

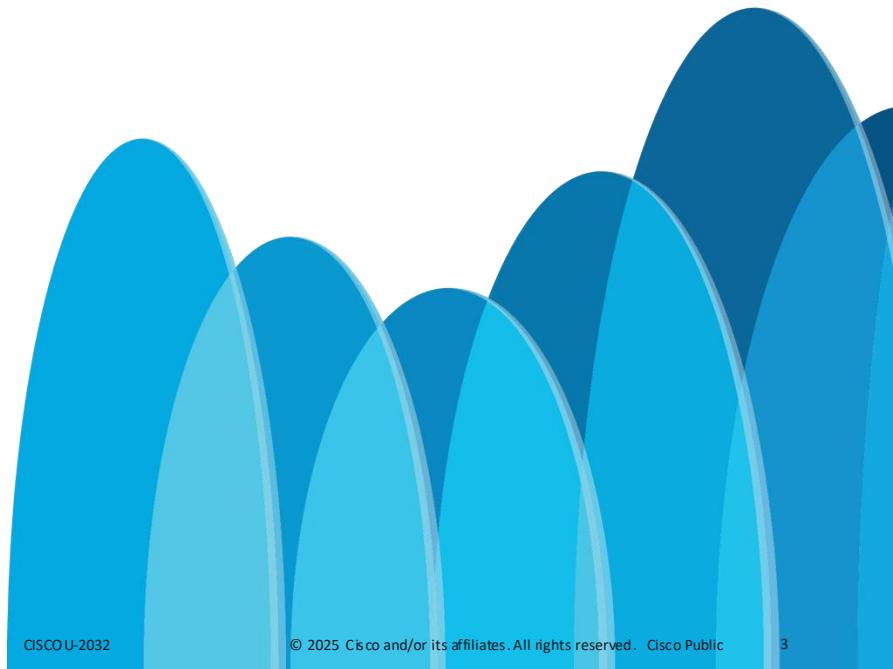


Become a network doctor using packet captures and Wireshark

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

Wi-Fi: en0

Quick access menu

Wireshark display filter

Packet listing

Packet layers

Packet bytes

Capture metadata

Frame 1: 547 bytes on wire (4376 bits), 547 bytes captured (4376 bits) on interface en0, id 0
Ethernet II, Src: 82:52:c4:b3:34 (82:52:c4:b3:34), Dst: 76:1a:52:1b:8c:04 (76:1a: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	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 TSval=4203520823 TSecr=231 Application Data
3	2024-11-04	16:08:08.101715	192.168.197.141	52.223.1.163	TLSv1.2	66	443 - 57839 [ACK] Seq=1049325794 Ack=2279766279 Win=1954 Len=0 TSval=1577653841 TSecr=231 Application Data
4	2024-11-04	16:08:08.140164	52.223.1.163	192.168.197.141	TCP	66	443 - 58180 [ACK] Seq=1641673934 Ack=2893573071 Win=122 Len=0 TSval=3886905425 TSecr=231 Application Data
5	2024-11-04	16:08:08.252185	99.83.250.143	192.168.197.141	TCP	66	443 - 58180 [ACK] Seq=1641673934 Ack=2893573071 Win=122 Len=0 TSval=3886905425 TSecr=231 Application Data
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	16:08:08.351209	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=265 Application Data	
9	2024-11-04	16:08:08.351363	192.168.197.141	20.189.173.8	TLSv1.2	1414 443 - 57839 [ACK] Seq=1049325794 Ack=2279766279 Win=1954 Len=1348 TSval=1577654247 TSecr=265 Application Data	
10	2024-11-04	16:08:08.351373	52.223.1.163	192.168.197.141	TCP	1047 Application Data	
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	16:08:08.543246	52.223.1.163	192.168.197.141	TLSv1.2	1047 Application Data	
13	2024-11-04	16:08:08.543366	192.168.197.141	52.223.1.163	TCP	66	57839 -> 443 [ACK] Seq=2279766279 Ack=1049328161 Win=2011 Len=0 TSval=4203521301 TSecr=1044 Application Data
14	2024-11-04	16:08:08.631847	2628:1ec:8fa::10	2401:4908:9006: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	2628:1ec:8fa::10	2401:4908:9006:e92d:546:e6bf:94::	TLSv1.2	306 Application Data	
16	2024-11-04	16:08:08.631855	2628:1ec:8fa::10	2401:4908:9006:e92d:546:e6bf:94::	TLSv1.2	185 Application Data	
17	2024-11-04	16:08:08.632147	2401:4908:9006:e92d:546:e6bf:94::	2628:1ec:8fa::10	TCP	74 58207 -> 443 [ACK] Seq=3989515143 Ack=853549788 Win=4978 Len=0	
18	2024-11-04	16:08:08.631880	20.189.173.8	192.168.197.141	TCP	66	443 - 57772 [ACK] Seq=269559361 Ack=1071932827 Win=16386 Len=0 TSval=15830986 TSecr=254 Application Data
19	2024-11-04	16:08:08.634591	20.189.173.8	192.168.197.141	TCP	66	443 - 57772 [ACK] Seq=269559361 Ack=1071934374 Win=16386 Len=0 TSval=15830990 TSecr=254 Application Data
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=113 Application Data
22	2024-11-04	16:08:08.666859	2401:4908:9006:e92d:546:e6bf:94::	2628:1ec:8fa::10	TLSv1.2	113 Application Data	
23	2024-11-04	16:08:08.670665	2401:4908:9006:e92d:546:e6bf:94::	2628:1ec:8fa::10	TLSv1.2	98 Application Data	
24	2024-11-04	16:08:08.671793	2401:4908:9006:e92d:546:e6bf:94::	2628:1ec:8fa::10	TCP	74 58207 -> 443 [FIN, ACK] Seq=3989515206 Ack=853549780 Win=4096 Len=0	
25	2024-11-04	16:08:08.695728	2628:1ec:8fa::10	2401:4908:9006: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:c4:b3:34 (82:52:c4:b3:34), Dst: 76:1a:52:1b:8c:04 (76:1a: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 1a 52 1b 8c 04 v-R: R- K-E:
0001 02 15 8f 31 40 00 f0 06 f0 36 3f 41 d0 01 c3 a8 1@- 674-
0002 c5 8d 01 bb e1 ef 3e 80 61 07 e2 78 62 80 18 > o-xb-
0003 00 98 e1 d7 00 00 00 00 00 00 00 00 00 00 00 00 > }-
0004 02 17 00 00 00 00 00 00 00 00 00 00 00 00 00 00 > }-
0005 63 99 74 02 24 fb 9e cc 23 24 39 f5 cf 83 9c e5 c t s- l #9-
0006 c5 e9 c1 fd 42 b2 24 fb 47 71 c4 66 24 f3 96 3a 63 B- w+ q,f\$:c:
0007 12 6a 2b 48 3b ca 64 5d 41 3f 0e 28 29 b7 06 j+@- d l @? -)-
0008 02 bc 11 a5 3b c2 a5 83 3c a8 d4 b7 4a eb c3 fb B- ;-- <-J-
0009 2@ 00 aa ab b5 1e 79 8c dc 03 85 3f 10 e6 a5 35 *-y- ?-5-
000a 41 98 81 83 73 5d cf f7 c2 64 81 4e d3 d8 81 2a A-s- -d N-*
000b 68 b2 56 22 80 5b 26 62 59 e0 8c bb 5a 4f 13 3c h-V" |6b Y- Z0-
000c 68 b2 56 22 80 5b 26 62 59 e0 8c bb 5a 4f 13 3c h-V" |6b Y- Z0-
000d c5 60 66 60 f7 57 9c ff 36 79 0d 63 52 3b J- g- 6- 7-
000e 5a 77 4c a9 31 3a 93 09 5d 8c 8b 55 41 c2 52 5b ZwL; 1- J- UA'Z-
000f 68 1e 9a 88 ff 6b 69 ff fb aa 0f 03 e9 07 h- ;i-
0010 74 93 2a 8d 76 37 13 41 fd 05 63 a8 4c 01 41 1f t % v7 A- c L A-
0011 20 0b 4e 4a 4f 36 fe ae db 4f 3d 44 72 28 84 f-FO6- 0-Dr-
0012 6e 01 92 13 16 83 a3 62 4e db f2 3e 09 27 2b 95 n-...- b N- > '+'-
0013 b0 11 72 a3 0e dd b3 85 2e c0 01 c7 c9 88 09 q- .-
0014 e2 b7 38 04 80 2d 02 4f 13 a2 72 68 17 ce -3- -0- R- D-
0015 e0 0f 80 2d c5 01 00 00 00 00 00 00 00 00 00 00 S- 0- D-
0016 67 1c 26 2b 08 96 51 09 43 38 f0 5b fd e0 01 77 Q- C8- !-
0017 35 8a dc f2 5e a8 fc 4b 3c 67 fd db 51 1a 14 -5- ^ k Kg- 0-
0018 f1 aa 5b 3d fe 17 22 99 9e 11 90 7b 34 ea 04 -> -> -{
0019 82 c8 7a 14 3b 7d 88 f6 75 ea e4 54 06 c2 83 z-);- u- T-
001a 86 69 0c 66 9b 1c a9 0e 08 1c f7 56 9e 00 cc i- f- V-
001b 0b d4 2b 43 6b 0e c3 07 80 d6 b1 dc 00 30 +Ck- 6- 0-
001c d4 c2 e8 bc cd 1e 2f ac 5d 62 52 ff 7a 55 9a ba -.- -> JBR zu-
001d 46 1e 9c 1c 1a c1 e1 70 71 ac 51 f2 7e 64 42 66 F- p q- -o-~Bf-
001e 27 b5 89 05 40 fe c7 bz cf ba 82 48 c3 38 69 68 -.- -> n- K 81'

