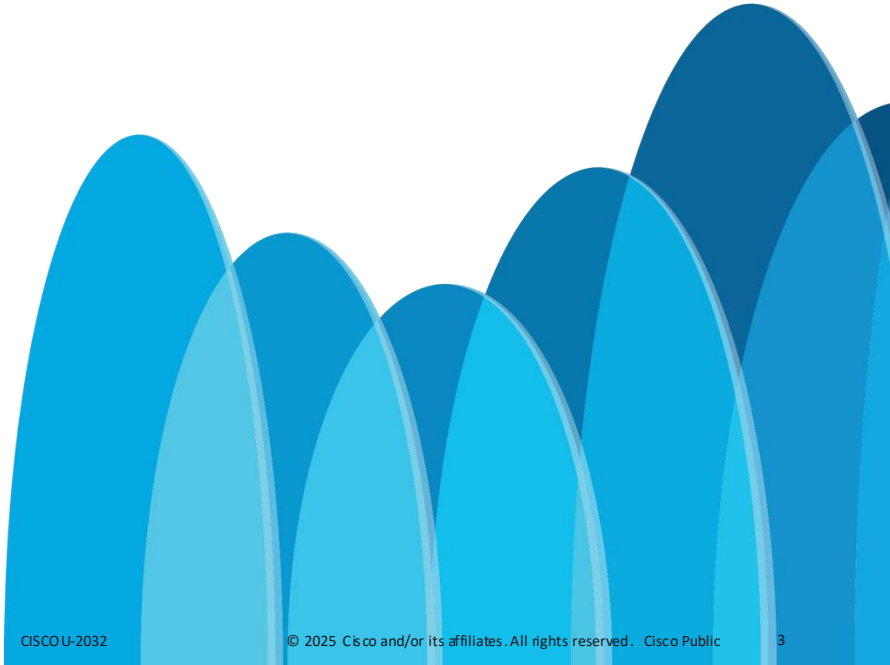
Become a network doctor using packet captures and Wireshark

Prapanch Ramamoorthy
Principal Engineer, CX Engineering
CISCOU-2032

Wireshark is a network engineer's best friend!

