How to capture network communication using Wireshark (Network Protocol Analyzer)

Introduction

In case there is a demand for inspection of network communication between the PC and the device, it is possible to record this communication using the Wireshark software. Wireshark is capable of capturing various communication traffic running on a computer network, no matter if communication is performed via cable or wireless.

Procedure of Wireshark installation and use

- 1. Download the Wireshark software installer from the <u>Wireshark Download section</u>. Choose the 32-bit or 64-bit installer version based on your Windows version.
- 2. Install Wireshark. During the installation procedure, keep the default parameters.
- 3. Start Wireshark. The initial window provides a list of available networks. It is necessary to select the respective network to which the device of interest is connected to.
 - Windows 11

If the device of interest is connected to the PC via Ethernet (LAN network), the name of the network can be found in Settings – Network & internet settings > Ethernet.



• Windows 10

If the device of interest is connected to the PC via Ethernet (LAN network), the name of the network can be found in Settings – Network status.

📕 The Wireshark Network Analyzer - 🗆 🗙	Settings	- 🗆 X
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	Home	Status
Apply a display filter <ctrl-></ctrl-> Expression +	Find a setting \wp	Network status
Welcome to Wireschark	Network & Internet	
Capture	토 Ethernet	You're connected to the Internet If you have a limited data plan, you can make this network a materiad measuring as changes are presented as
using this filter: Image: Constraint of the second se	ିଙ୍ଗ Dial-up %° VPN	Change connection properties Show available networks
VMware Network Adapter VMnet1	 Data usage Proxy 	Change your network settings
Learn		Change adapter options View network adapters and change connection settings.
User's Guide · Wiki · Questions and Answers · Mailing Lists You are running Wireshark 2.6.6 (v2.6.6-0-gdf942cd8). You receive automatic updates.		Sharing options For the networks you connect to, decide what you want to share.
Ready to load or capture No Packets Profile: Default		• HomeGroup Set up a homegroup to share pictures, music, files, and printers with other PCs on your network.

• Windows 7

If the device of interest is connected to the PC via Ethernet (LAN network), the name of the network can be found in Network and Internet – Network and Sharing Center.

The Wireshark Network Analyzer			
File Edit View Go Capture Analyze Statistics Telephony Wireless Te	ools Help		
◢ ■ ∅ ◉]} 🖹 🛪 🗖 ९ ⇔ ⇔ 🕾 🕆 ½ 🚍 🗐 ९ ९ ९			
Apply a display filter <ctrl-></ctrl->	ession +		
Welcome to Wireshark			
Capture			
	S S S S S S S S S S S S S S S S S S S	ernet Network and Sharing Center	▼ 4 Search Control Panel ♀
using this filter: 📕 Enter a capture filter 💌 All interfaces s	Control Panel Home	View your basic network information	on and set up connections
Local Area Connection 🔟	Change adapter settings	🔊 — — 🚑	See full map
	Change advanced sharing settings	WIN7-V-64 (This computer)	Internet
		View your active networks	Connect or disconnect
Learn User's Guide · Wiki · Questions and Answers · Mailing Lists		Public network	Access type: Internet Connections: Uncal Area Connection
You are running Wireshark 2.6.6 (v2.6.6-0-gdf942cd8). You receive automatic updates.			
Ready to load or capture No Packets Profi	le: Default		

- 4. In case the device is connected using a Wi-Fi network, it is necessary to select the correct Wi-Fi network in the list of networks.
- 5. Fill in the necessary information: in the *...using this filter:* item, specify which communication traffic should recorded. In case of recording the communication traffic of a device connected via LAN, it is necessary to insert the **tcp port** command and the **port number**.

📕 The	e Wireshark Network Analyzer	- 🗆 X	
File E	Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help		
	∅ 💿 🚞 🖾 🖾 ۹. ⇔ ⇔ 🕾 🗿 🛃 🚍 🔍 ۹. ۹. ۹. 🖽		
Арр	ly a display filter <ctrl-></ctrl->	+ ~	
	welcome to wireshark		
	Capture		
	using this filter: 📙 tcp port 2101 🛛 🛛 🖉 🤟 9 interfa	ices shown, 2 hidden 🔻	
	Ethernet	man i	
	Adapter for loopback traffic capture	N	
	Local Area Connection* 10		
	Local Area Connection* 9		
	Local Area Connection* 8		
	Local Area Connection* 2		
	Local Area Connection* 1		
	Wi-Fi		
	Event Tracing for Windows (ETW) reader		
	earn		
	Learn		
	· · · · · · ·		
	You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.		
02	Ready to load or capture No Packets	Profile: Default	

The **port number** value can typically be found in the device Setup dialog accessible under the 'Setup...' button in the System Configuration at the bottom of the dialog (see <u>online help for more info</u>).

