MUHAMMAD ARIFF BIN
BAHARUDIN

Introduction to: WIRESHARK

Objectives

1. Understand what Wireshark is and its significance in network analysis
2. Refresh basic networking concepts relevant to Wireshark.
3. Learn how to install, configure and navigate Wireshark.

What is Wireshark?

- Definition: Wireshark is the world’s foremost network protocol analyzer.
- Purpose: It lets you see what’s happening on your network at a microscopic level.
- Usage: Essential for network troubleshooting, analysis, software and protocol development.

Importance of Wireshark

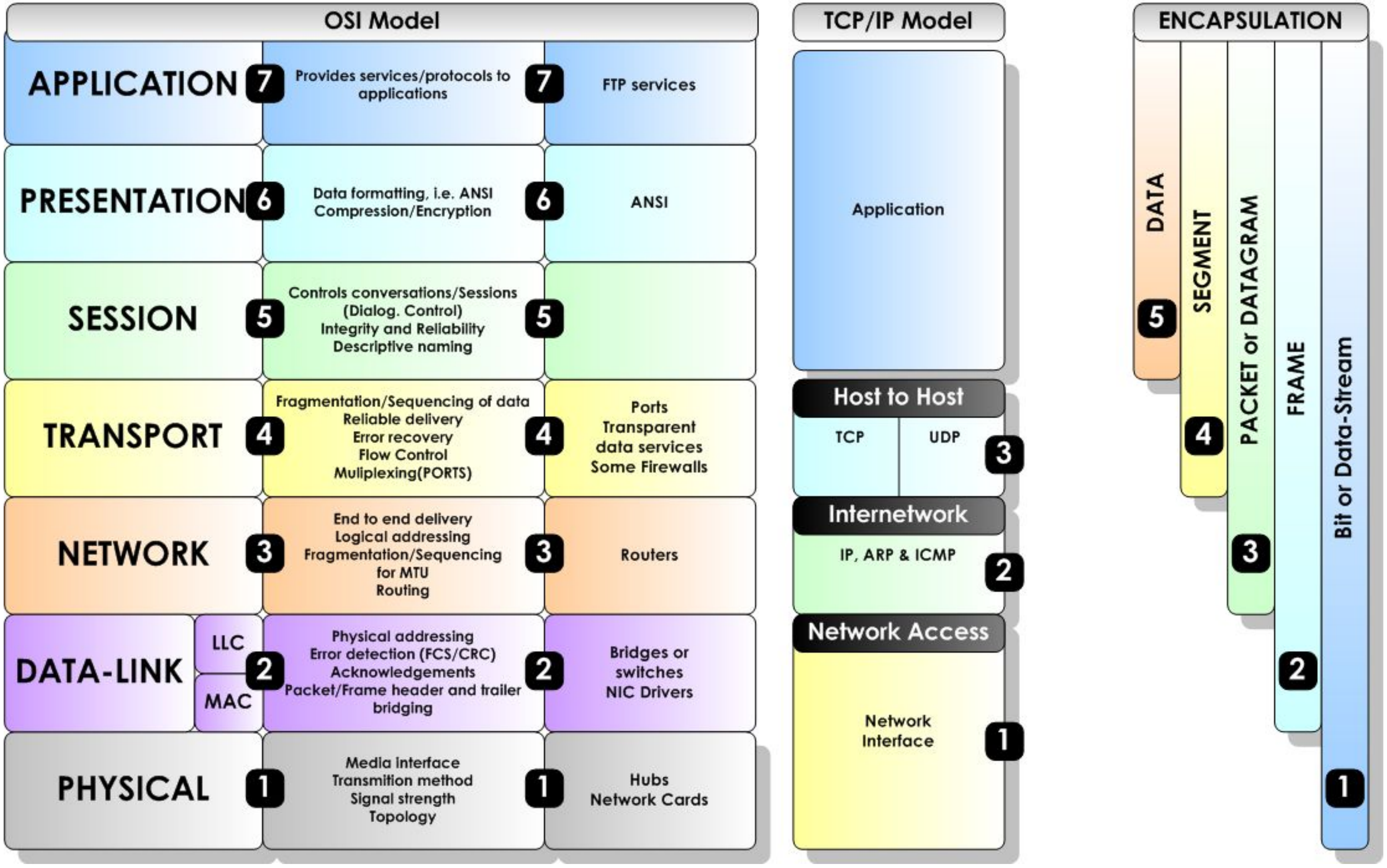
- Troubleshooting: Quickly identify and resolve network issues.
- Security Analysis: Detect network intrusions and vulnerabilities.
- Education: Learn about network protocols and their behavior

Real-world application

- Network Performance Monitoring
- Detecting Security Breaches
- Troubleshooting Network Problems
- Analyzing and developing Protocols.

The OSI Model (Open Systems Interconnection)

www.networkstuff.eu



OSI Model

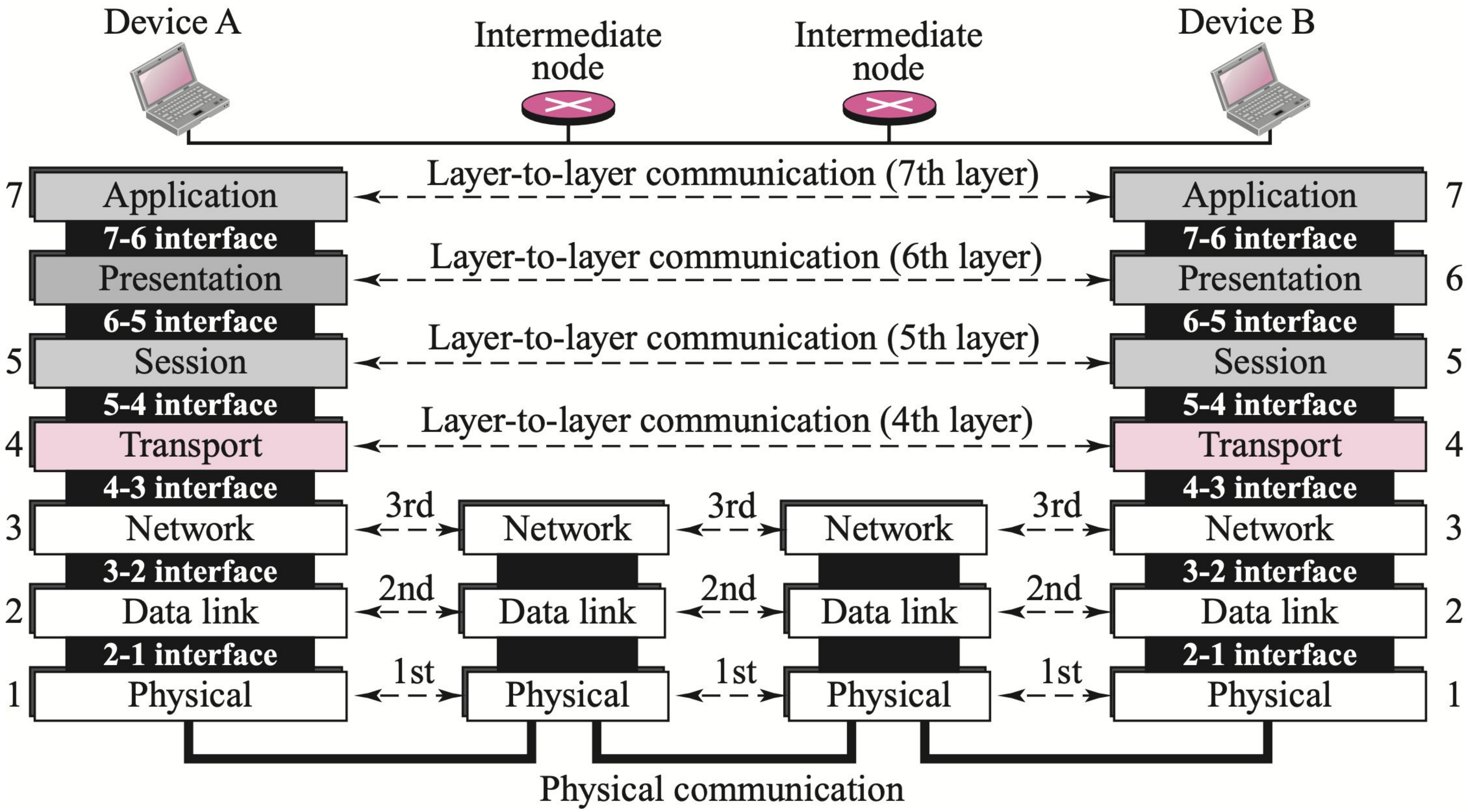
APPLICATION		7	Provides services/protocols to applications	7	FTP services
PRESENTATION		6	Data formatting, i.e. ANSI Compression/Encryption	6	ANSI
SESSION		5	Controls conversations/Sessions (Dialog. Control) Integrity and Reliability Descriptive naming	5	
TRANSPORT		4	Fragmentation/Sequencing of data Reliable delivery Error recovery Flow Control Muliplexing(PORTS)	4	Ports Transparent data services Some Firewalls
NETWORK		3	End to end delivery Logical addressing Fragmentation/Sequencing for MTU Routing	3	Routers
DATA-LINK	LLC MAC	2	Physical addressing Error detection (FCS/CRC) Acknowledgements Packet/Frame header and trailer bridging	2	Bridges or switches NIC Drivers
PHYSICAL		1	Media Interface Transmition method Signal strength Topology	1	Hubs Network Cards

TCP/IP Model

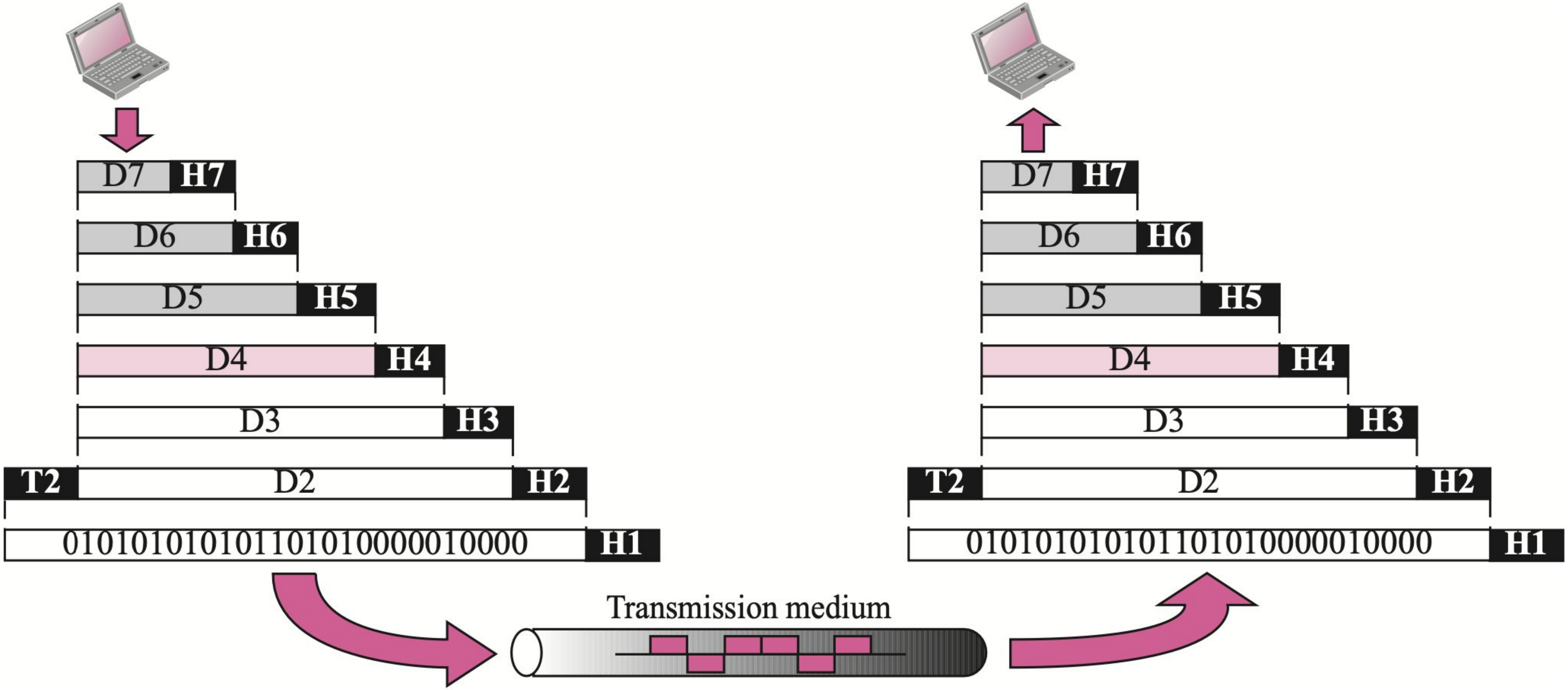
Application		
Host to Host	TCP UDP	3
Internetwork	IP, ARP & ICMP	2
Network Access	Network Interface	1

ENCAPSULATION

DATA	5
SEGMENT	4
PACKET or DATAGRAM	3
FRAME	2
Bit or Data-Stream	1



Device A
Intermediate node
Intermediate node
Device B
7 Application
Layer-to-layer communication (7th layer)
Application 7
7-6 interface
7-6 interface
Presentation
Layer-to-layer communication (6th layer)
Presentation 6
6-5 interface
6-5 interface
5 Session
Layer-to-layer communication (5th layer)
Session 5
5-4 interface
5-4 interface
4 Transport
Layer-to-layer communication (4th layer)
Transport 4
4-3 interface
4-3 interface
3 Network
3rd
Network
3rd
Network
3rd
Network 3
3-2 interface
3-2 interface
2 Data link
2nd
Data link
2nd
Data link
2nd
Data link 2
2-1 interface
2-1 interface
1 Physical
1st
Physical
1st
Physical
1st
Physical 1
Physical communication


