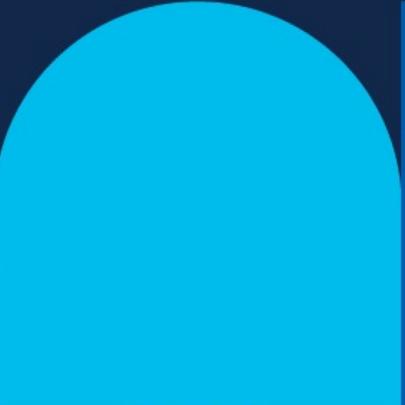


cisco *Live!*

Let's go

#CiscoLive



Cisco **U**.

Tech learning:
shaped to you,
built for Us.





The bridge to possible

Flowin' with Wireshark: Hacks and Tips to Rule the Network

Joe Clarke, Distinguished Engineer
CISCOU-2000



#CiscoLive



Packet Capture or It Didn't Happen

- Some wise network engineer

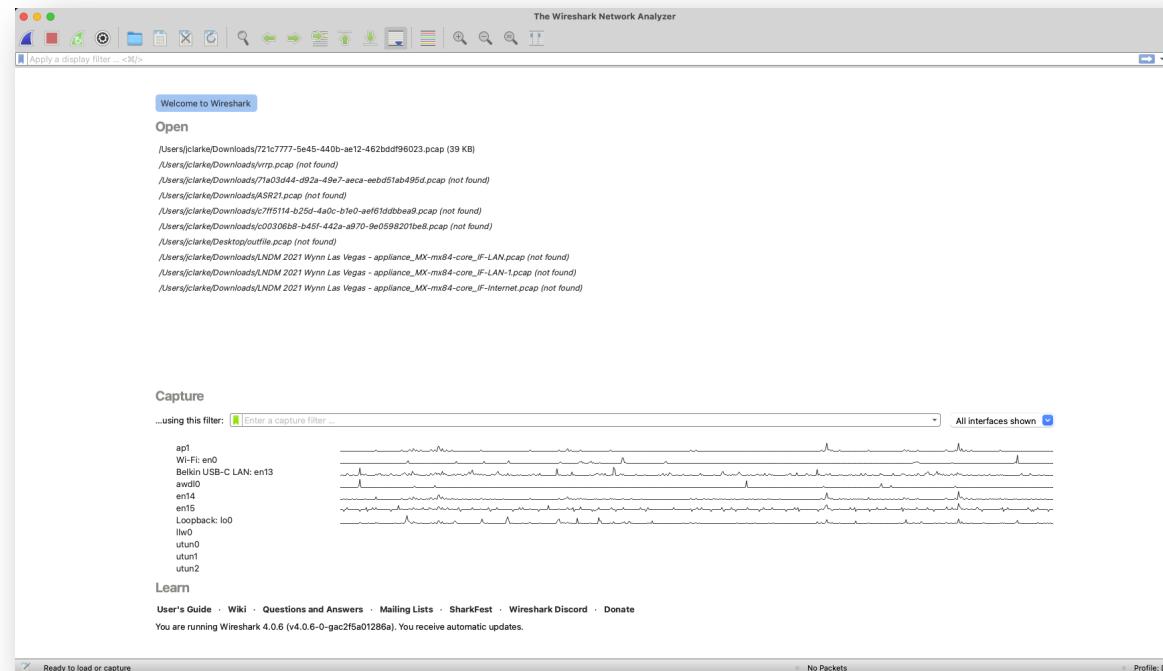
Agenda

cisco *Live!*

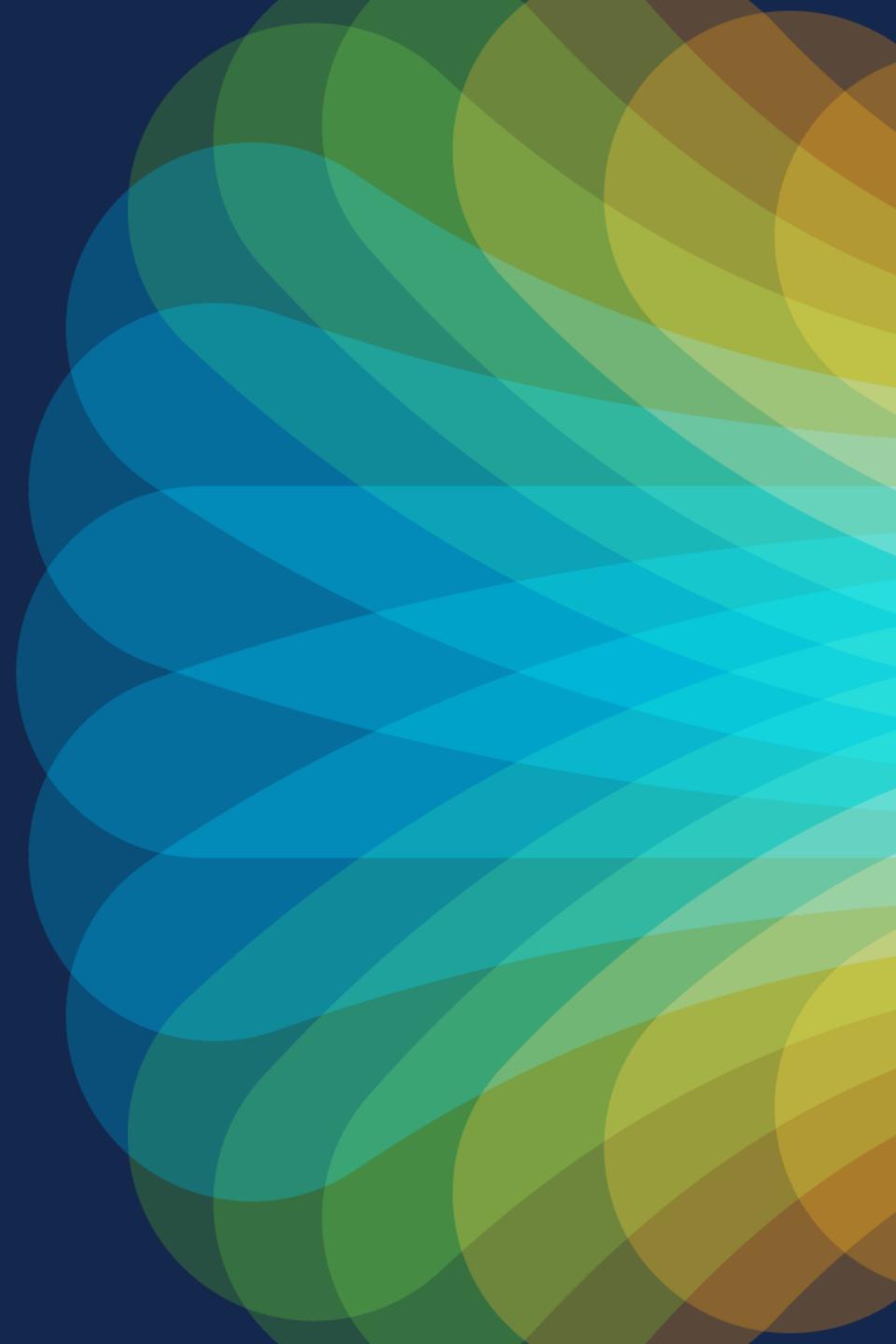
- Following Streams
- Decode As...
- Packet Diagrams
- Remote Capture
- Decrypt the Things!

But First...

- If you don't know or use Wireshark yet...
 - **GET IT NOW!**
 - <https://wireshark.org>



