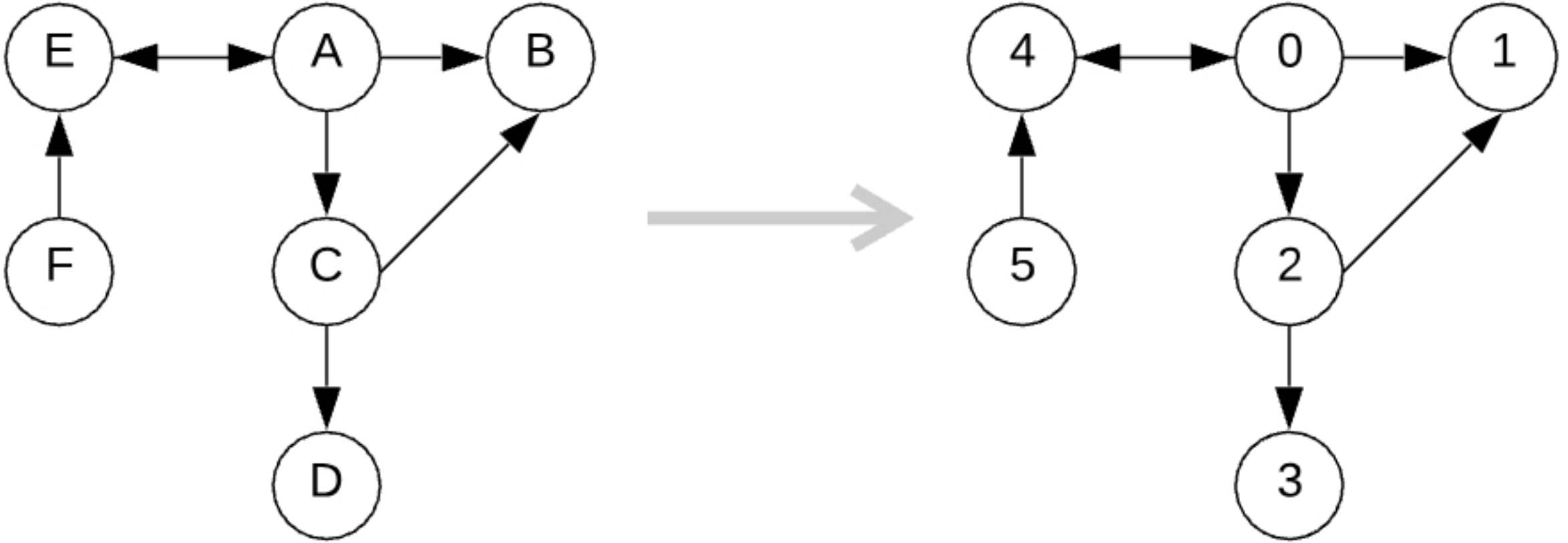
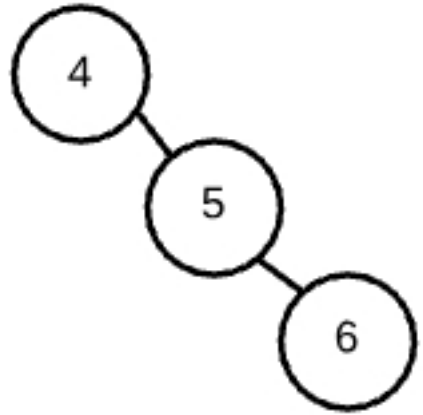
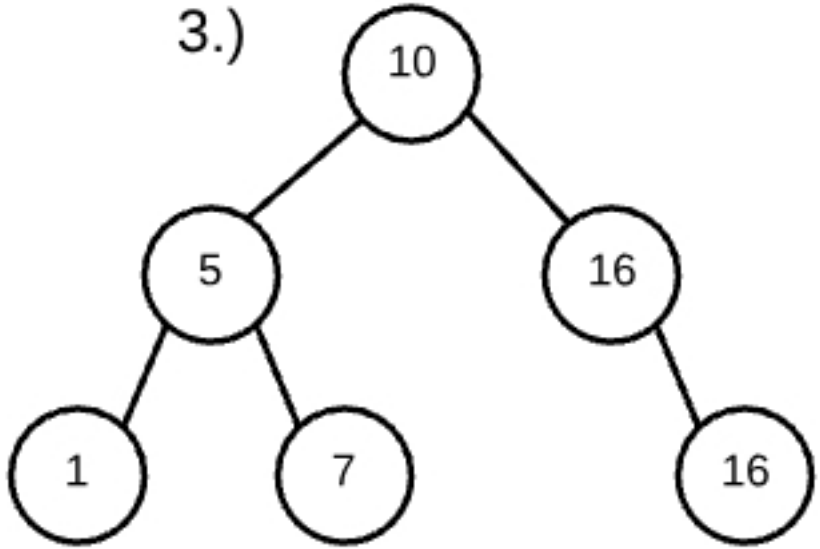