D7
H7
D6
H6
D5
H5
D4
H4
D3
H3
T2
D2
H2
01010101010101101010000010000
H1
Transmission medium
D7
H7
D6
H6
D5
H5
D4
H4
D3
H3
T2
D2
H2
01010101010101101010000010000
H1

TCP

Figure 15.9 *Connection establishment using three-way handshaking*

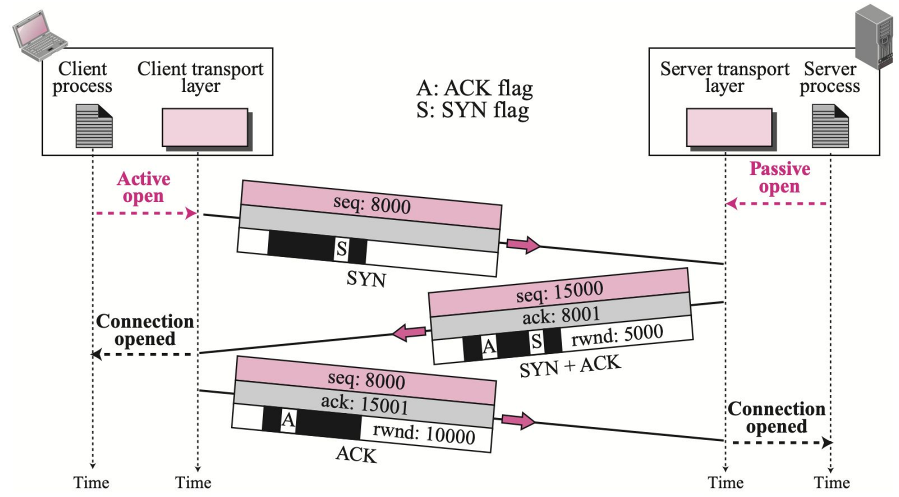


Figure 15.11 *Connection termination using three-way handshaking*

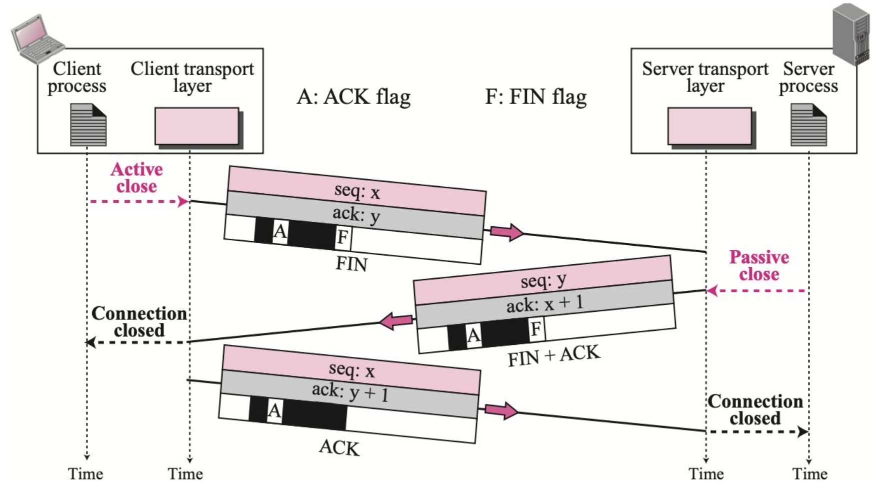
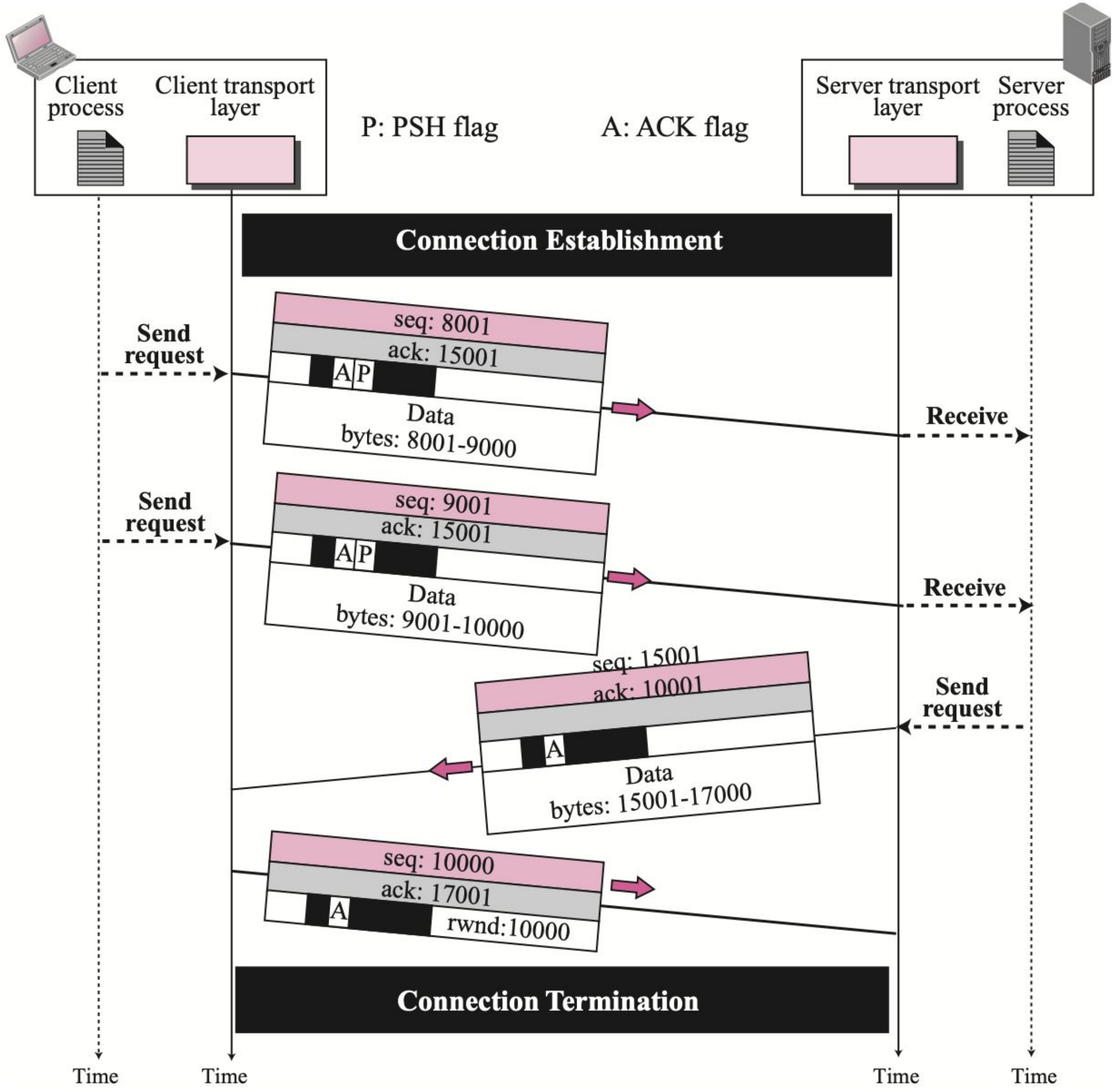
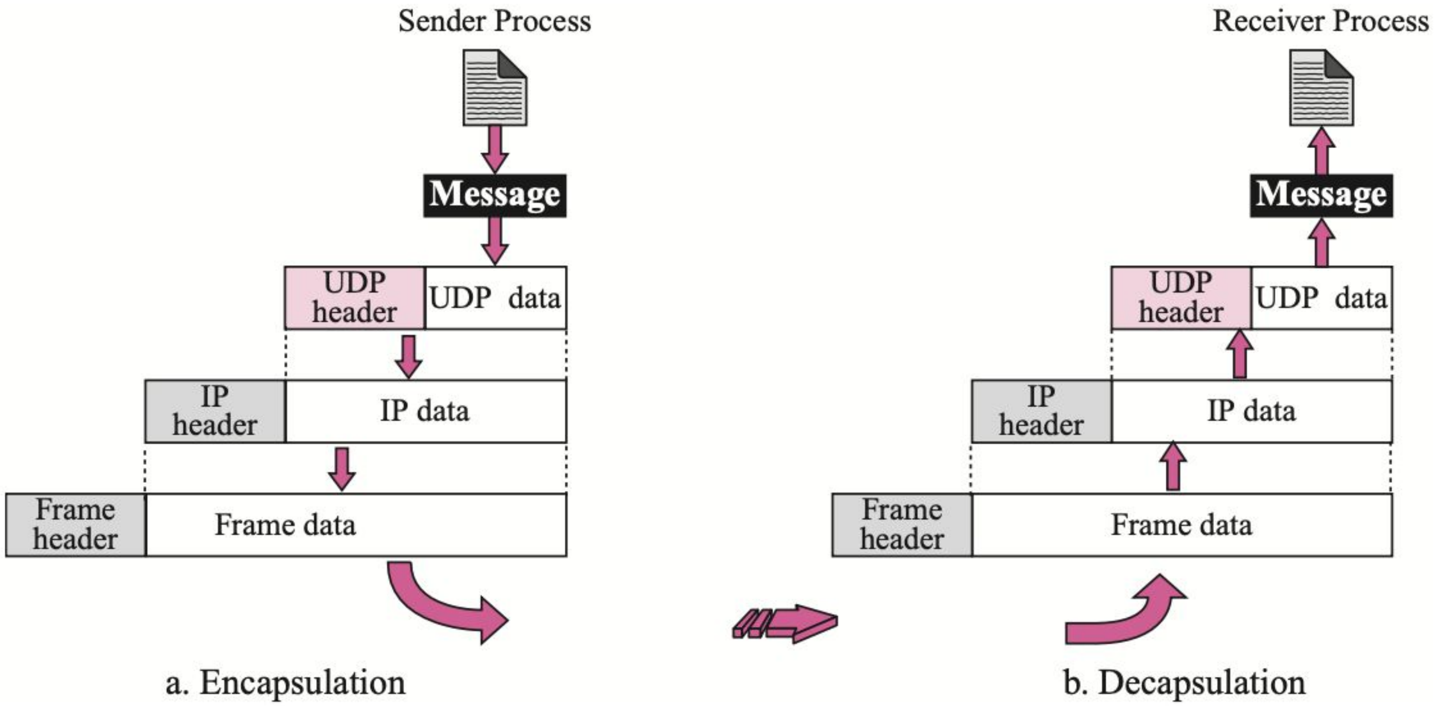


