Using Wireshark for Trouble Shooting

Hardware Requirements

There are no particular hardware requirements regarding the PC you run Wireshark on. Basically anything running any version of Windows can run Wireshark. There are also Linux and Mac OS X versions.

The "hardware requirement" that is of most concern is the means of connecting to the network. We typically just connect everything Ethernet to a switch and don't worry about it. However, switches are really unmanaged routers, and they filter traffic. Therefore, your PC will not see traffic passing back and forth between two other devices that are not the PC. In order to see that network traffic using Wireshark, you need to come up with the right kind of network connection.

If your PC itself is one end of the network conversation you wish to capture, for example when running ManageEngine or the Network Discovery Tool, then Wireshark will capture all network traffic to and from the PC however connected. It is when your PC wants to simply "eavesdrop" that you run into problems with the network switch.

A while back, 10BaseT hubs were common. A 10BaseT hub is not as smart as a switch and does not filter traffic. If you have an old 10BaseT hub collecting dust somewhere, you now have a new use for it. It will let Wireshark see all traffic from the PC that goes between any other devices connected to that 10BaseT hub. Beware of devices calling themselves "hubs" but support 100BaseT connections. These are switches.

Since manufacturers of hubs decided nobody should have a use for them anymore, they are generally out of production. A list of devices that have been tested can be found here: <u>https://wiki.wireshark.org/HubReference</u>. (Pay attention to comments. This is a list of tested devices, not strictly working devices, meaning some are tested and reported to not work with Wireshark.) Some of the devices listed can still be found on Amazon or eBay. Finding a 10BaseT hub for sale may require a little searching, but there are other alternatives.

One means of monitoring network traffic is to get a managed switch that supports "port mirroring". One such device we have tested is the TP-LINK model TL-SG105E. Setting it up requires utility software (provided with the switch) and takes a little effort to get configured. But once configured, it works well without any further monkeying around. And it is inexpensive.



The other means of monitoring traffic is with the use of a device made specifically for use with Wireshark. The "SharkTap" provides two connections for the network pass-through, and a third "tap" connection where you connect your PC running Wireshark. There is no configuration required. It is the simplest way to monitor network traffic, and it is a current production item available on Amazon (as of 2016).

Examples of Using Wireshark

Using Wireshark is fairly easy. Get a copy at www.wireshark.org and install it. Once installed, running it is straight forward. As of version 2.2.0 of Wireshark, the startup screen looks like the following. Double click on Local Area Connection to start capturing network traffic on your PC's Ethernet port. If you have multiple network connections, they will all be listed. Be sure to select the one that represents your Ethernet connection, typically "Local Area Connection".

The Wireshark Network Analyzer	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u>	ireless <u>T</u> ools <u>H</u> elp
🖌 🔳 🧵 💿 🕌 🛅 🕱 🖻 🔍 👄 🕾 🏵 💆 🚍 🗐 🏵	, G, Q, <u>#</u>
Apply a display filter <ctrl-></ctrl->	Expression +
Welcome to Wireshark	
Open	
CAAAA CER Literature 2016 Liter Cuides 200 Res 2020 Liter Cuid	
C:\AAA_CSI\Literature\2016 User Guides\BB-Pro V230 User Guid	e/v230-tran-v2.pcaping (26 KB)
C:\Users\Jim Hogenson\Documents\v230-snmp.pcapng (3397	(B) +
Capture	
using this filter: 📔 Enter a capture filter	•
Local Area Connection	
	I
Learn	
User's Guide · Wiki · Questions and Answers · Mailing	Lists
You are running Wireshark 2.2.0 (v2.2.0-0-g5368c50 from master-2.2	. You receive automatic updates.
Ready to load or capture	No Packets Profile: Default

The screen will look something like the example below once Wireshark starts collecting data. Click the red icon in the toolbar to stop capturing traffic. Control Solutions technical support will often ask for a copy of the Wireshark data when a network issue seems evident. You can save a copy of all of the network traffic captured under the File menu, and you will generally save it to a .pcap or .pcapng file. A Wireshark log with .pcap extension can be posted directly as an attachment in support tickets while .pcapng needs to be zipped first.

The screen shot below shows Wireshark capturing Modbus TCP traffic between a client and our Babel Buster Pro V210. If you click on a packet, the details of that packet will be displayed in the lower part of the screen. You can expand the tree view to see further detail. In the case of Modbus, we will see function code, register count or data count, etc.

A lot of times you will see a lot of network traffic that is not of interest to you. You can filter network traffic to only display traffic to/from the device you are interested in. Do this by entering "ip.addr==192.168.1.23" in the Filter window as illustrated below. (Substitute your own device's IP address.)

