



# APPLICATION NOTE

THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

**Product Family:** N/A

**Number:** AN-MISC-033

**Subject:** Using Wireshark to view/capture ethernet data

**Date Issued:** 5-5-2013

**Revision:** Original

Tools Needed:

- PC with Wireshark installed ([www.wireshark.org](http://www.wireshark.org))
- An Ethernet hub or a managed switch with "Port mirroring" capability

Wireshark installation is pretty straight forward. Be sure to install the WinPcap when it prompts you to. This is necessary to be able to capture the data.

Ethernet hubs are very difficult to find but they are by far the easiest to setup for a capture. You can still buy Netgear DS108 hubs occasionally but you have to search pretty extensively for them. Beware of switches that say they are hubs. The only way you will be able to tell is by trial and error in trying to capture data that you know for sure is present on a different port than your PC.

It is important to note that using both hubs and managed switches with port mirroring will affect the network timing. Port mirroring will affect the relative packet timing. You will also not be able to trust the timing that you see in Wireshark for the packets coming from the port mirror. The switch will typically queue up several mirrored packets before sending them out the port to Wireshark. Using a hub will force the devices to half duplex which will significantly affect the timing to all devices connected to the hub. The methods above should only be used for logical flow analysis and packet coherency. They should not be used to troubleshoot network timing issues. More complicated methods will have to be employed for this (using network taps or a PC with bridged network interfaces and using special software).

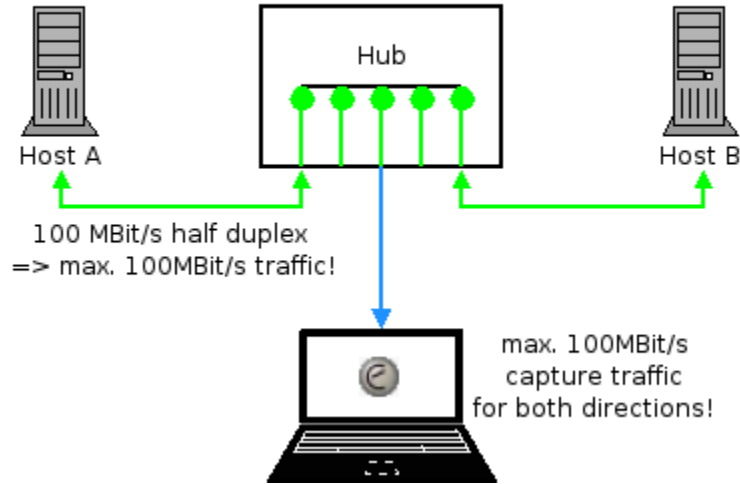
Also note that if you are capturing data coming from or to the PC that is running Wireshark, no hub or special switch is needed. This can be useful if testing Modbus and using the Modbus simulator tools (Modbus Poll and Modbus Slave). If you are capturing DirectSoft data, Lookout Direct or Kepware stuff, you shouldn't need a special switch or hub.



**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

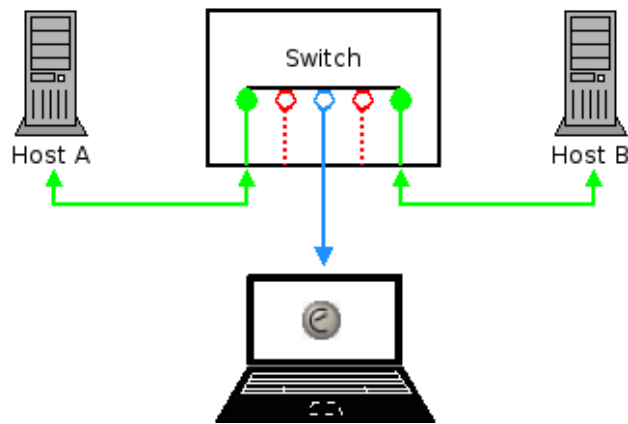
These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

## Shared Media



Example of a hub setup.

