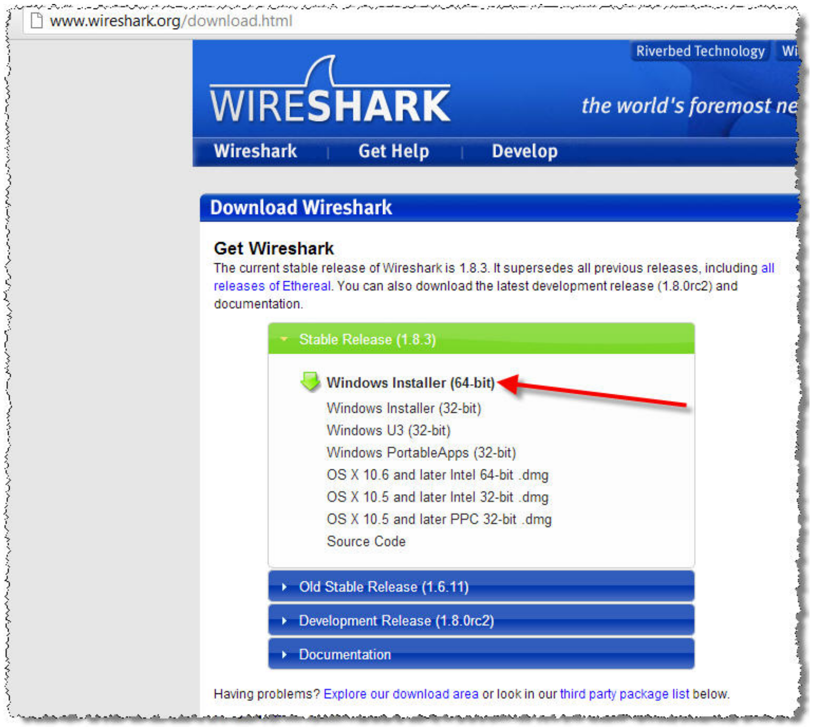
Installing and Using Wireshark for Capturing Network Traffic

These instructions are written for using a Windows computer, but are mostly valid for a Linux/Apple environment too.

In order to better troubleshoot issues with your ATA, you can capture all network traffic off of the network cable and submit to Cisco as follows.

Downloading Wireshark

Download the most current version of Wireshark from http://wireshark.org/download.html


www.wireshark.org/download.html

Riverbed Technology | Wi

WIRESHARK the world's foremost ne

Wireshark | Get Help | Develop

Download Wireshark

Get Wireshark

The current stable release of Wireshark is 1.8.3. It supersedes all previous releases, including all releases of Ethereal. You can also download the latest development release (1.8.0rc2) and documentation.

Stable Release (1.8.3)

- Windows Installer (64-bit)
- Windows Installer (32-bit)
- Windows U3 (32-bit)
- Windows PortableApps (32-bit)
- OS X 10.6 and later Intel 64-bit .dmg
- OS X 10.5 and later Intel 32-bit .dmg
- OS X 10.5 and later PPC 32-bit .dmg
- Source Code

Old Stable Release (1.6.11)

Development Release (1.8.0rc2)

Documentation

Having problems? Explore our download area or look in our third party package list below.

Install Wireshark and WinPcap and accept all defaults. [Additional help is located at: http://www.wireshark.org/docs/wsug_html_chunked/ChBuildInstallWinInstall.html]

Network Interfaces on Computer

You need to understand a little about your network in order to properly collect all network traffic. For example, your computer may be on a data VLAN and your ATA may be on a voice VLAN without you realizing it. For this reason, I recommend that you use a separate network interface for Wireshark such as a USB NIC [network interface card/connector]. I use the *Cisco-Linksys USB Ethernet Adaptor* with great success.

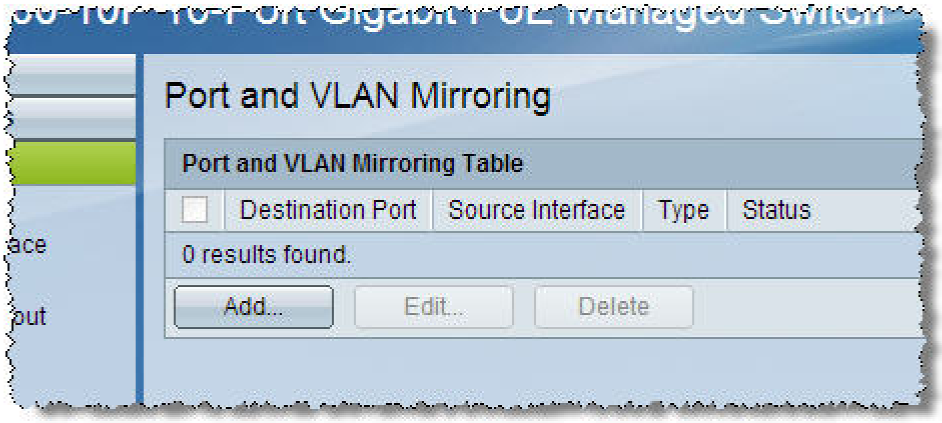
Using an additional adaptor allows my computer to remain connected to the network via its regular interface [wired or wireless, it doesn't matter] while my Wireshark USB NIC is connected to a switch port that is mirrored [also known as being in "span" mode] so that all switch data is seen by my Wireshark interface.

