

Q. How to get TCP/IP communication log?

A: Follow the procedure described below:

Step 1: Download the **WireShark** utility, the **WireShark** is a free and open-source packet analyzer. You can get it from the following web: <u>http://www.wireshark.org/download.html</u>



Step 2: Double click WireShark setup file to install the WireShark utility on your PC. Please follow these steps: (for example, install WireShark under 32-bit Windows XP)

- 1. Click the "<u>Next></u>" button to start the **WireShark** installation.
- 2. Click the "I Agree>" button to continue on the "License Agreement" window.
- 3. Click the "<u>Next></u>" button to continue on the **"Choose components"** window.
- 4. Click the "<u>Next></u>" button to continue on the "Select Additional Tasks" window.
- Click the "<u>Next></u>" button to install the driver into the **default** folder on the "Choose Install Location" window.
- 6. Click the "Install" button to install the WinPcap on the "Install WinPacap?" window.
- 7. Click the "<u>Next></u>" button to start the **WinPcap** installation.
- 8. Click the "I Agree>" button to continue on the "License Agreement" window.
- 9. Click the "Install" button to install the driver on the "Installation options" window.
- 10. Click the "Finish" button to complete the WinPcap installation.
- 11. Come back **Wireshark** installation, click the "<u>Next></u>" button on the "**Installation Complete**" window.
- 12. Check the "Run Wireshark x.xx.x (32-bti)" item then click the "Finish" button to complete the

WireShark installation.

For detailed information about the WireShark installation, please refer to <u>http://www.wireshark.org/docs/wsug_html</u> <u>chunked/ChBuildInstallWinInstall.html.</u>

🔏 Wireshark 1.10.5 (32-bit)	Setup
	Completing the Wireshark 1.10.5 (32-bit) Setup Wizard Wireshark 1.10.5 (32-bit) has been installed on your computer. Click Finish to close this wizard. Run Wireshark 1.10.5 (32-bit) Show News
	< Back Einish Cancel



Step 3: In the WireShark utility, select the "<u>Options...</u>" item from the "<u>Capture</u>" menu.



Step 4: In the **WireShark: Capture Options** window, click **"Start"** button to capture TCP/IP packet.

Wireshark: Capture Options					
Capture					
Capture Interface	Link-layer header	Prom. Mode Snaplen [H]Buffer [MiB]	Capture Filter	
☑ ■域連線 100.120	Ethernet	enabled default	2		E
					×
Capture on all interfaces				Man	age Interfaces
Use promiscuous mode on all interface	s				
Capture Filter:				Compile s	elected BPFs
Capture Files				Display Options	
File:			Browse	☑ Update list of packets in a	real time
Use multiple files	☑ Use pcap-ng format			🖌 Automatically scroll duri	ng live capture
✓ Next file every 1	megabyte(s)			🖌 Hide capture info dialog	
Ring buffer with 2	files			Name Resolution	
Stop capture after 1	file(s)			✓ Resolve MAC addresses	
Stop Capture Automatically After				🔲 Resolve network-layer n	ames
1	 ✓ ✓ 			Start par Start	ame ne resolver Close



Step 5: Running live capture of TCP/IP communication data.