- An unknown network engineer



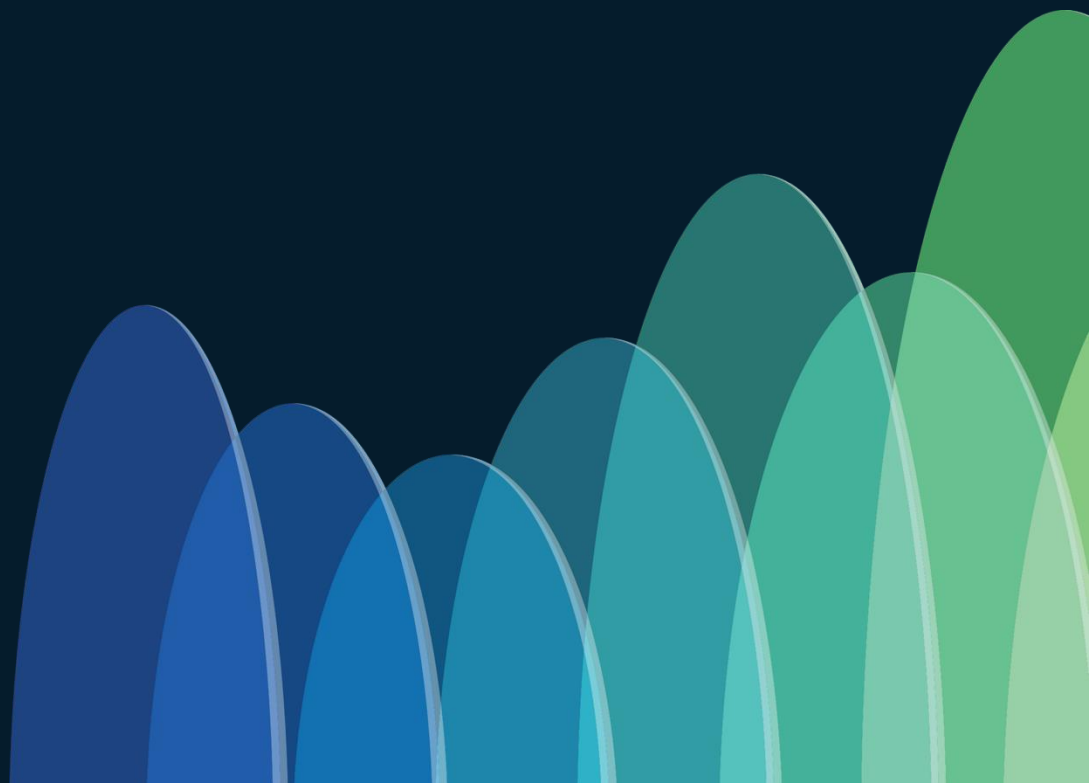
Agenda

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

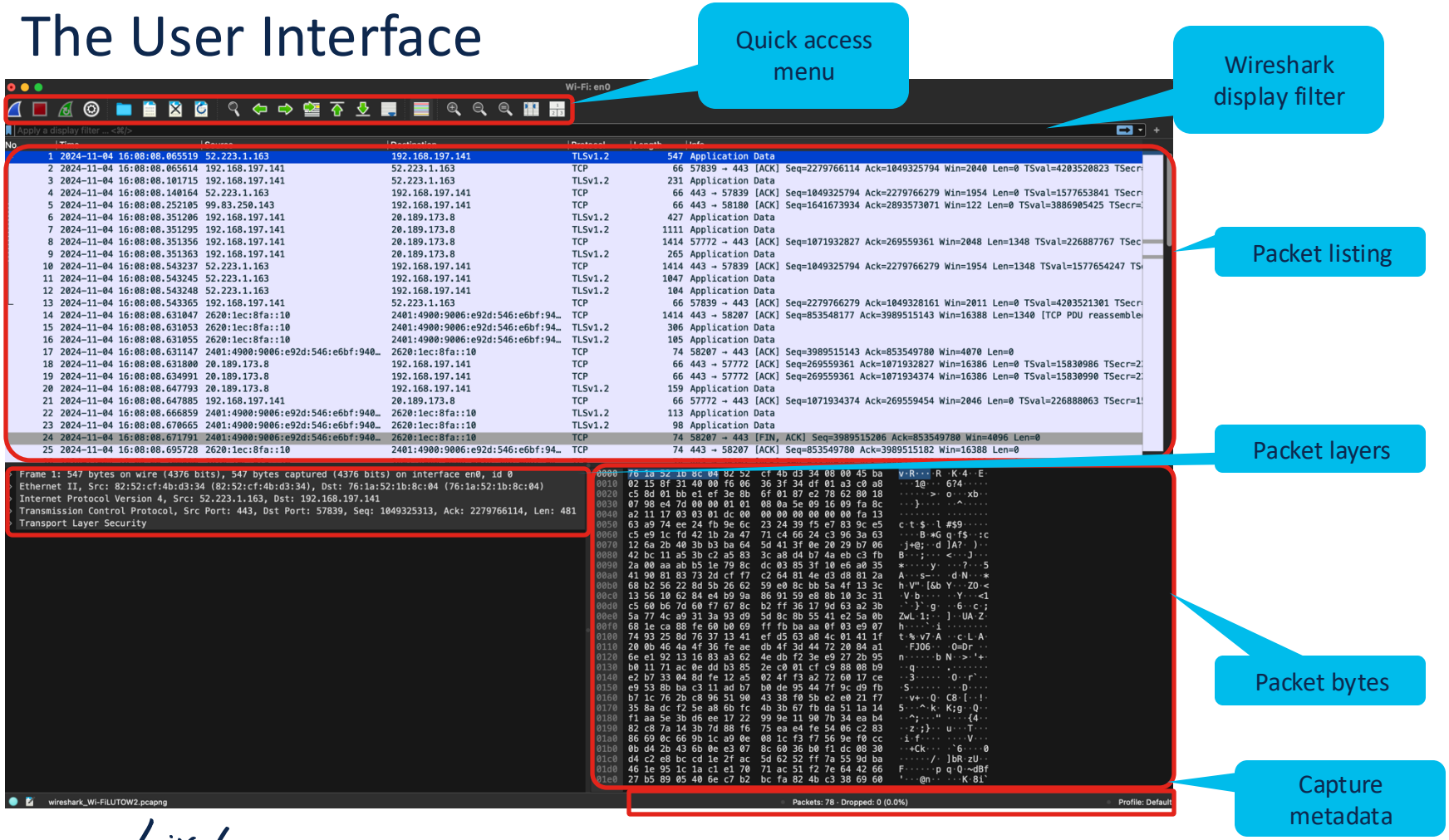
Install Wireshark

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

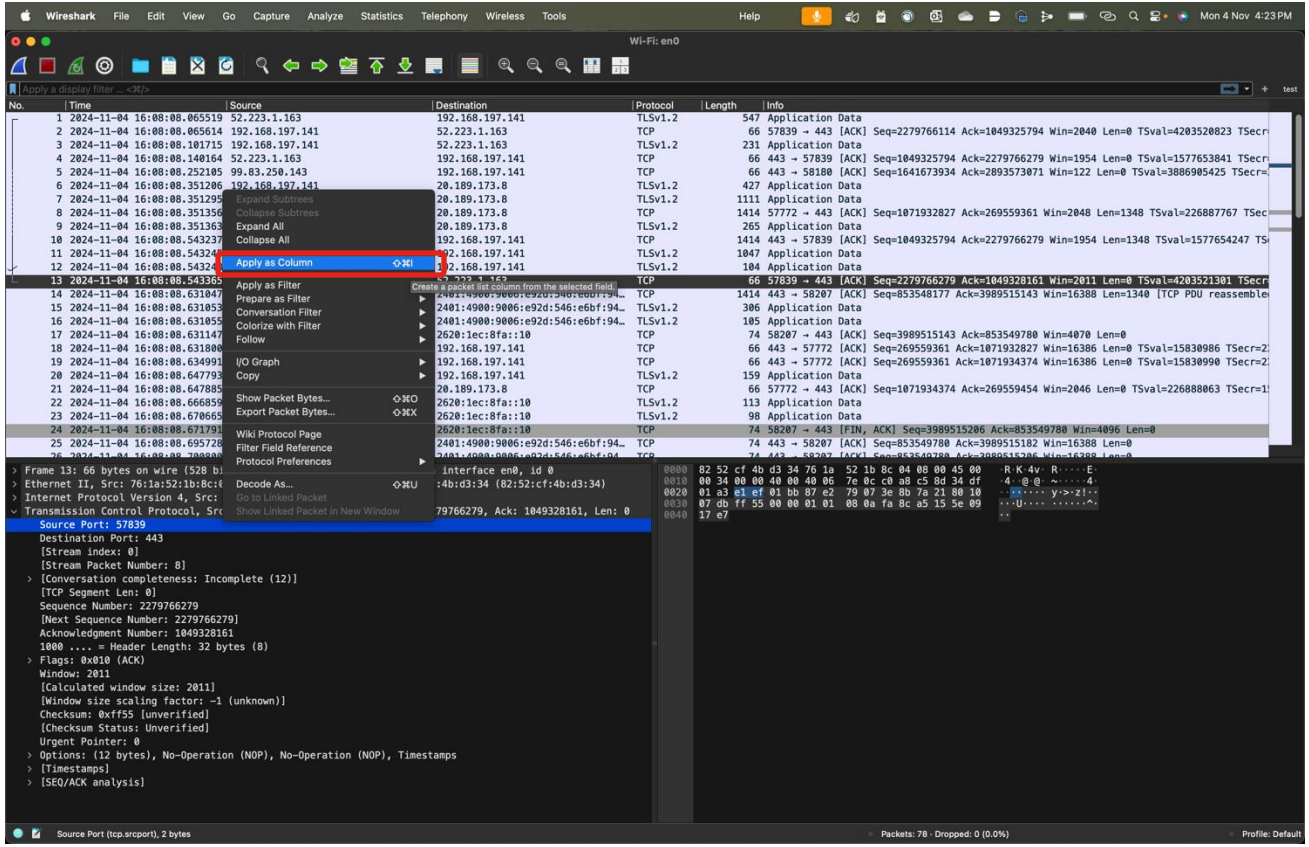
Getting familiar



The User Interface

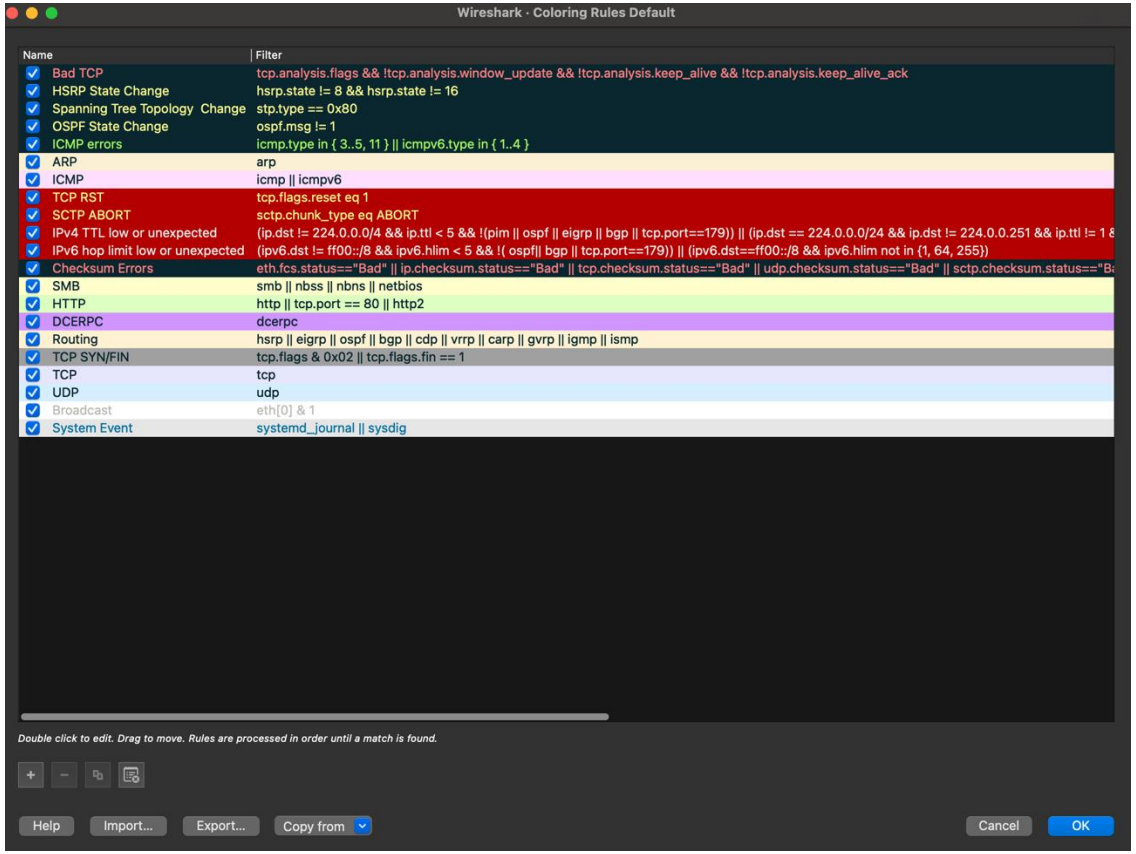


Customizing the UI - Columns



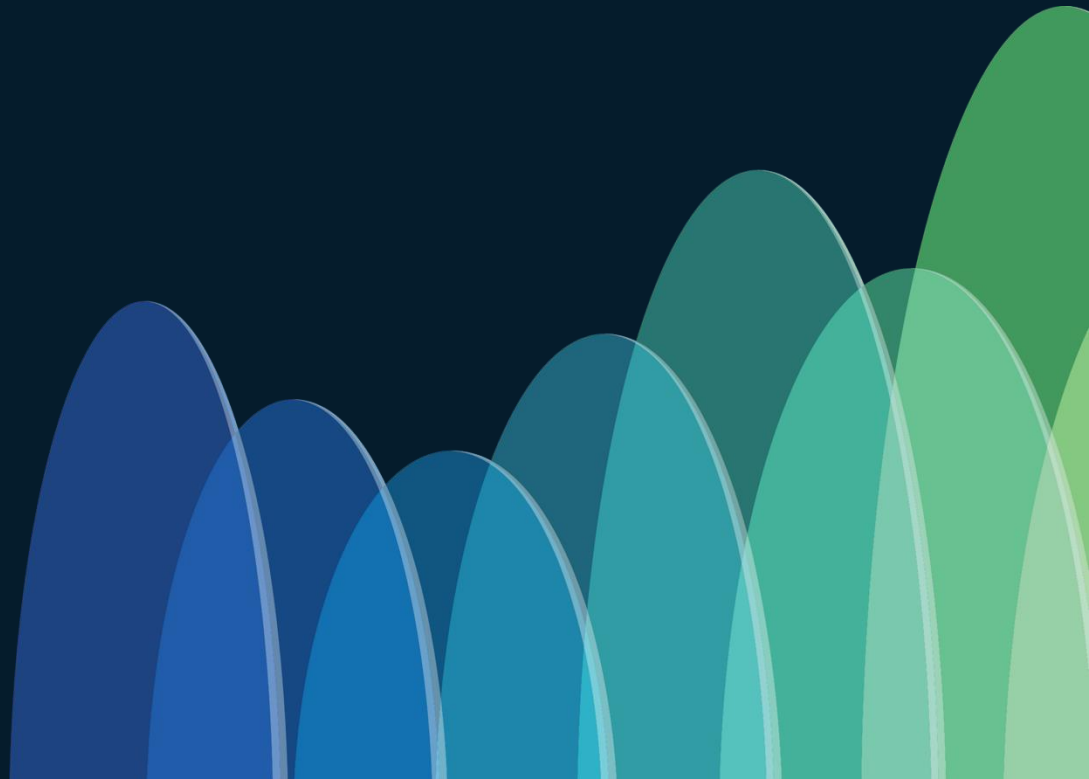
- Quick access within packet details/layers
- Also available at “Preferences > Appearance > Columns”

Customizing the UI – Coloring rules

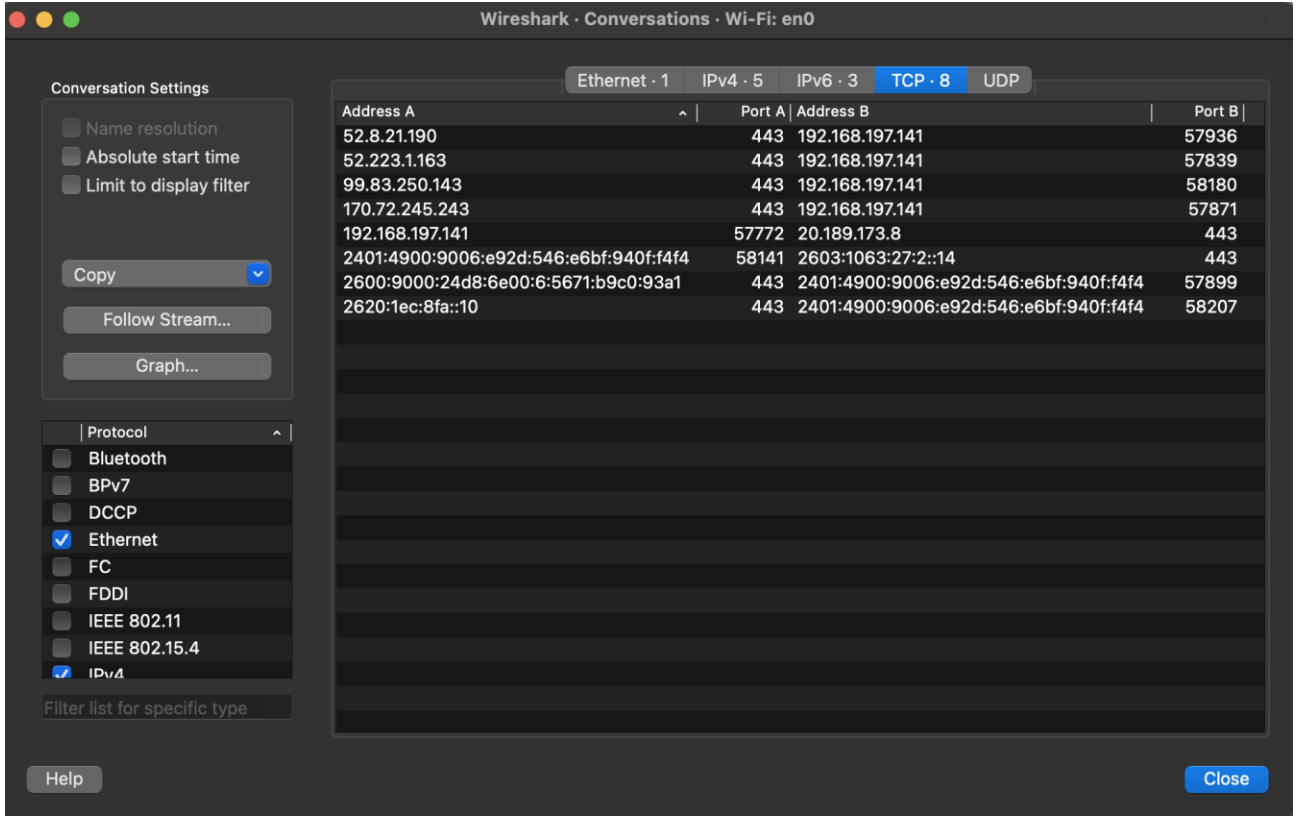


- A picture is worth a thousand words!
- Setup custom rules to quickly catch special conditions
- Accessible at “View > Coloring Rules”

