

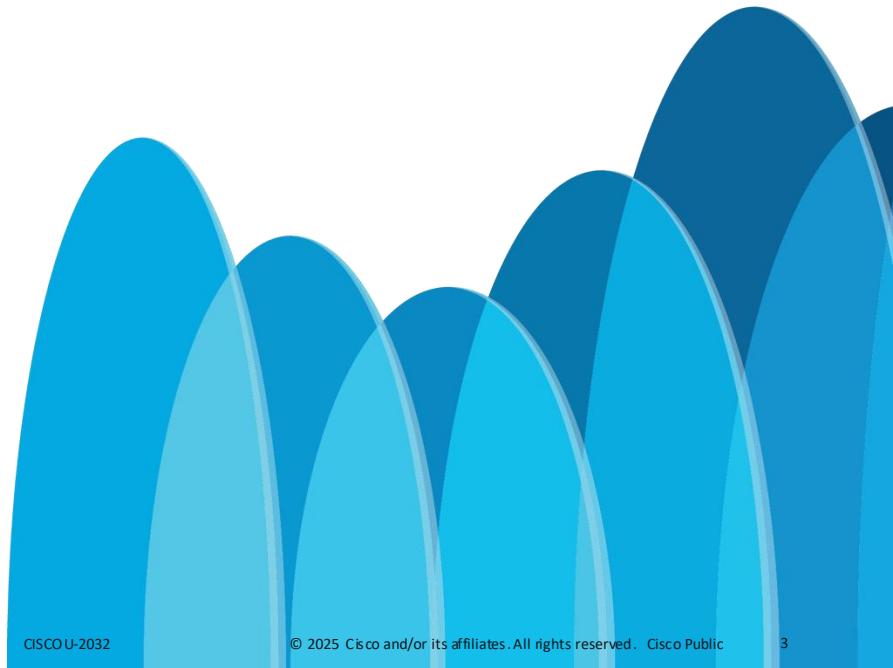


Become a network doctor using packet captures and Wireshark

Prapanch Ramamoorthy
Principal Engineer, CX Engineering
CISCOU-2032

Wireshark is a network engineer's best friend!

- An unknown network engineer





Agenda

- Introduction
- Getting familiar with the UI
- Summary and related metadata
- Troubleshooting using Wireshark
- Conclusion

Install Wireshark

<https://www.wireshark.org/download.html>



Getting familiar

The User Interface

Frame 1: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface en0, id 0
Ethernet II, Src: 82:52:cf:4bd:3:34 (82:52:cf:4b:0d:34), Dst: 76:1:a5:52:1b:8c:04 (76:1:a5:52:1b:8c:04)
Internet Protocol Version 4, Src: 52.223.1.163, Dst: 192.168.197.141
Transmission Control Protocol, Src Port: 443, Dst Port: 57839, Seq: 1049325313, Ack: 2279766114, Len: 481
Transport Layer Security

No.	Date	Time	Source	Destination	Protocol	Length	Info
1	2024-11-04	16:08:08.065519	52.223.1.163	192.168.197.141	TLSv1.2	547	Application Data
2	2024-11-04	16:08:08.065634	192.168.197.141	52.223.1.163	TCP	66	57839 → 443 [ACK] Seq=2279766114 Ack=1049325794 Win=2040 Len=0 TSval=4203520823 TSecr=
3	2024-11-04	16:08:08.101715	192.168.197.141	52.223.1.163	TLSv1.2	231	Application Data
4	2024-11-04	16:08:08.140164	52.223.1.163	192.168.197.141	TCP	66	443 → 57839 [ACK] Seq=1049325794 Ack=2279766279 Win=1954 Len=0 TSval=1577653841 TSecr=
5	2024-11-04	16:08:08.252105	99.83.250.143	192.168.197.141	TCP	66	443 → 58100 [ACK] Seq=1641673934 Ack=2893573071 Win=122 Len=0 TSval=3886905425 TSecr=
6	2024-11-04	16:08:08.351206	192.168.197.141	20.189.173.8	TLSv1.2	427	Application Data
7	2024-11-04	16:08:08.351295	192.168.197.141	20.189.173.8	TLSv1.2	1111	Application Data
8	2024-11-04	16:08:08.351356	192.168.197.141	20.189.173.8	TCP	1414	57772 → 443 [ACK] Seq=1071932827 Ack=269559361 Win=2048 Len=1348 TSval=2268877677 TSecr=
9	2024-11-04	16:08:08.351363	192.168.197.141	20.189.173.8	TLSv1.2	265	Application Data
10	2024-11-04	16:08:08.432327	192.168.1.163	192.168.197.141	TCP	1414	443 → 57839 [ACK] Seq=1049325794 Ack=2279766279 Win=1954 Len=1348 TSval=1577654247 TSecr=
11	2024-11-04	16:08:08.543245	52.223.1.163	192.168.197.141	TLSv1.2	1047	Application Data
12	2024-11-04	16:08:08.543248	52.223.1.163	192.168.197.141	TLSv1.2	104	Application Data
13	2024-11-04	16:08:08.543365	192.168.197.141	52.223.1.163	TCP	66	57839 → 443 [ACK] Seq=2279766279 Ack=1049328161 Win=2011 Len=0 TSval=4203521301 TSecr=
14	2024-11-04	16:08:08.631817	2620:1ec:8fa::10	2401:4900:9006:e92d:546:e6bf:94::	TCP	1414	443 → 58207 [ACK] Seq=853548177 Ack=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
15	2024-11-04	16:08:08.631853	2620:1ec:8fa::10	2401:4900:9006:e92d:546:e6bf:94::	TLSv1.2	306	Application Data
16	2024-11-04	16:08:08.631855	2620:1ec:8fa::10	2401:4900:9006:e92d:546:e6bf:94::	TLSv1.2	185	Application Data
17	2024-11-04	16:08:08.631147	2401:4900:9006:e92d:546:e6bf:94::	2620:1ec:8fa::10	TCP	74	58207 → 443 [ACK] Seq=3989515143 Ack=8535497980 Win=4070 Len=0
18	2024-11-04	16:08:08.631800	20.189.173.8	192.168.197.141	TCP	66	443 → 57772 [ACK] Seq=269559361 Ack=1071932827 Win=16386 Len=0 TSval=15830896 TSecr=
19	2024-11-04	16:08:08.634991	20.189.173.8	192.168.197.141	TCP	66	443 → 57772 [ACK] Seq=269559361 Ack=1071934374 Win=16386 Len=0 TSval=15830890 TSecr=
20	2024-11-04	16:08:08.647793	20.189.173.8	192.168.197.141	TLSv1.2	159	Application Data
21	2024-11-04	16:08:08.647885	192.168.197.141	20.189.173.8	TCP	66	57772 → 443 [ACK] Seq=1071934374 Ack=269559454 Win=2046 Len=0 TSval=226888063 TSecr=
22	2024-11-04	16:08:08.666859	2401:4900:9006:e92d:546:e6bf:94::	2620:1ec:8fa::10	TLSv1.2	113	Application Data
23	2024-11-04	16:08:08.670655	2401:4900:9006:e92d:546:e6bf:94::	2620:1ec:8fa::10	TLSv1.2	98	Application Data
24	2024-11-04	16:08:08.671791	2401:4900:9006:e92d:546:e6bf:94::	2620:1ec:8fa::10	TCP	74	58207 → 443 [FIN, ACK] Seq=3989515206 Ack=853549780 Win=4096 Len=0
25	2024-11-04	16:08:08.695972	2620:1ec:8fa::10	2401:4900:9006:e92d:546:e6bf:94::	TCP	74	443 → 58207 [ACK] Seq=853549780 Ack=3989515182 Win=16388 Len=0

Frame 1: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface en0, id 0
Ethernet II, Src: 82:52:cf:4bd:3:34 (82:52:cf:4b:0d:34), Dst: 76:1:a5:52:1b:8c:04 (76:1:a5:52:1b:8c:04)
Internet Protocol Version 4, Src: 52.223.1.163, Dst: 192.168.197.141
Transmission Control Protocol, Src Port: 443, Dst Port: 57839, Seq: 1049325313, Ack: 2279766114, Len: 481
Transport Layer Security

