Capturing Network Traffic With Wireshark

A White Paper From

For more information, see our web site at
http://www.goldstarsoftware.com

Capturing Network Traffic with Wireshark

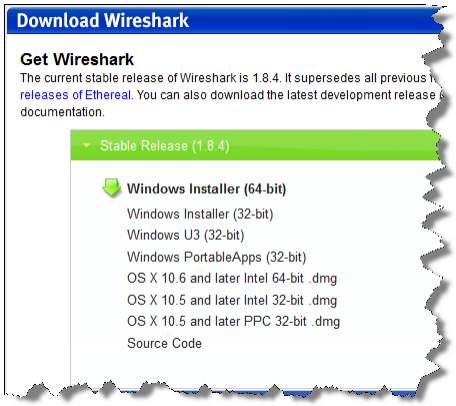
Last Updated: 02/26/2013

In some cases, the easiest way to identify problems in a network system, such as performance problems or system failures, is to grab a network capture -- a log of all networking packets that enter and leave a workstation. When typical "hit or miss" troubleshooting doesn't seem to be working, we may instruct you to collect a network trace, and these instructions serve as a simple way to perform this task.

Downloading and Installing Wireshark

The first step is to download Wireshark. Go to www.wireshark.org and click on the Download Wireshark Now button:

Then select the Windows Installer link from the next dialog.

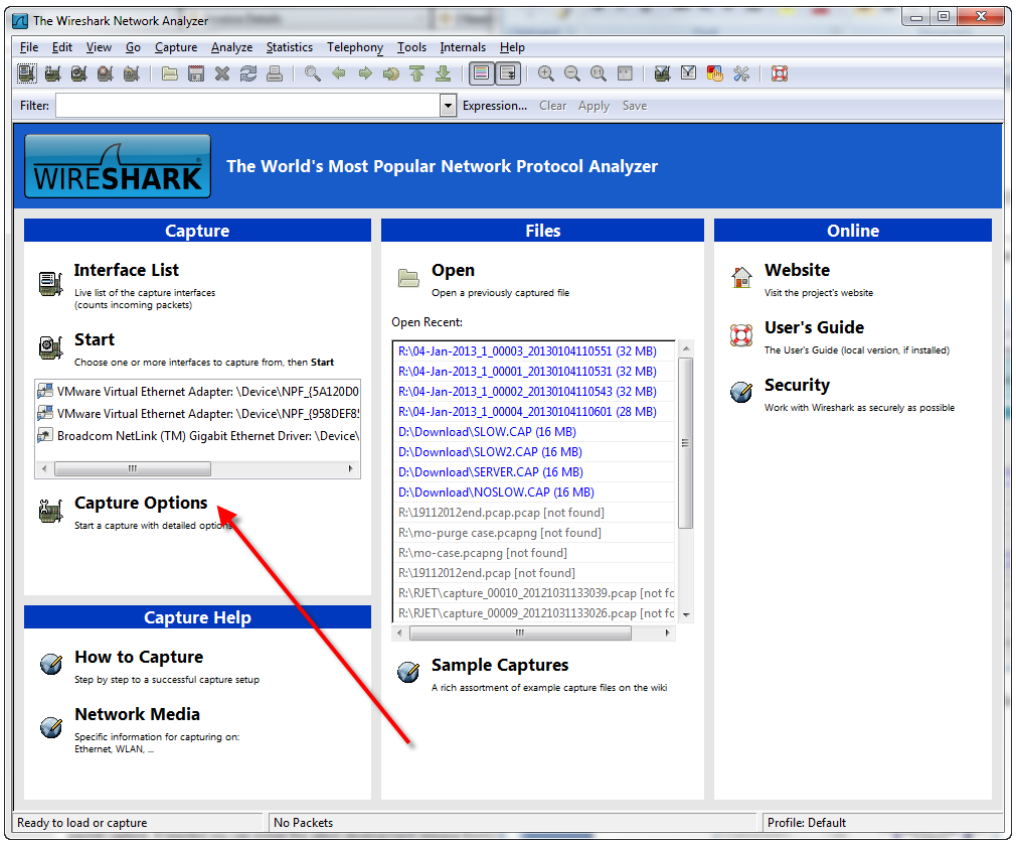


If you are running on a 64-bit operating system, then you may want the 64-bit version. Otherwise, download the **Windows Installer (32-bit)**.

