

Technical Note 179

Wireshark for Modbus RTU

Installation, setup and capture instructions

Introduction

Since its introduction in 1979, Modbus RTU became an industry standard for communication in control applications. It has been a standard in ABB drives for decades. As such, there is a significant installed base of applications using Modbus. When issues arise which require an understanding of what Modbus registers and services are being accessed, troubleshooting can stall without this information. This paper describes how to configure a common network analysis tool – Wireshark – to capture Modbus RTU traffic over RS-485, providing necessary information regarding Modbus communication in an application.

What is Wireshark?

Wireshark is a network packet analyzer. Historically, such an analysis tool was either expensive or proprietary. Wireshark, however, is available for free as an open-source project maintained by its users. It is widely considered to be one of the best packet analyzers available today.

Although best known as a capture and analysis tool for Ethernet-based protocols, it has evolved to also accept input from a computer's serial COM ports. As well, user-demand has driven Wireshark developers to add Modbus RTU protocol decoders to this open-source project, as it already supported Modbus/TCP over IP.

Network Example

Below is a simple network that will be used in this technical note. It features two ACH580s configured for Modbus RTU connected to a Modbus client (ModScan) hosted on a laptop. These are using COM6. COM7 is used separately to connect Wireshark to the Modbus RTU network and capture the traffic:



Wireshark installation

• The latest Wireshark application is available at the following link: <u>https://www.wireshark.org/</u>



• Click on the "Download" icon and select your operating system.

Join us 4-	8 November in V	Vienna for	SharkFest	24 EURC	PE, the of	ficial Wireshark Developer and User Conference	ې ن ې
WIRESHARK	Download	Shop	Learn	About	Blog	Get Help v Develop v Members	Donate
 Stable Release: 4.4.0 Windows x64 Installer Windows Arm64 Installer Windows x64 PortableApps® macOS Arm Disk Image macOS Intel Disk Image Source Code 						Always-on, scalabe Packet Capture with all your tools ere endace endaces Meteore	
 Old Stable Release: 4.2.7 Documentation 						Never Drop Packets! 23H2 Update 100Gbps 148Mpps sustained 24/7 Line Rate fol Poder Cytare	
	a d		- 6		- (Official TCP / IP Troublesheating Ceurse Training & Wiresheark Teols	ি ব× ফ 6:33 PM

• Launch the downloaded setup file to install Wireshark. The default installation options can typically be used, unless the user has a specific reason to select others.

Modbus RTU capture extension for Wireshark

• With Wireshark installed, there is an additional capture extension for Modbus RTU that must be installed. This extension can be found at the following link:

GitHub - jzhvymetal/WiresharkSerialAdapter: Wireshark Serial Adapter for Windows

Navigate to the latest version and download WireSharkSerialAdapter.exe:

Product ~ Solutions ~ Resou	rces 🗸 Open Source 🗸 Enterprise 🗸 Pricing	C Search or jump to / Sign in Sign up	
Jzhvymetal / WiresharkSerialA	dapter (Public)	Q Notifications ♀ Fork 2 ☆ Star 2	
<> Code ③ Issues \$1 Pull requests	📀 Actions 🗄 Projects 🛈 Security 🗠 Insights		
f Files	WiresharkSerialAdapter / VSCODE_v6 /		
₿° main 👻 Q	🙀 jzhvymetal Add files via upload 🚥		Sc5fb01 · 3 months ago 🕄 History
Q Go to file	Name	Lost commit message	Last commit data
> VSCODE_V1	Name	Last commit message	Last commit date
> VSCODE_V2	- • •		
> VSCODE_v3	vscode	Add files via upload	3 months ago
> VSCODE_v4	WireSharkSerialAdapter.cpp	Add files via upload	10 months ago
> VSCODE_v5	MireSharkSerial&danter.eve	Add files via upload	3 months and
✓			
> 📄 vscode	baud.ini	Add files via upload	10 months ago
WireSharkSerialAdapter.cpp			
WireSharkSerialAdapter.exe			
🗅 baud.ini			
00A_Wireshark Serial Adapter RS			
00_Wireshark Serial Adapter RS4			
01_Wireshark Serial Adapter Cop			
02_Wireshark Serial Adapter-Usin			
WiresharkSerialAdapter / VSCODE	E_v6 / WireSharkSerialAdapter.exe		
👔 jzhvymetal Add files via upload			ScSfb01 - 3 months ago 🕄 History
Code Blame 3.15 MB			Raw D the P

• With this file downloaded, navigate to the Wireshark application folder and locate the following subfolder:

System (C:) > Program Files > Wireshark > extcap > wireshark

- If it doesn't exist, create it. Copy WireSharkSerialAdapter.exe to this folder.
- Note that this isn't an executable to be explicitly launched by the user. Wireshark will execute it as an additional capture option.