0000 76 15 8f 31 40 ff f6 36 3f d4 d1 01 c3 a0 8 ··R ··R ·K 4 ·E ·
0001 02 15 8f 31 40 ff f6 06 36 3f d4 d1 01 c3 a0 8 ·@ ··R ·674 ·
0002 c0 81 0b 01 bb ef 3e 8b 6f 01 87 e2 78 62 88 18 ·> o ·xb ·
0003 07 98 64 7d 00 00 01 01 08 0a 06 09 16 09 fa 8c ·} ··A ·
0004 a2 19 01 83 73 00 00 00 00 00 00 00 00 00 00 13 ·} ··S ·
0005 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·c t ·l #9 ·
0006 c5 09 1c fd 42 1b 2a 47 1c 64 66 24 c3 96 3a 63 ·t-B ·o g f\$ ·:c ·
0007 12 6a 2b 48 03 b3 6a 54 1d 3f 0c 20 29 b7 06 ·j+oB ·d J@T ·j ·
0008 42 bc 11 a5 0b c2 a5 83 3c 38 d4 b7 4a eb c3 fb B ·: ·< J ·
0009 2a 00 aa ab 01 b5 1e 79 8c 03 85 3f 10 e6 a5 35 * ···y ·7 ·- 5 ·
000a 41 90 81 83 73 2d cf 2c 64 81 4e d3 d8 81 2a A ·s ·- dN ·* ·
000b 68 b2 56 22 8d 5b 26 52 59 0e 8c b5 5a 4f 13 3c h "b Y ·Zo <
000c 13 56 1b 62 84 e4 99 8a 86 91 59 e8 1b 30 31 V b ·Y ·- Y<1 ·
000d c5 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·} ·g ·- 6 ·c ·
000e 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Zwl ·1 ·- J ·UA Z ·
000f 69 1c ca 88 5e 6b 69 0f fb da 04 93 82 99 87 97 ·} ·- ·
0010 74 93 25 8d 76 37 13 41 ef d3 63 a8 4c 01 41 1f t % v7 A ·c l ·A ·
0011 20 00 46 4f 36 fe ee da 4f dd 42 74 20 84 1 ·F06 ·-0Dr ·
0012 6e e1 92 13 16 83 a2 62 4e fb 2f 3a e9 27 2b 95 n ·- b N > ·+ ·
0013 b6 11 71 ac 0d dd b3 85 2e c0 01 cf c9 88 0b 9 ·q ·- ·
0014 e2 b7 33 04 8f ee 12 05 4f f3 a2 72 60 17 ce 3 ·- ·- ·0 ·r ·
0015 e9 53 b8 2c b3 11 ab 07 bd 0e 95 44 7f 9c d9 fb S ·- ·D ·! ·
0016 b7 1c 76 2b c8 96 51 99 45 0e 8c 5a 4f 13 3c h "v ·Q C8 b1 ·
0017 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ·} ·- ·
0018 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ^ ·- ·Kg ·0 ·
0019 82 c8 7a 14 3b 7d 88 76 15 ea e4 fa 54 06 c2 83 z ·- ·u T ·- ·
0019 82 c8 7a 14 3b 7d 88 76 15 ea e4 fa 54 06 c2 83 z ·- ·u T ·- ·
0019 86 69 0c 66 9b 1c 09 e0 08 1c f3 56 9e 10 cc i ·f ·- ·V ·
0019 0b d4 2b 43 6b 08 e3 07 80 63 6e f1 dc 08 30 +Ck ·- ·6 ·0 ·
0019 d4 c2 e8 bc cd 1e 2f ac 5d 62 52 ff 7a 55 9d ba ·- ·]br zu ·
0019 46 1e 95 1c 1a c1 e1 70 71 ac 51 f2 7e 64 42 66 F ·- ·p q o ~bf ·
0019 27 b5 89 05 40 ge c7 bz fc ba ff 42 c3 38 69 60 ^ ·- ·@n k B1 ·

Wireshark display filter

Packet listing

Packet layers

Packet bytes

Capture metadata

Customizing the UI - Columns

The screenshot shows the Wireshark interface with a packet selected. A context menu is open over the selected packet, specifically the one at index 12. The menu items visible include:

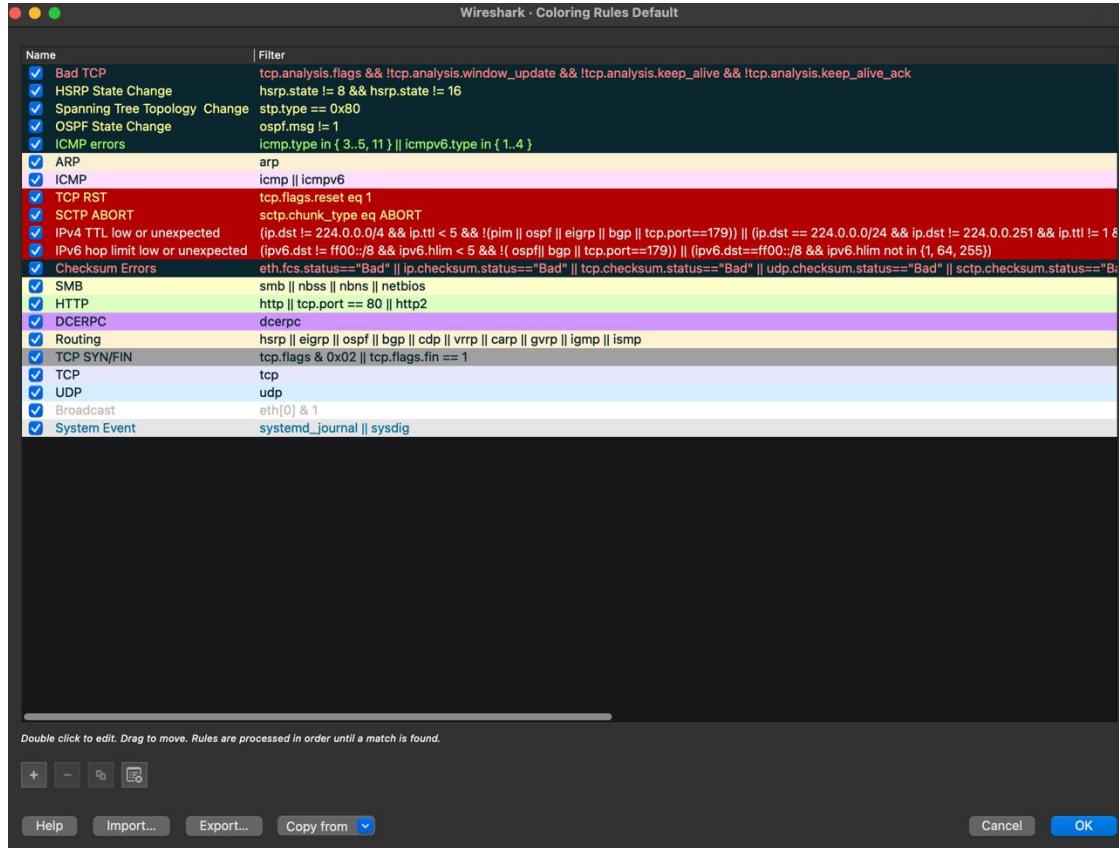
- Apply as Subtree
- Collapse Subtrees
- Expand All
- Collapse All
- Apply as Column (highlighted with a red box)
- QX

The selected packet details are shown in the main pane:

No.	Time	Source	Destination	Protocol	Length	Info
1	2024-11-04 16:08:08.065519	52.223.1.163	192.168.197.141	TLSv1.2	547	Application Data
2	2024-11-04 16:08:08.065614	192.168.197.141	52.223.1.163	TCP	66	57839 - 443 [ACK] Seq=2279766114 Ack=1049325794 Win=2040 Len=0 TStamp=4203520823 TSecr=
3	2024-11-04 16:08:08.101715	192.168.197.141	52.223.1.163	TLSv1.2	231	Application Data
4	2024-11-04 16:08:08.140164	52.223.1.163	192.168.197.141	TCP	66	443 - 57839 [ACK] Seq=1049325794 Ack=2279766279 Win=1954 Len=0 TStamp=1577653841 TSecr=
5	2024-11-04 16:08:08.252105	99.83.250.143	192.168.197.141	TCP	66	443 - 58188 [ACK] Seq=1641673934 Ack=2893573071 Win=122 Len=0 TStamp=3886905425 TSecr=
6	2024-11-04 16:08:08.351206	192.168.197.141	28.189.173.8	TLSv1.2	427	Application Data
7	2024-11-04 16:08:08.351295	28.189.173.8	192.168.197.141	TLSv1.2	1111	Application Data
8	2024-11-04 16:08:08.351356	28.189.173.8	192.168.197.141	TCP	1414	57839 - 443 [ACK] Seq=1071932827 Ack=269559361 Win=2048 Len=1348 TStamp=2268877677 TSecr=
9	2024-11-04 16:08:08.543237	28.189.173.8	192.168.197.141	TLSv1.2	1414	443 - 57839 [ACK] Seq=1049325794 Ack=2279766279 Win=1954 Len=1348 TStamp=1577654247 TSecr=
10	2024-11-04 16:08:08.543237	192.168.197.141	192.168.197.141	TLSv1.2	1047	Application Data
11	2024-11-04 16:08:08.543237	192.168.197.141	192.168.197.141	TLSv1.2	1048	Application Data
12	2024-11-04 16:08:08.543237	192.168.197.141	192.168.197.141	TCP	66	57839 - 443 [ACK] Seq=2279766279 Ack=1049328161 Win=2011 Len=0 TStamp=4203521301 TSecr=
13	2024-11-04 16:08:08.631047	192.168.197.141	192.168.197.141	TCP	1414	443 - 58207 [ACK] Seq=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
14	2024-11-04 16:08:08.631047	192.168.197.141	192.168.197.141	TCP	1414	443 - 58207 [ACK] Seq=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
15	2024-11-04 16:08:08.631055	192.168.197.141	192.168.197.141	TCP	1414	443 - 58207 [ACK] Seq=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
16	2024-11-04 16:08:08.631055	192.168.197.141	192.168.197.141	TCP	1414	443 - 58207 [ACK] Seq=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
17	2024-11-04 16:08:08.631147	192.168.197.141	192.168.197.141	TCP	1414	443 - 58207 [ACK] Seq=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
18	2024-11-04 16:08:08.631806	192.168.197.141	192.168.197.141	TCP	1414	443 - 58207 [ACK] Seq=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
19	2024-11-04 16:08:08.634991	192.168.197.141	192.168.197.141	TCP	1414	443 - 58207 [ACK] Seq=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
20	2024-11-04 16:08:08.647784	192.168.197.141	192.168.197.141	TLSv1.2	159	Application Data
21	2024-11-04 16:08:08.647784	192.168.197.141	28.189.173.8	TCP	66	57772 - 443 [ACK] Seq=1071934374 Ack=269559454 Win=2046 Len=0 TStamp=226888063 TSecr=
22	2024-11-04 16:08:08.646659	28.189.173.8	192.168.197.141	TLSv1.2	113	Application Data
23	2024-11-04 16:08:08.646659	192.168.197.141	28.189.173.8	TLSv1.2	99	Application Data
24	2024-11-04 16:08:08.674059	28.189.173.8	192.168.197.141	TCP	74	58207 - 443 [FIN, ACK] Seq=3989515206 Ack=53549788 Win=895 Len=0
25	2024-11-04 16:08:08.695726	192.168.197.141	28.189.173.8	TCP	74	443 - 58207 [ACK] Seq=3989515182 Win=16388 Len=0
> Frame 13: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en0, id 0					0000	82 52 cf 4b d3 34 76 1a 52 1b 8c 04 08 00 45 00 R K 4v R E
> Ethernet II, Src: Cisco (00:0c:29:00:00:00), Dst: 00:0c:29:00:00:00 (00:0c:29:00:00:00)					0010	00 34 00 00 40 00 40 06 7e 0c c9 a8 c5 d8 34 df 4 @ @ ~
> Internet Protocol Version 4, Src: 192.168.197.141 (192.168.197.141), Dst: 28.189.173.8 (28.189.173.8)					0020	01 a3 e1 e1 ff 01 bb 87 e2 79 07 3e 8b 21 88 10 ..+..y>z..
> Transmission Control Protocol, Src: 192.168.197.141 (192.168.197.141), Dst: 28.189.173.8 (28.189.173.8)					0030	07 db ff 55 00 00 01 01 08 0a fa 8c a5 15 5e 09 ..U.....~..~..
> Protocol Preferences					0040	17 e7 ..
Source Port: 57820						
Destination Port: 443						
[Stream Index: 0]						
[Stream Packet Number: 8]						
> Conversation completeness: Incomplete (12)						
[TCP Segment Len: 0]						
Sequence Number: 2279766279						
[Next Sequence Number: 2279766279]						
Acknowledgment Number: 1049328161						
1000 = Header Length: 32 bytes (8)						
> Flags: 0x010 (ACK)						
Window: 2011						
[Calculated window size: 2011]						
[Window size scaling factor: -1 (unknown)]						
Csum: 0xffff (Unverified)						
[Checksum Status: Unverified]						
Urgent Pointer: 0						
> Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps						
> [Timestamps]						
> [SEQ/ACK analysis]						

- Quick access within packet details/layers
- Also available at “Preferences > Appearance > Columns”

Customizing the UI – Coloring rules



- A picture is worth a thousand words!
- Setup custom rules to quickly catch special conditions
- Accessible at “View > Coloring Rules”

Capture Statistics

Conversations

The screenshot shows the 'Conversations' dialog in Wireshark. The title bar reads 'Wireshark · Conversations · Wi-Fi: en0'. The main area displays a table of TCP conversations. The columns are labeled 'Address A', 'Port A', 'Address B', and 'Port B'. The table contains the following data:

Address A	Port A	Address B	Port B
52.8.21.190	443	192.168.197.141	57936
52.223.1.163	443	192.168.197.141	57839
99.83.250.143	443	192.168.197.141	58180
170.72.245.243	443	192.168.197.141	57871
192.168.197.141	57772	20.189.173.8	443
2401:4900:9006:e92d:546:e6bf:940f:f4f4	58141	2603:1063:27:2::14	443
2600:9000:24d8:6e00:6:5671:b9c0:93a1	443	2401:4900:9006:e92d:546:e6bf:940f:f4f4	57899
2620:1ec:8fa::10	443	2401:4900:9006:e92d:546:e6bf:940f:f4f4	58207

The left sidebar contains 'Conversation Settings' with checkboxes for 'Name resolution', 'Absolute start time', and 'Limit to display filter'. It also includes buttons for 'Copy', 'Follow Stream...', and 'Graph...'. Below this is a 'Protocol' dropdown menu with checkboxes for various protocols, including 'Ethernet' (which is checked), 'IPv4' (which is checked), and 'IPv6'. At the bottom are 'Help' and 'Close' buttons.

- Accessible at “Statistics > Conversations”
- Quick summary of Layers 2, 3 and 4 conversations with statistics
- Ability to filter down if necessary

Export Objects

Wireshark · Export · HTTP object list

Text Filter: Content Type: All Content-Types

Packet	Hostname	Content Type	Size	Filename
178	eu.httpbin.org	text/html	9593 bytes	/
227	eu.httpbin.org	application/json	41 kB	spec.json
388	o.pki.goog	application/ocsp-request	84 bytes	wr2
417	o.pki.goog	application/ocsp-response	472 bytes	wr2
1484	o.pki.goog	application/ocsp-request	84 bytes	wr2
1506	o.pki.goog	application/ocsp-response	472 bytes	wr2
1641	o.pki.goog	application/ocsp-request	84 bytes	wr2
1685	o.pki.goog	application/ocsp-response	472 bytes	wr2

Help Preview Save All Close Save

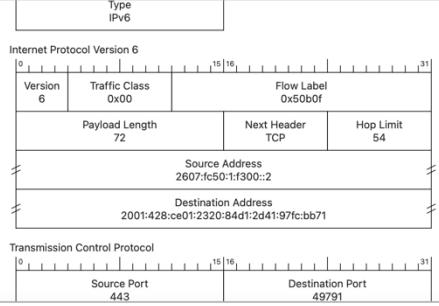
- Accessible at “File > Export Objects”
- Direct access to Application layer objects (files, etc.)
- Protocols supported include FTP, HTTP, SMB, TFTP.