E
A
B
F
C
D
4
0
1
5
2
3

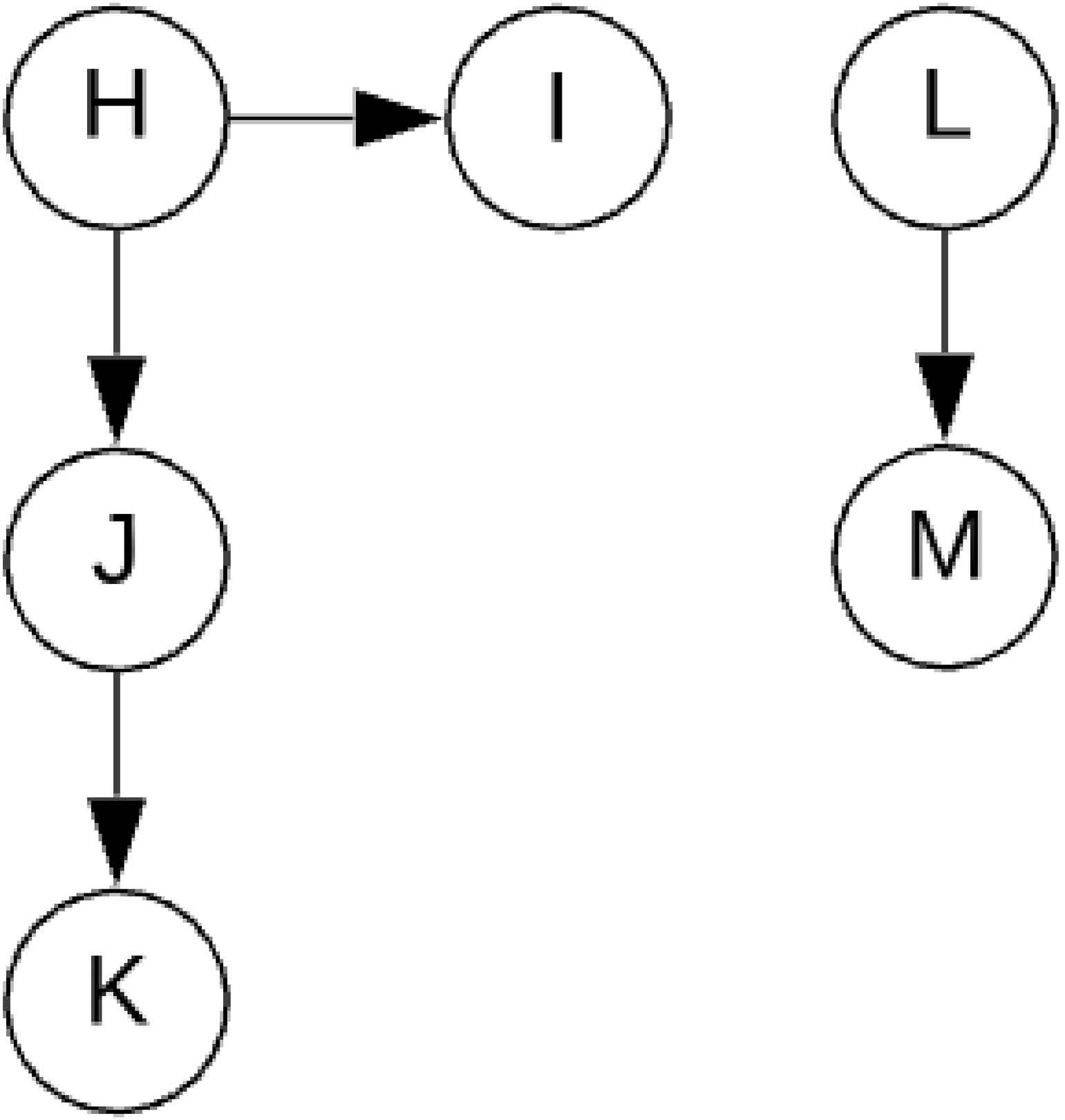
1.)

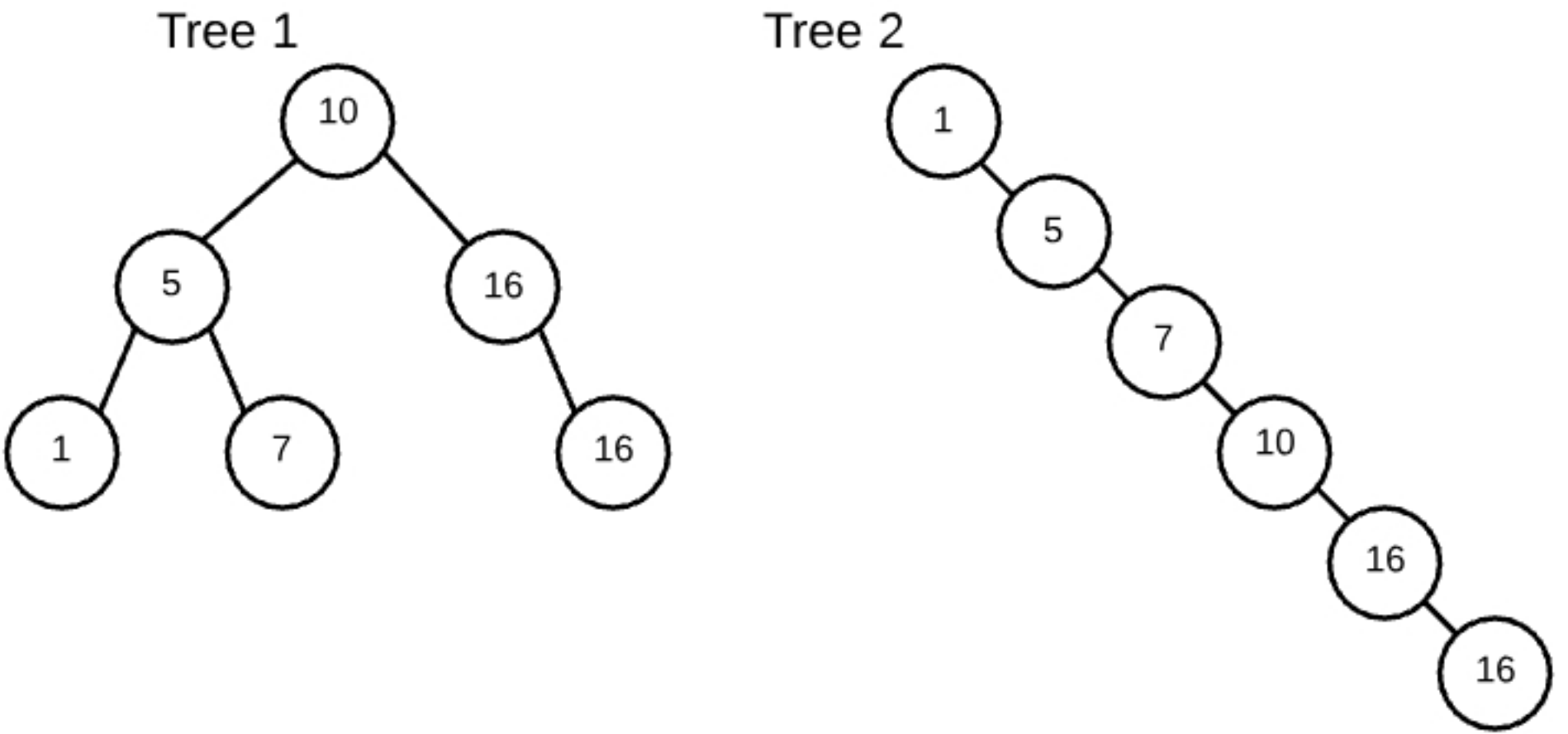
2.)