If yers Go Count Andre 2010: Transition Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Image Count Andre 2010: Transition Imag	Capturing	g from Local	Area Connec	tion [Wire	shark 1.12.2	(1122-0	-9898fa2	22 from ma	ster-11	2)]											00	
• • • • • • • • • • • • • • • • • • •	Eile Edit	View Go	Capture A	nalyze Sta	tistics Tel	ephony :	Lools [Internals	Help													
Filter padds:12165123 pression	• • 4	ی ک		x 2 -	Q 🗢 🕏	· 🔊 😵	2		0	Q Q			8 %	1 0	ġ.							
No. Time Source Destination Process() Length, Info	Filter: ip.ad	dr==192.168	1.23					· Express	ion	Clear #	Apply	Save										
<pre>3 8. 053/7700 132.168.1.23 192.168.1.23 TCP 56 03395-502 [ACK] Seq-109 Ack-228 Win-80 Len-0 42 9. 05306500 132.168.1.109 192.168.1.23 TCP 56 03395-502 [ACK] Seq-109 Ack-228 Win-80 Len-0 43 9. 06405/109 142.168.1.23 122.168.1.23 TCP 55 06 3395-502 [ACK] Seq-121 Ack-291 Win-73 Len-0 44 0. 0630501 122.168.1.109 192.168.1.23 TCP 55 06 3395-502 [ACK] Seq-121 Ack-291 Win-73 Len-0 46 10. 053061 122.168.1.109 192.168.1.23 TCP 55 06 3395-502 [ACK] Seq-121 Ack-291 Win-73 Len-0 46 10. 053061 122.168.1.109 192.168.1.23 TCP 55 06 3395-502 [ACK] Seq-133 Ack-291 Win-73 Len-0 46 10. 0574470 132.168.1.109 192.168.1.23 TCP 55 06 3395-502 [ACK] Seq-133 Ack-291 Win-51 Len-0 51 11. 0677840 132.168.1.109 192.168.1.23 TCP 56 06 Query: Trans: 7465 (UIT: 1, Func: 3: Read Holding Registers 52 11. 076450 132.168.1.109 192.168.1.23 TCP 56 06 Query: Trans: 7660; UNT: 1, Func: 3: Read Holding Registers 53 11. 057450 132.168.1.109 192.168.1.23 TCP 56 06 Query: Trans: 7660; UNT: 1, Func: 3: Read Holding Registers 54 11. 057450 132.168.1.109 192.168.1.23 TCP 56 06 Query: Trans: 7660; UNT: 1, Func: 3: Read Holding Registers 54 11. 057450 132.168.1.109 192.168.1.23 TCP 56 06 Query: Trans: 7660; UNT: 1, Func: 3: Read Holding Registers 54 11. 057450 132.168.1.109 192.168.1.23 Hodbus/TCP 66 Query: Trans: 7936; UNT: 1, Func: 3: Read Holding Registers 54 11. 057450 132.168.1.109 192.168.1.23 Hodbus/TCP 66 Query: Trans: 7936; UNT: 1, Func: 3: Read Holding Registers 54 13. 94350 132.168.1.109 192.168.1.23 Hodbus/TCP 66 Query: Trans: 7936; UNT: 1, Func: 3: Read Holding Registers 54 13. 94350 132.168.1.109 192.168.1.23 TCP 56 03 8395-502 [ACK] Seq-137 Ack-378 Win-132 Len-0 64 12. 068149 Ack/378 Min-122 Len-0 64 12. 068149 Ack/378 Min-132 Len-0 64 12. 068149 Ack/378 Min-132 Len-0 64 13. 059050 Trans: 07361 UNT: 1, Func: 3: Read Holding Registers 64 13. 94350 132.168.1.23 Hodbus/TCP 66 Query: Trans: 7456 UNT: 1, Func: 3: Read Holding Registers 64 13. 94350 132.168.1.23 Hodbus/TCP 66 Query: Trans: 7456 UNT: 1, Func: 3: Read Holding Registers 64 13. 945</pre>	No. Tin	me	Source		Destin	ation	2	Protoc	ol	Le	ength	Info										
40 8.3533500129:168.1.109 192.168.1.23 TCP 56 63395+502 [ACK] Seq-109 Ack-262 win-80 Len-0 42 9.656050139:168.1.23 192.168.1.31 Hodbus/TCP 68 Response: Trans: 7165; Unit: 1, Func: 3: Read Holding Registers 44 9.3532500139:168.1.109 192.168.1.23 192.168.1.23 Hodbus/TCP 88 Response: Trans: 7424; Unit: 1, Func: 3: Read Holding Registers 47 10.6734650139:168.1.20 192.168.1.33 TCP 56 63395-502 [ACK] Seq-133 Ack-20 win-83 Len-0 48 0.053450139:168.1.20 192.168.1.33 TCP 56 63395-502 [ACK] Seq-133 Ack-20 win-83 Len-0 49 10.67344570139:168.1.20 192.168.1.33 TCP 56 63395-502 [ACK] Seq-133 Ack-20 win-83 Len-0 52 11.67350139:128.168.1.109 192.168.1.33 TCP 56 63395-502 [ACK] Seq-133 Ack-20 win-83 Len-0 60 12.66150139:168.163.103 192.168.1.33 TCP 56 63395-502 [ACK] Seq-143 Ack-30 win-131 Len-0 61 12.75350139:128.168.1.109 192.168.1.33 TCP 56 63395-502 [ACK] Seq-143 Ack-32 win-33 Len-0 61 12.75350139:128.168.1.109 192.168.1.33 TCP 56 63395-502 [ACK] Seq-143 Ack-345 win-31 Len-0 61 12.75350139:128.168.1.109 192.168.1.33 TCP 56 63380-502 [ACK] Seq-145 Ack-345 win-31 Len-0	39 8.	. 63547700	192.168	1.23	192.	168.1.1	09	Modb	us/TC	P	83	Respons	e: Tra	ns :	6912;	Unit:	1. Fund	: 3	Read	Holding	Register	s