You must configure your network switch so that it copies (mirrors) network data to the Wireshark port. [Switches, by design, do not send all network traffic to all ports. Read more here if you're interested.]

Configuring Mirroring on the Network Switch

Here's an example of configuring a Cisco SG300-10P switch:

1. Log in to the switch as an administrative user.
2. Decide which port will be the mirror/span target. In my lab, I usually use the right-most port as the mirror target, making it easier for me to remember which port does what. Only one port can be a mirror target but multiple ports can be configured as mirror source ports.
3. Navigate to Administration > Diagnostics > Port and VLAN Mirroring:



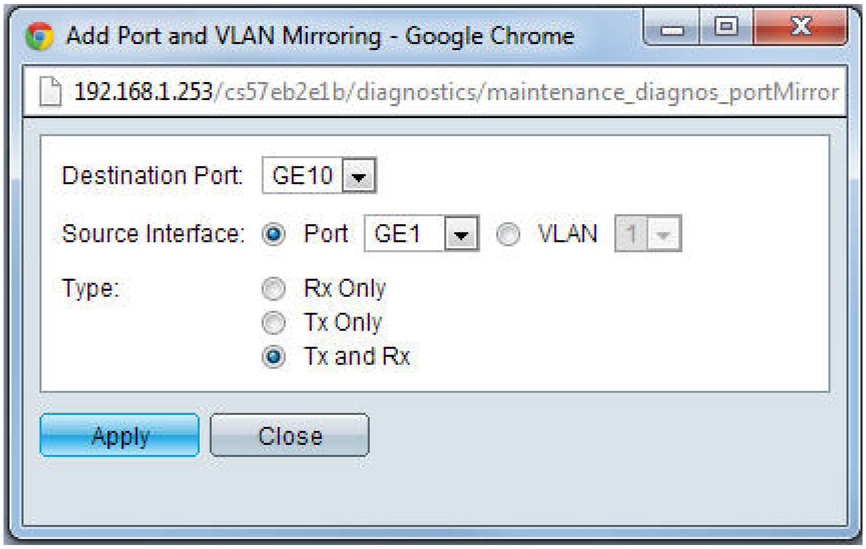
Port and VLAN Mirroring

Port and VLAN Mirroring Table

□	Destination Port	Source Interface	Type	Status

0 results found.

   a. Click Add to display the *Add Port and VLAN Mirroring* pop-up window.
   b. Select the Destination Port. I changed from the default of GE1 to GE10.
   c. Select the Source Interface. This is the port to which your ATA is connected and whose network traffic you want to see. In this example, I use GE1. [Leave VLAN unselected]
   d. Select the Type of **Tx and Rx** to allow you to see all network traffic transmitted (Tx) and received (Rx) by the connected ATA.
   e. Click Apply.



Add Port and VLAN Mirroring - Google Chrome

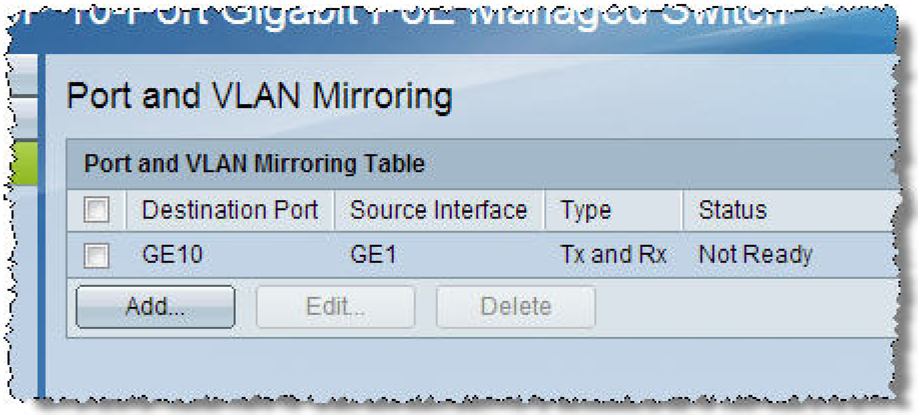
192.168.1.253/cs57eb2e1b/diagnostics/maintenance_diagnos_portMirror

Destination Port: GE10

Source Interface: ● Port GE1 ○ VLAN 1

Type: ○ Rx Only
○ Tx Only
● Tx and Rx

f. The Port and VLAN Mirroring Table is updated with the change:



Port and VLAN Mirroring

Port and VLAN Mirroring Table

□	Destination Port	Source Interface	Type	Status
□	GE10	GE1	Tx and Rx	Not Ready

g. Save the switch's configuration.

4. Connect to port GE10 of the switch, the network cable from the Wireshark interface.
5. Connect to port GE1 of the switch, the network cable from the ATA that you want to monitor.
6. You've now completed configuring the network switch.

Using Wireshark

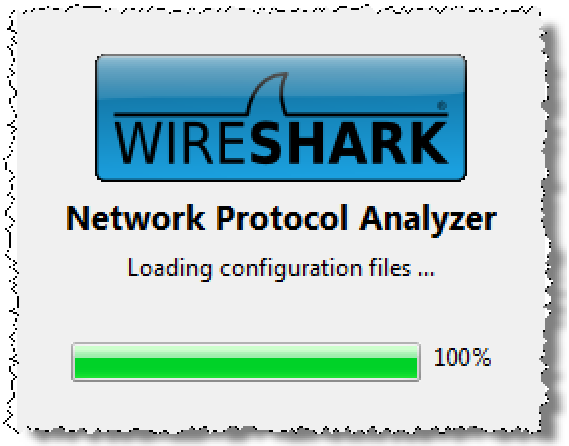
Wireshark is extremely capable and very powerful. This section provides the bare minimum information to get you started. The Wireshark University provides an excellent source of deep technical training on using Wireshark and protocol analysis.