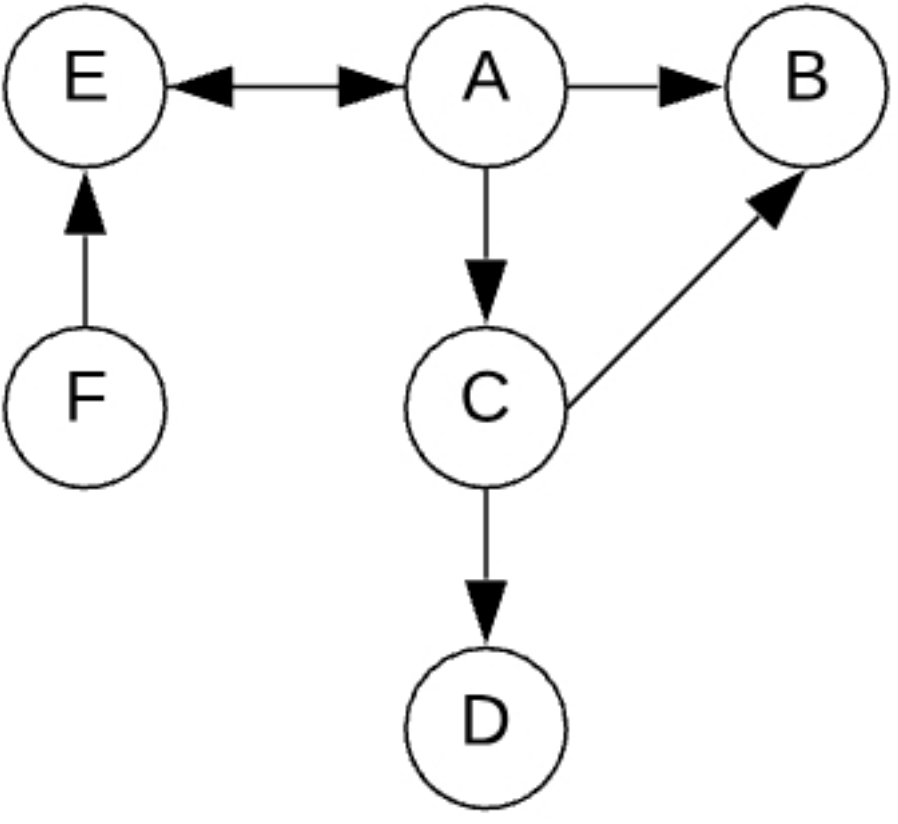


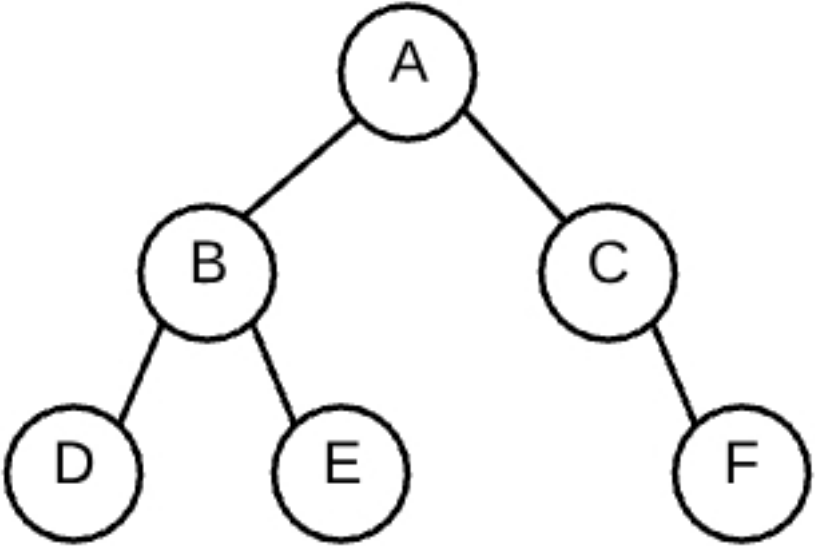
3.)



