Wireshark 101

Essential Skills for Network Analysis

R

Course Contents

• [Enter the topics you wish to cover.]

WARNING

Before you capture your first packet, ensure you have permission to listen to the network traffic. If you are an IT staff member, obtain written permission to listen in to network traffic for troubleshooting, optimization, security, and application analysis.

Consult a legal specialist to understand your local and national laws regarding packet capture on wired or wireless networks.

Fundamentals – Why Wireshark?

Wireshark Capabilities

- General traffic analysis
- Troubleshooting
- Security
- Application analysis

Supported OSes

- \circ Windows
- *NIX
- \circ MAC

- Determine **who is talking** in the trace file
- Determine which applications are in use
- Filter on the **conversation** of interest
- Graph the **IO rate** to look for drops in throughput
- Open the Expert to look for problems
- Determine the **round trip time** to identify path latency

Quick Reference Key Graphical Interface Elements

		tr-wins	ize.pca	png									0)							_		×	_
	<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u> </u>	o <u>C</u> ap	ture	<u>A</u> nalyze	e <u>S</u> ta	atistics	Tele	phony	<u>W</u> ire	eless	<u>T</u> ools	Help	(2)								
			۲		- X	C	۹ 🗢	e) 5	2	<u>₽</u>		€ ,	ପ୍ସ୍	1	3									
		Apply a c	lisplay f	filter .	<ctrl- <="" th=""><th>></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>4) 🗆</th><th></th><th>Expression</th><th>n +</th><th></th></ctrl->	>														4) 🗆		Expression	n +	
	No.		Т	ime		So	urce			I	Destinat	ion			Protoc	ol Lengt	h Info						1	•
		6591	L 1	6.9	94303	80 1	0.0.5	52.1	.64		204.	152	.184	.134	ТСР	54	[ТСР	Windo	ow Upd	ate]	2646	→ 80	[AC	
		6592	2 1	6.9	94324	4 2	04.15	52.1	.84.1	134	10.0	.52	.164		ТСР	151	4 80 →	2646	[ACK]	Seq=	46369	960 A	ck=4	
E	5)	6593	31	6.9	94352	28 1	0.0.5	52.1	.64		204.	152	.184	.134	ТСР	54	2646	→ 80	[ACK]	Seq=	:444 /	Ack=4	5384	
9	2	6594	1 1	6.9	94430	3 2	04.15	52.1	.84.1	L34 :	10.0	.52	.164		ТСР	151	<mark>.4 80</mark> →	2646	[ACK]	Seq=	46384	420 A	ck=4	
		6595	51	6.9	94443	36 1	0.0.5	52.1	.64	1	204.	152	.184	.134	ТСР	54	2646	→ 80	[ACK]	Seq=	:444 /	Ack=4	5398	
		6596	51	6.9	94518	36 2	04.15	52.1	.84.1	.34	10.0	.52	.164		ТСР	123	<mark>080</mark> →	2646	[PSH,	ACK]	Seq	=4639	380 🕏	,
	<																						>	
	>	Fram	e 65	92:	: 151	.4 b	ytes	on	wire	e (:	1211	2 bi	its)	, 15	14 b	ytes	captur	ed (12	2112 b	its)	on i	nterf	ac 🧉	4
	>	Ethe	rnet	: 11	C. Sr	·c:	3Com	Cor	p_c9	:51	: b6	(00:	:04:	75:c	9:51	:b6),	Dst:	SonyCo	orp_f4	:3a:0	9 (0	3:00:	46	
Ĉ					-,							·												
		Inte	rnet	: Pr	roto	: 01	Vers	ion	4, 9	Src	: 20	4.15	52.1	34.1	34,	Dst:	10.0.5	2.164						
ų	9	Inte Tran	rnet smis	: Pr sic	rotoc on Co	ol ontr	Vers ol P	ion roto	4, s ocol	Src , Si	: 20 rc P	4.15 ort:	52.18 : 80	34.1 (80	34,), D	Dst: st Po	10.0.5 rt: 26	2.164 46 (20	546),	Seq:	46369	960,	\с	
4	2	Inter Trans Sor	rnet smis urce	: Pr sic Pc	roto on Co ort:	ol ontr 80	Vers ol P	ion roto	4, s ocol	Src: , Si	: 20 nc P	4.15 ort:	52.18 : 80	34.1 (80	34,), D	Dst: st Po	10.0.5 rt: 26	2.164 46 (20	546),	Seq:	46369	960,	4c	
	2	Inter Trans Sor Des	rnet smis urce stin	: Pr sic Po ati	roto on Co ort: Lon F	ol ontr 80 Port	Vers ol P	ion roto 46	4, 9 ocol	Src: ,Si	: 20 rc P	4.15 ort:	52.18 : 80	84.1 (80	34,), D	Dst: st Po	10.0.5 rt: 26	2.164 46 (20	546),	Seq:	46369	960,	4c	,
C	2	Inter Trans Soc Des	rnet smis urce stin	: Pr sic Pr ati	rotoc on Co ort: ion F	ol ontr 80 Port	Vers ol P :: 26	ion roto 46	4, 9 0col	Src:	: 20 °C P	4.15 ort:	52.18 : 80	(80	34,), D	Dst: st Po	10.0.5 rt: 26	2.164	546),	Seq:	4636	960,	Ac	
	0	Inter Trans Soc Des 020	rnet smis urce stin 34	: Pr sic Po ati a4	on Coort:	col ontr 80 Port	Vers ol P : 26 a 56	ion roto 46 48	4, 9 ocol e7	Src: , Si b8	: 20 rc P 75	4.19 ort: b8 0	52.13 : 80	34.1 (80 ba	34,), D 50	Dst: st Po 10 78	10.0.5 rt: 26 4. <mark>.P</mark> .\	2.164 46 (20 /Hu	546),	Seq:	46369	960,	Ac	
6	9 0 0	Inter Trans Sor Des 020 030	rnet smis urce stin 34 ff 68	Pr sic Pr ati a4 ff	rotoc on Co ort: ion F 00 1 cc 1	ol ontr 80 Port 0 0 1c 0	Vers ol P : 26 0a 56 00 00	ion roto 46 48 e5 20	4, 9 ocol e7 48 be	Src: , Si b8 57	: 20 rc P 75 93	4.19 ort: b8 (63 3	52.13 : 80 08 de 36 04	(80 (80 ba 7a	34,), D 50 d6 00	Dst: st Po 10 78 ed	10.0.5 rt: 26 4. <mark>.P</mark> .\	2.164 46 (20 /Hu .H W.	546), P. c6.z.x	Seq:	4636	960,	Ac	
C		Inter Trans Sor Des 020 030 040 050	rnet smis urce stin 34 ff 68 15	Prisic Pristo Pristo Pristo Pristo Pristo Pristo Pristo Pristo Pristo Pr	on Co ort: ion F 00 1 cc 1 d5 a	ontr 80 Port 10 0 10 0 10 0	Vers ol P :: 26 0 56 0 00 16 e2	ion roto 46 48 e5 a0 5b	4, 5 ocol e7 48 be ec	Src: , Si b8 57 35 32	20 75 93 1d	4.15 ort: b8 (63 3 79 4 1d 4	52.11 : 80 08 do 36 04 48 50	(80 (80 ba 7a ad ad	34,), D 50 d6 00 dd	Dst: st Po 10 78 ed c2	10.0.5 rt: 26 4. <mark>.P</mark> .\	2.164 46 (26 /Hu .H W. 5.	546), P. c6.z.x yHP	Seq:	46369	960,	Ac	
		Inter Trans Des 020 030 040 050	rnet smis urce stin 34 ff 68 15	: Pr sic Pc ati a4 ff d0 f3	on Co on Co ort: ion F cc 1 d5 a b0 c	ontr 80 Port 0 0 1c 0 1c 0 1c 0	Vers ol P 26 27 26 26 26 26 26 26 26 26 26 26 26 26 26	ion roto 46 48 e5 a0 5b	4, s ocol e7 48 be ec	Src: , Si b8 57 35 32	: 20 rc P 75 93 1d ba	4.19 ort: b8 (63 3 79 4 1d e	52.11 : 80 08 do 36 04 48 50 ef 29	34.1 (80 ba 7a ad 4d	34,), D 50 d6 00 dd	Dst: st Po 10 78 ed c2	10.0.5 rt: 26 4P.\ h	2.164 46 (20 /Hu .H W. 5. [. 2.	546), P. c6.z.x yHP)M	Seq:	46369	960,	Ac	

wireshark.org/download.html



^

Wireshark Capture Elements



(c) Wireshark Ur

* GTK support will eventually be discontinued in Wireshark v2.

Dissect the Wireshark Dissectors



How Heuristic Dissectors Work



Frames vs. Packets vs. Segments



Wireshark Resource: Q & A Forum



p-google101.pcapng

The Default Three-Pane View

								http	p-goo	gle101	.pca	png						-		×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iev	v <u>G</u> o	<u>C</u> apt	ure <u>A</u>	nalyze	<u>S</u> tatistic	s Te	lephon	y <u>W</u> ire	less	Tools	<u>H</u> elp							
		۲	015	X	ି ବ୍	•	⇒ 😤 👔	4		. ⊕	୍ ୍	1 🎹								
	Apply a	display	filter <	:Ctrl-/>														Expre	ssion	+
No.		Time	Source			Destin	ation	1	Protoco	Lengt	n In	ō			-				-	>
7		1 0	24.6	0.1/3	3.220	75.	/5./5.	/5	DNS	74	St	canda	ird q	uery	0xae	06 A	WWW	.goog	gle	-
-		2 0 2 0	15.1	5./5 173)./5) 220	24.0	D.1/3.	75	DNS	154	t 51 c4	canda	ira qi	uery	resp	onse	Øxa	200 A	A WW.	
		20	75 7	5 75	5 75	24 6	5.75. 5.173	, , , , , , , , , , , , , , , , , , ,	DNS	10) St	tanda	and a		Pac	ket	List	Par	ne	
		5 0	24.6	.173	3.220	74.	125.22	4	ТСР	66	3	5145	→ 80	[SYN	Il Se	a=0	Win=	8192	Len.	
		6 0	74.1	25.2	224	24.0	5.173.	220	ТСР	66	8) → 3	5145	[SYN	I, AC	к] s	eq=0	Ack=	=1 W.	
		7 0	24.6	.173	3.220	74.3	125.22	4	тср	54	35	5145	→ 80	[ACK	.] Se	q=1	Ack=	1 Wir	1=65.	. 🗸
	Ether Inter User Doma: [R Tr Fl Qu An Au Ad	nnet Data in Na ansa ags: esti swer thor diti	II, Prot agram ame S nse I otion 0x01 ons: RRs: ity R onal	Src: ocol Pro yste ID: 00 S 1 0 Rs: RRs:	Hew Verstoco m (qu] 0xa itand 0 0	lett sion l, Si uery e0b ard	P_a7:b 4, Sr rc Por) query	f:a3 c: 2 t: 5	3 (d4 24.6. 51724	:85:6 173.2 (517	4:a) 20, 24)	7:bf: Dst: , Dst	a3), 75. Por	Dst: 75.75 Pa	Cad .75 .(52 	ant_	31:bl	s Pa	(00.	
00)10	00 3	3c 08	3d (00 00	80 (11 00	00	18	06 ad	dc	4b 4	b	.<.=.			KK			^
00	020	4b 4	lb ca	0c (00 35 00 00	00	28 50	b2	ae	0b 01 67 6f	00 6f	00 0 67 6		KK	5.(\				
00	140	65 6	00 00 03 63	6f	6d 00	003	01 00	9 01	00	07 OT	OT	07 0	C	P	ack	et E	Byte	s Pa	ne	
Ĺ		55 1																		~
0	7	Number	of querie	es in pa	cket (dn	s.count	queries), 2	bytes		Packe	ts: 37	4 • Displa	ayed: 37	4 (100.0	%) • Lo	ad time	: 0:0.9	Profile	e: Defa	ult 🔡

Use the Main Wireshark View

Note: The Start page appears when no trace file is open. Become accustomed to using the menus and toolbars in Wireshark.



Wireshark Resource: Wiki Pages

4	http-google101	.pcapng	- 🗆 🗙
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze	<u>S</u> tatistics Telephon <u>y</u> <u>W</u> irel	ess <u>T</u> ools <u>H</u> elp	
🔟 🗏 🙆 😺 😺 🖉 🖉) 😫 🗿 👲 📲 🔍 🔍	e, 🖳 🎹	
Apply a display filter <ctrl-></ctrl->			Expression +
No. Time Source	Destination	Protocol Lengt	n Info 🔨
1 0.000000 24.6.173.22	0 75.75.75.75	DNS 74	Standard query 0xae0b
▲ 2 0.013237 75.75.75	24.6.173.220	DNS 154	1 Standard query respons…
3 0.013971 24.6.173.22	0 75.75.75.75	DNS 74	Standard query 0x4553 🤤
	(FO2 hita) 74 hita		FO2 hits) on interface 0
Frame 1: 74 bytes on wire	right-click	es captured (1:27:6f:22)	592 Dits) on interface 0
A Internet Protocol Version	1. 3	+.a/.DI.a5),	5 75
0100 - Version: A	Expand Subtrees	Shift+Rig	ht p.r.s
0100 = Version. 4	Expand All	Ctrl+Righ	ot l
Differentiated Services	Collapse <u>A</u> ll	Ctrl+Left	(T)
Total Length: 60	Apply as Column		
Identification: 0x083d	Apply as Filter		•
▷ Flags: 0x00	Prepare a Filter		•
Fragment offset: 0	Conversation Filter		•
Time to live: 128	Colorize with Filter		•
Protocol: UDP (17)	Follow		•
Header checksum: 0x0000			
Source: 24.6.173.220	Copy		
Destination: 75.75.75.7	Export Packet Bytes	Ctrl+H	
Source GeoIP: United S	Wiki Protocol Page		cations, Inc., Milpitas…
Destination GeoIP: Uni	Eilter Field Reference		mmunications, Inc., Ind
User Datagram Protocol, Si	Protocol Preferences		• 3 (53)
Domain Name System (query)	Decode <u>A</u> s		
	Go to Linked Packet		
🔘 🝸 Internet Protocol Version 4 (ip), 20 byte	Show Linked Packet in Ne	w Window	:0.27 Profile: Default