42 9.63968900182.165.1.20 192.165.1.20 Modbus/TCP 66 Query: Trans: 7165; Unit: 1, Func: 3: Read Holding Registers 44 9.8392100182.165.1.20 192.165.1.23 TCP 54 63395-502 [AcK] seq-21 AcK-291 wirm/3 Lenn-0 44 0.063560182.165.1.29 192.165.1.23 Modbus/TCP 68 Response: Trans: 7124; Unit: 1, Func: 3: Read Holding Registers 47 10.6745860182.165.1.29 192.165.1.23 TCP 54 63395-502 [AcK] seq-121 AcK-291 wirm/3 Lenn-0 48 10.67445182.165.1.29 192.165.1.23 TCP 54 63395-502 [AcK] seq-13 AcK-200 wirm/5 Lenn-0 51 11.6677461182.165.1.29 192.165.1.23 Modbus/TCP 68 Response: Trans: 7460; Unit: 1, Func: 3: Read Holding Registers 52 11.567650182.165.1.23 192.165.1.23 Modbus/TCP 68 Response: Trans: 7460; Unit: 1, Func: 3: Read Holding Registers 52 11.56756182.165.1.23 192.165.1.23 Modbus/TCP 66 Query: Trans: 7460; Unit: 1, Func: 3: Read Holding Registers 53 11.56756182.161.23 192.165.1.23 Modbus/TCP 66 Query: Trans: 7460; Unit: 1, Func: 3: Read Holding Registers 54 12.661550192.165.1.109 192.165.1.23 Modbus/TCP 66 Query: Trans: 7405, Unit: 1, Func: 3: Read Holding Registers 54 12.661550192.165.1.109 192.165.1.23 Modbus/TCP 66 Query: Trans: 7405, Unit: 1, Func: 3: Read Holding Registers 54 13.75360192.165.1.109 192.165.1.23 Modbus/TCP 66 Query: Trans: 7405, Unit: 1, Func: 3: Read Holding Registers 65 13.75360192.165.1.23 192.165.1.23 Modbus/TCP 66 Query: Trans: 8145; Unit: 1, Func: 3: Read Holding Registers 67 13.475360192.165.1.23 192.165.1.23 Modbus/TCP 66 Query: Trans: 8445; Unit: 1, Func: 3: Read Holding Registers 77 14.7098450192.165.1.23 192.165.1.23 Modbus/TCP 65 Response: Trans: 8445; Unit: 1, Func: 3: Read Holding Registers 77 14.7098450192.165.1.23 192.165.1.23 Modbus/TCP 65 Response: Trans: 8445; Unit: 1, Func: 3: Read Holding Registers 77 14.7098450192.165.1.23 Modbus/TCP 66 Query: Trans: 8445; Unit: 1, Func: 3: Read Holding Registers 77 14.7098450192.165.1.23 Modbus/TCP 65 Response: Trans: 8445; Unit: 1, Func: 3: Read Holding Registers 77 14.7098450192.165.1.23 Modbus/TCP 66 Query: Trans: 8445; Unit: 1, Func: 3: Read Hol	40 8.	. 83538500	192.168	1.109	192.	168.1.2	3	TCP			54	63395-5	02 [AC	K]	seq=109	Ack=262	win=80	Len=0				
43 9.64607300192.166.1.23 192.166.1.23 TCP 58 8esponse: Trans: 7168; unit: 1, Func: 3: Read Holding Registers 44 9.832910192.166.1.109 192.166.1.23 TCP 56 63395-502 [AcL] Seq-123 Ack-220 win-65 Lem-0 45 10.6536560192.166.1.109 192.166.1.23 Modbus/TCP 58 Response: Trans: 7424; unit: 1, Func: 3: Read Holding Registers 45 10.677840192.166.1.109 192.166.1.23 Modbus/TCP 56 63395-502 [AcL] Seq-133 Ack-220 win-65 Lem-0 51 11.6677840192.166.1.23 192.166.1.23 TCP 54 63395-502 [AcL] Seq-133 Ack-20 win-65 Lem-0 60 12.681510192.166.1.23 TCP 56 63395-502 [AcL] Seq-133 Ack-320 win-61 Lem-0 60 12.681510192.166.1.23 TCP 56 63395-502 [AcL] Seq-134 Ack-320 win-61 Lem-0 61 12.681520192.166.1.23 TCP 56 63395-502 [AcL] Seq-134 Ack-320 win-61 Lem-0 61 12.681520192.166.1.20 192.166.1.20 Modbus/TCP 58 Response: Trans: 7936; unit: 1, Func: 3: Read Holding Registers 61 12.78360192.166.1.109 192.166.1.23 TCP 56 63395-502 [AcL] Seq-145 Ack-320 win-51 Lem-0 61 12.78360192.166.1.23 192.166.1.23 TCP 56 63395-502 [AcL] Seq-154 Ack-306 win-11 Lem-0 61 12.78360192.166.1.23 192.166.1.23 192.166.1.23 192.166.1.23 71 14.790450192.1	42 9.	. 63968900	192.168	1.109	192.	168.1.2	3	Modb	us/TC	P	66	Quer	r: Tra	ns :	7168;	Unit:	1, Fund	:: 3	Read	Holding	Register	s I