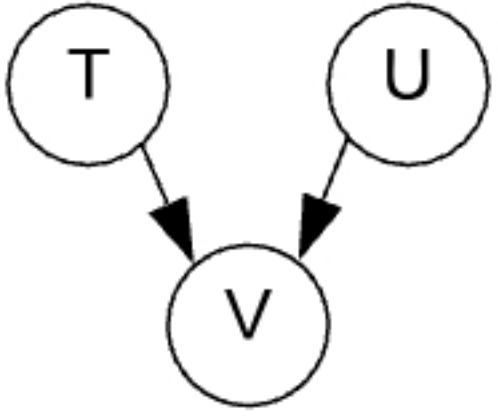

H
I
L
J
M
K


Tree 1
10
5
16
1
7
16
Tree 2
1
5
7
10
16
16

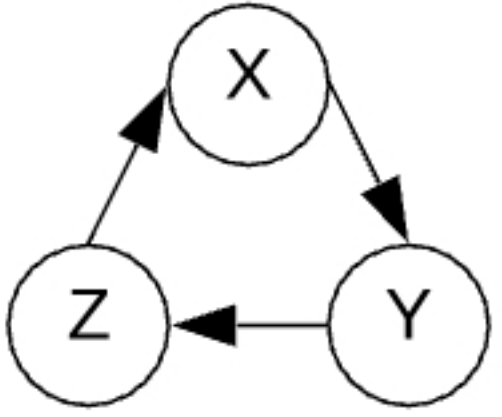

E
A
B
F
C
D


A
B
C
D
E
F

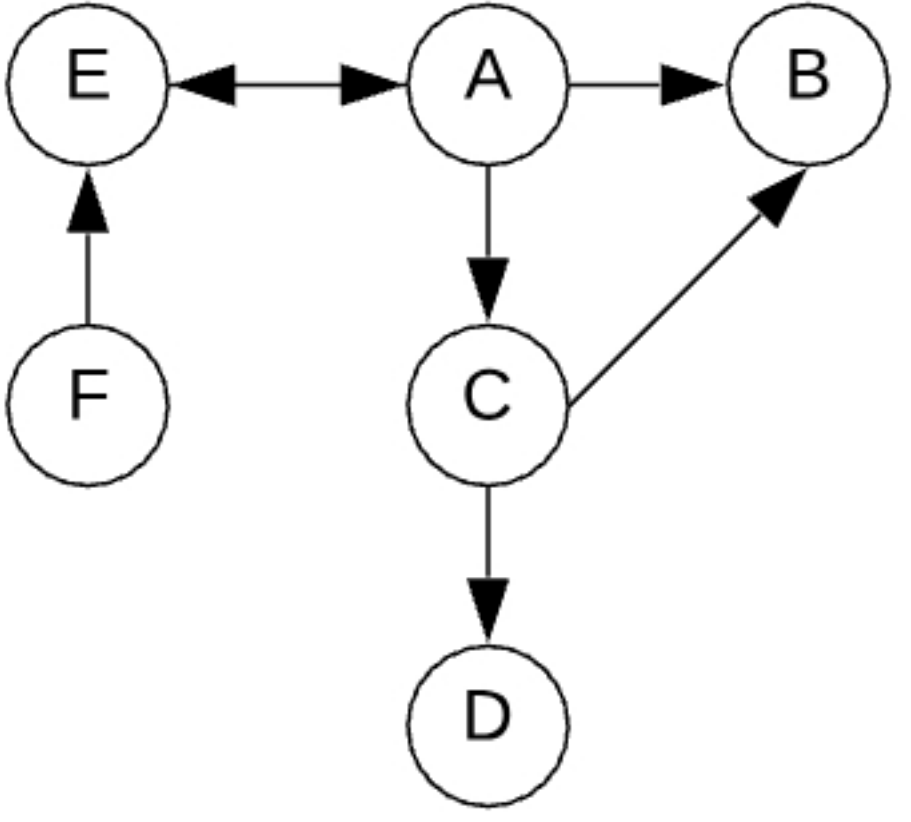
Graph 1



Graph 2



Graph 3



https://students.appacademy.com/my-homework?username="CoolStudent"
protocol
subdomain
second-level domain
TLD
application route
query parameters

https://students.appacademy.com/my-homework?username="CoolStudent"
protocol
subdomain
second-level domain
TLD
application route
query parameters

Client
I need to to get to students.appacademy.io...

DNS Root Name Server
I don't know that particular location, but @io might!

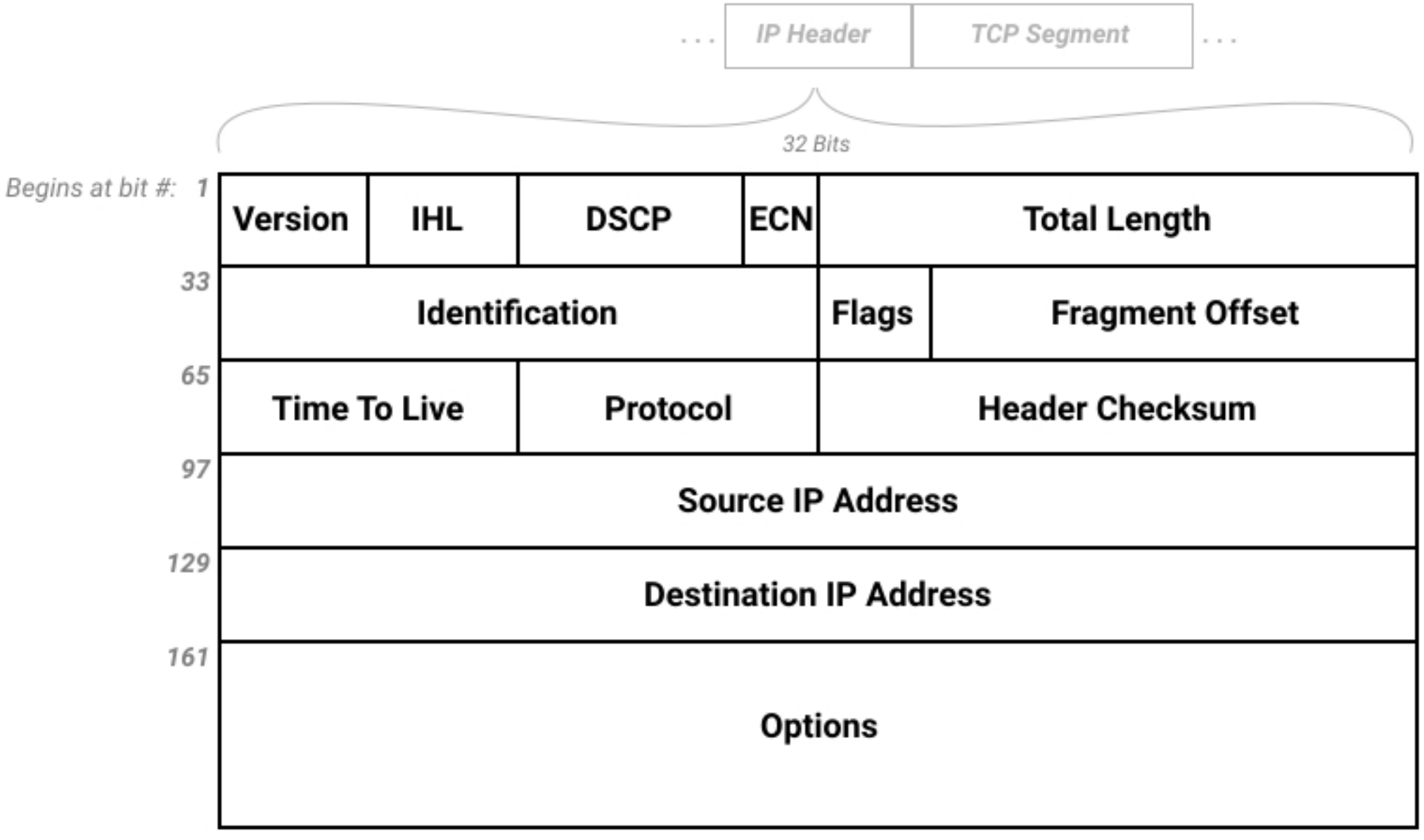
Client
Okay. @io can you help me find this location?