p-browse101.pcapng Customize Wireshark for Different Tasks

C	olumne	
	oluiiiis	
		<u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephon <u>y</u> <u>W</u> ireless <u>T</u> ools <u>H</u> elp
		🗙 🖬 🤄 🗢 🗢 🕸 💽 🗐 🤍 Q. Q. 뫺
	ignment	Expression +
		Source Destination Protocol Length Info
		. 75.75.75.75 24.6.173.2… DNS 135 Standard query response 0x8920 … 💾
C	oloring	. 174.137.42… 24.6.173.2… TCP 66 80→42379 [SYN, ACK] Seq=0 Ack=1…
Ŭ	oloring	. 24.6.173.2… 174.137.42… TCP 54 42379→80 [ACK] Seq=1 Ack=1 Win=… 🚽
		. 24.6.173.2 174.137.42 HTTP 345 GET / HTTP/1.1
	- :!!4	. 174.137.42… 24.6.173.2… TCP 6080→42379 [ACK] Seq=1 Ack=292 Wi… —
	Fliters	. 174.137.42 24.6.173.2 TCP 1 [TCP segment of a reassembled P 🖵
		AF bytes on wine (2760 bits) 345 bytes centured (2760 bits) on inte
		545 bytes on wire (2760 bits), 545 bytes captured (2760 bits) on inte
Dis	ssectors	, SPC. HewiettP_d7.DF.as (d4.85.84.a7.DF.as), DSt. Cadant_SI.DD.CI (
		rotocol version 4, Src: 24.6.1/3.220, Dst: 1/4.13/.42.75
		on Control Protocol, Src Port: 42379, Dst Port: 80, Seq: 1, Ack: 1, L
Viei	hla Danas	Transfer Protocol
VISI	DIE Falles	
		5c 31 bb c1 d4 85 64 a7 bf a3 08 00 45 00\1 dE.
Extra	a Analysis	18 84 40 00 80 06 00 00 18 06 ad dc ae 89 .K@
		a5 8b 00 50 08 09 ae 7a d1 c9 6b 08 50 18 *KPzk.P.
	0030 40	9f f4 00 00 47 45 54 20 2f 20 48 54 54 50 @)GE T / HTTP
	🔵 🍸 http-browse:	Packets: 2011 · Displayed: 2011 (100.0%) · Load time: 0:0.343 Profile: Wireshark101

Locate Key Wireshark Configuration Files

About Wireshark ? × Folders Wireshark Authors Plugins Keyboard Shortcuts License Name Location Typical Files "File" dialogs capture files D: \Trace Files \Master Distributed \ C:\Users\LAURA ~1\AppData\Local\Temp untitled capture files Temp dfilters, preferences, ethers, ... Personal configuration C: Users Jaura 000 Ap...ta Roaming Wireshark d:\Program Files\Wireshark dfilters, preferences, manuf, ... Global configuration d:\Program Files\Wireshark System ethers, ipxnets Program d: \Program Files \Wireshark program files C:\Users\laura_000\Ap...ing\Wireshark\plugins Personal Plugins dissector plugins Global Plugins d:\Program Files\Wireshark\plugins\2.0.1 dissector plugins d:\Program Files\Wireshark\extcap Extcap Plugins search path Extcap path Select Help | About Wireshark | Folders to locate the global and personal configuration directories

Your custom profiles are located in a profiles directory under the Personal configuration folder

OK

p-google101.pcapng

Related Packets Indicator



Work with Columns in the Packet LIST Pane

	http-es	pn101.pcapng								_		×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> a	pture <u>A</u> nalyze	Statistics Telephor	y <u>W</u> ireless <u>T</u> ool	s <u>H</u> elp						
		🖲 📙 🔚 🗙	🔄 🤇 🗢 🖻	🖻 🗿 🕹 📃 🗏	🗏 🔍 Q, Q, 🌉							
	Apply a d	lisplay filter <ctrl-< th=""><th>·/></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>Expression</th><th>. +</th></ctrl-<>	·/>								Expression	. +
No.		Time	Source		Destination		Protocol	Length	Time to live	Info		^
	1	0.0000	00 24.6.	173.220	75.75.75	.75	DNS	72	128	Standard	quer.	
Ł	2	0.0147	49 75.75	Expand Subtree	5	Shift+Right	DNS	88	7 59	Standard	quer.	
	3	0.0158	70 24.6.	Expand All		Ctrl+Right	DNS	71	128	Standard	quer.	
	4	0.0292	05 75.75	Collapse <u>A</u> ll		Ctrl ceft	DNS	122	59	Standard	quer.	 ~
~	Inte	ernet Pro	tocol Ve	Apply as Colun	n), D;	t: 75	5.75.75	.75		^
	01	00	= Versio	Apply as Filter		,	1	/				
	••	0101	= Header	Prepare a Filter		•						
	∽ Di	fferenti	ated Ser	Conversation F	ilter	•	- sø,	ECN:	Not-EC1	r)		
	(000 00.	. = Diff	Colorize with F	ilter	•	int:	Defa	ult (0)			
		00	9 = Expl:	Follow		•	bn:	Not E	CN-Capa	ble Trans	port.	
	То	tal Leng	th: 58	Сору		•			•		•	
	Id	entifica	tion: 0x	Export Packet <u>E</u>	ytes	Ctrl+H						
	~ F1	ags: 0x0	0	Wiki Protocol P	age							
	6	a	. = Rese	Filter Field Refe	rence							
		9	= Don't	Protocol Prefer	ences	•						
		 A	- Mono	Decode <u>A</u> s								
				Go to Linked Pa	acket							
	Fr.	agment O	TTSEL: 0	right-click	acket in New Window	N						
	11	me to li	ve: 128	13			_					~
0	🖌 т	ime to live (ip.ttl), 1	byte			Pad	kets: 4900 · I	Displayed: 49	00 (100.0%) · L	.oad time: 0:0.175	Profile: Defa	ault

p-google101.pcapng

Sort and Reorder Columns

http-google101.pcapng			– 🗆 X
<u>File Edit View Go Capture Analyze Statistics</u> T	elephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp		
∡ ■ ∅ ◎ 📙 🗟 🗙 🖻 ९ ⇔ ⇔ 🕾 🗿 🎍		lara	
Apply a display filter <ctrl-></ctrl->	Click P	lere	Expression +
No. Time Source	Destination Protoco	Leigth Info	^
→ 10.000000 24.6.173.220	75.75.75.75 DNS	🗸 74 Standard query	/ 0xae0b A www
↓ 2 0.013237 75.75.75.75	24.6.173.220 DNS	154 Standard query	response Oxa
3 0.013971 24.6.173.220	75.75.75.75 DNS	74 Standard query	0x4553 AAAA 1
4 0.027695 75.75.75.75	24.6.173.220 DNS	102 Standard query	response 0x4
231 0.558709 24.6.173.220	75.75.75.75 DNS	75 Standard query	0x6fbd A plu
232 0.558727 24.6.173.220	75.75.75.75 DNS	75 Standard query	0xa730 A man
232 0 558808 24 6 173 220	75 75 75 75 DNS	75 Standard query	$0 \times 0 \times$
		75 Standard query	OXE250 A PIA
	73.73.73.75 DN3	75 Standard query	OX/SAD A SSI
A http-google101.pcapng			– 🗆 X
File Edit View op Capture Analyze Unistics T	elephony Wireless Tools Help		
	N Q Q A		
Click and Drag Cttl-/>			Expression +
No. Source Destination	Protocol Time	Length Info	<u> </u>
- 1.4.6.173.220 75.75.75	.75 DNS 0.000000	74 Standard query	/ 0xae0b A www
2 75.75.75 24.6.173	.220 DNS 0.013237	/ 154 Standard query	response Øxa
3 24 173 220 75 75 75	.75 DNS 0.013971	74 Standard query	0x4553 ΔΔΔΔ
4 75 75 75 75 24 6 173	220 DNS 0 027695	102 Standard query	response 0x4
	24 90 TCD 0 029600	$\sim 66.351/15 \rightarrow 90$	NI Sog-A Win-
	24.00 TCP 0.020095		
0 /4.125.224.80 24.6.1/3	.220 TCP 0.0460/1	1 00 80 → 35145 [SY	N, ACK] Seq=0

Hide, Display, Rename, and Remove Columns

	http-goo	ogle101.pcapng						— C) X
Fil	e Edit	View Go Capture	Analyze Statistics Telep	hony Wireless Tools He	lp				
		🖲 📘 🖬 🗙 😂	९ 🗢 🔿 🗟 🗿 🛓 📑	📃 ପ୍ ପ୍ ସ୍ 🎹					
	Apply a di	isplay filter <ctrl-></ctrl->						Expres	sion +
No.		Time	Source	Destination	Protocol	Length Unf	n		^
T	•	10.000000	24.6.173.220	75.75.75.75	DNS	74 👌	Align Left	0xae0b	A ww
۹L	-	20.013237	75.75.75.75	24.6.173.220	DNS	154	Align Center Align Right	respons	e Øx
		30.013971	24.6.173.220	75.75.75.75	DNS	74		0x4553	AAAA
		40.027695	75.75.75.75	24.6.173.220	DNS	102	Column Preferences	respons	e Øx
		50.028699	24.6.173.220	74.125.224.80	ТСР	66	Resize To Contents	N] Seq=0	Win
		6 0.046071	74.125.224.80	24.6.173.220	ТСР	66	Resolve Names	N, ACK]	Seq=
		7 0.046258	24.6.173.220	74.125.224.80	ТСР	54	No	K] Seq=1	Ack
		8 0.046998	24.6.173.220	74.125.224.80	HTTP	342 🔍	Time		
		9 0.065701	74.125.224.80	24.6.173.220	ТСР	66 🔨	Source	K] Seq=1	Ack
	1	10 0.120474	74.125.224.80	24.6.173.220	нттр	1484 🗸	Destination	K (text	/htm
	1	110.122674	74.125.224.80	24.6.173.220	ТСР	1484	Protocol	K] Seq=1	431
	1	12 0.122680	74.125.224.80	24.6.173.220	тср	86: ~	Length	H, ACK]	Seq=
	1	13 0.122682	74.125.224.80	24.6.173.220	тср	1484	inio	K] Seq=3	670
	1	14 0.122685	74.125.224.80	24.6.173.220	тср	1484	Remove This Column	K] Seq=5	100
۲.,	~~~~		224-9	24	70~~	~290,80	A in many of	u ackn	\$^q=/

Change the Time Column Setting

View | Time Display Format | Seconds Since Previous Displayed Packet

	http-op	enoffice101b.pcap	ong							_		×
<u>F</u> il	e <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> a	pture <u>A</u> nalyze <u>S</u> tatistics	Telephon <u>y W</u> ireless <u>T</u> oo	ols <u>H</u> elp							
		ی 🖪 📙	🔄 🍳 🗢 🔿 🗟 👔	🌡 📃 🗏 Q. Q. 🛛	E							
	Apply a d	lisplay filter <ctrl-< td=""><td>-/></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>Expression.</td><td>. +</td></ctrl-<>	-/>								Expression.	. +
No.	1	Time	Source	Destination	Protocol	Length Info						^
		0.226388	190.101.135.12	24.6.173.220	ТСР	66 80 -	→ 21458	[SYN,	ACK]	Seq=	0 Ack=1	L
	19	0.207913	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 2145 8	[ACK]	Seq=1	0221	Ack=1	L
	144	0.205086	24.6.173.220	150.101.135.12	ТСР	54 214	58 → 80	[ACK]	Seq=1	166 /	Ack=143	3
	14	0.195098	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=4	381 /	Ack=116	5
	43	0.193580	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[PSH,	ACK]	Seq=3	35041 A	A
	25	0.193321	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=1	7521	Ack=11	L
	9	0.193286	150.101.135.12	24.6.173.220	ТСР	60 80 -	→ 21458	[ACK]	Seq=1	Ack:	=1166 N	N
	32	0.192023	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=2	4821	Ack=1	L
	77	0.190336	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=7	1541	Ack=1	L
	117	0.189079	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=1	15341	1 Ack=1	L
	95	0.188946	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=9	0521	Ack=1	L
	176	0.188778	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=1	75201	1 Ack=1	L
	58	0.186775	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=5	1101	Ack=1	L
	207	0.184125	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=2	07321	1 Ack=	L
	295	0.182731	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=2	97841	1 Ack=	L
	80	0.181651	150.101.135.12	24.6.173.220	ТСР	1514 80 -	→ 21458	[ACK]	Seq=8	28404	41 Ack	= 🗸

0 🛛

Packets: 17483 · Displayed: 17483 (100.0%) · Load time: 0:0.311 Profile: wireshark101

Right-Click in the Packet LIST Pane

🚄 http-google101.pcapng	– 🗆 X
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephony <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
◢ ■ ∅ ◎ _	
Apply a display filter <ctrl-></ctrl->	Expression +
lo. Time Source Destination Protocol Length Info	^
1 0.000000 24.6.173.220 75.75.75 DNS 74 Standard quer	∽y 0xae0b A www
2 0.013237 75.75.75.75 24.6.173.220 154 Standard quer	ry response 0xa
→ 3 0.013971 24.6.173.220 75.75.75.75	y 0x4553 AAAA
4 0.027695 75.75.75.75 24.6.173.220 Mark/Unmark Packet Ctrl+M	y response 0x4
5 0.028699 24.6.173.220 74.125.224.8	YN] Seq=0 Win=
6 0.046071 74.125.224.80 24.6.173.220 Time Shift Ctrl+Shift+T	YN, ACK] Seq=0
7 0.046258 24.6.173.220 74.125.224.8 Packet Comment	CK] Sea=1 Ack=
8 0.046998 24.6.173.220 74.125.224.8 Edit Resolved Name	1
9 0.065701 74.125.224.80 24.6.173.220	CKl Sea=1 Ack=
10 0 120474 74 125 224 80 24 6 173 220 Apply as Filter	OK (text/html
Prepare a Filter	>
Ename 3: 74 bytes on wine (592 bits) 7 Colorize Conversation	its) on inter
Ethennet TI Snc: HewlettP a7:hf:a3 (dd SCTP	adant 31.bb.
Internet Distance Vencion 4 Space 24 6	
Hernet Protocol Version 4, Src: 24.6.	
User Datagram Protocol, Src Port: 63342	(53)
0000 00 01 5c 31 bb c1 d4 85 64 a7 bf	dE. ′
0010 00 3c 08 3e 00 00 80 11 00 00 18 Decode <u>As</u>	КК
0020 4b 4b f7 6e 00 35 00 28 5c b2 45	↓(\.ES
0030 00 00 00 00 00 03 77 77 77 06 67 6f 6f 67 6c	.w ww.googl
Rackets: 374 · Displayed: 374 (100.0%) · /	Load time: 0:0.7 Profile: Default