Following Streams



Following Streams

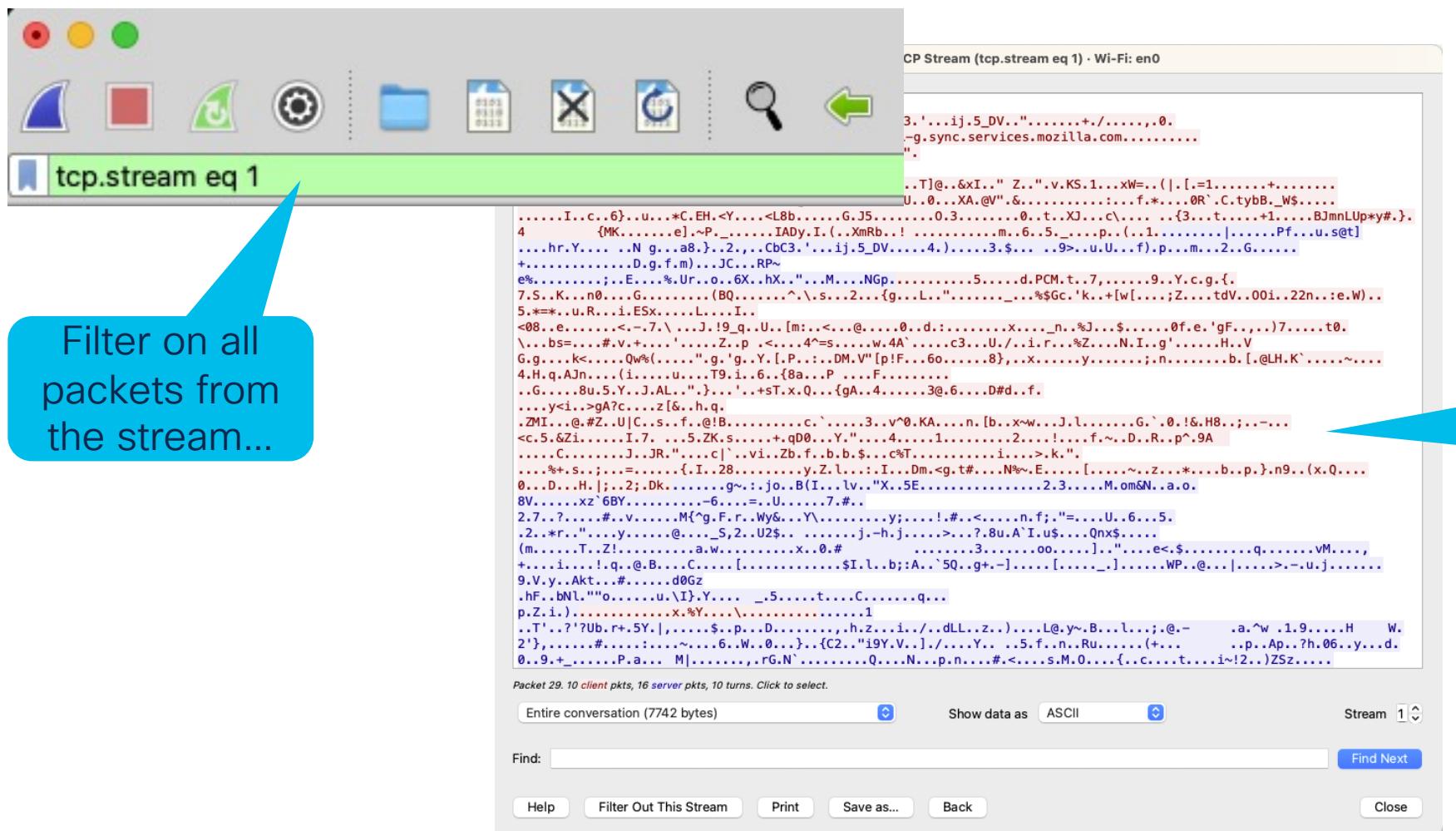
No.	Time	Src MAC	Dest MAC	Source
1	0.000000	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
2	0.001193	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
3	0.001297	Cisco_5f:05:f4	Apple_74:b0:67	2600:1901:0:e988::
4	0.002434	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
5	0.002947	Apple_74:b0:67	Cisco_5f:05:f4	10.116.79.233
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	Follow
18	0.434443	Apple_74:b0:67	Cisco_5f:05:f4	Mark/Unmark Packet
19	0.453942	Cisco_5f:05:f4	Apple_74:b0:67	Ignore/Unignore Packet
20	0.454240	Apple_74:b0:67	Cisco_5f:05:f4	Set/Unset Time Reference
21	0.456926	Apple_74:b0:67	Cisco_5f:05:f4	Time Shift...
22	0.475223	Cisco_5f:05:f4	Apple_74:b0:67	Packet Comments ▶
23	0.476287	Cisco_5f:05:f4	Apple_74:b0:67	Edit Resolved Name

> 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

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

Pick the stream to follow based on initial packet

Following Streams



Filter on all
packets from
the stream...

...And assembles
all data bytes in
one screen

Decode As...

Decode As...