44 9.8322100192.165.1.109 192.165.1.23 TCP 54 63395-502 [Ack] Seq-121 Ack-291 win-73 tem-0 44 10.653650192.165.1.29 192.165.1.23 192.165.1.23 Modbus/TCP 88 Response: Trans: 7424; unit: 1, Func: 3: Read Holding Registers 43 10.674840192.165.1.20 192.165.1.23 TCP 56 63395-502 [Ack] Seq-133 Ack-20 win-65 Len-0 53 11.6677840192.165.1.20 192.165.1.23 TCP 56 63395-502 [Ack] Seq-133 Ack-20 win-65 Len-0 54 10.674860192.165.1.20 192.165.1.23 Modbus/TCP 66 Query: Trans: 7680; unit: 1, Func: 3: Read Holding Registers 50 11.65150192.165.1.20 192.165.1.23 Modbus/TCP 66 Query: Trans: 7980; unit: 1, Func: 3: Read Holding Registers 50 12.65150192.165.1.109 192.165.1.23 Modbus/TCP 66 Query: Trans: 64050 1.86160 51 1.655020192.165.1.109 192.165.1.23 Modbus/TCP 66 Query: Trans: 8192; unit: 1, Func: 3: Read Holding Registers 65 13.675192.165.1.109 192.165.1.23 Modbus/TCP 66 Query: Trans: 8192; unit: 1, Func: 3: Read Holding Registers 70 14.709480192.165.1.20 192.165.1.23 TCP 54 63395-502 [Ack] Seq-157 Ack-376 Win-132 Len-0 65 13.67519192.165.1.109 192.165.1.23 TCP 54 63395-502 [Ack] Seq-157 Win-132 Len-0 67 13.91472165	43 9.	. 64607300	192.168	1.23	192.	168.1.1	.09	Modb	us/TC	P	83	Respons	e: Tra	ns :	7168;	Unit:	1, Fund	:: 3	Read	Holding	Register	s
<pre>4 10.6336560192.168.1.20 102.168.1.23 Modbus/TCP 66 Query: Trans: 7424; unit: 1, Func: 3: Read Holding Registers 4 10.674860192.168.1.23 102.168.1.23 TCP 54 63395-502 [Ack] Seq.133 Ack-220 Win-65 Len-0 31 11.674560192.168.1.23 102.168.1.23 Modbus/TCP 66 Query: Trans: 7860; unit: 1, Func: 3: Read Holding Registers 52 11.674560192.168.1.23 102.168.1.23 Modbus/TCP 66 Query: Trans: 7860; unit: 1, Func: 3: Read Holding Registers 53 11.674560192.168.1.20 102.168.1.23 TCP 54 63395-502 [Ack] Seq.133 Ack-220 Win-65 Len-0 01 21.66150192.168.1.20 102.168.1.23 TCP 58 Response: Trans: 7860; unit: 1, Func: 3: Read Holding Registers 60 12.6816510192.168.1.20 102.168.1.23 TCP 56 Query: Trans: 7860; unit: 1, Func: 3: Read Holding Registers 60 12.6816510192.168.1.20 102.168.1.23 TCP 56 Query: Trans: 7936; unit: 1, Func: 3: Read Holding Registers 60 12.6816510192.168.1.20 102.168.1.23 TCP 56 Query: Trans: 7936; unit: 1, Func: 3: Read Holding Registers 61 12.6916280192.168.1.20 102.168.1.23 TCP 56 Query: Trans: 8192; unit: 1, Func: 3: Read Holding Registers 65 13.69916280192.168.1.20 102.168.1.23 TCP 56 Query: Trans: 8192; unit: 1, Func: 3: Read Holding Registers 65 13.69916280192.168.1.109 102.168.1.23 TCP 56 Query: Trans: 8192; unit: 1, Func: 3: Read Holding Registers 66 13.69916280192.168.1.109 102.168.1.23 TCP 56 Query: Trans: 8192; unit: 1, Func: 3: Read Holding Registers 71 14.7167150192.168.1.109 102.168.1.23 TCP 58 G3995-502 [Ack] Seq.169 Ack-407 Win-116 Len-0 70 14.709464092.102.168.1.23 102.168.1.109 Modbus/TCP 83 Response: Trans: 8448; unit: 1, Func: 3: Read Holding Registers 71 14.7167150192.168.1.23 102.168.1.23 Modbus/TCP 83 Response: Trans: 8448; unit: 1, Func: 3: Read Holding Registers 71 14.7167150192.168.1.23 102.168.1.20 Modbus/TCP 83 Response: Trans: 8448; unit: 1, Func: 3: Read Holding Registers 71 14.7167150192.168.1.23 Hold/Hold/Hold/Hold/Hold/Hold/Hold/Hold/</pre>	44 9.	. 83929100	192.168	1.109	192.	168.1.2	3	TCP			54	63395-5	02 [AC	K]	seq=121	Ack=291	Win=73	Len=0				
44 10.6748860 192.168.1.23 192.168.1.23 TCP 58 Response Trans: 7424; Unit: 1, Func: 3: Read Molding Registers 31 11.6677840 192.168.1.20 192.168.1.23 TCP 56 63395-502 [Ack] Seq.13 Ack-220 wine55 Lend 51 11.6677840 192.168.1.21 192.168.1.23 TCP 56 63395-502 [Ack] Seq.13 Ack-220 wine55 Lend 52 11.6774560 192.168.1.20 192.168.1.23 TCP 56 63395-502 [Ack] Seq.13 Ack-230 wine55 Lend 60 12.680510122.168.1.109 192.168.1.23 TCP 56 63395-502 [Ack] Seq.13 Ack-349 Wine131 Lend 60 12.680510122.168.1.109 192.168.1.23 TCP 56 63395-502 [Ack] Seq.15 Ack-349 Wine131 Lend 61 12.75806192.168.1.109 192.168.1.23 Modbus/TCP 38 Response Trans: 7936; Unit: 1, Func: 3: Read Molding Registers 62 12.681930102.168.1.20 192.168.1.23 Modbus/TCP 58 Response: Trans: 8125; Unit: 1, Func: 3: Read Molding Registers 63 13.6916280192.168.1.20 192.168.1.23 Modbus/TCP 68 Query: Trans: 8122; Unit: 1, Func: 3: Read Molding Registers 64 13.51560192.168.1.23 192.168.1.23 Modbus/TCP 68 Query: Trans: 8122; Unit: 1, Func: 3: Read Molding Registers 67 13.514520192.168.1.20 192.168.1.23 Modbus/TCP 66 Query: Trans: 8122; Unit: 1, Func: 3: Read Molding Registers 70 14.7069460192	46 10	0.6536560	192.168	1.109	192.	168.1.2	13	Modb	US/TC	P	66	Quer	y: Tra	ns:	7424;	Unit:	1, Fund	:: 3	Read	Holding	Register	s