Starting Wireshark for the First Time

Make sure that the network interface that you plan to use for Wireshark captures is properly connected to your computer and to the network switch, or else Wireshark may not properly detect the interface when Wireshark starts up. Locate the Wireshark shortcut on your desktop if you installed a shortcut during Wireshark installation. Otherwise, click Start > All Programs > and locate and double-click the Wireshark icon

Wireshark

Wireshark will load its configuration files and display its progress:



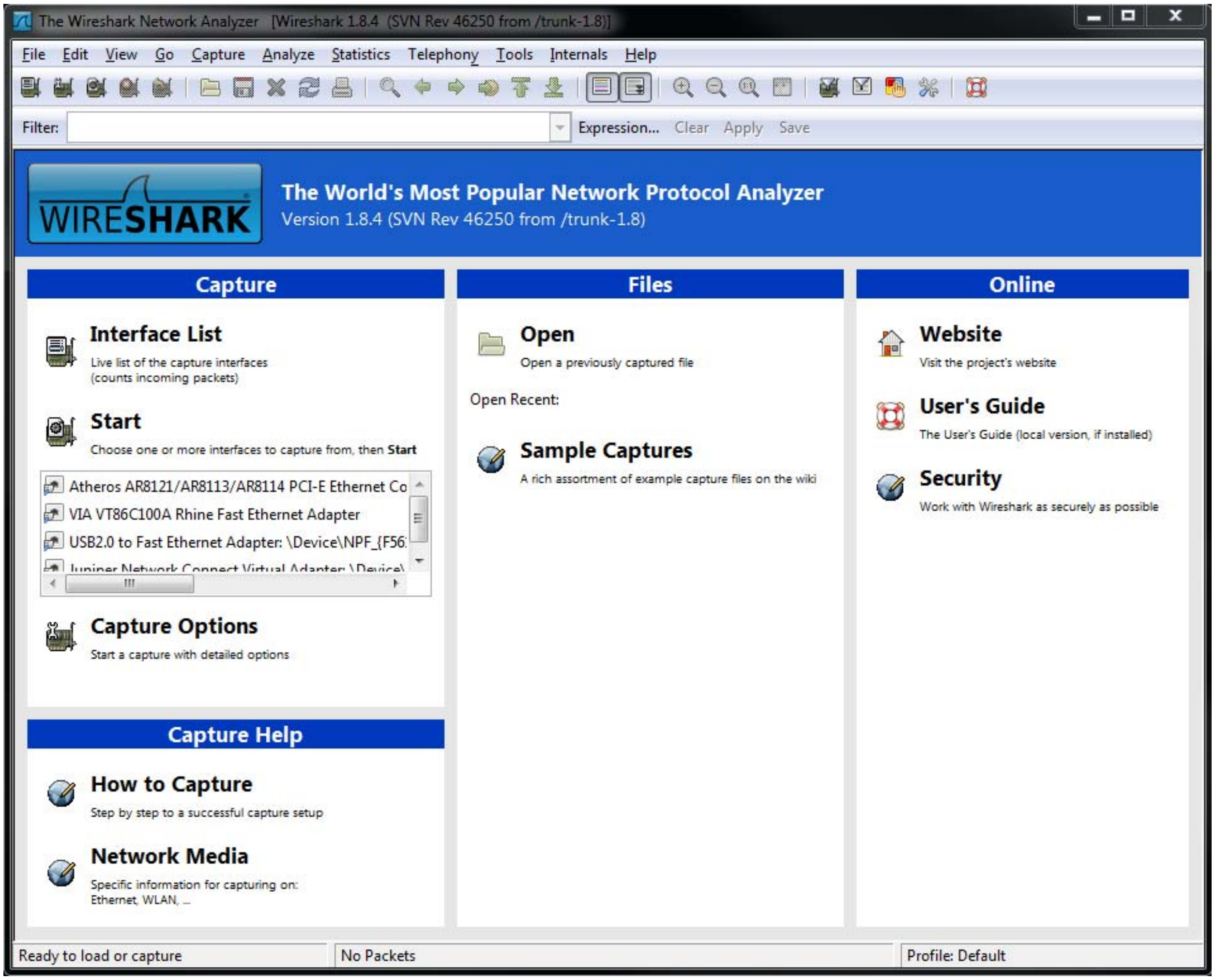
WIRESHARK

Network Protocol Analyzer

Loading configuration files ...

100%

Once Wireshark is running, its main interface will display:


The Wireshark Network Analyzer [Wireshark 1.8.4 (SVN Rev 46250 from /trunk-1.8)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save
WIRESHARK
Capture
Files
Online
Capture Help

The World's Most Popular Network Protocol Analyzer
Version 1.8.4 (SVN Rev 46250 from /trunk-1.8)

Interface List
Live list of the capture interfaces (counts incoming packets)

Start
Choose one or more interfaces to capture from, then **Start**

Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Co
VIA VT86C100A Rhine Fast Ethernet Adapter
USB2.0 to Fast Ethernet Adapter: \Device\NPF_{F56:
Juniper Network Connect Virtual Adapter: \Device\

Capture Options
Start a capture with detailed options

How to Capture
Step by step to a successful capture setup

Network Media
Specific information for capturing on: Ethernet, WLAN, ...