USB-to-485 communication adapter

• This technical note is written assuming a USB-to-485 communication adapter has already been installed and setup on the user's computer. If assistance is needed in getting this setup, please refer to ABB Technical Note 76:

https://search.abb.com/library/Download.aspx?DocumentID=LVD-EOTKN076U-EN&LanguageCode=en&DocumentPartId=&Action=Launch

Wireshark COM port setup

• Launch the Wireshark application. The initial start-up screen will list the available capture ports. This list will be different for each user's computer, depending on its configuration. Below is an example of what this screen looks like:

🚄 The Wireshark Network Analyzer	_		×
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help			
📕 🗏 🐵 🚞 🖺 🏹 🏹 🗣 🐡 🕮 🗿 💆 📃 🔍 Q, Q, 🎞 🔡			
Apply a display filter <ctrl-></ctrl->		-	· +
Welcome to Wireshark			
Capture			
using this filter: 📕 Enter a capture filter 🔹 2 interfaces s	hown, 11	hidden 🔻]
BACnet MS/TP on COM6 Serial Port Adapter (WireSharkSerialAdapter eye)			
Learn			
User's Wiki Questions and Mailing Lists SharkFest Wireshark D Guide Answers	Discord	Donate	•
You are running Wireshark 4.4.0 (v4.4.0-0-g009a163470b5). You receive automatic updates.			
Ready to load or capture No Packets	P	rofile: Def	ault 🔡

• In this list, Serial Port Adapter (WireSharkSerialAdapter.exe) should be an option. Click on the settings icon 🙆 to the left to bring up the setup options:

Wireshark · Interface Option	s: Serial Port Adapter (WireSharkSerialAdapter.exe)	×
Default		
Port	COM7 ~	٢
Baud Rate	19200 ~	C
Byte Size	8 ~	C
Parity	EVEN ~	C
Stop Bits	1 ~	C
Interframe Timing Detection	Event ~	C
Interframe Timebase	Multipler :1X Modbus Character	C
Interframe Multipler	3.0	C
Interframe Delay(us)	0.0	C
Interframe Correction	Modbus CRC ~	C
Wireshark DLT	147: User DLT v	C
Save parameter(s) on captur	e start	
Restore Defaults	Start Save Discard H	elp

- Launch Windows Device Manager to confirm the COM port assigned to the connected USB-485 adapter
- Select this COM port and set the baud rate, byte size, parity and stop bits of the Modbus RTU channel to be monitored.
- Use the Interframe settings shown in the screenshot above.
- Select User DLT 147 as the Wireshark DLT.
- Save these settings.

• Returning to the main screen, select Preferences from the Edit pull-down menu and navigate to Protocols:

Wireshark · Preferences Appearance Columns Frotocols Display hidden protocol items	-		×
Appearance Columns Fact and Column Protocols Display hidden protocol items			
Layout Capture Expert Filter Buttons Name Resolution Protocols RSA Keys Statistics Advanced Display byte fields with a space character between bytes Look for incomplete dissectors Enable stricter conversation tracking heuristics Deinterlacing conversations key NONE The max number of hashes to keep in memory for determining duplicates frames	0		
OK Cancel Appl		Help	c

• Expand Protocols and select DLT_User. Click on Edit to add an entry to the Encapsulation Tables. Click the "+" button to add a DLT:

Wireshark · Preference	ies	- 🗆 X
DB-LSP-DISC DCCP	DLT User	
DCERPC DCOM	Encapsulations Table Edit	
DCT2000 DDTP	User DLTs Table	- 🗆 X
DECT-MITEL- DeviceNet DHCP/BOOTI DHCPFO DHCPv6 DHCPv6 Bulk Diameter DICOM DIS DISCARD DISCARD DISTCC DJIUAV DLEP DLM3 DLSW DLT DLT_USER	DLT Payload dissector Header size Header dissector Trailer size	e Trailer dissector
DMP DMX Channe DNP 3.0		\Roaming\Wireshark\user_dlts
	OK Copy from	Cancel Help

User DLTs Table				— C) X	
DLT	Payload dissector	Header size	Header dissector	Trailer size	Trailer dis	
User 0 (DLT=147)	mbrtu	0		0		
+ - 9 ^ ~		C:\Users\USJEB	ing\Wireshar	<u>ark\user_dlts</u>		
		ОК	Copy from Ca	ancel	Help	

• Select User 0 (DLT = 147) and manually edit the Payload dissector to be mbrtu:

• Click OK and return to the main screen.

