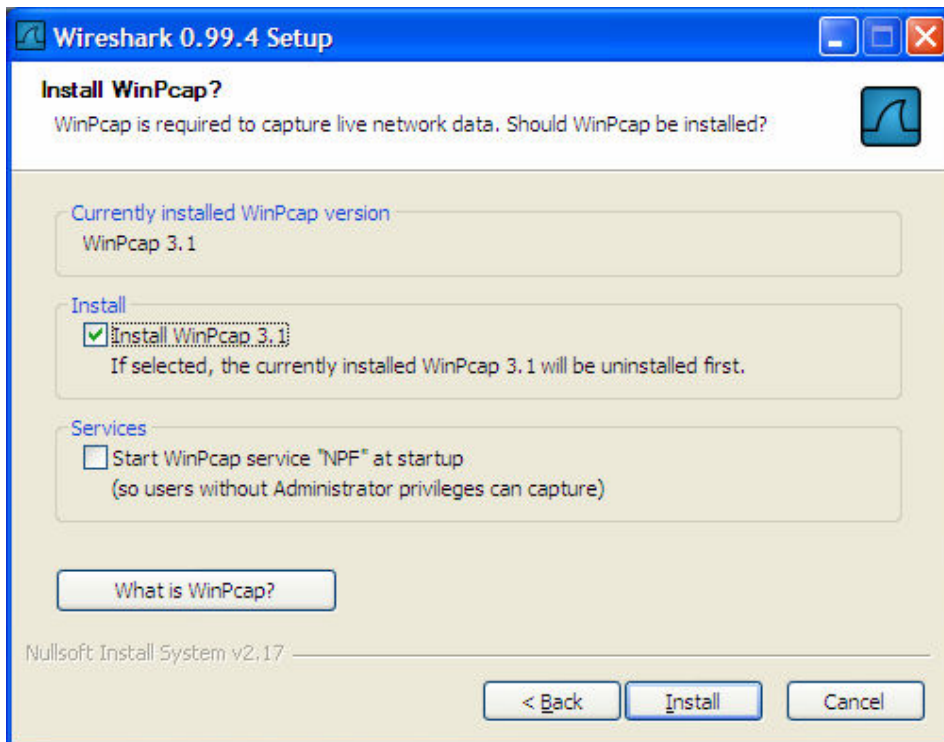
Ethernet Captures using Wireshark

Introduction

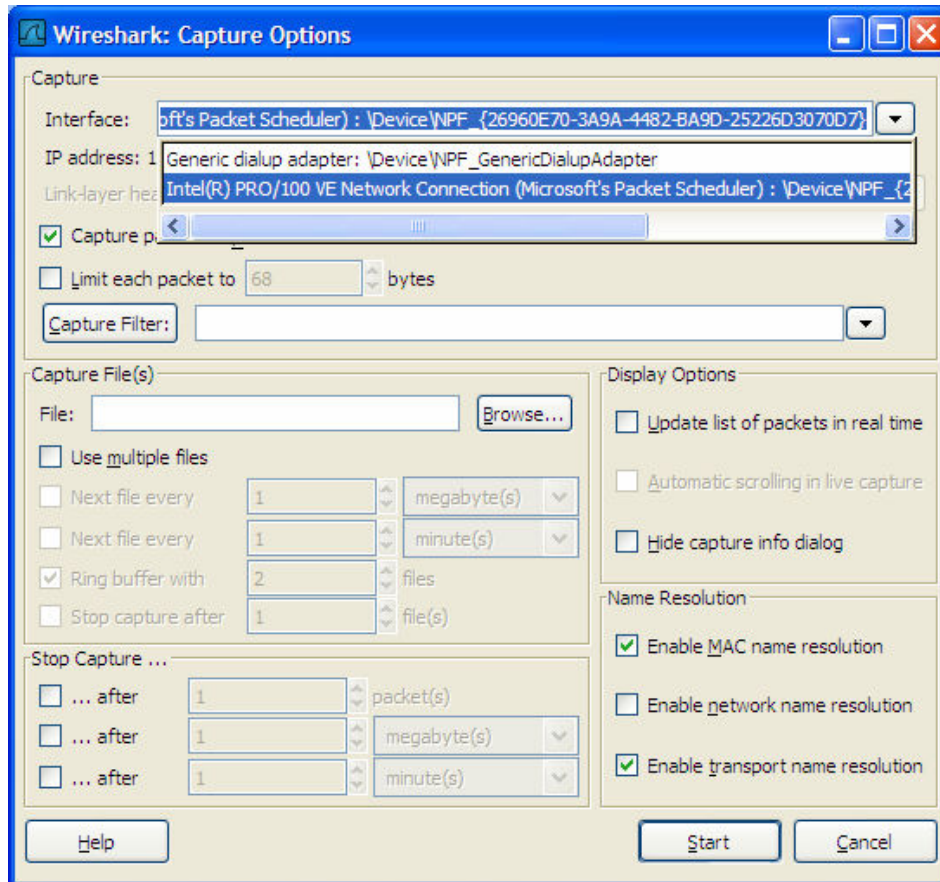
Since a large number of communication protocols communicate across Ethernet, it is important for troubleshooting purposes to get a capture of Ethernet traffic. This eNote describes the procedure to download and run Wireshark which is a free external capture utility that logs Ethernet traffic.