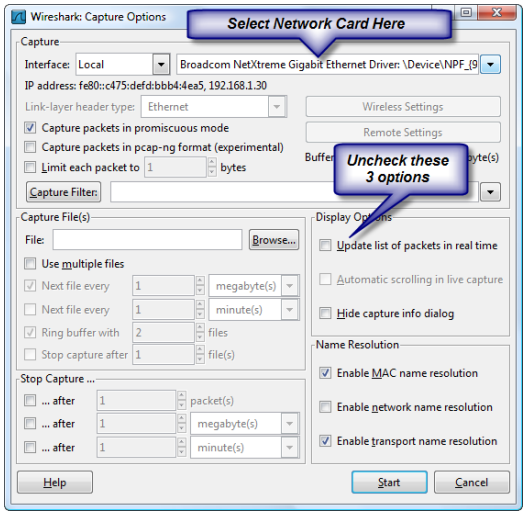
When the download finishes, run it with all of the default options (click next, next, etc.) to install the software. When it is done installing, launch Wireshark.

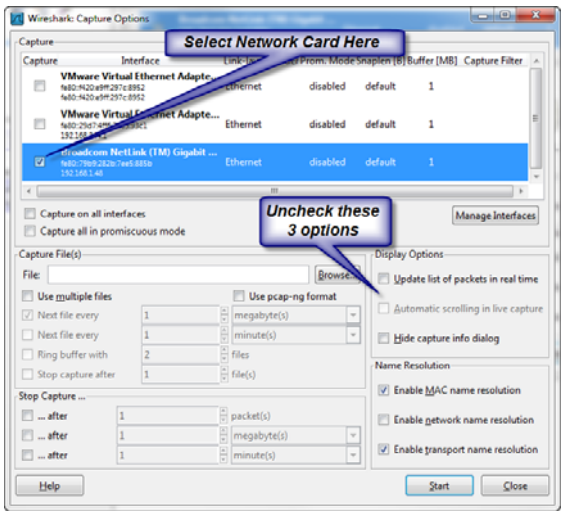
Starting Wireshark and Setting up a Simple Capture

A simple capture is used when you can easily duplicate your network problem, like starting an application. When Wireshark launches, you will see a standard welcome screen, which looks something like this:



Click on the **Capture Options** button, as indicated above, and you will see the **Capture Options** dialog box. Users of older versions of Wireshark will see the screen on the left, while users of newer versions will see the image on the right.





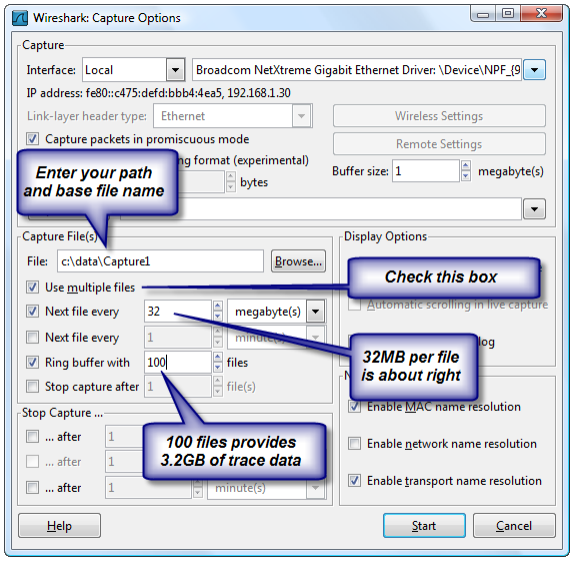
First, verify that the correct network card is indicated in the box on the top, or your capture will likely be empty.

Second, verify that the three **Display Options** are NOT checked. (The default is checked, but we want to keep the capture process as simple as possible.)

Setting up a Circular Buffer Capture

For some issues, you may need to capture a LOT of data, or you may not know when the error will occur. Wireshark handles smaller capture files very well, but when your files get TOO large, the system starts to get sluggish. To avoid this, we recommend setting up a "circular buffer" capture, which grabs the network data in a number of smaller, more manageable, capture files.

First, follow the steps above as in the simple capture. Then, we'll make a few more changes in the **Capture Options** dialog box. (We're showing the older style dialog box, but the fields we are looking at are the same on both styles.)



First, enter a path and base filename for the capture. This location should have enough disk space for the total size of the capture -- so you will want to verify this FIRST.

Then, check the **Use multiple files** option, as well as the **Next file every** and **Ring buffer with** options.