٦	Capt	uring	fror	n Et	連線	(hos	st 10.	0.8.1	1)	[Wire	sharl	1.10.	5 (SV)	l Rev	54262	from /	trunk	-1.1	0)]														
Eile	Ē	dit ∖	/iew	Go	⊆ap	ture	Ana	alyze	Sta	tistics	Tel	ephony	<u> </u>	ls Ir	nternals	Help																	
0	۲			۵			×	2		\ \	\$	A A	7 L			Ð,	Q (0	**	¥	¥ 🖻) 🖪	*	ģ	2								
	Filter														~ E:	xpressic	m		lear		App		Sat	Ve									
No.	97	Tim	e 06	0270	Sou	ce	2 1 1			D	estinat	ion 8 20			Protoco	ol Le	ngth	Info	0		749	Incu	00	ы	500-	1106		ck=20	170	win-	5940	Lor	~
	83	6 27	.06	0421	010.	.0.8	3.20			1	0.0	8.11			TCP		61	. 47	748 :	> n(dmp	[PSH		к]	Seq=	2070		ck=11	.99	win=	-6550	6 L6	en=
	83	7 27	.06	1876	010.	0.8	3.11			1	0.0	8.20			TCP		60) nd	imp :	> 47	748	[PSH	, AC	к]	Seq=	1199	A	ck=20)77	win=	5840	Ler	n=3
	83	8 27	.06	1970	010.	0.8	3.20			1	0.0	8.11			TCP		60) 47	48 :	> no	dmp	[PSH	, AC	к]	seq=	2077	7 A	ck=12	02	win=	6550	3 L6	en=
	83	9 27	.06	3400	010.	.0.8	3.11			1	0.0	8.20			TCP		60) nd	: qmb	> 47	748	[PSH	, AC	к]	seq=	1202	2 A	ck=20	83	win=	5840	Ler	า=4
	84	0 27	.06	3478	010.	.0.8	3.20			1	0.0	8.11			TCP		58	3 4 7	48 :	> no	dmp	[PSH	, AC	K]	seq=	2083	3 A	ck=12	06	win-	6549	9 L6	en=
	84	1 27	.06	4906	010.	.0.8	3.11			1	0.0	8.20			TCP		61	. nd	imp :	> 47	748	LPSH,	, AC	КJ	seq=	1206	δA	ck=20	87	Win=	-5840	Ler	n=7
	84	2 27	.06	5033	010.	.0.8	3.20			1	0.0	8.11			TCP		60	147	48 :	> no	amp	[PSH,	, AC	кJ	seq=	2087	<u> </u>		13	พาทะ	-6549	2 L6	en=
	84	3 27	.06	64 UL	010.	0.8	2 70			1	0.0	0.11			TCP		60		. umu	> 4,	/48 dmp	EPSH,	, дс	K J	Seq=	2002	э ж > х	CK = 21	195	Wiri= Wiri=	= 384 U	Ler	1=3
	84	4 27 5 77	.00	7874	010	0.0	2 11			1	0.0	8 20			TCP		60) =/	40. mn	× 40	ump 74.8	[PSH	, AC	KJ V	seq-	12093	5 0		100	win-	-5840	J LC	2-3
	84	6 27	.16	5861	010.	0.8	3.20			1	0.0	8.11			TCP		54	nr	nfi	lema	ac b	doci	, men	r∖_ †um	-5 [ACK]	ŝ	ea=20	481	Ack	=215	05 V	vin
	84	7 27	.16	7991	010.	0.8	3.20			1	0.0	8.11			TCP		1078	3 pr	ofi	lema	ac >	doci	umen	tum	-s [PSH.	A	ск1 з	ea=	2048	31 AC	k=21	150
	84	8 27	.21	8573	010.	0.8	3.11			1	0.0	8.20			TCP		60) do	ocum	enti	um-s	> pr	rofi	٦em	ac [ACK]	s	eq=21	505	Ack	=215	05 V	√in
	84	9 27	.26	6443	010.	0.8	3.20			1	0.0	8.11			TCP		54	47	48 :	> no	dmp	[ACK]] Se	q=2	099	Ack=	12	19 W1	n=6	5486	i Len	=0	
	85	0 27	.70	6304	010.	0.8	3.11			1	0.0	8.20			TCP		1078	8 em	icrm:	irc	cd >	ssa	d [P	sн,	ACK] Se	eq=	21505	AC	k=21	505	win=	=58