Packets: 78 - Dropped: 0 (0.0%) Profile: Default

Profile: Default

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:

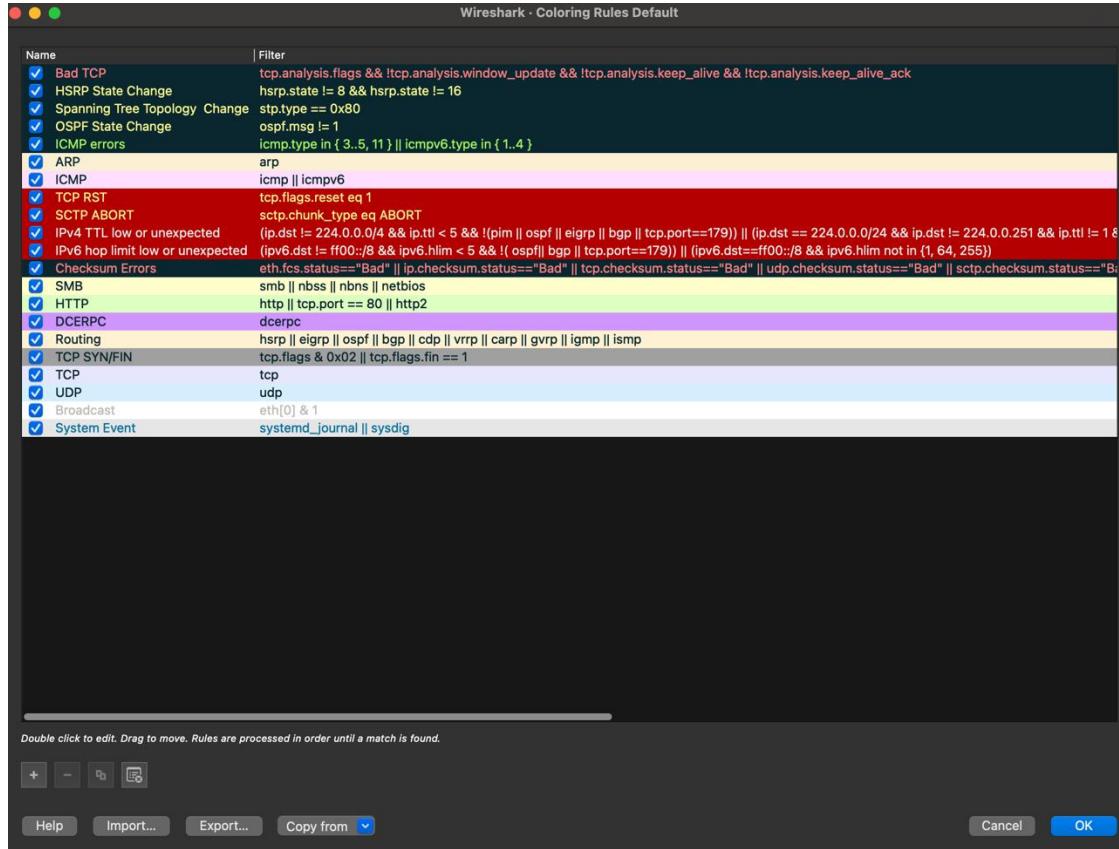
- Apply as Subtree
- Collapse Subtrees
- Expand All
- Collapse All
- Apply as Column **(highlighted)**
- QXK

The "Apply as Column" option is highlighted with a red box. Below the menu, the "Selected" column header is also highlighted with a red box.

Below the menu, the packet details, bytes, and timeline panes are visible, showing the selected packet's information.

- 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 lists several entries:

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'.