Figure 15.10 *Data transfer*



UDP

Figure 14.5 *Encapsulation and decapsulation*



a. Encapsulation

b. Decapsulation

DN
S

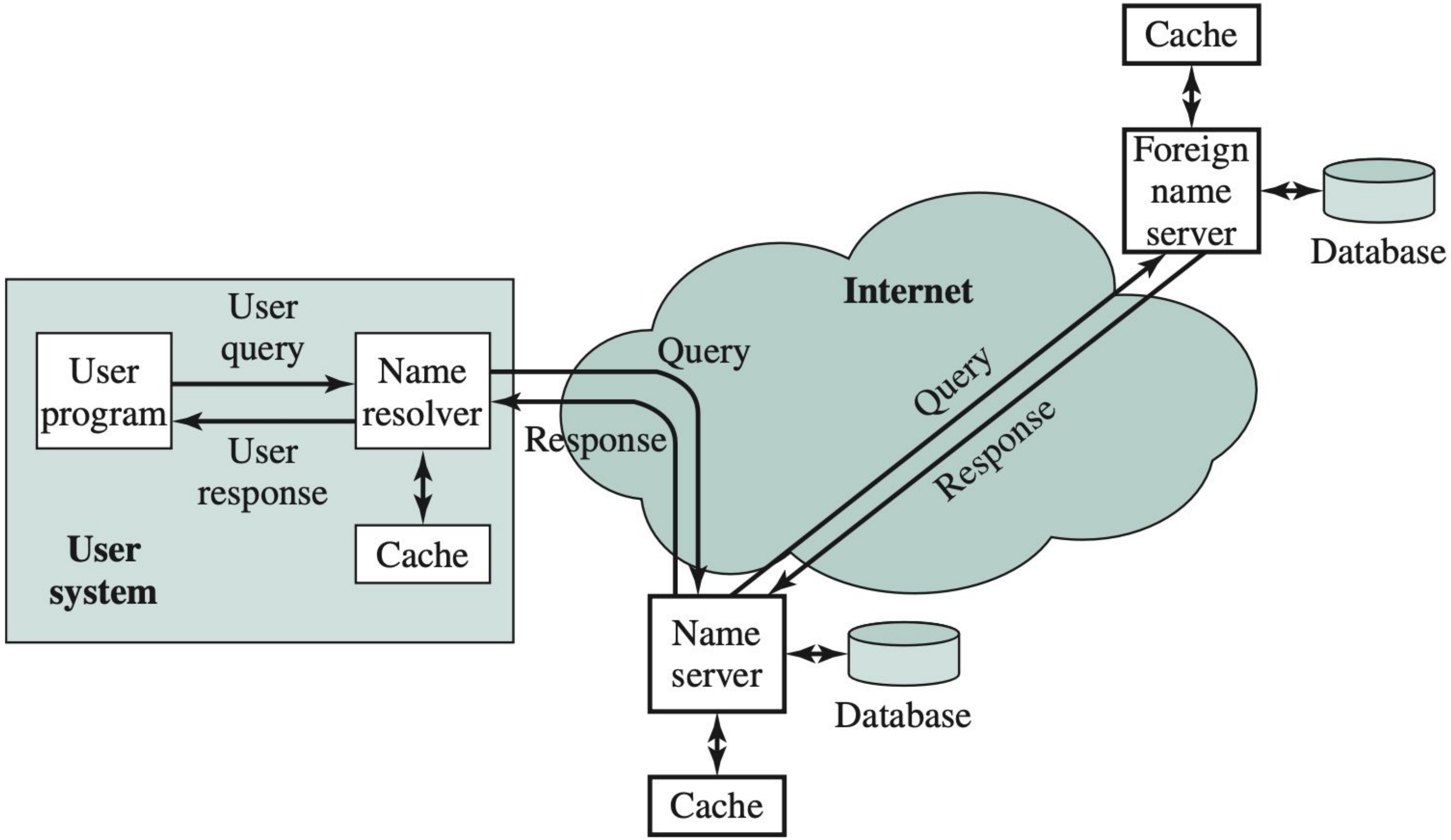
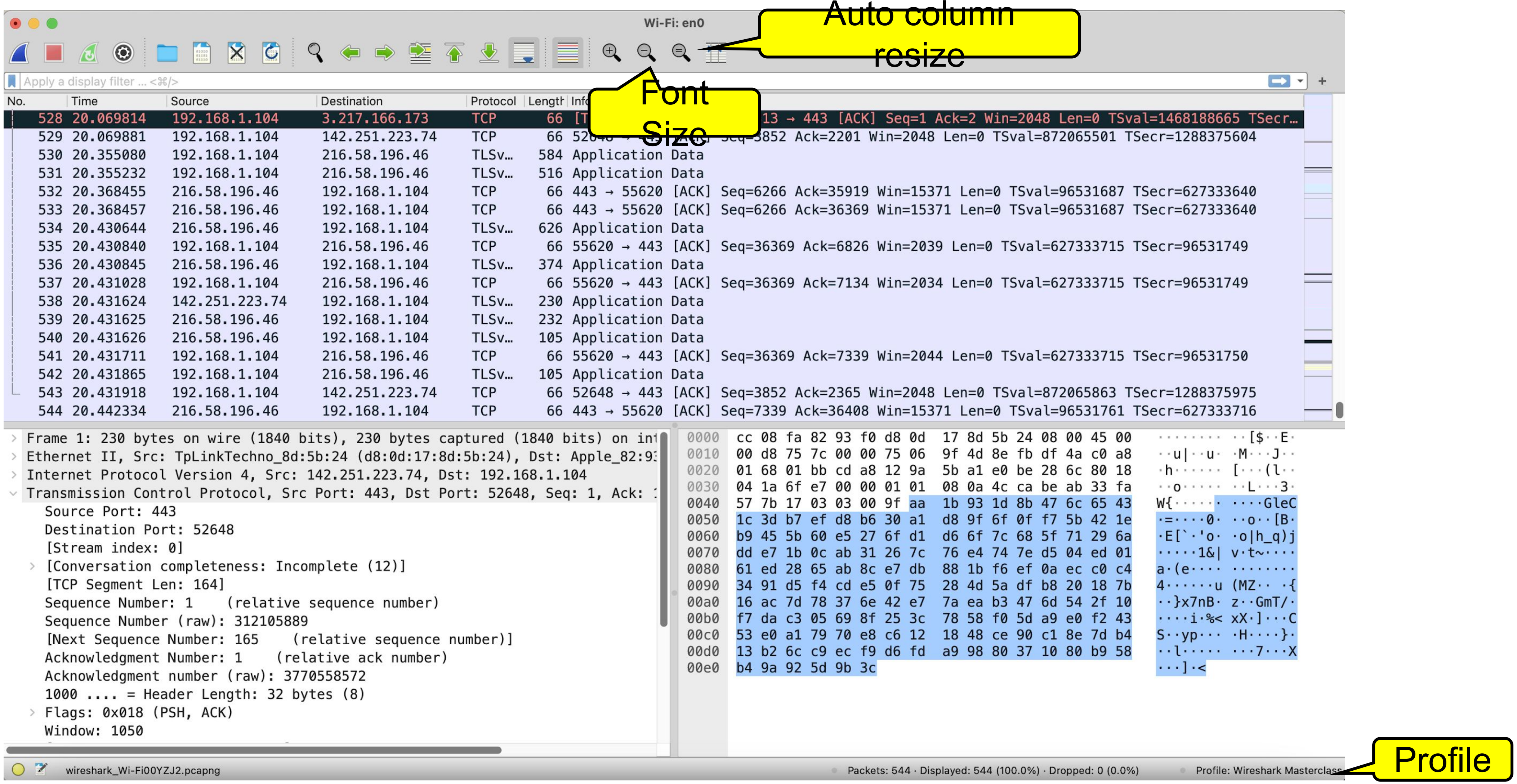


Figure 24.6 DNS Name Resolution

Configuring Wireshark



Wi-Fi: en0

Auto column resize

Font Size

Profile

Apply a display filter … <⌘/>

```
No.   Time       Source          Destination     Protocol Length Info
  528 20.069814  192.168.1.104   3.217.166.173   TCP        66 [T    13 → 443 [ACK] Seq=1 Ack=2 Win=2048 Len=0 TSval=1468188665 TSecr…
  529 20.069881  192.168.1.104   142.251.223.74  TCP        66 526        Seq=3852 Ack=2201 Win=2048 Len=0 TSval=872065501 TSecr=1288375604
  530 20.355080  192.168.1.104   216.58.196.46   TLSv…     584 Application Data
  531 20.355232  192.168.1.104   216.58.196.46   TLSv…     516 Application Data
  532 20.368455  216.58.196.46   192.168.1.104   TCP        66 443 → 55620 [ACK] Seq=6266 Ack=35919 Win=15371 Len=0 TSval=96531687 TSecr=627333640
  533 20.368457  216.58.196.46   192.168.1.104   TCP        66 443 → 55620 [ACK] Seq=6266 Ack=36369 Win=15371 Len=0 TSval=96531687 TSecr=627333640
  534 20.430644  216.58.196.46   192.168.1.104   TLSv…     626 Application Data
  535 20.430840  192.168.1.104   216.58.196.46   TCP        66 55620 → 443 [ACK] Seq=36369 Ack=6826 Win=2039 Len=0 TSval=627333715 TSecr=96531749
  536 20.430845  216.58.196.46   192.168.1.104   TLSv…     374 Application Data
  537 20.431028  192.168.1.104   216.58.196.46   TCP        66 55620 → 443 [ACK] Seq=36369 Ack=7134 Win=2034 Len=0 TSval=627333715 TSecr=96531749
  538 20.431624  142.251.223.74  192.168.1.104   TLSv…     230 Application Data
  539 20.431625  216.58.196.46   192.168.1.104   TLSv…     232 Application Data
  540 20.431626  216.58.196.46   192.168.1.104   TLSv…     105 Application Data
  541 20.431711  192.168.1.104   216.58.196.46   TCP        66 55620 → 443 [ACK] Seq=36369 Ack=7339 Win=2044 Len=0 TSval=627333715 TSecr=96531750
  542 20.431865  192.168.1.104   216.58.196.46   TLSv…     105 Application Data
  543 20.431918  192.168.1.104   142.251.223.74  TCP        66 52648 → 443 [ACK] Seq=3852 Ack=2365 Win=2048 Len=0 TSval=872065863 TSecr=1288375975
  544 20.442334  216.58.196.46   192.168.1.104   TCP        66 443 → 55620 [ACK] Seq=7339 Ack=36408 Win=15371 Len=0 TSval=96531761 TSecr=627333716
```

```
> Frame 1: 230 bytes on wire (1840 bits), 230 bytes captured (1840 bits) on int
> Ethernet II, Src: TpLinkTechno_8d:5b:24 (d8:0d:17:8d:5b:24), Dst: Apple_82:93
> Internet Protocol Version 4, Src: 142.251.223.74, Dst: 192.168.1.104
v Transmission Control Protocol, Src Port: 443, Dst Port: 52648, Seq: 1, Ack: 1
    Source Port: 443
    Destination Port: 52648
    [Stream index: 0]
  > [Conversation completeness: Incomplete (12)]
    [TCP Segment Len: 164]
    Sequence Number: 1    (relative sequence number)
    Sequence Number (raw): 312105889
    [Next Sequence Number: 165    (relative sequence number)]
    Acknowledgment Number: 1    (relative ack number)
    Acknowledgment number (raw): 3770558572
    1000 .... = Header Length: 32 bytes (8)
  > Flags: 0x018 (PSH, ACK)
    Window: 1050
```

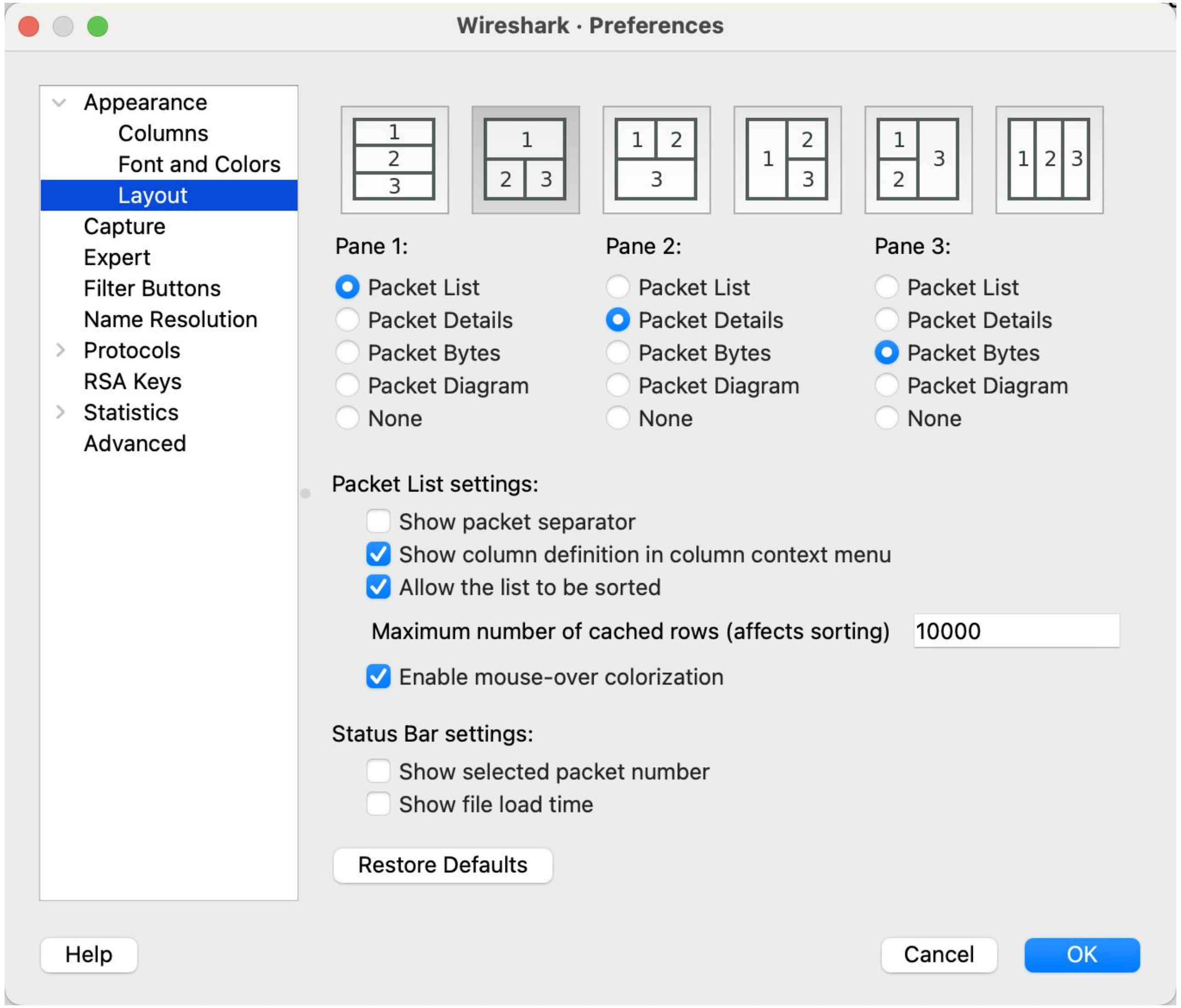
```
0000  cc 08 fa 82 93 f0 d8 0d  17 8d 5b 24 08 00 45 00   ········ ··[$··E·
0010  00 d8 75 7c 00 00 75 06  9f 4d 8e fb df 4a c0 a8   ··u|··u· ·M···J··
0020  01 68 01 bb cd a8 12 9a  5b a1 e0 be 28 6c 80 18   ·h······ [···(l··
0030  04 1a 6f e7 00 00 01 01  08 0a 4c ca be ab 33 fa   ··o····· ··L···3·
0040  57 7b 17 03 03 00 9f aa  1b 93 1d 8b 47 6c 65 43   W{······ ····GleC
0050  1c 3d b7 ef d8 b6 30 a1  d8 9f 6f 0f f7 5b 42 1e   ·=····0· ··o··[B·
0060  b9 45 5b 60 e5 27 6f d1  d6 6f 7c 68 5f 71 29 6a   ·E[`·'o· ·o|h_q)j
0070  dd e7 1b 0c ab 31 26 7c  76 e4 74 7e d5 04 ed 01   ·····1&| v·t~····
0080  61 ed 28 65 ab 8c e7 db  88 1b f6 ef 0a ec c0 c4   a·(e···· ········
0090  34 91 d5 f4 cd e5 0f 75  28 4d 5a df b8 20 18 7b   4······u (MZ·· ·{
00a0  16 ac 7d 78 37 6e 42 e7  7a ea b3 47 6d 54 2f 10   ··}x7nB· z··GmT/·
00b0  f7 da c3 05 69 8f 25 3c  78 58 f0 5d a9 e0 f2 43   ····i·%< xX·]···C
00c0  53 e0 a1 79 70 e8 c6 12  18 48 ce 90 c1 8e 7d b4   S··yp··· ·H····}·
00d0  13 b2 6c c9 ec f9 d6 fd  a9 98 80 37 10 80 b9 58   ··l····· ···7···X
00e0  b4 9a 92 5d 9b 3c                                  ···]·<
```

wireshark_Wi-Fi00YZJ2.pcapng

Packets: 544 · Displayed: 544 (100.0%) · Dropped: 0 (0.0%)