Packet Diagrams

Packet Diagrams

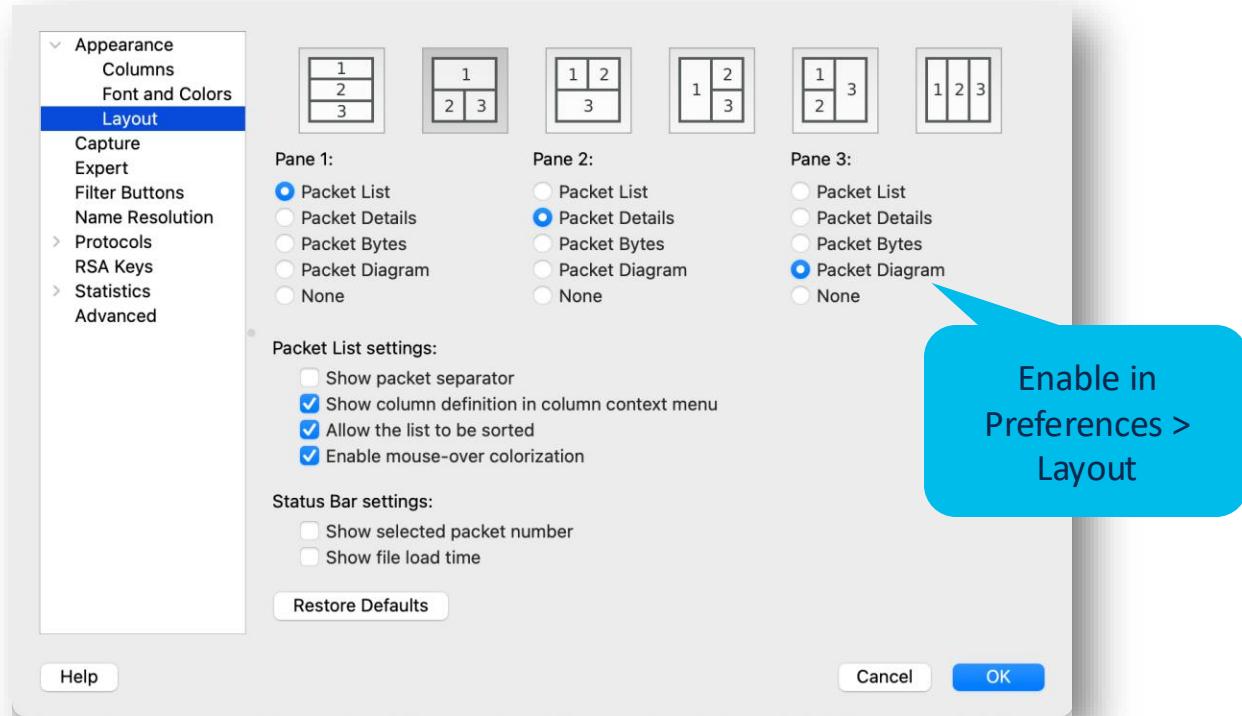
No.	Time	Src MAC	Dst MAC	Source	Destination	Protocol	Length	Info
402	10.9990..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	468	443 - 49791 [PSH, ACK] Seq=3715 Ack=518 Win=66304 Len=382 Tsvl=3527492959 TSec=3527492959
403	10.9990..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TLSv1.3	637	Application Data, Application Data, Application Data
404	10.9992..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TCP	86	49791 - 443 [ACK] Seq=518 Ack=6468 Win=126528 Len=0 Tsvl=2345773811 TSecr=3527492959
405	11.0039..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TCP	166	[TCP Window Update] 49791 - 443 [ACK] Seq=518 Ack=6468 Win=131072 Len=0 Tsvl=2345773811 TSecr=3527492959
406	11.0059..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TLSv1.3	166	Change Cipher Spec, Application Data
407	11.0060..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TLSv1.3	561	Application Data
408	11.0061..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TLSv1.3	389	Application Data
409	11.0703..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TLSv1.3	389	Application Data
410	11.0703..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TLSv1.3	389	Application Data
411	11.0705..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	86	49791 - 443 [ACK] Seq=1073 Ack=5254 Win=130432 Len=0 Tsvl=2345773882 TSecr=3527493037
412	11.0733..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	1324	443 - 49791 [ACK] Seq=5254 Ack=1073 Win=66304 Len=1238 Tsvl=3527493037 TSecr=3527493037
413	11.0733..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	1324	443 - 49791 [ACK] Seq=6492 Ack=1073 Win=66304 Len=1238 Tsvl=3527493037 TSecr=3527493037
414	11.0733..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	1324	443 - 49791 [ACK] Seq=7730 Ack=1073 Win=66304 Len=1238 Tsvl=3527493037 TSecr=3527493037
415	11.0733..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TLSv1.3	151	Application Data
416	11.0734..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TCP	86	49791 - 443 [ACK] Seq=1073 Ack=5254 Win=127232 Len=0 Tsvl=2345773885 TSecr=3527493151
417	11.0735..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TCP	86	[TCP Window Update] 49791 - 443 [ACK] Seq=1073 Ack=9033 Win=131072 Len=0 Tsvl=2345773885 TSecr=3527493151
428	11.1211..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TLSv1.3	516	Application Data
442	11.1875..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	1324	443 - 49791 [ACK] Seq=9033 Ack=1497 Win=66304 Len=1238 Tsvl=3527493151 TSecr=3527493151
443	11.1875..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	1324	443 - 49791 [ACK] Seq=10271 Ack=1497 Win=66304 Len=1238 Tsvl=3527493151 TSecr=3527493151
444	11.1875..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	1324	443 - 49791 [ACK] Seq=11589 Ack=1497 Win=66304 Len=1238 Tsvl=3527493151 TSecr=3527493151
445	11.1875..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	1324	443 - 49791 [ACK] Seq=12747 Ack=1497 Win=66304 Len=1238 Tsvl=3527493151 TSecr=3527493151
446	11.1875..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TLSv1.3	126	Application Data

Frame 446: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface en0, id 0
 Ethernet II, Src: Cisco_32:72:42 (0:c:60:4f:32:72:42), Dst: Apple_37:20:69 (bc:d0:74:37:20:69)
 Internet Protocol Version 6, Src: 2607:fc50:1:f300::2, Dst: 2001:428:ce01:2320:84d1:2d41:97fc:bcb0ff:0110 = Version: 6
 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
 0101 0011 1011 0000 1111 = Flow Label: 0x50b0f
 Payload Length: 72
 Next Header: TCP (6)
 Hop Limit: 54
 Source Address: 2607:fc50:1:f300::2
 Destination Address: 2001:428:ce01:2320:84d1:2d41:97fc:bb71
 Transmission Control Protocol, Src Port: 443, Dst Port: 49791, Seq: 13985, Ack: 1497, Len: 40
 Source Port: 443
 Destination Port: 49791
 [Stream index: 36]
 [Conversation completeness: Incomplete, DATA (15)]
 [TCP Segment Len: 40]
 Sequence Number: 13985 (relative sequence number)
 Sequence Number (raw): 2646950740
 [Next Sequence Number: 14025 (relative sequence number)]
 Acknowledgment Number: 1497 (relative ack number)



- New to Wireshark 3.4
- Save or print them
 - Copy as raster images
 - Teach new engineers how a frame becomes a packet

Packet Diagrams



Following Streams

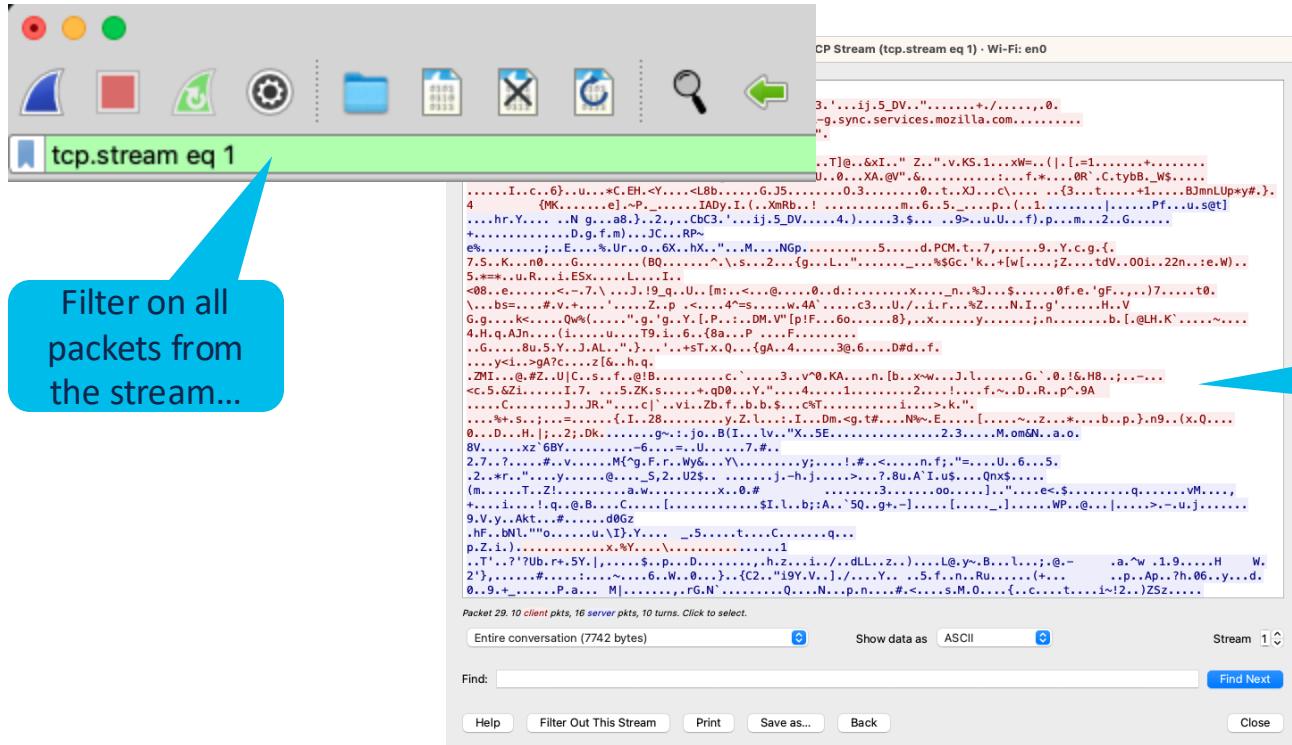
Following Streams

No.	Time	Src MAC	Dest MAC	Source
1	0.000000	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
2	0.001193	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
3	0.001297	Cisco_5f:05:f4	Apple_74:b0:67	2600:1901:0:e988::
4	0.002434	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
5	0.002947	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
6	0.007578	Cisco_5f:05:f4	Apple_74:b0:67	64.102.6.247
7	0.011914	Cisco_5f:05:f4	Apple_74:b0:67	64.101.105.66
8	0.017469	Cisco_5f:05:f4	Apple_74:b0:67	64.102.6.247
9	0.018983	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
10	0.020056	Cisco_5f:05:f4	Apple_74:b0:67	64.102.6.247
11	0.021160	Cisco_5f:05:f4	Apple_74:b0:67	64.102.6.247
12	0.399883	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
13	0.401712	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
14	0.425368	Cisco_5f:05:f4	Apple_74:b0:67	64.102.6.247
15	0.429318	Cisco_5f:05:f4	Apple_74:b0:67	64.102.6.247
16	0.433944	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
17	0.434071	Apple_74:b0:67	Cisco_5f:05:f4	Mark/Unmark Packet Ignore/Unignore Packet Set/Unset Time Reference Time Shift... Packet Comments
18	0.434443	Apple_74:b0:67	Cisco_5f:05:f4	Edit Resolved Name
19	0.453942	Cisco_5f:05:f4	Apple_74:b0:67	Apply as Filter Prepare as Filter Conversation Filter Colorize Conversation SCTP
20	0.454240	Apple_74:b0:67	Cisco_5f:05:f4	Follow
21	0.456926	Apple_74:b0:67	Cisco_5f:05:f4	Copy
22	0.475223	Cisco_5f:05:f4	Apple_74:b0:67	Protocol Preferences Decode As... Show Packet in New Window
23	0.476287	Cisco_5f:05:f4	Apple_74:b0:67	TCP Stream UDP Stream DCCP Stream TLS Stream HTTP Stream HTTP/2 Stream QUIC Stream SIP Call

- TCP
- UDP
- DCCP
- TLS
- HTTP[2]
- QUIC
- SIP

Pick the stream to follow based on initial packet

Following Streams



Decode As...