Capture Statistics

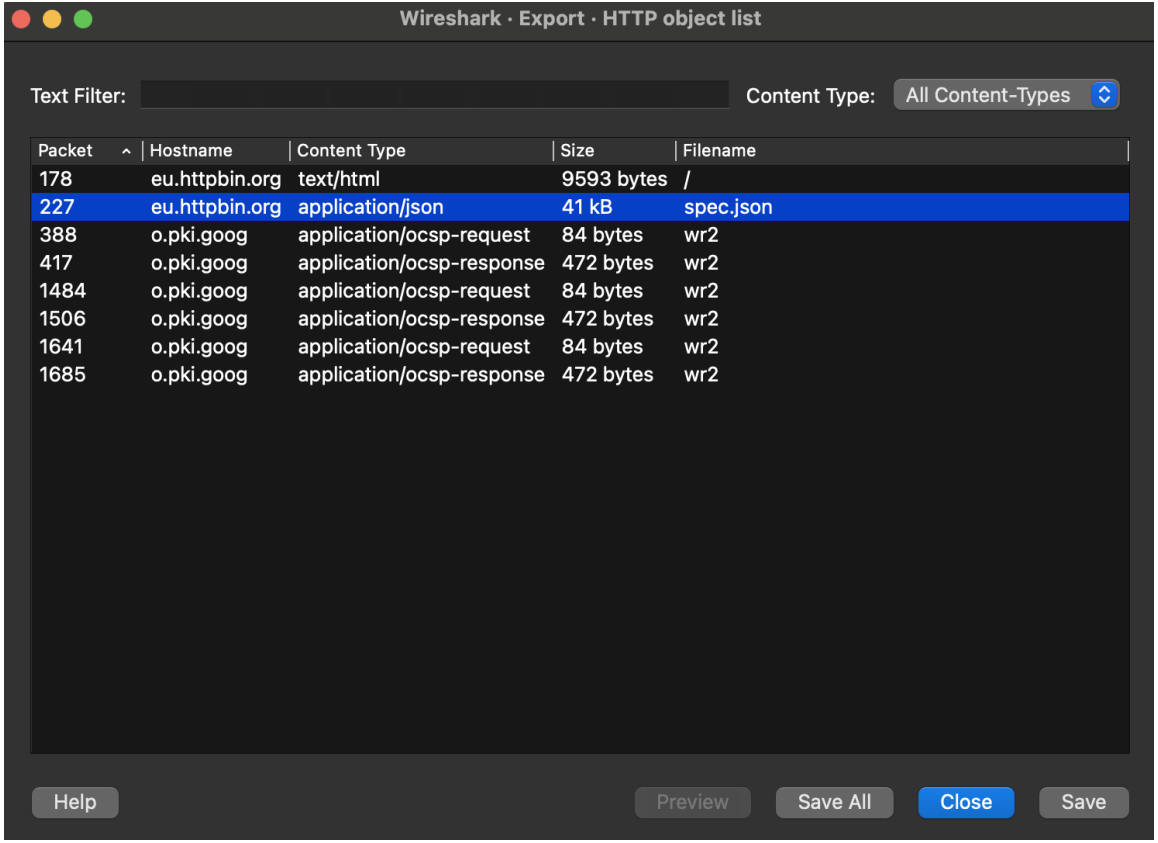


Conversations



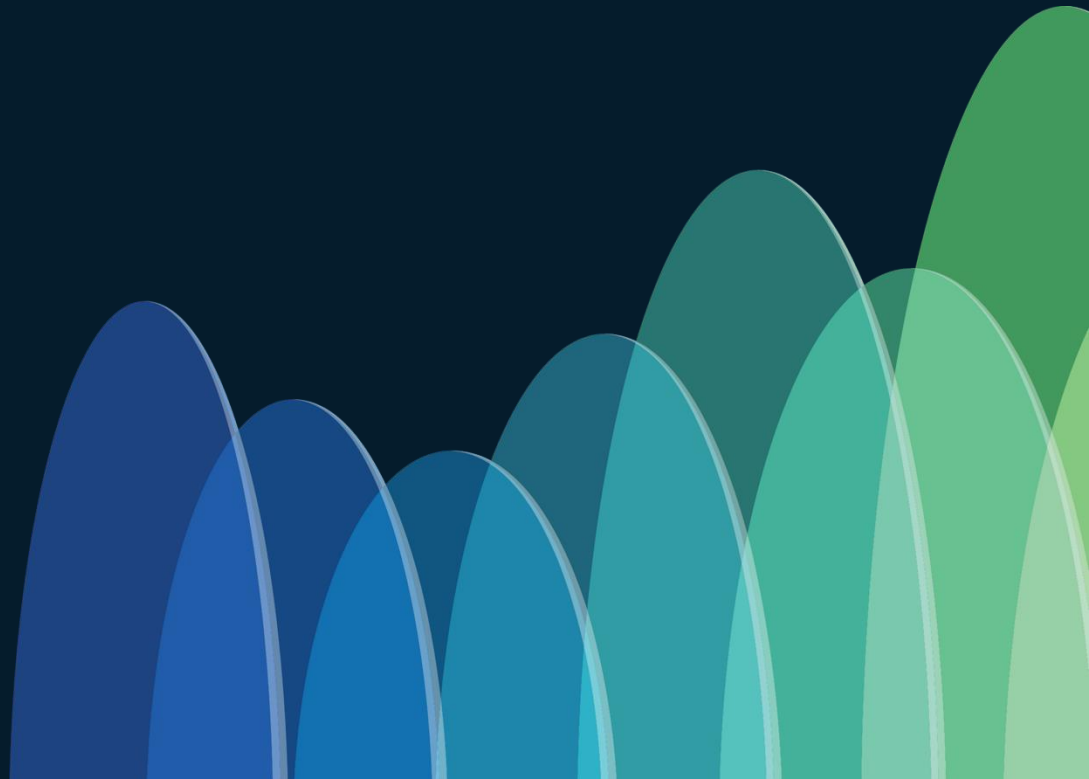
- Accessible at “Statistics > Conversations”
- Quick summary of Layers 2, 3 and 4 conversations with statistics
- Ability to filter down if necessary

Export Objects

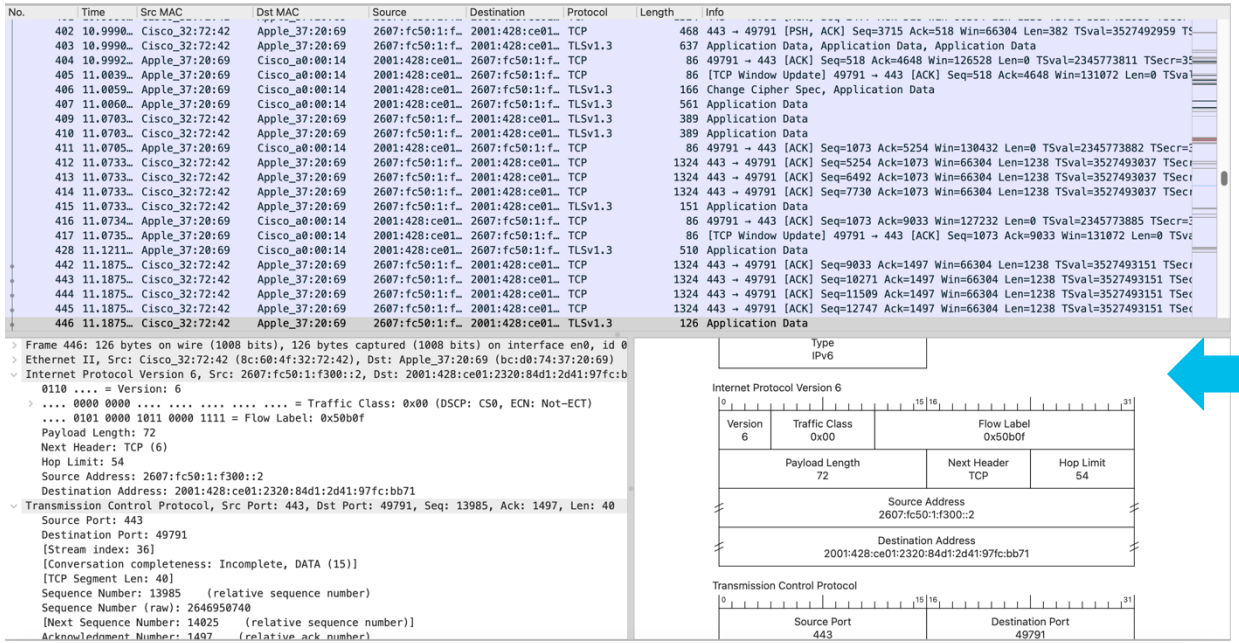


- Accessible at “File > Export Objects”
- Direct access to Application layer objects (files, etc.)
- Protocols supported include FTP, HTTP, SMB, TFTP.

