

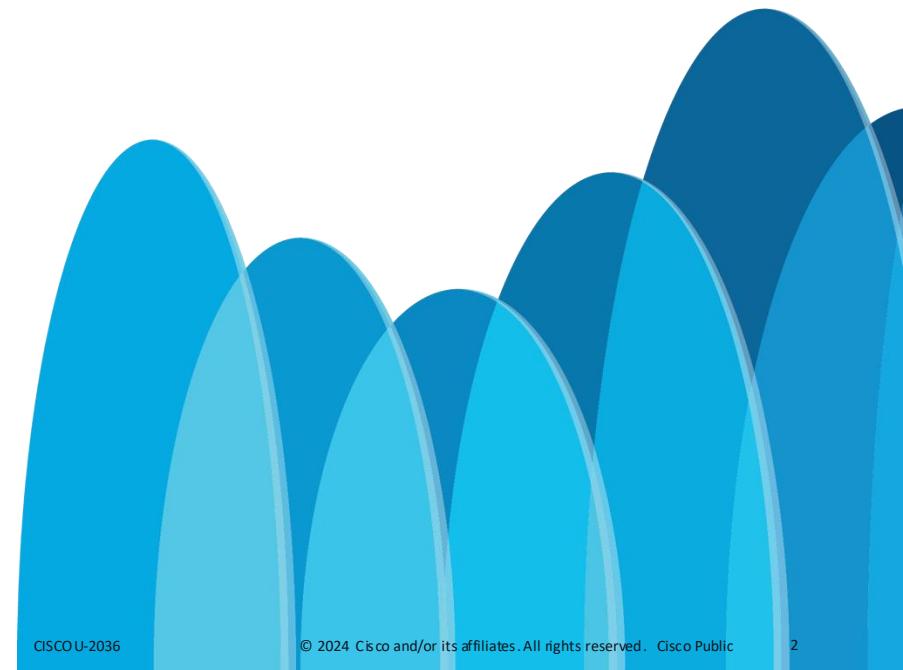


Become a network doctor using packet captures and Wireshark

Prapanch Ramamoorthy
Principal Engineer, CX Engineering
CISCOU-2036

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: B2:52:cfa:b3:34 (B2:52:cfa: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	Details
1	2024-11-04	16:08:08.005519	52.223.1.163	192.168.197.141	TLSv1.2	547	Application Data
2	2024-11-04	16:08:08.005614	192.168.197.141	52.223.1.163	TLSv1.2	66	57839 -> 443 [ACK] Seq=2279766114 Ack=1049325794 Win=2040 Len=0 TStamp=4203520823 TSect=
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 TSect=
5	2024-11-04	16:08:08.252185	99.83.250.143	192.168.197.141	TCP	66	443 -> 58188 [ACK] Seq=1641673934 Ack=2893573871 Win=122 Len=0 TStamp=3886905425 TSect=
6	2024-11-04	16:08:08.351286	192.168.197.141	20.189.173.8	TLSv1.2	472	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	144	57772 -> 443 [ACK] Seq=1071932827 Ack=269559361 Win=2048 Len=1348 TStamp=2268887767 TSect=
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	16:08:08.542337	52.223.1.163	192.168.197.141	TCP	144	443 -> 57839 [ACK] Seq=1049325794 Ack=2279766279 Win=1954 Len=1348 TStamp=1577654247 TSect=
11	2024-11-04	16:08:08.542345	52.223.1.163	192.168.197.141	TLSv1.2	1047	Application Data
12	2024-11-04	16:08:08.542348	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 TStamp=4203521301 TSect=
14	2024-11-04	16:08:08.631847	2620:lec:8fa:10	2401:4900:9006:92d:546:e6bf:94...	TCP	144	443 -> 58207 [ACK] Seq=853548177 Ack=3989515143 Win=16388 Len=1340 [TCP PDU reassembled]
15	2024-11-04	16:08:08.631853	2620:lec:8fa:10	2401:4900:9006:92d:546:e6bf:94...	TLSv1.2	306	Application Data
16	2024-11-04	16:08:08.631855	2620:lec:8fa:10	2401:4900:9006:92d:546:e6bf:94...	TLSv1.2	105	Application Data
17	2024-11-04	16:08:08.631147	2401:4900:9006:92d:546:e6bf:940...	2620:lec:8fa:10	TCP	74	58207 -> 443 [ACK] Seq=3989515143 Ack=853549780 Win=4070 Len=0
18	2024-11-04	16:08:08.631808	20.189.173.8	192.168.197.141	TCP	66	443 -> 57772 [ACK] Seq=269559361 Ack=1071932827 Win=16386 TStamp=15830986 TSect=2:
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 TStamp=15830990 TSect=2:
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 TStamp=226888063 TSect=1:
22	2024-11-04	16:08:08.666859	2401:4900:9006:92d:546:e6bf:940...	2620:lec:8fa:10	TLSv1.2	113	Application Data
23	2024-11-04	16:08:08.670665	2401:4900:9006:92d:546:e6bf:940...	2620:lec:8fa:10	TLSv1.2	98	Application Data
24	2024-11-04	16:08:08.671791	2401:4900:9006:92d:546:e6bf:940...	2620:lec:8fa:10	TCP	74	58207 -> 443 [FIN, ACK] Seq=3989515206 Ack=853549780 Win=4096 Len=0
25	2024-11-04	16:08:08.695728	2620:lec:8fa:10	2401:4900:9006:92d:546:e6bf:94...	TCP	74	443 -> 58207 [ACK] Seq=853549780 Ack=3989515182 Win=16388 Len=0

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)
- Q(X) (highlighted with a red box)