## Switched Media (with monitor port)



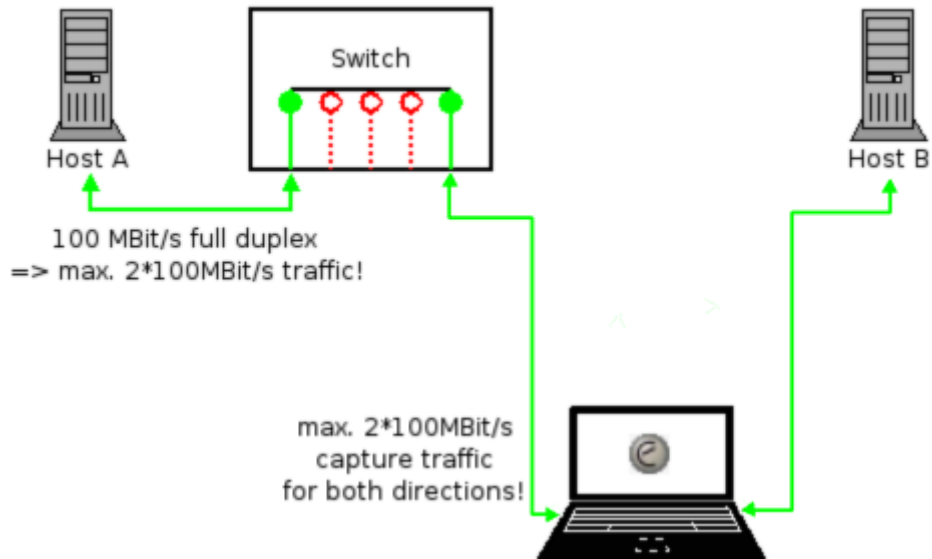
Example of a port mirror setup.



**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

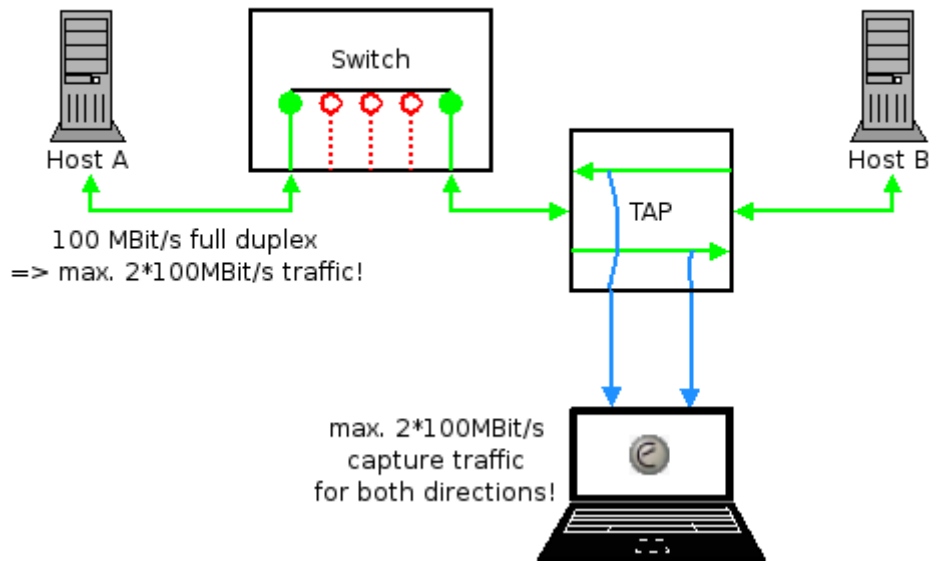
These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

### Machine-in-the-middle



Example of using a PC with 2 network interfaces.

### Switched Media (with TAP)



Example of using a Network Tap (note that a Tap has 2 outputs which equates to difficulty of use with Wireshark).



**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

Setting up port mirroring on a managed switch is pretty simple with most switches. Basically, all you are doing is tell the switch to take data coming from 1 port and to send it out another port (the port that your PC running Wireshark is connected to). The example shown below is how you would accomplish this with our Stride Managed switches. In the example below, you would plug the PC running Wireshark into Port 1 (the Monitor port) and you would be able to see all of the traffic that is going in and out of Port 4. Multiple ports could be enabled to monitor.

