

Wireshark trace - How to make a trace of call

- Program Wireshark is used for tracing the communication between devices interconnected by LAN. The devices (e.g. PBX connected with a GSM gateway via LAN) send to each other packets which are captured by the above mentioned program. Wireshark is distributed under the Open source licence (http://www.wir eshark.org/download.html).
- In order to capture all the packets which are sent via particular LAN, the devices have to be part of the same segment (they have to be connected via HUB). If you do not have a hub, you can use a switch which supports so called port mirroring (http://en.wikipedia.org/wiki/Port_mirroring).

Installation

• Download the program and appropriate installer (e.g. Windows installer).





Wiresbark 1.0.8 Setup		I XI
Choose Components Choose which features of Win	eshark 1.0.8 you want to install.	
The following components are	available for installation.	
Select the type of install:	Wireshark (GTK2 user interface)	
Or, select the optional components you wish to install:	Image: Second state state Image: Second state Image: Seco	
Space required: 90.2MB	Position your mouse over a component to see its description.	
Nullsoft Install System v2.44		
	< <u>B</u> ack <u>N</u> ext > Cancel	
-		
		and second lite
Wireshark 1.0.8 Setup		
Select Additional Tasks Which additional tasks should	be done?	
Create Shortcuts Create Short	be done?	
Create Shortcuts Associate trace file ext cap, enc, erf, fdc, pcap	ensions to Wireshark (5vw, acp, apc, atc, bfr, , pkt, snoop, syc, tpc, tr1, trace, trc, wpc, wpz, rf5)	
Select Additional Tasks Which additional tasks should Create Shortcuts Start Menu Group Desktop Icon Quick Launch Icon File Extensions Associate trace file ext cap, enc, erf, fdc, pcap Nullsoft Install System v2,44	ensions to Wireshark (5vw, acp, apc, atc, bfr, , pkt, snoop, syc, tpc, tr1, trace, trc, wpc, wpz, rf5)	



The Lines i			
🔴 Wireshark 1.0.8 Setup			
Choose Install Location			
Choose the folder in which to install Wireshark	1.0.8.		G
	1.0.0.		
Choose a directory in which to install Wireshark	ς.		
- Destination Folder			
C:\Program Files\Wireshark		Brov	vse
Space required: 90-2MB			
Space available: 76.8GB			
Space analiable notedb			
Nullsoft Install System v2.44			
	- Back	Nevts	Cancel
		Mext >	
Wiresbark 108 Setup			
Install WinPcap?			a
WinPcap is required to capture live network da	ta. Should WinPca	ap be installed?	L 🕂
- Currently installed WinDean yersion			
Currenciy installed winecap version			
WipPcap is currently not installed			
WinPcap is currently not installed			
WinPcap is currently not installed			
WinPcap is currently not installed			
WinPcap is currently not installed Install IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	stall any undetect	ed old WinPcap	versions)
WinPcap is currently not installed Install ✓ Install WinPcap 4.0.2 (Use Add/Remove Programs first to unin	stall any undetect	ed old WinPcap	versions)
WinPcap is currently not installed Install Install (Use Add/Remove Programs first to unin Services	stall any undetect	ed old WinPcap	versions)
WinPcap is currently not installed Install Install IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	stall any undetect	ed old WinPcap	versions)
WinPcap is currently not installed Install Install IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	stall any undetect s can capture)	ed old WinPcap	versions)
WinPcap is currently not installed Install Image: Install WinPcap 4.0.2 (Use Add/Remove Programs first to unin Services Image: Start WinPcap service "NPF" at startup (so users without Administrator privilege	stall any undetect s can capture)	ed old WinPcap	versions)
WinPcap is currently not installed Install Install IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	stall any undetect s can capture)	ed old WinPcap	versions)
WinPcap is currently not installed Install Install IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	stall any undetect s can capture)	ed old WinPcap	versions)
WinPcap is currently not installed Install Image: Install WinPcap 4.0.2 (Use Add/Remove Programs first to unin Services Image: Image: Start WinPcap service "NPF" at startup (so users without Administrator privilege What is WinPcap?	stall any undetect s can capture)	ed old WinPcap	versions)
WinPcap is currently not installed Install Install Image: Install WinPcap 4.0.2 (Use Add/Remove Programs first to unin Services Services Start WinPcap service "NPF" at startup (so users without Administrator privilege What is WinPcap? Nullsoft Install System v2.44	stall any undetect s can capture)	ed old WinPcap	versions)
WinPcap is currently not installed Install ✓ Install WinPcap 4.0.2] (Use Add/Remove Programs first to unin Services ✓ Start WinPcap service "NPF" at startup (so users without Administrator privilege What is WinPcap? Nullsoft Install System v2.44	stall any undetect s can capture) < Back	ed old WinPcap	versions)