Decode As...

No.	Time	Source	Destination	Protocol	Length	Info
2984	109.081002	10.21.9.164	162.223.13.118	UDP	64	62139 → 5514 Len=22

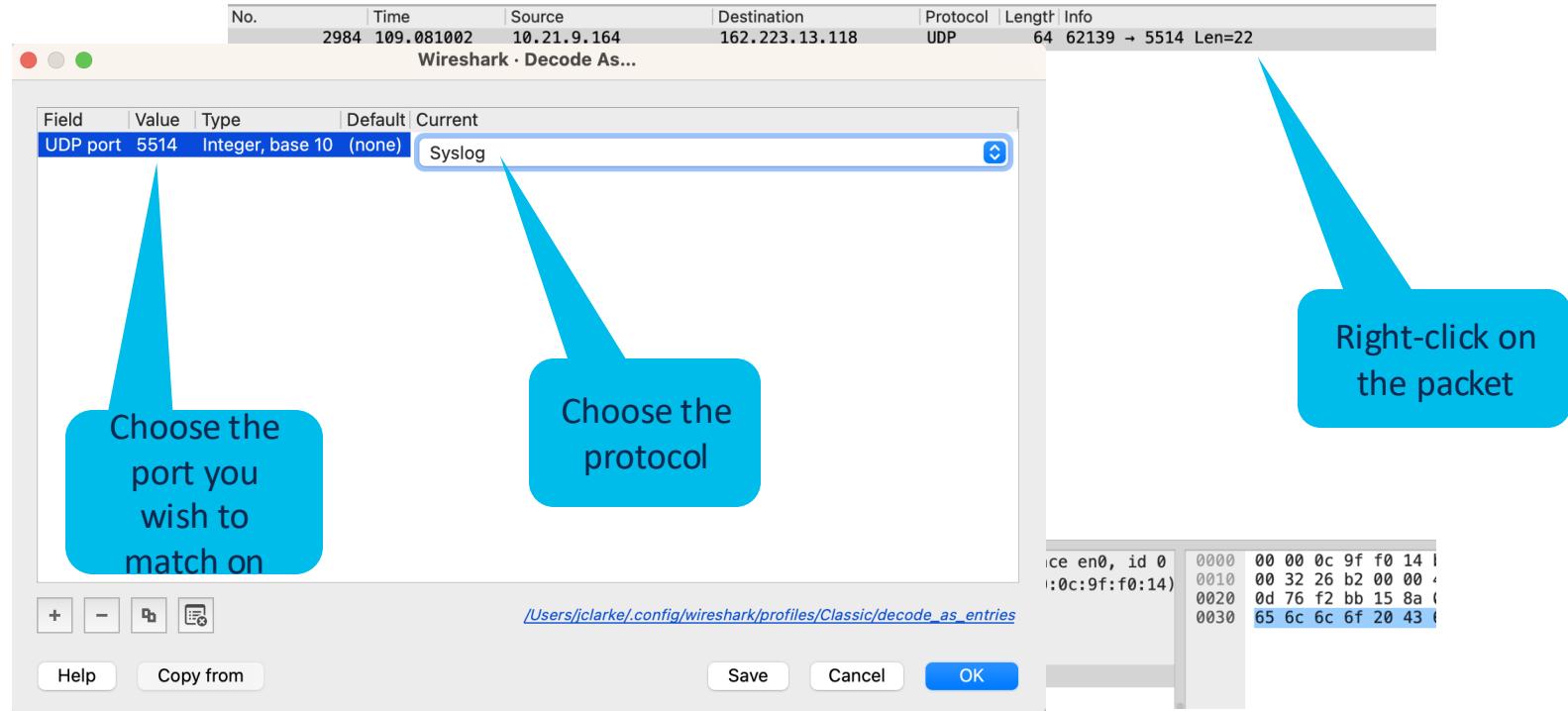
Let's say you have a data stream using non-standard ports. You still want to make use of wireshark's dissectors.

64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface en0, id 0 , Src: Apple_37:20:69 (bc:d0:74:37:20:69), Dst: Cisco_9f:f0:14 (00:00:0c:9f:f0:14) otocol Version 4, Src: 10.21.9.164, Dst: 162.223.13.118 am Protocol, Src Port: 62139, Dst Port: 5514

0000 00 00 0c 9f f0 14 !
0010 00 32 26 b2 00 00 !
0020 0d 76 f2 bb 15 8a !
0030 65 6c 6c 6f 20 43 !

▼ Data (22 bytes)
Data: 3c3135393e48656c6c6f20436973636f4c6976652100
[Length: 22]

Decode As...



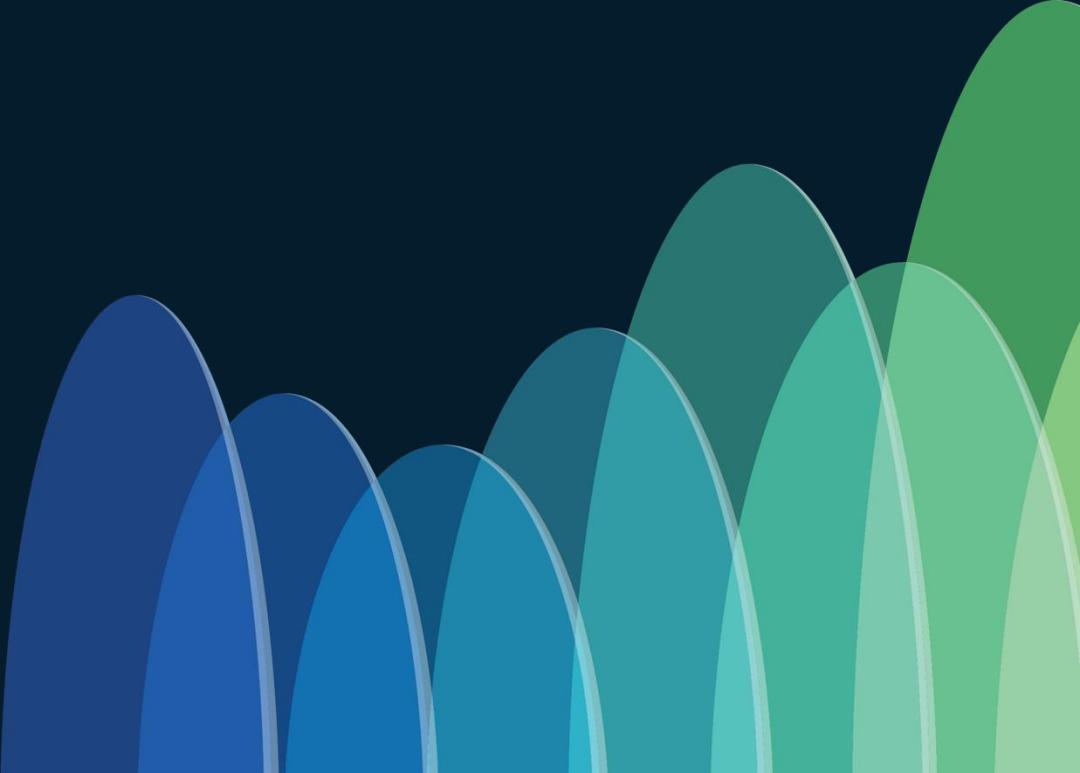
Decode As...