**Stride**  
WEB INTERFACE TOOL  
brought to you by  
AUTOMATIONDIRECT

[Quick Setup](#) [Help Index](#)

Managed Switch Menu  
Monitoring  
Setup  
Main Settings

- System Settings
- Remote Access Security
- Port Settings
- Port Mirroring
- Set IP per Port
- Switch Time Settings
- Manage Firmware
- Install Firmware

Redundancy Settings  
Traffic Priority  
Multicast Filtering (IGMP)  
Virtual LANs (VLANs)  
Security Settings  
Monitoring Settings  
Advanced Operations

---

**Model:** SE-SV6MG-4P  
**Serial number:** 5006655  
**Firmware rev:** 5.0.130  
**MAC address:** 00:a0:1d:18:b6:0a

---

**Name:** SE-SV6MG-4P  
**IPv4 address:** 10.11.0.92/16  
**IPv6 address:** fe80::2a0:1dff:fe18:b60a/64  
**Location:** <Set location of switch>  
**Contact:** <Set name (and e-mail) of contact for switch>

Usage subject to [Software License Agreement](#).

**PORT MIRRORING** [Help](#)

Perform advanced diagnostics by using port mirroring to copy messages from one or more source ports to a monitor port connected to a network analysis software.

Monitor port

Port	Name	Data to Monitor
1	port_1	None
2	port_2	None
3	port_3	None
4	port_4	Both
5	port_5	None
6	port_6	None
7	port_7	None
8	port_8	None

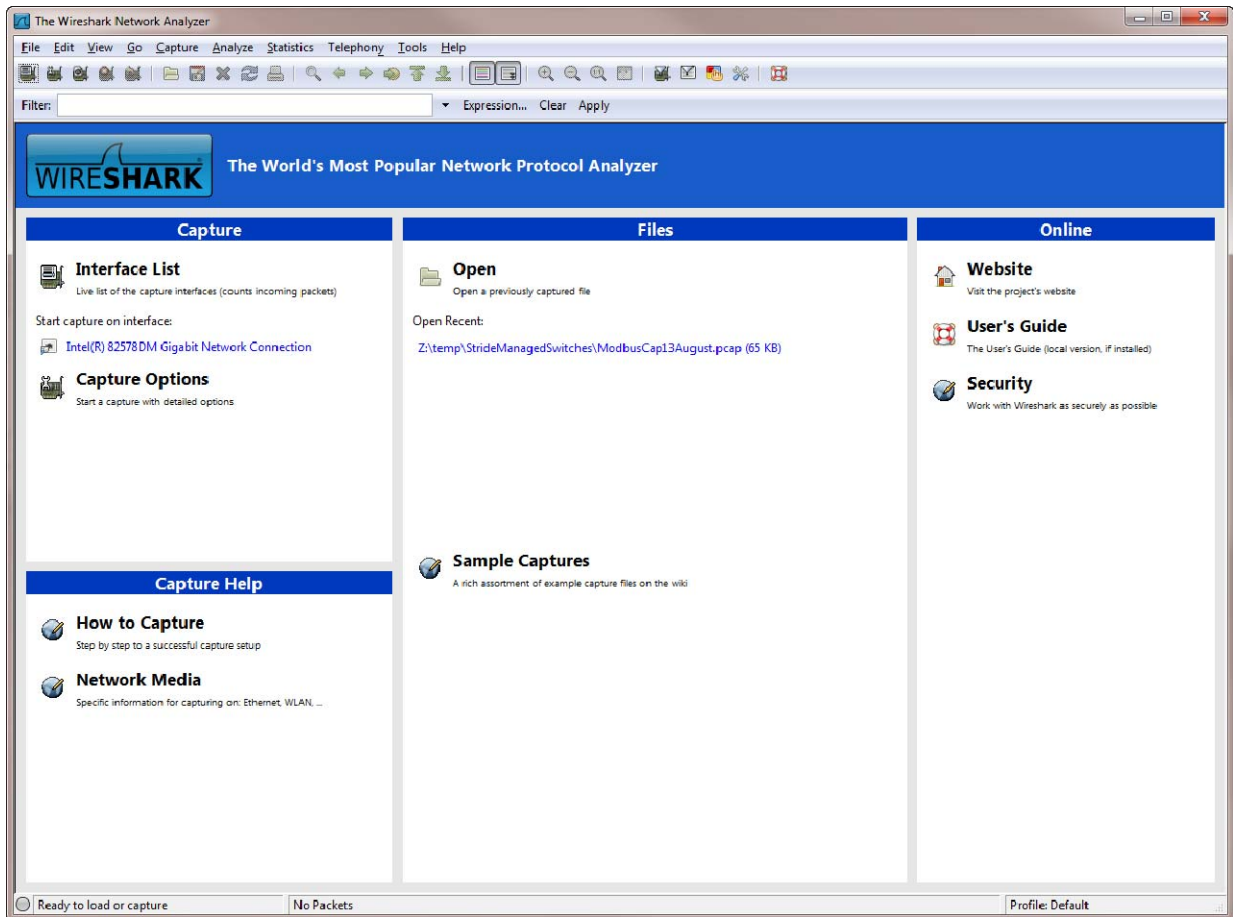


**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

Instructions:

Start Wireshark session:

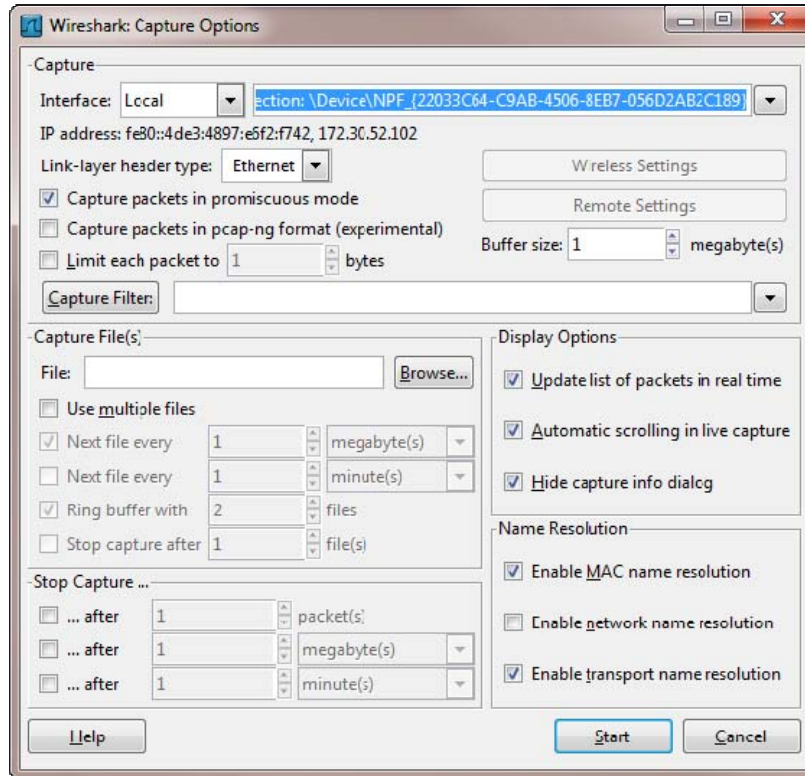




**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

Click on Capture and Options:



There are several important selections in this dialog box.

- Interface: On many PCs, there are multiple Network cards. You will need to select the network card that is physically connected to the hub or port mirror output port. The easiest way to figure out which interface to use is simple trial and error. Pick one, start the capture and look for data. If you don't see it, stop the capture, pick a different interface and try again until you see the data you are expecting. You can also choose Capture>Interfaces to quickly choose the interface you want capture data on. In that dialog box, it shows the traffic that is currently being seen by the interfaces. This may help in determining which interface you want to capture.
- Buffer size: If you are expecting a long capture, increase the buffer size to a sufficiently large number. If you increase the number to too large a value it will bog down your PC.
- Capture packets in promiscuous mode: Leave this on
- Limit each packet: It's best to leave this off.
- Capture Filter: This is good to use when doing long captures. You can select the IP addresses of the devices you care about and it will only save the data for those devices and you can save tremendously on file size.
- Display options: This is completely based on personal preference. If you are looking for specific events that are occurring frequently, turn all these on and you can see the traffic as it is being captured.



**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

- Name Resolution: Leave as set above.
- Capture Files: This is used for very long captures. You can set it up to capture to multiple files to keep the file size smaller.
- Stop Capture: You can use this to automatically stop the capture based on file size, packet count or time.

The dialog below shows a quick way of choosing the Interface to capture on if you do not need the more advanced selections of the Capture>Options window.



You can also click on the Details button in the Wireshark Capture Interfaces dialog to cross reference with the Network Interface properties.

Once you have made all the correct selections, hit the Start button and Wireshark will start capturing data.