Right-Click in the Packet Details Pane

http-google101.pcapng		-	
File Edit View Go Capture Analyze	Statistics Telephony Wireless Tools	Help	
🚄 🔳 🖉 🛞 📙 🛅 🔀 🗳 I 🛠 🗢 🛛	⇒ 🕾 🗿 🖢 🚍 📃 @, Q, Q, Щ		
Apply a display filter <ctrl-></ctrl->	Expression	+ GET POST CONNECT HEAD HTTP4xx H	ITTP5xx HTTP3xx
No. Time Length S	ource Destination Prot	ocol Info	^
1 0.000000 74 2	4.6.173 75.75.75.75 DN	S Standard query 0xae0b	A www
↓ 2 0.013237 154 7	25.75.75.75 24.6.173 DN	S Standard query respons	se Øxae… 🗸
Frame 1: 74 bytes on	right-click its), 74 bytes	captured (592 bits) on in	terfac ^
Interface id: 0 (\D	Expand Subtrees Shift-	Right 5E4-EEFF300A9B9F})	
Encapsulation type:	Expand All Ctrl+	Right	
Arrival Time: Oct 2	Collapse All Ctrl+	Left Fic Daylight Time	NOTE
[Time shift for thi	Apply as Column	, ,	
Epoch Time: 1350938	Apply as Filter	•	RIGNT-CIICK TO
Time delta from pr	Prepare a Filter	▶ 000 seconds]	view
[Time delta from pr	Conversation Filter	▶ 2000 seconds]	numorouo
[Time since referen	Colorize with Filter	▶ seconds]	numerous
Frame Number: 1	Follow	•	options in the
Frame Length: 74 by	Сору	•	Packet Details
Capture Length: 74	Export Packet Bytes Ctrl+	н	
[Frame is marked: F	Wiki Protocol Page		pane
[Frame is ignored:	Filter Field Reference		
[Protocols in frame	Protocol Preferences	•	
[Coloring Rule Name	Decode As		
[Coloring Rule Stri	Go to Linked Packet		
> Ethernet II, Src: Hew	Show Linked Packet in New Window	a3), Dst: Cadant_31:	bb:c1
Tutanuat Duataan Van-			×
💛 🔄 Frame (frame), 74 bytes	Packets: 374 * Dis	splayed: 574 (100.0%) * Load time: 0:0.11 Profil	e: wresnark101

p-google101.pcapng

Pay Attention to the Status Bar

0030 00 00 00 00 00 00 03 77 0040 65 03 63 6f 6d 00 00 01	77 77 06 67 6f 6f 67 6c 00 01 e.	w ww.googl
🔵 🍸 Total Length (ip.len), 2 bytes	Packets: 374 · Displayed: 64 (17.1%) · Load time: 0:0.8	Profile: wireshark101
Field, capture or trace file information Annotation button Expert Infos button	Packet count and load time information	Current profile in use
	NOTE Contents of this column changes depending on wh you've highlighted in the the panes	at ree

Quick Reference

Capture Options



Apply Capture Filters

Local Area Connection* 2 Wi-Fi	Ethernet	enabled enabled nter your cap reduce the r packets ca	default default oture filter to number of aptured	2	
Enable promiscuous mode on all interfaces Capture Filter for selected Interfaces: Enter a capture	e filter			Manage Interfaces Compile BPF	s
Enable promiscuous mode on all interfaces Capture Filter for selected Interfaces: Enter a capture	e filter	packets ca	aptured	Manage Interfaces	



Use Proper Display Filter Syntax (Wireshark-Specific Syntax)

Filter Type	Filter Example
Protocol	arp
Application	dns
Field Existence	http.host
Characteristic Existence	tcp.analysis.zero_window
Field Value	http.host=="www.wireshark.org"
Regex [*] Search Term	http.host matches "\.(?i)(exe zip)"

*Wireshark uses the Pearl-Compatible Regular Expression (PCRE) engine.

Display Filter Techniques

- **Type in** if you know the field names/syntax (error detection mechanism)
- Auto-complete to walk you through building a display filter
- Expressions to walk you through building a display filter with/without comparison operators
- **Recall** saved or previously-used filter
- **Right-click** in the Packet List pane for conversation filters or on a Table row
- Create buttons out of your favorite display filters.

Learn the Field Names

	http-	browse101.pcapn	g							×
<u>F</u> il	e <u>E</u> di	it <u>V</u> iew <u>G</u> o	<u>C</u> apture <u>A</u> nalyze <u>S</u> tati	stics Telephon <u>y W</u> ireless	<u>T</u> ools <u>H</u> e	elp				
		0 🕒 🔚	🗙 🛅 । ९ 👄 🔿 🗟	🗿 🕹 📃 📃 🔍 Q 🖉	ə, 🎹					
	Apply a	a display filter <c< th=""><th>Ctrl-/></th><th></th><th></th><th></th><th>🖘 🔹 Exp</th><th>pression</th><th>+ HTT</th><th>P Errors</th></c<>	Ctrl-/>				🖘 🔹 Exp	pression	+ HTT	P Errors
No.	^	Time	Source	Destination	Protocol	Info				^
	10	0.000853	24.6.173.220	174.137.42.75	HTTP	GET / HTTP/1.1				
	11	0.020101	174.137.42.75	24.6.173.220	ТСР	80 → 42379 [ACI	K] Seq=1 Ack=29	92 Win	=6912	
	12	0.003404	174.137.42.75	24.6.173.220	HTTP	HTTP/1.1 200 O	K [Unreassemble	ed Pac	ket]	
	13	0.001870	174.137.42.75	24.6.173.220	ТСР	80 → 42379 [ACI	K] Seq=1461 Acl	(=292	Win=6	9
	14	0.000662	24.6.173.220	174.137.42.75	ТСР	42379 → 80 [AC	K] Seq=292 Ack	=2921	Win=6	5 🗸
>	> Frame 10: 345 bytes on wire (2760 bits), 345 bytes captured (2760 bits) on interface 0 ^									
>	> Ethernet II, Src: HewlettP_a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant_31:bb:c1 (00:01:5c:3									
>	> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 174.137.42.75									
>	> Transmission Control Protocol, Src Port: 42379 (42379), Dst Port: 80 (80), Seq: 1, Ack: 1									
~	Y Hypertext Transfer Protocol									
	✓ GET / HTTP/1.1\r\n									
	<pre>> [Expert Info (Chat/Sequence): GET / HTTP/1.1\r\n]</pre>									
		Request M	1ethod: GET ┥			-				
		Request L								
			JRI: /							
		Request \	JRI: /							~

Quickly Filter on a Field in a Packet (the right-click method)

			Expand Subtrees	Shift+Right		
			Expand All	Ctrl+Right		
🚄 http-e	spn101.pcapng		Collapse <u>A</u> ll	Ctrl+Left		
<u>F</u> ile <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u> ap	ture <u>A</u> naly: 🖸 🍳 🗢	Apply as Column		Chand	
Apply a	display filter <ctrl- <="" th=""><th>></th><th>Apply as Filter</th><th></th><th>Selected</th><th>xpression +</th></ctrl->	>	Apply as Filter		Selected	xpression +
No.	Time	Source	Compared a Futer		not selected	^
8	0.000665	24.6.1	Conversation Filter		<u>a</u> nd Selected	
. 9	0.041099	199.18	Colorize with Filter	•	<u>o</u> r Selected	manen
			Follow	•	a <u>n</u> d not Selected	······································
> Fram > Ethe > Inte > Tran ~ Hype ~ GE >	e 8: 603 by rnet II, Sr smission Co rtext Trans T / HTTP/1. [Expert Inf Request Met Request URI	rtes on rc: Hew] col Vers ontrol F ofer Pro 1\r\n Fo (Chat chod: GE	Copy Export Packet Bytes Wiki Protocol Page Filter Field Reference Protocol Preferences Decode As Go to Linked Packet right-click cet in New W	Ctrl+H	o <u>r</u> not Selected 3), Dst: Cadar 199.181.132.25 .), Dst Port: 8	s) on… ^ it_31:b… 0 0 (80)…
	Request Ver	sion H	TTP/1 1			
Ac	cept: appli	cation/	x-ms-application, i	image/jpeg, a	application/xam	ıl+xml,
Ac	cept-Langua	ige: en-l	US\r\n			
Us	er-Agent: M	lozilla/	4.0 (compatible; MS	SIE 8.0; Wind	dows NT 6.1; WC	W64; T
(c) Wireshark University	HTTP Request-URI (htt	p.request.uri),	1 byte Packets: 4900 · D	isplayed: 4900 (100.0%)) · Load time: 0:0.83 Profi	e: wireshark101

p-browse101.pcapng

Use Auto-Complete to Build Display Filters

📕 http-bro	01.pcapng – 🗆 🗙	
<u>F</u> ile <u>E</u> dit	/ <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Telephon <u>y W</u> ireless <u>T</u> ools <u>H</u> elp	
🛋 🔳 🙆	📙 🛅 🕱 🔄 🍳 👄 🕸 🗿 👲 🚍 🖳 🔍 Q. Q. 🏨	
http.requ	Expression + HTTP Errors	
No.	tp.request.full_uri Destination Protocol Info	
1	tp.request.method 2.2.2.2.2.2.75.75.75.75 DNS Standard query 0x9ba8 A www.wireshark	
2	tp.request.uri	
3	Auto-complete lists all available 300783 24.6.17 Auto-complete lists all available diamlay filters that has in with	
4	030017 24.6.17 http.request. ard guery 0x8920 AAAA www.wiresha	
5	203284 75,75,75,75 24,0,173,220 phy scandard query response 0x8920 AAAA ww	
– 6	http-browse101.pcapng –	×
	a Edit View Go Canture Analyze Statistics Telephony Wireless Tools Help	
		TD Erro
	top.analysis.ack lost segment	IP Erro
	tcp.analysis.ack_rtt 75_75_75_DNS_Standard_cucpus_AvObaS_A_statu_ui_nochank	
	1 (tcp.analysis.acks_frame 75.75.75 DNS Standard query 0X9Da8 A www.w1resnark	•
	2 tcp.analysis.duplicate_ack 24.6.1/3.220 DNS Standard query response 0x9ba8 A www.	w
	3 (tcp.analysis.duplicate_ack_frame 75.75.75 DNS Standard query 0x8920 AAAA www.wiresh	a
	4 (tcp.analysis.fast_retransmission 75.75.75 DNS Standard query 0x8920 AAAA www.wiresh	a
	5 (tcp.analysis.initial rtt 24.6.17 response 0x8920 AAAA w	W
	6 (tcp.analysis.keep_alive 174. TCP packets analyzed by Wireshark's Seq=0 Win=8192 Len=0	
	7 (tcp.analysis.lost segment 24.6 Expert System can be viewed using esponse 0x8920 AAAA w	W
	8 (tcp.analysis.out_of_order 24.6 cone of the filters beginning with ACK] Seq=0 Ack=1 Win	=
	9 transmission 174.1 Seg=1 Ack=1 Win=6570	0
	10 (tcp.analysis.rto 174.137.42.75 HTTP GET / HTTP/1.1	
	tcp.analysis.rto_frame 11 (tcp.analysis.sourious_retransmission 24.6.173.220 TCP 80 \rightarrow 42379 [ACK] Seg=1 Ack=292 Win=69	1
	12 (tcp.analysis.tfo_syn V 24.6.173.220 HTTP HTTP/1.1.200 OK [Upreaseembled Packet	1
	12 CH 2004 270 177 127 127 127 127 127 127 220 THE	1
ireshark U	ISITY	~

Comparison Operators

Operation	English	Example	Description
==	eq	ip.src == 10.2.2.2	Display all IPv4 traffic from 10.2.2.2
!=	ne	tcp.srcport != 80	Display all TCP traffic from any port except port 80
>	gt	<pre>frame.time_relative > 1</pre>	Display packets that arrived more than 1 second after the previous packet in the trace file
<	lt	tcp.window_size < 1460	Display when the TCP receive window size is less than 1460 bytes
>=	ge	dns.count.answers >= 10	Display DNS response packets that contain at least 10 answers
<=	lt	ip.ttl <= 10	Display any packets that have 10 or less in the IP Time to Live field
	contains	http contains "GET"	Display all the HTTP client GET requests

Note: Be careful using the != operator.