Packet Diagrams



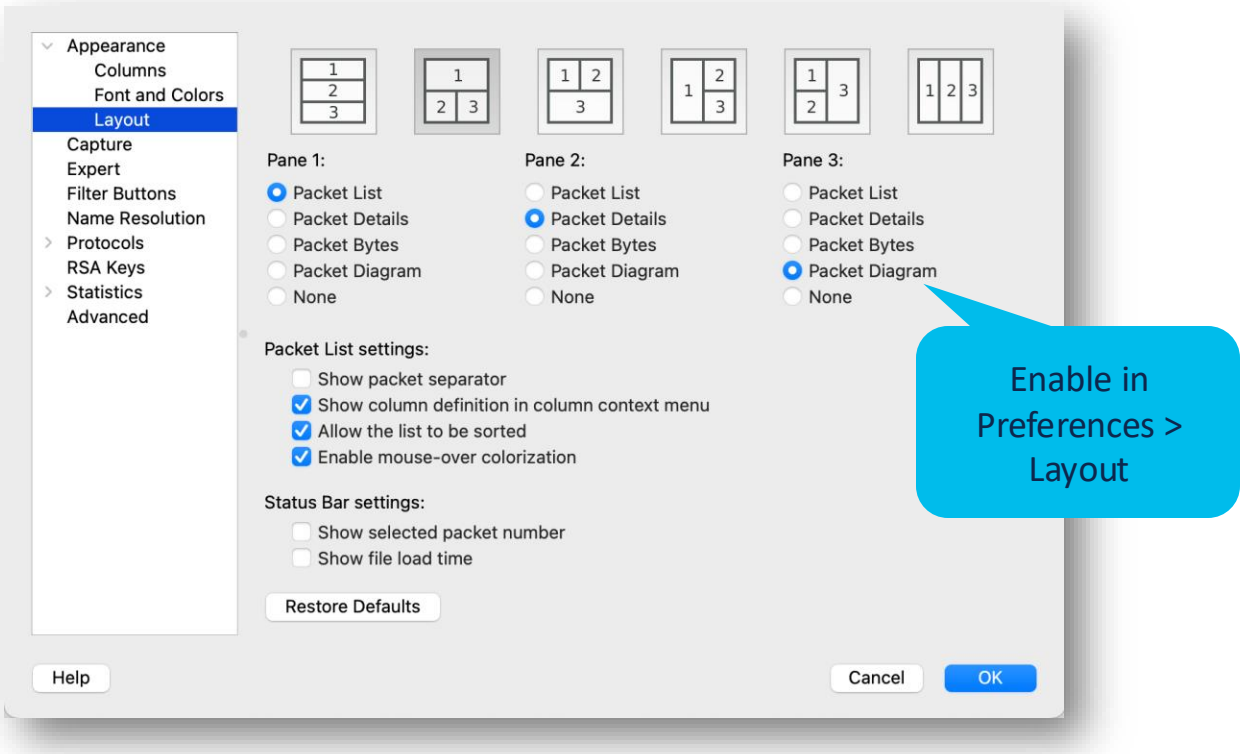
Packet Diagrams



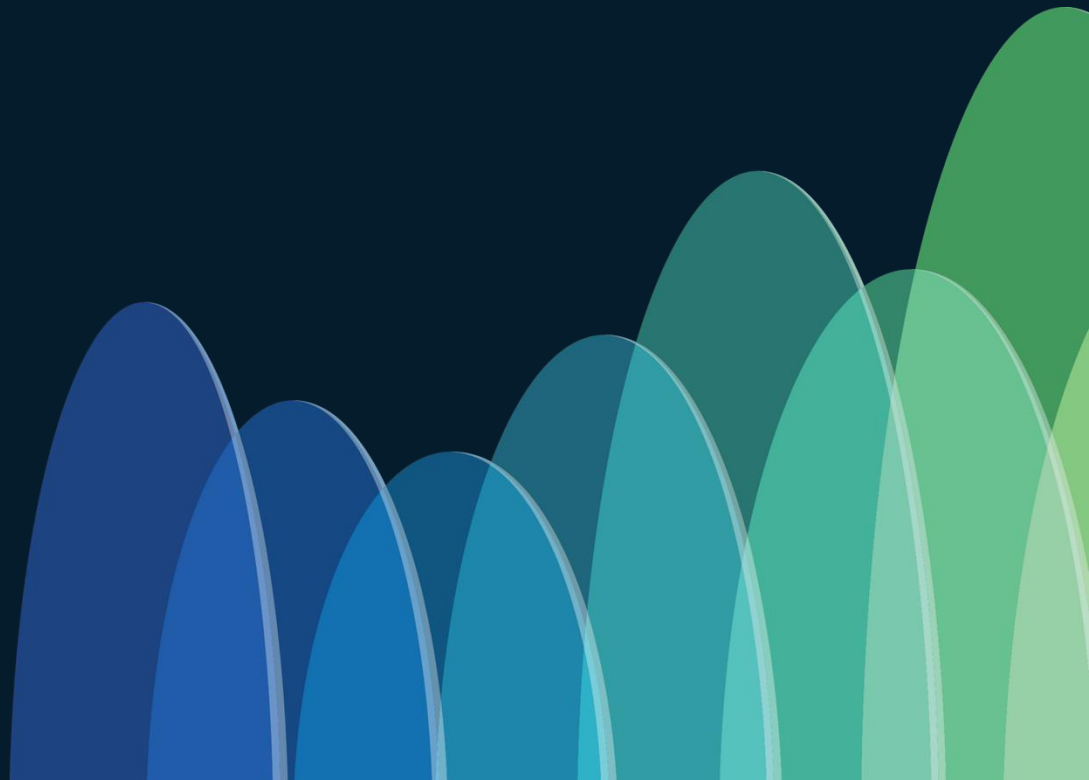
New to Wireshark 3.4

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

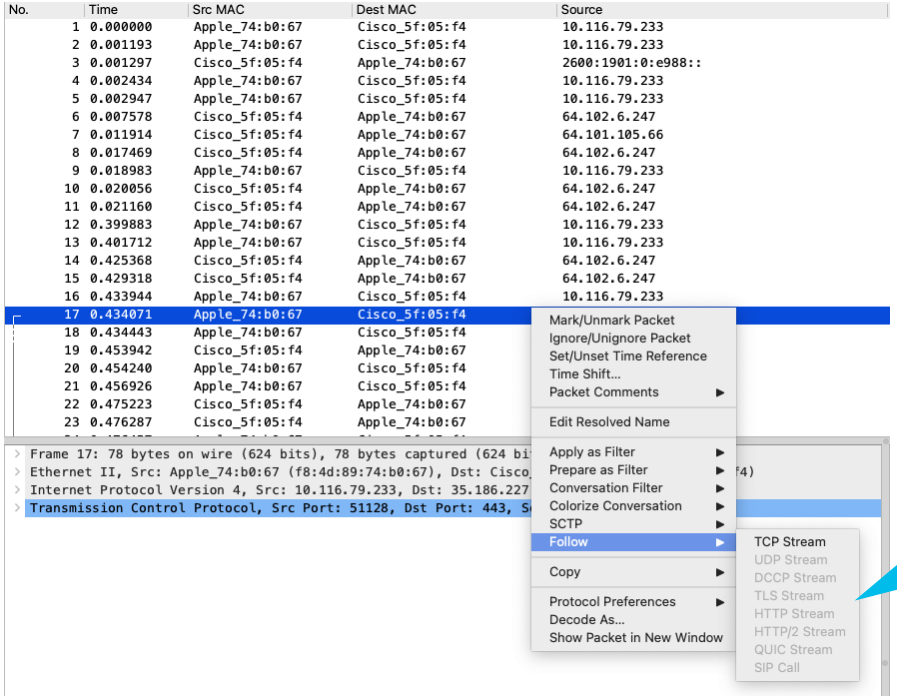
Packet Diagrams



Following Streams



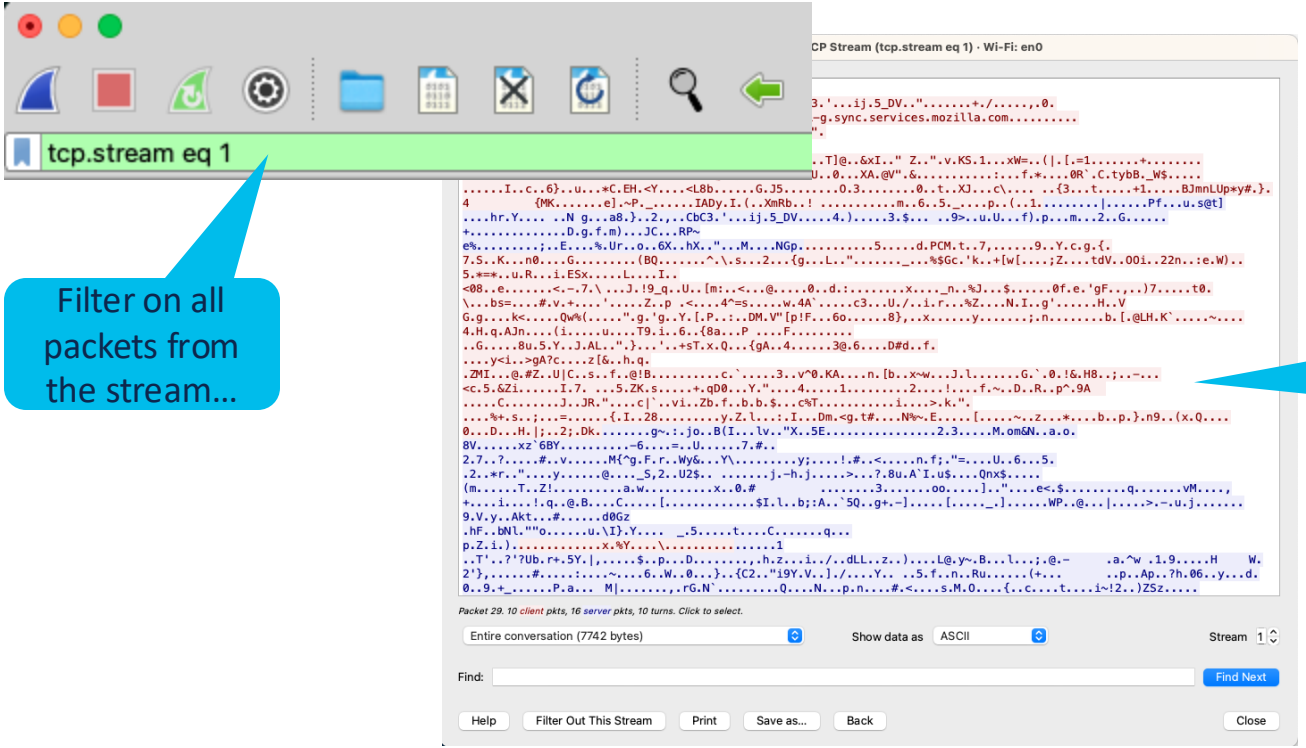
Following Streams



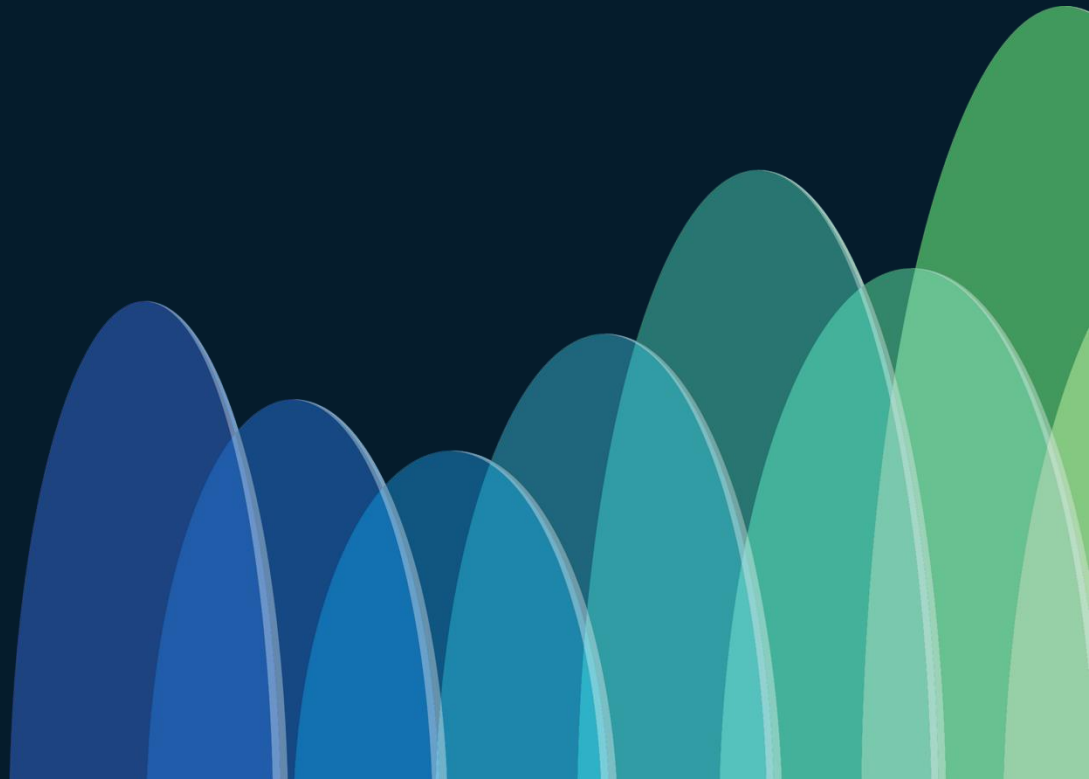
- TCP
- UDP
- DCCP
- TLS