No.	Time	Source	Destination	Protocol	Length	Info
2984	109.081002	10.21.9.164	162.223.13.118	Syslog	64	LOCAL3.DEBUG: Hello CiscoLive!\000

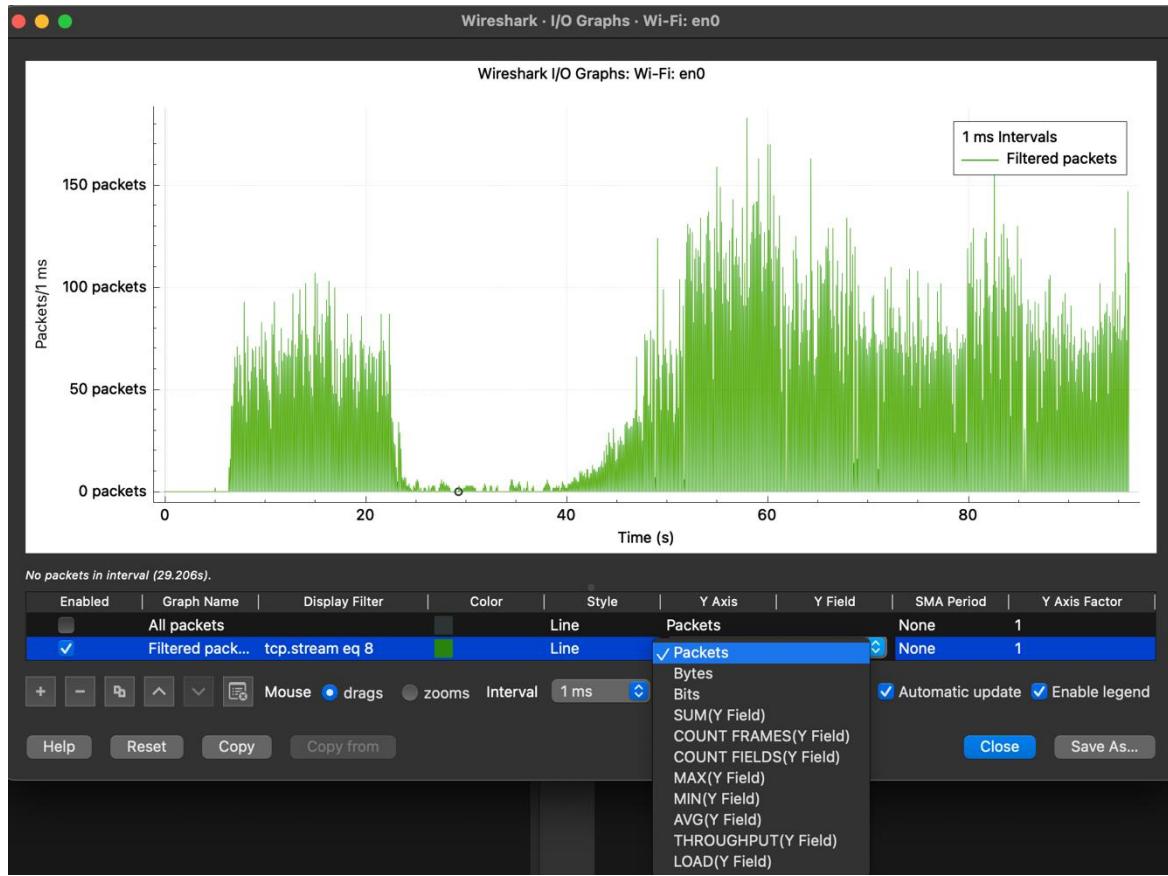
```
> Frame 2984: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface en0, id 0
> Ethernet II, Src: Apple_37:20:69 (bc:d0:74:37:20:69), Dst: Cisco_9f:f0:14 (00:00:0c:9f:f0:14)
> Internet Protocol Version 4, Src: 10.21.9.164, Dst: 162.223.13.118
> User Datagram Protocol, Src Port: 62139, Dst Port: 5514
▼ Syslog message: LOCAL3.DEBUG: Hello CiscoLive!\000
    1001 1... = Facility: LOCAL3 - reserved for local use (19)
    .... .111 = Level: DEBUG - debug-level messages (7)
    Message: Hello CiscoLive!
```

```
0000 00 00 0c 9f f0 14 l
0010 00 32 26 b2 00 00 ,
0020 0d 76 f2 bb 15 8a (
0030 65 6c 6c 6f 20 43 )
```

Traffic performance troubleshooting

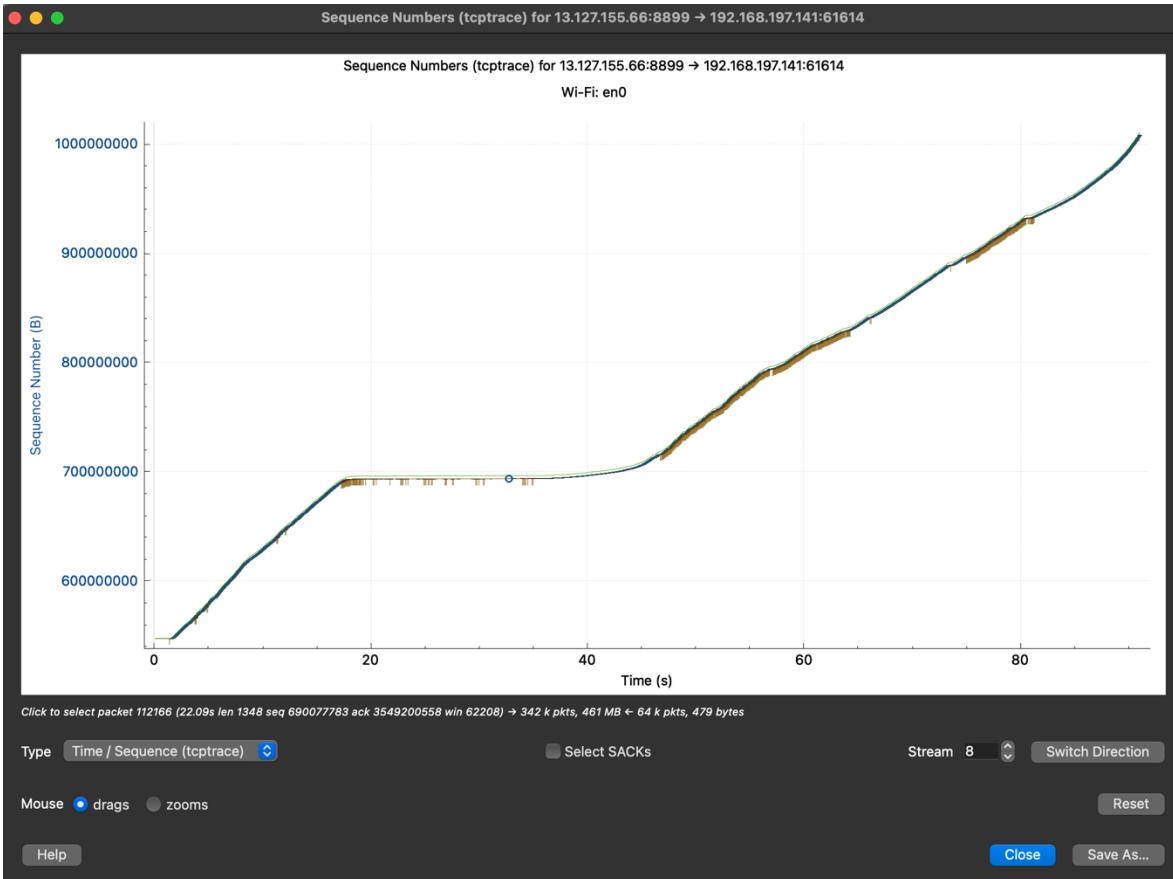


Input/Output (I/O) graphs



- Accessible at “Statistics > I/O Graphs”.
- Ability to graph for various parameters
- Multiple graphs in a single window – easy comparison

TCP graphs - tcptrace



- Accessible at “Statistics > TCP Stream Graphs”.
- Plots sequence, acknowledgement, sack, window size in a single graph
- Linear line = good!
- Steeper line = higher throughput

Remote Capture

Remote Capture

Input Output Options

Interface	Traffic	Link-layer Header	Promisc	Snaplen (B)	Buffer (MB)	Mo
Ethernet Adapter (en4): en4	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—
Ethernet Adapter (en5): en5	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—
Ethernet Adapter (en6): en6	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—
Thunderbolt 1: en1	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—
Thunderbolt 2: en2	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—
Thunderbolt 3: en3	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—
Thunderbolt Bridge: bridge0	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—
ap1	_____	Ethernet	<input checked="" type="checkbox"/>	default	2	—
gif0	_____	BSD loopback	<input checked="" type="checkbox"/>	default	2	—
stf0	_____	BSD loopback	<input checked="" type="checkbox"/>	default	2	—
(Cisco remote capture: ciscodump	_____	Remote capture dependent DLT	—	—	—	—
(Random packet generator: randpkt	_____	Generator dependent DLT	—	—	—	—
(SSH remote capture: sshdump	_____	Remote capture dependent DLT	—	—	—	—
(UDP Listener remote capture: udpdump	_____	Exported PDUs	—	—	—	—
(Wi-Fi remote capture: wifidump	_____	Remote capture dependent DLT	—	—	—	—