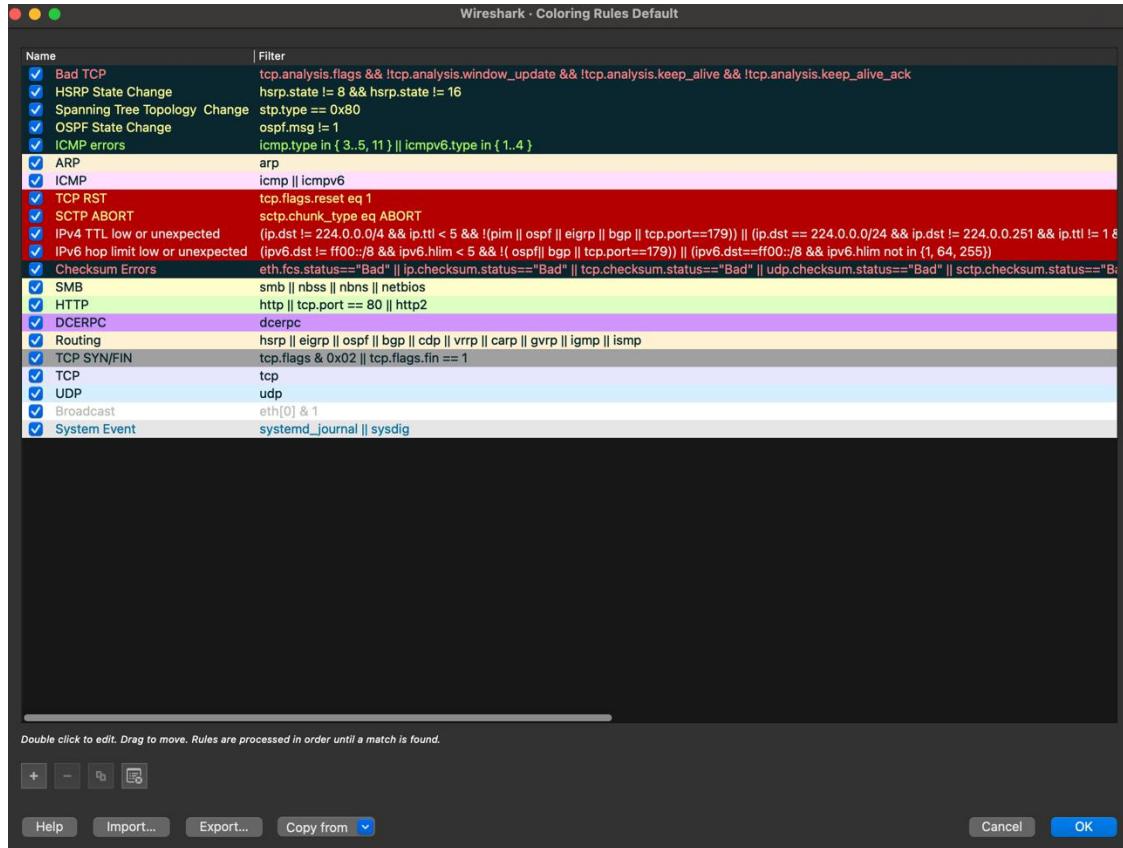
The main pane displays the packet details for the selected frame 12. The selected packet is a TCP segment from port 54327 to port 197.141. The details pane shows the following fields:

Field	Value
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]	

The bytes pane shows the raw hex and ASCII data for the selected packet.

- 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'. Below these are buttons for 'Copy', 'Follow Stream...', and 'Graph...'. A protocol filter section shows 'Protocol' selected, with checkboxes for 'Bluetooth', 'BPv7', 'DCCP', 'Ethernet' (which is checked), 'FC', 'FDDI', 'IEEE 802.11', 'IEEE 802.15.4', and 'IPv4' (which is checked). 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

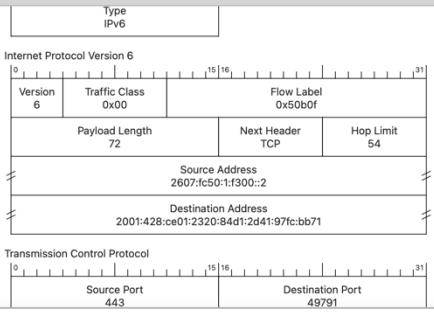
Help Preview Save All Close Save

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

Packet Diagrams

Packet Diagrams

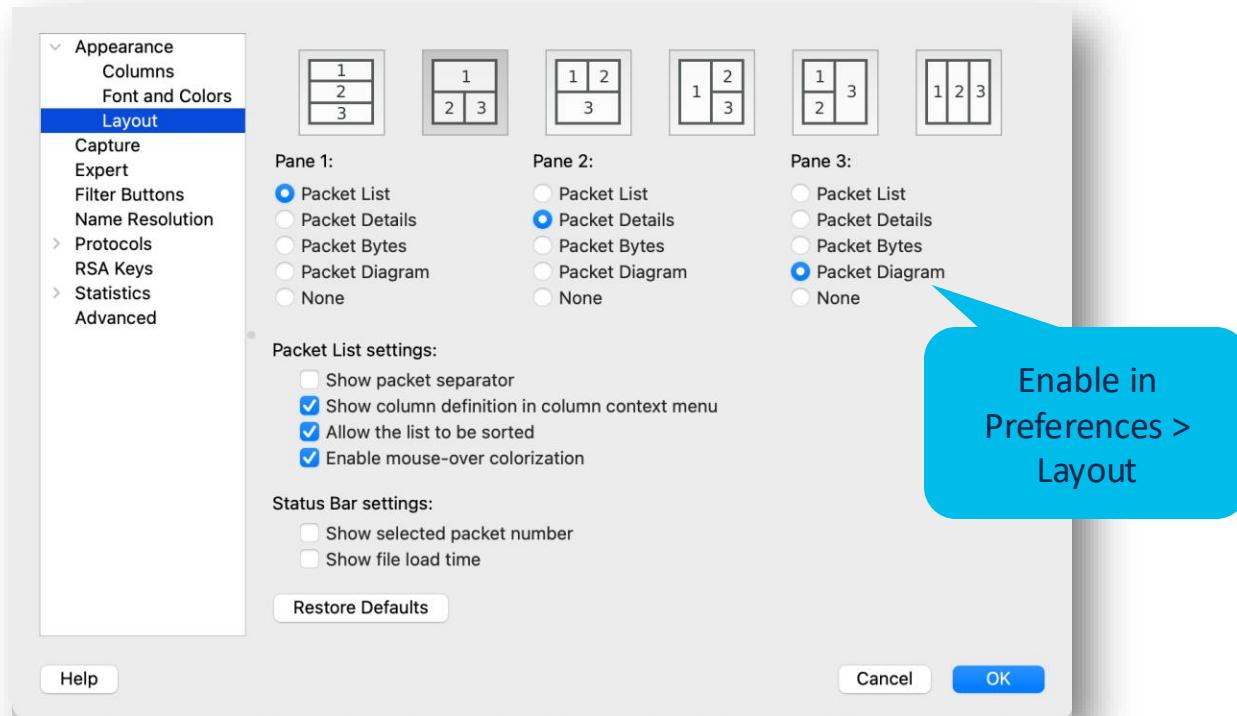
No.	Time	Src MAC	Dst MAC	Source	Destination	Protocol	Length	Info
402	10.9990..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f..	2001:428:ce01..	TCP	468	443 - 49791 [PSH, ACK] Seq=3715 Ack=518 Win=66304 Len=382 Tsvl=3527492959 TSec=518 Application Data, Application Data, Application Data
403	10.9990..	Cisco_32:72:42	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 0010 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