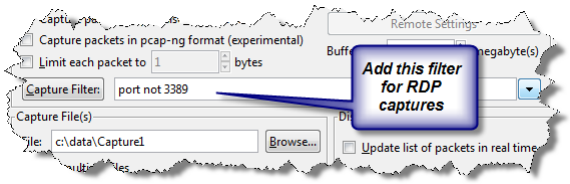
Put 32 into the **Next file every** box, so that each trace file will be 32MB -- a size small enough that Wireshark can handle with ease on just about any system.

Finally, put a number into the **Ring buffer with** box that corresponds to the amount of data that you need to keep. Note that 100 files of 32MB each = 100*32 = 3.2GB. In many cases, even this is FAR too much, and you might be able to get away with 10, 20, or so. This is a good time to re-verify that you have enough disk space in the location provided. If you run out of disk space, bad things can happen!

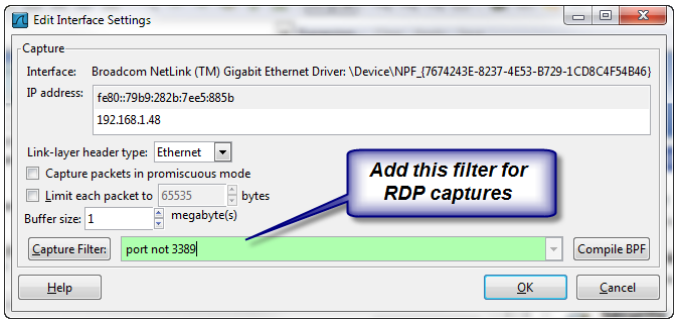
Capturing from a Remote Desktop Session

When you are remotely controlling a machine via Remote Desktop, the network capture will get all of your RDP packets, as well as the rest of the data that you want. Obviously, this can change the environment enough such that you don't get a valid capture, so this is not recommended.

However, if you must use an RDP session, then you want to make one more change to the Capture Options dialog box:



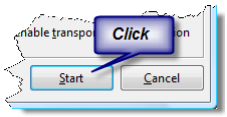
If you are running the newer Wireshark releases, double-click on the NIC entry to bring up the Interface Settings dialog box:



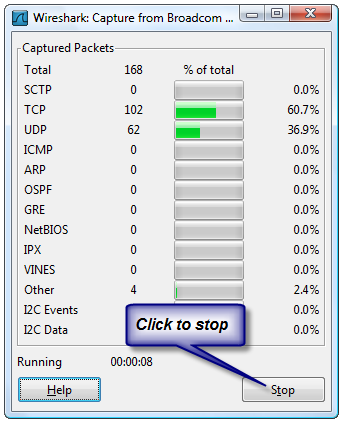
By adding "port not 3389" to the capture filter, you will exclude the RDP traffic, and get a better handle on exactly what you ARE looking for. Again, if RDP is contributing to the problem, then this filter may actually help disguise the problems you are trying to troubleshoot.

Starting and Stopping the Capture

When you have set up the capture buffer as you need it, click **Start** to begin the capture.



You will get the **Captured Packets** screen, which looks like this:



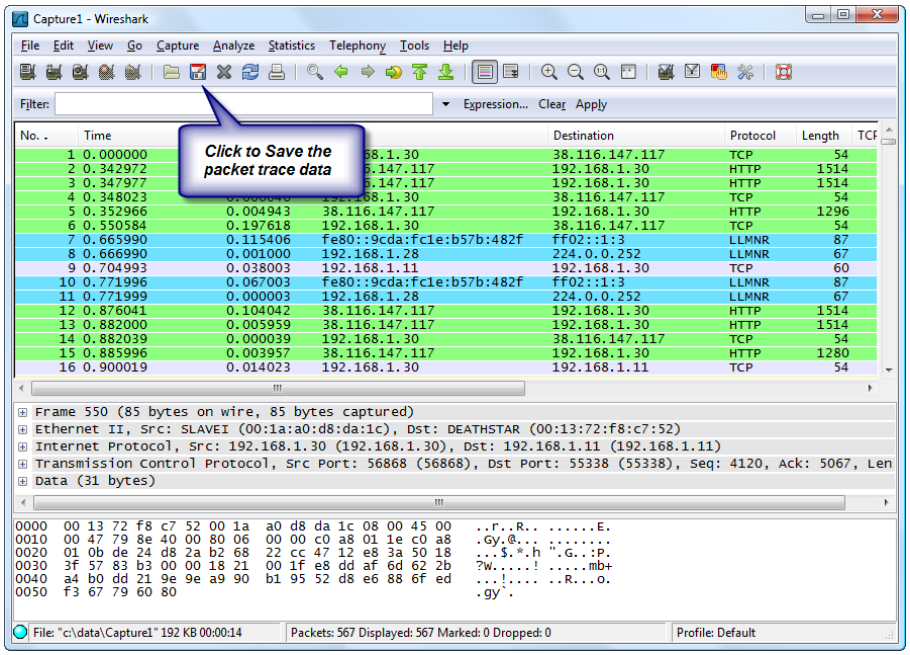
You will see the timer running, and packets will start accumulating into each bucket. If you do NOT see any packets, then you may have selected the wrong interface. Go back to the **Capture Options** screen and try a different network card.