Wireshark capture

• With the COM port properly configured, a traffic capture is initiated by double-clicking the selected COM port. The content of the capture will depend on the connected devices. The following is an example of the active window panes:

Capturing from Serial Port Adapter (WireSharkSerialAdapter.exe) -	
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
/ I I X X X + + I I I I I A A A I I I I I X X X X X X X	
Apply a display filter <ctrl-></ctrl->	
No. Time Source Destination Protocol Lengtrinto	
71 17.443759 Modbus KIU 8 Query: Unit: 1, Func: 3: Read Holding M	egisters
72 17.005202 Produce nity if negociate the analysis in the second	egisters
74 18,184491 Modbus RTU 13 Response: Unit: 1, Func: 3: Read Holding F	egisters
75 18.449539 Modbus RTU 8 Query: Unit: 1, Func: 3: Read Holding F	egisters
76 18.699401 Modbus RTU 17 Response: Unit: 1, Func: 3: Read Holding F	egisters
77 18.992287 Modbus RTU 8 Query: Unit: 1, Func: 3: Read Holding F	egisters
78 19.173526 Modbus RTU 13 Response: Unit: 1, Func: 3: Read Holding P	egisters
79 19.438765 Modbus RTU 8 Query: Unit: 1, Func: 3: Read Holding P	egisters
80 19.687607 Modbus RTU 17 Response: Unit: 1, Func: 3: Read Holding R	egisters
81 19,995799 Modbus RTU 8 Query: Unit: 1, Func: 3: Read Holding R	egisters
82 20.173875 Modbus RTU 13 Response: Unit: 1, Func: 3: Read Holding H	egisters
93 20.4443366 PRODUKTU S QUERY: UNIT: 1, FUNC: 3: Read Holding N 94 20.718511 Modbur FTI 17 Personase Unit: 1 Euro; 3: Read Holding N	egisters
85 20. 905462 Module STIL 8 Output Unit 1. Surger 3: Read Holding F	egisters
86 21.153563 Modbus RTU 13 Resonse: Unit: 1, Func: 3: Read Holding F	egisters
87 21,416400 Modbus RTU 8 Query: Unit: 1, Func: 3: Read Holding F	egisters I
88 21.688220 Modbus RTU 17 Response: Unit: 1, Func: 3: Read Holding F	egisters
89 22.004529 Modbus RTU 8 Query: Unit: 1, Func: 3: Read Holding F	egisters
Frame 44: 17 bytes on wire 136 bits), 17 bytes captured (136 00000 01 03 0c 1a d3 00 00 00 03 00 00 05 0d 48	0a
DLT: 147, Payload: mbrtu (Modbus RTU)	
> Modbus RTU	
V Modeus	
(Report Fores 43)	
[Time from request: 0.248228800 seconds]	
Byte Count: 12	
> Register 105 (UINT16): 6867	
> Register 106 (UINT16): 0	
> Register 107 (UINT16): 3	
> Register 108 (UINT16): 0	
> Register 109 (UINT16): 89	
> Register 110 (UINT16): 3400	

- The main pane is an overall summary of the Modbus RTU traffic, with a brief description of each message type. When a frame is selected in this pane, the lower-left pane contains a breakdown of the packet content by fieldtype, and the lower-right packet is the packet content in hexadecimal format.
- The selected frame number is displayed in the packet details frame on the lower left, as well as the contents of the Modbus message. In this example, the results of the Modbus Read Holding Request for 6 registers is shown.
- The Wireshark capture is stopped by clicking on the red square, second from the left.

Wireshark capture save

• Finally, the contents of the Wireshark capture can be saved to a file for later review. This is found under the File->Save pulldown:

Savo in:	Documents		v 🙆 🏚 🛛	🦻 🖽 🗸			
oave <u>i</u> n.	Documenta	^					
-	Name		Status	Date modified			
	ACH550		\odot	12/15/2022 11:55	i AN		
Quick access	ACH580		\bigcirc	12/15/2022 11:54	AN		
	ACS320		\odot	12/1/2022 1:39 P	М		
	ACS400		\bigcirc	8/19/2021 6:57 A	M		
Desktop	BACnet		Q	5/13/2022 12:58	PM		
	Eclipse		0	12/1/2022 12:53	PM		
-	E-Clipse Scr	eens	\bigcirc	3/28/2022 3:59 P	М		
Libraries	Expenses		6	11/14/2022 7:06	PM		
	FENA-11 Te	sting	0	1/18/2021 2:21 P	М		
	LON		\odot	9/13/2022 10:56 AM			
This PC	ModScan		6	1/20/2021 9:24 AM			
	RAE			12/21/2022 2:36 PM			
	Silkroad		\odot	1/20/2022 11:38	AM		
Network	Spiceroad		0	9/23/2022 2:42 PM			
	Spider		\odot	6/14/2022 3:18 PM			
	Tools		0	12/27/2022 10:38	3 AN		
	File <u>n</u> ame:	Test_Capture		∽ <u>S</u> av	е		
	Save as type:	Wireshark/ pcapn	g (*.ntar.gz;*.ntar.zst;*.ntar.lz4	k*.⊢∨ Canc	el		
				Help	þ		