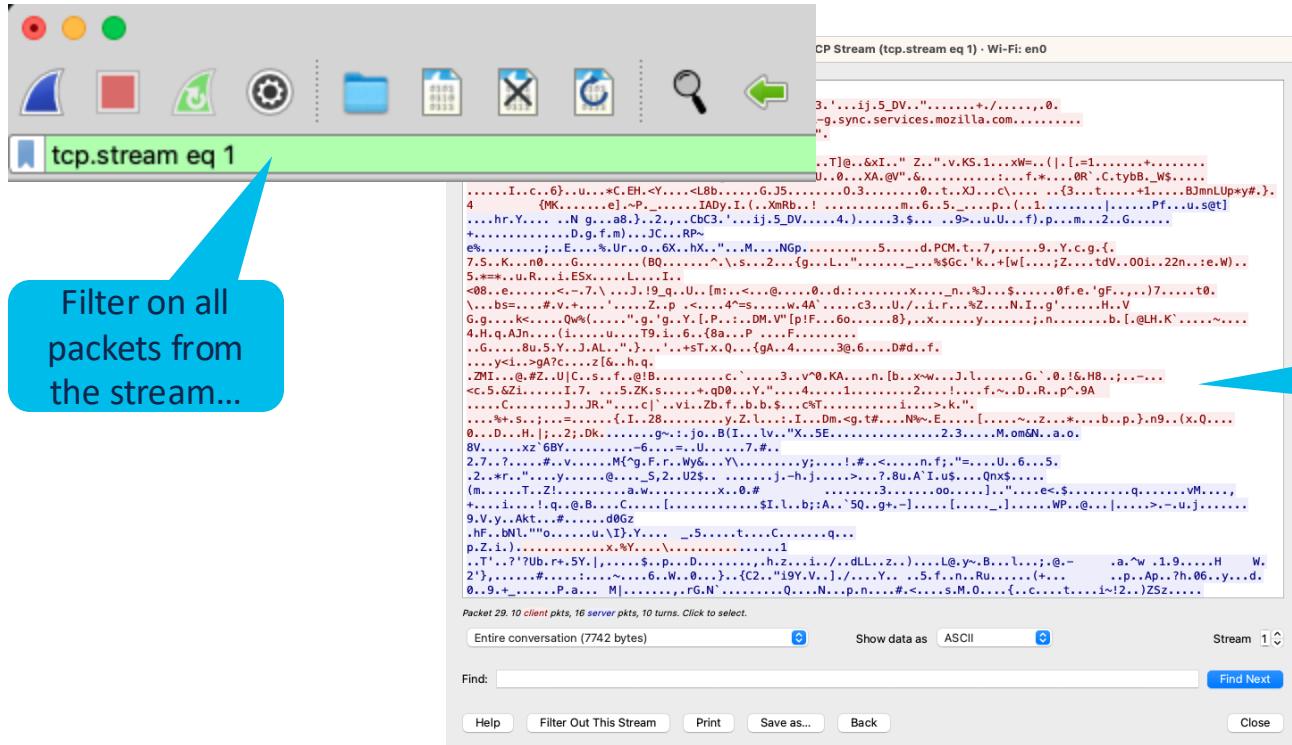
Following Streams

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 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



isco Live!

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

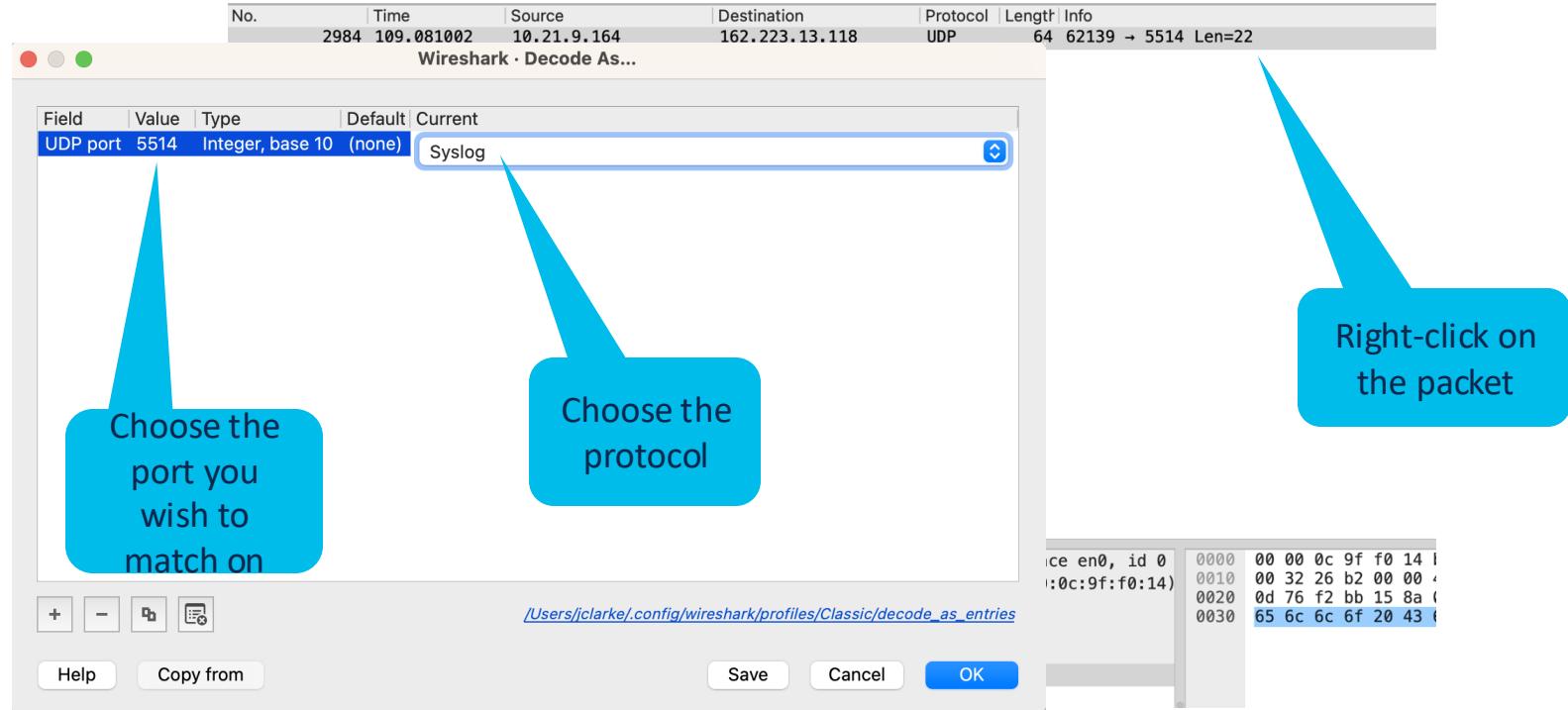
Let's say you have a data stream using non-standard ports. You still want to make use of wireshark's dissectors.