The following contains some examples of port number values for various devices.

Device Setup in the Clarity System Configuration	Adapted Wireshark Settings
Setup X Communication GPIB TCP Auto Detect GPIB Board: gpib0 Address: 1 IV IP Address: Port: 9100 Add Remove Common OK Cancel Help	Capture using this filter: tcp port 9100 I read and the shown read

Device Setup in the Clarity System Configuration	Adapted Wireshark Settings
Detector Setup X Communication Settings Interface : Interface : Ethernet (LAN) IP Adress : AutoDetect Port : 10001 Test Test Press Test to check if unit is connected Detector Settings Name : Stop lamps when closing instrument window Stop lamps when closing instrument window Set User's Specification OK Cancel Help	Capture using this filter: tcp port 10001 All interfaces shown VMware Network Adapter VMnet8 Ethernet VMware Network Adapter VMnet1
Setup Connection IP Port 4242 * the configuration of GC is out-of-date. AutoDetect	Capture using this filter: tcp port 4242 Image: Transmission of the second

For other devices, this information about can be found in the Hardware Configuration or in the Help documentation.

😭 Help		- 0	×	🔧 Help			-		×
) 🕅 🗂 🛦	: 4		Hide Locate Back Forward Stop Refre	ish Home F	nt Print			
Hide Locate Back Forward Stop	o Refresh Home For	t Print		Contents Index Search Favorites	Menu P	ath: Instrument / Method / LC Control / LC Status		4 1	~
Contents Index Search Far	Format of the port set	ttings in COMMDRV.INI	~	Brief Description					
Dist Description	Communication	Format syntax		Distallation procedure	Hardw	are Configuration -	1000	1.78	
Requirements	Serial	COMx (where x is the number of the COM port)		Setup - communication		Hardware Configuration	x		
lnstallation procedure	LAN communication			U Using the control module					
Substrate the control module	LAN COmmunication	TCP IP x x x 2101 since version 6.1		🗄 🔷 Method Setup - LC					
Report Setup		(where x x x y is the IP address)		🐵 🌪 Method Setup - LC Gradient		Type of Machine :			
Troubleshooting	LISB communication	FTD2XX SNy (where y is the serial number of							
Clarity Main help		the sampler)					_		

6. Then, it is necessary to start the recording of communication traffic using the icon of Wireshark (blue dorsal fin).

🚄 The Wireshark Network Analyzer	-		×
Fin Edit View Go Capture Analyze Statistics Telephony	Wireless	Tools	»
🎽 🖉 🐵 📙 📾 🗙 🖸 I 9. 🗢 🗢 🕾 T 🕹 🚍 📃	\oplus \bigcirc	₽,₩	
Apply a display filter <ctrl-></ctrl->	🗾 👻 Exp	pression	+
Welcome to Wireshark			
Capture			
using this filter: 📕 tcp port 2101	All interfaces	s shown 🔻	

7. During capturing, the screen of Wireshark will be populated with communication. The trouble with the device should be repeated right now while the capturing is running.

-																									
	Cap	turi	ng f	rom	h Eth	erne	et (to	p po	ort 21	01)											-			×	(
File	Ec	lit	Vi	ew	Go		Cap	ture	Ar	nalyz	e	Stat	istic	s	Tele	pho	ny	Wir	eless	То	ols	He	lp		
		۵	۲			110	X	G	٩	æ	۲	•	Î	4				Ð,	$\Theta_{\mathbf{k}}$	Q, 1					
	Apply	a d	lispla	iy filt	ter	. <c< td=""><td>trl-/:</td><td>></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>→</td><td>•</td><td>Exp</td><td>ression.</td><td>. </td><td>÷</td></c<>	trl-/:	>												→	•	Exp	ression.	.	÷
No.			Time				s	ource						De	stina	tion				Pr	otoc	ol	Length	Info	^
	2387	71	321	. 33	757	2	1	92.1	168.	111	.12	7		19	2.1	68.	111.	163		T	CP		70	210	2
	238	72	321	.33	764	6	1	92.1	168.	111	.16	3		19	2.1	68.	111.	127		T	CP		54	654	4
	2387	73	321	.33	773	0	1	92.1	168.	111	.16	3		19	2.1	68.	111.	127		T	СР		70	654	4
	2387	74	321	. 34	187	2	1	92.1	168.	111	.12	7		19	2.1	68.	111.	163		т	СР		60	210	
	2387	75	321	.37	795	4	1	92.3	168.	111	.12	7		19	2.1	68.	111.	163		T	CP		70	210	
																									۷
<																								>	
>	Fram	e :	1:	66	bvt	es	on	wire	(5	28	bit	s),	66	by	tes	ca	otur	ed	(528	bit	ts)	on	inter	ace	^
>	Ethe	rn	et	п,	Sn	c:	Gig	a-By	rt 9	c:9	0:0	b (90:	2b :	34:9	9c : 9	90:0	b),	Dst	: Di	igib	oar	75:b4	l:fe	;
>	Inte	rn	et	Pro	toc	01	Ver	sion	ı 4 ,	Sn	c:	192 1	.16	8.1	11.:	163	, Ds	t:	192.	168.	.111	.12	7		¥
<																								>	
0.00	20	00	40	od	75	b 4	fc	00	26	24	96	00	Qh	00	00	45	00		a		4				
001	10	80	34	2e	92	40	00	80	20 06	00	90	-0	a8	6f	a3	-9	a8		1.6		-				
002	20	6f	7f	ff	c4	08	35	67	ad	e9	fd	00	00	00	00	80	02	0	w	e.					
003	80	fa	fØ	60	9a	00	00	02	04	05	b4	01	03	03	08	01	01								
004	10	04	02																						
0	7	E	ther	net:	<live< td=""><td>e cap</td><td>oture</td><td>in pr</td><td>ogre</td><td>ss></td><td></td><td>Pad</td><td>ets:</td><td>238</td><td>75 •</td><td>Displ</td><td>ayed</td><td>: 238</td><td>375 (10</td><td>0.09</td><td>%) </td><td>Pro</td><td>file: Def</td><td>ault</td><td></td></live<>	e cap	oture	in pr	ogre	ss>		Pad	ets:	238	75 •	Displ	ayed	: 238	375 (10	0.09	%)	Pro	file: Def	ault	