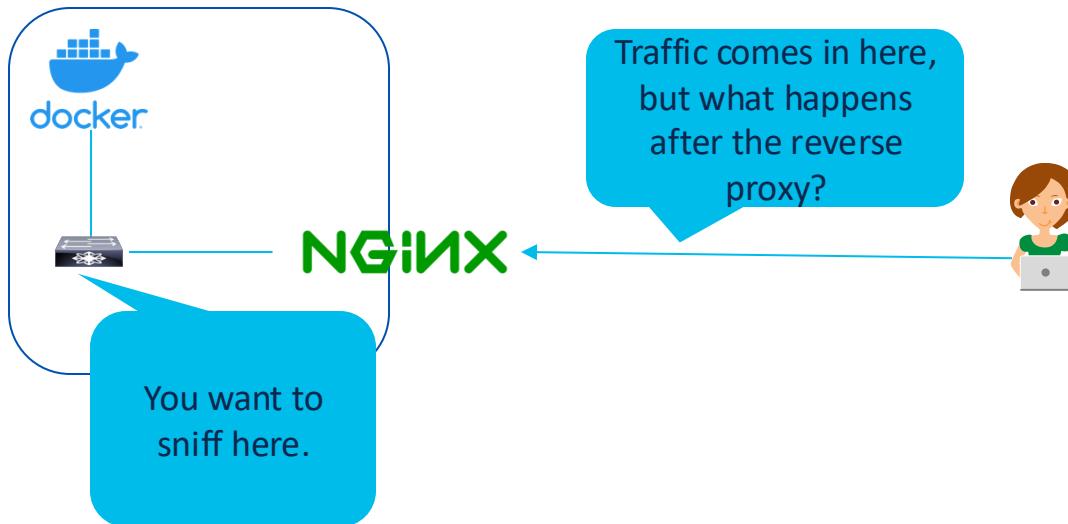
Enable promiscuous mode on all interfaces Manage Interfaces...

Capture filter for selected interfaces: Compile BPFs

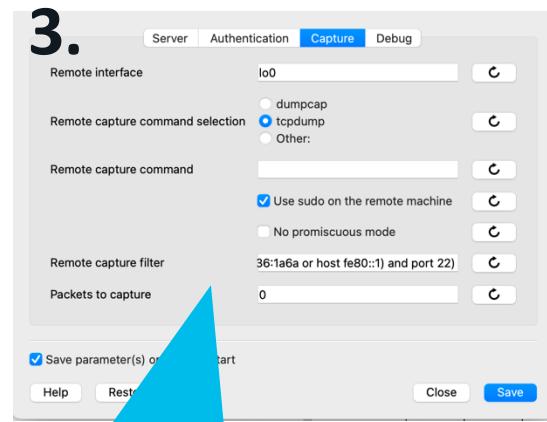
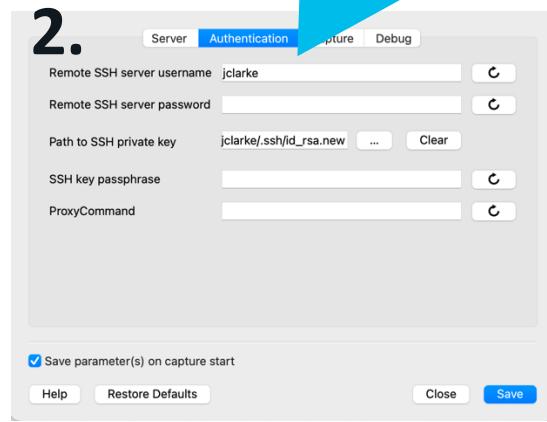
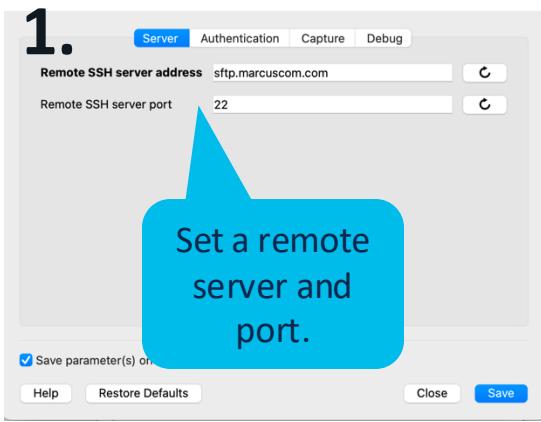
Help Close Start

- Don't forget to scroll down and explore the full interface list
- Remote captures are excellent for troubleshooting embedded services or setting up a SPAN server

Remote Capture



Remote Capture



Decrypt the Things!

Decrypt the Things!

Well this is
terribly useful

```
... .j. $.....%Tr.ae.\.4EQ.
..... /5.....www.marcuscom.com.....
..... #.h2.http/1.1.....
3.k.i....m-..7m..a!.L..u..K.#).0nn0d..A.rB....x.M....^.'i.X.J....S.t...C?<.be.).M8)...e.+.....
..... @.....
..... [.....a..17.8]....>..2..N..Pu..;..U..?..V.....+...3.$....=..Ru4.S..)d..y[.'H.....*k....j.&I....+1.]....y....y....F...
1.R..t....0..d.8.Hco....1K'7.R..HTId..8..0.....Ny..2..H..F..<....#....b....~/[d...*,$]....*N..G..X..V..C..C..k./..y!..7.c..9..P.)....PBS..L.....
4.G.H..T..!..V..'DXWG..NS!Vs.W..<....&..5.9..i..<..9.eK..u..tx..t..&..F..K..)DLE..;J..g..y..j..eBj..q..4..kx....UMY..]
d..g..D..m....W(Y)..J.Y..Z..L..<..0ecdX..J..&..(..d..9.p..l..)....0....n..11..R..7.j..z..L..1..98b..;
1.N'..t..?....?....^..c.y.a11..v1..Z..-..J..t..|. ....4..PGw..@..&..c..z..9....B>..X..~..R.._..!..J..d..4..L....E..T\..!..
0..A..n..Mw..)....v..i..p..C..[..9..~..4C
..... KZ....i.C..?..T..L..0..Q..0....5'G.s..?..a.o..)(NsU)..c.....
..... L..t..~(..#..L..T..AP..Y..L..f..^..t..t..t..=..)....q..05..c..3c..)'..4F'....c..1..*..mq....h....I..Cr7.....
..... Z..0..#..a..s..z..-..b..EE..L..j..(a..e..s..@..r..v..)....V..Z..D..G..-..b..6Yv..H..q..KVC..t..c.....
..... ~..8D..T..(v..6..$/..C..A..V..R..Ics..DM..RWyV..>....0..!..V..P..*..r..]....1..n..A..Q....[..h..u..s..h..h.....
..... e..L..oFU..W..I..5..j..WL..j..a..'*..E..f..8t..h..~..x..b..t..EM7LS..]..6..)....V..P..*..r..]....1..n..A..Q....[..h..u..s..h..h.....
..... W..G..>..M..A..F..Ph..V..4..9Z..A..0.....
..... 0..A..>..M..1..4Cy..sr..Er..p..)"..0..Bq..>[..W..Km..+....5..&..G..B..J..3..N..-....V..aAU..<..7^..W..C..4..;q..P..<..B..<..R..t..j..m..*,*.....
kvvi+.g51..M..T..Y..M..A..A..K..o..(..J..1..12..oW..RN..>....<..D..6..0!..1^..'.
..... f..M..a..o..C..c..m..!..5<..1..(..d..Y5S..)Ui..g..2..<..g..(..GD..<..A..L..v$Q..m..;....0..I..G..^..d..".I..v=v.....
2..zp../....Gg..dt..@..L..p..L..j..9..2..n..2..)....x..C..Y..O..Z..I..M..4..Bmx..IGINF..3..4..~..b..+..J..j.....
..... t..x..p..[....5ZG..E..u..yt..v..].....
..... !..x..w..Q..0.....
0..of..A;>..x..h..x..2..X0..a..h..N..0..Z)..[..B..].....
..... p.v..s..Dj.....
..... W..n.....
..... y..f..E..^..m..a..b..u..T..L..D....ld..w.."
%9g.C.U.x.%Z
J..x..A..*..kPlq.....<..l1..<....[.....Yg..)....A..+(....B..n..Z..P..)....2..841..X..l..c.....
..... W..V..DA.....
..... r..OR..)..d..>.....
..... 6f..p..c..*..D..Cw..<(j..4..r..Q..a..0.....
x..?24..D..g..I..E..(....B..T..)"..4.....
..... %..Tw..d....G..P:#..3..N..6..o..A..i..W..S..i..0..)C..7....<..!..IC....5"....FAt..o..W..n..x.....
..... 4..5..p..*..k..R..:..1..l..d..v..w..[....Vt..0..0..E..S..3..]....P..k..u..u..Foy..)....m..-..0..=%..>..=..b..B..B.....
[...y..s..p..T..+..f..+..d..8t..#..y..1..@..<..x..4..h@W..k..0..Y..U..61..Z..q..7..W..2..e..a..Zt..K..L..s..:..B..#..)....a..K..85..p4W..!
U..L..V..V..p..&..ZqR..AS..ogh?..(..M9..`..P..4..HR..k..F..0..(..u..g..Th..T..L..m..=..H..4g../_..c..F..s..,T../_..i..3h..G.....
..... #..y..FR$..4..p..C..d..,itd.....
..... @..hb..F..5..X.....
9..t.....
..... G..S....j0..3..%....i..3..0..)....|..0..">..C..*..1..c..Sk..3..L..B..1..3B..*..h..64..(.D..dV..h..2..T.....
8..6..*..ft..r..,..u..-..I..)....V..E..S..G..z..-..61..6D..BB..hu..A..>..n..,"..Dq..H..,..v..B0..066..0..,..^..&..|..)....0K..wV0..C..-..^..<.....
5..7..?..A..GU..ve..M..*..[..w..~..(..gh..ER..aj..C..,..Z..-..)....$..p..-..y..)....2..0..-..b..%..6..c..i..%..m..-..2..#..#3..0..o..h..t..u..u..a..>.....
..... J..a..,..K..7..),....(_..xn..Ig..Ag..-..f..,..g..0..)....1..BeBe..246..</..o..<..-..l..-..S..:..r..Q..w..I..R..<..P..CG.....
7..3..k..E..,..%..E..&..5H..Py..1..0..JR..1..)".....
..... ?..F2..-..ud..Y4T..(....V..K..G..)....9..%..p..G..ST..o..!..p..p..C..m..-..D..e..ld..a..H..s..4..a..,....p..@..r..qlj..IG.....
..... <..-..c..o..,..Et..EZ..0..,..u..5K89..1..)....EcDr..l..,..-..:..S..Vo..18..R..ahJ6q..,..s..K..R..i..>..@.."-..0..u..!..I..o..A..~..cdXX..3..k..l..j..=..S..t..(..p..N..
9..,..c..6..,..eG..E..+..Aj..-..1..E..)....a..0..,..#..W..(..6..)....4..K.....
..... ST..H..$..Rm..-..d..1.....
..... J..u..USK..m..,..uc..0..,..t..u..u..,..
```