	85	1 27	.70	7156	010.	.0.8	3.20			1	0.0	8.11			TCP		60) 47	748 :	> no	dmp	[PSH	, AC	к]	seq=	2099) A	ck=12	19	Win=	6548	6 L6	en=
	85	2 27	.70	8622	010.	.0.8	3.11			1	0.0	8.20			TCP		60) nd	: qmb	> 47	748	[PSH	, AC	к]	seq=	1219) A	ck=21	.05	win=	5840	Ler	n=3
	85	3 27	.70	8735	010.	.0.8	3.20			1	0.0	8.11			TCP		60) 47	748 :	> no	dmp	[PSH	, AC	к]	seq=	2105	jΑ	ck=12	22	win=	6548	3 L6	en=
	85	4 27	. 71	0095	010.	.0.8	3.11			1	0.0	8.20			TCP		60) nd	: qmt	> 4,	748	LPSH	, AC	К]	Seq=	1222	2 A	CK=23	.11	W1n=	=5840	Ler	1=3
	85	5 27	.81	0590	010	. U. 8	5.20			1	0.0	8.11			TCP		E0/8	5 5 5	sad :	> en	mcrn	inneel	а ЦР Н ГА	SH,	ACK	.J 56	2q=.	215U:		K=22	(529 /10 F	W1D=	=65
	95	7 77	.00	2104	010	0.0	2 20			1	0.0	Q 11			TCP		54	/ em	1CFm 74.9 ·	100	dmn	Face	1 [A 1 GA		5ec 111	0 C k =	-17	75 W	-223 n=6	29 V 5490	0111=3	-0	Le
	0.0		.00		0 I U.						0.0.	.0.11			TCP		54		40.	~ 110	ump	LACK.] 26	ч-2		ACK-	-12	2 1 10	11-0	5460	/ Len	-0	V
œ	=ran	ne 1	: 1	078	byte	s oi	n w1	rei	862	4 b1	ts)	, 107	8 byt	es o	aptur	ed (8	3624	b1	ts)	on	1nt	ertad	te O			- 0.2							
±	≞tne Int/	erne	τι. + ο	I, S noto	rc: col	TCD	das_ cion	50:0	78:C	10 (U	0:0	a:eu: > 11	50:08 (10.0	:C6	J, DST	: ASI	ustei Lo o	кс_	_ca:	28:0 (1.0	C9 (/4:au	1:20	:ca	:28:	C9)							
	Ince Trar	erne Somi	c Pi	noto on C	ontr	oli	Drot	14, 000	SILC I C	ii Iu Tro B	ort		cruic <i>c</i>	cd i	(10004	οι:	10.0	.e.	201	ad.	. 0. e	50)	Sen	• 1	0.0	k• 1		en•	102	л			
Ŧ	Data	a (1)	024	hvt	es)	011	FIUC	.000	·, -	a c r	ore	. emc		.cu i	(10004), U.	SU P	ort		au	(47	JU),	зеч	• -	,	к. <u>т</u>	., '	-en.	102	4			
		. (~,-	/																												
00	00	74 (d0 ;	2b c	a 28	с9	00	0d	e0	50 0	8 ci	5 08	00 45	00	t.+	. (.P		.E.														~
00	L0 20	04 3	28 4 14 1	4e C 27 1	F 00	00	40	06 76	03 67	e3 0	a 01	08 0	0b 0a 03 50	00	• (Ņ	@.		•••															
00	30	16 0	do i	be 3	5 00	00	30	30	30	30 3	0 3	35	39 3a	10		500	5 000	055	9														
00	10	0a i	0b (0⊂ Õ	d Qe	0Ê	10	11	12	13 1	4 1	5 16 :	17 18	19			1.1		123														
00	50 50	1a 1	10 1 26 1	1C 1	d 1e d 20	1† 2f	20	21	22	23 2	4 2	26	27 28 27 39	29	***	- 701	· · · #:	\$%& 456	780														
00	70	3a 3	3b 3	3 C 3	d 3e	ŝŕ	40	41	42	43 4	4 4	46	47 48	49	:;<	=>?@/	A BCI	DEF	GHI														
00	30	4a 4	4b 4	4⊂ 4	d 4e	4f	50	51	52	53 5	4 5	5 56	57 58	59	JKL	MNOPO	RS	TUV	WXY														~
	40.0	- A -	- IT	ר <i>י</i> ור	1 58	٦T	nil	nı	n/	ns h	4 h'	nh	n/hX	nu	213	174 2		пет	11117	_	_		-	-					_				_