- HTTP[/2]
- QUIC
- SIP

Pick the stream to follow based on initial packet

Following Streams



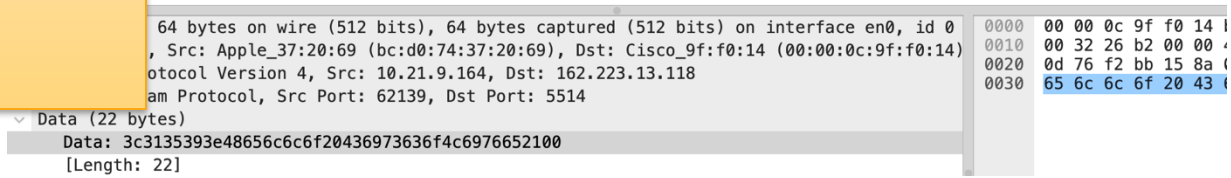
Decode As…



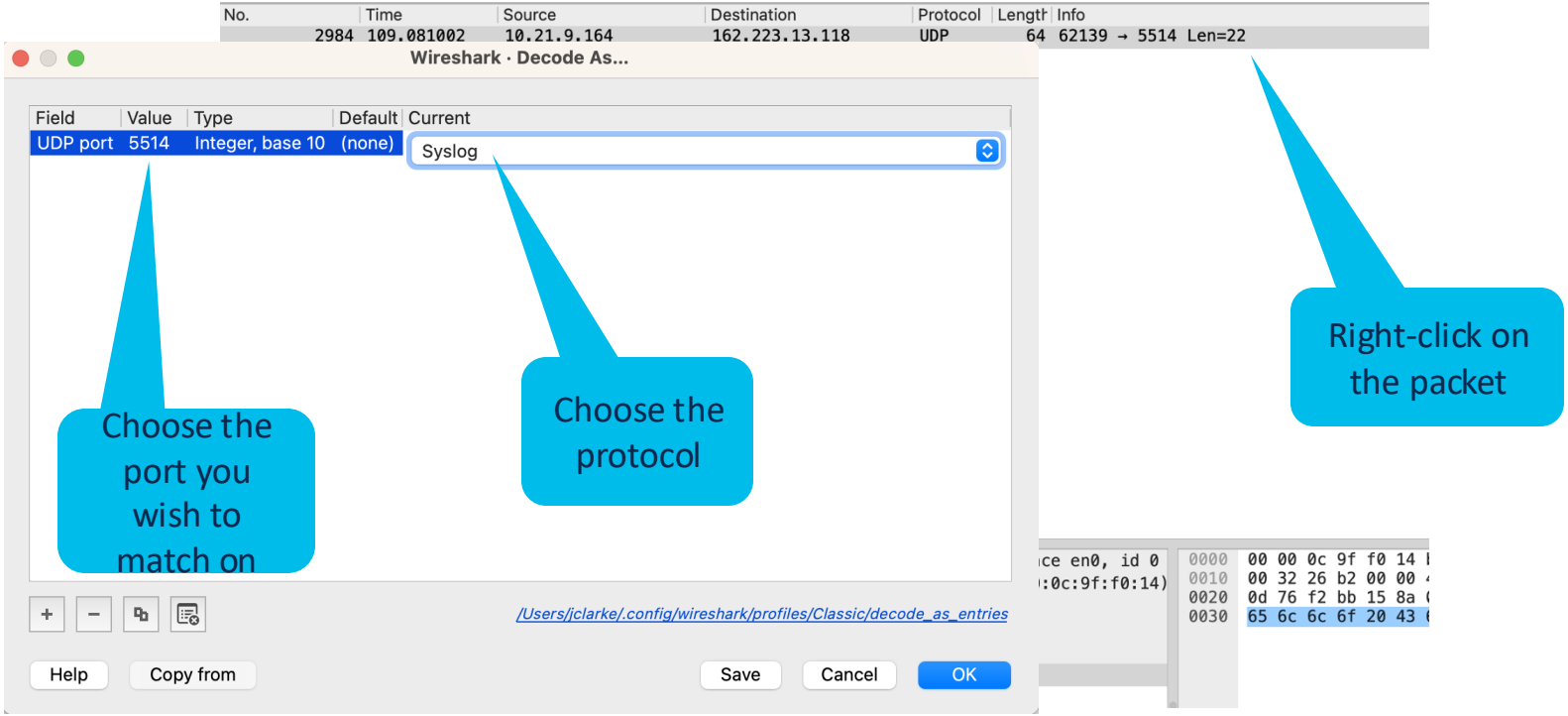
Decode As…

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

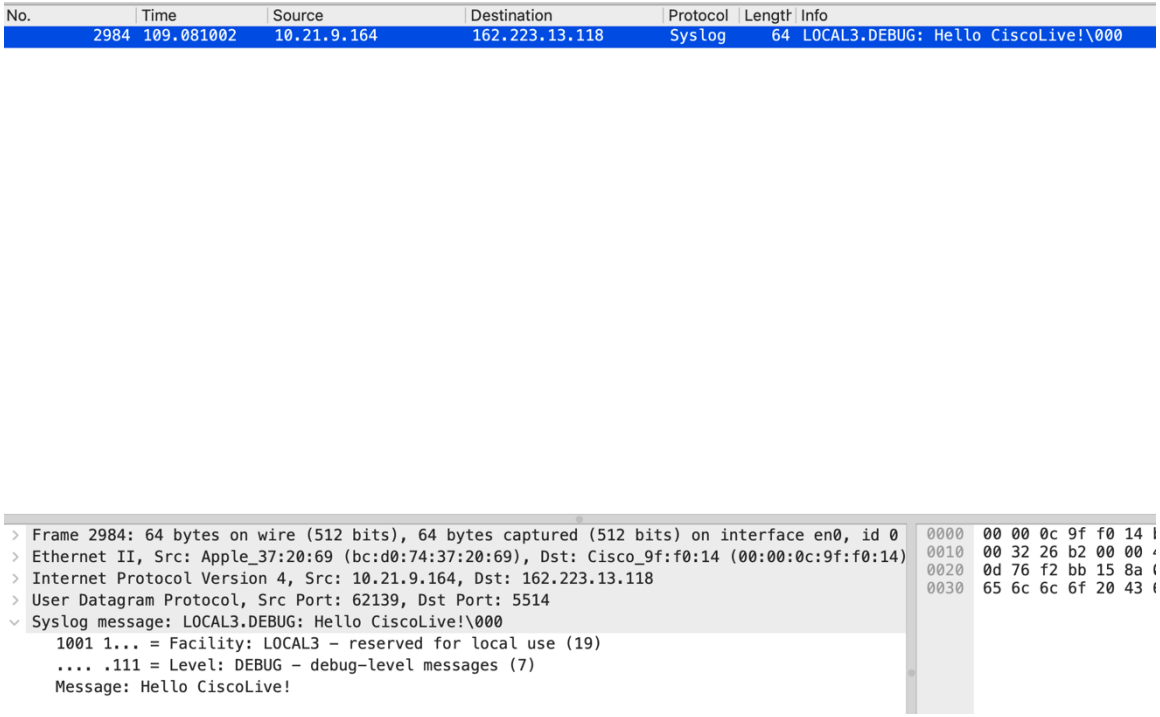
Let’s say you have a data stream using non-standard ports. You still want to make use of wireshark’s dissectors.