Filter on a Single TCP or UDP Conversation (the right-click method)

🚄 http-espn101.pcapng		– 🗆 X
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>Go</u> <u>C</u> apture <u>A</u> nalyze <u>S</u> tatistics Teleph	ion <u>y W</u> ireless <u>T</u> ools <u>H</u> elp	
🚄 🔳 🖉 💿 📙 🛅 🔀 💼 । ९. 🗢 🗢 堅 🚯 🚍	📃 @, Q, @, 🎹	
Apply a display filter <ctrl-></ctrl->		Expression +
No. Time Source Destina	tion right-click	^
<pre>508 0.000303 24.6.173.220 184 509 0.000188 24.6.173.220 184 510 0.000040 24.6.173.220 75.7 511 0.000250 24.6.173.220 75.7 512 0.000003 24.6.173.220 184 </pre>	84.222.42 Mark/Unmark Packet Ctr 84.222.48 Ignore/Unignore Packet Ctr '5.75.75 Set/Unset Time Reference Ctr '5.75.75 Time Shift Ctr '84.222.48 Packet Comment Ctr '5.75.75 Edit Resolved Name Apply as Filter '3 (d4:85:6 Stilter	rl+M rl+D rl+T rl+Shift+T on interface 0 bb:c1 (00:01:5c:
 > Internet Protocol Version 4, Src: > Transmission Control Protocol, Src 	24.6.173.2 Conversation Filter Colorize Conversation	ENIP IO ENIP Explicit
<pre> Hypertext Transfer Protocol GET /prod/assets/tabs-A-sprite.p Expert Info (Chat/Sequence): </pre>	SCTP SCTP Follow	Ethernet IPv4
Request Method: GET Request URI: /prod/assets/tabs Request Version: HTTP/1.1 Accept: */*\r\n	Copy Protocol Preferences Decode <u>A</u> s Show Packet in New <u>W</u> indow	PN-CBA PN-IO AR
	Packets: 4900 · Displayed: 4900 (100.0%) · L	oad time: 0:0.80 Profile: wireshark101

Use Filters to Spot Communication Delays

🚄 http-downlo	ad101d.pcapng				-		×	
<u>F</u> ile <u>E</u> dit <u>V</u> ie	w <u>G</u> o <u>C</u> apture <u>A</u> nalyze <u>S</u> t	atistics Telephon <u>y W</u> i	eless <u>T</u> ools	<u>H</u> elp				
	📙 🛅 🔀 🔂 । ९ 👄 🖶	2 🗿 🕹 📃 📃 🍳	ର୍ ବ୍ 🏢					
Calculateta	> 1				E E	xpression	. +	
Conversatio	source	Destination	Protocol Ir	nfo				
ns	000000 216.239.11.	. 192.168.1.64	ТСР [[TCP Retran	smission] 80	ð → 18	328	
Timestamps	.885 216.239.11.	. 192.168.1.64	TCP 8	30 → 18280	[ACK] Seq=2	249861	L A	
setting	9.41 216.239.11.	. 192.168.1.64	ТСР [[TCP Retran	smission] 80	ð → 18	328	
must be	129637 216.239.11.	. 192.168.1.64	TCP 8	30 → 18280	[ACK] Seq=20	ð16566	51	
anablad to	size value: 5840						^	
	napled to lated window size: 5840]							
see this	w size scaling fa	ctor: -1 (unkn	own)]					
Ilimestamp	um: 0x6fd5 [valid	ation disabled]					
s] section	s section pointer: 0							
> [SEQ/	> [SEQ/ACK analysis]							
💊 [Time	<pre>>[Timestamps]</pre>							
[Ti	[Time since first frame in this TCP stream: 37.248064000 seconds]							
[Ti	me since previous	frame in this	TCP stre	eat: 1.51812	25000 second	ls]		
🔵 📝 Time de	elta from previous frameis TCP strea	m (tcp.time_delta Packets	24098 · Displaye	red: 4 (0.0%) · Load t	ime: 0:0.431 Profile:	wireshark	101	

Use Right-Click to Follow a Stream

🚄 http-espn101.pcapng		- 🗆 ×
<u>File Edit View Go Capture Analyze Statistics Te</u>	lephon <u>y W</u> ireless <u>T</u> ools <u>H</u> el	p
🚄 🔳 🖉 💿 📙 📑 🗙 🛅 I 🔍 👄 🕾 🕾 🕭	📃 📃 🔍 🔍 🔍 🎹	
tcp.stream eq 0		Expression +
No. Tin Destina	tion Protocol	Info
5 1 right-click 173.3 0 29.	181.132.250 TCP	19941 → 80 [SYN] Seq=0 Win=8192 Len=
6 Mark/Unmark Packet	173.220 TCP	80 → 19941 [SYN, ACK] Seq=0 Ack=1 Wi…
7 Ignore/Unignore Packet Ctr D	81.132.250 TCP	19941 → 80 [ACK] Seq=1 Ack=1 Win=657
8 Set/Unset Time Reference Ctrl+	1,132.250 HTTP	GET / HTTP/1.1
9 Declet Connect	173.220 11 W	ireshark · Follow TCP Stream (tcp.stream eq 0) · http-espn — 🛛 🛛 🗙
31	81.132.250 TC	
Edit Resolved Name	ta) 66 hyta 0a	I / HITP/1.1
Apply as Filter	LS), 00 Dyte: AC	cept: application/x-ms-
Prepare a Filter	as (04:65:04 ap	plication, image/jpeg,
Conversation Filter	24.0.1/3.22(ap	plication/xaml+xml, image/git,
Colorize Conversation	ic Port: 1994. im	age/pjpeg, application/x-ms-xbap,
	ap	plication/vnd.ms-excel,
Follow	TCP Stream	plication/vnd.ms-powerpoint,
Сору	ODP Stream Packet	8. 1 client pkt(s), 1 server pkt(s), 1 turn. Click to select.
C Protocol Preferencer	SSL Stream Entire	conversation (979 bytes) Show data as ASCII Stream 0
Sec Protocol Preferences	sequence nul Find:	Find Next
Ack Show Packet in New Window		Hide this stream Print Save as Close Help
Hea		
	Packets: 4900	Displayed: 7 (0, 1%) : Load time: 0:0, 101 Profile: wiresbark 101
tp-espn101.pcapng

Filter on a Conversation from Wireshark Statistics

🚄 Wireshark	Conve	rsations · http-e	espn101													_		\times
Ethernet · 1	IPv4	· 37 IP	TCP · 63	3 DP ·	82													
Address A	Port A	Address B	Port B	Packets	By	ight-click	У	tes A \rightarrow B	Packets B	→A	Byte	es B → A	Rel Start		Duration	$Bits/s\:A\toB$	Bits/s	s ^
24.6.173.220	19996	184.84.222.88	80	1,855		Ight-click		30 k		1322		1989 k	9.72647	9000	64.450526	3765	j	
24.6.173.220	19976	184.84.222.120	80	534/	2	Apply as Filter	F	Sel	ected		•	A +	• B	000	62.455871	1413	}	
24.6.173.220	19980	184.84.222.10	80	251		Prepare a Filter	۲	No	t Selected		•		- D	000	61.220801	620)	
24.6.173.220	19945	184.84.222.48	80	150		Find	•					A -	+ D	000	68.853274	847		
24.6.173.220	19956	184.84.222.152	80	137		rinu	ĺ	a	nd Selected	1	•	В –	٠A	000	17.293814	3944	ļ	
24.6.173.220	19942	68.71.216.176	80	127		Colorize	•	0	r Selected			A +	+ Any	000	24.512076	2332	2	
24.6.173.220	19944	184.84.222.48	80	121	1161	k 42		a	nd not Sele	ected	•	Δ -	+ Anv	000	68.853471	665)	
24.6.173.220	19981	184.84.222.10	80	120	119	k 41			r not Select	tod		<u> </u>		000	61.220638	359)	
24.6.173.220	20002	68.71.216.157	80	112	10	k 57		0	i not selec	leu		Any	y→A	000	42.514690	586	5	
24.6.173.220	19983	184.84.222.152	80	111	1111	k 38		6082		73		Any	y ↔ B	000	66.207100	734	ļ	
24.6.173.220	19961	74.125.224.59	80	110	103 I	k 37		3751		73		Any	v→B	000	65.383440	458	3	
24.6.173.220	19943	184.84.222.48	80	90	81	k 34		5823		56			A	000	68.852948	676	j	
24.6.173.220	19950	184.84.222.48	80	88	85	k 29		4579		59		в-	• Any	000	57.356422	638	3	
24.6.173.220	19954	184.84.222.48	80	67	62	k 25		4006		42		58 k	3.21628	4000	56.403650	568	3	
24.6.173.220	19978	184.84.222.120	80	61	59 I	k 21		1734		40		57 k	7.91303	6000	61.259194	226	5	~
<	10055	*******	00		- 10 1	20				24			2.24000	2000	FC 400070	50	` >	
Name resolu	ution	🗌 Limit t	o display filt	ter					Сор	у 🔻	Fo	ollow Strea	m (Graph		Conversa Close	tion Typ Help	es

Turn Your Key Display Filters into Buttons

- 1. Create a display filter and click .
- 2. Name your Filter Expression button. (Reorder/edit/disable or delete in **Preferences | Filter Expression.**)

	k					_	
<u>F</u> ile <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u>	apture <u>A</u> nalyze <u>S</u> tati	istics Telephon <u>y W</u> ir	eless <u>T</u> ools <u>H</u> e	p		
	🖲 📙 🗈 🔀	रे 📴 । ९ 🗢 🔿 🕾	T 🕹 📃 🔳 🔍	ର୍ ବ୍ 🏢			
📕 http.reque	est.method matche	es "(GET POST)"				🛛 🔁 🕶 E	xpression
Filter Express	sion Preferences.		Label: GET POST	Filter:	d matches "(GET POST)"	ОК	Cancel
No.	Time	Source	Destination	Protocol Info			
35	0.00000	24.6.169.43	108.160.161	HTTP GET	/subscribe?h	lost_int=36	542662
L.	×z 52	~24.6/~~~42	Masa V		~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	- int=36	4
	and the second se		V				
📕 http-cha	ppellu101b.pcap	ong				_	
 http-cha <u>F</u> ile <u>E</u> dit	ppellu101b.pcap <u>V</u> iew <u>G</u> o <u>C</u> a	ong apture <u>A</u> nalyze <u>S</u> tati	• istics Telephon <u>y W</u> ire	eless <u>T</u> ools <u>H</u> e	lp	-	
▲ http-cha File Edit ▲ ■ ▲ 0	ppellu101b.pcap	ong apture <u>A</u> nalyze <u>S</u> tati ✿ █ੇ ♥ ↔ ↔	istics Telephony <u>W</u> ire	eless <u>T</u> ools <u>H</u> e Q Q III	lp	-	
<pre>▲ http-cha File Edit ▲ ■ Ø 0 </pre>	ppellu101b.pcap	ong apture <u>A</u> nalyze <u>S</u> tati	istics Telephony <u>W</u> in	eless <u>T</u> ools <u>H</u> el Q Q III	lp X	Expression	
http-cha <u>File</u> <u>E</u> dit <u>M</u> <u>M</u> <u>M</u> <u>M</u> <u>M</u> No.	ppellu101b.pcap	ong apture <u>A</u> nalyze <u>S</u> tati	istics Telephony <u>W</u> ire	eless <u>T</u> ools <u>H</u> el Q Q III Protocol	lp Info	Expression	+ GETIPO
http-cha <u>File E</u> dit <u>Mile Mitp.reque</u> No. 21	ppellu101b.pcap	ong apture <u>A</u> nalyze <u>S</u> tati	istics Telephony Wire Image: Stress Stress Image: Stress Destination 0 69.59.180.	eless <u>T</u> ools <u>H</u> el Q Q II Protocol 202 HTTP	Info GET /pdf2htm	Expression	+ GET PC
http-cha <u>File</u> <u>E</u> dit <u>Mine</u> <u>Mo</u> <u>21</u> <u>29</u>	ppellu101b.pcap	ong apture <u>A</u> nalyze <u>S</u> tati	v istics Telephony <u>Win</u>	eless Tools He Q Q I Protocol 202 HTTP 202 HTTP	Info GET /pdf2htm GET /pdf2htm	Expression 1/view_onl 1/top.php	+ GET PC Line.p HTTP/

Quick Reference Coloring Rules Interface

ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> aptur	re <u>A</u> nalyze <u>S</u> tatistics Telephole <u>W</u> ireless <u>T</u> ools <u>H</u> elp	
Apply a display-filter << Ctrl-/>	Expression Later GET POST CONVECT HEAD HTTP4xx HTTP5x	ᢁ᠆ᢆᡰᡃᠧᢪ
Wireshark · Co' Rules · w	vireshark101	? >
Name 🔰	Filter	
🗹 Delays	frame.time_delta > 1 tcp.time_delta > 1	
HSRP State Change	hsrp.state != 8 && hsrp.state != 16	
✓ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update	
🗹 Spanning Tree Topology Cha	nange_stp.type == 0x80	
OSPF State Change	ospf.msg != 1	
ICMP errors	icmp.type eq 3 icmp.type eq 4 icmp.type eq 5 icmp.type eq 11 icmpv6.type eq 1 icmpv6.type eq	2 icm
ARP ARP	arp	
	icmp icmpvб	
TCP RST	tcp.flags.reset eq 1	
SCTP ABORT	sctp.chunk_type eq ABORT	
TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.25	1 && ip
	eth.fcs_bad==11Lip.checksum_bad==11Ltcp.checksum_bad==11Ludp.checksum_bad==11Lsctp.check	sum ba
Checksum Errors		>
✓ Checksum Errors <		
Checksum Errors	are processed in order until a match is found.	

