

## 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 last fact the					23
-	≪ Local Disk (C:)   HYPACK 2014   Supp	oort 🕨 Utilities 🕨 Wires	hark	✓ ✓ Search Wireshark	5	Q
:e 🔻	Include in library 👻 Share with 💌	Burn New folder			• ==	?
•	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

The Winshed Makuad Andres		— <b>T</b> X
File Edit View Go Canture Analyze Statistics Telenhony Tools Heln		
Filter: • Expression Cle	r Apply	
WIRESHARK The World's Most Popular Network Proto	col Analyzer	
Capture	Files	Online
<ul> <li>Interface List         <ul> <li>Description on interface</li> <li>County of the capture interface (counts incoming packet)</li> <li>Description</li> <li>Interface List             <li>Interface List             <li>Interface List             <li>Interface List             <li>Interface List             </li> </li></li></li></li></ul> </li> </ul>	<ul> <li>Popen Dyna previously captured the Core Recent:         <ul> <li></li></ul></li></ul>	<ul> <li>Website Wate projects website</li> <li>Sector Subice The Guide (local version if installed) Website Website Website Sector Wate web Wireshafer as securely as possible         </li> </ul>
Readults load or casture     No Backetr		Brofiles Default
		Prome: Default
	And and a second se	► 😼 🔐 ♥ 7/15/2014

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

The Wireshark Netwo	rk Analyzer						-
<u>File Edit View Go</u>	<u>Capture</u> <u>Analyze</u> <u>Statistics</u> Telephony <u>T</u> oo	ls <u>H</u> elp					
			99		i 🗹 🔞	* 3	
Filter:			ar Apply				
	Wireshark: Capture Interfaces			-	l	_ 0	×
WIRESH	Description	IP	Packets	Packets/s		Stop	
	Bluetooth PAN Driver	fe80::e9ad:a32f:28ca:7e05	0	0	Start O	ptions Deta	ils Files
	Intel(R) 82579LM Gigabit Network Connection	fe80::fcf4:3049:d3e8:1ee3	0	0	<u>Start</u>	ptions Deta	ils
Interfac	Microsoft	fe80::2150:bfef:830e:9ad8	4086	59	<u>Start</u>	ptions Deta	ils
Live list of the	Microsoft	fe80::d957:eef4:3268:207e	0	0	<u>Start</u>	ptions Deta	ils
Start capture on inte	Help					Close	
Bluetooth PA							
Microsoft				A rich a	assortment o	f example captur	e files on the wiki
Microsoft							
Start a capture w	Dptions th detailed options						

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.)

			200													
Cap	oturing	g from	Micro:	soft - Wire	eshark	A PARTY			-					-		
<u>F</u> ile	Edit	View	Go	Capture	Analyze	<b>Statistics</b>	Telepho	ny <u>T</u> ools	<u>H</u> elp							
			<b>M</b>			BIO	4	~ ~				152		1 40   FR		
							-	1 W		144				98   <del>89</del>		
Filter:	udp	port ==	5656						<ul> <li>Expression.</li> </ul>	Clear	Apply					
		•														
No.		ime		Source		D	estination		Protocol	Info						
4	55 2	5.395	662	192.16	58.1.13	7 1	92.168	.1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	56 2	5.397	561	192.10	58.1.13	7 1	92.168	.1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	58 2	5.600	884	192.10	58.1.13	1	92.168	.1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	59 2	5.602	446	192.10	08.1.13	1	92.168	1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	60 2	5.803	727	192.10	08.1.13		92.168	1.255	UDP	Source	port:	blackja	ack I	Destination	port:	5050
4	64 7	5.808	045	102.10	00.1.13	7 1	92.108	1 255	UDP	Source	port:	blackje	ack i	Destination	port:	5050
4	66 2	6 017	806	102.10	58 1 13	7 1	92.100	1 255	UDP	Source	port:	blacki	ack i	Destination	port:	5656
4	67 2	6 213	340	102.10	58 1 13	7 1	92.108	1 255	LIDP	Source	port:	blacki	ack i	Destination	port:	5656
4	68 2	6.214	984	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackja	ack r	Destination	port:	5656
4	70 2	6.418	173	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackia	ack r	Destination	port:	5656
4	71 2	6.419	786	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blacki	ack [	Destination	port:	5656
4	73 2	6.623	310	192.10	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackj	ack I	Destination	port:	5656
4	74 2	6.624	836	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	75 2	6.626	388	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackja	ack I	Destination	port:	5656
4	76 2	6.831	858	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackja	ack 🛛	Destination	port:	5656
4	77 2	6.833	417	192.10	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	78 2	7.032	471	192.16	58.1.13	7 1	92.168	.1.255	UDP	Source	port:	blackja	ack I	Destination	port:	5656
4	79 2	7.034	118	192.16	58.1.13	7 1	92.168	.1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	80 2	7.237	292	192.10	58.1.13	7 1	92.168	.1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	81 2	7.238	878	192.10	8.1.13	1	92.168	1.255	UDP	Source	port:	blackja	ack [	Destination	port:	5656
4	82 2	7.442	3/1	192.10	08.1.13		92.168	1.255	UDP	Source	port:	blackja	ack I	Destination	port:	5656
4	84 Z	7.445	015	102.10	08.1.13		92.168	1 255	UDP	Source	port:	blackja	ack I	Destination	port:	5050
4	85 2	7 649	461	102.10	00.1.15 50 1 17	7 1	92.108	1 255	UDP	Source	port:	blacki	ack i	Destination	port:	5656
4	88 7	7 858	065	102.10	58 1 13	7 1	92.108	1 255	LIDP	Source	port:	blacki	ack i	Destination	port:	5656
4	90 2	7 860	806	192.10	58 1 13	7 1	92.168	1 255	LIDP	Source	port:	blacki	ack r	Destination	port:	5656
4	91 2	8.056	358	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blacki	ack r	Destination	port:	5656
4	93 2	8.061	458	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackia	ack I	Destination	port:	5656
4	94 2	8.261	159	192.10	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackj	ack [	Destination	port:	5656
4	95 2	8.263	162	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackja	ack I	Destination	port:	5656
4	96 2	8.466	000	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackja	ack I	Destination	port:	5656
4	97 2	8.470	461	192.16	58.1.13	7 1	92.168	1.255	UDP	Source	port:	blackja	ack I	Destination	port:	5656
4																
						25.05					1000					
0000	tt	TT T		TT TT	00 60	35 Of a	e aa 08	89 60	28 1kp	. 5	<mark>E</mark> .					
0020	01	ff 0	4 01	16 18	00 58	c3 e1 2	4 47 50	47 47	41	.X \$G	PGGA					
0030	2c	32 3	0 35	31 31	37 2e	33 2c 3	4 31 33	35 2e	36 ,20511	7. 3,41	35.6					
0040	31	38 3	3 34	2c 4e	2c 30	37 32 3	4 33 26	2 34 32	31 1834,N	,0 7243	.421					
0060	20	39 2	c 4d	2c 2d	33 34	2e 32 2	c 4d 20	37 2e	32 .9.M	-34 .2.M	.7.2					
0070	2c	30 3	1 33	33 2a	37 44	Od Oa			,0133*	7D						

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.