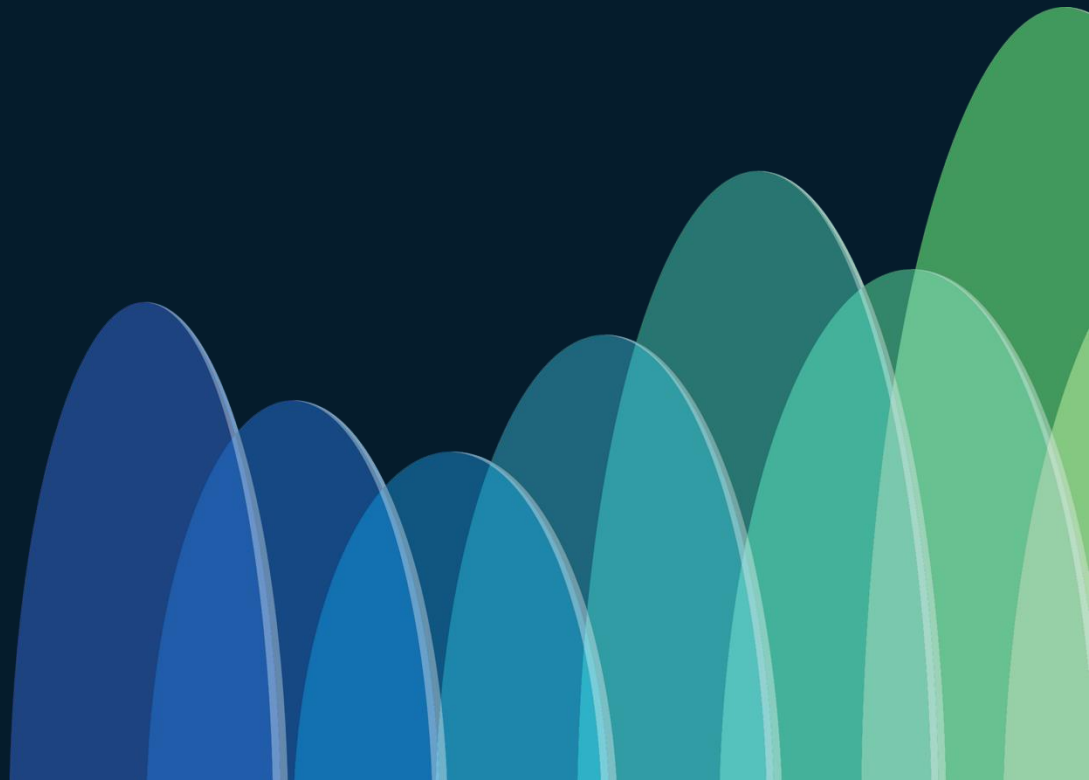
Decode As…



Decode As…

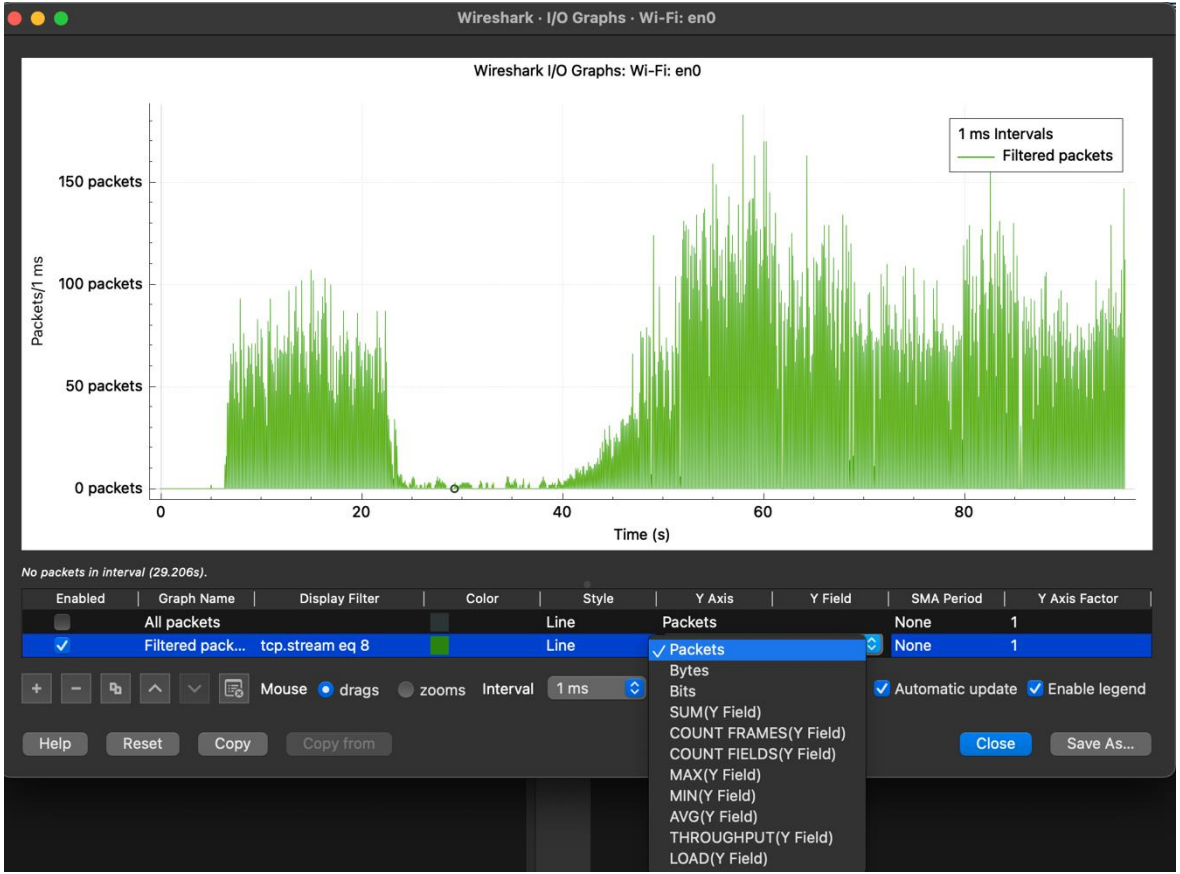


Traffic performance troubleshooting



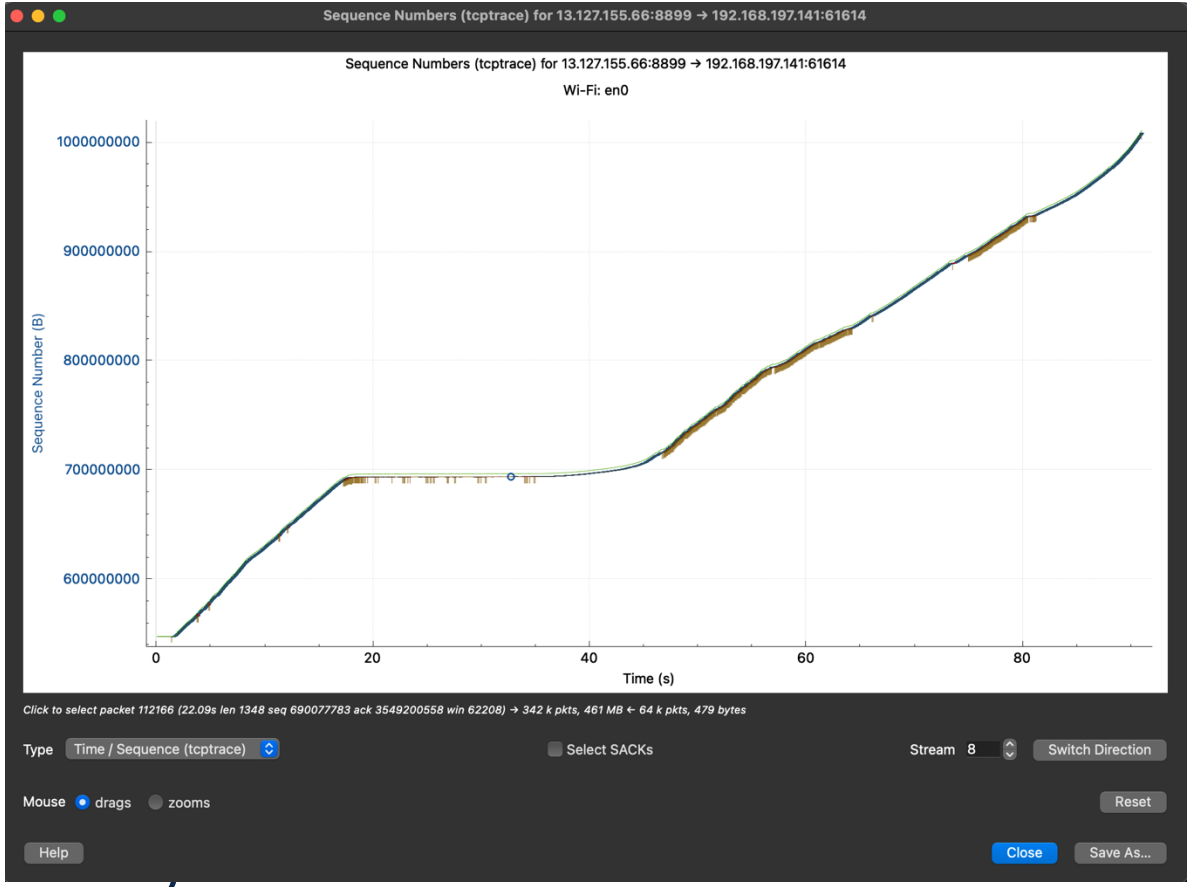
cisco Live!