(c) Wireshark University

8

Identify Applied Coloring Rules

	sec	-nessus.pcapr	ıg									_		×
Ei	le <u>E</u>	dit <u>V</u> iew	<u>G</u> o <u>C</u> apt	ure <u>A</u> nalyze	<u>S</u> tatisti	cs Telepho	n <u>y W</u> ireles	is <u>T</u> ools <u>I</u>	<u>H</u> elp					
		0	na 🔀	ै 🔍 🗢 🖻	> 🗟 {	F 🕹 📃	. 🗐 🗐	९ 🎹						
	Appl	y a display filte	′ <ctrl-></ctrl->				Expr	ession +	GET POST	CONNECT	HEAD HTT	P4xx HT	TP5xx	HTTP3xx
No	. ^	Time	Sour	ce		Destination		Protocol	Info					^
	▶ 1	0.000	000 19	2.168.1.	141	192.168	3.1.123	ICMP	Echo	(ping)	reques	t id	l=0xd	b2
-	- 2	0.000	034 19	2.168.1.	123	192.168	3.1.141	ICMP	Echo	(ping)	reply	id	l=0xd	b2
	3	0.007	928 19	2.168.1.	141	192.168	3.1.123	ICMP	Echo	(ping)	reques	t id	l=0xd	b2 🔍
>	Pa	cket cor	ments							· · ·				^
~	Fra	ame 1: 9	8 byt	es on wir	re (7	/84 bit	s), 98	bytes c	apture	ed (784	bits)	on ir	nterf	ac
		Interfa	e id:	0 (unkno	own)									
		Encapsul	lation	type: Ef	therr	net (1)								
		Arrival	Time:	Jan 10,	2006	6 09:56	:33.941	505000	Pacifi	ic Stan	dard Ti	me		
		[Time sł	nift fo	or this p	packe	et: 0.0	000000	0 secon	ds]					
		Epoch Ti	ime: 1:	136915793	3.941	505000	second	s						
		[Time de	elta fi	rom previ	ious	capture	ed fram	e: 0.00	000000	00 seco	nds]			
		[Time de	elta fi	rom previ	ious	display	yed fra	me: 0.0	000000	000 sec	onds]			
		[Time si	ince re	eference	or f	irst f	rame: 0	.000000	000 se	econds]				
	I	Frame Nu	umber:	1										
		Frame Le	ength:	98 bytes	s (78	4 bits)							
	(Capture	Lengt	h: 98 byt	tes (784 bi	ts)							
		[Frame i	is marl	ked: Fals	se]									
		- [Frame i	is igno	ored: Fal	Lse]									
		- Protoco	ols in	frame: e	eth:e	therty	pe:ip:i	cmp:dat	a]					
	Г		ng Rul	e Name:]	[CMP]				-					
		- [Colorin	ng Rul	e String:	: icn	np i	cmp∨6]							~
	2	sec-nessus					Packets: 2	021 · Displave	d: 2021 (10	0.0%) · Load	time: 0:0.620	Profile	: wiresha	ark101

Build a Coloring Rule to Highlight Delays

frame.time_delta > 1 || tcp.time_delta > 1



Master the Intelligent Scrollbar

	ftp-bou	nce.pcapng				- D >	<
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew <u>G</u> o <u>C</u>	apture <u>A</u> nalyze <u>S</u> ta	atistics Telephon <u>y W</u> ire	eless <u>T</u> ool	ls <u>H</u> elp	
		🖲 📙 🛅 🔰	रे 🖸 । ९ 👄 🖻	i 🕆 🕹 🥃 🔳 Q	ର୍ ବ୍ 🏢		
A	pply a di	isplay filter <ctr< td=""><td>r -/></td><td></td><td>Expression</td><td>. + GET POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3</td><td>bxx</td></ctr<>	r -/>		Expression	. + GET POST CONNECT HEAD HTTP4xx HTTP5xx HTTP3	bxx
No.		Time	Source	Destination	Protocol	Info	^
	30	0.201725	5 204.181.64.	2 24.6.103.134	ТСР	64712 → 21 [ACK] Seq=63 Ack=322	
	31	7.209497	7 204.181.64.	2 24.6.103.134	FTP	Request: TYPE I	
	32	0.040956	6 24.6.103.13	4 204.181.64.2	FTP	Response: 200 Type secto I.	
	33	0.097859	9 204.181.64.	2 24.6.103.134	FTP	Requests DACK	
	34	0.126899	9 24.6.103.13	4 204.181.64.2	FTP	Recommand custom coloring rule	
	35	0.090889	9 204.181.64.	2 24.6.103.134	ТСР	64 5	
	36	0.00016	5 24.6.103.13	4 204.181.64.2	ТСР	1303 → 64444 [SYN, ACK] Q Ac	Η.
	37	0.089448	8 204.181.64.	2 24.6.103.134	ТСР	64444 → 1303 [ACK] Seq=1 Ack	
	38	0.001690	0 204.181.64.	2 24.6.103.134	FTP	Request: STOR in design template	•
	39	0.133418	8 24.6.103.13	4 204.181.64.2	ТСР	21 Red stripes are TCP Resets -	
	40	0.002159	9 24.6.103.13	4 204.181.64.2	FTP	Re a default coloring rule	
	41	0.057583	3 24.6.103.13	4 204.181.64.2	TCP	1303 → 44 [FIN, Acm, 7 Acm.	
	42	0.000090	0 24.6.103.13	4 204.181.64.2	FTP	Respon . 425 Error: Possible bo	Η.
	43	0.051747	7 204.181.64.	2 24.6.103.134	FTP	FTP Data: 512 bytes	F
ł	44	0.000074	4 24.6.103. <u>1</u> 3	4 204.181.64.2	ТСР	1303 → 64444 [RST] Seq=2 Win=0 L	
ł	45	0.002597	7 204.181.64.	2 24.6.103.134	FTP	FTP Data: 512 bytes	~
0	7				Packets: 5	53 · Displayed: 53 (100.0%) · Load time: 0:0.5 Profile: wireshark101	

Export Packets that Interest You



p browse101.pcapng

Export Packet Details

	http-br	owse10)1.pcap	ng										_		×
<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	<u>S</u> ta	tistics	Telephony	<u>W</u> irel	ess <u>T</u>	ools <u>H</u> e	elp				
	Open				Ctrl+O		<u>۲</u>	& ☴ ☴	⊕ €	Q @						
	Open l	Recent				+	- E	Expression	+ GE	T POST	CONNE	CT HEAD	HTTP4xx	HTTP	'5xx HT	TP3xx
	<u>M</u> erge						т	CP Delta		Sour	rce		Destination	ı		Pro ^
	<u>I</u> mpor	from	Hex Du	mp						24	.6.17	3.220	75.75	.75.	75	DN
	Close				Ctrl+W						75 7	5.75	24.6.	173.	220	DN
	<u>S</u> ave				Ctrl+S				A	l col	umn da	ata will	be expo	orted		DN
	Save <u>A</u>	s			Ctrl+Shift+	s				- ado	d colun	nns as	desired	to		DN
	File Se	t				•				expo	rt addi	tional i	nformat	ion	0	DN
	- .					_	0	.000000	000	24	.6.17	3.220	174.1	37.4	12.75	ТС
	Export	Specifi	Direct	Kets						75	.75.7	5.75	24.6.	173.	220	DN
	Export	Packet	Dissec	tions	Ctrl+H	- I	A	s Plain <u>T</u> ext		17	4.137	.42	24.6.	173.	220	ТС
	Export	PDUs t	to File.		Cultur		A	s CSV		24	.6.17	3.220	174.1	37.4	12.75	тс
	Export	SSL Se	ssion K	evs			A	s C Arrays		24	.6.17	3.220	174.1	37.4	12.75	H1
	Export	Object	ts	-,		•	A	s PSML XML		17	4.137	.42	24.6.	173.	220	т
		-			C1 1 D	Ξ.	A	s PDML XML	·	17	4.137	.42	24.6.	173.	220	н
	Print				Ctrl+P		0	.001870	000	17	4.137	.42	24.6.	173.	220	т
	Quit				Ctrl+Q		0	.000662	000	24	.6.17	3.220	174.1	37.4	12.75	тс
	15	0.	0214	.04	1514	L	0	.021404	000	17	4.137	.42	24.6.	173.	220	Т
<		^		~ *			^					40		170	222	<u>-</u>
0	7						Pack	ets: 2011 · Dis	olayed: 2	2011 (10	00.0%) · I	Load time:	0:0.34 P	rofile: v	wireshark	101

Section 5 Skills

Build and Interpret Charts and Graphs

IO Graph Interface



tp-espn101.pcapng

 \Box

Х

Find Out Who's Talking to Whom

Wireshark · Conversations · http-espn101

Ethernet 1	IPv4 · 37	IPv6	TCP • 63	UDP · 82					
Address A	Address B	Packets	Bytes	Packets $A \rightarrow B$	Bytes A \rightarrow B	$Packets\;B\toA$	Bytes B → A	Rel Start	^
24.6.173.220	184.84.222.88	1,855	2020 k	533	30 k	1322	1989 k	9.726479000	
24.6.173.220	184.84.222.48	720	649 k	265	43 k	455	605 k	0.322923000	
24.6.173.220	184.84.222.120	613	628 k	195	14 k	418	614 k	6.716176000	
24.6.173.220	184.84.222.10	371	382 k	119	7502	252	374 k	7.950911000	
24.6.173.220	184.84.222.152	303	286 k	110	25 k	193	261 k	3.261301000	
24.6.173.220	68.71.216.176	127	134 k	38	7147	89	127 k	0.168701000	
24.6.173.220	74.125.224.59	142	115 k	51	9643	91	105 k	2.843065000	
24.6.173.220	184.84.222.16	41	36 k	15	1768	26	35 k	7.951909000	
24.6.173.220	184.84.222.75	36	33 k	12	1602	24	32 k	5.377013000	
24.6.173.220	138.108.7.20	31	24 k	11	1675	20	23 k	5.436636000	
24.6.173.220	68.71.216.171	29	24 k	12	1007	17	23 k	5.192672000	
24.6.173.220	75.75.75.75	180	22 k	90	6973	90	15 k	0.000000000	
24.6.173.220	68.71.216.157	132	20 k	66	3672	66	16 k	21.802866000	
24.6.173.220	184.84.222.137	30	19 k	14	1638	16	17 k	3.270647000	×
<								>	
Name resolu	ution] Limit to di	isplay filte	er			Cor	nversation Type	s
				Сору 🔻	Follow Stream	Graph	Close	Help	

Locate the Top Talkers

🧲 Wireshark · Conversa	tions · http-misc	traffic1	01				_		×
Ethernet · 1 IPv4 · 2	2 IPv6 TC	P·7	UDP						
Address A Port A A	ddress B P	ort B P	ackets	Bytes	Packets A → B	Bytes A → B	Packets B	→A	Bytes B
24.6.181.160 1266 10	07.6.133.250	80	475	533 k	126	8261		349	
24.6.181.160 1260 20	8.118.237.137	80	127	122 k	37	3086		90	
24.6.181.160 1264 20	8.118.237.137	80	40	36 k	14	1705		26	
24.6.181.160 1261 20	8.118.237.137	80	10	2141	5	1174		5	
24.6.181.160 1263 20	8.118.237.137	80	10	2012	5	1175		5	
24.6.181.160 1262 20	8.118.237.137	80	10	2011	5	1174		5	
24.6.181.160 1265 20	8.118.237.137	80	10	1821	5	1169		5	
									-
Name resolution	Limit to dis	play filte	r				Convers	sation	Types
		Cop	ру 🔻	Follow	Stream Gr	aph	Close	ł	Help

List Active Applications

1

4

4

22

6

1.4

4.8

5.6

17.3

8.4

1514

5176

6056

9084

18626

Wireshark · Protocol Hierarchy Statistics · http-browse101b Protocol Percent Packets Packets Percent Bytes Bytes Bits/s End Packets Frame 100.0 100.0 107708 108 k 0 195 Ethernet 100.0 195 100.0 107708 108 k 0 Internet Protocol Version 6 8.2 16 1.9 2062 2074 0 User Datagram Protocol 8.2 16 1.9 2062 2074 0 Domain Name System 8.2 16 1.9 2062 2074 16 Internet Protocol Version 4 91.8 179 98.1 105646 106 k 0 Transmission Control Protocol 179 91.8 98.1 105646 106 k 114 Hypertext Transfer Protocol 33.3 65 42.7 45965 46 k 0.5 Portable Network Graphics 1 1.1 1229 1236 1

0.5

2.1

2.1

11.3

3.1

No display filter.

Media Type

Compuserve GIF

Line-based text data

JPEG File Interchange Format

Unreassembled Fragmented Packet

Close

33

1

4

4

16

6

1523

5207

6092

18 k

9139

Help

End Bytes End Bits/s

0

0

0

0

0

2074

60 k

13 k

1236

1523

5207

6092

9599

9139

0

0

0

0

0

2062

59681

13364

1229

1514

5176

6056

9542

9084

Copy

 \times

Graph Application and Host Bandwidth Usage



Identify TCP Errors on the Network

> Differentiated Services Field: 0x00 (DSCP: CS0, EC Total Length: 58 Identification: 0x622a (25130)

> Flags: 0x00

Packets: 4900 · Displayed: 4900 (100.0%) · Load time: 0:0.119

everity	Group Pre	
Warn	Sequence	
Warn		
Note		1S 1S
Chat	Sequence Sequence	
Chat	Sequence	
to be the second	going to	D
Limit to Display Filter Search:	change	· · · · · · · · · · · · · · · · · · ·
By default Wireshark di severity - in this cas	plays all five levels of there are no Error ems to show	

Understand what the Expert Infos Errors Mean

- Packet Loss, Recovery, and Faulty Trace Files
- Asynchronous or Multiple Path Indications
- Keep-Alive Indication
- Receive Buffer Congestion Indications
- TCP Connection Port Reuse Indication
- Possible Router Problem Indication
- Misconfiguration or ARP Poisoning Indication

Graph Various Network Errors



File and Object Reassembly Options

	http-disney101.pcapng						- 0	×
<u>F</u> ile	<u>E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> aptu	re <u>A</u> nalyze <u>S</u>	tatistics Telephony	<u>W</u> ireless <u>T</u> o	ols <u>H</u> elp			
	Open	Ctrl+O	🛯 🐨 🕹 📃 📃	Θ Θ Θ				
	Open Recent	•		Expression	+ GET POST CONNECT	T HEAD HTTP4x	x HTTP5xx	HTTP3xx
	<u>M</u> erge		Destination	Protocol In	fo			^
	Import from Hex Dump		208.111.1	TCP	abt aliak [ACK]	Seq=1 Ack	=1 Win=	:65
	Close	Ctrl+W	208.111.1	HTZ	gill-click sets/3	14da08c2c	ç0c65e4	17e
	Save	Ctrl+S	24.6.173	ТСР	Mark/Unmark Packet	Ctrl+M	Ack=1	L W
	Save <u>A</u> s	Ctrl+Shift+S	24.6.173	ТСР	Ignore/Unignore Packet	Ctrl+D	Ack=1	W
	File Set	•	24.6.173	ТСР	Set/Unset Time Reference	Ctrl+T	Ack=1	L W
	The Sec		208.111.1	ТСР	Time Shift	Ctrl+Shift+T	1 Win=	:65
	Export Specified Packets		208.111.1	ТСР	Packet Comment		1 Win=	:65
	Export Packet Dissections	•	208.111.1	ТСР	Edit Resolved Name		:1 Win=	-65
	Export Packet <u>B</u> ytes	Ctrl+H	208.111.1	HTTP	Apply as Filter	•	3a7912	86
	Export PDUs to File		208 111 1	HTTD	Prepare a Filter	•	ed/1310	30 4
	Export SSL Session Keys			74 b	Conversation Filter	•	interf	ac ^
	Export Objects	,	<u>D</u> ICOM	d4:85	Colorize Conversation	•	1:bb:c	1
	<u>P</u> rint	Ctrl+P		6.173	SCTP	0		
	Quit	Ctrl+Q		0.173	Follow	C	TCP S	tream
-	0101 = He	ader Leng	th: 20 bytes		Conv	ß	UDP S	tream
	Differentiated	Services	Field: 0v00		сору		SSL St	ream
	Total Longth	60	, 11210. 0X00		Protocol Preferences	(4)		
	Tdentifientien	00	(27006)		Decode <u>A</u> s			
	Identification	: 0x69/e	(27006)		Show Packet in New Window	1		
	> Fiags: 0X00							~
\bigcirc	2	Packets: 6143 ·	Displayed: 6143 (100.0%) · Load time: 0	:0.124		Profile: wires	hark101