Open
Open a previously captured file

Open Recent:

Sample Captures
A rich assortment of example capture files on the wiki

Website
Visit the project's website

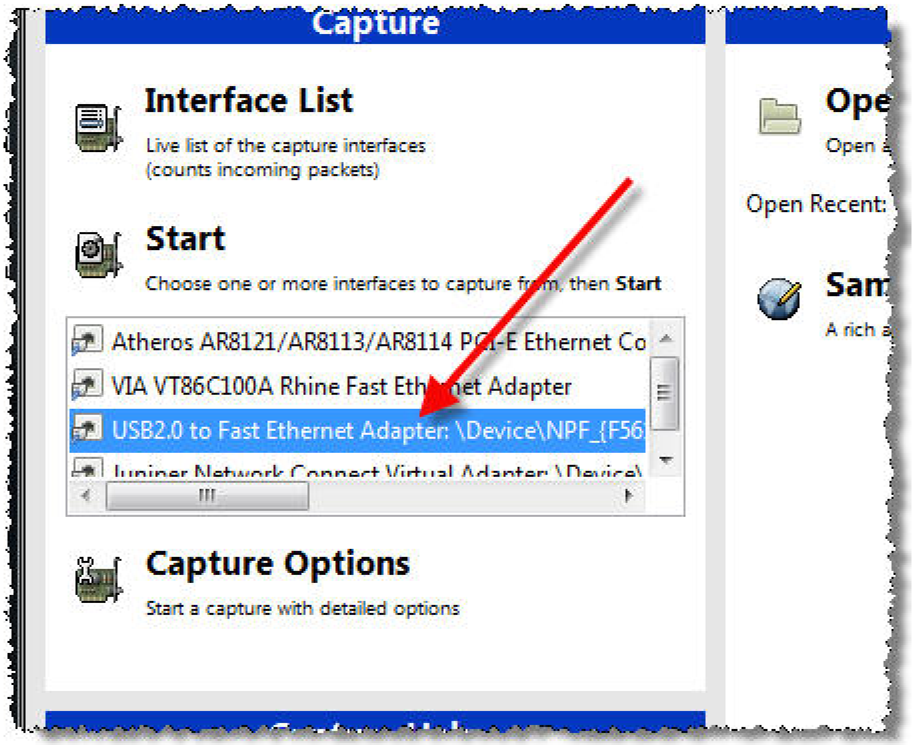
User's Guide
The User's Guide (local version, if installed)

Security
Work with Wireshark as securely as possible

Ready to load or capture | No Packets | Profile: Default

Selecting a Wireshark Capture Interface

You must select an interface from the available interfaces on your computer. In this example, I'll select the USB2.0 to Fast Ethernet Adapter from the list:



Capture

Interface List

Live list of the capture interfaces (counts incoming packets)

Start

Choose one or more interfaces to capture from, then **Start**

Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Co

VIA VT86C100A Rhine Fast Ethernet Adapter

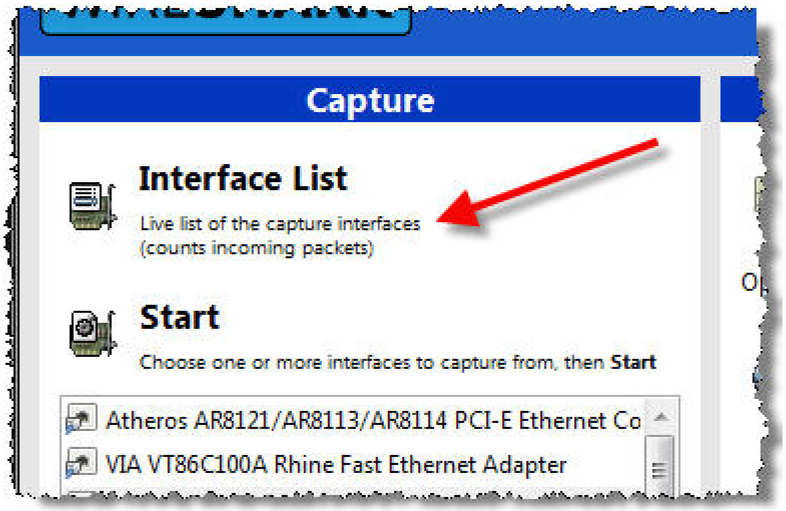
USB2.0 to Fast Ethernet Adapter: \Device\NPF_{F56

Juniper Network Connect Virtual Adapter: \Device\

Capture Options

Start a capture with detailed options

If you are not sure which interface to use, click Interface List to view details about each interface which may help with your selection:



Capture

Interface List

Live list of the capture interfaces (counts incoming packets)