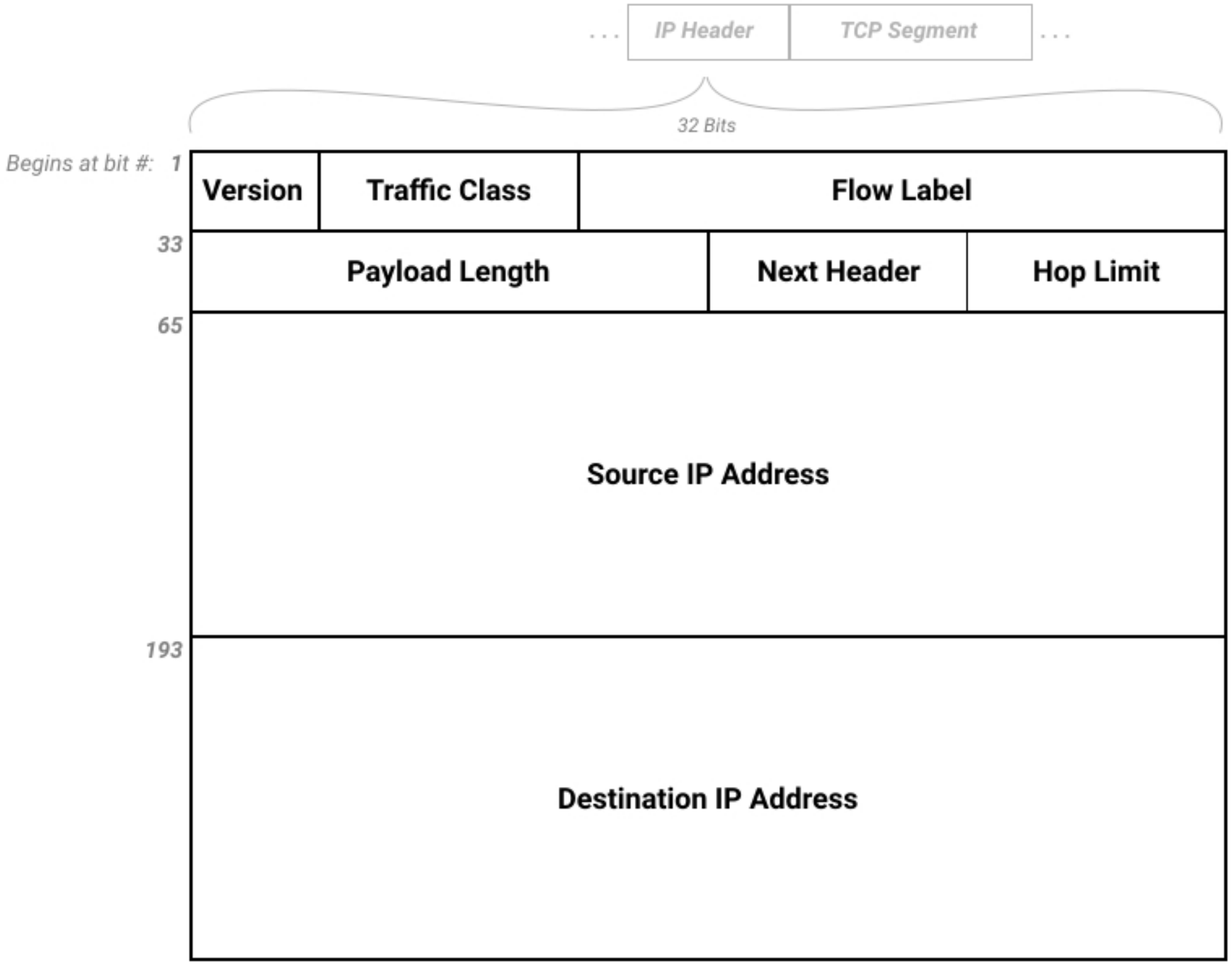
.Io Name Server
I don't know exactly either. Try @appacademy.

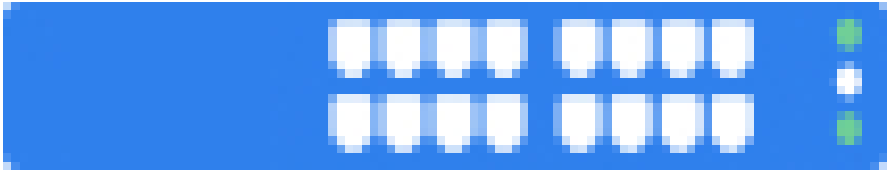
Client
@appacademy any ideas?

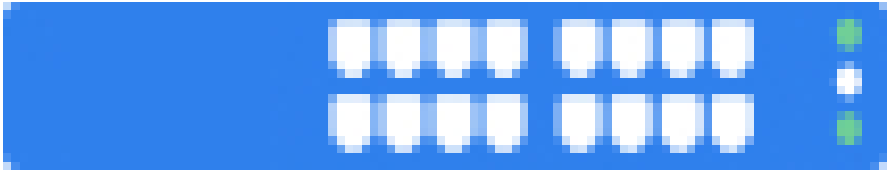
.AppAcademy Name Server
Oh yeah, the `students` subdomain? It's at `10.1.0.101`.

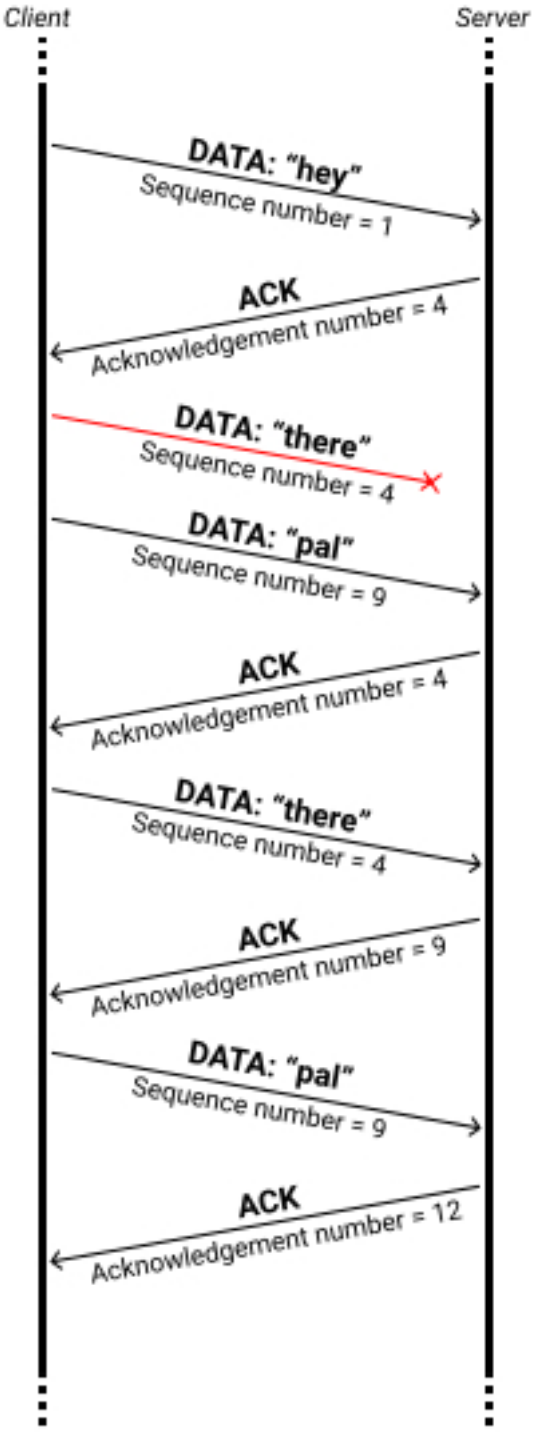
Client
Perfect, I'll go there - thank you!