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...



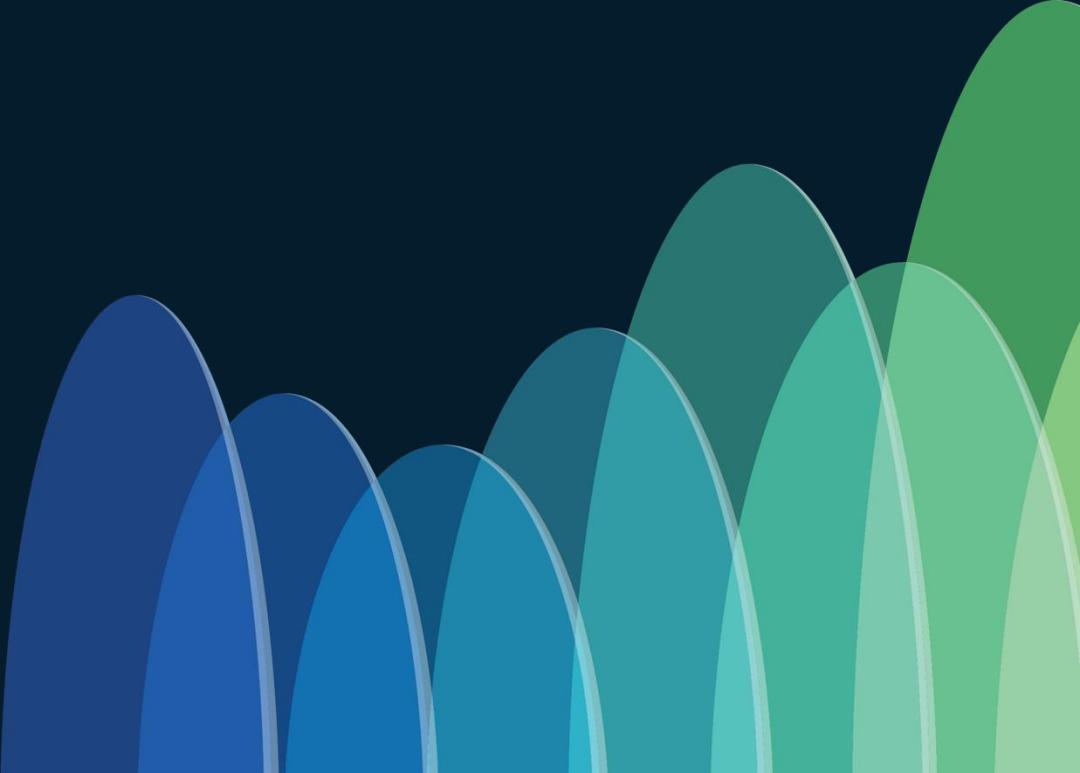
Decode As...