• Enter a filename and save to a known location. The file extension is .pcapng. This file can be shared for additional review.

Wireshark capture review

To review a previous Wireshark capture, simply double-click on the .pcapng file and Wireshark will automatically open, proceeding immediately to the capture window shown previously. From here, additional review and filtering can be done to analyze network issues.

Wireshark capture file filtering

Due to typically large capture files, one of the more useful filtering options is to sort specifically for the device that is reported to have issues. Thus, only those transactions for the device of interest can be isolated and saved to a separate file. This makes capture files much more manageable.

• Select any frame in the upper pane and expand the details in the lower left pane by clicking on the caret next to the Modbus RTU portion of the packet.

• The field of interest for this example is Unit ID. Select it in the lower left pane by clicking on it, and right-mouse click to display the filtering options. From these, select Apply as Filter->Selected:

*Serial Port Adapter (WireSharkSerialAdapter.exe)			- 🗆 X
File Edit View Go Capture Analyze Statistics Telephony	Wireless Tools Help		
_ ■ 2 @ = 1 X 2 9 + + 2 7 ± = 0			
Apply a display filter <ctrl-></ctrl->	Expand Subtrees		
No. Time Source Destination	Collapse Subtrees		
19 4.715421	Expand All		: 3: Read Holding Registers
20 4.731459	Collapse All		:: 3: Read Holding Registers
21 5.002732 22 5.019023	Apply as Column	Ctrl+Shift+I	:: 3: Read Holding Registers :: 3: Read Holding Registers
23 5.722504	Apply as Filter	•	Apply as Filter: mbrtu.unit_id == 2
24 5./38853	Prepare as Filter	•	Selected
26 6.026162	Conversation Filter	•	Net
27 6.713132	Colorize with Filter	•	Not selected
28 6.729712	Follow	•	and Selected
29 7.001237			or Selected
30 7.017204	I/O Graph	•	and not Selected
31 7.721287	Сору	•	or not Selected
32 7.736825	Show Packet Puter	Ctrl Shift O	:: 3: Kead Holding Kegisters
33 7.993283	Show Packet Bytes	Cul+3iiiit+0	:: 3: Read Holding Registers
35 8 727995	Export Packet Bytes	Ctrl+Shift+X	: 3: Read Holding Registers
36 8.743874	Wiki Protocol Page		: 3: Read Holding Registers
37 9.015383	Filter Field Reference		: 3: Read Holding Registers
38 9.031635	Protocol Preferences	•	: 3: Read Holding Registers
	The contraction of the contracti		
> Frame 29: 8 bytes on wire (64 bits), 8 bytes captu	Decode As	Ctrl+Shift+U	···i····
DLT: 147, Payload: mbrtu (Modbus RTU)	Go to Linked Packet		
V Modbus RTU	Show Linked Packet in New Window		
Unit ID: 2			1
CRC-16: 0x15e/ [unverified]			
[CRC-16 Status: Unverified]			
7 Houbus			
Unit ID (mbrtu.unit_id), 1 byte		Packets: 68 · Drop	oped: 0 (0.0%) Profile: Default

• This will populate the display filter field with the filter syntax to select Modbus device #2. Only transactions for this device will be displayed:

	*Se	erial f	Port	Adap	ter (V	Vire	Sharks	Seria	lAdapte	er.ex	:e)															_		×
File	e	Edit	V	iew	Go	Ca	pture	Α	nalyze	St	atisti	cs	Telephony	Wirele	ess	Tools	s Hel	р										
		B	0			X	3	Q	(2 7			⊕ ⊜	Θ		1											
	mh	rtuu	nit i	d	2			•		_		-				•											X	- +
	IIID	rtu.ui	T	u	2																							
No	•		Tim	18			Sour	ce			Des	tina	tion	Proto	col		Lengtł	In	nfo									
		9	2.0	137	0									Modbu	s R	TU	8		Query:	Unit:	2,	Func:	3:	Read	Holding	Reg	isters	
		10	2.0	2972	21									Modbu	s R	RTU	17	Re	esponse:	Unit:	2,	Func:	3:	Read	Holding	Reg	isters	
		13	3.0	0476	59	$\overline{\ }$								Modbu	s R	RTU	8		Query:	Unit:	2,	Func:	3:	Read	Holding	Reg	isters	1.1
		14	3.0	02079	95									Modbu	s R	RTU	17	Re	esponse:	Unit:	2,	Func:	3:	Read	Holding	Reg	isters	
		17	3.9	9623	80					_				Modbu	is R	RTU	8	_	Query:	Unit:	2,	Func:	3:	Read	Holding	Reg	isters	
		18	4.0)1133	37									Modbu	s R	RTU	17	Re	esponse:	Unit:	2,	Func:	3:	Read	Holding	Reg	isters	
		21	5.6	00273	52									Modbu	IS K		47		Query:	Unit:	2,	Func:	3:	Read	Holding	Reg	isters	
		22	5.6	1902	2.5									Modbu	s R		1/	ĸe	esponse:	Unit:	> 2,	Func:	3:	Read	Holding	Reg	isters	
		25	6.6		51 'n									Modbu	IS K		17	п.	Query:	Unit:	2,	Func:	3:	Read	Holding	Keg	isters	
		20	7.0	2010	7									Modbu			1/	Re	Ouenvi	Unit:	2,	Func:	2.	Read	Holding	Reg	istens	
		30	7.0	1720	о <i>г</i>									Modbu	s R		17	Re	Query.	Unit:	2, 2	Func:	3.	Road	Holding	Reg	istons	
		33	7 0	10328	23									Modbu	e R		1/	ne	Ouenv:	Unit:	2,	Func:	3.	Road	Holding	Reg	istone	
		34	8.0	0886	18									Modbu	IS R	TU	17	Re	esnonse.	Unit:	2,	Func:	3.	Read	Holding	Reg	isters	
		37	9.6	91538	13									Modbu	IS R	ти			Ouerv:	Unit:	2.	Func:	3.	Read	Holding	Reg	isters	
		38	9.6	3163	5									Modbu	is R	ати	17	Re	esponse:	Unit:	2.	Func:	3:	Read	Holding	Reg	isters	
		41	10.	0227	64									Modbu	s R	RTU	8		Ouerv:	Unit:	2.	Func:	3:	Read	Holding	Reg	isters	
		42	10.	0383	61									Modbu	s R	TU	17	Re	esponse:	Unit:	2,	Func:	3:	Read	Holding	Reg	isters	
		45	10.	9982	17									Modbu	s R	τυ	8		Ouerv:	Unit:	2.	Func:	3:	Read	Holding	Reg	isters	
		46	11.	0294	25									Modbu	s R	TU	17	Re	esponse:	Unit:	2.	Func:	3:	Read	Holding	Reg	isters	
-																												
>	Fra	ame	29:	8 b	ytes	on	wir	e (64 bit	:s),	81	byte	es captur	ed (64	bi	ts)	0000	6	02 03 00	69 00	06 1	5 e7		L.	è		• •	·i····
	DL1	r: 1	47,	Pay	load	l: m	brtu	(M	odbus	RTU	J)																	
~	Mod	lbus	RT	U																								
		Unit	tΙ	D: 2																								
		CRC	-16	: 0x	15e7	[u	nveri	ifie	ed]																			
		[CRO	C-1	6 St	atus	: U	nveri	ifie	ed]																			
>	Mod	lbus																										
L L					_			_	_								-				_							
		R 1	Init		brtu	unit	id) 1	buto											Dacket	- 60 Die	plave	d. 24 (50.0	0/) F	roppe	d: 0 (0 0%)		rofilo: Do	foult
		U U	mit	in (m	briu.	unit_	iu), I	byte											Packets	5. 00 · DIS	ріауе	u. 54 (50.0	/0) · L	vohhe	u. 0 (0.0%)	P	ionie. De	auit

- These can then be saved to a new capture file which only includes these frames.
- Similar filters can be applied to other message fields to isolate only the frames of interest. This makes capture file sharing and analysis much more manageable.

Summary

Modbus RTU communication issues can be difficult to isolate without visibility of the network traffic. However, with a capture of network traffic, troubleshooting often proceeds very quickly. Wireshark is a free network packet analyzer that is very powerful. Once installed and setup, capturing the traffic on a Modbus RTU network can be accomplished easily, and has shown to be a very valuable tool. This technical note summarizes the installation and setup of Wireshark for Modbus RTU packet traffic.