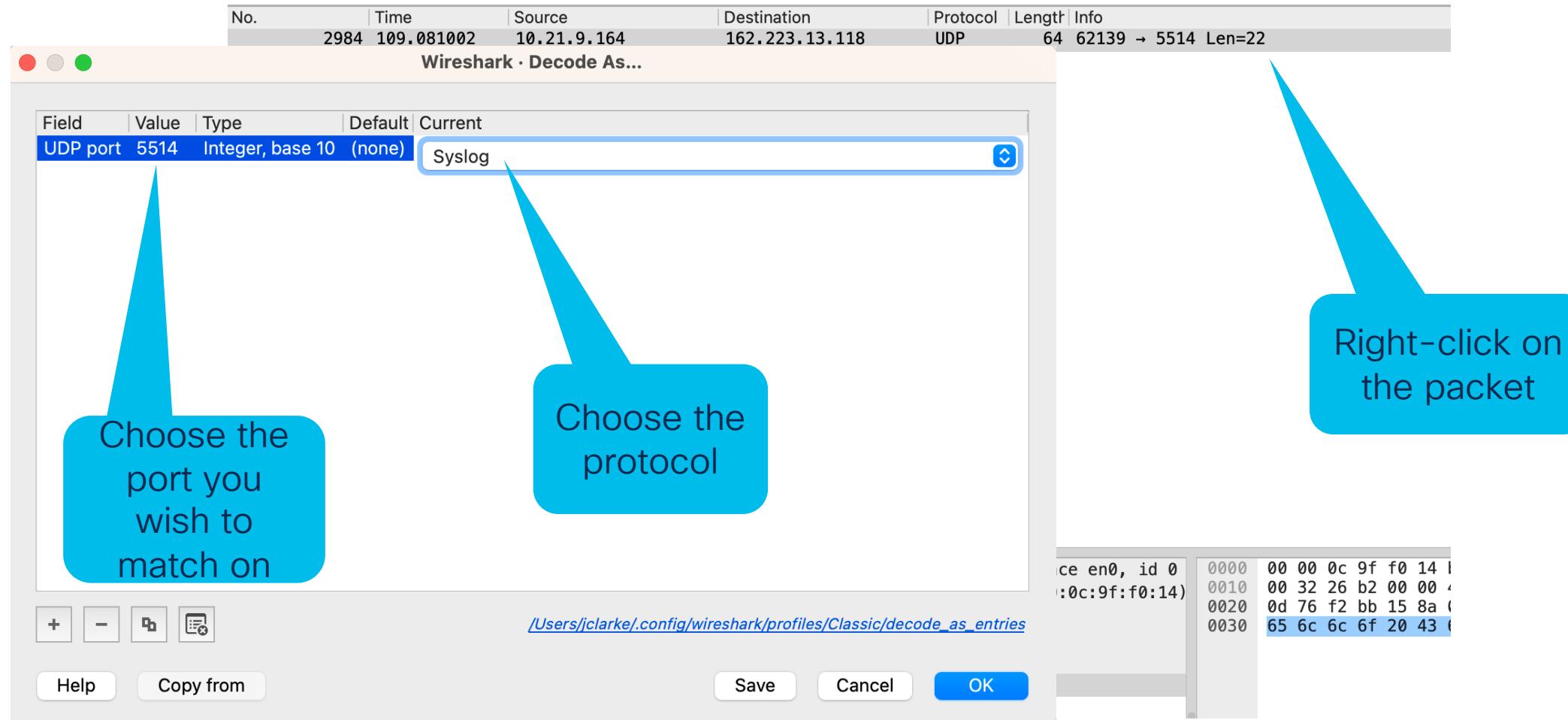
No.	Time	Source	Destination	Protocol	Length	Info
2984	109.081002	10.21.9.164	162.223.13.118	UDP	64	62139 → 5514 Len=22

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

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

0000	00 00 0c 9f f0 14	I
0010	00 32 26 b2 00 00	4
0020	0d 76 f2 bb 15 8a	0
0030	65 6c 6c 6f 20 43	6