**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

The screenshot shows the Wireshark interface with a packet capture of Modbus/TCP traffic. The top pane displays a list of packets with columns for No., Time, Source, Destination, and Protocol Info. The middle pane shows the details of a selected Modbus/TCP packet, including transaction identifier, protocol identifier, length, unit identifier, and Modbus function (Read multiple registers). The bottom pane shows the raw packet bytes in hex and ASCII format.

No.	Time	Source	Destination	Protocol	Info
10	4.058062	10.11.0.101	10.11.0.85	Modbus/	query [ 1 pkt(s)]: trans: 5932; unit: 1, func: 3: Read multiple reg
11	4.058624	10.11.0.85	10.11.0.101	TCP	asa-app1-prot0 > deskshare [ACK] Seq=30 Ack=25 win=8180 Len=0
12	4.059766	10.11.0.85	10.11.0.101	Modbus/	response [ 1 pkt(s)]: trans: 5932; unit: 1, func: 3: Read multiple reg
13	4.091262	10.11.0.101	10.11.0.85	Modbus/	query [ 1 pkt(s)]: trans: 5933; unit: 1, func: 3: Read multiple reg
14	4.091962	10.11.0.85	10.11.0.101	TCP	asa-app1-prot0 > deskshare [ACK] Seq=59 Ack=37 win=8180 Len=0
15	4.093101	10.11.0.85	10.11.0.101	Modbus/	response [ 1 pkt(s)]: trans: 5933; unit: 1, func: 3: Read multiple reg
16	4.113729	10.11.0.101	10.11.0.85	Modbus/	query [ 1 pkt(s)]: trans: 5934; unit: 1, func: 3: Read multiple reg
17	4.114374	10.11.0.85	10.11.0.101	TCP	asa-app1-prot0 > deskshare [ACK] Seq=88 Ack=49 win=8180 Len=0
18	4.115526	10.11.0.85	10.11.0.101	Modbus/	response [ 1 pkt(s)]: trans: 5934; unit: 1, func: 3: Read multiple reg
19	4.146933	10.11.0.101	10.11.0.85	Modbus/	query [ 1 pkt(s)]: trans: 5935; unit: 1, func: 3: Read multiple reg
20	4.147489	10.11.0.85	10.11.0.101	TCP	asa-app1-prot0 > deskshare [ACK] Seq=117 Ack=61 win=8180 Len=0
21	4.148631	10.11.0.85	10.11.0.101	Modbus/	response [ 1 pkt(s)]: trans: 5935; unit: 1, func: 3: Read multiple reg
22	4.180136	10.11.0.101	10.11.0.85	Modbus/	query [ 1 pkt(s)]: trans: 5936; unit: 1, func: 3: Read multiple reg
23	4.180818	10.11.0.85	10.11.0.101	TCP	asa-app1-prot0 > deskshare [ACK] Seq=146 Ack=73 win=8180 Len=0

Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)  
Ethernet II, Src: AsustekC\_e0:7d:d7 (00:1a:92:e0:7d:d7), Dst: HostEngi\_90:00:cc (00:c0:62:90:00:cc)  
Internet Protocol, Src: 10.11.0.101 (10.11.0.101), Dst: 10.11.0.85 (10.11.0.85)  
Transmission Control Protocol, Src Port: deskshare (1702), Dst Port: asa-app1-prot0 (502), Seq: 25, Ack: 59, Len: 12  
Modbus/TCP  
transaction identifier: 5933  
protocol identifier: 0  
length: 6  
unit identifier: 1  
Modbus  
function 3: Read multiple registers  
reference number: 0  
word count: 10

```
0000 00 e0 52 90 00 ec 00 1a 92 e0 7d d7 08 00 45 00  .b.....E...  
0010 00 34 f2 2c 40 00 80 06 f3 c7 0a 0b 00 65 0a 0b  .4.8.....e...  
0020 00 55 06 a6 01 f6 ff 0c cc 73 00 f9 84 bc 50 18  .U.....s...P.  
0030 ff c5 29 19 00 00 17 2d 00 00 00 06 01 03 00 00  .).....  
0040 00 0a
```

There are 3 panes that contain the packet data. The top pane contains the network Packet List. It contains a list of all the packets going back and forth between the different devices (depending upon whether you are using a hub, port mirroring on managed switch and filter settings). The middle pane is the Packet Details view that interprets the data bytes and displays them in a more easily read fashion. The bottom pane is the Packet Bytes view shown in hex format.