Reassemble Web Brow Sing Sessions

Wireshark · Follow TCP Stream (tcp.stream eq 0) · http-browse101 × GET / HTTP/1.1 Host: www.wireshark.org User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv: 16.0) Gecko/20100101 Firefox/16.0 Accept: text/html,application/xhtml+xml,application/ xml;q=0.9,*/*;q=0.8 Accept-Language: en-US, en; q=0.5 Accept-Encoding: gzip, deflate Connection: keep-alive HTTP/1.1 200 OK Server: Apache/2 Vary: Accept-Encoding X-Slogan: If it can shock or blind you it's layer 1. Cache-Control: no-cache Content-Type: text/html Date: Sat, 20 Oct 2012 23:37:20 GMT Keep-Alive: timeout=5, max=67 Transfer-Encoding: chunked ETag: "240b17-40ad-4cb18943247f3" Packet 10, 1 client pkt(s), 9 server pkt(s), 1 turn. Click to select. Stream 0 🖨 Entire conversation (13 kB) Show data as ASCII Find: Find Next Print Close Hide this stream Save as... Help

Reassemble a File Transferred Via FTP

	(ftp-dov	wnload101.pcap	ng							— [×
Fi	e Edit	View Go	Capture Analyze Statis	tics Telephony Wireless	s Tools H	elp						
		O	🔀 🖸 🍳 🗢 🖻 🗟	🗿 🕹 📃 🔳 🍳 Q	Q. 🎹							
	Apply a o	display filter <c< th=""><th>Ctrl-/></th><th>Expr</th><th>ression +</th><th>GET POS</th><th>T CONNEC</th><th>T HEAD</th><th>HTTP4xx</th><th>HTTP5x</th><th>х НТТРЗ</th><th>3xx</th></c<>	Ctrl-/>	Expr	ression +	GET POS	T CONNEC	T HEAD	HTTP4xx	HTTP5x	х НТТРЗ	3xx
No		Time	Source	Destination	Protocol	Info						^
	79	0.000944	24.6.173.220	131.246.123.4	FTP	Re	quest:	RETR	/pub/	/wires	shar	
	80	0.210322	131.246.123.4	24.6.173.220	ETD		sponse	: 150	Open:	ing Bl	INAR	
	81	0.026085	131.246.123.4	24.6.173.220	right-c	IICK r	P Data	• 1460	hvte	es		
	82	0.000984	131.246.123.4	24.6.173.220	Mark/U	nmark Pac	:ket	Ctrl+M	- te	es		
	83	0.000004	131.246.123.4	24.6.173.220	Ignore/	Jnignore I	Packet	Ctrl+D	t e	es		
	84	0.000173	24.6.173.220	131.246.123.4	Set/Uns	et Time Ke	erence	Ctrl+Shi	н.т 🤇] Seq:	=1 A	
	85	0.167047	24.6.173.220	131.246.123.4	Packet (Comment.		Curtoni	50	eq=420	0 Ac	
	86	0.044281	131.246.123.4	24.6.173.220	Tucket	20mmenta	•		t«	es		
	87	0.000981	131.246.123.4	24.6.173.220	Edit Res	olved Nan	ne		t•	es		
ш	88	<u>a aaaaa</u> o	131 2/6 123 /	24 6 173 220	Apply a	s Filter			- • •	ac		×
>	Fram	e 81: 151	l4 bytes on wir	e (12112 bits)	Prepare	a Filter			- •	bits)	on i	
>	Ethe	rnet II,	Src: Cadant_31	:bb:c1 (00:01:	Convers	ation Filte	r		∣ h a	7:bf:	a3 (d	I
>	Inte	rnet Prot	tocol Version 4	, Src: 131.246	Colorize	Conversa	tion					
>	Tran	smission	Control Protoc	ol, Src Port:	SCTP				6	6 (64	666)	
	FTP	Data (146	50 bytes data)		Follow				• (TCP S	tream	
					Сору				•	UDP S	tream	
					Protoco	l Preferen	ces		• E	SSL St	ream	
					Decode	As						
					Show Pa	acket in N	ew Window					

(c) Wireshar

Export HTTP Objects Transferred in a Web Browsing Session

Enable Allow subdissector to reassemble TCP stream (TCP preference).

× Wireshark · Export · HTTP object list Packet Hostname Content Type Filename Size 9 text/html 227 bytes \ www.espn.com 107 a.espncdn.com application/x-javascript 26 kB mbox.js 128 text/html 266 kB \ espn.go.com 132 a.espncdn.com 74 kB c?css=espn.teams.r4j.css text/css 178 a.espncdn.com 309 kB btn-toggle-tablet.css text/css text/xml 329 bytes brief?url=http:%2F%2Fespn.go.com%2F&shz=1&guid=%7 180 ratings-wrs.symantec.com 291 a.espncdn.com application/x-javascript 431 kB espn.insider.201112021227.js,espn.espn360.stub.r9.js,espn.n 320 491 bytes bg frontpage red.jpg a1.espncdn.com image/jpeg 325 92 bytes standard?mboxHost=espn.go.com&mboxSession=1325973 espndotcom.tt.omtrdc.net 339 a.espncdn.com 245 bytes social_facebook_14.png image/png 340 87 bytes_user?callback=jQuery171044244468988128804_13259732489. broadband.espn.go.com text/html 350 a1.espncdn.com image/png 114 bytes trans_border.png 351 a1.espncdn.com 16 kB bg_frontpage_elements.jpg image/jpeg 366 a1.espncdn.com image/png 10 kB header_sprite_fp.v3.png < > Help

Save All

Save

Close

Quick Reference

File and Packet Annotation Options



Add Your Comments to Trace Files

Only .pcapng file format supports comments.

(c) Wire

Details	pture File Properties · htt	p-winpcap101		_		×
File: "D:\000-Boo	k Projects - All\000	Wireshark 101 Bool	k\All	ok\All traces and sup	plements -	^
Length:	166 kB					
Format:	Microsoft NetMon 2.x					
First packet:	2012-10-25 21:46:46					
Elapsed:	00:00:05					
Capture file commer	nts					•
From Laura: Tyler complained at suspicious servers. p.s. Brenda mentio	bout this web browsing ses Look through this file and med similar web browsing is	sion. I didn't see the pa let me know what you t ssues as well.	acket loss, but : think.	I did see some conne	ctions to	

Add Comments to Individual Packets

📕 http-	cheez101.pcapng							_	- 🗆	\times
<u>F</u> ile <u>E</u> d	it <u>V</u> iew <u>G</u> o <u>C</u> ap	ture <u>A</u> nalyze <u>S</u> tatistics	Telephon <u>y</u> <u>W</u> ir	eless <u>T</u> ools	<u>H</u> elp					
🦲 🔳 🖉	1 💿 📙 🛅 🗙	🗳 । ९ 🗢 🗢 🗟 👔	<u>&</u> ⊒ ⊇ Q	ର୍ ବ୍ 🏢						
Apply a	a display filter <ctrl- <="" th=""><th>></th><th></th><th>Expression</th><th>+ GET POST</th><th>CONNEC</th><th>T HEAD</th><th>HTTP4xx</th><th>HTTP5xx</th><th>HTTP3xx</th></ctrl->	>		Expression	+ GET POST	CONNEC	T HEAD	HTTP4xx	HTTP5xx	HTTP3xx
No.	Time	Source	Destination	Protocol	Info					-
6	0.092074	208.43.72.115	24.6.173.2	20 TCP	80 → 6	413 [S	YN, A	ACK] Se	eq=0 /	Ack
7	0.000279	24.6.173.220	208.43.72.	115 TCP	6412		ск] з	Seq=1 4	Ack=1	Wi
8	0.001194	24.6.173.220	208.43.72.	115 HTTP,	ngn	-CIICK	.1			
9	0.092492	208.43.72.115	24.6.173.2	20 TCP	Mar Mar	k/Unmark F	acket	Ctrl+	М	5 、
× Pac	ket comments	1			lgno	re/Unignor	e Packet	Ctrl+	D	1
~ T	his nacket s	, shows the first	GET reque	st to th	e -	Unset Time	Reference	e Ctrl+	T CLIOL T	
	[Expert Inf	Fo (Comment/Com	ment): This	s nacket	Im	e Shitt		Ctrl+	Shift+ I	.0
[This packet shows the first GET request to [Severity level: Comment] Apply as Filter										
> F				9 byt	es 🥄 📍	are a Filter			•	:e
 > Et From Laura: This packet shows the first GET request to the site. > In Tr Colorize Conversation SCTP 413 (64 										
D.	escinación r Stream index	ок са ог. оч с. р]	ncel Help		Cop Prot	y ocol Prefere	ences		•	
	TCP Segment	Len: 485]	**	·····l-	Dec Show	ode <u>A</u> s v Packet in	New <u>W</u> ir	ndow		
	Packets: 4438 · Displayed: 4438 (100.0%) · Load time: 0:0.123 Profile: wireshark101									

Export Packet Comments Tor a Report

	sec-sus	picious101.pcapng								_		×
E	e <u>E</u> dit	<u>View Go C</u> ap	ture <u>Analyze</u> Statistics	Telephony	<u>Wireless</u> <u>T</u> ools	Help						
4	1	🖲 📙 🛅 🗙	🖸 । ९. 👳 🕾 😨		ର୍ ପ୍ ଭ୍ 🎹							
6	pkt_comm	nent				• Expression	+ GET POST	CONNECT	HEAD H	rTTP4xx	HTTP5xx	HTTP3xx
No		Time	Source	Destination	Protocol	Comment						^
Г	- 1	0.000000	24.6.173.220	74.125.22	24.84 HTTP	This is	the ori	ginal	search	quer	y for	the
+	5	0.062672	74.125.224.84	24.6.173	.220 HTTP	In this	s respons	e, the	serve	r sen	ds nu	mero
	7	0.475050	24.6.173.220	74.125.22	24.84 HTTP	Now we	clicked	on the	image	load	the	expa
	12	0.043454	74.125.224.84	24.6.173	.220 HTTP	We get	the expa	nded i	mage t	hroug	h Goo	gle 🗸
<												>
~	Packe	et comments	5									^
L	~ Thi	is is the c	original search	query fo	or the "Pe	ter Lik	for sale	' image	es.			
L	~ [[Expert Inf	Fo (Comment/Com	ment): Th	nis is the	origina	1 search	query	for t	he "P	eter	Li
L		[This is	the original s	earch que	ry for th	e "Peter	Lik for	sale"	image	s.]		
L		[Severity	/ level: Commer	t]	-				-	-		
L	[Group: Comment]											
>	> Frame 1: 1097 bytes on wire (8776 bits), 1097 bytes captured (8776 bits) on interface 0											
>	> Ethernet II, Src: HewlettP a7:bf:a3 (d4:85:64:a7:bf:a3), Dst: Cadant 31:bb:c1 (00:01:5c											
>	> Internet Protocol Version 4, Src: 24.6.173.220, Dst: 74.125.224.84											
~	V Transmission Control Drotocol Src Dort: 50262 (50262) Det Dort: 90 (90) Sec. 1 Ack. V											
C	7					Packets: 12	72 · Displayed: 19	(11.0%) · L	oad time: 0:	0.6 Pro	file: wiresh	hark101

Quick Reference Ommand-Line Tools Key Options

EDITCAP

editcap -h	View Editcap parameters.
editcap -i 360 big.pcapng 360secs.pcapng	Split <i>big.pcapng</i> into separate 360secs*.pcapng files with up to 360 seconds of traffic in each file.
editcap -c 500 big.pcapng 500pkts.pcapng	Split <i>big.pcapng</i> into separate <i>500pkts*.pcapng</i> files with up to 500 packets in each file.

MERGECAP

mergecap -h	View Mergecap parameters.
mergecap -w merged.pcapng files*.pcapng	Merge <i>files*.pcapng</i> into a single file called <i>merged.pcapng</i> (merge based on packet timestamps).
mergecap -a -w ab.pcapng a.pcapng b.pcapng	Merge <i>a.pcapng</i> and <i>b.pcapng</i> into a single file called <i>ab.pcapng</i> (merge based on the order files are listed).

TSHARK

tshark -h	View Tshark parameters.
tshark -D	List the available capture interfaces that can be used with the –i parameter.
tshark -i2 -f "tcp" -w tcp.pcapng	Capture only TCP-based traffic on interface 2 and save it to tcp.pcapng.
tshark -i1 -Y "ip.addr==10.2.1.1"	Capture all traffic on interface 1, but only display traffic to or from 10.2.1.1.
tshark -r "myfile.pcapng" -Y "http.host contains ".ru"" -w myfile-ru.pcapng	Open a trace file called myfile.pcapng and apply a display filter for the value ".ru" in the HTTP host field – save the results to a file called myfile-ru.pcapng.

Split a Large Trace File into a File Set

 Use capinfos <filename> to obtain file information first.