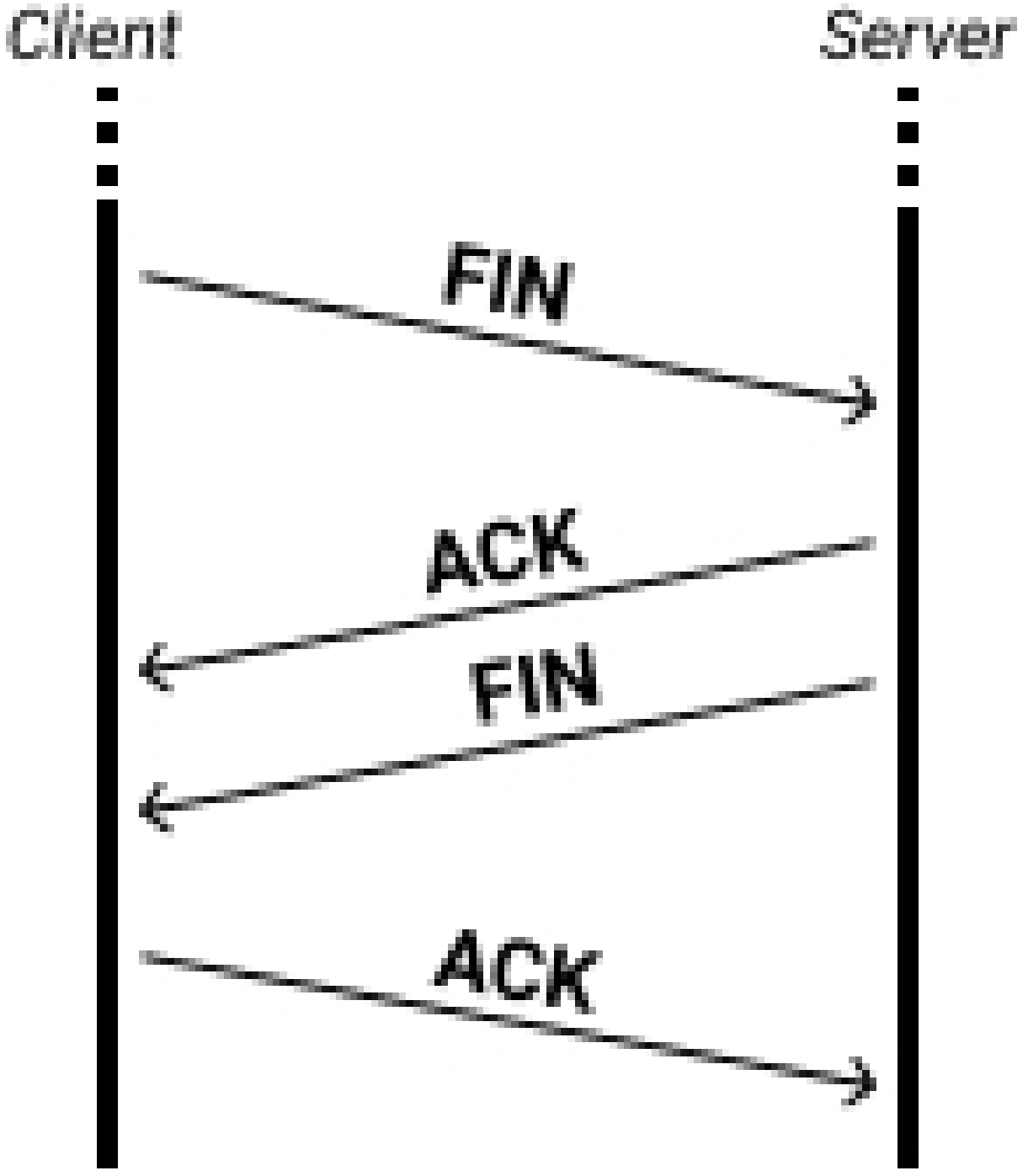

. . .
IP Header
TCP Segment
. . .
32 Bits
Begins at bit #:
1
33
65
97
129
161
Version
IHL
DSCP
ECN
Total Length
Identification
Flags
Fragment Offset
Time To Live
Protocol
Header Checksum
Source IP Address
Destination IP Address
Options