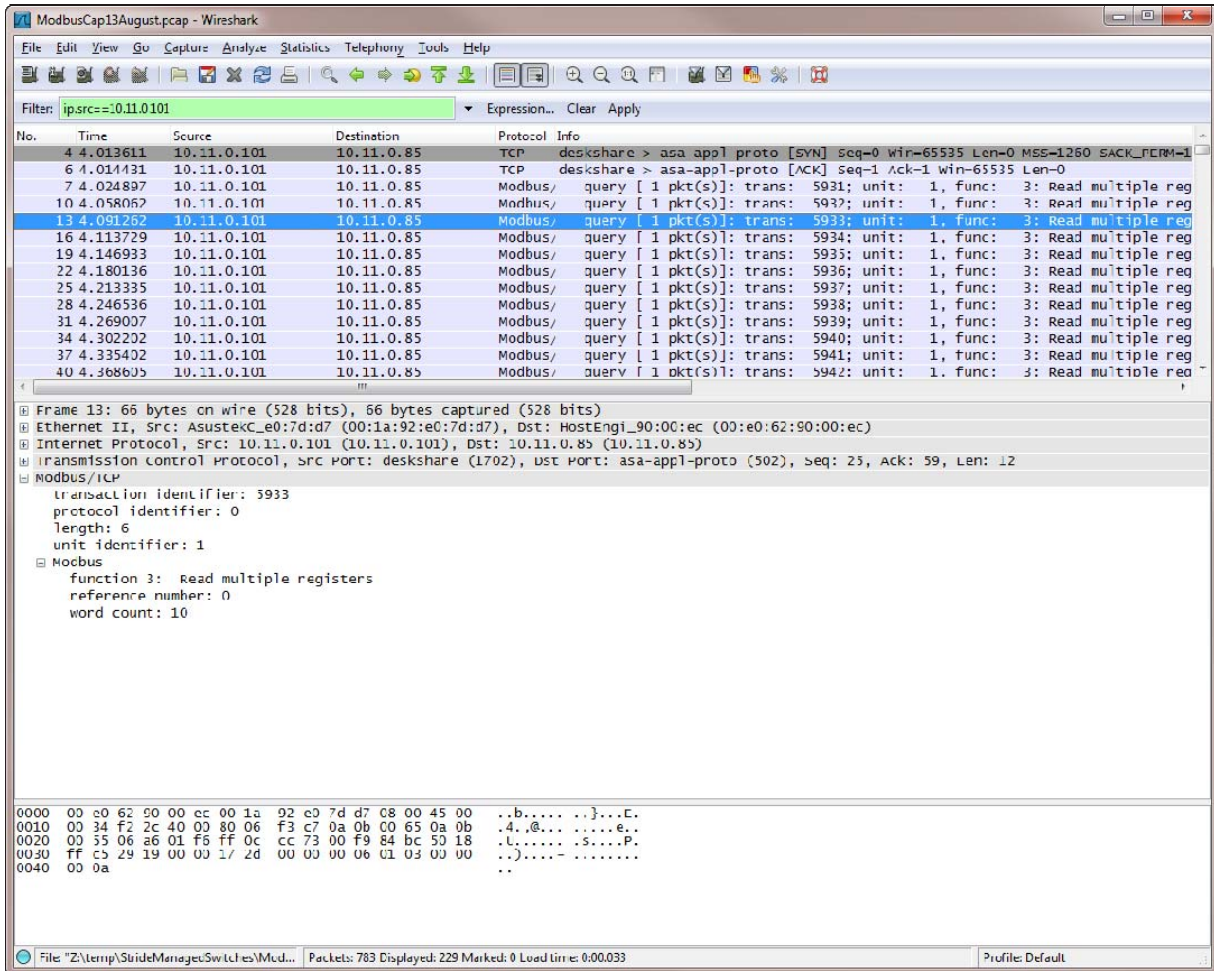
There is also a Display Filter option that can be used to remove some of the 'chatter' that you see in the Packet List pane but still have the data available to view if needed by clearing out the display filter. Here is an example of a display filter to show all of the packets that were sourced from a specific IP address. To view the different syntax and filter options available, click on the Expression button to the right of the Display filter line.