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

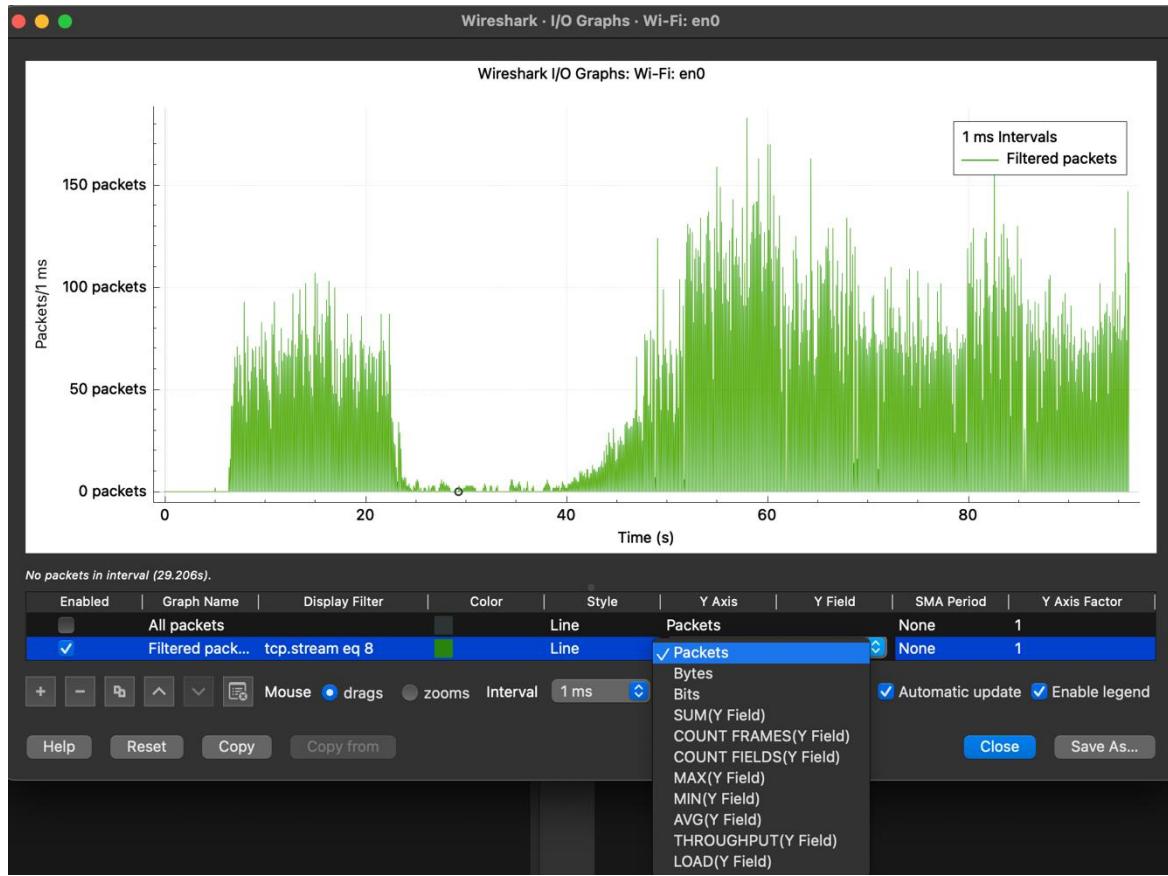
```
> Frame 2984: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface en0, id 0
> Ethernet II, Src: Apple_37:20:69 (bc:d0:74:37:20:69), Dst: Cisco_9f:f0:14 (00:00:0c:9f:f0:14)
> Internet Protocol Version 4, Src: 10.21.9.164, Dst: 162.223.13.118
> User Datagram Protocol, Src Port: 62139,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

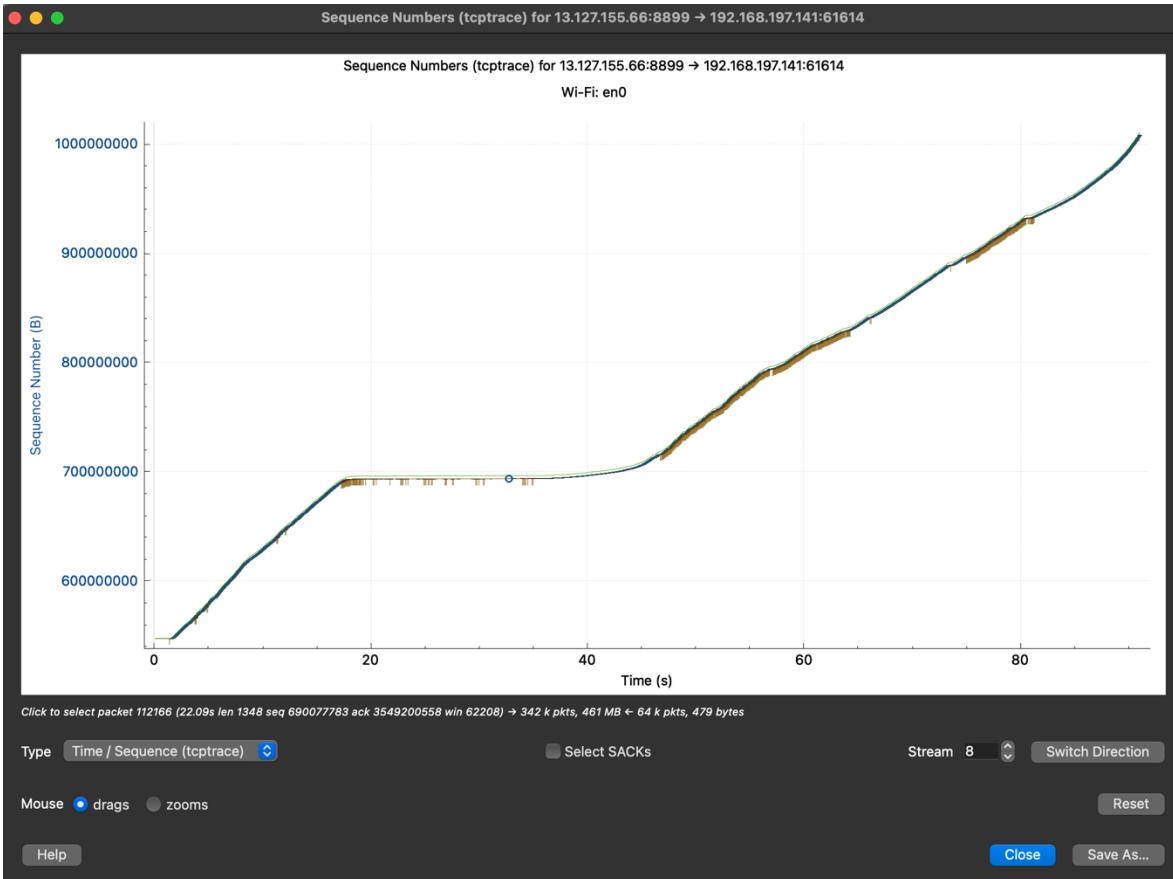


Input/Output (I/O) graphs



- 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	—	—	—	—

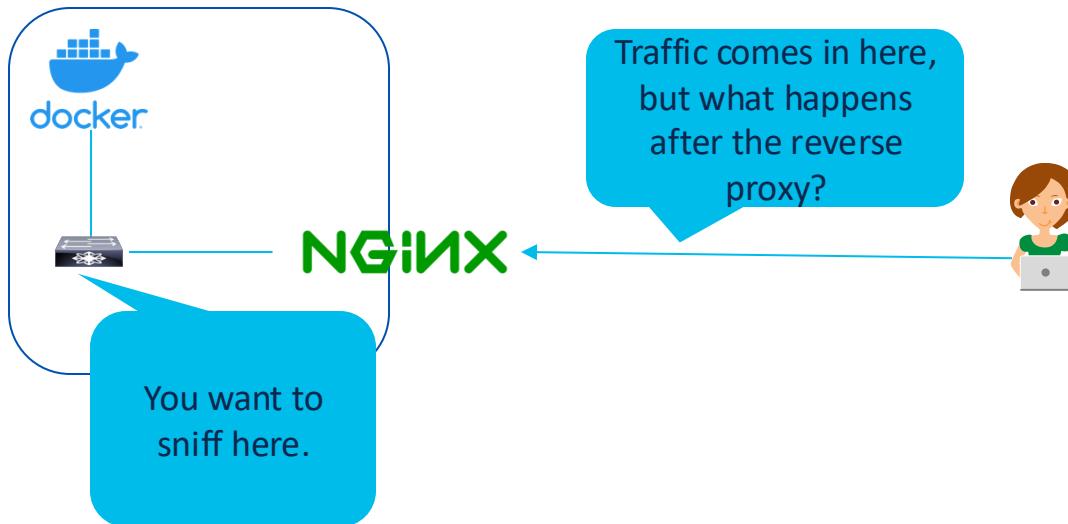
Enable promiscuous mode on all interfaces Manage Interfaces...

Capture filter for selected interfaces: Compile BPFs

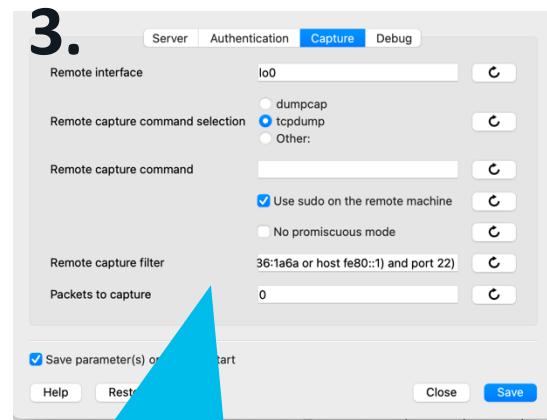
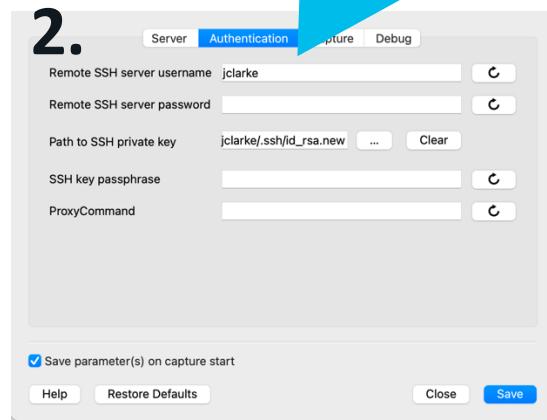
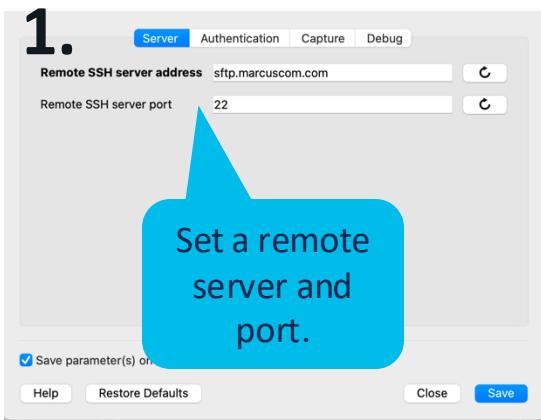
Help Close Start

- 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..<...#..~..b..~..|[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.eC..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^.....0..0edclx..J..&(.d..9.p..l..){.0 ..n.11..R7..j..z'..L..98B..;  
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..~..f..~..[.ZL..T..AP..Y..I..f..<..]..tpe..t..(=..)....q..0$..c..3c..)|..I..,4F)..c/..1*..mq....h....I..Cr7....  
..Z..0#..a..s..z..~..b..EE..1..j(a..e..s..@..rv..|..V..Z..D..G..~..b..~..6Y..H.q..KVC.t..  
.....^..8D..T..{v6..$/..C..A..A..V..R..Ics..DM..RwyFv..,>..`..!...  
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..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!..!..  
..f..m..a..o..C..m..!..s<..,..Y$&..Ui..g..2..<..g..(....GD..=<|..A..L..v$0..m..;....0..,..I..6^..d..\"....I..=v..  
2.zp...../..G0..d1..@..m..l..p..L..J..9..2..n..2..)....x..C..Y..O..Z..I..M..4..Bmx..1GINF..3..4..~..b..+,..J..  
t..x..p..{..]..5Z..E..u..yt..V..  
..1..w..0..  
..0..of..A..>..x..H..x..2..X..0..a..H..N..0..Z..)[..B..]....p.v..s..dj  
..W..n..  
..y..f..E..^m..A..b..u..T..L..D....ld..w.."  
#9g..C..U..x..%Z..  
J..x..A..*..#..KPlq.....<..l1..<..[....Yg..)....A..+(....B..n..Z..P..)....2..841..X..l..c.....W..V..DA.....r..0R..|..d..>..  
6..f..p..c..!..D..Cw..!..<(4..r..Q..a..0..  
x..72..D..g..I..E..B..T..4..%..Tw..d..G..P:#..3..N..6..o..A..i..W*S(..i..0..)..C..7..<..!..C ..5"....FAt..o..W..n..X..  
4..S..p..*..R..:..1..Id..V..w..V..t..O..E..S..3..P..k..u..Foy..)....m..o..=%>P=w..%..b..B..  
[y..$..p..T..+..f..dB..t..#..1..@..<..x..4..h@W..k..0..Y..U..61..Z..q.._7W..2e..a..Zt..K..L..$.:.B#.)..a..K..85..p4W..!  
U..L..V..V..P..ZgR..AS..ogh?..{M9.._..P..4..HR..K..F..0..u..g..Th..T..L..m..=..H..4g../.cf..s..,..T.. /..i..3h..G..  
..,\..#..y..r5..4..p..C..d..1td  
..@b..F..S..X  
9..t..  
..G..5.....j..0..3=..%..1..3..0..)....0..>..C..*..1..c..Sk..3..L..B..1..3Be..*..h*64..(..D..dv..h2..T..  
8..6..h..*ft..r..,..U..-..I..).....V..E..S..G..z^.._61..6j..BB..hu..A..>..n..".Dq..Hi..,..Bg..066..0..,..^..&..|..)....0K..,..w0..c..,..^..<..,..5  
?..A..GU..ve..M..*..[W..^..{\..Gh..E#R..aj..C..z..=;..)sp..y..)....2..0..,..b..%,..6..c..m..,..2..#..3..o..h..[..u..,..a..>..J..a..,..K..7..).  
5..5..s..,..E..,..5H..Yp..l..y..0..JR..1..1..)....3p..,..H..16..>..3..1..I..N..58..,..Cs..1L..L..F..-..P..,..M..=..e..j..,..7..s..[uXN..Zh..i..t..  
(..xn..Ig..Ag.._..f..g..0..)....I..Ib..3..246..<../..o..<..~..l..,..S..,..W..,..0..w..I..R..,..<..P..CG..  
.....k..E..*..?Fz..ud..YAT..V..&N..9..4p..G..$T..o!..;..p..C..,..m..,..D..eld..I..R..,..<..P..CG..  
7..3..,\..>..c..0..Et..EZ..0..,..5k89e..9..j..-..ECDrl..,..d0..,..(....S..Vo..18..R..ahJ6q..,..s..K..Ri..^..>..@..,..0..u..!.I..o..,..A..~..cdXX..,..3..kli..J..,..S..t..{..p..N..  
90..,..&..,..e\$..E..A..,..1..E..,..a..0..,..#..W..,..(..6..),..4..K..  
SL..H..$,..Rm..,..d..1..  
.....J..0sR..m..uc..,..0..,..t..u..u..  
5 client pkts, 603 server pkts, 7 turns.
```