Input/Output (I/O) graphs



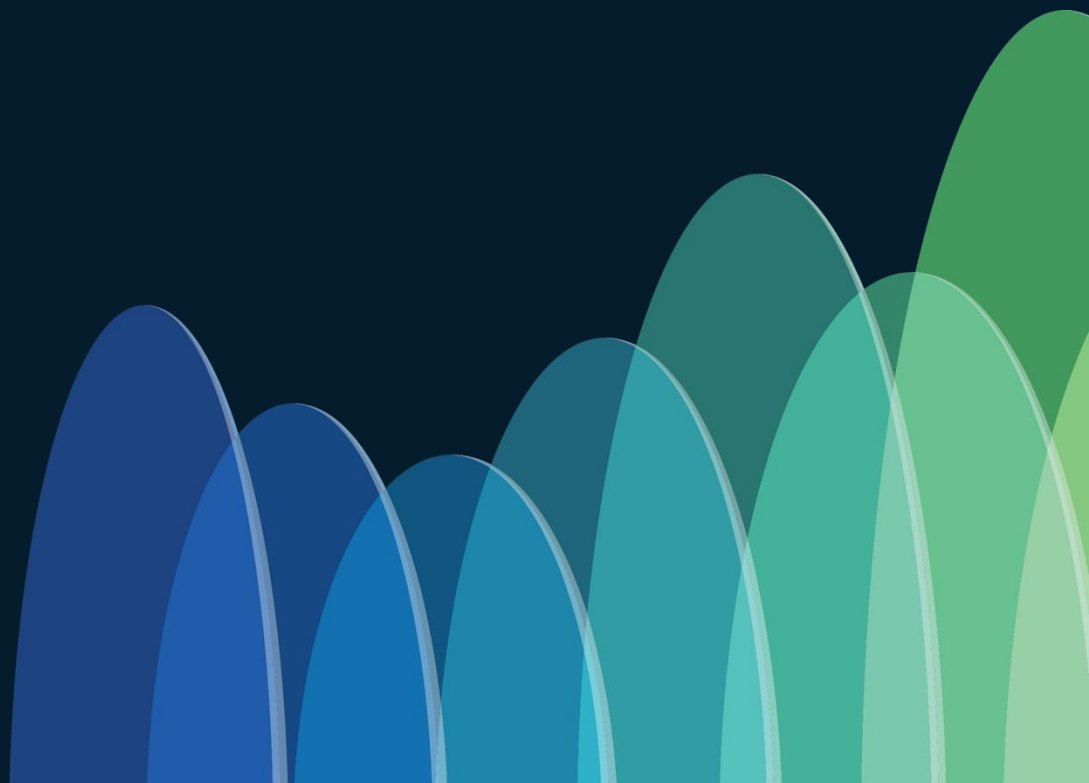
- Accessible at “Statistics > I/O Graphs”.
- Ability to graph for various parameters
- Multiple graphs in a single window – easy comparison

TCP graphs - tcptrace

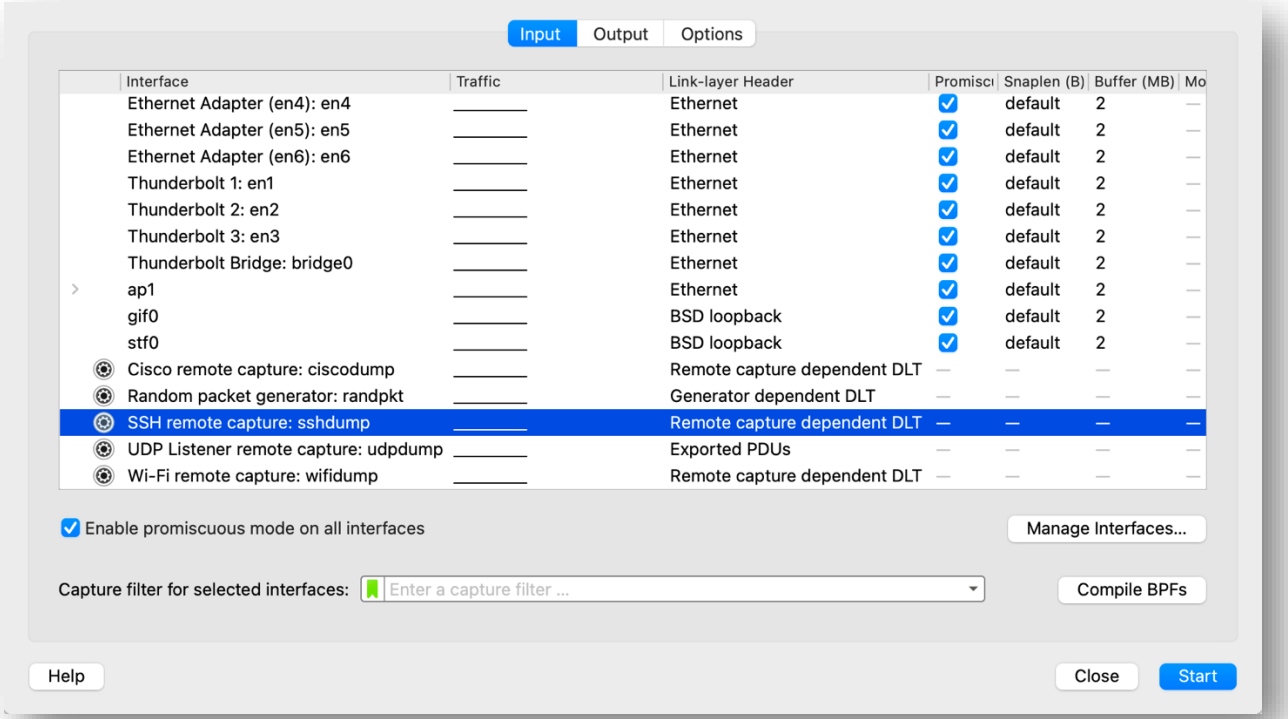


- Accessible at “Statistics > TCP Stream Graphs”.
- Plots sequence, acknowledgement, sack, window size in a single graph
- Linear line = good!
- Steeper line = higher throughput

Remote Capture

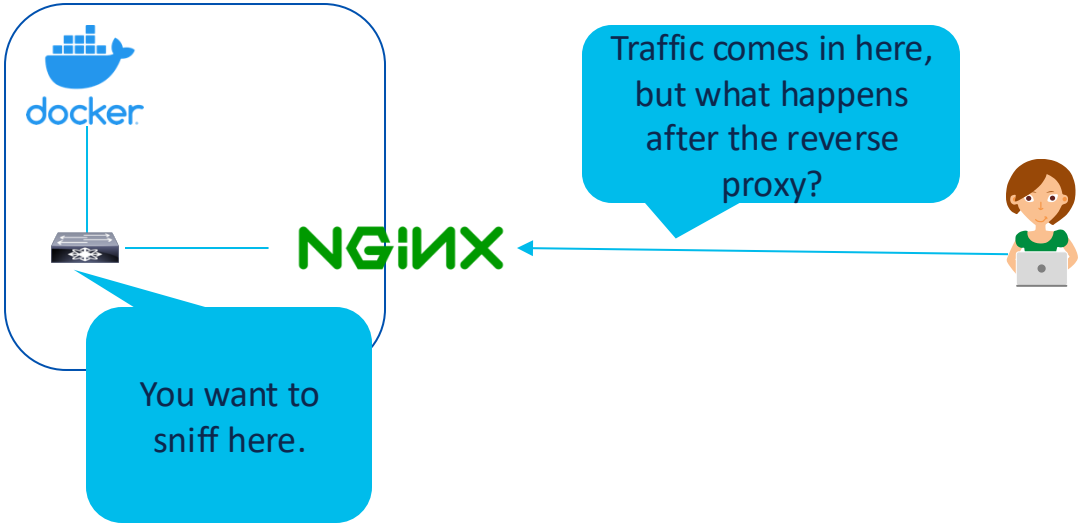


Remote Capture

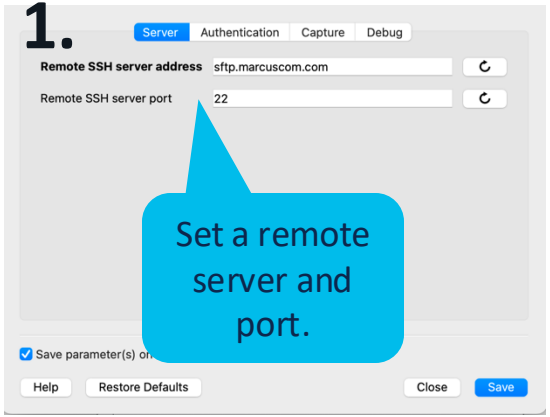


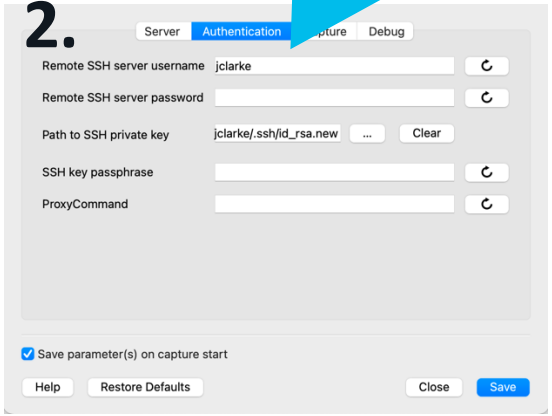
- Don’t forget to scroll down and explore the full interface list
- Remote captures are excellent for troubleshooting embedded services or setting up a SPAN server

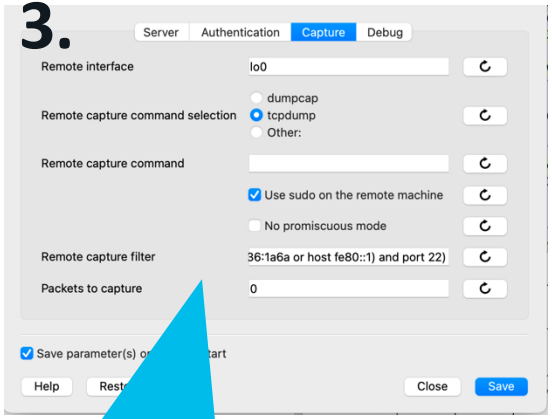
Remote Capture



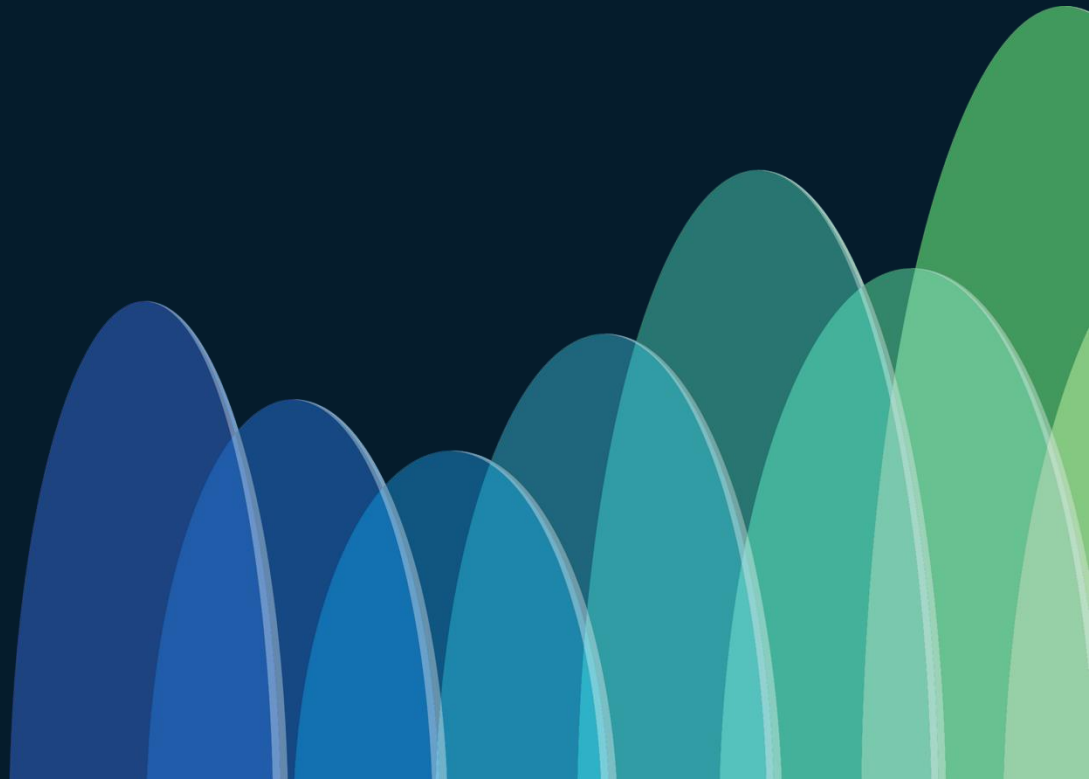
Remote Capture







Decrypt the Things!



cisco Live!