Profile: Wireshark Masterclass

Configuring Wireshark - layout



Wireshark · Preferences

Pane 1:	Pane 2:	Pane 3:
● Packet List	○ Packet List	○ Packet List
○ Packet Details	● Packet Details	○ Packet Details
○ Packet Bytes	○ Packet Bytes	● Packet Bytes
○ Packet Diagram	○ Packet Diagram	○ Packet Diagram
○ None	○ None	○ None

Packet List settings:

- □ Show packet separator
- ☑ Show column definition in column context menu
- ☑ Allow the list to be sorted

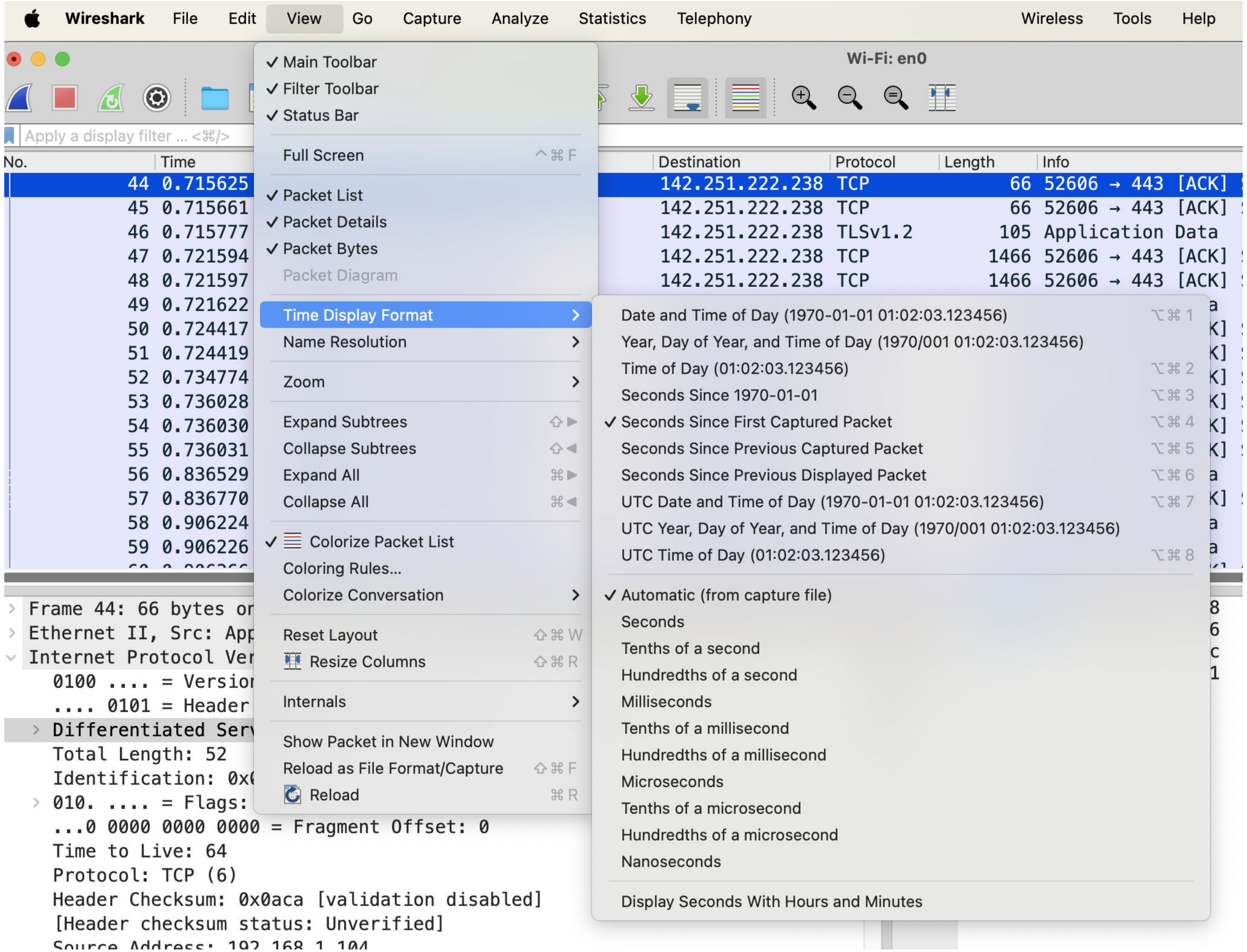
Maximum number of cached rows (affects sorting) 10000

- ☑ Enable mouse-over colorization

Status Bar settings:

- □ Show selected packet number
- □ Show file load time

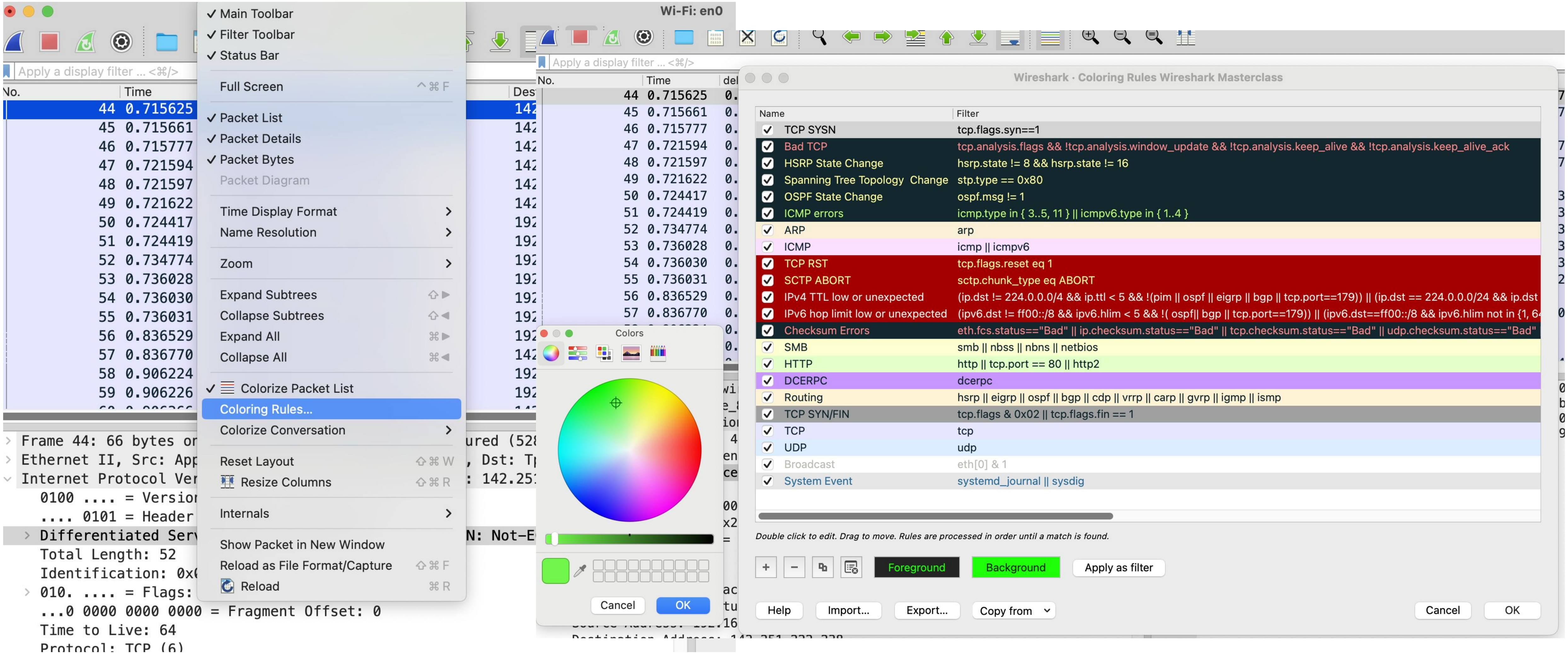
Configuring Wireshark – time format


Wireshark
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Wi-Fi: en0
Apply a display filter ... <⌘/>
✓ Main Toolbar
✓ Filter Toolbar
✓ Status Bar
Full Screen ^⌘F
✓ Packet List
✓ Packet Details
✓ Packet Bytes
Packet Diagram
Time Display Format
Name Resolution
Zoom
Expand Subtrees ⇧▶
Collapse Subtrees ⇧◀
Expand All ⌘▶
Collapse All ⌘◀
✓ Colorize Packet List
Coloring Rules...
Colorize Conversation
Reset Layout ⇧⌘W
Resize Columns ⇧⌘R
Internals
Show Packet in New Window
Reload as File Format/Capture ⇧⌘F
Reload ⌘R
Date and Time of Day (1970-01-01 01:02:03.123456) ⌥⌘1
Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
Time of Day (01:02:03.123456) ⌥⌘2
Seconds Since 1970-01-01 ⌥⌘3
✓ Seconds Since First Captured Packet ⌥⌘4
Seconds Since Previous Captured Packet ⌥⌘5
Seconds Since Previous Displayed Packet ⌥⌘6
UTC Date and Time of Day (1970-01-01 01:02:03.123456) ⌥⌘7
UTC Year, Day of Year, and Time of Day (1970/001 01:02:03.123456)
UTC Time of Day (01:02:03.123456) ⌥⌘8
✓ Automatic (from capture file)
Seconds
Tenths of a second
Hundredths of a second
Milliseconds
Tenths of a millisecond
Hundredths of a millisecond
Microseconds
Tenths of a microsecond
Hundredths of a microsecond
Nanoseconds
Display Seconds With Hours and Minutes

```
No.  Time        Destination      Protocol  Length  Info
  44 0.715625    142.251.222.238  TCP           66  52606 → 443 [ACK]
  45 0.715661    142.251.222.238  TCP           66  52606 → 443 [ACK]
  46 0.715777    142.251.222.238  TLSv1.2      105  Application Data
  47 0.721594    142.251.222.238  TCP         1466  52606 → 443 [ACK]
  48 0.721597    142.251.222.238  TCP         1466  52606 → 443 [ACK]
  49 0.721622
  50 0.724417
  51 0.724419
  52 0.734774
  53 0.736028
  54 0.736030
  55 0.736031
  56 0.836529
  57 0.836770
  58 0.906224
  59 0.906226
```

```
> Frame 44: 66 bytes or
> Ethernet II, Src: App
v Internet Protocol Ver
    0100 .... = Versior
    .... 0101 = Header
  > Differentiated Serv
    Total Length: 52
    Identification: 0x(
  > 010. .... = Flags:
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
    Header Checksum: 0x0aca [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.104
```

Configuring Wireshark – coloring rules



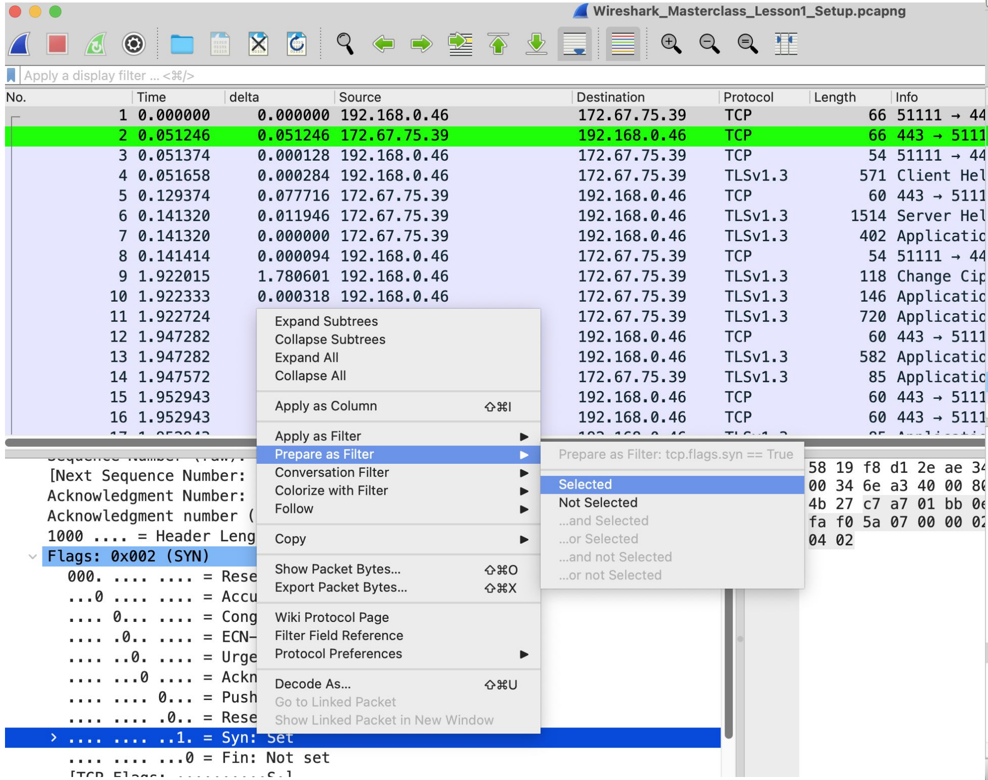
```
44 0.715625
45 0.715661
46 0.715777
47 0.721594
48 0.721597
49 0.721622
50 0.724417
51 0.724419
52 0.734774
53 0.736028
54 0.736030
55 0.736031
56 0.836529
57 0.836770
58 0.906224
59 0.906226
```

```
> Frame 44: 66 bytes or
> Ethernet II, Src: App
v Internet Protocol Ver
    0100 .... = Versior
    .... 0101 = Header
  > Differentiated Serv
    Total Length: 52
    Identification: 0x0
  > 010. .... = Flags:
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: TCP (6)
```