- 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

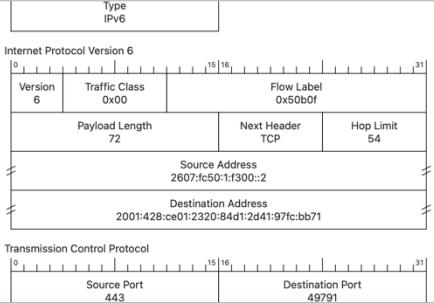
Help Preview Save All Close Save

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

Packet Diagrams

Packet Diagrams

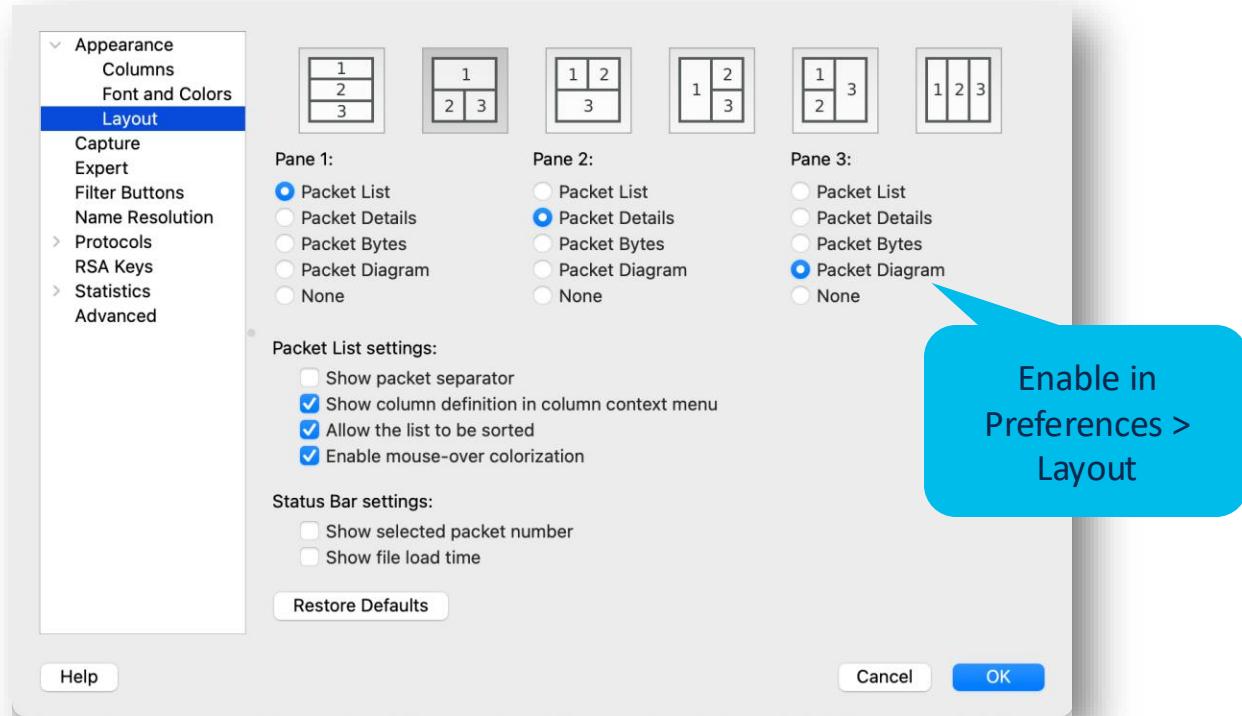
No.	Time	Src MAC	Dst MAC	Source	Destination	Protocol	Length	Info
402	10.9990..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	468	443 - 49791 [PSH, ACK] Seq=3715 Ack=518 Win=66304 Len=382 Tsvl=3527492959 TSec=518 Application Data, Application Data, Application Data
403	10.9990..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TLSv1.3	637	443 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=3518 Change Cipher Spec, Application Data
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=3518 Change Cipher Spec, Application Data
406	11.0059..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TLSv1.3	561	Application Data
407	11.0060..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01..	2607:fc50:1:f..	TLSv1.3	389	Application Data
408	11.0703..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	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..	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=130432 Len=0 Tsvl=2345773882 TSecr=5254 Application Data
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=1073 Application Data
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=1073 Application Data
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=1073 Application Data
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=5254 Application Data
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=9033 Application Data
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=1497 Application Data
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=10271 Application Data
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=11589 Application Data
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=12747 Application Data
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 (0c:60:4f:32:72:42), Dst: Apple_37:20:69 (bc:0d:74:37:20:69)								
Internet Protocol Version 6, Src: 2607:fc50:1:f300::2, Dst: 2001:428:ce01:2320:84d1:2d41:97fc:bcb0ff0100 = 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)								



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

New to Wireshark 3.4

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
20	0.454240	Apple_74:b0:67	Cisco_5f:05:f4	Prepare as Filter
21	0.456926	Apple_74:b0:67	Cisco_5f:05:f4	Conversation Filter
22	0.475223	Cisco_5f:05:f4	Apple_74:b0:67	Colorize Conversation
23	0.476287	Cisco_5f:05:f4	Apple_74:b0:67	SCTP

> Frame 17: 78 bytes on wire (624 bits), 78 bytes captured (624 bits)
> Ethernet II, Src: Apple_74:b0:67 (f8:4d:89:74:b0:67), Dst: Cisco_5f:05:f4 (08:00:27:00:00:04)
> Internet Protocol Version 4, Src: 10.116.79.233, Dst: 35.186.227
> Transmission Control Protocol, Src Port: 51128, Dst Port: 443, S

Follow

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

The screenshot shows the Wireshark interface with a specific stream selected. A blue callout points to the stream identifier "tcp.stream eq 1" at the top left. Another blue callout points to the assembly view on the right, which displays the reconstructed data bytes from the selected stream.

Filter on all packets from the stream...