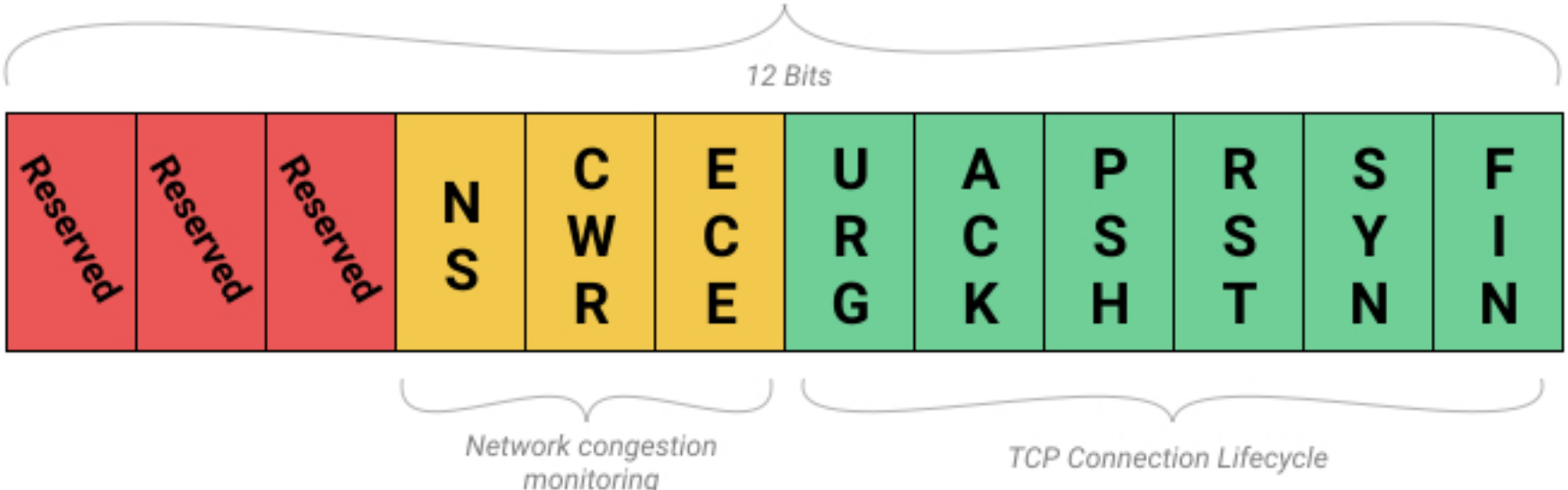

. . .
IP Header
TCP Segment
. . .
32 Bits
Begins at bit #:
1
33
65
193
Version
Traffic Class
Flow Label
Payload Length
Next Header
Hop Limit
Source IP Address
Destination IP Address