a 10.627440102.166.1.109 192.168.1.23 TCP >> 46 3393-302 ACK 320 When 5 (End) 51 11.6764560132.166.1.129 192.168.1.23 Modbus/TCP 66 Query: Trans: 7680; Unit: 1, Func: 3: Read Holding Registers 52 11.677450132.166.1.109 192.168.1.23 TCP 56 63395-502 ACK 320 Wints: 1, Func: 3: Read Holding Registers 60 12.6816510132.166.1.109 192.168.1.23 TCP 56 63395-502 ACK 45-39 Wints: 1, Func: 3: Read Holding Registers 61 12.6816510132.166.1.109 192.168.1.23 Modbus/TCP 66 Query: Trans: 1/396; Unit: 1, Func: 3: Read Holding Registers 65 13.695260132.166.1.109 192.168.1.23 Modbus/TCP 54 63395-502 ACK 526 Wints: 1, Func: 3: Read Holding Registers 67 13.315360132.166.1.109 192.168.1.23 Modbus/TCP 54 63395-502 ACK 526 Wints: 1, Func: 3: Read Holding Registers 67 13.315360132.166.1.109 192.168.1.23 Modbus/TCP 54 63395-502 ACK 526 Wints: 1, Func: 3: Read Holding Registers 70 14.7084840132.166.1.109 192.168.1.23 Modbus/TCP 56 63395-502 ACK 156 CH 6 Frame 61: 83 bytes on wire (656 bits), 83 bytes captured (664 bits) on interface 0 If thernet 11, Func: 3: Read Holding Registers 71 14.7084840192.166.1.00 Register 1 (UNIT6): 0 Re	47 10	0.6748860	192.168	1.23	192.	168.1.1	.09	Modb	us/TC	P	83	Respons	e: Tra	ns:	7424;	Unit:	1, Fund	- 3	Read	Holding	Register	5
<pre>111.60/340132.165.1.109 192.165.1.23 Modbus/TCP B0 Gquery Frans: 7680; Unit: 1, Func: 3: Read Holding Registers 52 11.677476132.165.1.109 192.165.1.23 TCP 54 63395-502 [ACK] Seq=155 Ack-349 Win-131 Len-0 60 12.805301032.165.1.109 192.165.1.23 Modbus/TCP 54 63395-502 [ACK] Seq=155 Ack-349 Win-131 Len-0 60 12.805301032.165.1.109 192.165.1.23 Modbus/TCP 54 63395-502 [ACK] Seq=155 Ack-349 Win-131 Len-0 65 13.0916280132.165.1.109 192.165.1.23 Modbus/TCP 56 Gquery: Trans: 7336; Unit: 1, Func: 3: Read Holding Registers 61 12.805500132.165.1.109 192.165.1.23 Modbus/TCP 56 Gquery: Trans: 8137; Unit: 1, Func: 3: Read Holding Registers 61 12.93560132.165.1.109 192.165.1.23 Modbus/TCP 56 Gquery: Trans: 8137; Unit: 1, Func: 3: Read Holding Registers 61 12.93560132.165.1.109 192.165.1.23 Modbus/TCP 56 Gquery: Trans: 8137; Unit: 1, Func: 3: Read Holding Registers 61 12.93560132.165.1.109 192.165.1.23 Modbus/TCP 56 Gquery: Trans: 8148; Unit: 1, Func: 3: Read Holding Registers 61 12.93560132.165.1.109 192.165.1.23 Modbus/TCP 56 Gquery: Trans: 8149; Unit: 1, Func: 3: Read Holding Registers 71 14.7167190122.165.1.109 192.165.1.23 Modbus/TCP 56 Gquery: Trans: 8446; Unit: 1, Func: 3: Read Holding Registers 71 14.7167190122.165.1.109 Modbus/TCP 56 Gguery: Trans: 8446; Unit: 1, Func: 3: Read Holding Registers 70 is thernet Trotocol Version 4, Src: 192.166.1.23 (192.165.1.20) Modbus/TCP 56 Register 50 (197.16) FCP 56 Register 7 (UNITG): 0 Register 0 (UNITG): 0 Register 1 (UNITG): 0 Register 1 (UNITG): 0 Register 1 (UNITG): 0 Register 9 (</pre>	48 10	0.8744470	192.168	1.109	192.	168.1.2	3	TCP			54	63395-5	DZ LAC	K]	Seq=133	ACK=320	Win=65	Len=0	-			
<pre>2 11.0 40 300 122.165.1.23 192.165.1.23 102.165.1.23 102 53 Kegan Holding Kegisters 5 11.6 774760 132.165.1.109 192.165.1.23 102 54 Kegan Holding Kegisters 6 12.6 84 6510 132.165.1.109 192.165.1.23 Modbus/rCP 6 6 Query: Trans: 7336; Unit: 1, Func: 3: Read Holding Kegisters 6 2 12.6 85 1490 132.165.1.109 192.165.1.23 Modbus/rCP 5 4 6 3395-502 (ACK) Sequels Arck-378 Min-123 Len-0 6 6 13.6 956260 132.165.1.109 192.165.1.23 Modbus/rCP 5 4 6 3395-502 (ACK) Sequels Arck-378 Min-123 Len-0 6 6 13.6 13610 122.165.1.109 192.165.1.23 Modbus/rCP 5 4 6 3395-502 (ACK) Sequels Arck-378 Min-123 Len-0 6 6 13.6 13610 122.165.1.109 192.165.1.23 Modbus/rCP 5 4 6 3395-502 (ACK) Sequels Arck-378 Min-123 Len-0 7 0 14.7 0384.80 132.165.1.109 192.165.1.23 Modbus/rCP 6 6 Query: Trans: 6 1392; Unit: 