...And assembles all data bytes in one screen

CP Stream (tcp.stream eq 1) · Wi-Fi: en0

tcp.stream eq 1

3.'...ij.5_DV..".....+./.....,0.
-g.sync.services.mozilla.com.....
".
..T@..&I.." Z.."v.K5.1...xW=(.|.[.=1.....+.....
..,0..XA,@V..&.....:..T.*..0R'.C.tybB_W\$.....
.....I..c..6)...u...*C.EH.<Y....<L8b.....G.J5.....0.3.....0..t..XJ...C\.....{3..t..+1..BjmnUp*y#,}.
4...{MK.....e}~P.....IDAY.I.(..XnRB.!.....m..6.5.....p.(..1.....[.....Pf..u.s@].....
.....hr.Y.....N.g..a8.)..2...Cbc3.'...ij.5_DV..(4...)3.\$... ..9...u.U.f.p.m..2.G.....
+...hr.Y.....D.g..f.m)...JC...RB.....
E%.....;..E...%..Ur.o...6X..HX..M...NGp.....5.....d..PCM.t..7.....9..Y.c.g.{.....
7.S..K...n0...G.....(BQ.....^.\s..2...(g...).%".....%SGC..k.+[V[...;Z...tdV..00i..22n..:e.W)..
5...m...u.R...i..ESx.....L..I.....
<08..e.....<-..7.\J..!9..q..U..[m:..<..@..0..d:.....x.....n..%3.....\$.....0f.e.'gf..,..,7....t0.
V...bs.....#..v...+.....Z..p.....4'=S.....w..4A'.....C3..U..1..F..%Z..N..I..g'.....H..V
G..g...k...0w(..."..g..g..Y..[..P..,..DM..V" [p1F..,..60..,..8)...x...y.....b..[..@H..K'.....~.....
4..H..q..AIn.....(1...0...T9..1..6..(8a..,..P.....f.....
.G...,.8u..5.Y..J..A..l..,"..).....+ST..x..0...{gA..4.....3@..6...D#d..,..f.....
...,.y<..>A?C?....z{..h..q.....
ZHI...@#Z..U|C..s...f..@!B.....c.....3..v^0..KA...n..b..x..w..J..l..G..,..0..!..H..B..;..-...
..c..5..&2i.....I..7.....5..2K..s.....+qD0..Y".....4..1.....2..1..f..~..D..R..p^..9A
...C.....J..JR..,"..c)'..v1..2b..f..b..b..\$..%>T.....1.....>..k".
...%+..s..v..=.....{.I..28.....y..Z..l.....I..Dm..g..t#..N%..E.....[.....z...*...b..p..],n9..(x..Q.....
0...D...H..j..-2..DK.....g..-..j..o..B..I..,..lv..,..X..5E.....2..3...M..omGN..a..o.....
8V.....xz..6BY.....6..=..U..,..7.#.....
2..7..?..#..v.....M(^g..F..r..Wy6.....y.....!,..#..<..n..f..,".....U..,..5.....
2..,..x..r..,"..y.....@..S..2..U2S.....j..-h..j.....>..?..8u..A..I..u.....0nx5.....
(m.....T..Z|.....A..W.....x..0..#.....3..oo..o.....,".....e<..\$.....q.....vM.....
a..i.....l..q..@..B..,..C..l.....\$..I..l..b..A..,..50..g..-].....[....._..].....WP..@..,..|.....>..-..u..j.....
9..V..y.....Akt.....#.....0062.....
hf..bn1..,"..o..u..(\..)Y.....5.....t.....C.....q...
P..Z..1.....,.....x..8%.....,.....1.....
.1'..,..f..70B..r..5V..,.....\$..p..,..0.....,..h..z..i..,..d..L..z..,.....L..q..y..B..,..l..,..,..@..-.....a..^w..1..9.....H..W..
2'..,.....#.....~..6..W..,..,..{C..2..,..'19Y..V..,..,..Y..,..5..f..n..R..,.....(+..,..p..Ap..?..h..06..y..d..
0..9..+,.....P..a..,..,..r..G..N'.....0..N..p..,..#..<..s..M..0..,..{..c..,..t..,..i..-l..2..)2S..,.....

Packet 29. 10 client pkts, 16 server pkts, 10 turns. Click to select.

Entire conversation (7742 bytes) Show data as ASCII Stream 1

Find: Find Next

Help Filter Out This Stream Print Save as... Back Close

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

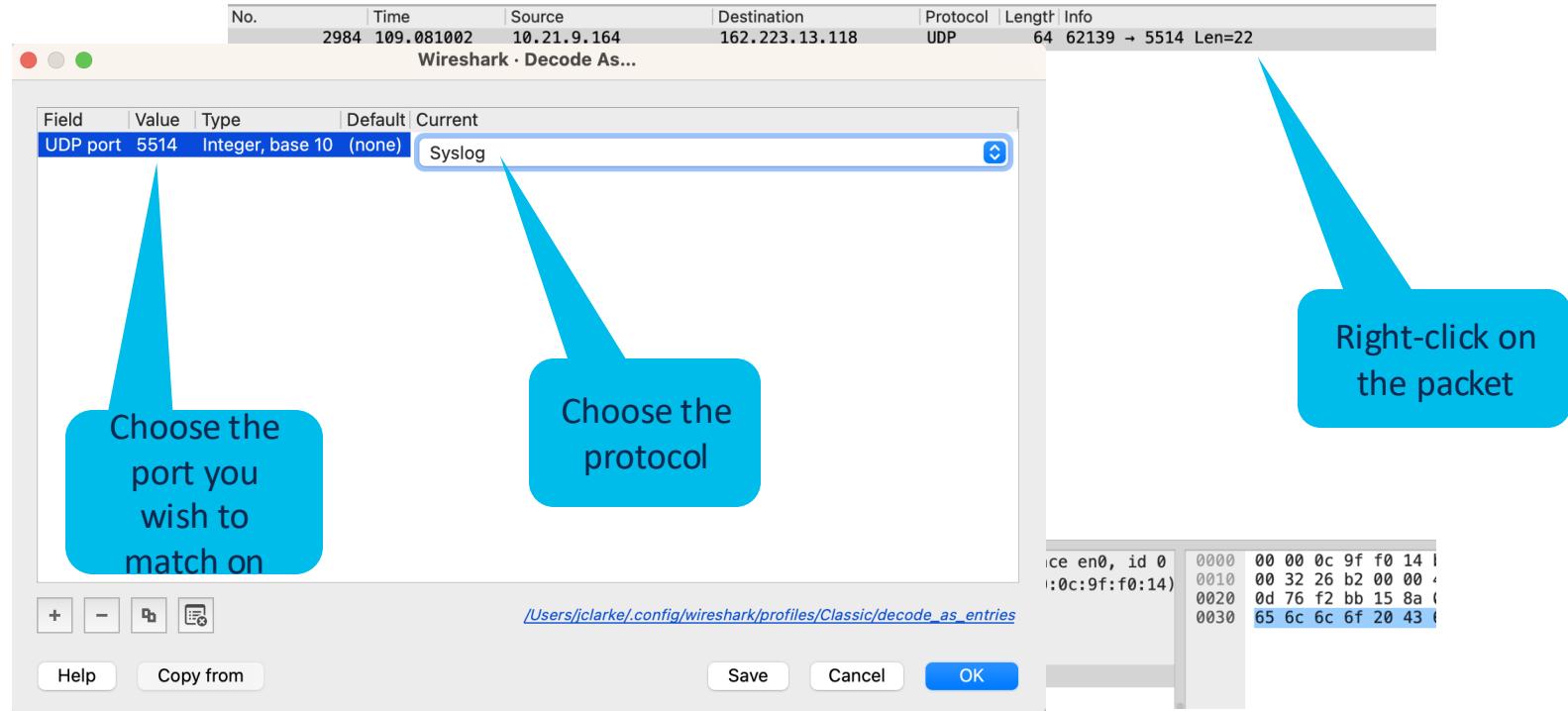
Let's say you have
a data stream
using non-
standard ports.
You still want to
make use of
wireshark's
dissectors.

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...