Decrypt the Things!

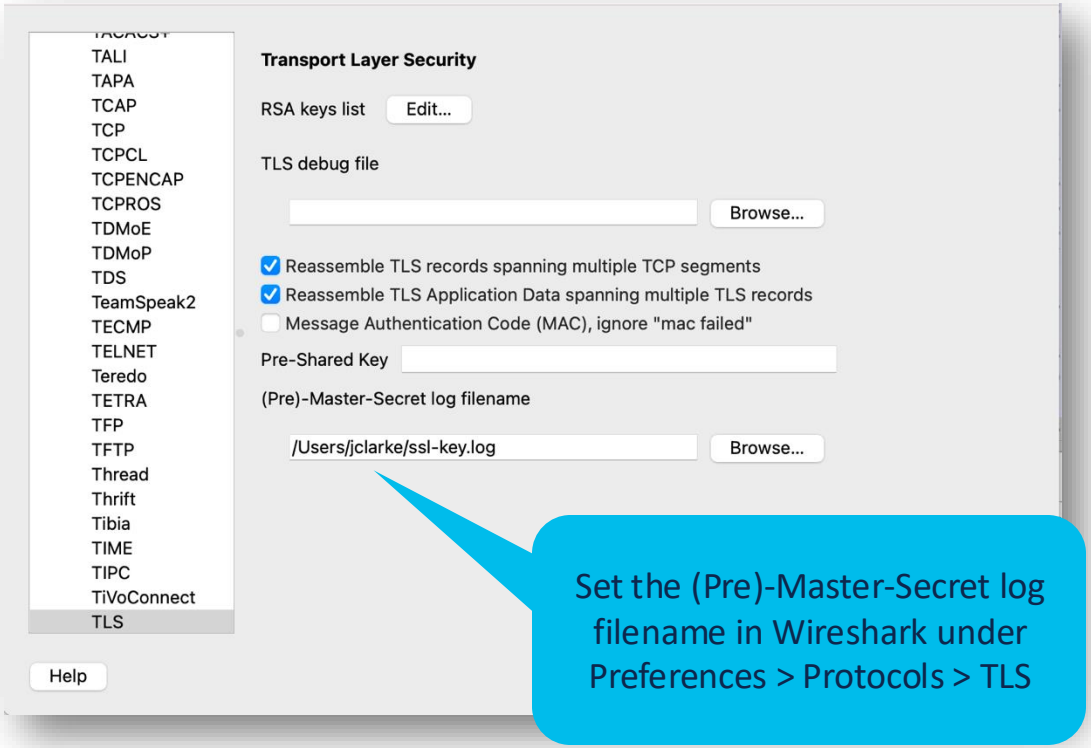
Well this isn't terribly useful…

Decrypt the Things!

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

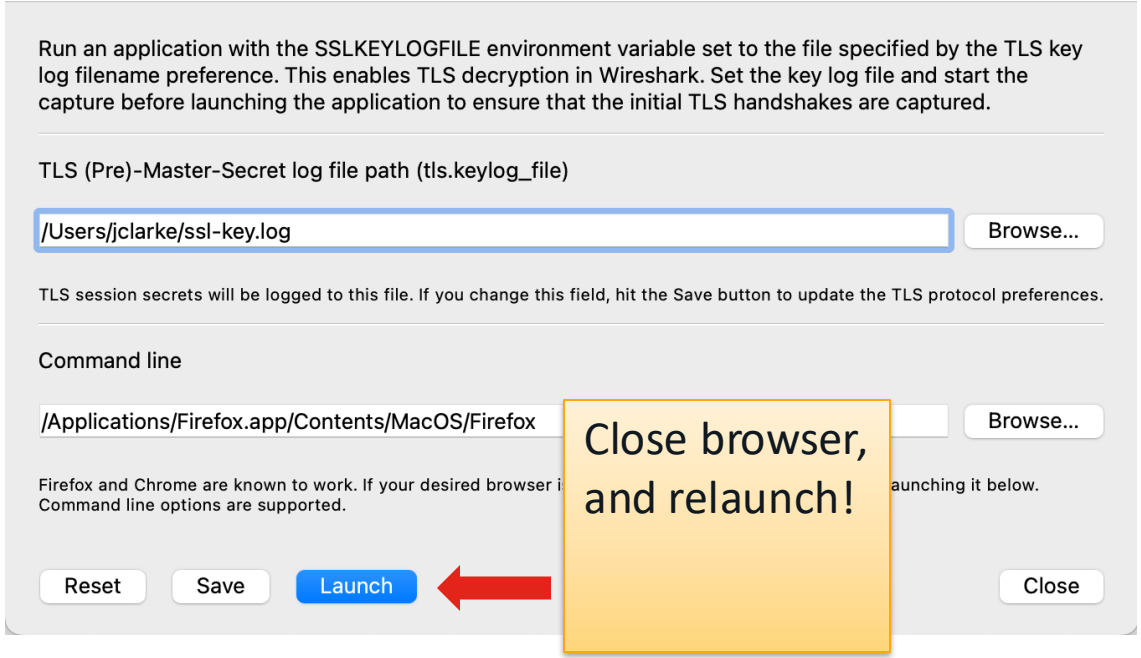
```
$ export SSLKEYLOGFILE=~/ssl-key.log
$ open /Applications/Firefox.app
```

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=el25xoAiIe009cwh6Es3ONg3WGU6MTY4NjA2ODcwODA4NTUxMTk3NQ

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="el25xoAiIe009cwh6Es3ONg3WGU6MTY4NjA2ODcwODA4NTUxMTk3NQ" />
          <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/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.

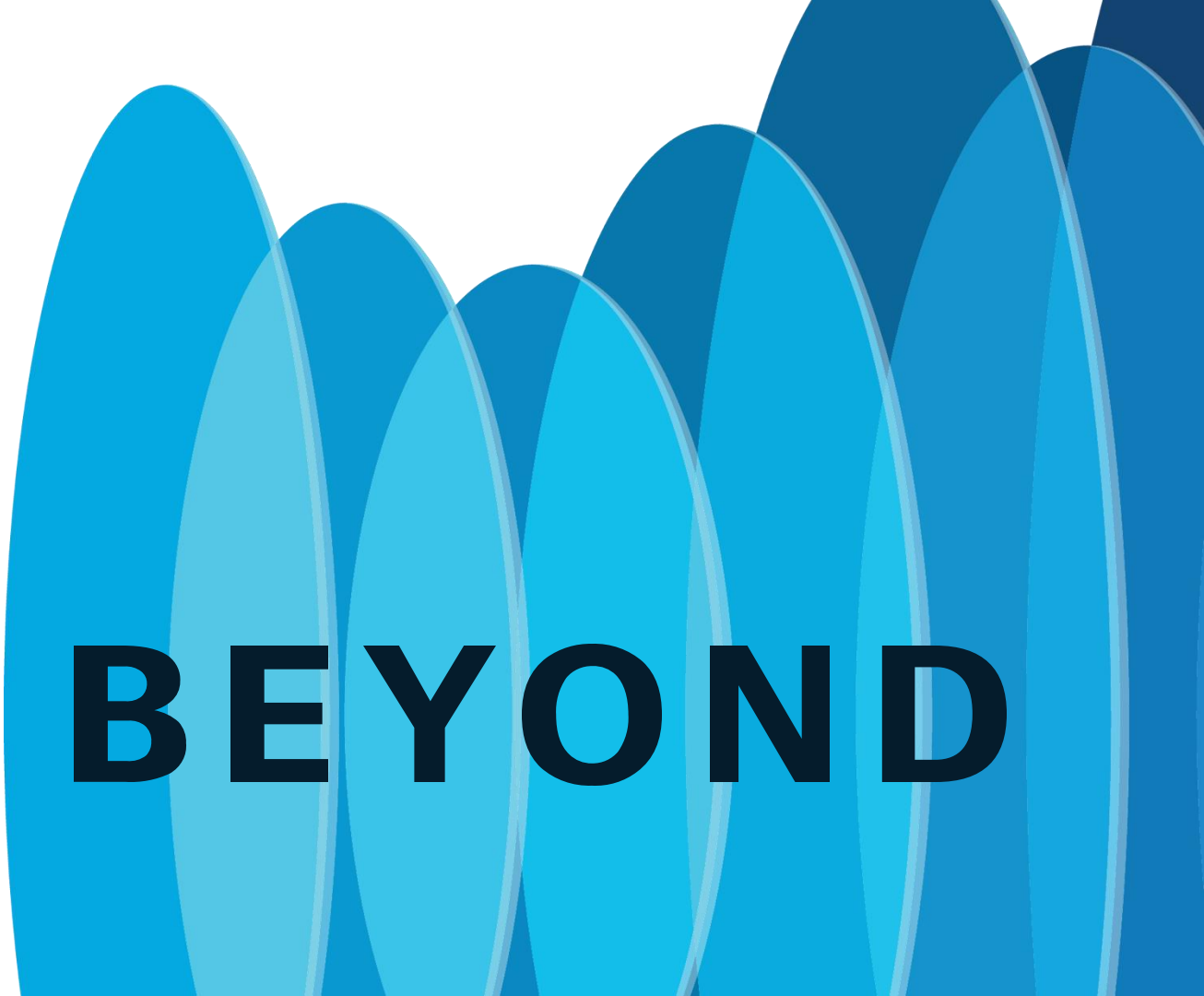
Continue your education

- 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: praprama@cisco.com


cisco
Thank you
cisco Live!

cisco Live!



GO BEYOND