Step 6: Click the **"Stop"** button to stop the running live capture.

💪 Cap	turin	g from	區域	連線 (hos	t 10.0.8	.11) [Wi	eshark 1	.10.5	(SVN R	lev 54262	from /trunk-1.10)]
File E	Edit	View	Go	Capture	Analyz	e Statistic	; Telep	honv	Tools	Internals	Help
0 (0 🖌	(٥		×	<u>,</u>		» Ŧ	<u>_</u>		
Filte	ar:	C								✓ E:	ixpression Clear Apply Save
No.	Ti	n I		1		0	Destination			Protoco	ol Length Info
83	352			0.8	.11		10.0.8	.20		TCP	60 ndmp > 4748 [PSH, ACK] Seq=1196 Ack=2070 win=5840 Len=3
83	36 2		_	D d	.20		10.0.8	.11		TCP	61 4748 > ndmp [PSH, ACK] Seq=2070 Ack=1199 Win=65506 Len=
8.	37 2	-	070/	1	.11		10.0.8	.20		TCP	60 ndmp > 4748 [PSH, ACK] Seq=1199 Ack=2077 Win=5840 Len=3
8.	38 2	7.061	9700		20		10.0.8	.11		TCP	60 4/48 > nomp [PSH, ACK] Seq=20// ACK=1202 Win=65503 Len=
8. 0	39 Z	7.063	4000				10.0.8	.20		TCP	60 namp > 4748 [PSH, ACK] Seq=1202 ACK=2083 Win=5840 Len=4
84	40 Z 41 D	7.064	4780	10.0.8	.20		10.0.8	. 11		TCP	58 4748 > nomp [PSH, ACK] Seq=2083 ACK=1206 Win=65499 Len=
0.	41 Z 47 7	7.004	0220	10.0.8			10.0.8	11		TCP	60 4748 > pdmp [PSH, ACK] Seq=1200 ACK=2007 Will=3640 Len=7
8	42 2	7.066	1010	10.0.0	11		10.0.8	20		TCP	60 ndmp \ 4748 [PSH, ACK] Seq=2007 ACK=2213 Win=03492 Len=
8	44 2	7.066	4901	10.0.8	20		10.0.8	11		TCP	60 4748 > pdmp [PSH, ACK] Seq=2093 Ack=2093 win=5640 Len=
8	45 2	7.067	8740	10.0.8	. 11		10.0.8	. 20		TCP	60 ndmp > 4748 [PSH, ACK] Seq=1216 Ack=2099 win=5840 Len=3
84	46 Z	7.165	8610	10.0.8	.20		10.0.8	.11		TCP	54 profilemac > documentum-s [ACK] Sec=20481 Ack=21505 Win
84	47 2	7.167	9910	10.0.8	.20		10.0.8	.11		TCP	1078 profilemac > documentum-s [PSH, ACK] Seg=20481 Ack=2150
84	48 2	7.218	5730	10.0.8	.11		10.0.8	.20		TCP	60 documentum-s > profilemac [ACK] Seq=21505 Ack=21505 Win
84	49 2	7.266	4430	10.0.8	.20		10.0.8	.11		TCP	54 4748 > ndmp [ACK] Seq=2099 Ack=1219 Win=65486 Len=0
8	50 2	7.706	3040	10.0.8	.11		10.0.8	.20		TCP	1078 emcrmirccd > ssad [PSH, ACK] Seq=21505 Ack=21505 win=58
8	51 2	7.707	1560	10.0.8	.20		10.0.8	.11		TCP	60 4748 > ndmp [PSH, ACK] Seq=2099 Ack=1219 win=65486 Len=
8	52 2	7.708	6220	010.0.8	.11		10.0.8	.20		TCP	60 ndmp > 4748 [PSH, ACK] Seq=1219 Ack=2105 win=5840 Len=3
8	53 2	7.708	7350	10.0.8	.20		10.0.8	.11		TCP	60 4748 > ndmp [PSH, ACK] Seq=2105 Ack=1222 win=65483 Len=
8	54 2	7.710	0950	10.0.8	.11		10.0.8	.20		TCP	60 ndmp > 4748 [PSH, ACK] Seq=1222 Ack=2111 win=5840 Len=3