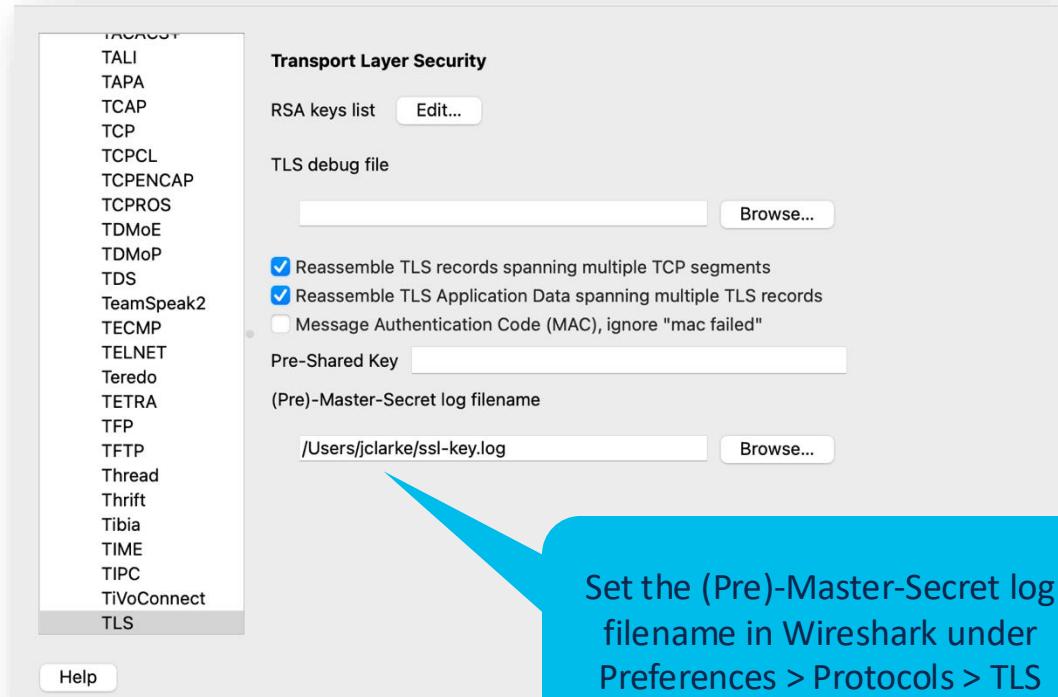
Well this isn't
terribly useful...

Decrypt the Things!

- Set the SSLKEYLOGFILE environment variable
- Refresh your environment (e.g., source your .bashrc)
- Restart your browser

```
$ export SSLKEYLOGFILE=~/ssl-  
key.log  
$ open  
/Applications/Firefox.app
```

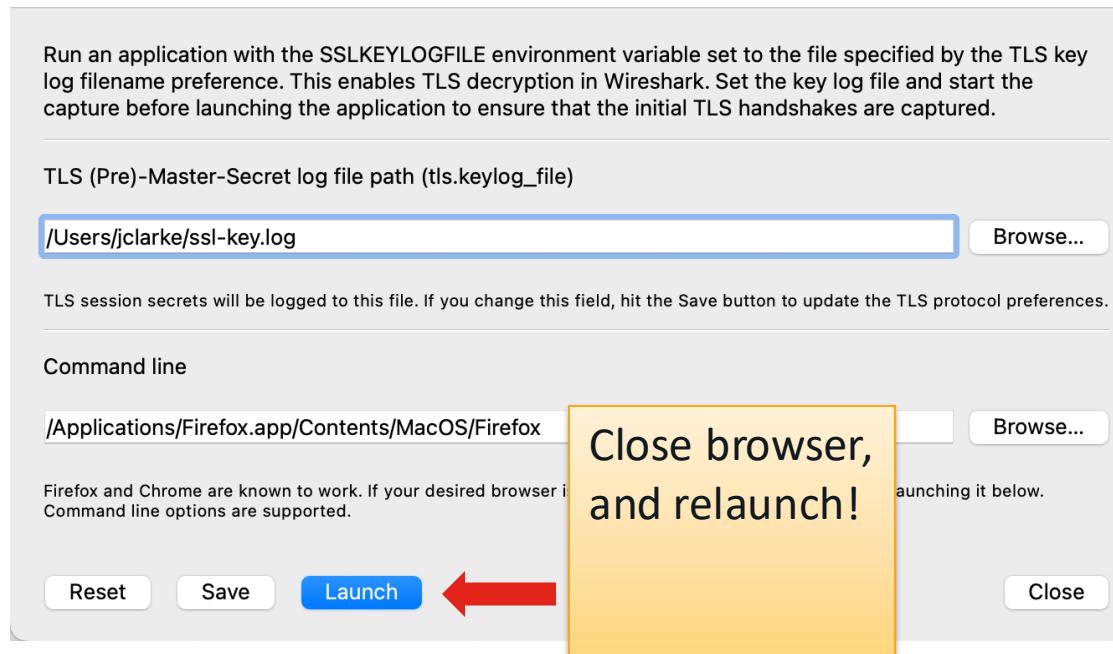
Decrypt the Things!



Set the (Pre)-Master-Secret log filename in Wireshark under Preferences > Protocols > TLS

Wireshark 4.2 Makes It Easier

Tools > TLS Keylog Launcher



Decrypt the Things!

```
GET /git HTTP/1.1
Host: www.marcuscom.com
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
sec-ch-ua: "Google Chrome";v="113", "Chromium";v="113", "Not-A.Brand";v="24"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "macOS"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: lang=en-US; i_like_gogs=aae7ad4c5bb693b9; _csrf=el25xoA1e009cwh6Es30Ng3WGU6MTY4NjA20Dcw0DA4NTUxMTk3NQ

HTTP/1.1 200 OK
Date: Tue, 06 Jun 2023 16:25:32 GMT
Server: Apache/2.4.57 (FreeBSD) OpenSSL/1.1.1t PHP/8.1.19 SVN/1.14.2
Content-Type: text/html; charset=UTF-8
X-Content-Type-Options: nosniff
X-Frame-Options: DENY
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Transfer-Encoding: chunked

<!DOCTYPE html>
<html>
<head data-suburl="/git">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
    <meta name="author" content="Gogs" />
    <meta name="description" content="Gogs is a painless self-hosted Git service" />
    <meta name="keywords" content="go, git, self-hosted, gogs" />
    <meta name="referrer" content="no-referrer" />
    <meta name="_csrf" content="el25xoA1e009cwh6Es30Ng3WGU6MTY4NjA20Dcw0DA4NTUxMTk3NQ" />
    <meta name="_suburl" content="/git" />
    <meta property="og:url" content="https://www.marcuscom.com/git/" />
    <meta property="og:type" content="website" />
</head>
```

Profit!

Packet 32. 3 client pkts, 3 server pkts, 5 turns. Click to select.

Download the slides

[https://github.com/praprama/CIS
COU-2036](https://github.com/praprama/CISCOU-2036)



Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging into the Session Catalog and clicking the 'Participant Dashboard' link at
<https://www.ciscolive.com/emea/learn/session-catalog.html>.





Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

Contact me at: prarama@cisco.com



Thank you

cisco *Live!*



GO BEYOND