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!
```

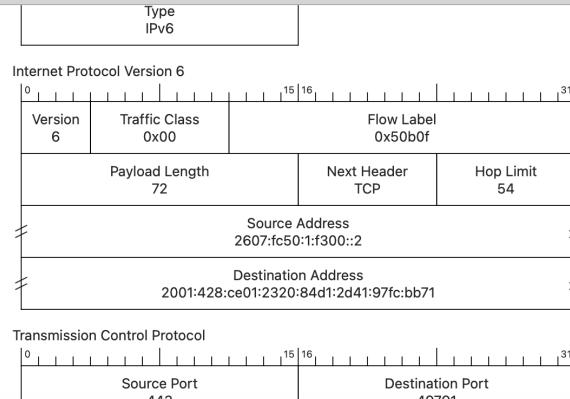
0000	00 00 0c 9f f0 14	I
0010	00 32 26 b2 00 00	^
0020	0d 76 f2 bb 15 8a	(
0030	65 6c 6c 6f 20 43)

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 TStamp=3527492959 TS...
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=4648 Win=126528 Len=0 TStamp=2345773811 TSecr=35...
405	11.0039..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01...	2607:fc50:1:f...	TCP	86	[TCP Window Update] 49791 → 443 [ACK] Seq=518 Ack=4648 Win=131072 Len=0 TStamp=3527492959 TS...
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
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 TStamp=2345773882 TSecr=35...
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 TStamp=3527493037 TSecr=35...
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 TStamp=3527493037 TSecr=35...
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 TStamp=3527493037 TSecr=35...
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=9033 Win=127232 Len=0 TStamp=2345773885 TSecr=35...
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 TStamp=3527493151 TS...
428	11.1211..	Apple_37:20:69	Cisco_a0:00:14	2001:428:ce01...	2607:fc50:1:f...	TLSv1.3	510	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 TStamp=3527493151 TSecr=35...
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 TStamp=3527493151 TSecr=35...
444	11.1875..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f...	2001:428:ce01...	TCP	1324	443 → 49791 [ACK] Seq=11509 Ack=1497 Win=66304 Len=1238 TStamp=3527493151 TSecr=35...
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 TStamp=3527493151 TSecr=35...
446	11.1875..	Cisco_32:72:42	Apple_37:20:69	2607:fc50:1:f...	2001:428:ce01...	TLSv1.3	126	Application Data

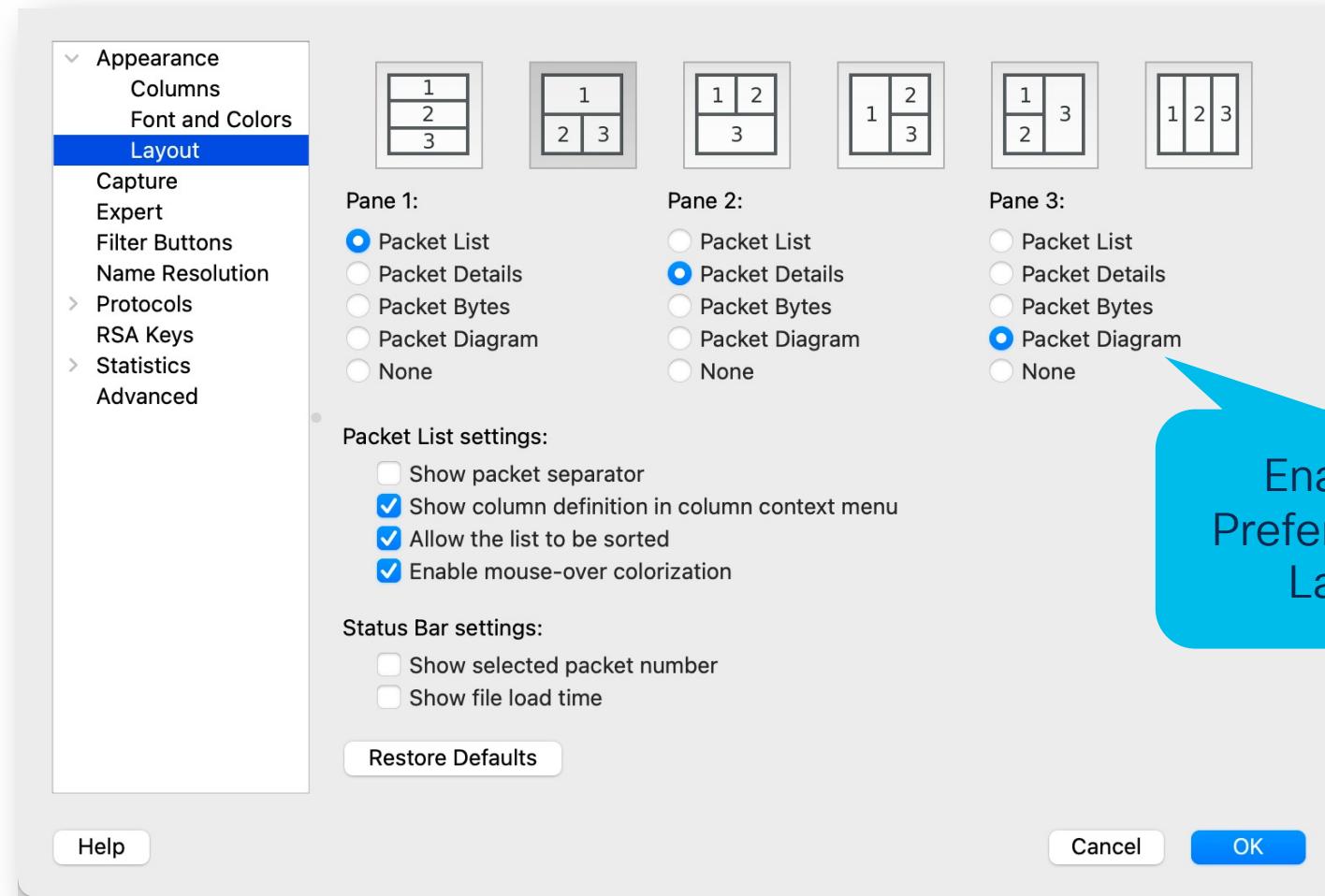
Frame 446: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface en0, id 0
Ethernet II, Src: Cisco_32:72:42 (8c:60:4f:32:72:42), Dst: Apple_37:20:69 (bc:d0:74:37:20:69)
Internet Protocol Version 6, Src: 2607:fc50:1:f300::2, Dst: 2001:428:ce01:2320:84d1:2d41:97fc:b010... = Version: 6
.... 0000 0000 = Traffic Class: 0x00 (DSCP: CS0, ECN: Not-ECT)
