How to use Wireshark to capture

To analyze network issues, it's necessary to get some network packages. And Wireshark is a useful software to capture network package. Here is the quick guide of how to use it.

1. Run the software. You can choose capture and configure capture filter.



Configure capture filter. In the Capture Filter option, please fill in the right filter.
 For example, 'ip src host 172.6.21.134' means we can capture all the network package from the device with the IP address 172.6.21.134. Then click 'Start'.

Capture											
Interface: Lo	cal	-	it Network Cor	nection: \De	evice\NPF_{5						
IP address: fe	30::b037:	cbf3:230	d:772e	e, 172.6.21.101							
Link-layer he	ader type	: Ethe		Wireless Settings							
🔽 Capture p	ackets in	promis		Remote Settings							
Capture p	ackets in i packet f	pcap-n to 1	g form	at (experimental)	Buffer size:	1	megabyte(s)				
Capture Filte	n ip s	rc host 1	72.6.2	1.134							
apture File(s)					Display (Options					
File:				Browse	Vpd	ate list <mark>o</mark> f pa	ckets in real time				
🔲 Use <u>m</u> ultij	ole files										
✓ Next file e	very	1		megabyte(s)	- Auto	omatic scroll	ing in live capture				
 Next file every Ring buffer with 		1		minute(s)	- Hide	Hide capture info dialog					
		2		files							
Stop capture after		1 * file(s)		-Name Re	esolution —						
Stop Capture .			2		Enal	ole <u>M</u> AC nan	ne resolution				
🔲 after	1		÷ pa	acket(s)	Enal	Enable network name resolution					
🔽 after	1	1		megabyte(s)	•						
🔲 after		4 14	minute(s)	- Enal	Enable transport name resolution						

3. Stop capture. After you get the information you want. You can stop capture. Just

by click 'Stop'.

	ntel(R) 82579V Gig	abit Network Connect	ion: Capturing - V	Wireshark				×
Eile	Edit View G	io <u>A</u> nalyze	Statistics Tele	ephony <u>T</u> ools I	Help			
8		Interfaces	Ctrl+I	*****		🗹 🎬 🗹 !	🖲 🛠 🙀	
Filte	er:	Start	Ctrl+E		 Expression Clear Apply 			
No.	- Time	ei ster	1000		Destination	Protocol	Info	
	326 21.199	90 M Restart	Ctrl+R .	21.134	172.6.21.101	TCP	Interleaved channel 0x00, 16 bytes	
	328 21,200	Capture Filters		21.134	172.6.21.101	TCP	[TCP segment of a reassembled PDu]	
	329 21.200	731	172.6.	21.134	172.6.21.101	TCP	Interleaved channel 0x00, 3612 bytes	
	330 21.280	026	172.6.	21.134	172.6.21.101	TCP	Interleaved channel 0x02, 332 bytes	
	331 21.360	122	172.6.	21.134	172.6.21.101	TCP	Interleaved channel 0x02, 332 bytes	