Name	Filter
☑ TCP SYSN	tcp.flags.syn==1
☑ Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
☑ HSRP State Change	hsrp.state != 8 && hsrp.state != 16
☑ Spanning Tree Topology Change	stp.type == 0x80
☑ OSPF State Change	ospf.msg != 1
☑ ICMP errors	icmp.type in { 3..5, 11 } || icmpv6.type in { 1..4 }
☑ ARP	arp
☑ ICMP	icmp || icmpv6
☑ TCP RST	tcp.flags.reset eq 1
☑ SCTP ABORT	sctp.chunk_type eq ABORT
☑ IPv4 TTL low or unexpected	(ip.dst != 224.0.0.0/4 && ip.ttl < 5 && !(pim || ospf || eigrp || bgp || tcp.port==179)) || (ip.dst == 224.0.0.0/24 && ip.dst
☑ IPv6 hop limit low or unexpected	(ipv6.dst != ff00::/8 && ipv6.hlim < 5 && !(ospf|| bgp || tcp.port==179)) || (ipv6.dst==ff00::/8 && ipv6.hlim not in {1, 6
☑ Checksum Errors	eth.fcs.status=="Bad" || ip.checksum.status=="Bad" || tcp.checksum.status=="Bad" || udp.checksum.status=="Bad"
☑ SMB	smb || nbss || nbns || netbios
☑ HTTP	http || tcp.port == 80 || http2
☑ DCERPC	dcerpc
☑ Routing	hsrp || eigrp || ospf || bgp || cdp || vrrp || carp || gvrp || igmp || ismp
☑ TCP SYN/FIN	tcp.flags & 0x02 || tcp.flags.fin == 1
☑ TCP	tcp
☑ UDP	udp
☑ Broadcast	eth[0] & 1
☑ System Event	systemd_journal || sysdig

Double click to edit. Drag to move. Rules are processed in order until a match is found.

Configuring Wireshark – buttons



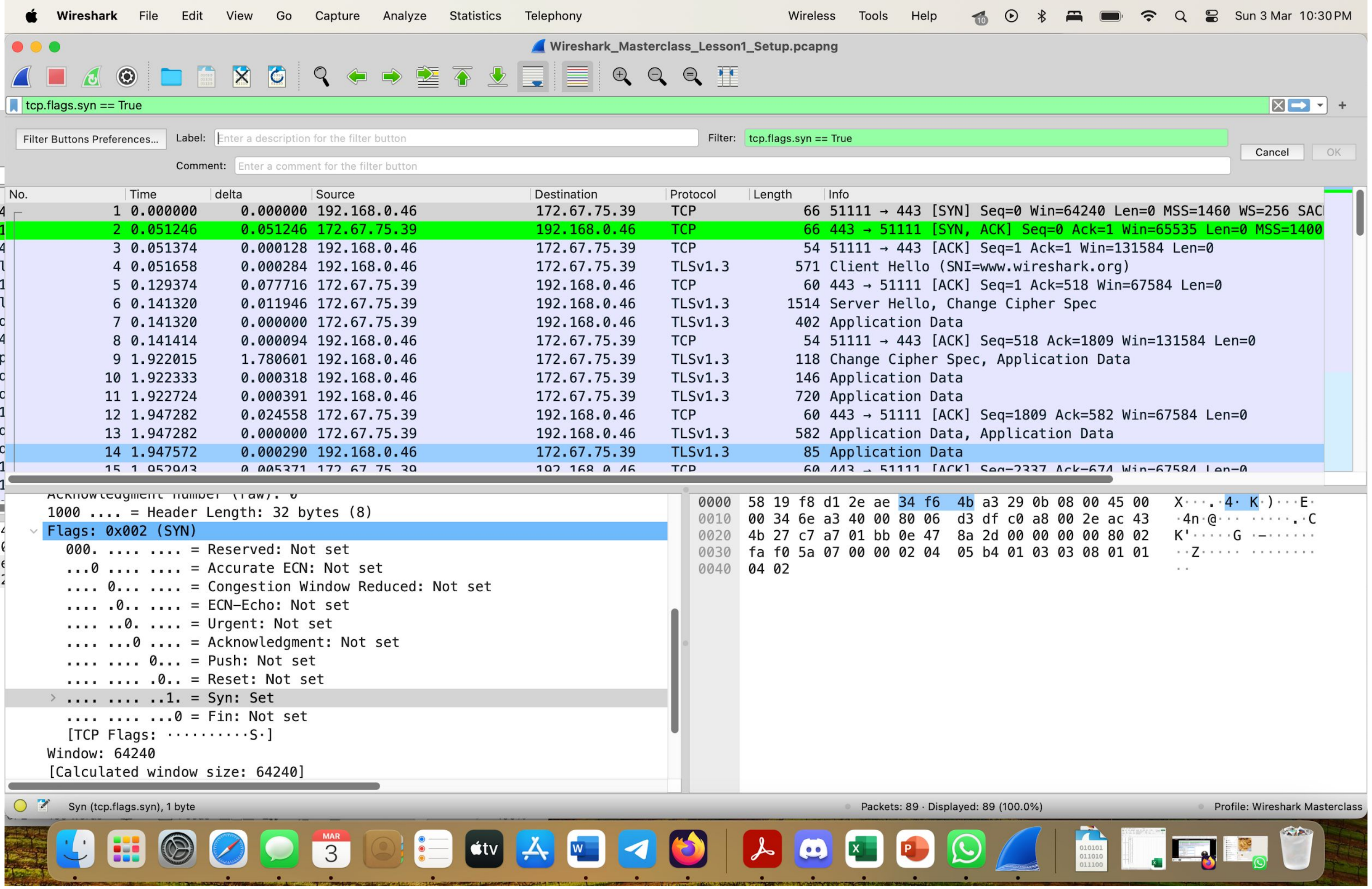
Wireshark_Masterclass_Lesson1_Setup.pcapng

Apply a display filter … <⌘/>

```
No.     Time      delta     Source          Destination    Protocol  Length Info
      1 0.000000  0.000000 192.168.0.46    172.67.75.39   TCP          66 51111 → 44
      2 0.051246  0.051246 172.67.75.39    192.168.0.46   TCP          66 443 → 5111
      3 0.051374  0.000128 192.168.0.46    172.67.75.39   TCP          54 51111 → 44
      4 0.051658  0.000284 192.168.0.46    172.67.75.39   TLSv1.3     571 Client Hel
      5 0.129374  0.077716 172.67.75.39    192.168.0.46   TCP          60 443 → 5111
      6 0.141320  0.011946 172.67.75.39    192.168.0.46   TLSv1.3    1514 Server Hel
      7 0.141320  0.000000 172.67.75.39    192.168.0.46   TLSv1.3     402 Applicatic
      8 0.141414  0.000094 192.168.0.46    172.67.75.39   TCP          54 51111 → 44
      9 1.922015  1.780601 192.168.0.46    172.67.75.39   TLSv1.3     118 Change Cip
     10 1.922333  0.000318 192.168.0.46    172.67.75.39   TLSv1.3     146 Applicatic
     11 1.922724                           172.67.75.39   TLSv1.3     720 Applicatic
     12 1.947282                           192.168.0.46   TCP          60 443 → 5111
     13 1.947282                           192.168.0.46   TLSv1.3     582 Applicatic
     14 1.947572                           172.67.75.39   TLSv1.3      85 Applicatic
     15 1.952943                           192.168.0.46   TCP          60 443 → 5111
     16 1.952943                           192.168.0.46   TCP          60 443 → 5111
```

```
  [Next Sequence Number:
  Acknowledgment Number:
  Acknowledgment number (
  1000 .... = Header Leng
⌄ Flags: 0x002 (SYN)
    000. .... .... = Rese
    ...0 .... .... = Accu
    .... 0... .... = Cong
    .... .0.. .... = ECN-
    .... ..0. .... = Urge
    .... ...0 .... = Ackn
    .... .... 0... = Push
    .... .... .0.. = Rese
  › .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
```

```
58 19 f8 d1 2e ae 34
00 34 6e a3 40 00 80
4b 27 c7 a7 01 bb 0e
fa f0 5a 07 00 00 02
04 02
```



Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Sun 3 Mar 10:30 PM

Wireshark_Masterclass_Lesson1_Setup.pcapng

tcp.flags.syn == True

Label: Enter a description for the filter button

Filter: tcp.flags.syn == True

Comment: Enter a comment for the filter button

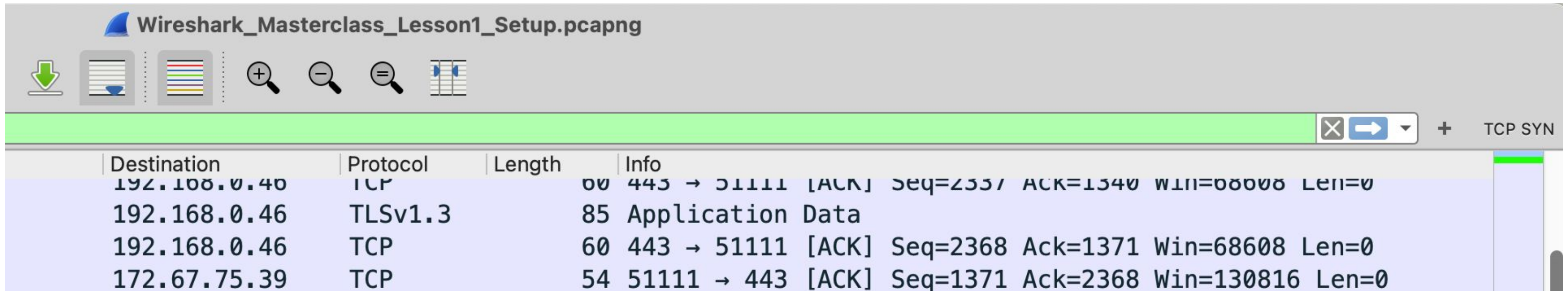
```
No.     Time      delta     Source          Destination    Protocol  Length Info
      1 0.000000  0.000000 192.168.0.46    172.67.75.39   TCP          66 51111 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SAC
      2 0.051246  0.051246 172.67.75.39    192.168.0.46   TCP          66 443 → 51111 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1400
      3 0.051374  0.000128 192.168.0.46    172.67.75.39   TCP          54 51111 → 443 [ACK] Seq=1 Ack=1 Win=131584 Len=0
      4 0.051658  0.000284 192.168.0.46    172.67.75.39   TLSv1.3     571 Client Hello (SNI=www.wireshark.org)
      5 0.129374  0.077716 172.67.75.39    192.168.0.46   TCP          60 443 → 51111 [ACK] Seq=1 Ack=518 Win=67584 Len=0
      6 0.141320  0.011946 172.67.75.39    192.168.0.46   TLSv1.3    1514 Server Hello, Change Cipher Spec
      7 0.141320  0.000000 172.67.75.39    192.168.0.46   TLSv1.3     402 Application Data
      8 0.141414  0.000094 192.168.0.46    172.67.75.39   TCP          54 51111 → 443 [ACK] Seq=518 Ack=1809 Win=131584 Len=0
      9 1.922015  1.780601 192.168.0.46    172.67.75.39   TLSv1.3     118 Change Cipher Spec, Application Data
     10 1.922333  0.000318 192.168.0.46    172.67.75.39   TLSv1.3     146 Application Data
     11 1.922724  0.000391 192.168.0.46    172.67.75.39   TLSv1.3     720 Application Data
     12 1.947282  0.024558 172.67.75.39    192.168.0.46   TCP          60 443 → 51111 [ACK] Seq=1809 Ack=582 Win=67584 Len=0
     13 1.947282  0.000000 172.67.75.39    192.168.0.46   TLSv1.3     582 Application Data, Application Data
     14 1.947572  0.000290 192.168.0.46    172.67.75.39   TLSv1.3      85 Application Data
     15 1.952943  0.005371 172.67.75.39    192.168.0.46   TCP          60 443 → 51111 [ACK] Seq=2337 Ack=674 Win=67584 Len=0
```

```
  Acknowledgment number (raw): 0
  1000 .... = Header Length: 32 bytes (8)
⌄ Flags: 0x002 (SYN)
    000. .... .... = Reserved: Not set
    ...0 .... .... = Accurate ECN: Not set
    .... 0... .... = Congestion Window Reduced: Not set
    .... .0.. .... = ECN-Echo: Not set
    .... ..0. .... = Urgent: Not set
    .... ...0 .... = Acknowledgment: Not set
    .... .... 0... = Push: Not set
    .... .... .0.. = Reset: Not set
  › .... .... ..1. = Syn: Set
    .... .... ...0 = Fin: Not set
    [TCP Flags: ··········S·]
  Window: 64240
  [Calculated window size: 64240]
```

```
0000  58 19 f8 d1 2e ae 34 f6  4b a3 29 0b 08 00 45 00   X····.4·K·)···E·
0010  00 34 6e a3 40 00 80 06  d3 df c0 a8 00 2e ac 43   ·4n·@··· ·····.·C
0020  4b 27 c7 a7 01 bb 0e 47  8a 2d 00 00 00 00 80 02   K'·····G ·-······
0030  fa f0 5a 07 00 00 02 04  05 b4 01 03 03 08 01 01   ··Z····· ········
0040  04 02                                              ··
```