You should now use your system normally and duplicate the problem that you are trying to troubleshoot. If possible, note the EXACT time that the problem occurs. Then, stop the capture by clicking on the **Stop** button on the **Captured Packets** dialog.

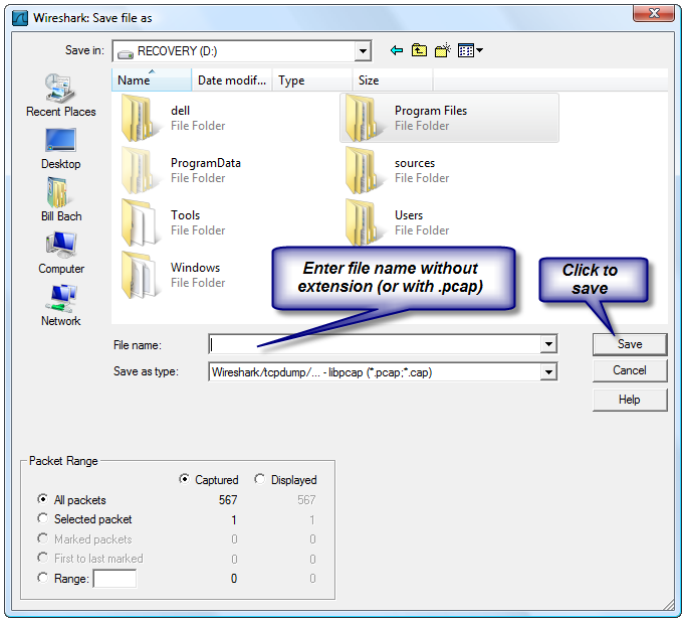
Saving the Capture

If you created a circular buffer, then your packet capture is already saved into one or more files in the location you specified. Each filename includes a timestamp of when the file was CREATED, so that you can isolate the file which contains the "interesting" packets.

If you were using a simple capture, then you'll instead see a screen like this:



Click the **Save** button to bring up the **Save As** dialog box.



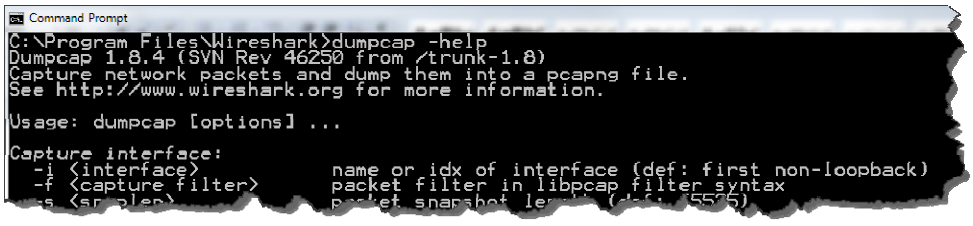
Then, enter a filename without an extension (or with a .pcap extension) and click **Save**.

You can then submit the saved trace data to Goldstar Software via Email or (for larger data sets) via FTP.

Visual C++ Crashes

In recent versions, memory allocation seems to be an issue, and this has been causing pop-up dialog boxes that indicate the Visual C++ Library is crashing. It is unclear if this is a problem caused by recent changes to the Wireshark code, or by changes to the Microsoft libraries. However, you may have issues getting a large capture using the steps above.

The solution is to avoid the user interface and use the command-line tool *dumpcap*. Use the option "-help" to get information about the command line options:



A command like this should work for most users:

```
dumpcap -i 1 -b filesize:32768 -b files:100 -f "port not 3389" -w C:\Cap.pcap
```

If you still can't get it to work, contact Goldstar Software and let us work with you to help! Please note that this may be a billable support call if you have already used up your free support time.