Split based on packet count

 editcap -c 1000 a.pcapng a1000set.pcapng

Split based on time (seconds)

 editcap -i 360 b.pcapng b360set.pcapng

Merge Trace Files

List all Mergecap parameters •mergecap -h Use Wildcards when Merging •mergecap -w c.pcapng c30set*.*

Capture Traffic at Command Line

Tshark Examples

- •tshark -h
- •tshark -D
- •tshark -c 100 -w 100.pcapng

```
Command Prompt
                                                                      ×
         D:\Traces101>tshark -r http-espn101.pcapng -Y "dns.flags.response==1"
          -w dns-espn-responsesonly.pcapng
         D:\Traces101>dir dns-espn-responsesonly.pcapng
         Volume in drive D is MainDrive
         Volume Serial Number is 4EAF-C465
          Directory of D:\Traces101
         01/11/2016 04:06 PM
                               18,212 dns-espn-responsesonly.pcapng
                                      18,212 bytes
                       1 File(s)
                       0 Dir(s) 1,756,655,288,320 bytes free
         D:\Traces101>_
(c) Wireshark Universit
```

Use Capture Filters during Command-Line Capture

Use the –f parameter

(c) Wiresha

Command Pr	ompt	_		×	
D:\Traces101> File: port21. Packets captu Packets recei flushed:0/ps	dumpcap -i3 -f "tcp port 21" -w port21.pcap Capturing on 'Wi-Fi' pcapng wred: 164 .ved/dropped on interface 'Wi-Fi': 164/0 (pc ifdrop:0) (100.0%)	<mark>ng</mark> ap:0/du	ітрсар	:0/	
D:\Traces101>	<pre>© Command Prompt D:\Traces101>tshark -i3 -f "tcp port 21 an -w "myport21.pcapng" Capturing on 'Wi-Fi' 293</pre>	d host	_ 192.1	68.44	× .7"
k University	D:\Traces101>	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		~~~~	<u>~</u> _

Use Display Filters during Command-Line Capture

Consider a two-step process if you want to capture, apply a display filter, and save the trace file

Command Prompt		_		×		
D:\Traces101> <mark>tshark -i3 -f "tcp" -</mark> Capturing on 'Wi-Fi'	-w tcptraffic.pc	apng		^		
496	Command Prom	pt			- 🗆 X	
D:\Traces101>	D:\Traces101> <mark>ts</mark> -w tcpanalysisf	hark - lags.p	r "tc capng	ptraf	<pre>ffic.pcapng" -Y "tcp.analysis.flags"</pre>	î
	D:\Traces101> <mark>di</mark> Volume in driv Volume Serial I	<mark>r tcpa</mark> e D is Number	nalys Main is 4	<mark>isfla</mark> Drive EAF-C	<mark>ags.pcapng</mark> e C465	
	Directory of D	:\Trac	es101			
	01/11/2016 04:4	44 PM 1 File 0 Dir((s) s) 1	,756,	1,072 tcpanalysisflags.pcapng 1,072 bytes ,563,681,280 bytes free	
	D:\Traces101>	×	\sim	·······		

Use Tshark to Export Specific Field Values and Statistics from a Trace File

-T fields -e <field name>

C:1	Command Promp	t				_		×
								^
D:\	Traces101> <mark>tsh</mark>	ark -i3 -	-f "dst port	80 and ho	st 192.168.	44.7" -	T field	ds
-e	frame.number	-e ip.sro	c -e ip.dst -	e tcp.win	dow_size			
Сар	turing on 'Wi	-Fi'						
1	192.168.	44.7 6	58.71.212.186	63620				
2	192.168.	44.7 2	23.59.197.231	261				
3	192.168.	44.7 2	23.216.11.9	251				
4	192.168.	44.7 2	23.216.11.9	256				
5	192.168.	44.7 6	58.71.222.248	63397				
6	192.168.	44.7 6	54.233.177.15	6 256				
7	192.168.	44.7 2	23.61.194.170	256				
8	192.168.	44.7 2	23.61.194.170	256				
9	192.168.	44.7 2	23.61.194.170	256				
10	192.168.	44.7 2	23.61.194.170	256				
11	192.168.	44.7 2	23.61.194.170	256				
12	192.168.	44.7 2	23.61.194.170	256				
13	192.168.	44.7 2	23.216.11.9	796				
14	192.168.	44.7 2	23.216.11.9	796				
15	192.168.	44.7 2	23.216.10.218	254				
16	192.168.	44.7 2	23.216.10.218	254				
17	192.168.	44.7 2	23.61.194.243	256				
28		44.7	3. 6.11-9	256	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~	<u> </u>	

Continue Learning about Wireshark and Network Analysis

- Visit *www.wiresharkbook.com* (other Wireshark books and links to related tools).
- Visit *www.wireshark.org* to sign up for the Wireshark-Announce mailing list (new Wireshark version information).
- Sign up for the newsletter at *www.chappellU.com* to participate in free online Wireshark events.
- Practice capturing your own traffic.
- Continue customizing Wireshark by adding new profiles and new display filters, coloring rules, and Filter Expression buttons.
- Share your customized settings with other IT team members to create a master profile that improves your team's network analysis efficiency.

Course Conclusion

Filtering Slides

IPv4/IPv6 Capture Filters

host 10.3.1.1	Capture traffic to/from 10.3.1.1
host 2406:da00:ff00::6b16:f02d	Capture traffic to/from the IPv6 address 2406:da00:ff00::6b16:f02d
not host 10.3.1.1	Capture all traffic except traffic to/from 10.3.1.1
src host 10.3.1.1	Capture traffic from 10.3.1.1
dst host 10.3.1.1	Capture traffic to 10.3.1.1
host 10.3.1.1 or host 10.3.1.2	Capture traffic to/from 10.3.1.1 and any host it is communicating with and traffic to/from 10.3.1.2 and any host it is communicating with
host www.espn.com	Capture traffic to/from any IP address that resolves to www.espn.com (this will only work if the host name can be resolved by Wireshark prior to capture)
Subnet Capture Filters

net	10.3.0.0/16	Capture traffic to/from any host on network 10.3.0.0
net	10.3.0.0 mask 255.255.0.0	Same result as previous filter
ip6	net 2406:da00:ff00::/64	Capture traffic to/from any host on network 2406:da00:ff00:0000 (IPv6)
not	dst net 10.3.0.0/16	Capture all traffic except traffic to an IP address starting with 10.3
dst	net 10.3.0.0/16	Capture traffic to any IP address starting with 10.3
src	net 10.3.0.0/16	Capture traffic from any IP address starting with 10.3
net	10.3.0.0/16	Capture traffic to/from any host on network 10.3.0.0

Broadcast and Multicast Capture Filters

ip broadcast	Capture traffic to 255.255.255.255
ip multicast	Capture traffic to 224.0.0.0 through 239.255.255.255 (also catches traffic to 255.255.255.255 unless you add and not ip broadcast)
dst host ff02::1	Capture traffic to the IPv6 multicast address for all hosts
dst host ff02::2	Capture traffic to the IPv6 multicast address for all routers

MAC Address Capture Filters

ether host 00:08:15:00:08:15	Capture traffic to or from 00:08:15:00:08:15
ether src 02:0A:42:23:41:AC	Capture traffic from 02:0A:42:23:41:AC
ether dst 02:0A:42:23:41:AC	Capture traffic to 02:0A:42:23:41:AC
not ether host 00:08:15:00:08:15	Capture traffic to or from any MAC address except for traffic to or from 00:08:15:00:08:15

Capture Traffic for a Specific Application

port 53	Capture UDP/TCP traffic to or from port 53 (typically DNS traffic)
not port 53	Capture all UDP/TCP traffic except traffic to or from port 53
port 80	Capture UDP/TCP traffic to or from port 80 (typically HTTP traffic)
udp port 67	Capture UDP traffic to or from port 67 (typically DHCP traffic)
tcp dst port 21	Capture TCP traffic to port 21 (typically the FTP command channel)
portrange 1-80	Capture UDP/TCP traffic to or from ports from 1 through 80
tcp portrange 1-80	Capture TCP traffic to or from ports from 1 through 80

Combine Port-Based Capture Filters

port 20 or port 21	Capture all UDP/TCP traffic to or from port 20 or port 21 (typically FTP data and command ports)
host 10.3.1.1 and port 80	Capture UDP/TCP traffic to or from port 80 that is being sent to or from 10.3.1.1
host 10.3.1.1 and not port 80	Capture UDP/TCP traffic to or from 10.3.1.1 except traffic to or from port 80
udp src port 68 and udp dst port 67	Capture all UDP traffic from port 68 to port 67 (typically traffic sent from a DHCP client to a DHCP server)
udp src port 67 and udp dst port 68	Capture all UDP traffic from port 67 to port 68 (typically traffic sent from a DHCP server to a DHCP client)
port 20 or port 21	Capture all UDP/TCP traffic to or from port 20 or port 21 (typically FTP data and command ports)
host 10.3.1.1 and port 80	Capture UDP/TCP traffic to or from port 80 that is being sent to or from 10.3.1.1

Capture Specific ICMP Traffic

icmp	Capture all ICMP packets.
icmp[0]=8	Capture all ICMP Type 8 (Echo Request) packets.
icmp[0]=17	Capture all ICMP Type 17 (Address Mask Request) packets.
icmp[0]=8 or icmp[0]=0	Capture all ICMP Type 8 (Echo Request) packets or ICMP Type 0 (Echo Reply) packets.
<pre>icmp[0]=3 and not icmp[1]=4</pre>	Capture all ICMP Type 3 (Destination Unreachable) packets except for ICMP Type 3/Code 4 (Fragmentation Needed and Don't Fragment was Set) packets.
icmp	Capture all ICMP packets.
icmp[0]=8	Capture all ICMP Type 8 (Echo Request) packets.

Apply Display Filters based on an IP Address, Range of Addresses, or Subnet

Address Filter Type	Filter Example
Single IPv4 Address	ip.addr==10.3.1.1
Single IPv6 Address	ipv6.addr==2406:da00:ff00::6b16:f02d
Host Name*	ip.host==www.wireshark.org
Range of Addresses	ip.addr > 10.3.0.1 && ip.addr < 10.3.0.5
Subnet (IPv4)	ip.addr==10.3.0.0/16
Subnet (IPv6)	ipv6.addr >= fe80:: && ipv6.addr < fec0::

* You must enable Wireshark's **Resolve network (IP) addresses** setting (**Edit | Preferences | Name Resolution**) in order to use this display filter.

(c) Wireshark University

Expand Display Filters with Multiple Include and Exclude Conditions (using Operators)

Operator	English	Example	Description
& &	and	ip.src==10.2.2.2 && tcp.port==80	View all IPv4 traffic from 10.2.2.2 that is to or from port 80
11	or	tcp.port==80 tcp.port==443	View all TCP traffic to or from ports 80 or 443
!	not	!arp	View all traffic except ARP traffic
!=	ne	tcp.flags.syn != 1	View TCP frames that do not have the TCP SYN flag (synchronize sequence numbers) set to 1

Why Didn't my Filter Work?

Incorrect	ip.addr != 10.2.2.2	Display packets that do not have 10.2.2.2 in the IP source address field <i>or</i> IP destination address field.
Correct	!ip.addr == 10.2.2.2	Display packets that do not have 10.2.2.2 in the IP source address field and also does not have 10.2.2.2 in the destination address field.
Incorrect	!tcp.flags.syn==1	Display all packets that do not have a TCP SYN bit set to 1 (regardless of whether they are a TCP packet or not)
Correct	<pre>tcp.flags.syn !=1</pre>	This filter will only display TCP packets that contain a SYN set to 0.

Use Parentheses to Change Filter Meaning





(c) Wireshark University

Determine Why Your Display Filter Area is Yellow

Yellow Background: This filter may not work as expected.

ip.addr != 10.2.2.2

Green Background: The syntax is correct, but it doesn't ensure the logic is correct.

arp && bootp && tcp

Red Background: This filter will not work – there is a syntax error.

ip.addr=10.2.2.2

Filter on a Keyword in a rrace File

Use contains for a general filter Use matches for a Regex filter



ftp.request.arg contains "anonymous"

(c) Wireshark University

Using matches for Regex Filters

Consider case sensitivity

ftp.request.arg matches "anonymous"

ftp.request.arg matches "(?i)anonymous"

Consider variable characters

- frame matches "building[Aa]eng"
- frame matches "building[AaBb]eng"

frame matches "(?i)(cat|dog)"

Use Wildcards in Display Filters



Challenge Slides

(c) Wireshark University

Section 0 Challenge

Open challenge101-0.pcapng and use the techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

We will focus on what you can learn about communications based on the main Wireshark view.

Question 0-1.	How many packets are in this trace file?
Question 0-2.	What IP hosts are making a TCP connection in frames 1, 2, and 3?
Question 0-3.	What HTTP command is sent in frame 4?
Question 0-4.	What is the length of the largest frame in this trace file?
Question 0-5.	What protocols are seen in the Protocol column?
Question 0-6.	What responses are sent by the HTTP server?
Question 0-7.	Is there any IPv6 traffic in this trace file?

Section 1 Challenge

Open challenge101-1.pcapng and use the techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

Important: This trace file includes an HTTP communication running over a non-standard port number. Before you can answer these questions, you must force Wireshark to dissect this traffic as HTTP.

Question 1-1. In which frame number does the client request the default web page ("/")?

Question 1-2. What response code does the server send in frame 17?

Question 1-3. What is the largest TCP delta value seen in this trace file?

Question 1-4. How many SYN packets arrived after at least a 1 second delay?

Section 2 Challenge

This challenge requires access to the Internet. You will capture traffic to a web site and analyze your findings. The answer key is located in Appendix A.

First, configure Wireshark to capture only traffic to and from your MAC address and port 80, and save the traffic to a file named **mybrowse.pcapng**. Then ping and browse to www.chappellU.com. Stop the capture and examine the trace file contents.

Question 2-1.Did you capture any ICMP traffic?Question 2-2.What protocols are listed for your browsing session towww.chappellU.com?

Now configure Wireshark to capture all your ICMP traffic, and save your traffic to a file called myicmp.pcapng. Again, ping and browse to www.chappellU.com. Stop the capture and examine the trace file contents.

- Question 2-3. How many ICMP packets did you capture?
- Question 2-4. What ICMP Type and Code numbers are listed in your trace file?

Section 3 Challenge

Open *challenge101-3.pcapng* and use your display filter and coloring rule skills to locate traffic based on addresses, protocols and keywords to answer these Challenge questions.

You will practice your display filter to locate traffic based on addresses, protocols, and keywords.