8. The capturing can be stopped using the red square icon.

🙍 Ca	pturing from Ethern	et (tcp port 2101)		-		×
File	🕂 View Go	Capture Analyze Stati	stics Telephony Wireles	s Tools H	lelp	
		🎗 🛱 🍳 🗢 🕾	T 👲 📃 🔳 🍳 Q	् 🎹		
App	ly a display filter <0	Strl-/>		🗾 🕶 Ex	pression	+
No.	Time	Source	Destination	Protocol	Length	Infc ^
23	871 321.337572	192.168.111.127	192.168.111.163	TCP	70	210
23	872 321.337646	192.168.111.163	192.168.111.127	TCP	54	654
23	873 321.337730	192.168.111.163	192.168.111.127	TCP	70	654
23	874 321.341872	192.168.111.127	192.168.111.163	TCP	60	210
23	875 321 377954	192.168.111.127	192.168.111.163	TCP	70	216

9. Invoke the Save dialog using the 'Save As' command from the 'File' menu.

	'Ethern	et (tcp p	ort 21	01)		
File	Edit	View	Go	Capture	Analyze	Sta
	Open			C	Ctrl+O	
	Open l	Recent				۲.
	Merge					
	Import	t from H	lex Du	mp		
	Close			C	Ctrl+W	
	Save			C	Ctrl+S	
	Save A	s		C	trl+Shift+	S

10. Name the communication traffic record and save it as the file type shown below.

🚄 Wireshark: Sa	ave file as				×
Save in:	Desktop	~	G 🤌 📂		
Quick access Desktop Libraries This PC	Name	^	Date modifie 29.01.2019 12 31.05.2018 7: 10.08.2018 11 18.01.2018 11 18.01.2018 10 06.06.2018 11 11.10.2018 7: 18.05.2018 11 12.07.2018 11 13.06.2018 10 15.01.2019 9:	ed 2:45 44 3:20 1:58 0:07 4:15 55 3:28 5:43 5:08 02	Type File folder File folder File folder File folder File folder File folder File folder File folder File folder File folder Shortcut
Network	<	Communication		_	>
	Save as type:	Wireshark/ pcapng (*.ntar.gz;*.n	tar;*.pcapnç ~		Cancel
	Compress with g	Wireshark/ pcapng (* ntar.gz;* n Wireshark/tcpdump/ pcap (*.dm Wireshark/tcpdump/ nanosecon Modified tcpdump - pcap (*.dmp.gz;* Jakia tcndump - pcap (*.dmp.gz;* d	tar;*.pcapng.gz; p.gz;*.dmp;*.cap d pcap (*.dmp.g *.dmp;*.cap.gz;*. mp;*.cap.gz;*.ca	.pcapng) .gz;*.cap; z;*.dmp;*.c .cap;*.pcap	.pcap.gz;*.pc ap.gz;*.cap; o.gz;*.pcap) z;*.pcap)

- 11. Contact DataApex Support Team at support@dataapex.com and provide this captured communication.
- 12. DataApex Support Team can also provide guidance regarding types of communication and port numbers for respective devices upon request.