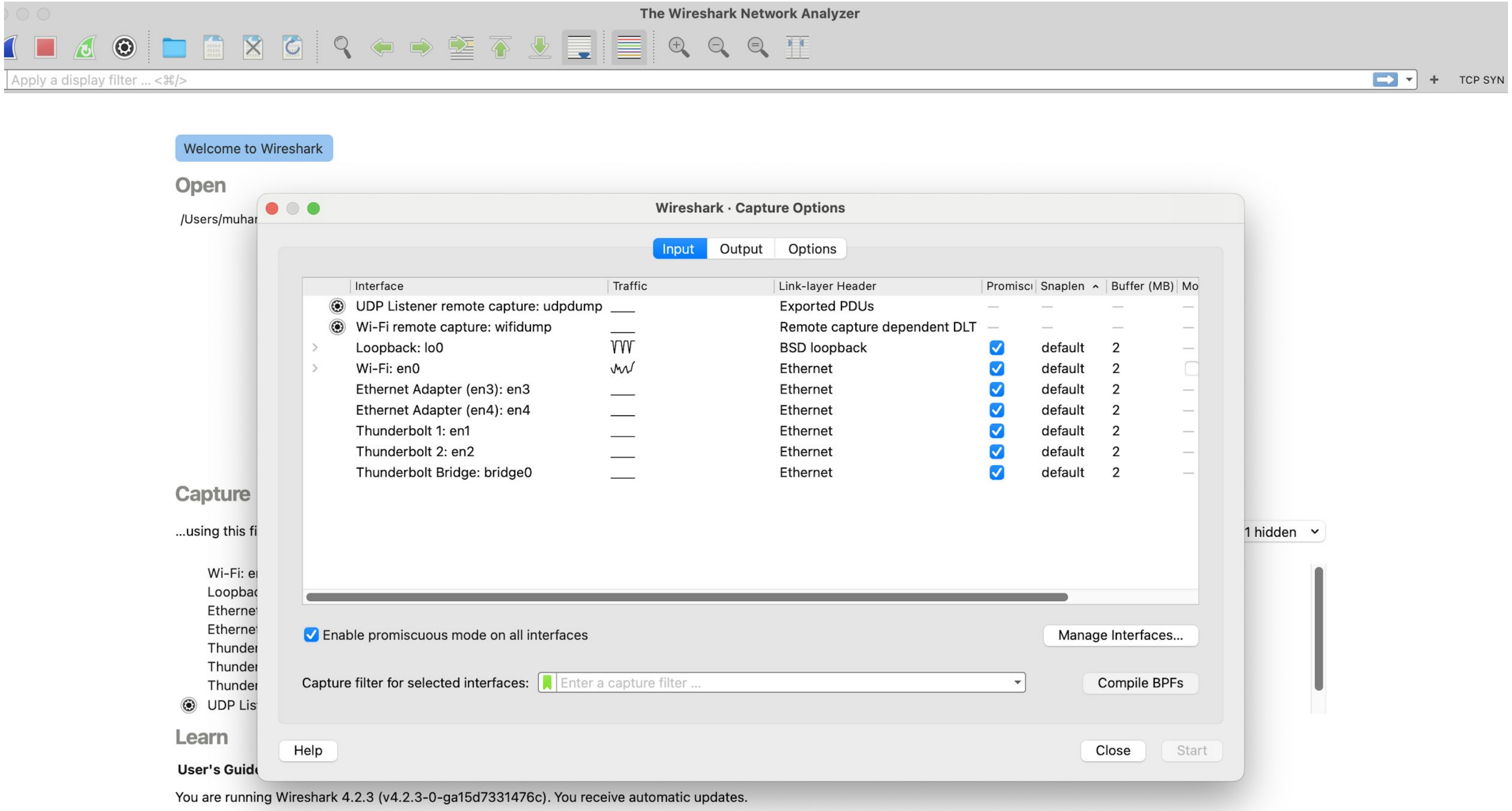
Syn (tcp.flags.syn), 1 byte   Packets: 89 · Displayed: 89 (100.0%)   Profile: Wireshark Masterclass

Configuring Wireshark – buttons



```
Destination     Protocol    Length   Info
192.168.0.46    TCP             60   443 → 51111 [ACK] Seq=2337 Ack=1340 Win=68608 Len=0
192.168.0.46    TLSv1.3         85   Application Data
192.168.0.46    TCP             60   443 → 51111 [ACK] Seq=2368 Ack=1371 Win=68608 Len=0
172.67.75.39    TCP             54   51111 → 443 [ACK] Seq=1371 Ack=2368 Win=130816 Len=0
```

Configuring Wireshark – capture options



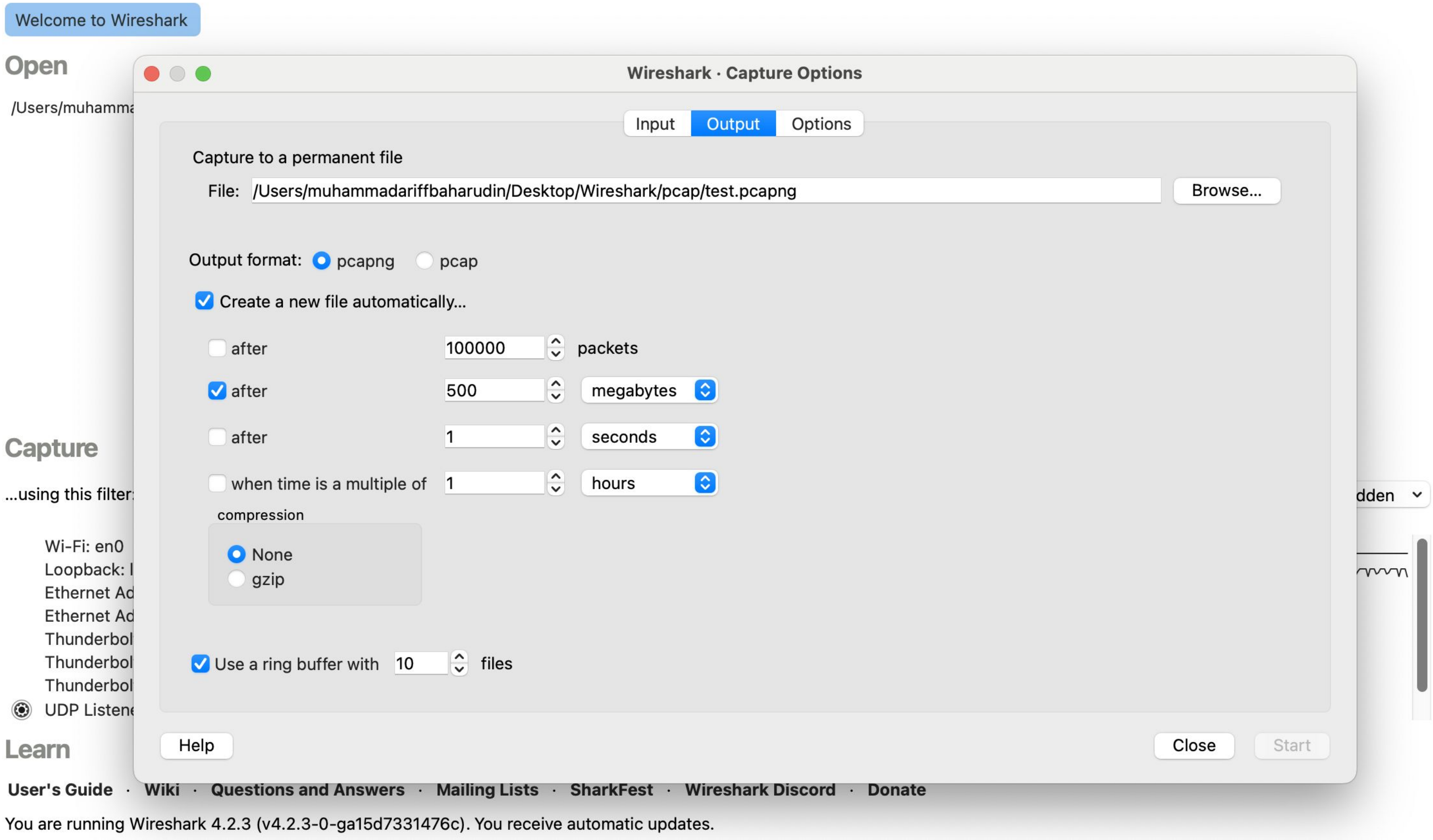
Interface	Traffic	Link-layer Header	Promiscı	Snaplen	Buffer (MB)	Mo
UDP Listener remote capture: udpdump		Exported PDUs	—	—	—	—
Wi-Fi remote capture: wifidump		Remote capture dependent DLT	—	—	—	—
Loopback: lo0		BSD loopback	☑	default	2	—
Wi-Fi: en0		Ethernet	☑	default	2	□
Ethernet Adapter (en3): en3		Ethernet	☑	default	2	—
Ethernet Adapter (en4): en4		Ethernet	☑	default	2	—
Thunderbolt 1: en1		Ethernet	☑	default	2	—
Thunderbolt 2: en2		Ethernet	☑	default	2	—
Thunderbolt Bridge: bridge0		Ethernet	☑	default	2	—

☑ Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter ...

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.

Configuring Wireshark – capture options



Capture to a permanent file

File: /Users/muhammadariffbaharudin/Desktop/Wireshark/pcap/test.pcapng

Output format: ● pcapng ○ pcap

☑ Create a new file automatically...

□ after	100000	packets
☑ after	500	megabytes
□ after	1	seconds
□ when time is a multiple of	1	hours

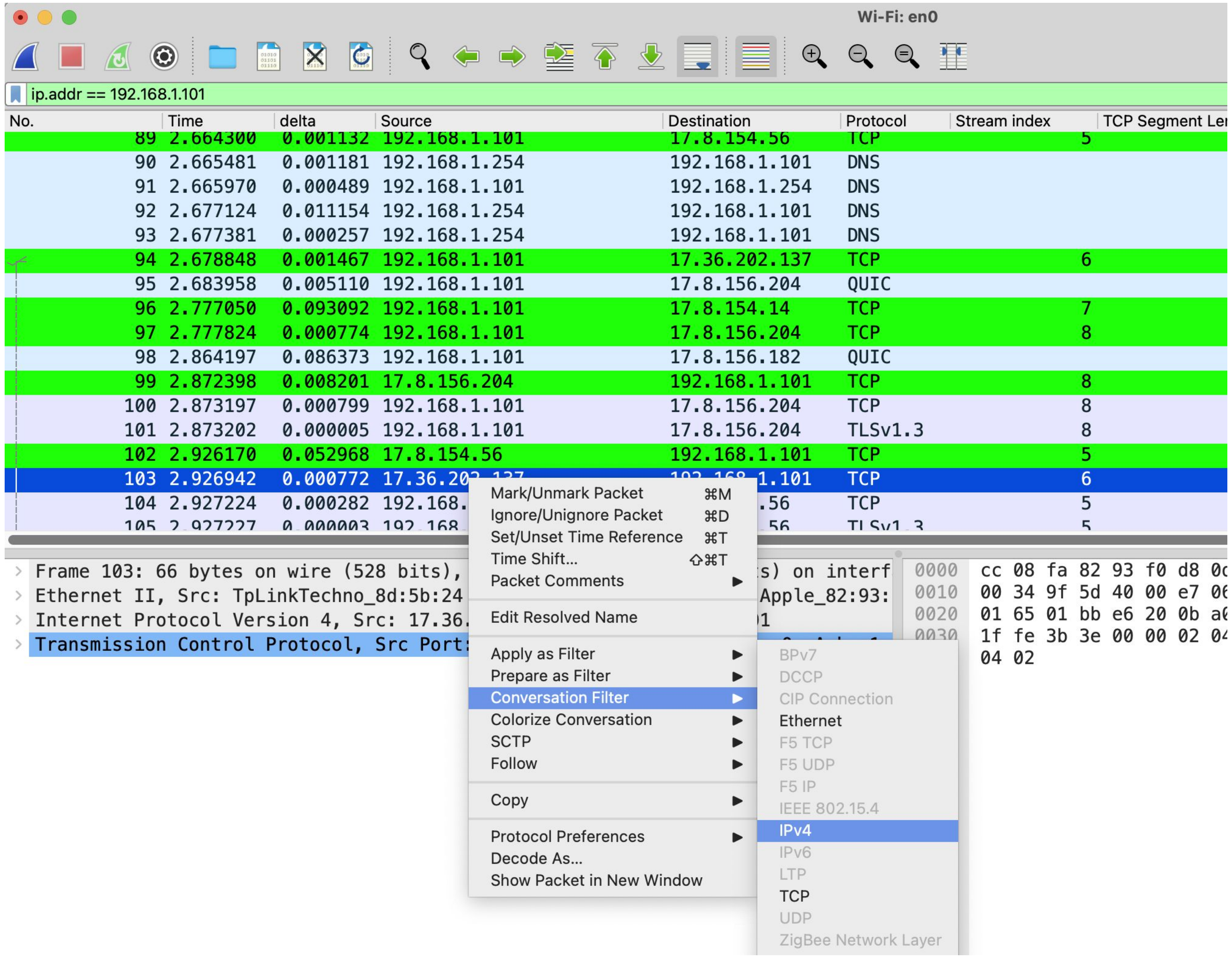
compression

● None
○ gzip

☑ Use a ring buffer with 10 files

You are running Wireshark 4.2.3 (v4.2.3-0-ga15d7331476c). You receive automatic updates.