1, Func: 3: Read Holding Registers 7 0 14.7 0384.80 132.165.1.109 192.165.1.23 Modbus/rCP 6 6 Query: Trans: 6 446; Unit: 1, Func: 3: Read Holding Registers 7 114.7 114751 50 132.165.1.109 192.165.1.23 Modbus/rCP 6 6 Query: Trans: 6 446; Unit: 1, Func: 3: Read Holding Registers 7 114.7 114751 50 132.165.1.109 192.165.1.23 Modbus/rCP 6 6 Query: Trans: 6 446; Unit: 1, Func: 3: Read Holding Registers 7 14.7 114751 50 132.165.1.109 192.165.1.109 H02.170 Modbus/rCP 6 6 Query: Trans: 6 446; Unit: 1, Func: 3: Read Holding Registers 7 14.7 114751 50 132.165.1.109 H02.170 Modbus/rCP 6 6 Query: Trans: 6 446; Unit: 1, Func: 3: Read Holding Registers 7 14.7 114751 50 132.165.1.109 H02.170 Modbus/rCP 6 6 Query: Trans: 6 446; Unit: 1, Func: 3: Read Holding Registers 7 14.7 114751 50 132.165.1.109 H02.165.1.109 H0</pre>	51 11	1.00//840	192.108	1.109	192.	108.1.2	5	Modo	US/TC	P	00	Quer	y: Tra	ns:	7680;	Unit:	1, Fund		Read	Holding	Register	5
<pre>11.0/0700302:100:11:03 102:100:11:03 102:100:12:03 100:0102/1CP 66 Query: Trans: 7936; unit: 1, Func: 3: Read Holding Registers 01.12/0505/00.102/160:103 102:106:1.23 102/160:1.23 10</pre>	52 11	1 0774760	102.108	1 100	102	169 1 3	.09	TCD	us/ic	P	64	ESSOC.C	an Ind	115:	7000;	Ack-240	L, Fund	1 00-	Read	noraring	Regiscer	>
03 12:03070000021005/1025 102:1030/1000 102:10300/10000 102:1030/1000	60 13	2 6816510	192.100	1 109	192.	168 1 2	2	Modh	ne /TC	D	56	00000	Tra	nc ·	7926-	Hoit:	1 5000	· 2	Read	Holding	Penister	2
0:12.831490192.168.1.109 192.168.1.23 TCP 54 63395-502 (ACK) Seq-157 ACK-375 win-123 Lem-0 65 13.7153660192.168.1.109 192.168.1.23 Modbus/TCP 63 Response: Trans: 8192: Unit: 1, Func: 3: Read Holding Registers 67 13.9145320192.168.1.109 192.168.1.23 TCP 54 63395-502 (ACK) Seq-157 ACK-375 win-123 Lem-0 70 14.709480192.168.1.109 192.168.1.23 TCP 54 63395-502 (ACK) Seq-169 ACK-407 win-116 Lem-0 70 14.709480192.168.1.123 192.168.1.23 Modbus/TCP 66 Query: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167180192.168.1.123 192.168.1.129 Modbus/TCP 66 Query: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167180192.168.1.23 192.168.1.109 Modbus/TCP 68 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167180192.168.1.23 192.168.1.123 Modbus/TCP 68 Query: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 8 Frame 61: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0	61.12	2.6865700	192.168	1.23	192	168 1 1	09	Modb	US/IC	2	00	Respons	P Tra	05.	7930,	Unite:	1 EUD		Reau	Holding	Register	5
65 13.6956200 192.168.1.109 192.168.1.23 Modbus/TCP 83 Response: Trans: \$192; unit: 1, punc: 3: Read Holding Registers 66 13.7155660 192.168.1.109 192.168.1.23 TCP 54 63395-502 [Ack] Seq=169 Ack=407 Wim=116 Len=0 70 14.7094480 192.168.1.109 192.168.1.23 TCP 54 63395-502 [Ack] Seq=169 Ack=407 Wim=116 Len=0 70 14.7094480 192.168.1.109 192.168.1.23 Modbus/TCP 63 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.715130 121.66.1.23 192.168.1.23 Modbus/TCP 63 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 7 14.7167130 192.166.1.23 192.168.1.20 Modbus/TCP 63 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 8 Frame 61: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0	62 12	2.8814930	192,168	1,109	192.	168.1.2	3	TCP	Carlo and a		54	63395-5	02 [AC	K]	Sed=157	Ack=378	win=12	Len=)	inconcorning.	and particular	-
66 13.7153660 192.168.1.23 192.168.1.23 TCP 54 63395-502 [Ack] sequebox Achor Win-116 Lem-O 70 14.7098480 192.168.1.109 192.168.1.23 TCP 54 63395-502 [Ack] sequebox Achor Win-116 Lem-O 70 14.7167180 192.168.1.23 192.168.1.23 Modbus/TCP 66 Query: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167180 192.168.1.23 192.168.1.23 Modbus/TCP 86 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 70 Frame 61: 83 bytes on wire (664 bits), 83 bytes captured (664 bits) on interface 0	65 13	3. 6956280	192.168	1,109	192.	168.1.2	3	Modb	US/TC	P	66	Quer	V: Tra	ns :	8192;	Unit:	1. Fund	: 3	Read	Holdina	Register	5