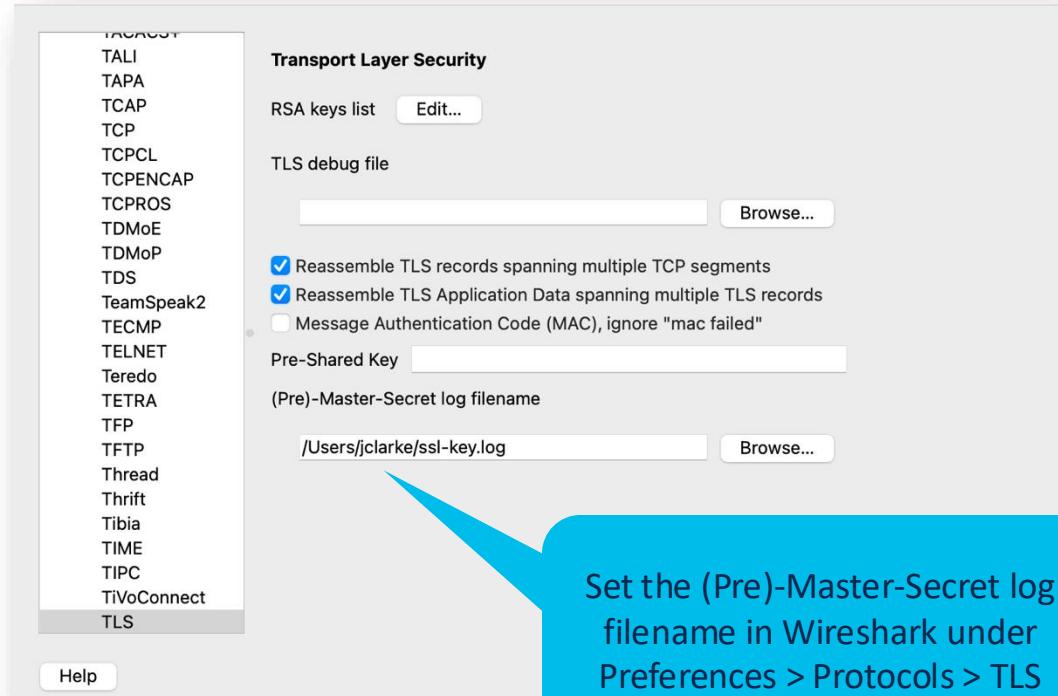
Well this isn't
terribly useful...