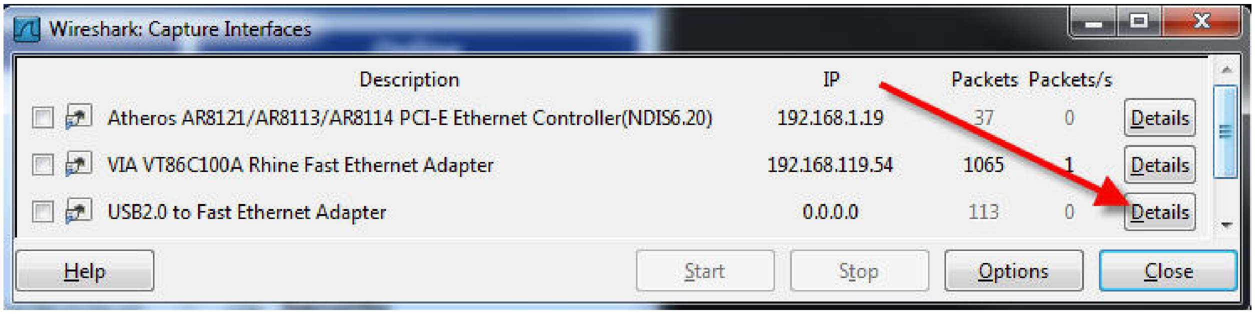
Start

Choose one or more interfaces to capture from, then **Start**

Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Co

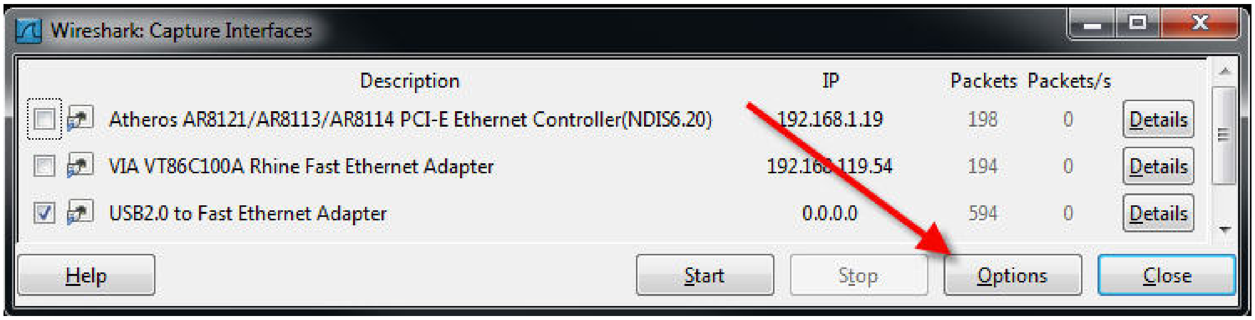
VIA VT86C100A Rhine Fast Ethernet Adapter

You can also click the Details button if you need more help selecting the appropriate interface:


Wireshark: Capture Interfaces

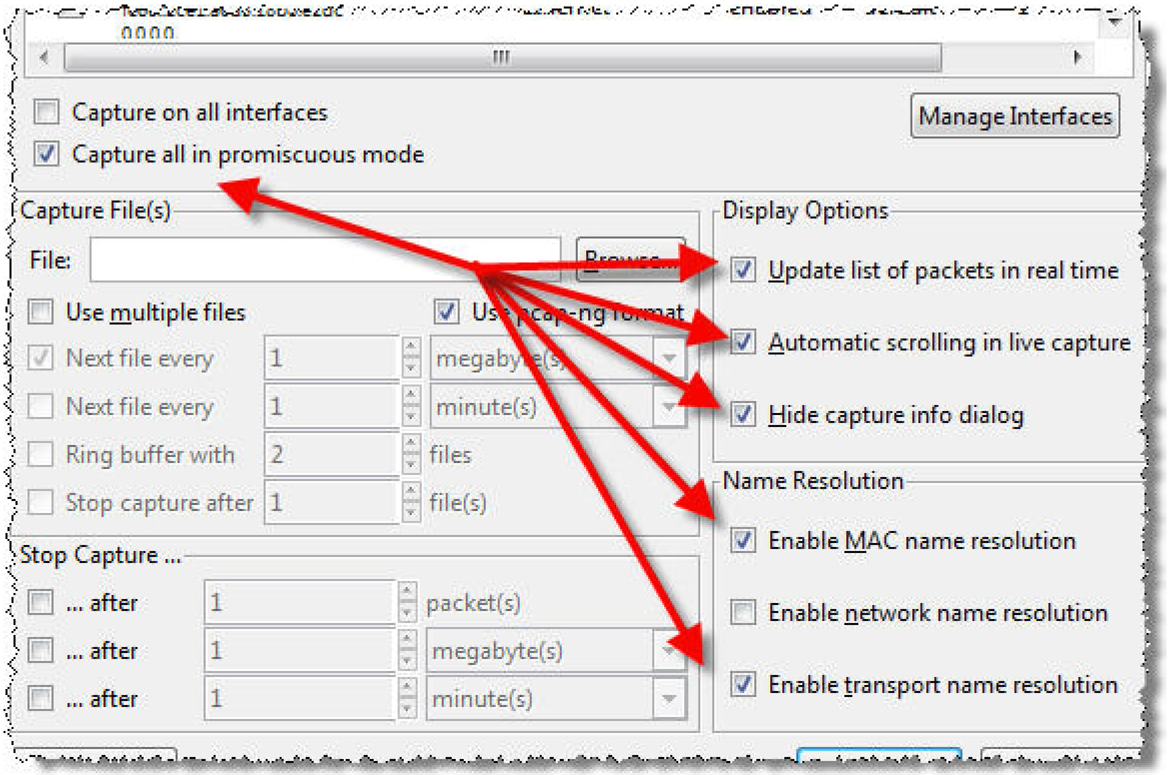
	Description	IP	Packets	Packets/s	
□	Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller(NDIS6.20)	192.168.1.19	37	0	Details
□	VIA VT86C100A Rhine Fast Ethernet Adapter	192.168.119.54	1065	1	Details
□	USB2.0 to Fast Ethernet Adapter	0.0.0.0	113	0	Details