67 13.9145320192.168.1.109 192.168.1.23 TCP 54 63395-502 [AcK] Seq-169 Ack-407 win-116 Len-0 70 14.709480192.168.1.23 192.168.1.23 Modbus/TCP 66 Query: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167150192.168.1.23 192.168.1.109 Modbus/TCP 83 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 8 Frame 61: 83 bytes on wire (664 bits), 83 bytes captured (666 bits) on interface 0 Internet Tr, Src: 0191boar_76:df:fc (00:40:9d:76:df:fc), Dst: 0ell_1a:23:86 (18:03:73:1a:23:86) 9 Internet Protocol version 4, Src: 192.168.1.23 (192.168.1.23), Dst: 192.168.1.109 (192.168.1.109) State 100 [192.168.1.23 10 Internet Protocol version 4, Src: 192.168.1.23 (192.168.1.23), Dst: 192.168.1.109 (192.168.1.109) State 100 [192.168.1.109] 10 Toternet Protocol version 4, Src: 192.168.1.23 (192.168.1.23), Dst: 192.168.1.109 (192.168.1.109) State 100 [192.168.1.109] 10 Toternet Protocol version 4, Src: 192.168.1.23 Modbus/TCP State 100 [192.168.1.109] 8 Modbus/TCP State 100 [192.168.1.23 Not 100 [192.168.1.109] State 100 [192.168.1.23 9 Modbus Transmission control Protocol, Src Port: 502 (502), Dst Port: 63395 (63395), Seq: 349, Ack: 157, Len: 29 State 100 [192.168.1.23 9 Modbus Fame Control Protocol, Src Port: 502 (502.100 [192.168.1.23 State 100 [192.168.1.109] 9 Regist	66 13	3.7153660	192.168	1.23	192.	168.1.1	.09	Modb	us/TC	P	83	Respons	e: Tra	ns:	8192:	Unit:	1. Fund	: 3	Read	Holding	Register	s
70 14.7098480 192.168.1.109 192.168.1.23 Modbus/TCP 66 Query: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167150 192.168.1.23 192.168.1.109 Modbus/TCP 83 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167150 192.168.1.23 192.168.1.109 Modbus/TCP 83 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167150 192.168.1.23 192.168.1.109 Modbus/TCP 83 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167150 192.168.1.23 192.168.1.109 Modbus/TCP 83 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 14.7167150 192.168.1.23 (192.168.1.109 Modbus/TCP 83 Response: Trans: 8448; Unit: 1, Func: 3: Read Holding Registers 71 Tarking Store of Uris 104, Src: 192.168.1.23 (192.168.1.23), DST: 192.168.1.109 (192.168.1.109) 71 Tarking Store Orocol, Src Port: 502 (502), DST Port: 63395 (63395), Seq: 349, Ack: 157, Len: 29 72 Modbus 74 Modbus/TCP 74 Modbus/TCP 74 Modbus/TCP 74 Modbus/TCP 74 Modbus/TCP 74 Modbus 74 Modbus 75 Modb	67 13	3.9145320	192.168	1.109	192.	168.1.2	3	TCP			54	63395-5	02 [AC	K]	Seq=169	Ack=407	win=110	5 Len=)			
<pre>71 14.7167150192.168.1.23 192.168.1.109 Modbus/TCP 83 Response: Trans: 8448; unit: 1, Func: 3: Read Holding Registers</pre>	70 14	4.7098480	192.168	1.109	192.	168.1.2	3	Modb	us/TC	P	66	Quer	: Tra	ns :	8448;	Unit:	1, Fund	: 3	Read	Holding	Register	s
w w w	71 14	4.7167150	192.168	1.23	192.	168.1.1	.09	Modb	us/TC	P	83	Respons	e: Tra	ns:	8448;	Unit:	1, Fund	:: 3	Read	Holding	Register	5 7
0000 18 03 73 1a 23 86 00 40 9d 76 df fc 08 00 45 00 s.#@.vvE. 0010 00 45 0b c8 00 00 3c 06 ef 16 c0 a8 01 17 c0 a8 s.#@.vvE. 0020 16 d0 1f 6f 7 a3 45 49 b0 77 14 35 d4 46 95 01 8	 Bransmi Transmi Modbus/ Modbus/ Modbus/ Byte Regis 	/TCP tion Code Count: 2 ster 0 (U ster 1 (U ster 2 (U ster 3 (U ster 4 (U ster 5 (U ster 6 (U ster 7 (U ster 8 (U	<pre>i: Read H io introl Pr io introl Pr io introl: in</pre>	olding R olding R 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	egister:	; (3)	(502),	DST PO	rt: 6	3395	(6339	5), Seq	349,	Acl	k: 157,	, Len: 29						
Stars Connection: cline contracts proce Derived: 254 (Displayed: 225 (51 891)) Profile: Default	0000 18 0010 00 0020 01 0030 20 0040 00 0050 00	03 73 1a 45 0b c8 6d 01 f6 00 ef 0e 00 00 00 00 00	23 86 0 00 00 3 f7 a3 4 00 00 1 00 00 0	0 40 9d c 06 ef 5 d9 b0 f 00 00 0 00 00	76 df f 16 c0 a 77 14 5 00 00 1 00 00 0	c 08 00 8 01 17 6 e4 69 10 01 03 10 00 00 10 00 00	45 0 c0 a 50 1 14 0 00 0	05 8 .E. 8 .m. 0 0	. #@ <. E.	.v.]	E. . iP.											1