.... 0101 0000 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 4.0

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

Packet Diagrams



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: udpcdump	_____	Exported PDUs	—	—	—	—
(Wi-Fi remote capture: wifidump	_____	Remote capture dependent DLT	—	—	—	—

Enable promiscuous mode on all interfaces [Manage Interfaces...](#)

Capture filter for selected interfaces: Enter a capture filter ... [Compile BPFs](#)

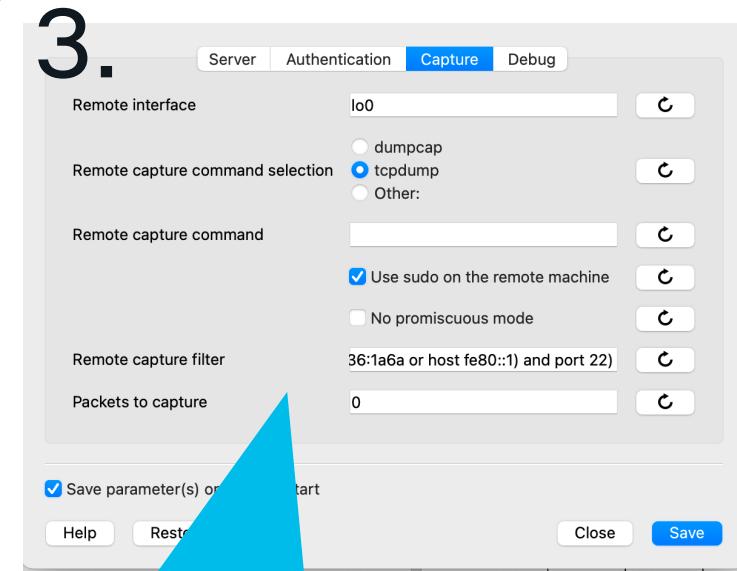
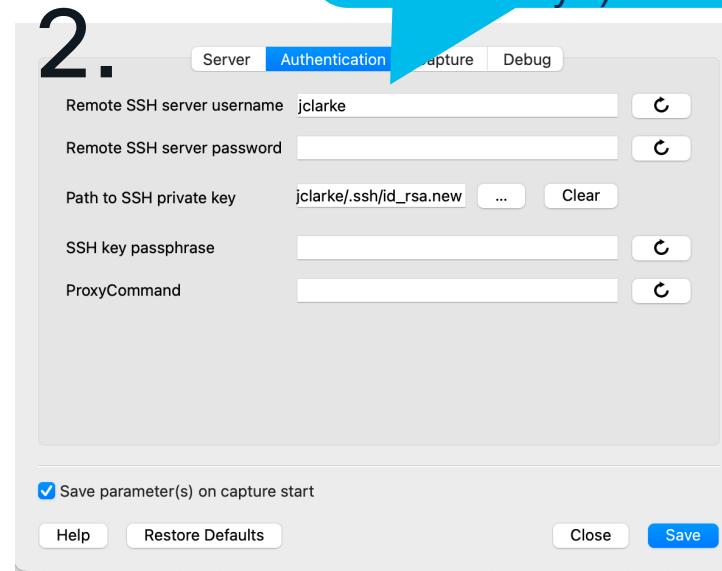
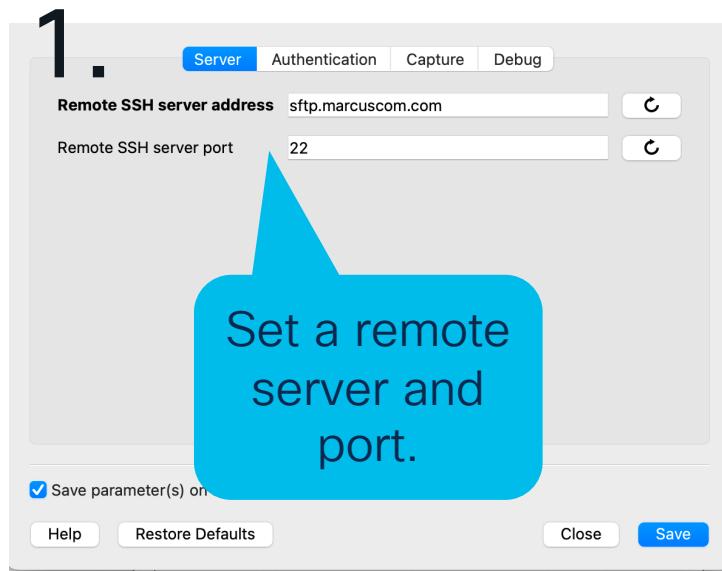
[Help](#) [Close](#) [Start](#)

- 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.#).0nn0d..A.rB.....x.M.....^'..i.?..X.J.....S...t...C?<..be.}..M8},e....+.....  

.....-.....@.....z..v..  

....._.....a.!7.83... .>..2.....N.Pu.;..U....?..V.....+....3.$... .=...._Ru4.S..)d..y[..H.....*k.....j.&I.....+l.|.....y.....F...
1.R..t.....0..d.8.Hco.....]k'7.R.'HIid-..8...0.....Ny..2..H.F..<.....#..`.....b..~.../[d...*.$'..*.N.r..x.V.c...C./K..y!.7.c;..9...P.).....P%$..[. ....  

4.G.H.:T.....'.....V..`DXwG ..N#sV.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^`.....0ecdIx.....J.....&(..d...9.p....l)...{.0 ..n.1!.|..R?..j.|..z'....L|....98b.;  

1.N".^t.!.....?.....|.^c.y.al1..v1]Z=-..J..t.|.....4...PGV...@.&.....c.z....9....].B>..X..~....].R....!J....d.4..L.....E..T....  

0..A..n.....WW...}.v.....z..I/p.C[..9....{.4C  

...kZ....i.C.=?..T..t....Qx..0.....5'G.s..#.a.o....(N&u.)...  

c.[...,t....~{..#.ZL.T.AP.....Y..[....f..~]&..tpe..`t..l.=...)....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..{v{6/$/.C..A.....V..R.Ics..DM..RwyFV..>.....\0..[...  

.e.....Lc.oFU...W.....I..5....j..WL...}w.j.....a.....E..f'..8t..h...~x.b...t..EM7ls]...6..}V...P*....r.],.....1.n.A...Q .....[..h.U.s..h.  

....._w'{..G;~`..A..F..Ph..V.4.9Z..A.  

..0...A....>M.....4Cy....sr.E+r.p...."Q..Bq. [>V....WKM....+.5...&..G....B....J..3..N--....V..aAU+<....7^....W....C.4.;q....P..,\..<..B.<..R..tJ.m#.,*....|  

kvvi+gS1.mT..Y.....M..A%.K...o..{.J..A..12..oW..KN~.....<..,D..6..0(!^..'  