8	552	7.810	5900	010.0.8	.20		10.0.8	.11		TCP	1078 ssad > emcrmirccd [PSH, ACK] Seq=21505 Ack=22529 win=65
8	562	7.862	1040	010.0.8	.11		10.0.8	.20		TCP	60 emcrmirccd > ssad [ACK] Seq=22529 Ack=22529 win=5840 Le
8	572	7.869	9200	010.0.8	.20		10.0.8	.11		TCP	54 4748 > ndmp [ACK] Seq=2111 Ack=1225 Win=65480 Len=0 🕑
🕀 Fra	ame :	1: 10	78 k	bytes or	n wire	(8624 b	its),	1078	bytes	captur	ed (8624 bits) on interface 0
Etr	hern	et II	, sr	'c: Icpo	as_50	:08:c6 (00:0d:	e0:50	:08:0	:6), Dst	: AsustekC_ca:28:c9 (74:d0:2b:ca:28:c9)
Int	ern	et Pr	otoc	col vers	510n 4	, src: 1	0.0.8.	11 (1	0.0.8	5.11), D	ost: 10.0.8.20 (10.0.8.20)
⊞ Ira	insm	15510	n co	ntrol H	rotoc	ol, src	Port:	emcrm	nrcco	1 (10004), DST PORT: SSAG (4750), Seq: 1, ACK: 1, Len: 1024
± Dat	.a (1024	byte	:5)							
0000	74	d0 2	b ca	28 c9	00 0d	e0 50	08 c6	08 00	45 C	10 t.+	. (PE. 🔼
0010	04	28 4	e ct 7 14	12 80	40 06	03 e3	da do	45 02	0a 0	10 . (N	
0030	16	do b	é 35	00 00	30 30	30 30	30 35	35 39	- 3a C	0	500 000559:.
0040	0a	0b 0	c 0d	0e 0f	10 11	12 13	14 15 :	16 17	18 1	.9	
0050	1a	1b 1	< 10	11e 1f	20 21	22 23	24 25	26 27	28 2	9	···· ! "#\$%&`()
0060	2 d. 3 a	20 Z	c 20 c 3d	28 2T	30 31 40 41	32 33 42 43	54 55 44 45 -	30 37 46 47	- 30 - 3 - 48 - 4	9 +,	/VI 23430/09 =>20A BCDEFGHI
0080	4a	4b 4	c 4d	i 4e 4f	50 51	52 53	54 55	56 57	58 5	9 JKLI	MNOPQ RSTUVWXY
0090	5.a	Sh S	c 5d	I Se Sf	60 61	62 63	64 65	66 67	68 F	9 71	1A `a bodefohi 🖉
0 💅	區域	重線: <	ive ca	apture in p	rogress:	> File: C:\I	Packets:	857 · C	Displaye	d: 857 (10	00.0%) Profile: Default

Copyright © 2014 ICP DAS Co., Ltd. All Rights Reserved.



Step 7: Select the "Save <u>As...</u>" item from the "<u>File</u>" menu to save captured packets.



Step 8: In the "Wireshark: Save file as" dialog box, select destination folder to saved capture file.

Step 9: Type file name in the File <u>Name</u>: field (for example, pds-782_log).

Step 10: Specify the **default file save format (*.pcap)** of the **WireShark** by clicking on the **Files of** <u>type</u>: type drop down box.

Step 11: Click "Save" button.

Wireshark: Save	file as	3
Save in:	🛅 Desktop 🕑 🕜 🎓 🖽 -	
My Recent Documents Desktop My Documents	System Volume Information 1.	pds-782_
My Computer	2 3.	
My Network	File name: pds-782_log Files of type: Wireshark/tcpdump/ pcap (*.pcap.;*.pcap.gz v	
	Compress with gzip	

(Finish)