# Un outils parmi beaucoup d'autres pour surveiller un réseau informatique

## Free Network Analyzer: Wireshark.

Wireshark is a network packet analyzer. A network packet analyzer presents captured packet data in as much detail as possible.

You could think of a network packet analyzer as a measuring device for examining what's happening inside a network cable, just like an electrician uses a voltmeter for examining what's happening inside an electric cable (but at a higher level, of course).

In the past, such tools were either very expensive, proprietary, or both. However, with the advent of Wireshark, that has changed. Wireshark is available for free, is open source, and is one of the best packet analyzers available today.

#### 1.1.1. Some intended purposes

Here are some reasons people use Wireshark:

- Network administrators use it to troubleshoot network problems
- Network security engineers use it to *examine security problems*
- QA engineers use it to verify network applications
- Developers use it to *debug protocol implementations*
- People use it to *learn network protocol* internals

Wireshark can also be helpful in many other situations.

### 1.1.2. Features

The following are some of the many features Wireshark provides:

- Available for UNIX and Windows.
- *Capture* live packet data from a network interface.
- *Open* files containing packet data captured with tcpdump/WinDump, Wireshark, and many other packet capture programs.
- *Import* packets from text files containing hex dumps of packet data.
- Display packets with very detailed protocol information.
- *Save* packet data captured.
- *Export* some or all packets in a number of capture file formats.
- Filter packets on many criteria.
- *Search* for packets on many criteria.
- *Colorize* packet display based on filters.
- Create various *statistics*.
- ...and a lot more!

However, to really appreciate its power you have to start using it.

Figure 1.1, "Wireshark captures packets and lets you examine their contents." shows Wireshark having captured some packets and waiting for you to examine them.

right 1.1. Wheshark captures packets and res you examine their contents
---

	tv-netf	lix-prob	lems	s-201	1-07	7-06	.pcap	)																	
File	Edit	View	Go	。(	Capt	ure	An	alyz	e	Stat	istic	s	Tele	pho	ny	Wire	eless	5 1	Fools	He	lp				
		۲		010		C	9	æ	⇒	Ð	Ŷ	ł	2			Ð	Q,	Q							
	Apply a d	display f	ilter	<ci< td=""><td>trl-/&gt;</td><td>&gt;</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></td><td></td><td></td><td></td><td></td></ci<>	trl-/>	>																			
No.	т	Time		Sour	ce				De	estin	atior	ווווו ו			Pro	tocol		Len	gth	Info					
	343 6	5.142	415	192	.168	8.0	.21		17	74.	129	. 249	9.2	28	TC	Р			66	4055	5 →	80	[AC	К]	Sec
	344 6	5.142	715	192	.168	8.0	.21		17	74.	129	. 249	9.2	28	HT	TΡ			253	GET	/cl	ien	ts/n	etf	11)
	345 6	5.230	738	174	.129	9.24	49.2	28	19	92.	168	.0.3	21		TC	Р			66	80 →	40	555	[AC	К]	Sec
	346 6	5.240	742	174	.129	9.24	49.2	28	19	92.	168	.0.3	21		HT	TΡ			828	HTTF	/1.	1 3	02 M	ove	d 1
	347 6	5.241	592	192	.168	8.0	.21		17	74.	129	. 249	9.2	28	TC	Р			66	4055	5 →	80	[AC	К]	Sec
*	348 6	5.242	532	192	.168	8.0	. 21		19	92.	168	.0.:	1		DN	S			77	Star	dar	d q	uery	0x	218
+	349 6	5.276	870	192	.168	8.0	.1		19	92.	168	.0.1	21		DN	S			489	Star	Idar	d q	uery	re	spo
i	350 6	5.277	992	192	.168	8.0	.21		63	3.8	0.24	42.4	48		TC	Р			74	3706	3 →	80	[SY	N]	Sec
i	351 6	5.297	757	63.8	80.2	242	.48		19	92.	168	.0.1	21		TC	Р			74	80 ⊣	37	063	[SY	Ν,	ACI
i	352 6	5.298	396	192	.168	8.0	.21		63	3.8	0.24	42.4	48		TC	Р			66	3706	3 →	80	[AC	К]	Sec
i i	353 6	5.298	687	192.	.168	8.0	.21		63	3.8	0.24	42.4	48		HT	TP			153	GET	/us	/nr	d/cl	ien	ts,
	354 6	55.318	730	63.8	80.2	242	.48		19	92.	168	.0.:	21		TC	Р			66	80 ⊣	37	063	[AC	к]	Sec
	355 6	55.321	733	63.8	80.2	242	.48		19	92.	168	.0.:	21		TC	Р		1	.514	[TCF	se	gme	nt o	fa	n
<																									
> L ~ [	Jser D Domain <u>[Re</u>	Name Quest	am P Sys In:	roto tem <u>348</u>	ocol (re 3]	L, S espo	onse	Port )	t: 5	53	(53)	),[	Dst	Por	rt:	3403	36	(34(	<b>3</b> 36)						
	[Ti	me: 0	034	3380	900	sec	ond	s]																	
	Tra	nsacti	Lon 🗄	ID:	0x2	2188	3																		
	> Fla	gs: 0)	(818)	0 St	cand	lard	l que	ery	nes	spoi	nse,	, No	o ei	rnor	•										
	Que	stions	s: 1																						
	Ans	wer RF	<s: 4<="" td=""><td>4</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></td><td></td><td></td><td></td><td></td><td></td><td></td></s:>	4																					
	Aut	hority	/ RR:	s: 9 -	)																				
	Add	itiona	al Ri	Rs:	9																				
	✓ Que	ries																							
	>	can-0.	nT13	ximg	;.co	im:	туре	εА,	C1	.ass	5 II	1													
	> Ans	wers																							
	Aut	norita	ILIV	e na	mes	serv	ers																		
002	00 00	15 00	35	84	f4	01	c7	83	3f	21	88	81	80	00	01		5		?	!. <mark>.</mark>					
003	80 <b>00</b>	04 00	0 09	00	09	05	63	64	6e	2d	30	07	6e	66	6c	•		••••	c dr	-0.n	fl				
004	10 78	69 60	1 67	03	63	61	6d ee	00	00	01	60	61	67	0C	00	X:	ımg	. cor	"		•••				
005	0 07	6e 6	5 74	66	60 60	69	78	03	63	69 6f	6d	09	65	64	67		net:	) fli:	· · ·	om.e	dg				
007	0 65	73 75	5 69	74	65	03	6e	65	74	00	c0	2f	00	05	00	e	sui	te.i	n et	/.					
	-	1	tion			tion	(dec	id) i	2 byt																

# **1.1.3.** Live capture from many different network media

Wireshark can capture traffic from many different network media types, including Ethernet, Wireless LAN, Bluetooth, USB, and more. The specific media types supported may be limited by several factors, including your hardware and operating system. An overview of the supported media types can be found at

https://gitlab.com/wireshark/wireshark/wikis/CaptureSetup/NetworkMedia.