77 Wireshark 1.0	.8 Setup		
		Completing the Wireshark 1.0.8 Setup Wizard	
		Wireshark 1.0.8 has been installed on your computer.	
		Click Finish to close this wizard.	
		Run Wireshark 1.0.8	
		Show News	
		< <u>Back</u> <u>Finish</u> Cancel	
/ireshark is then ir	nitiated		
📶 The Wireshark Netw	vork Analyzer		_
The Wireshark Netw File Edit View Go	vork Analyzer Capture Analyz	ze Statistics Help	!
The Wireshark Netv File Edit View Go	vork Analyzer Capture Analyz	ze Statistics Help	[
The Wireshark Netv File Edit View Go	vork Analyzer Capture <u>A</u> nalyz	ze Statistics Help X 2 🖶 Q, 🗢 🗢 🐳 藩 🧟 🗐 🕞 Q, Q, Q, 🖭 🍯 V Expression Clear Apply	[
The Wireshark Netv Eile Edit View Go	vork Analyzer	ze Statistics Help X 2 🖶 🔍 🗢 🗢 🐨 🤽 🗐 🖬 🕀 🔍 🔍 📰 📓 V Expression Glear Apply	 //
The Wireshark Netv File Edit View Go	vork Analyzer	ze Statistics Help X 2 4 0 0 0 7 2 1 4 0 0 0 1 4 1 4 0 0 0 1 4 1 4 1 4 1 4	
The Wireshark Netv File Edit View Go	vork Analyzer Capture Analyz	ze Statistics Help X 2 4 0 0 0 7 2 1 4 0 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	 #
The Wireshark Netv Eile Edit View Go	vork Analyzer Gapture Analyz	ze Statistics Help X 22 📇 🔍 🔅 🗼 🐨 🛣 🗐 🗐 🗐 🔍 Q 🔍 🕅 🗃 V Expression Clear Apply	
The Wireshark Netv File Edit View Go	vork Analyzer	ze Statistics Help X 2 4 0 0 0 7 2 1 4 0 0 0 1 4 1 4 1 1 1 1 1 1 1 1 1 1 1	
The Wireshark Netv File Edit View Go	vork Analyzer	ze Statistics Help X 2 4 0 0 7 4 0 7 4 6 0 7 4 6 0 7 4 6 6 6 7 4 6 6 7 4 6 7 1 4 6 6 6 7 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
The Wireshark Netv File Edit View Go	vork Analyzer	ze Statistics Help X 2 4 0 0 7 1 1 1 1 1 0 0 0 0 1 1 1 1 1 1 1 1	
The Wireshark Netv Eile Edit View Go	vork Analyzer Capture Analyz	ze Statistics Help X 2 4 4 4 2 7 2 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	
The Wireshark Netv Elle Edit View Go Eller:	vork Analyzer Gapture Analyz	ze Statistics Help X 2 4 0 0 7 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1	
The Wireshark Netv Eile Edit View Go Eilter:	vork Analyzer Capture Analyz	ze Statistics Help X 2 4 4 4 2 7 2 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 2 2	
The Wireshark Netv Eile Edit View Go Eilter:	vork Analyzer Gapture Analyz	ze Statistics Help X 2 4 0 0 7 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1	
The Wireshark Netv Eile Edit View Go	vork Analyzer	ze Statistics Help Control Control Co	
The Wireshark Netv Eile Edit View Go Eilter:	vork Analyzer Gapture Analyz	ze Statistics Help C C C C C C C C C C C C C C C C C C C	
The Wireshark Netv File Edit View Go	vork Analyzer Capture Analyz	ze Statistics Help	
The Wireshark Netv File Edit View Go Eilter:	vork Analyzer <u>C</u> apture <u>A</u> nalyz	ze statistics Help	

Start capturing: "Capture->Start" or use icon #1 End capturing: "Capture->Stop" or use icon #2 Restart capturing with deletion of previously captured packets: "Capture->Restart" or use icon #3