Decrypt the Things!

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

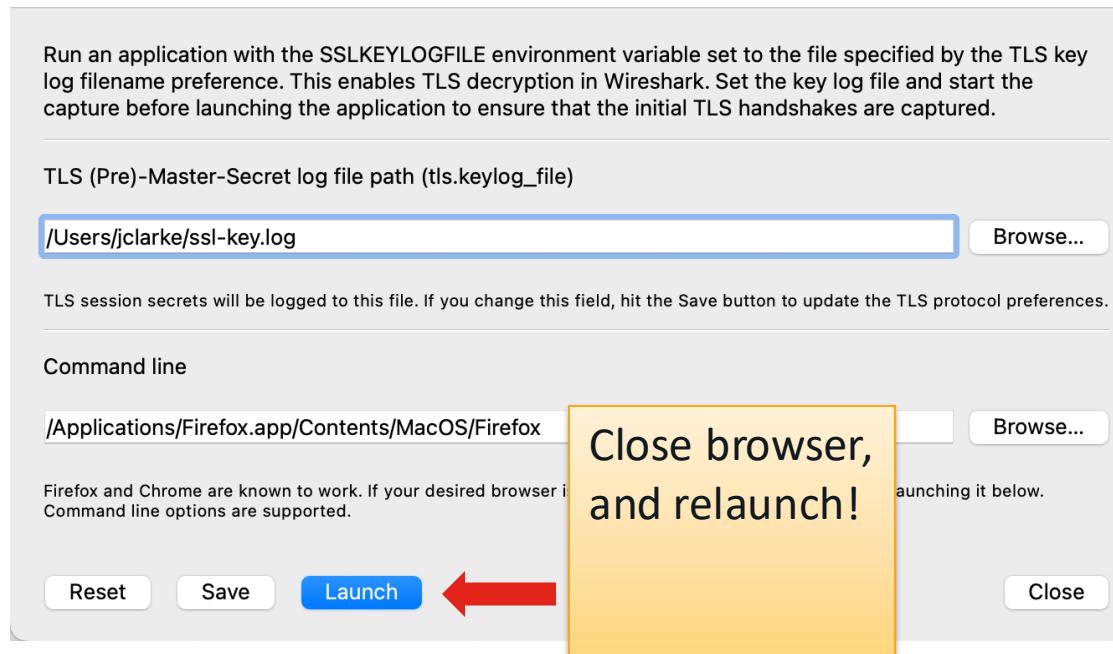
```
$ export SSLKEYLOGFILE=~/ssl-  
key.log  
$ open  
/Applications/Firefox.app
```

Decrypt the Things!