**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.



Some examples of Display filters:

ip.src == 10.11.0.101 (Shows only packets where 10.11.0.101 is the source device)

ip.addr == 10.11.0.101 (Shows only packets where 10.11.0.101 is the source or destination)

tcp (Shows only packets where TCP protocol is in the packet)

Other useful display filters for ADC products:

tcp.port==502 works for Modbus TCP

tcp.port==44818 works for EtherNet/IP

udp.port==2222 works for EtherNet/IP I/O Messaging

udp.port==28784 for HOST Ethernet products (EBC100, ECOM100, EDRV, etc..)

udp.port==8888 works for Productivity3000 discovery

udp.port==9999 works for Productivity3000 software connection

tcp.port==9999 works for C-more Programming Software

tcp.port==25 for SMTP email, also typing in smtp works as well

tcp.port==21 for FTP

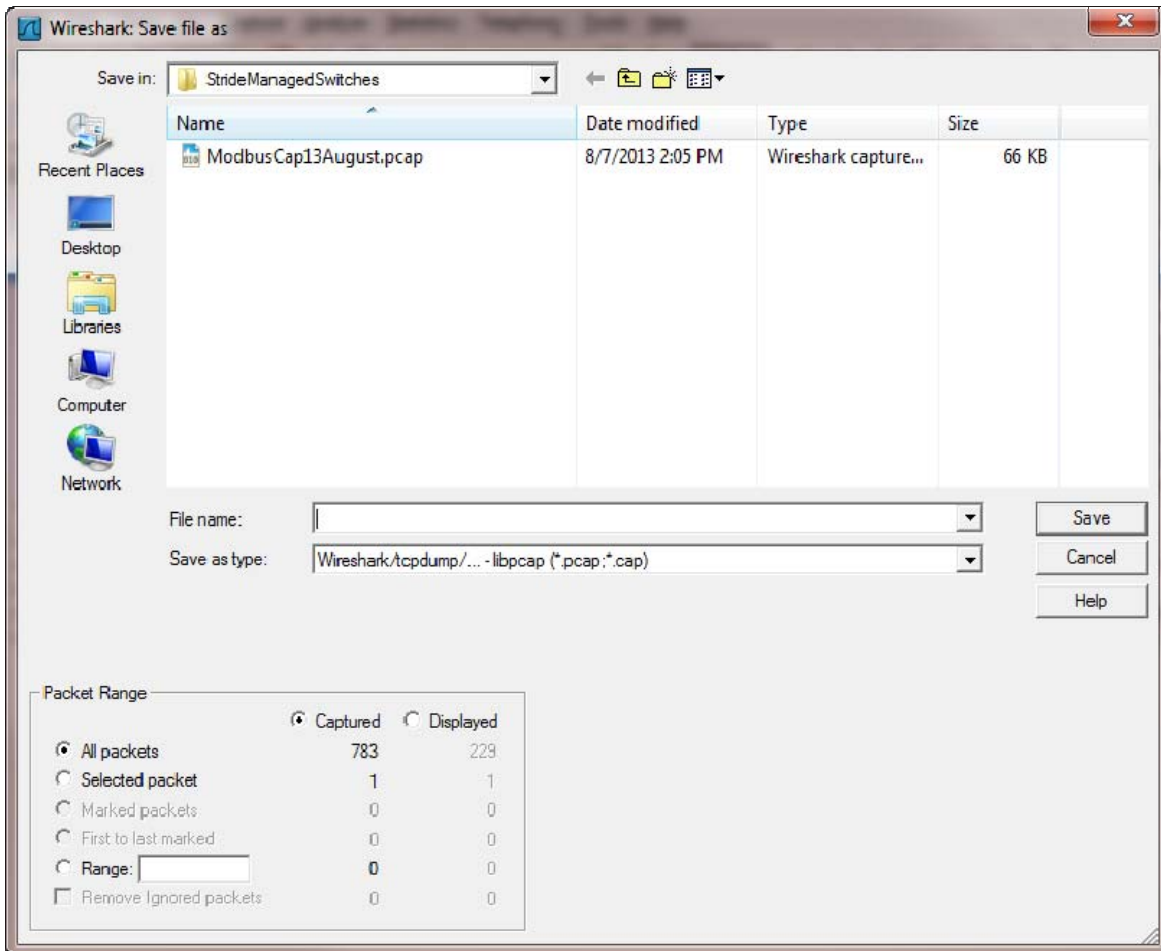


**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

tcp.port==11110 for C-more passthrough  
tcp.port==80 for web servers  
tcp.port==11102 for C-more remote access

To save a capture, simply click on File>Save As. There are a couple of choices you can make. You can save only the data shown after the Display filter is applied or you can save all of the captured data. You can also choose a range of Ethernet frames to save.