Filtering – conversation filter



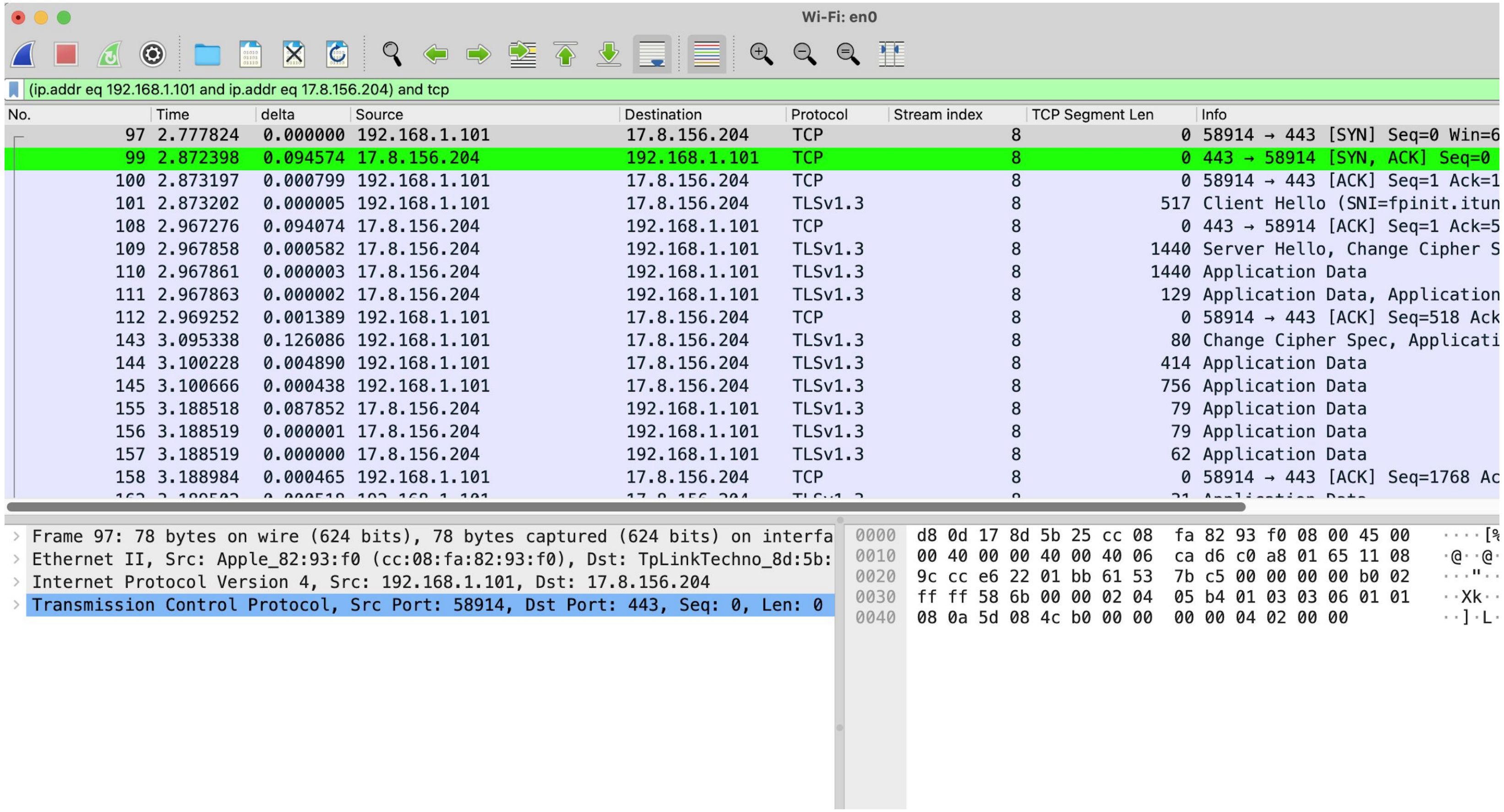
ip.addr == 192.168.1.101

```
No.     Time      delta     Source          Destination     Protocol  Stream index  TCP Segment Le
 89  2.664300  0.001132  192.168.1.101   17.8.154.56     TCP          5
 90  2.665481  0.001181  192.168.1.254   192.168.1.101   DNS
 91  2.665970  0.000489  192.168.1.101   192.168.1.254   DNS
 92  2.677124  0.011154  192.168.1.254   192.168.1.101   DNS
 93  2.677381  0.000257  192.168.1.254   192.168.1.101   DNS
 94  2.678848  0.001467  192.168.1.101   17.36.202.137   TCP          6
 95  2.683958  0.005110  192.168.1.101   17.8.156.204    QUIC
 96  2.777050  0.093092  192.168.1.101   17.8.154.14     TCP          7
 97  2.777824  0.000774  192.168.1.101   17.8.156.204    TCP          8
 98  2.864197  0.086373  192.168.1.101   17.8.156.182    QUIC
 99  2.872398  0.008201  17.8.156.204    192.168.1.101   TCP          8
100  2.873197  0.000799  192.168.1.101   17.8.156.204    TCP          8
101  2.873202  0.000005  192.168.1.101   17.8.156.204    TLSv1.3      8
102  2.926170  0.052968  17.8.154.56     192.168.1.101   TCP          5
103  2.926942  0.000772  17.36.202.137   192.168.1.101   TCP          6
104  2.927224  0.000282  192.168.        .56             TCP          5
105  2.927227  0.000003  192.168.        .56             TLSv1.3      5
```

```
> Frame 103: 66 bytes on wire (528 bits),                  s) on interf
> Ethernet II, Src: TpLinkTechno_8d:5b:24                   Apple_82:93:
> Internet Protocol Version 4, Src: 17.36.                  1
> Transmission Control Protocol, Src Port:
```

```
0000  cc 08 fa 82 93 f0 d8 0c
0010  00 34 9f 5d 40 00 e7 06
0020  01 65 01 bb e6 20 0b a6
0030  1f fe 3b 3e 00 00 02 04
      04 02
```

Filtering – adding option manually



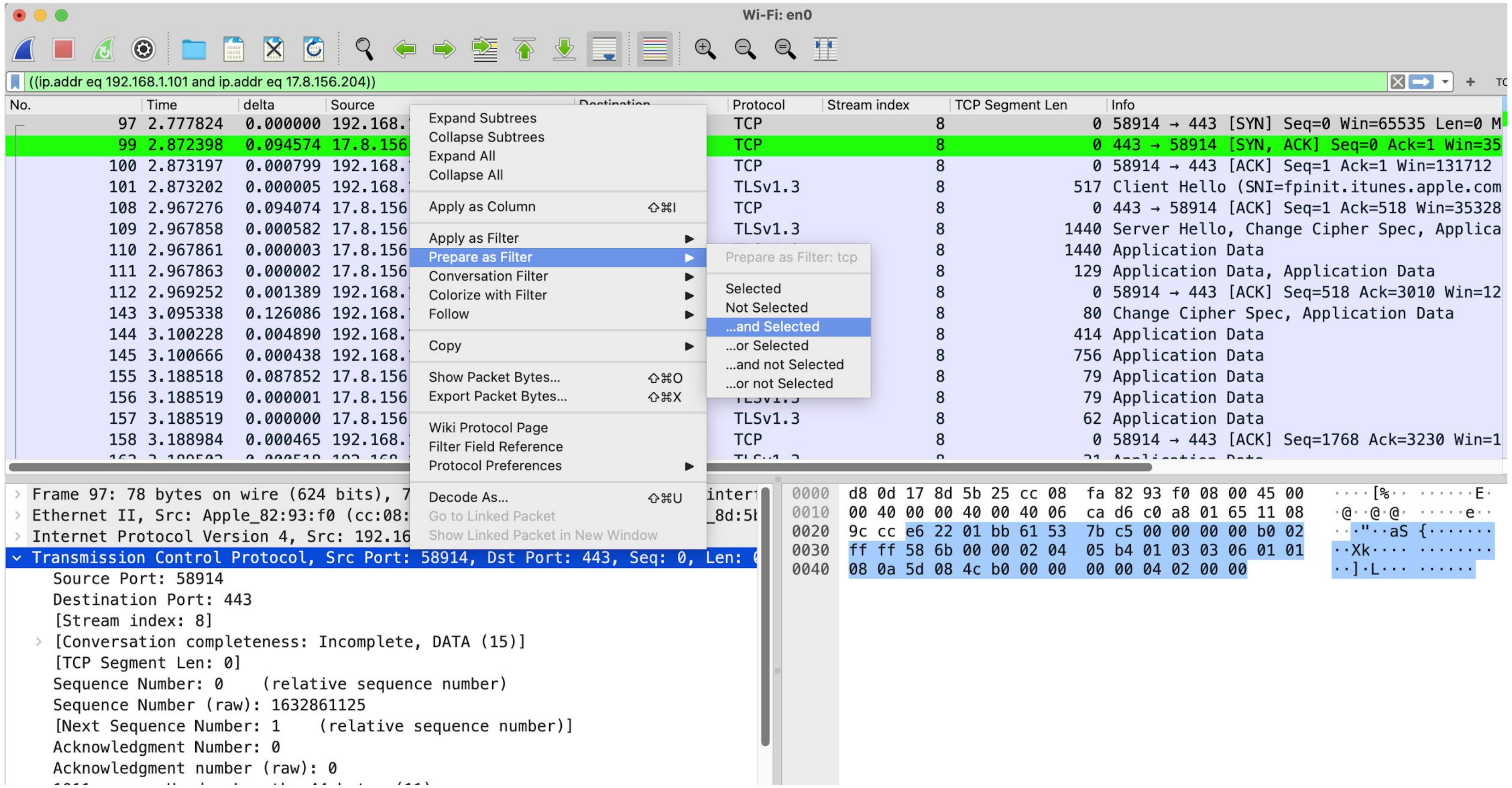
(ip.addr eq 192.168.1.101 and ip.addr eq 17.8.156.204) and tcp

No.	Time	delta	Source	Destination	Protocol	Stream index	TCP Segment Len	Info
97	2.777824	0.000000	192.168.1.101	17.8.156.204	TCP	8	0	58914 → 443 [SYN] Seq=0 Win=6
99	2.872398	0.094574	17.8.156.204	192.168.1.101	TCP	8	0	443 → 58914 [SYN, ACK] Seq=0
100	2.873197	0.000799	192.168.1.101	17.8.156.204	TCP	8	0	58914 → 443 [ACK] Seq=1 Ack=1
101	2.873202	0.000005	192.168.1.101	17.8.156.204	TLSv1.3	8	517	Client Hello (SNI=fpinit.itun
108	2.967276	0.094074	17.8.156.204	192.168.1.101	TCP	8	0	443 → 58914 [ACK] Seq=1 Ack=5
109	2.967858	0.000582	17.8.156.204	192.168.1.101	TLSv1.3	8	1440	Server Hello, Change Cipher S
110	2.967861	0.000003	17.8.156.204	192.168.1.101	TLSv1.3	8	1440	Application Data
111	2.967863	0.000002	17.8.156.204	192.168.1.101	TLSv1.3	8	129	Application Data, Application
112	2.969252	0.001389	192.168.1.101	17.8.156.204	TCP	8	0	58914 → 443 [ACK] Seq=518 Ack
143	3.095338	0.126086	192.168.1.101	17.8.156.204	TLSv1.3	8	80	Change Cipher Spec, Applicati
144	3.100228	0.004890	192.168.1.101	17.8.156.204	TLSv1.3	8	414	Application Data
145	3.100666	0.000438	192.168.1.101	17.8.156.204	TLSv1.3	8	756	Application Data
155	3.188518	0.087852	17.8.156.204	192.168.1.101	TLSv1.3	8	79	Application Data
156	3.188519	0.000001	17.8.156.204	192.168.1.101	TLSv1.3	8	79	Application Data
157	3.188519	0.000000	17.8.156.204	192.168.1.101	TLSv1.3	8	62	Application Data
158	3.188984	0.000465	192.168.1.101	17.8.156.204	TCP	8	0	58914 → 443 [ACK] Seq=1768 Ac

```
> Frame 97: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interfa
> Ethernet II, Src: Apple_82:93:f0 (cc:08:fa:82:93:f0), Dst: TpLinkTechno_8d:5b:
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 17.8.156.204
> Transmission Control Protocol, Src Port: 58914, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  d8 0d 17 8d 5b 25 cc 08  fa 82 93 f0 08 00 45 00   ····[%
0010  00 40 00 00 40 00 40 06  ca d6 c0 a8 01 65 11 08   ·@··@·
0020  9c cc e6 22 01 bb 61 53  7b c5 00 00 00 00 b0 02   ···"··
0030  ff ff 58 6b 00 00 02 04  05 b4 01 03 03 06 01 01   ··Xk··
0040  08 0a 5d 08 4c b0 00 00  00 00 04 02 00 00         ··]·L·
```