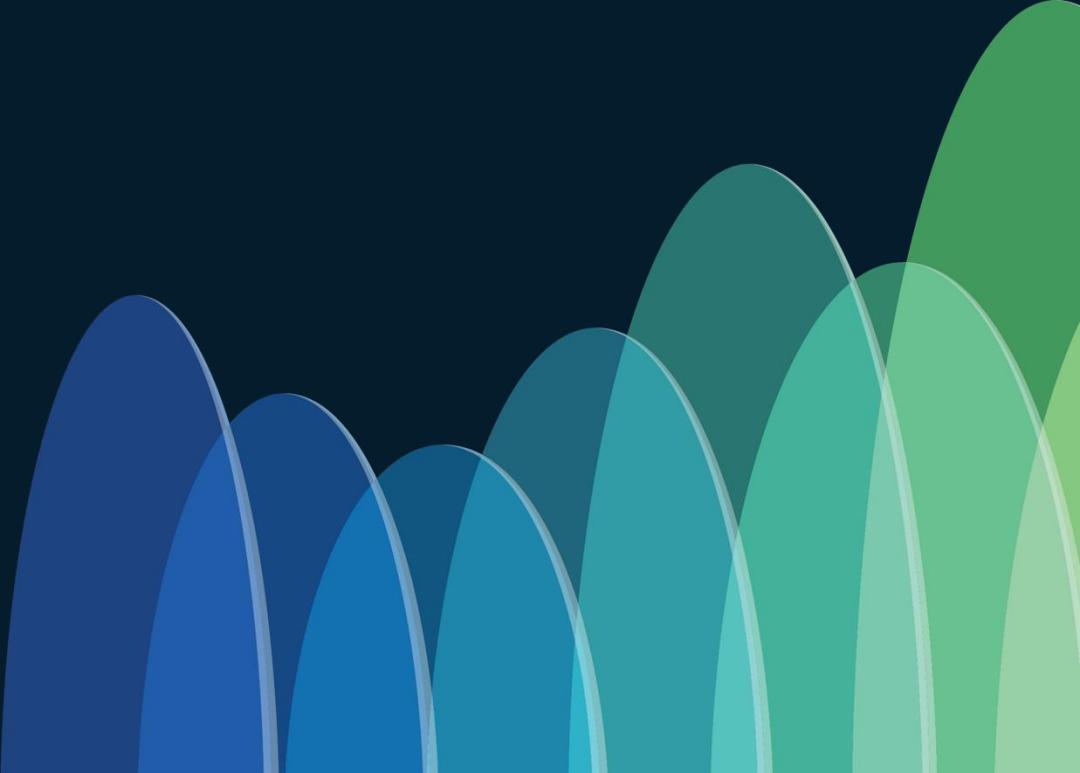
Decode As...