Once you've selected the appropriate interface, click Options to make user-display selections:


Wireshark: Capture Interfaces

	Description	IP	Packets	Packets/s	
□	Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller(NDIS6.20)	192.168.1.19	198	0	Details
□	VIA VT86C100A Rhine Fast Ethernet Adapter	192.168.119.54	194	0	Details
☑	USB2.0 to Fast Ethernet Adapter	0.0.0.0	594	0	Details

I find these options to be best for my every-day use:


0.0.0.0

□ Capture on all interfaces
☑ Capture all in promiscuous mode

Capture File(s)
File:
□ Use multiple files ☑ Use pcap-ng format
☑ Next file every 1 megabyte(s)
□ Next file every 1 minute(s)
□ Ring buffer with 2 files
□ Stop capture after 1 file(s)

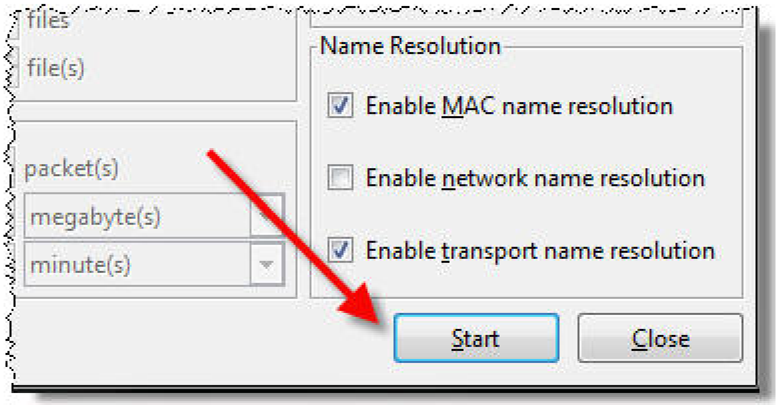
Stop Capture ...
□ ... after 1 packet(s)
□ ... after 1 megabyte(s)
□ ... after 1 minute(s)

Display Options
☑ Update list of packets in real time
☑ Automatic scrolling in live capture
☑ Hide capture info dialog

Name Resolution
☑ Enable MAC name resolution
□ Enable network name resolution
☑ Enable transport name resolution

Starting a Capture

You're finally ready to start your first capture. Click any of the Start buttons:



files
file(s)
packet(s)
megabyte(s)
minute(s)

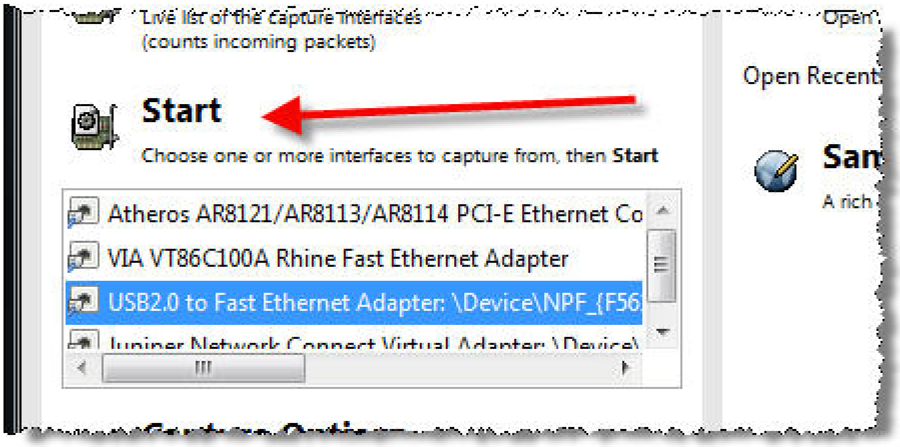
Name Resolution

☑ Enable MAC name resolution

☐ Enable network name resolution

☑ Enable transport name resolution

Or:



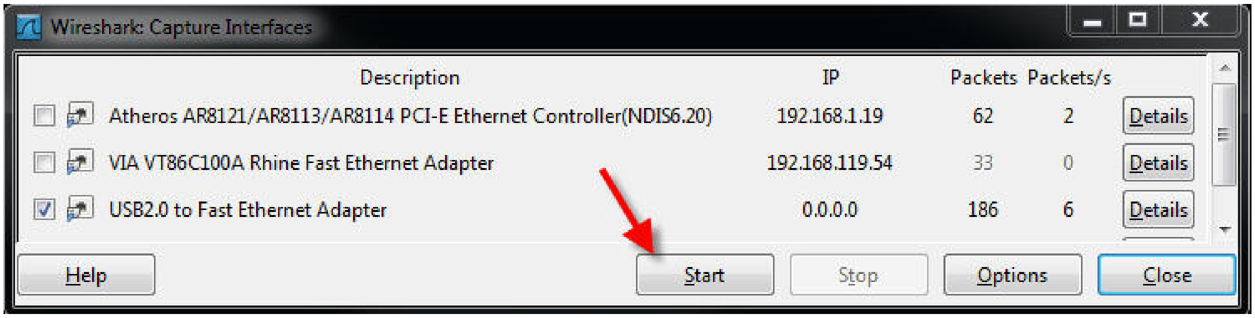
Live list of the capture interfaces
(counts incoming packets)