...f.M..a..o.....C..m..!*S<1.....d...Y$&..Ui:..g.2.....(<..,g..(.GD=.....<..A..L..v$Q.m.....;.....0.....I..G^..d..".....I..=v.....  

2.zp...../..Gg0..dT..@m.l~..p..L..j9..2....n.2.).....x.....C..Y..0..Z..I..M../.4.Bmx..iGINF!.3.4....~..b+..J...  

.t..x..p..{....5ZG.E'..u..yt..V..  

...|w:..Q.  

...Q..of....A;>;x..H..x..2..X0.a.H.N.0....Z}..[..B....}.. .....pv.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.....!`.....<j4.....r..Q....a.Q.  

x..?z4..D..g..I..E...../..B..T..".4.....%Tw....d....G..P:#..3..N..6\o.A.....i..W$({....i..0..}.C.7....<e.. ..!C ..5"....FAt.o..W..n|..X....`.....[....  

4..S..p:.*....R.....:1....!d..V*..w[....Vt....0.E ..S....3..}..P..k..u..Foy)..m..-o.=.%&P=w..%,..b..B...  

ly.$....p....T+f..d8-t..#Yi..@[~<..x..4....hRW....k....Q..Y.....U..6I.....Z..q....._7+W.....2e..a....Zt.....K..L..$....B#.}.....a....K..85....p4W..!  

Uj.._L..V..V..P..&..ZqR..AS.ogh?..{M9..`..P..4..HR ..k..F..0..(u..g.....Th....T..L..m....=H..4g..//..cF..s....T.. /....i....3h..G.  

...`.....#....y..FR$....4....p..C.....d..itd  

@hb..F..5..X  

9..t..  

..G..S ..j0..3....%..i..3..Q..}|D....0..>C..*..1..c..Sk..3..L..B..l..3Be..*..h&4..(..D..dV...h2....T.  

8..6..h....*ft....r.....U....-..I}.....V..E..S..G.....z^..&1..6]..DB..hu..A..>....n.."Dq..Hi.....\..Bq"....0G6..0....^..&..|..)....0K..wV0..c.....^..<.....5  

...?..A..GU..ve..M..*,..{....^....qH..E#R..aj..C.....Z..=;..)$p....y..}..2..0..q....`..b..%..6..ci..%..m..(....2 ..#3 ..o..h..[..u..a..>....J..a....K ..7..}.  

5....5.....,..E..&..5H..Yp..!..y..0..R....1....)".....3p;....H..ig..>..3..ij.....I..N..58....C$..r..1L..L..F..-..P..M..=..e..j.....7....s..[uXN..Zh..i..t...  

(_..xn..Ig..AG.._..f.....^..g..0..IiBeJ..246..</..0..<....~..l..`..S..:..rw..... O..w.....I..R..<....P..CG).  

.....k..E..* ..$Fz....ud..Y4T{....V-k$N(..9..%p..G..$TT..oxf!..;..p.....C.....m..{..D'.eld[....a..H.....$.4]a.. ..p....@....r....qlj..IG.  

7....3....\..>..c..o..Et..EZ..0..:..U..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..c....&"E..Aj.....1..E..}..a..0.....#.W..{..6}..,..4..K.  

..Sl..H..$..Rm..d..`1  

.....J..OsR..m..uc..0.....t..u..U...  

5 client pkts, 603 server pkts, 7 turns.
```