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

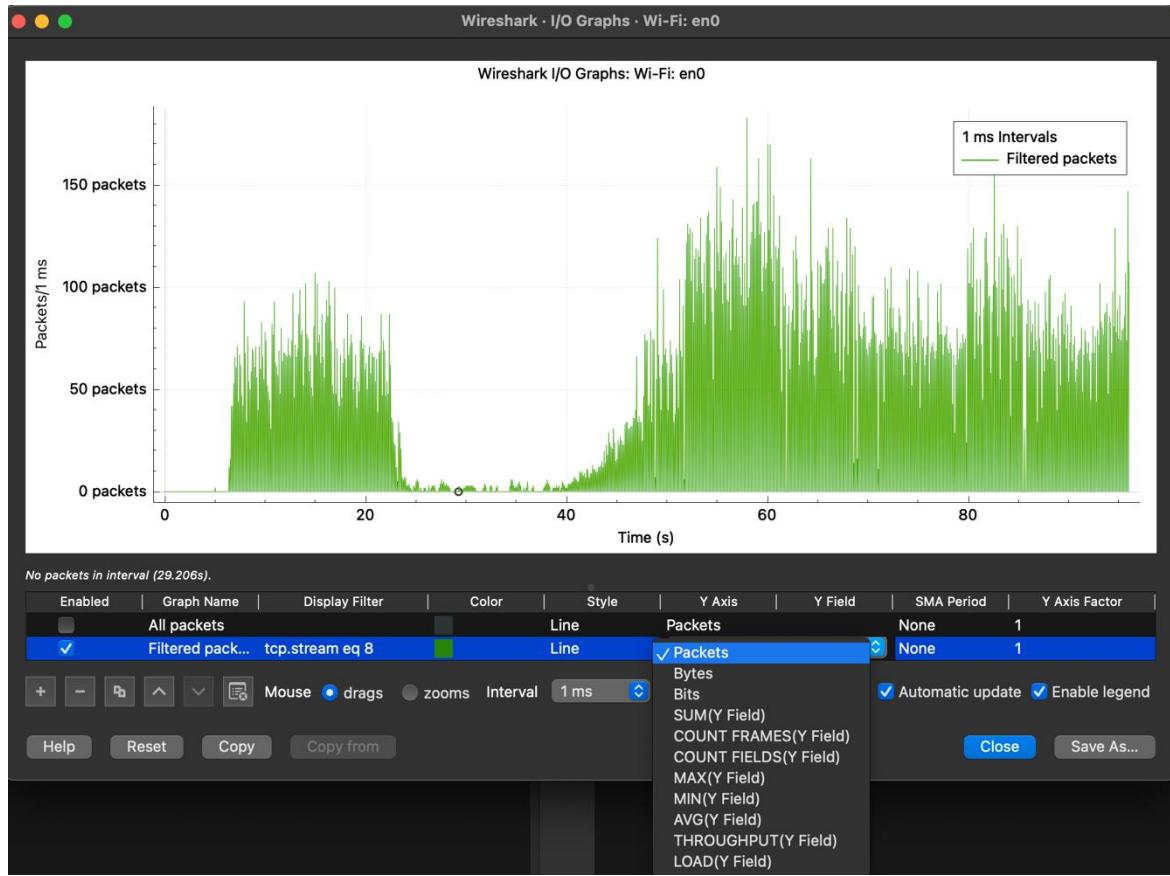
```
> Frame 2984: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface en0, id 0
> Ethernet II, Src: Apple_37:20:69 (bc:d0:74:37:20:69), Dst: Cisco_9f:f0:14 (00:00:0c:9f:f0:14)
> Internet Protocol Version 4, Src: 10.21.9.164, Dst: 162.223.13.118
> User Datagram Protocol, Src Port: 62139, 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

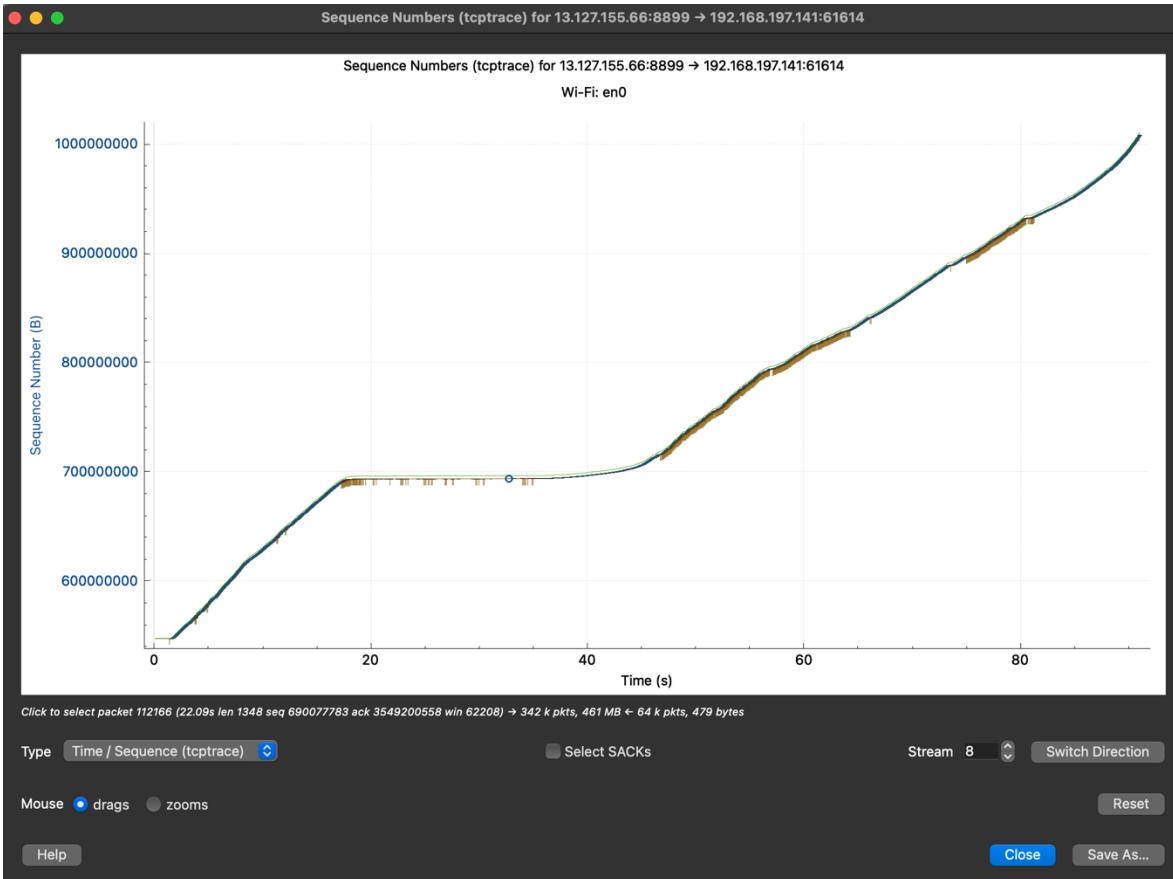


Input/Output (I/O) graphs



- 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	—	—	—	—

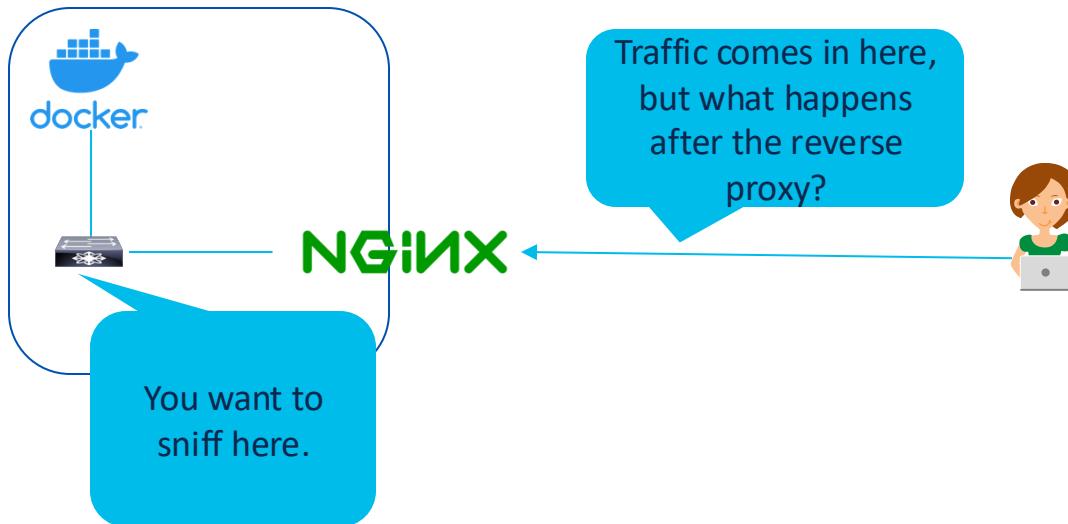
Enable promiscuous mode on all interfaces Manage Interfaces...

Capture filter for selected interfaces: Compile BPFs

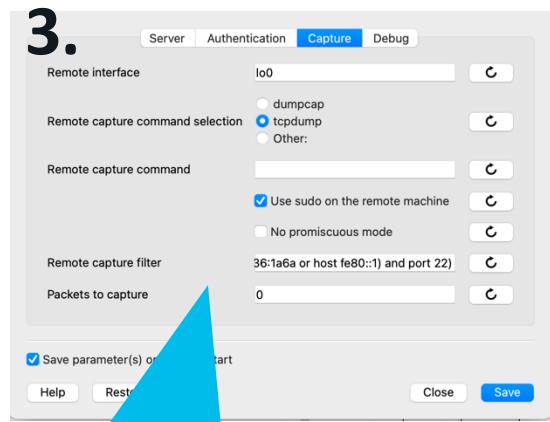
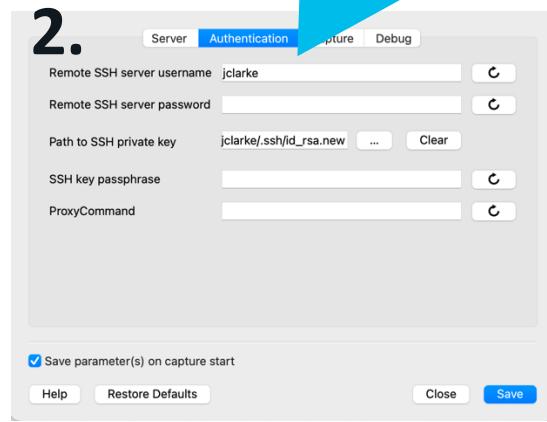
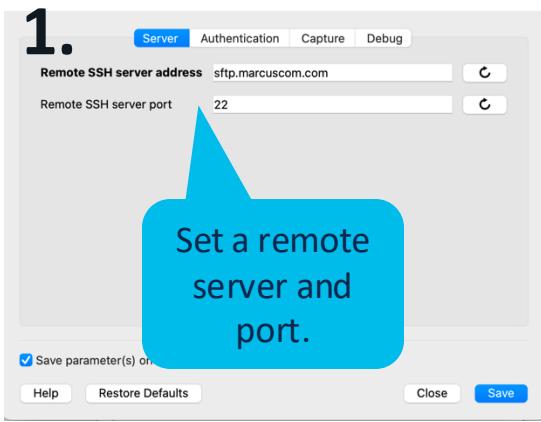
Help Close Start

- 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!