	332 21.440	J83	172.6.	21.134	172.6.21.101	TCP	inder leaved channel UXU2, 332 bytes	
	334 21.520	043	172.6	21.134	172.6.21.101	TCP	Interleaved channel 0x02. 332 bytes	
	335 21,600	292	172.6.	21.134	172.6.21.101	TCP	Interleaved channel 0x02, 332 bytes	
	336 21.680	023	172.6.	21.134	172.6.21.101	TCP	Interleaved channel 0x02, 332 bytes	
	337 21.759	999	172.6.	21.134	172.6.21.101	TCP	Interleaved channel 0x02, 332 bytes	
	338 21.840	164	172.6.	21.134	172.6.21.101	TCP	Inter leaved channel 0x02, 332 bytes	
	340 22 000	035	172.6	21.134	172 6 21 101	TCP	Inter leaved channel 0x02, 332 bytes	
	341 22.080	077	172.6.	21.134	172.6.21.101	TCP	Inter leaved channel 0x02, 332 bytes	
	342 22.160	009	172.6.	21.134	172.6.21.101	TCP	Interleaved channel 0x02, 332 bytes	
	343 22.240	024	172.6.	21.134	172.6.21.101	TCP	Interleaved channel 0x02, 332 bytes	
	rame 1 (738	bytes on wire.	738 bytes c	aptured)				
•	thernet II.	Src: SmdInfor_	7a:d9:6c (00):40:48:7a:d9	:6c), Dst: 04:7d:7b:3	5:c8:01 (04:	7d:7b:35:c8:01)	
	nternet Pro	tocol, Src: 172	.6.21.134 (1	72.6.21.134)	. Dst: 172.6.21.101 (1	172.6.21.101	0	
	ransmission	Control Protoc	ol. Src Port	: rtsp (554)	. Dst Port: 49843 (498	843). Sea: 1	L. Ack: 1. Len: 672	
ΞĒ	TSP Interle	aved Frame, Cha	nnel: 0x02,	332 bytes				
	TCD Totonlo	aund Ename Cha	-040 · 1000	777 hittor				
000	0 04 7d 7b	35 c8 01 00 40	48 7a d9 6	c 08 00 45 00) .}{5@ Hz.lE.			
001	0 02 d4 00	4a 40 00 40 06	b4 e2 ac 0	6 15 86 ac 0	5 3@.@			1
002	0 11 98 62	d3 00 00 01 01	08 02 00 5	3 02 87 00 0	5 b 5			
004	0 a1 d2 24	02 01 4c 80 80	13 22 00 0	0 d3 09 23 4	3\$L"#C			
005	0 88 8f 67	67 67 67 67 67	67 67 67 67	7 67 67 67 67	· · gggggg gggggggg			
006	0 67 67 67	67 67 67 67 67 67	67 67 67 67 67	7 11 67 67 67 6	gggggggg gggg.ggg			
008	0 67 67 67	67 ff 67 67 67	67 67 67 67 6	7 67 67 67 67 67	7 0000,000 0000000			
009	0 67 67 67	67 67 67 67 67	67 67 67 6	7 67 67 67 6	7 99999999 99999999			
00a	0 67 67 67	67 67 67 67 67 67	67 67 67 67	7 67 67 67 67	2 99999999 99999999			
000	0 67 67 67	67 67 67 67 67 67	67 67 67 67 ft	f 67 67 67 67 6				
000	0 67 67 67	67 67 67 67 67	67 67 67 67	7 67 67 67 67 6	7 gaagaaaa gagagaaga			
00e	0 67 67 67	67 67 67 67 67 67	67 67 67 67	7 67 67 67 67	99999999 99999999			
00f	0 67 67 67	67 67 67 67 67 67	67 67 67 6	7 67 67 67 6	7 aaaaaaaa aaaaaaaa			
O	ntel(R) 82579V Gig	abit Network Connecti	on Packets: 34	13 Displayed: 343 N	larked: 0		Profile	
		ê 🔉			M 🥂 M		▲ 🕅 🗰 🗇 9:29 2012-06	-28