Procedure – Wireshark Capture

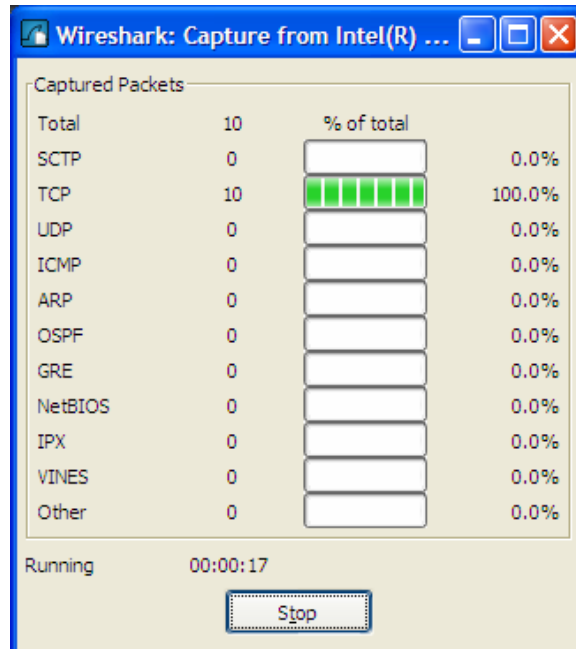
- 1) Go to www.wireshark.org/download.html to access the download page.
- 2) Select the download site for your operating system.
- 3) Download the following file: Wireshark-setup-0.99.4.exe
- 4) Run the executable.
- 5) When installing Wireshark, install WinPcap 3.1 as well by checking the install box.



- 6) Run Wireshark.
- 7) Click on the 'Show the Capture Options' button on the top left.
- 8) Go to the Interface option and select the Ethernet adapter from the drop-down menu.



- 9) Enter a filename under Capture File(s) and select a location for that file.
- 10) "In the filter section, enter the following 'port not 1024'. This will filter out all of the Ethernet messages of the FieldServer Utilities."
- 11) Hit the 'Start' button to start a capture. Once the capture is going, a screen will appear with the types of Ethernet traffic captured.