```
.....2.j.$.'....%Tr..ae.\.4EQ.  
WV.>..2...N.Pu.;.U...?...V...'+/.,.,.,0.  
...../.5.....www.marcuscom.com.....  
.....#....h2.http/1.1.....  
.....3.K.i...m.-_7m...a\l...u...K.#).0m0d...A.Rb.....x.M.....^'.1.7.X.J.....S..t...C?<.be.).M8)...e...+.....  
.....-.-.-.-.-.-@.....  
.....[.....a..17.8j...>..2....N.Pu.;.U...?...V...+...3.$...=..._Ru4.S..)d..y!..H.....*k.....j.&I...+l.|.....y.....y.....F...  
1.R...t.....0...d.B.Hco.....]K'7.R..H1id..B...0.....Ny..2...H..F..<...#..`..~.../d..*.$.._..N..r..x..v.c..C./k..y!.7.c;..9...P.).....%S..[...  
4.G.H.:T..'.V...'DXw6.....N$V.m..<.%...&..5.9..1~..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^.....J.....&(.d...9.p..l.)...{.0.....n.11.|.R7.j|..z'|..L|..9Bb.;  
1.N^..t'.....?...|.....^c.y.a1..v1.Z=..J...t|......4...P6V...@.&...c.z...9...].B>..X..~..]..R...!..J...d.4.L.....E.\T.!..  
0'.A...n...Wm..).v...z.I/[p.C[..9...~..].4C  
.....K2...i.C.=?..T..t..0x..0...5'G.s..#.a...0...(...NSu.)...  
c.[...t...~(.ZL.T.AP.....Y...I...f...<...tpe..t.e..=...)...q.0$..c+3c.|..`I...4F)'.....c/..1*mq...h....I..Cr7...  
.....Z..0#..a..s...z...~...b..EE/1..j(a..e.s...@rV.|..V.Z\..D.G...-..b.....6Yv.....H.q.....KVC.t..  
.....'.....^..8D..T..(v6..$/^..C...A...A.....V..R.Ics.DM..RwyFv.,>.....\0..!...  
e.e...Lc..oFU..W...I...5...j..WL..jw.j...a...'.....E..f'.8t..h...~x.b..t..EM7LS..6..)...)V..P*..r.].....1.n.A..0.....[..h.U.s..h.  
.....`w..G..~..`A..F..Ph..V..4..9Z...A  
.0..K2...i.C.=?..T..t..0x..0...5'G.s..#.a...0...(...NSu.)...  
kvvi=qSl.mT..Y.....M...A%..K...0...{.J...A..12..0W..KN.....<...D...6..0!..!...  
.....fM..a...o...C.m.!<1...Y$&..Ui..g.2...(<...g...GD=<|...A...L.v$0.m.....;.....0...I..G^..d..".....I..v=.....  
2.zp...../..Gg0..d1..@m.l..p...L..j9..2...n.2)..x...C...Y..O..Z..I..M..4..Bmx..1GINF..3..4..~..b+..J...  
t..x..p...{...].5ZG.E'.u..yt..V..  
.....1..w..0..  
.....of...A..>x..h..x..2..X0.a..h..N..0...Z)...[..B...)]...p.v.s.Dj  
.....W..n..  
.....y..f...E..^m..A..b..u..T..L..D....ld.w.."  
Bg9..C..U..x..%Z..  
.....J..x..A...*..#..KPlq.....<..l1..<...[.....Yg..)....A..+(.....B..n..Z..P..)....2..841..X..l..c.....W..V..DA.....;.....r..0R|..d*..>  
.....6f..p..c...D..Cw...!..<(j4...r..Q...a..0..  
x..72..D..g..I..E...B..T..4.....%..Tw..d...G..P:#..3...N..6..o..A.....i..W*5(..i...0..)C..7.....<...!C.....5"....FAt.o..W..n..X.....|....  
4..S..p..*..R..:..T..1..Id..V..w[.....Vt..0..E..S...3..)P..k..u..Foy..)m..o..o..=%>P=w..%..b..B..  
[y..$...p...T..+..f..dB..t..#y..1..@<..x..4..h@W..k...0..Y.....U..61..Z..q.....7W..2e..a...Zt.....K..L..$.:.B#.)...a..K..85...p4W..!  
Uj..L..V..V..P..ZgR..AS..ogh?..(M9..`..P..4..HR..K..F..0..u..g...Th..T..L..m..=H..4g../.cf..s...T../.i..3h..G.  
.....\..#..y..r5...4..p..C.....d..1td  
.....@nb..F..S..X  
9...t..  
.....G..5.....j0...3=...%...1..3..0..)D...0..>C..*..1..c..Sk..3..L..B..1..3Be...*..h&64..(..d..v..h2..T.  
8..6..h...*ft...r...,.U...-..I)...V..E..S..G...z^.._61..6j..BB..hu..A...>...n..".Dq..Hi.....Bg..066..0...^..&..|..)....0K..wV..c.....^...<.....5  
.....?..A..Gu..ve..M..*..[W..^..{\..Gh..E#R..aj..C..z..=;)...S..p..y..)2..0...b..%..6..c..m..%.2..#..3..M..h..[..u..a..a..>...J..a..K..7.).  
5...5...,,..E..&..5H..Yp..1..y..0..JR..1..1..)"...3p..H..16..>..3..1..I..N..58..Cs..1L..L..F..-..P..M..=e..j..7..s..[uXN..Zh..i..t..  
(_..xn..Ig..Ag.._f..g..0..)I..Ibe3..246..<..0..<..~..1..S..:..W.....0..w..I..R..<..P..CG).  
.....k..E..*..?Fz..ud..YAT..V..&G(N.._9..4p..G..$T..o!..)p..C.....m..,..D..eld..a..H..$..4)..a...p..@.....r..qlj..IG.  
7...3...,\..>..c..o..Et..EZ..0..1..5k89e..9..j..-'..EDCrl..,..d0..(....S..Vo..18..R..ahJ6q..,...,s..K..Ri..^..>..@..0..u..!..I..o...A..~..cdXX..3..kli..J..=..S..t..{..p..N.  
90..&..h..Rm..d..1  
.....J..0sR..m..uc..0...t.u..u..  
5 client pkts, 603 server pkts, 7 turns.
```

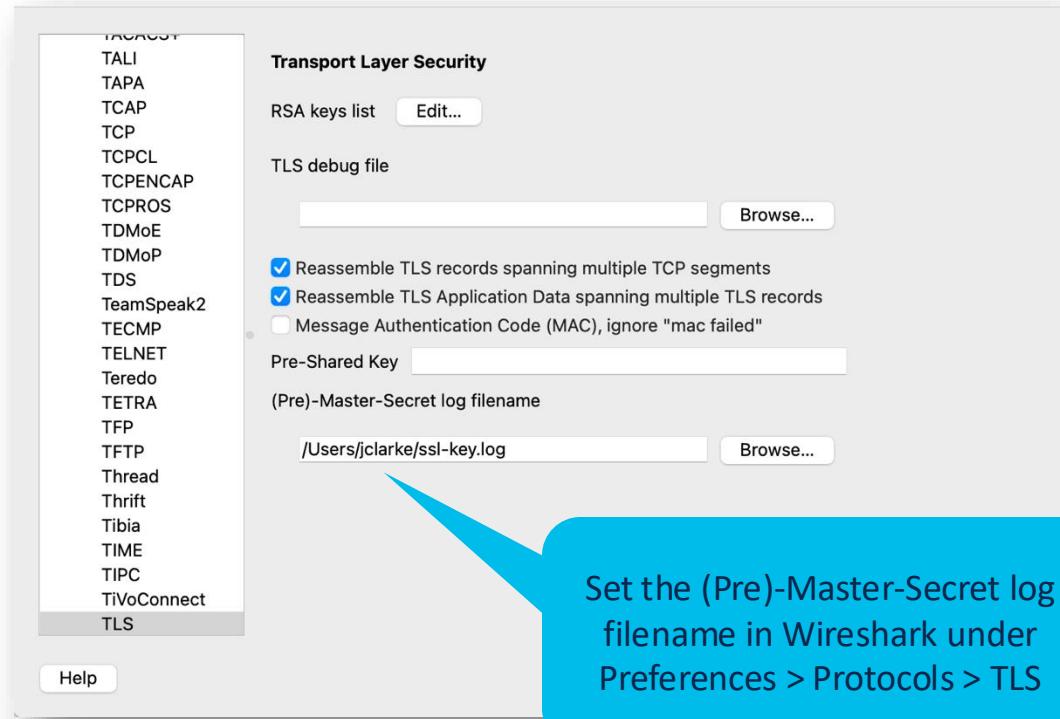
Well this isn't
terribly useful...

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
```