Save results: "File->Save As->Wireshark/tcpdump/... -libpcap(*.pcap;*.cap) Open previously saved trace: "File->Open" Basics of filter application:

1. I want to filter the packets according to source IP- eg: ip.src_host=="192.168.5.7"

- 2. I want to filter the packets according to destination IP eg: ip.dst_host=="192.168.5.7"
- 3. Protocol type: tcp, udp, sip, ...
- 4. The terms can be combined via logical expressions : and, or, not, ...
- 5. Applying a filter Apply, Deleting a filter Clear

Example of captured communication

🗖 pokus_wireshark.pcap - Wireshark								
<u>Eile Edit View Go Capture Analyze S</u>	tatistics <u>H</u> elp							
	3 占 🔍 🗢 🛸 😜 ዥ 🔽							
Eilter: Expression Clear Apply								
No Time Source	Destination	Protocol Info						
57 5 772010 100 168 0	:00 Spanning=tree=tro 56 255 255 255 255	IN-UN SIP RSI, RUUL = 327087						
58 6.055340 192.168.2.	239.255.255.250	SSDP M-SEARCH * HTTP/1.						
59 6.056268 192.168.2.3	239.255.255.250	SSDP M-SEARCH * HTTP/1.						
60 6.079625 HewlettP_4	e:82:26 Broadcast	ARP Who has 192.168.1.						
61 6.098099 192.168.2.3	139 192.168.3.255	NBNS Name query NB SERV						
62 6.098102 Kollmorg_T	1:29:50 Broadcast	ARP Who has 192.168.2.						
03 0.279981 192.108.1.	22 192.168.3.255	NBNS Name query NB DCZN						
		<u> </u>						
■ Frame 57 (956 bytes on wire,	956 bytes captured)							
Ethernet II, Src: HwServer_0	0:bb:97 (00:0a:59:00:bb:97),	Dst: Broadcast (ff:ff:ff:ff:ff:ff)						
I Internet Protocol. Src: 192.	168.2.56 (192.168.2.56). Dst:	255.255.255.255 (255.255.255.255)						
Hiser Datagram Protocol, Src	Port: distinct (9999). Dst Pr	art: distinct (9999)						
B baca (SIA Byces)								
4								
0000 ff ff ff ff ff ff ff 00 0a	59 00 bb 97 08 00 45 00	, Y, E.						
0020 ff ff 27 of 27 of 03 9a	22 fe 3c 3f 78 6d 6c 20	'.' ". xml</td						
0030 76 65 72 73 69 6f 6e 3d	22 31 2e 30 22 20 65 6e ve	rsion= "1.0" en						
0040 63 6f 64 69 6e 67 3d 22	55 54 46 2d 38 22 3f 3e co	ding="UTF-8"?>						
Frame (frame), 956 bytes	Packets: 63 Displayed: 63 Marked: 0	Profile: Default						

Example of captured communication after applying a filter



File Edit View Go Capture Analyze Statistics Help						
	¥ -					
Ejiter: jp.src_host=="192.168.2.56" and udp						
No Time Source Destination Protocol Info 27 2.634493 192.168.2.56 255.255.255 UDP Source port: 36 3.703857 192.168.2.56 255.255.255 UDP Source port: 57 5.773219 192.168.2.56 255.255.255 UDP Source port:	disti disti disti					
	_					
■ Frame 57 (956 bytes on wire, 956 bytes captured)						
Ethernet II, Src: HwServer_00:bb:97 (00:0a:59:00:bb:97), Dst: Broadcast (ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	†:††:††) 255 255`					
HILEFINEL PHOLOGON, SIC. 192.108.2.30 (192.108.2.30), DSL. 233.233.233.233 (233.233. HISER Datagram Protocol. Src Port: distinct (9999). Dst Port: distinct (9999)	200.200,					
B Data (914 bytes)						
<u>त</u>	Þ					
0000 ff ff ff ff ff ff 00 0a 59 00 bb 97 08 00 45 00	•					

Important:. In order to provide us with detailed information about the possible problem with the device, please do not apply any filter and simply capture all the communication during the test call. Save it via Save as>Wireshark/tcpdump/... -libpcap(*.pcap;*.cap) and send it to us.

More product information:

 $2N^{\circledast}$ NetStar IP (Official Website 2N)

2N[®] NetStar (Official Website 2N)

Manuals:

Product support for 2N[®] NetStar (wiki.2n.cz)