Question 3-1.	How many frames travel to or from 80.78.246.209?
Question 3-2.	How many DNS packets are in this trace file?
Question 3-3.	How many frames have the TCP SYN bit set to 1?
Question 3-4. lower case?	How many frames contain the string "set-cookie" in upper case or
Question 3-5.	How many frames contain a TCP delta time greater than 1 second?

Section 4 Challenge

Open *challenge101-4.pcapng* and use your packet coloring and export skills in this Section to answer these Challenge questions.

Question 4-1. What coloring rule does frame 170 match?

Question 4-2. Temporarily color TCP stream 5 with a light blue background and apply a filter on this traffic. How many packets match your filter?

Question 4-3. Create and apply a coloring rule for TCP delta delays greater than 100 seconds. How many frames match this coloring rule?

Question 4-4. Export this filtered TCP delta information in CSV format. Using a spreadsheet program, what is the average TCP delta time?

Section 5 Challenge

Open *challenge101-5.pcapng* and use the techniques covered in this Section to answer these Challenge questions.

Question 5-1. Create an IO Graph for this trace file. What is the highest packets-persecond value seen in this trace file?

Question 5-2. What is the highest bits-per-second value seen in this trace file?

Question 5-3. How many TCP conversations are in this trace file?

Question 5-4. How many times has "Previous segment not captured" been detected in this trace file?

Question 5-5. How many retransmissions and fast retransmissions are seen in this trace file?

Section 6 Challenge

Open *challenge101-6.pcapng* and use the techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

Question 6-1.	What two .jpg files can be exported from this trace file?
Question 6-2. reside?	On what HTTP server and in what directory does next-active.png
Question 6-3.	Export booksmall.png from this trace file. What is in the image?
Question 6-4. this stream?	Reassemble TCP stream 7. What type of browser is the client using in

Section 7 Challenge

Open *challenge101-7.pcapng* and use the techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

Question 7-1. V	What information is contained in the trace file annotation?
-----------------	---

Question 7-2. What packet comments are contained in this trace file?

7-3. Add a comment to the POST message in this trace file. What packet

Question 7-3. did you alter?

Section 8 Challenge

Use *challenge101-8.pcapng* and the command-line tool techniques covered in this Section to answer these Challenge questions. The answer key is located in Appendix A.

Question 8-1. What Tshark parameter should you use to list active interfaces on your Wireshark system?

Question 8-2. Using Tshark to extract protocol hierarchy information, how many UDP frames are in *challenge101-8.pcapng*?

Question 8-3. Use Tshark to export all DNS packets from *challenge101-8.pcapng* to a new trace file called *ch8dns.pcapng*. How many packets were exported?

Lab Slides

Starting at Lab 4

(c) Wireshark University

http-disney101.pcapng

Add the HTTP Host Field as a Column

During a browsing session, an HTTP client sends requests for HTTP objects to one or more HTTP servers. In each of the requests, the client specifies the name or the IP address of the target HTTP server. This can be very revealing.

Note: All frames from 24.6.173.220 will appear with a black background and red foreground if Wireshark is set to validate IP header checksums. You will disable this feature in Lab 6.

http-pcaprnet101.pcapng

Set Key Wireshark Preferences (IMPORTANT LAB)

Wireshark offers several key preference settings to enhance your analysis sessions. In this lab you will use the Edit Preferences button on the main toolbar and the right-click method to view and change the preference settings. These are the settings we will view and alter in this lab:

- Increase the number of display filters that Wireshark remembers.
- Increase the number of recently opened files that Wireshark remembers.
- Ensure IP, UDP, and TCP checksum validations are disabled.
- Enable the TCP *Calculate conversation timestamps* setting.
- Enable the TCP *Track number of bytes in flight* setting.
- Disable the TCP *Allow subdissector to reassemble* TCP streams setting.

Create a New Profile Based on the Default Profile

Profiles enable you to work with customized settings to be more efficient when analyzing traffic.

In this lab you will create a new profile called "wireshark101."

You will base it on your Default profile to ensure any previously created settings will be copied over to your new profile.

httpdnsprofile2.zip and dns-nmap101.pcapng

Import a DNS/HTTP Errors Profile

Once you've created that fabulous profile that detects various types of HTTP or DNS problems perhaps, consider installing that profile on your other Wireshark systems.

Since Wireshark bases profiles on text files, this is a simple process.

http-slow101.pcapng

Spot Path and Server Latency Problems

Let's practice using these two columns to detect latency.

- In this lab you will set the Time column to **Seconds Since Previous Displayed Packet** and add the **TCP Delta** column.
- You may have some of these columns set already if you followed along with the previous section in your Student Manual.

Capture to File Sets

In this lab you will get a chance to practice capturing to file sets using an auto-stop condition.

Use a Ring Buffer to Conserve Drive Space

In this lab exercise, we will set up a ring buffer to ensure we see the most recent traffic.

We will create a problem and manually stop the capture to analyze the issue.

Capture Only Traffic to or from Your IP Address

In this lab you will determine your current IP address and apply a capture filter for that traffic.

Capture Only Traffic to or from Everyone Else's MAC Address

In this lab you will determine your current MAC address and apply a capture filter that filters out your traffic—you are interested in everyone else's traffic only.

If you have a dual-stack host, it is much more effective to make a single filter based on your MAC address than to make a more complex filter based on your IPv4 and IPv6 addresses.

Create, Save and Apply a DNS Capture Filter

In this exercise you will use several skills learned in this Section. You will configure Wireshark to capture only DNS traffic and save that traffic to a file called **mydns101.pcapng**.

http-sfgate101.pcapng

Use Auto-Complete to Find Traffic to a Specific HTTP Server

In this lab we use Wireshark's auto-complete feature to filter on specific HTTP communications.

Ultimately, we are interested in client requests to a particular server. This trace file, *http-sfgate101.pcapng*, was captured as someone browsed a web site and then filled in a feedback form on that site asking about iPad support.
Use a Default Filter as a "Seed" for a New Filter

You can use the default display filters as a template to create and save new custom display filters.

This method helps you remember the display filter syntax and ensures that the syntax is correct. We will create a display filter for all traffic to or from your IP address.

http-disney101.pcapng

Filter on HTTP Traffic the Right Way

This is a quick lab.

We will just compare the results from applying two different display filters to the traffic.

We will use http and then we will replace it with the proper filter for this web browsing traffic.

mybackground101.pcapng

Filter on Traffic to or from Online Backup Subnets

In this lab, we will apply a subnet display filter to examine traffic to or from a backup server for Memeo which offers an online backup product. This traffic runs in the background, constantly checking in with the server.

http-errors101.pcapng

Filter on DNS Name Errors or HTTP 404 Responses

In this lab we will look for specific DNS or HTTP error responses using the right-click method.

This is a great filter that you may want to save.

gen-startupchatty101.pcapng

Detect Background File Transfers on Startup

There may be a number of background processes that run when you start up your machine.

- Some of these may update your virus detection mechanism, your operating system, or applications.
- In this lab, you will detect and filter on the most active conversation of a host that is just starting up.

general101b.pcapng

Locate TCP Connection Attempts to a Client

Client processes send TCP connection requests to server processes. There are very few reasons to allow incoming TCP connections to user machines on your network (as they typically won't be running server processes).

In this lab we will create a display filter that detects incoming TCP connection attempts to anyone on a particular subnet.

We will focus on subnet 24.6.0.0/16.

http-pictures101.pcapng

Filter to Locate a Set of Key Words in a Trace File

In this lab we will use the matches operator to find the keywords *sombrero* or *football* in upper case or lower case anywhere in a trace file.

http-pictures101.pcapng

Filter with Wildcards between Words

In this lab we will use the matches operator to find the keywords baby and smiling in a trace file. We will see how the repeating character option settings can affect what matches your filter.

Our display filter ftp.request.arg matches "me. {1,3}r" would look for the "." up to three times between the "me" and "r" as mentioned in this section.

This time we will look for the keywords *baby* and *smiling* with up to three characters separating the words.

dfilters_sample.txt

Import Display Filters into a Profile

In this lab you will import a set of display filters from your student USB stick (or the *wiresharkbook.com* website) into your existing display filter file (*dfilters*).

Use this same technique if you want to move display filters from one profile to another on a single host or other Wireshark systems.

http-chappellu101b.pcapng and *filterexpressions101.txt*

Create and Import HTTP Filter Expression Buttons

We will begin by creating a single Filter Expression button and then we'll import the set of Filter Expression buttons shown below into your *wireshark101* profile.

Wireshark · Preferences			?
 Appearance Layout Columns Font and Colors Capture Filter Expressions Name Resolution Protocols Statistics Advanced 	Enabled	Button Label GET POST CONNECT HEAD HTTP4xx HTTP5xx HTTP5xx	Filter Expression http.request.method matches "(GET POST)" http.request.uri contains "CONNECT" http.request.uri contains "HEAD" http.response.code > 399 && http.response.code < 500 http.response.code > 499 http.response.code > 299 && http.response.code < 400
4	+ -	P b	OK Cancel Help

http-sfgate101.pcapng

Add a Column to Display Coloring Rules in Use

Adding a column to identify coloring rules is a great idea when you are new to Wireshark or you just aren't familiar with the coloring rules set.

ftp-crack101.pcapng

Build a Coloring Rule to Highlight FTP User Names, Passwords, etc.

In this lab you will create a coloring rule to call your attention to FTP request arguments, including those associated with USER, PASS, TYPE, SIZE, MDTM, RETR, and CWD commands.

http-browse101d.pcapng

Create Temporary Conversation Coloring Rules

In this lab, you will apply three temporary coloring rules to differentiate TCP conversations. When you scroll through the trace file, you will be able to easily see when an earlier conversation begins to surface.

net-lost-route.pcapng

Create Temporary Conversation Coloring Rules

In this lab we will create a new coloring rule to identify TCP retransmissions. TCP retransmissions are a sign of packet loss on a network and are part of Wireshark's TCP analysis flagged packets. We'd like to just look at the Intelligent Scrollbar to know if retransmissions (packet loss indications) are seen.

http-misctraffic101.pcapng

Export a Single TCP Conversation

When you are focused on a specific application or a specific file download, it helps to extract conversations into separate trace files. In this lab, you will create and extract a new trace file after locating traffic from an executable file download process.

http-au101b.pcapng

Export a List of HTTP Host Field Values from a Trace File

In this lab, you will alter the Packet List pane to display the HTTP Host field before exporting information to CSV format.

http-misctraffic101.pcapng

Filter on the Most Active TCP Conversation

Pulling out the most active conversation is a common network analysis task when trace files contain tens or even hundreds of conversations.

http-browse101c.pcapng

Set up GeoIP to Map Targets Globally

Wireshark can use the MaxMind GeoLite database files to list the country, city, AS (Autonomous System) number, latitude, and longitude of an IP address and map IPv4 and IPv6 addresses on a map of the earth. In this lab, you will configure Wireshark to use this database and map IP addresses seen in a trace file.

general101c.pcapng

Detect Suspicious Protocols or Applications

When you are concerned that there may be a security issue in your trace file, open the Protocol Hierarchy window first.

Look for suspicious applications or protocols and the dreaded "data" under IP, UDP, or TCP.

http-espn101.pcapng

Compare Traffic to/from a Subnet to Other Traffic

In this lab you will compare all the traffic to or from subnet 184.0.0.0/8 to all other traffic. To do this, you will use two IP address filters—one inclusion filter and one exclusion filter.

http-download101.pcapng

Identify an Overloaded Client

In this lab we use the Expert Infos window to identify the cause of poor network performance. Not only is the client overloaded in this trace file, but there is packet loss along the path as well.

general101d.pcapng

Detect and Graph File Transfer Problems

In this lab we examine a file transfer process that takes place over TCP. Before we can consider troubleshooting the application itself, we must rule out TCP problems.

http-wiresharkdownload101.pcapng

Use Reassembly to Find a Web Site's Hidden HTTP Message

It is not unusual to have numerous "hidden" messages sent to your browser when you hit a web site. In this lab you will analyze a trace file that contains two hidden messages. Afterwards, visit the same web site again to catch other interesting messages.

ftp-clientside101.pcapng

Extract a File from an FTP File Transfer

In this lab you will follow an FTP data stream to reassemble the file that was transferred.

First you will reassemble the command channel traffic to see the client login and file retrieval commands, and then you will reassemble the data transfer channel traffic to view the file transferred.

http-college101.pcapng

Carve Out an HTTP Object from a Web Browsing Session

In this lab, you will open a trace file that contains a web browsing session.

Using the **File | Export Objects** process, you will extract one of the images transferred during the web browsing session.

sec-suspicous101.pcapng

Read Analysis Notes in a Malicious Redirection Trace File

It can be a blessing to have notes inside the trace file to assist other analysts (or even you) in following along with the traffic flow. In this lab you will examine the notes left in a trace file that contains

unusual communications.

sec-suspicous101.pcapng

Export Malicious Redirection Packet Comments

We will use the *sec-suspicious101.pcapng* trace file again in this lab. We will use a two-step process for comment export.

- First we will prepare the trace file to export the field information we are most interested in. We will export the fields in text format.
- Unlike in the previous section, we will export the packet comments using the Packet summary line.

http download101c.pcapng

Split a File and Work with Filtered File Sets

You will be working with *http-download101c.pcapng* in this lab. This trace file is only 27 MB, but we will use it to practice splitting a file.

After splitting the file, we will move through the file set while a display filter is applied.

Wireshark automatically applies the display filter to each file as it is opened.

http-downloadc5000*.pcapng

Merge a Set of Files using a Wildcard

In this lab you will merge the six-file *http-downloadc5000*.pcapng* set that you created in Lab 42.

You will use a wildcard to make this process a bit easier and less errorprone.

Use Tshark to Capture to File Sets with an Autostop Condition

In this lab, you will get a chance to use Tshark with various parameters. We'll define file set "next file" parameters and include an autostop condition for unattended capture.

http-espn101.pcapng

Use Tshark to Extract HTTP GET Requests

In this lab you will use the $-\mathbf{r}$ parameter to read a trace file and then apply a display filter with the $-\mathbf{R}$ parameter.

Finally you will save a trace file that contains only the HTTP GET requests.

Use Tshark to Extract HTTP Host Names and IP Addresses

In this lab we will use a combination of display filters and field names to create a file that contains both the IP addresses and host names of HTTP servers contacted on the network.