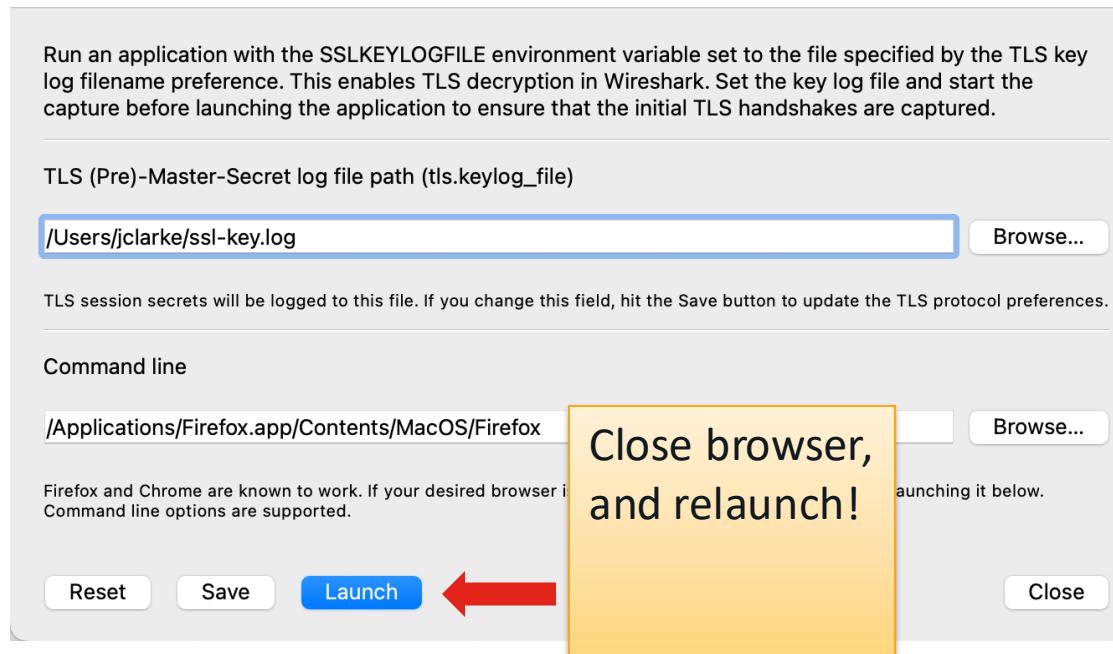
Decrypt the Things!



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

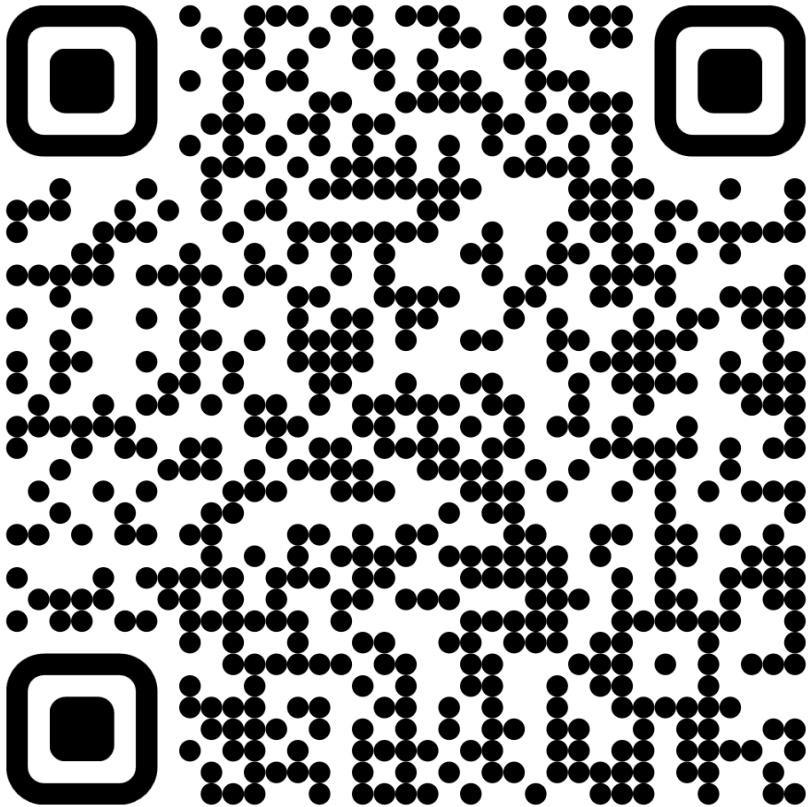
<!DOCTYPE html>
<html>
<head data-suburl="/git">
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <meta http-equiv="X-UA-Compatible" content="IE=edge"/>
    <meta name="author" content="Gogs" />
    <meta name="description" content="Gogs is a painless self-hosted Git service" />
    <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