Start

Choose one or more interfaces to capture from, then **Start**

- Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Co
- VIA VT86C100A Rhine Fast Ethernet Adapter
- USB2.0 to Fast Ethernet Adapter: \Device\NPF_{F56
- Juniper Network Connect Virtual Adapter: \Device\

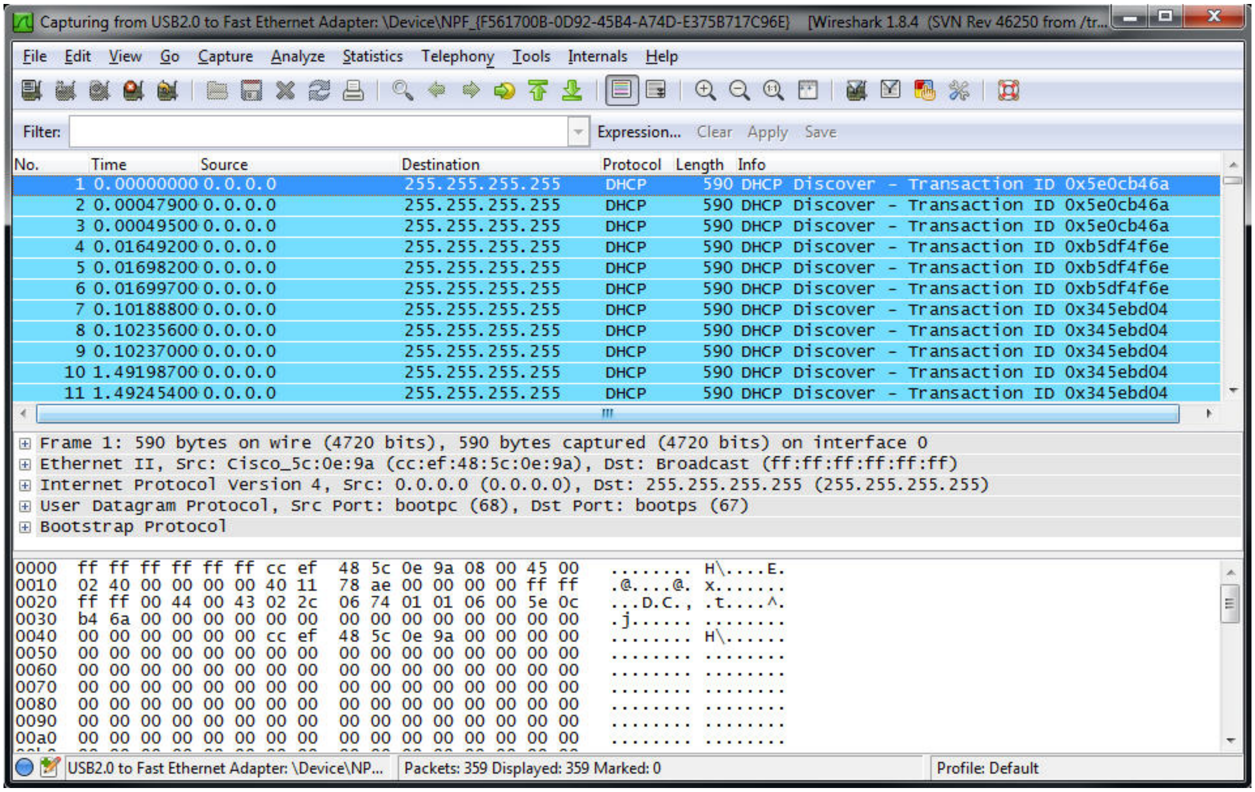
Or:



Wireshark: Capture Interfaces

	Description	IP	Packets	Packets/s	
☐	Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller(NDIS6.20)	192.168.1.19	62	2	Details
☐	VIA VT86C100A Rhine Fast Ethernet Adapter	192.168.119.54	33	0	Details
☑	USB2.0 to Fast Ethernet Adapter	0.0.0.0	186	6	Details

Wireshark will display the capture window:


Capturing from USB2.0 to Fast Ethernet Adapter: \Device\NPF_{F561700B-0D92-45B4-A74D-E375B717C96E}   [Wireshark 1.8.4 (SVN Rev 46250 from /tr...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.     Time       Source      Destination       Protocol  Length  Info
      1 0.00000000 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0x5e0cb46a
      2 0.00047900 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0x5e0cb46a
      3 0.00049500 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0x5e0cb46a
      4 0.01649200 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0xb5df4f6e
      5 0.01698200 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0xb5df4f6e
      6 0.01699700 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0xb5df4f6e
      7 0.10188800 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0x345ebd04
      8 0.10235600 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0x345ebd04
      9 0.10237000 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0x345ebd04
     10 1.49198700 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0x345ebd04
     11 1.49245400 0.0.0.0     255.255.255.255   DHCP      590 DHCP Discover - Transaction ID 0x345ebd04
```

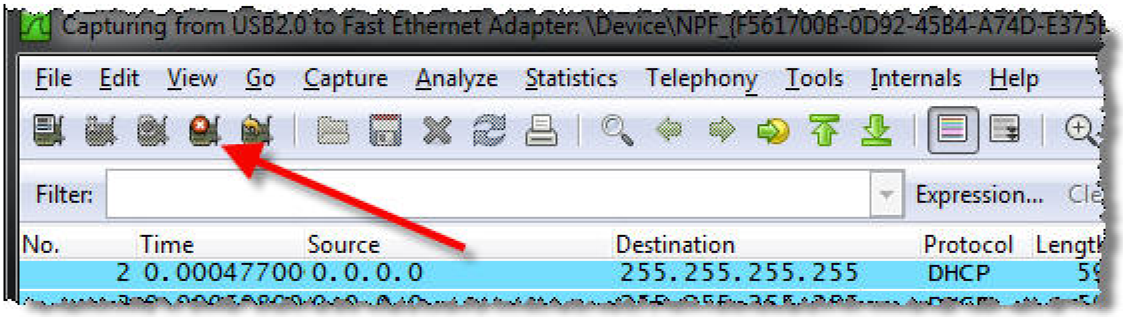
```
⊞ Frame 1: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
⊞ Ethernet II, Src: Cisco_5c:0e:9a (cc:ef:48:5c:0e:9a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
⊞ User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
⊞ Bootstrap Protocol
```

```
0000  ff ff ff ff ff ff cc ef  48 5c 0e 9a 08 00 45 00   ........ H\....E.
0010  02 40 00 00 00 00 40 11  78 ae 00 00 00 00 ff ff   .@....@. x.......
0020  ff ff 00 44 00 43 02 2c  06 74 01 01 06 00 5e 0c   ...D.C., .t....^.
0030  b4 6a 00 00 00 00 00 00  00 00 00 00 00 00 00 00   .j...... ........
0040  00 00 00 00 00 00 cc ef  48 5c 0e 9a 00 00 00 00   ........ H\......
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

USB2.0 to Fast Ethernet Adapter: \Device\NP... | Packets: 359 Displayed: 359 Marked: 0 | Profile: Default

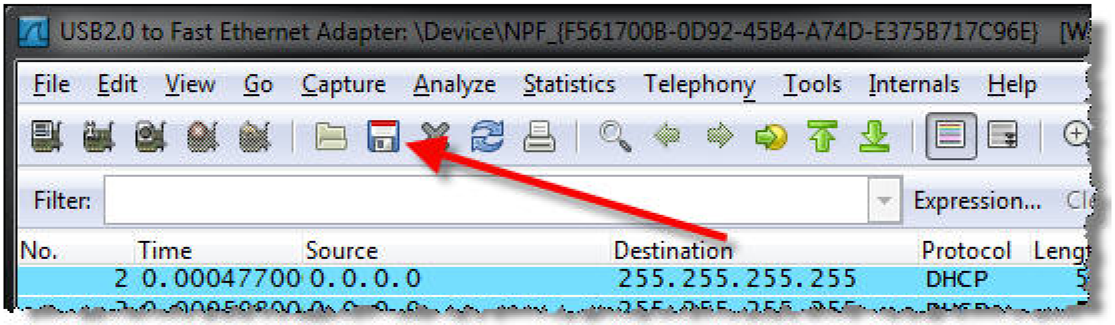
Stopping and Saving a Capture

Once you have replicated the scenario that you wanted to capture, for example, the SPA ATA's network behavior when power is applied to it, you must stop the capture by clicking on the stop icon:


Capturing from USB2.0 to Fast Ethernet Adapter: \Device\NPF_{F561700B-0D92-45B4-A74D-E375
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Cle

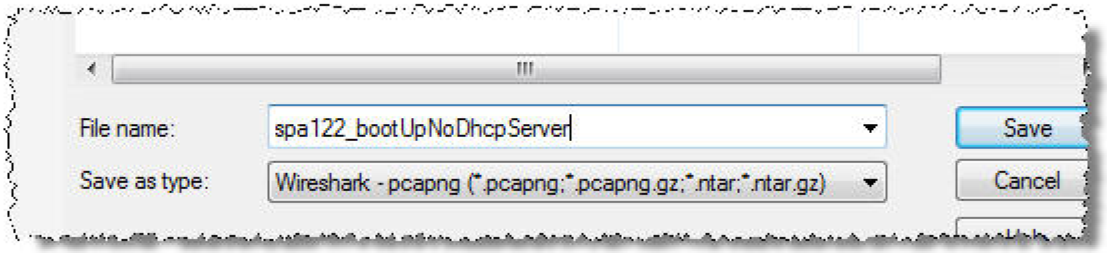
No.	Time	Source	Destination	Protocol	Length
2	0.00047700	0.0.0.0	255.255.255.255	DHCP	59

Once the capture is stopped, click the save icon:


USB2.0 to Fast Ethernet Adapter: \Device\NPF_{F561700B-0D92-45B4-A74D-E375B717C96E} [W
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Cle

No.	Time	Source	Destination	Protocol	Length
2	0.00047700	0.0.0.0	255.255.255.255	DHCP	5

When saving the Wireshark trace, be sure to use a descriptive name to help you easily recall why you captured the trace.


File name: spa122_bootUpNoDhcpServer

Save as type: Wireshark - pcapng (*.pcapng;*.pcapng.gz;*.ntar;*.ntar.gz)

You can now locate the trace on your storage device and compress it and share with someone for analysis.

<end>