Filtering – using the filter options



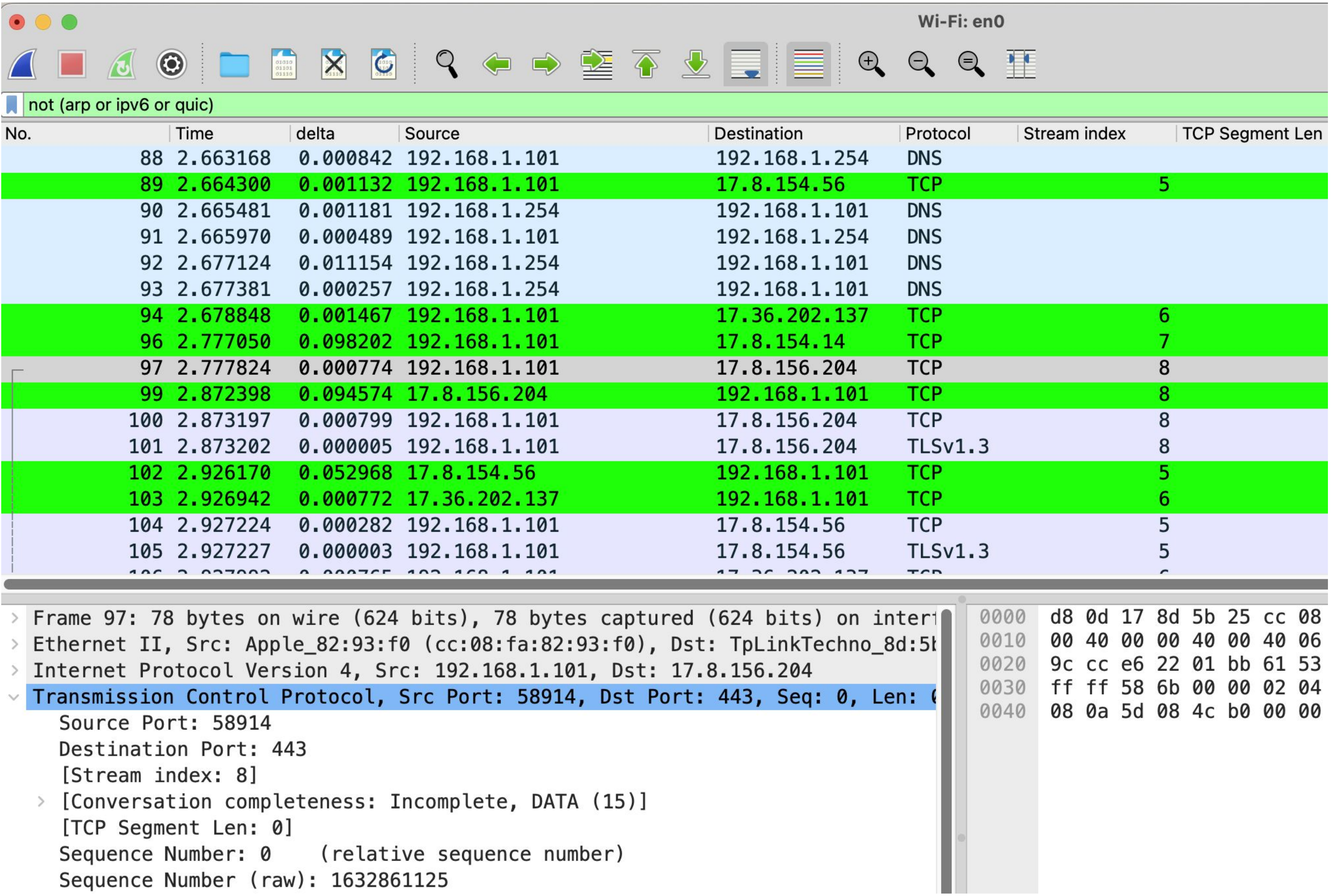
```
((ip.addr eq 192.168.1.101 and ip.addr eq 17.8.156.204))
```

```
No.    Time      delta     Source      Protocol  Stream index  TCP Segment Len  Info
 97 2.777824 0.000000 192.168.     TCP       8     0 58914 → 443 [SYN] Seq=0 Win=65535 Len=0 M
 99 2.872398 0.094574 17.8.156     TCP       8     0 443 → 58914 [SYN, ACK] Seq=0 Ack=1 Win=35
100 2.873197 0.000799 192.168.     TCP       8     0 58914 → 443 [ACK] Seq=1 Ack=1 Win=131712
101 2.873202 0.000005 192.168.     TLSv1.3   8   517 Client Hello (SNI=fpinit.itunes.apple.com
108 2.967276 0.094074 17.8.156     TCP       8     0 443 → 58914 [ACK] Seq=1 Ack=518 Win=35328
109 2.967858 0.000582 17.8.156     TLSv1.3   8  1440 Server Hello, Change Cipher Spec, Applica
110 2.967861 0.000003 17.8.156               8  1440 Application Data
111 2.967863 0.000002 17.8.156               8   129 Application Data, Application Data
112 2.969252 0.001389 192.168.               8     0 58914 → 443 [ACK] Seq=518 Ack=3010 Win=12
143 3.095338 0.126086 192.168.               8    80 Change Cipher Spec, Application Data
144 3.100228 0.004890 192.168.               8   414 Application Data
145 3.100666 0.000438 192.168.               8   756 Application Data
155 3.188518 0.087852 17.8.156               8    79 Application Data
156 3.188519 0.000001 17.8.156               8    79 Application Data
157 3.188519 0.000000 17.8.156     TLSv1.3   8    62 Application Data
158 3.188984 0.000465 192.168.     TCP       8     0 58914 → 443 [ACK] Seq=1768 Ack=3230 Win=1
```

```
> Frame 97: 78 bytes on wire (624 bits), 7                                  interf
> Ethernet II, Src: Apple_82:93:f0 (cc:08:                                  _8d:5b
> Internet Protocol Version 4, Src: 192.16
v Transmission Control Protocol, Src Port: 58914, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 58914
    Destination Port: 443
    [Stream index: 8]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1632861125
    [Next Sequence Number: 1    (relative sequence number)]
    Acknowledgment Number: 0
    Acknowledgment number (raw): 0
```

```
0000  d8 0d 17 8d 5b 25 cc 08  fa 82 93 f0 08 00 45 00   ····[%·· ······E·
0010  00 40 00 00 40 00 40 06  ca d6 c0 a8 01 65 11 08   ·@··@·@· ·····e··
0020  9c cc e6 22 01 bb 61 53  7b c5 00 00 00 00 b0 02   ···"··aS {·······
0030  ff ff 58 6b 00 00 02 04  05 b4 01 03 03 06 01 01   ··Xk···· ········
0040  08 0a 5d 08 4c b0 00 00  00 00 04 02 00 00         ··]·L··· ······
```

Filtering – getting rid of what you don’t want



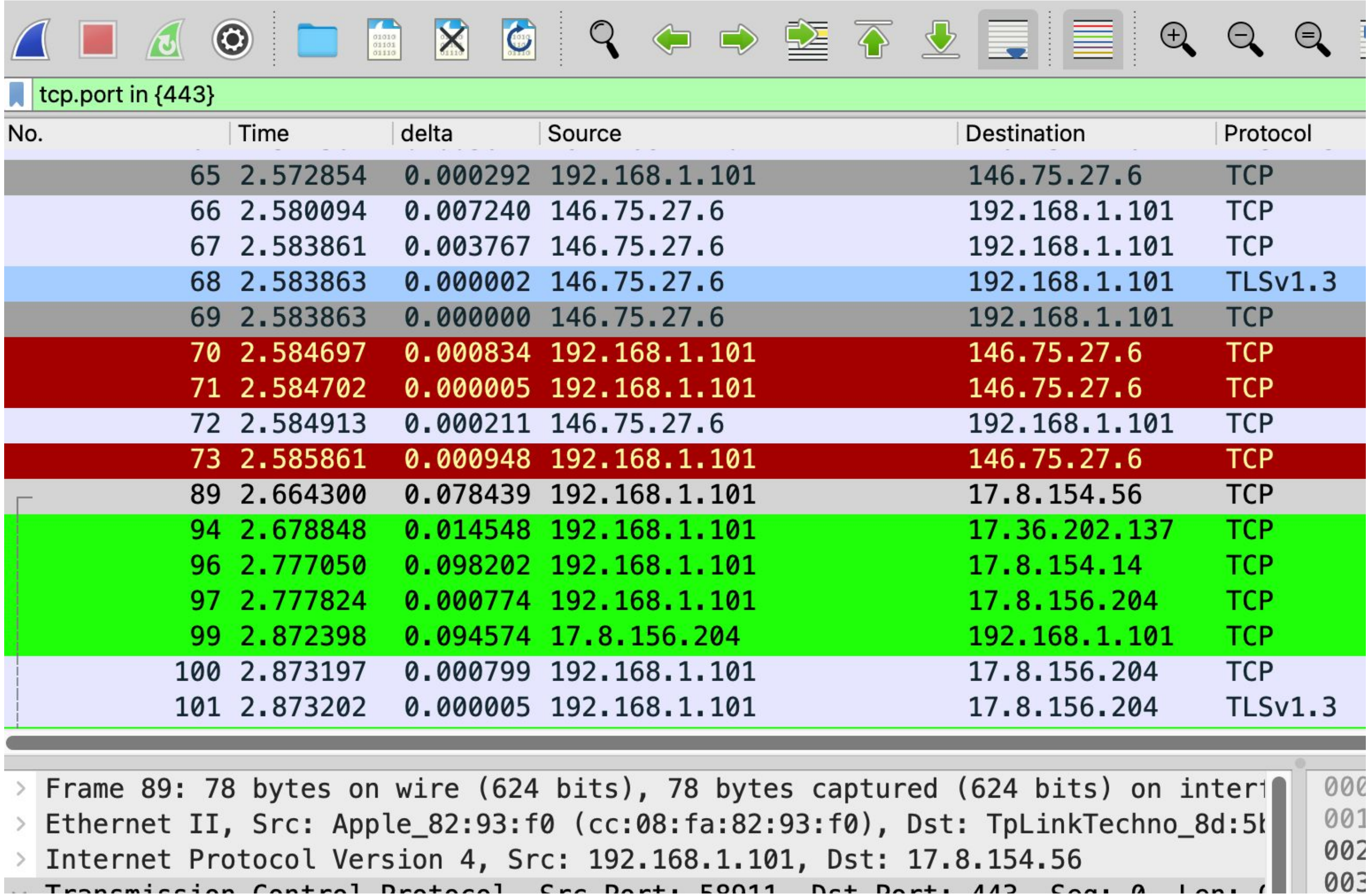
not (arp or ipv6 or quic)

No.	Time	delta	Source	Destination	Protocol	Stream index	TCP Segment Len
88	2.663168	0.000842	192.168.1.101	192.168.1.254	DNS		
89	2.664300	0.001132	192.168.1.101	17.8.154.56	TCP	5	
90	2.665481	0.001181	192.168.1.254	192.168.1.101	DNS		
91	2.665970	0.000489	192.168.1.101	192.168.1.254	DNS		
92	2.677124	0.011154	192.168.1.254	192.168.1.101	DNS		
93	2.677381	0.000257	192.168.1.254	192.168.1.101	DNS		
94	2.678848	0.001467	192.168.1.101	17.36.202.137	TCP	6	
96	2.777050	0.098202	192.168.1.101	17.8.154.14	TCP	7	
97	2.777824	0.000774	192.168.1.101	17.8.156.204	TCP	8	
99	2.872398	0.094574	17.8.156.204	192.168.1.101	TCP	8	
100	2.873197	0.000799	192.168.1.101	17.8.156.204	TCP	8	
101	2.873202	0.000005	192.168.1.101	17.8.156.204	TLSv1.3	8	
102	2.926170	0.052968	17.8.154.56	192.168.1.101	TCP	5	
103	2.926942	0.000772	17.36.202.137	192.168.1.101	TCP	6	
104	2.927224	0.000282	192.168.1.101	17.8.154.56	TCP	5	
105	2.927227	0.000003	192.168.1.101	17.8.154.56	TLSv1.3	5	

```
> Frame 97: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interf
> Ethernet II, Src: Apple_82:93:f0 (cc:08:fa:82:93:f0), Dst: TpLinkTechno_8d:5b
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 17.8.156.204
v Transmission Control Protocol, Src Port: 58914, Dst Port: 443, Seq: 0, Len: 0
    Source Port: 58914
    Destination Port: 443
    [Stream index: 8]
  > [Conversation completeness: Incomplete, DATA (15)]
    [TCP Segment Len: 0]
    Sequence Number: 0    (relative sequence number)
    Sequence Number (raw): 1632861125
```

```
0000  d8 0d 17 8d 5b 25 cc 08
0010  00 40 00 00 40 00 40 06
0020  9c cc e6 22 01 bb 61 53
0030  ff ff 58 6b 00 00 02 04
0040  08 0a 5d 08 4c b0 00 00
```

Filtering – list



tcp.port in {443}

No.	Time	delta	Source	Destination	Protocol
65	2.572854	0.000292	192.168.1.101	146.75.27.6	TCP
66	2.580094	0.007240	146.75.27.6	192.168.1.101	TCP
67	2.583861	0.003767	146.75.27.6	192.168.1.101	TCP
68	2.583863	0.000002	146.75.27.6	192.168.1.101	TLSv1.3
69	2.583863	0.000000	146.75.27.6	192.168.1.101	TCP
70	2.584697	0.000834	192.168.1.101	146.75.27.6	TCP
71	2.584702	0.000005	192.168.1.101	146.75.27.6	TCP
72	2.584913	0.000211	146.75.27.6	192.168.1.101	TCP
73	2.585861	0.000948	192.168.1.101	146.75.27.6	TCP
89	2.664300	0.078439	192.168.1.101	17.8.154.56	TCP
94	2.678848	0.014548	192.168.1.101	17.36.202.137	TCP
96	2.777050	0.098202	192.168.1.101	17.8.154.14	TCP
97	2.777824	0.000774	192.168.1.101	17.8.156.204	TCP
99	2.872398	0.094574	17.8.156.204	192.168.1.101	TCP
100	2.873197	0.000799	192.168.1.101	17.8.156.204	TCP
101	2.873202	0.000005	192.168.1.101	17.8.156.204	TLSv1.3

```
> Frame 89: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interf
> Ethernet II, Src: Apple_82:93:f0 (cc:08:fa:82:93:f0), Dst: TpLinkTechno_8d:5b
> Internet Protocol Version 4, Src: 192.168.1.101, Dst: 17.8.154.56
v Transmission Control Protocol, Src Port: 58911, Dst Port: 443, Seq: 0, Len: (
```