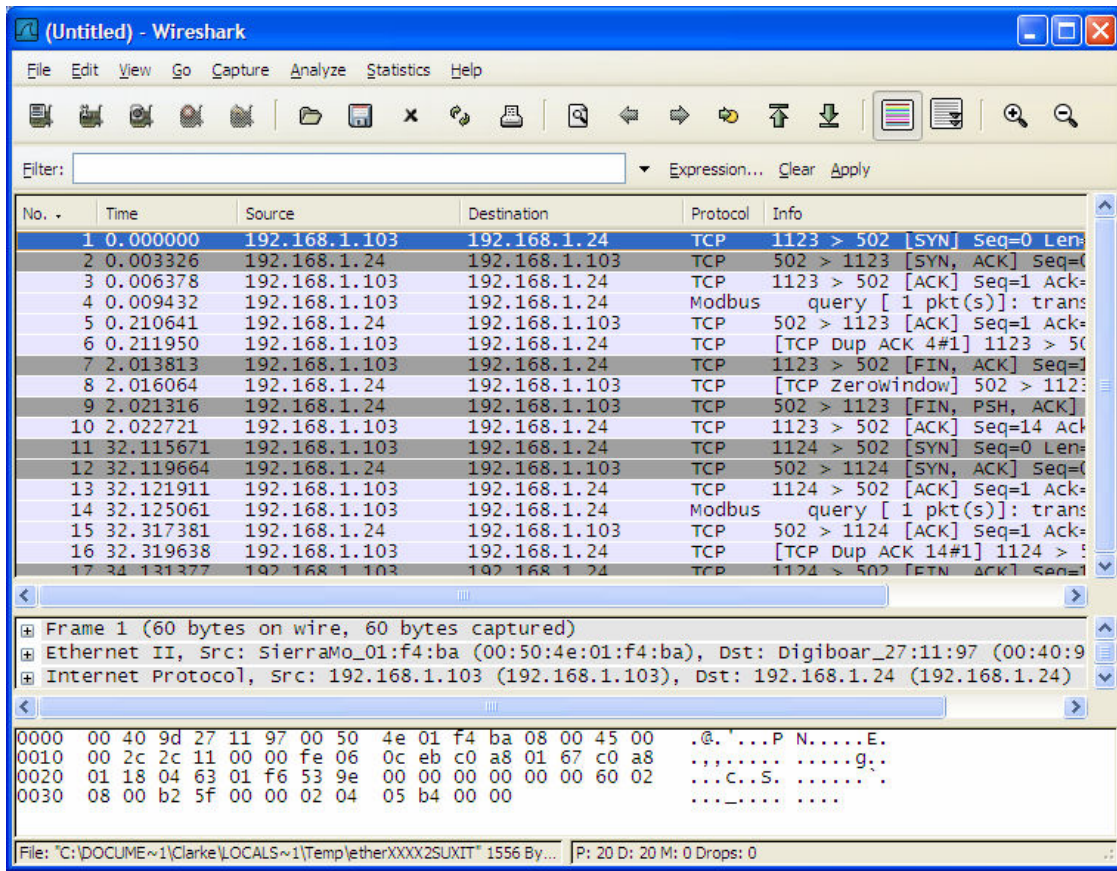


- 12) Ensure that the suspected problem occurs while the Wireshark capture is running.
- 13) Please use the FST diagnostic utility to take a 10 minute capture while the Wireshark capture is running. Download the diagnostic utility from <http://www.fieldserver.com/techsupport/utility/utility.asp>. Please read the FST Diag manual before running the utility. Under article 3, there are some steps to take to ensure that the program will work correctly.
- 14) Email the capture file(s) to support@FieldServer.com.

Notes: - Wireshark Capture

1. Verifying the Wireshark Capture

- Check the Main display after stopping the capture. Check the Source and Destination columns to see that the FieldServer IP address is shown and the remote device's IP is shown.
- If neither IP address is present in the window, the problem could be that the PC's IP address is not on the same subnet as the FieldServer and/or remote device. To be on the same subnet, all of the device's IP addresses need to have similar numbers for the first three octets. (Eg. X.X.X.45)



2. Hub/Switch/Router Issues

- The FS-B20 and FS-B40 Series FieldServers are 10baseT devices and when connected to an auto sensing 10/100 hub the FieldServer's messages may not be visible to the PC.(See note above). In this case, you will need to connect all of the devices to a 10 base T hub.
- Switches and Routers do not echo all messages on all ports, but direct messages to the appropriate ports to increase bandwidth. Thus, a capture with a PC on port 1 might not see the messages on the ports the FieldServer and remote device are on. A solution for this connecting everything to a non-switching hub.

3. FieldServer Utilities

- Do not run Ruinet.exe (Remote User Interface) while the Ethernet Capture is running. This will make your capture file unnecessarily large.
- Please run a Serial Capture at the beginning and the end of the Ethernet Capture.

Doc. No. ENOTE0063	Rev. 5
-----------------------	-----------

THIS PAGE INTENTIONALLY LEFT BLANK