The screen shot below shows Wireshark capturing BACnet IP traffic between a client and our Babel Buster Pro V230. If you click on a packet, the details of that packet will be displayed in the lower part of the screen. You can expand the tree view to see further detail.

)	(# 2	E E X 2	ii ° ,	7 2 🗐		1	a 🕅 🗖 🔹	50		
ilter:										
5. Ti 1 0	100000				Dungangian Class	Analy C				
1 0		12111111	1211111111111111		copression Creat	whhia a	HEYE:			
10	ime	Source	Destination	Protocol Le	ngth Info	an - 70	2			
2 0	0.000000	0x1b	0x15	BACnet	8 BACnet MS	TP TO	ken			
20	0.000000	0x15	0x16	BACnet	8 BACnet MS	TP TO	ken			
3 0	0.000000	0x16	0x1b	BACnet	8 BACnet MS	TP TO	ken			
4 0	0.000000	0x1b	0x16	BACnet -	23 Confirmed	-REQ	readPropert	y[88]	analog-value,1	present-value
5.0	0,000000	0x16	0x1b	BACnet -	29 Complex-A	εĸ	readPropert	y[88]	analog-value,1	present-value
6 0	0.000000	0x1b	0x36	BACnet	8 BACnet MS	TP PO	II For Maste	r		
7 0	0.000000	0x1b	0x15	BACnet	8 BACnet MS	TP TO	ken			
8 0	0.000000	0x15	0x16	BACnet	8 BACnet MS	TP TO	ken			
9 0	0.000000	0x16	0x1b	BACnet	8 BACnet MS	TP TO	ken			
Buildi 0011 Invo Serv Obje Prop [3] Pres][3]	ing Automa 0000 = 1 oke ID: 84 vice Choid cctIdentii perty Iden sent-value	ation and Cont APDU Type: Com POU Flags: 0xC 8 ce: readProper fier: analog- ntifier: prese e: 44.910000 (rol Network AP iplex-ACK (3) 00 rty (12) ralue, 1 ent-value (85) (Real)	DU						
000 55	ff 06 11 01 19 55	0 16 00 13 81 5 3e 44 42 33	01 00 30 58 0 a3 d7 3f dc d	c Oc OO 80 D	U					

Capturing a series of SNMP traffic will look like the example below. In this example, a series of Get requests is being performed by the SNMP client. Click on any one packet and expand the tree structure in the middle window to see full detail of the request or response.



If you are configuring a device to send traps, you may want to look at traps with Wireshark. If you are working on getting a trap receive rule to work in a Babel Buster Pro, you will be interested in looking at traps in Wireshark there, too. A trap from an RFC 1628 UPS is illustrated below, with the trap message expanded in the tree view, as well as the varbinds expanded to show OID and value.



Article ID: 36 Created On: Tue, Dec 6, 2016 at 9:28 PM Last Updated On: Thu, Feb 9, 2017 at 9:19 AM