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=el25xoAile009cwh6Es30Ng3WGU6MTY4NjA20Dcw0DA4NTUxMTk3NQ

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="el25xoAile009cwh6Es30Ng3WGU6MTY4NjA20Dcw0DA4NTUxMTk3NQ" />
    <meta name="_suburl" content="/git" />

        <meta property="og:url" content="https://www.marcuscom.com/git/" />
        <meta property="og:type" content="website" />

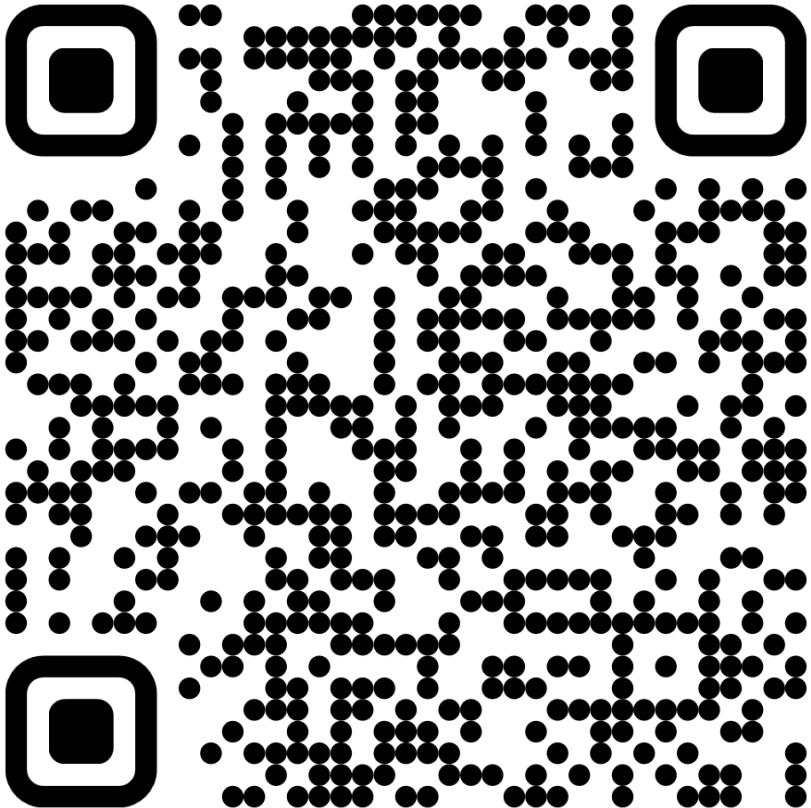
```

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

Profit!

Download the slides

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



Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education

- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: **Insert preferred comms method**

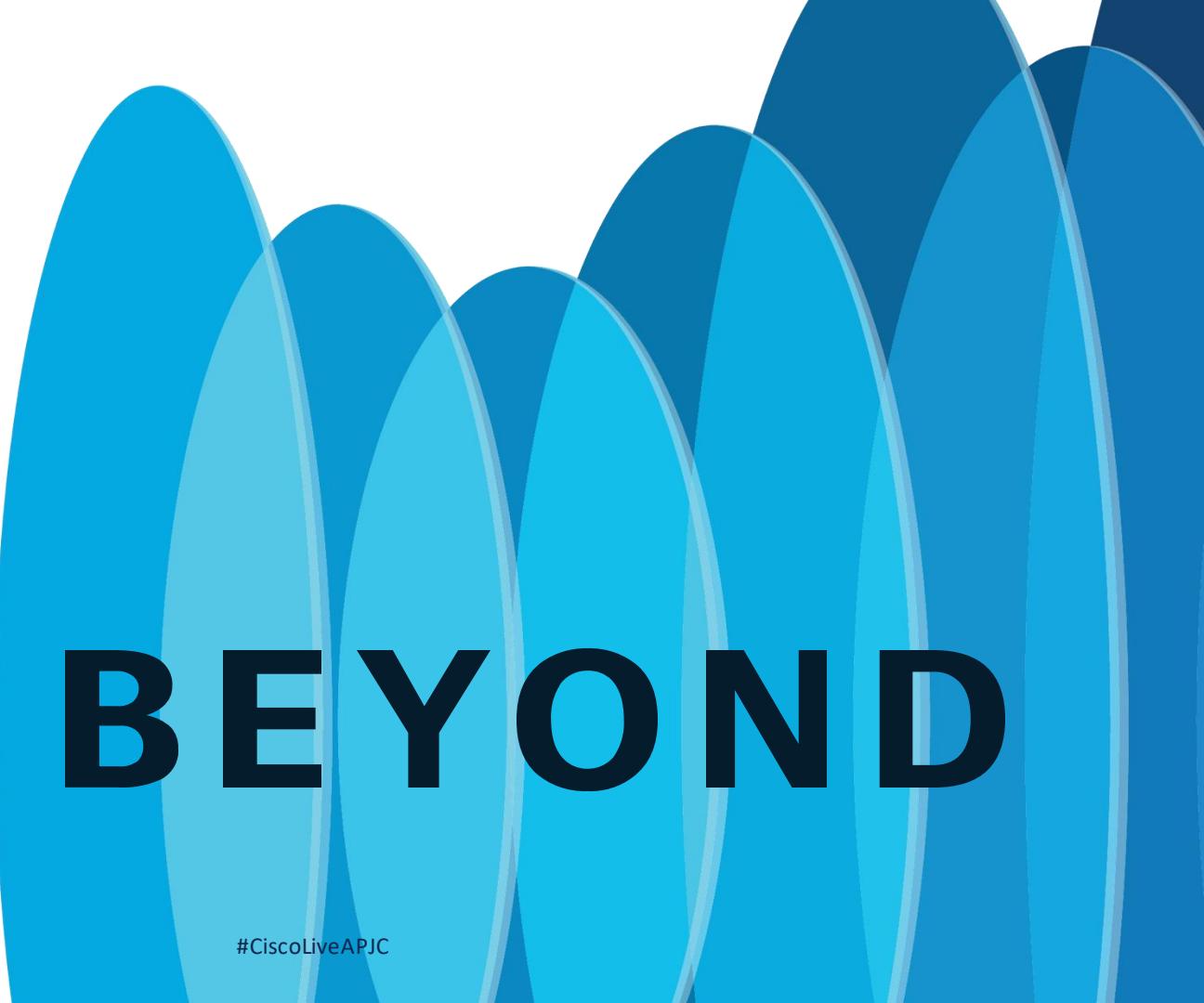


Thank you

CISCO Live!

#CiscoLiveAPJC

cisco *Live!*



GO BEYOND

#CiscoLiveAPJC