4. Save the captured package. After you stop. You can save the information by

click 'Save' . Name it and save it.

📶 (Untitl	led) - Wireshark							_						
<u>File</u> Edi	it <u>V</u> iew <u>G</u> o <u>C</u> apt	ture Analyze Statistics Telephony Tools	Help											
		🕞 X 😂 占 🔍 🔶 🔶 😽			5 %	100								
Filter:		Save this capture file	 Expression Clear Apply 											
No	Time	Source	Destination	Protocol	Info									
	1 0.000000	172.6.21.134	172.6.21.101	TCP	ir dm	> 49784	PSH.	ACK S	eq-1 Ack-	1 Win=289	6 Len-8 TSV	-5418563	TSER-34716	70
	2 8 039750	172.6.21.134	172.6.21.101	TCP	irdmi	> 49784	EPSH.	ACK]	seq=9 ALK-	-1 win=209	o Len=o i Sv	CV=5419367	TSER=347	072
	4 12,059730	172.6.21.134	172.6.21.101	TCP	irdm	i > 4978/	EPSH.	ACK1	Seg=25 Ack	-1 Win=28	96 Len=8 T	SV-5419769	1 TSER=348	374
7	5 16,083320	172.6.21.134	172.6.21.101	TCP	irdmi	i > 49784	PSH.	ACK1	Seg=33 Ack	=1 win=28	96 Len=8 Tf	5V=5420171	TSER=348	776
	6 19, 342331	172, 6, 21, 134	172.6.21.101	TCP	irdm'	+ 49825	SYN/	ACK1	Seg=0 Ack+	0 win-579	2 I.en=0 MS	5=1460 TSV	=5420497 7	ESER=3
	7 19.343124	172.6.21.134	172.6.21.101	TCP	irdmi	> 49825	FACK1	Seg=1	Ack=36 Wi	n=2896 Le	n=0 TSV=547	20497 TSER	=349484	
1	8 19.344775	172.6.21.134	172.6.21.101	TCP	irdmi	1 > 49825	FPSH,	ACK]	Seg=1 Ack=	-36 Win=28	96 Len=16 T	TSV=542049	47 TSER=34'	9484
	9 19.350759	172.6.21.134	172.6.21.101	TCP	irdmi	> 4982F	STAN,	ACK]	Seg=0 Ack-	0 win=579	2 Len=0 MSS	5=1460 TSV	-5420498 7	(SER=3
1	0 19.360860	172.6.21.134	172.6.21.101	TCP	irdmi	i > 4982F	FACK]	Seg=1	Ack=36 Wi	n=2896 Le	n=0 TSV=547	20499 TSER	c=349486	
1	1 19.362680	172.6.21.134	172.6.21.101	TCP	irdmi	i > 4982F	j [PSH.	ACK]	Seg=1 Ack=	-36 Win=28	96 Len=16 T	TSV=542049	9 TSER=34	9486
1	2 19.367856	172.6.21.134	172.6.21.101	TCP	irdmi	> 49827	ESYN,	ACK]	seq=0 Ack=	0 win=579	2 Len=0 MSS	5=1460 TSV	=5420499 7	(SER=3
1	3 19.368729	172.6.21.134	172.6.21.101	TCP	irdmi	> 49827	[ACK]	Seq=1	Ack=32 Wi	n=2896 Le	n=0 T5V=547	20499 TSER	=349487	
1 1	4 19.371484	172.6.21.134	172.6.21.101	TCP	irdmi	/ > 49827	[PSH,	ACK] S	Seq=1 Ack=	32 Win=28	96 Len=196	TSV=54205	00 TSER=3/	49487
¥	5 19.372428	172.6.21.134	172.6.21.101	ТСР	irdmi	> 49827	[RST,	ACK]	5eq=197 Ac	k=33 Win=	2896 Len=0	TSV=54205	JOO TSER=3/	49487
I I	.6 19.377172	172.6.21.134	172.6.21.101	TCP	irdmi	/ > 49828	[SYN,	ACK]	Seq=0 Ack=	0 Win=579	2 Len=0 M55	5=1460 TSV	=5420500 7	/SER=3
1	7 19.379814	172.6.21.134	172.6.21.101	TCP	irdmi	/ > 49825	[ACK]	Seq=17	7 Ack=37 W	/in=2896 L	en=0 TSV=54	420501 TSE	R=349484	
j 1'	.8 19.387392	172.6.21.134	172.6.21.101	TCP	irdmi	, > 49828	[ACK]	Seq=1	Ack=32 Wi	n=2896 Le	n=0 TSV=542	20501 TSER	=349489	
 Ether Inte Tran Data 	rnet II, Src: 9 Innet Protocol, Ismission Contr a (8 bytes)	SmdInfor_7a:d9:6c (00:40:48:7a:d6 src: 172.6.21.134 (172.6.21.134 ol Protocol, Src Port: irdmi (80):6c), Dst: 04:7d:7b:35:), Dst: 172.6.21.101 (1: 00), Dst Port: 49784 (4	:c8:01 (04: 72.6.21.101 9784), Seq	:7d:7b: 1) : 1, Ac	35:c8:01) k: 1, Le) n: 8							
0000	04 7d 7h 35 c8	01 00 40 48 72 49 66 08 00 45 (10 3{5 @ H7] E											
0010 /	00 3c bd 7f 40	00 40 06 fa 44 ac 06 15 86 ac f	06 <@.@D											
0020 .*	15 65 1f 40 c2	. 78 81 82 24 52 64 79 bc ca 80 1	.e.@.x \$Rdy											
0030 0	0b 50 44 cf 00	00 01 01 08 0a 00 52 ae 43 00 C	J5 .PD R.C											
0040 4	4c 20 00 00 00	08 00 00 00 02	L											
1														
1											G	th 1 9	1	-
A File */	C\Ukers\Tern\AnnDz	Packets: 613 Displayed: 613	Marked: 0 Dropped: 0					-				Protiler \$ 8	,.5K/S 1 0K/	,S 😕
- THE	. (USEISTICITY) PROVIDE	Ad Local (Terring)	Marked: 0 propped. 0			Committee of						FIGHE		0-30
						101		And the owner of the				- Na 🕅 I	AT 10	9:26
				1000 V		And ()							2017	2-06-28



After all these steps, you are successful to capture some network package.