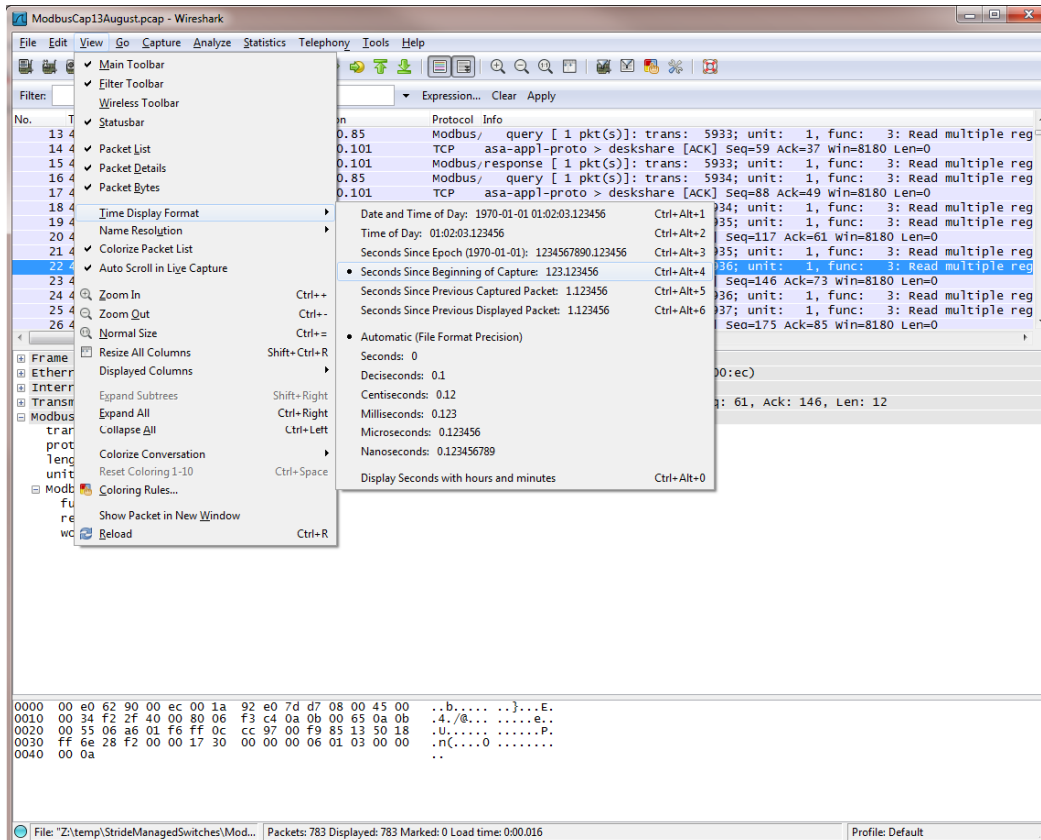
Also note that the PCAP file will ZIP very well. It will typically save to about 20% of the size of the original file. Very good for emailing...



**THIS INFORMATION PROVIDED BY AUTOMATIONDIRECT.COM TECHNICAL SUPPORT IS PROVIDED "AS IS" WITHOUT A GUARANTEE OF ANY KIND.**

These documents are provided by our technical support department to assist others. We do not guarantee that the data is suitable for your particular application, nor do we assume any responsibility for them in your application.

Another setting that is used frequently is the Time Display format that is shown on the left hand side in the Traffic view pane. Sometimes it is easier to view the time elapsed from the previous packet and sometimes it is easier to view the time elapsed from the beginning of the capture to more easily reference time between non-adjacent packets. To change this view, go to View>Time Display Format and you will see the various selections there.



## Technical

**Assistance:** If you have questions regarding this Application Note, please contact us at 770-844-4200 for further assistance.