

Testing the Flow of Data over a Network Connection Using Wireshark

-by Rob Baird

We often receive phone calls for HYPACK Tech Support from users that are not sure if their network device is communicating properly with HYPACK. While we have the serial port-testing WCOM32 utility built into the HARDWARE program, there is no equivalent program in HYPACK® to test the flow of data over a network connection; however, there *is* a third-party software known as Wireshark that can capture the network packets that come through a specified network port.

1. **Install the Wireshark Program.** The 32-bit and 64-bit installer packages for the Wireshark program can be found in your \HYPACK 2014\Support\Utilities\Wireshark folder.

	the law face if		-			, 0	23
-	≪ Local Disk (C:) HYPACK 2014 Su	pport 🕨 Utilities 🕨 Wires	-		Q		
• •	Include in library 👻 Share with 👻	Burn New folder			• ==		?
<u> </u>	Name	Date modified	Туре	Size			
	wireshark-win32-1.4.2.exe	12/9/2010 9:14 AM	Application	18,787 KB			
	wireshark-win64-1.4.2.exe	12/9/2010 9:14 AM	Application	21,017 KB			

FIGURE 1. Wireshark Install Files in the HYPACK® Install

2. Open Wireshark to find the home page.

FIGURE 2. Wireshark Home Page

Fore VIRESHARK The World's Most Popular Network	ssion Clear Apply vrk Protocol Analyzer	
Capture Interface List Une for the capture interfaces (counts incoming packan) It capture on interface: Bustooth PAN Driver Inter[R32575LM Gigabit Network Connection Microsoft Capture Options But a capture with detailed options	Files Popen Open a periodusty captures file Open Recent: Sample Captures A ich assomment of example capture files on the wild	Online Website Wat me project website. Website User's Guide User's Guide (local version, if installed) Website Security Work with Westhark as securely as possible
Capture Help How to Capture See by the the a successful capture stup Network Media Specific information for capturing on: Ethernet, WLAN		

3. List the available network connections from which to capture data. Click on the icon to the top left of the home page.

		▼ Expression Clea	ir Apply	,				
	Wireshark: Capture Interfaces			-			ı x	Ŋ
/IRE SH	Description	IP	Packets	Packets/s	[Stop		
_	Bluetooth PAN Driver	fe80::e9ad:a32f:28ca:7e05	0	0	Start	Options	Details	Files
	Intel(R) 82579LM Gigabit Network Connection	fe80::fcf4:3049:d3e8:1ee3	0	0	Start	Options	Details	riles
Interfac	😥 Microsoft	fe80::2150:bfef:830e:9ad8	4086	<mark>5</mark> 9	Start	Options	Details	
Live list of the		fe80::d957:eef4:3268:207e	0	0	Start	Options	Details	
rt capture on int	<u>H</u> elp						lose	
Bluetooth PA Intel(R) 82579 Microsoft Microsoft	2		1	Ø A rich a	assortme	nt of example	e capture files	s on the wil

FIGURE 3. Launching the Wireshark Capture Interfaces Dialog

4. Identify which network connections have data packets flowing through them and choose the connection from which you would like to view network packets. Click [Start] to display all packets from that connection.

If you don't see any packets coming through your desired network connection, HYPACK will NOT receive any data on that network connection!

Let's say you can see that there are network packets on your 5656 connection, which is a known port specified for a GPS connection, and we want to view all packets coming across. In this example, you would enter the following into the Filter bar:

Udp.port == 5656

(Note that there are spaces between the port and the first "=" (equal sign), and between the second "=" and the port number.) After opening up port 5656, we should see the flow of data over the network. In this test case, I was connected to a differential GPS that is mounted on the roof at HYPACK and was recognized by my computer as a "Microsoft" connection.

As soon as I typed in the udp.port == 5656, the scroll of network packets started. (See Figure 4.)

ile	Edit	View	v <u>c</u>	jo	Captu	re <u>A</u>	Analyz	e <u>S</u> ta	tistics	Te	lepł	ony	Ī	ols	Hel	р											
N	i (N 6	1			8	Xá	2 8) @	~		•	2	T	⊉		*	€ 6	20	Q E	9 8	1		*	Ø		
ilter	: udj	p.port	== 5	5656											•	Expressi	on	Clear	Арр	ly							
		Time			Sourc	e				Desti	nati	on				Protoc	ol Inf	o									
	455	25.3	956	62	192.	168	.1.1	37		192	.16	8.1	.25	5		UDP	50				blac			estin	ation	port:	56
					192.					192						UDP					blac					port:	
	458	25.6	008	84	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP					black					port:	
	459	25.6	024	46	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP	S	ource	po	rt:	black	kjack		estin	ation	port:	56
	460	25.8	037	27	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP	S	ource	po	rt:	black	kjacl	C D	estin	ation	port:	56
	461	25.8	083	36	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP	S	ource	po	rt:	black	kjacl	C D	estin	ation	port:	56
	464	26.0	099	45	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP	S	ource	po	rt:	black	kjack	C D	estin	ation	port:	56
	466	26.0	128	06	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP					black			estin	ation	port:	56
	467	26.2	133	40	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP	S	ource	poi	rt:	blac	kjacl	C D	estin	ation	port:	56
	468	26.2	149	84	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP					blac					port:	
	470	26.4	181	73	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP	S	ource	poi	rt:	blac	kjacl	C D	estin	ation	port:	56
	471	26.4	197	86	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP	S	ource	por	rt:	blac	kjacl				port:	
					192.					192						UDP					blac	1. Sec.				port:	
	474	26.6	248	36	192.	168	.1.1	37		192	.16	8.1	. 25	5		UDP	S	ource	ро	rt:	blac	kjacl				port:	
					192.					192	.16	8.1	. 25	5		UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP			1.1		blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					blac					port:	
					192.					192						UDP					black					port:	
					192.					192						UDP UDP					blac	100 C				port:	
	497	20.4	/04	01	192.	109		57		192	. 10	0.1	. 25	2		UDP	ാ	Junce	poi	. с .	Diaci	Gaci	C L	est in		port:	20
	_	_	-	-	_	_	_	_	_	_	-	-	-	-	_	_	_	_	_	-	_	_	_	-	111		_
00	ff	ff	ff	ff	ff f	f 0	0 60	35	Of	ae a	aa	08	00	45	00			5.	E								
10	00) 6c	6b	52	00 0	0 4	0 11	8a	56	c0 a	a8	01 ;	89	c0	a8			v.									
20					16 1				e1									\$									
30 40					31 3 2c 4				2C 32									3,4:									
50		30								31								8,1									

FIGURE 4. Viewing the Network Data in Wireshark

To view the contents of any packet, all I had to do was select a packet and look to the bottom of the screen for the actual format and contents of the network packet.

I selected packet # 479, which shows the IP address and port for the connection. The content of the packet was a \$GPGGA message, as shown at the bottom of Figure 4.

In this case, we were able to show the flow of network packets and the content of each packet using the Wireshark program. If the port information was not properly entered, the green Filter bar would instead be red, and no packets would be shown.

Thanks to the inclusion of Wireshark in your HYPACK installation, you now have an easy network connection testing tool that is always at your disposal.