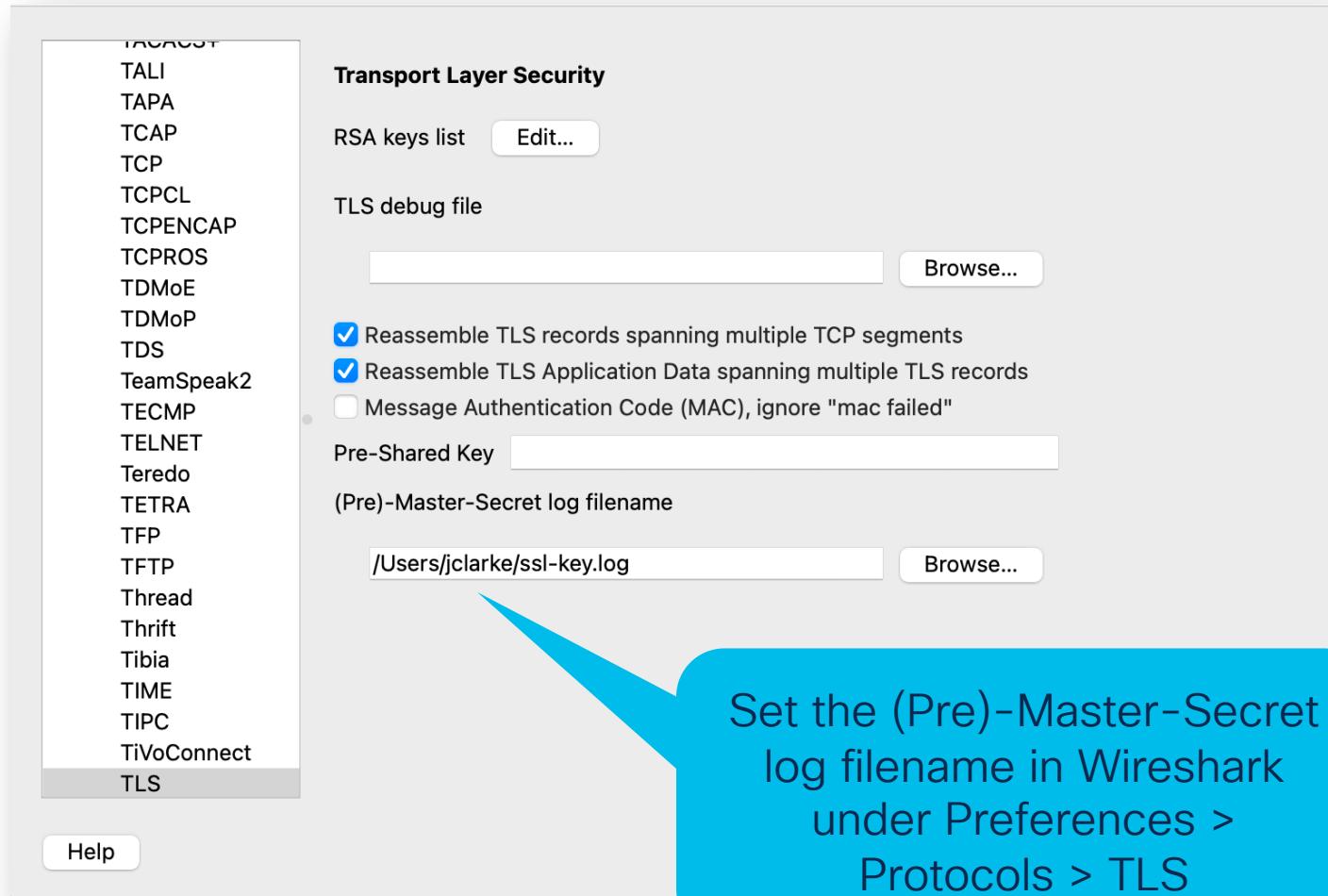
Well this isn't terribly useful...

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

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,*/*;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=el25xoAiIe009cwh6Es30Ng3WGU6MTY4NjA20Dcw0DA4NTUxMTk3NQ

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="el25xoAiIe009cwh6Es30Ng3WGU6MTY4NjA20Dcw0DA4NTUxMTk3NQ" />
    <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!

It's Your Turn

- Get Wireshark (if you don't have it)
- Make use of its powerful features to rule your network
- Keep flowin'

Get Wireshark



These Slides





The bridge to possible

Thank you

cisco *Live!*

#CiscoLive

cisco *Live!*

Let's go

#CiscoLive