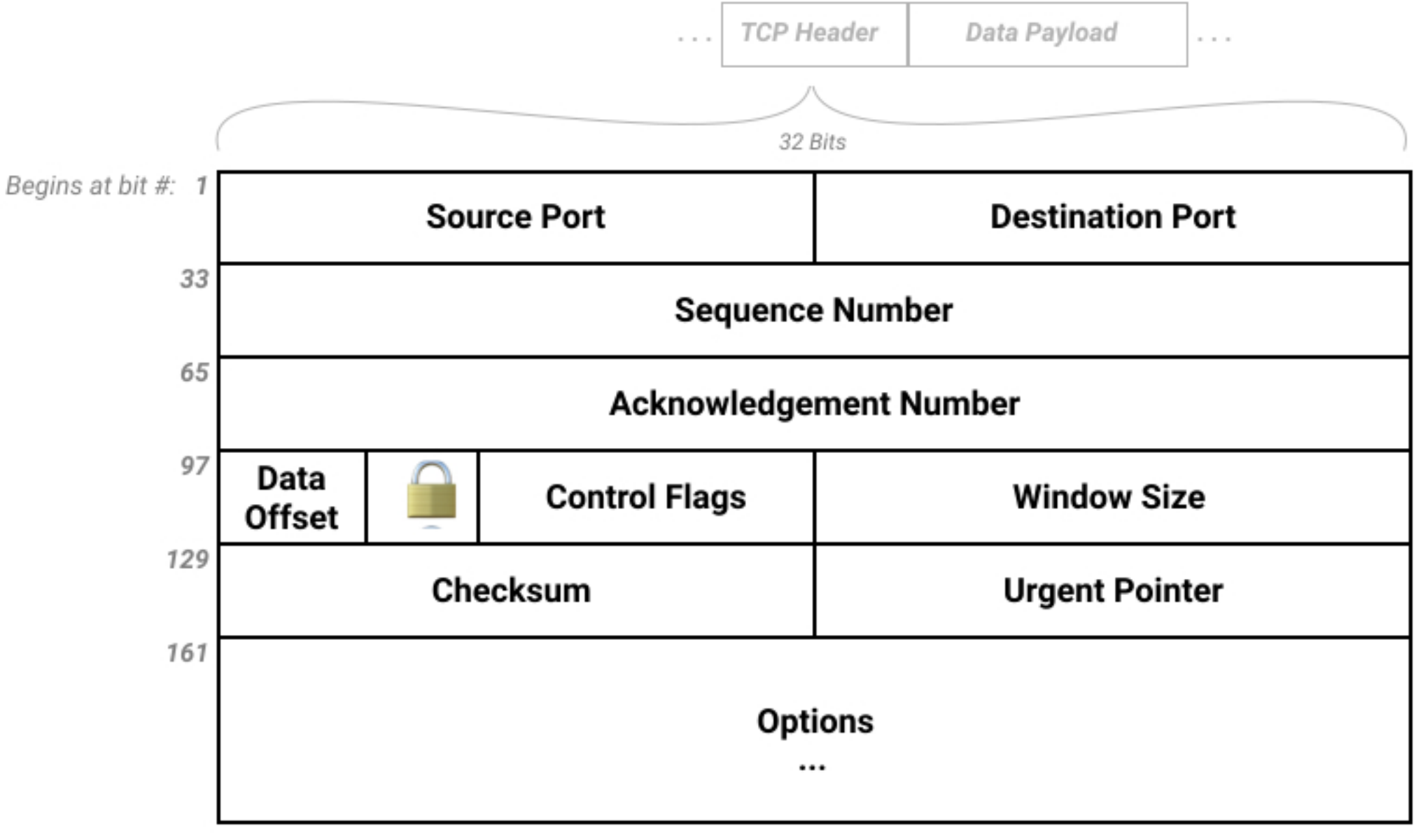


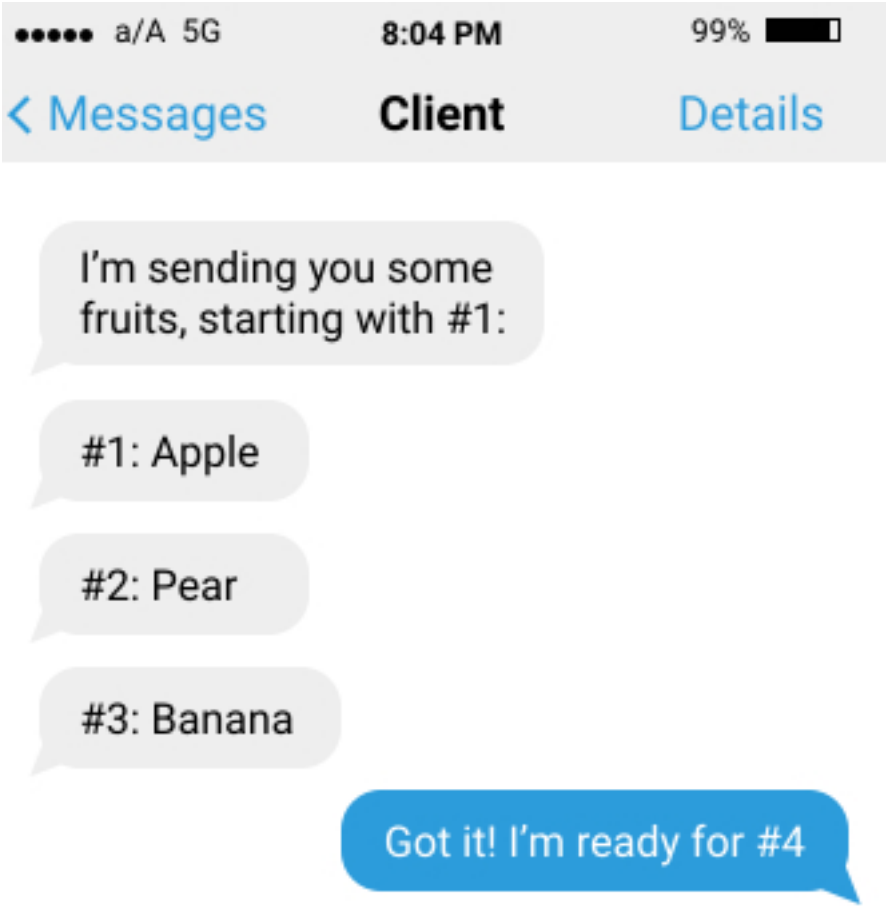


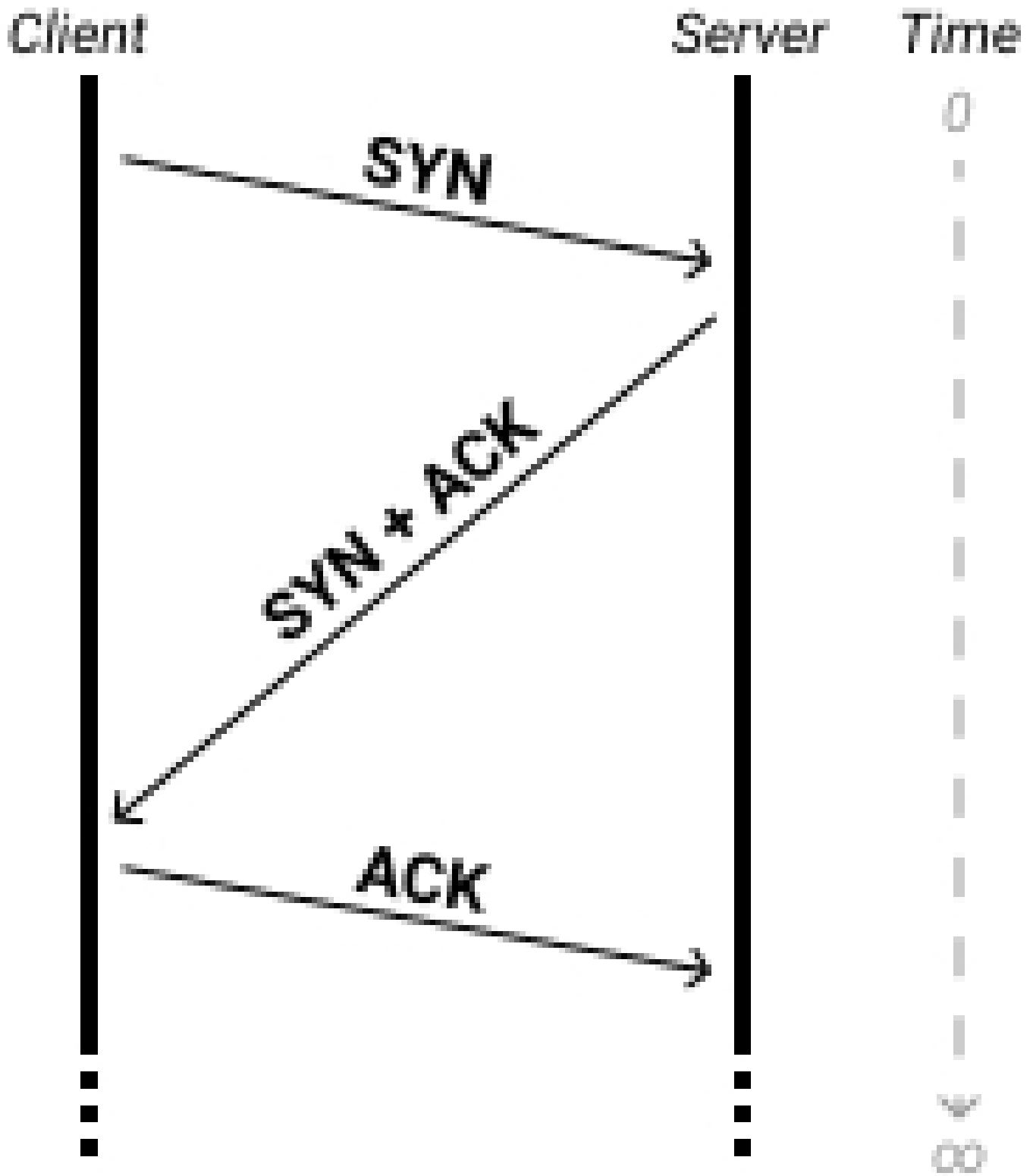

Client
Server
DATA: "hey"
Sequence number = 1
ACK
Acknowledgement number = 4
DATA: "there"
Sequence number = 4
DATA: "pal"
Sequence number = 9
ACK
Acknowledgement number = 4
DATA: "there"
Sequence number = 4
ACK
Acknowledgement number = 9
DATA: "pal"
Sequence number = 9
ACK
Acknowledgement number = 12

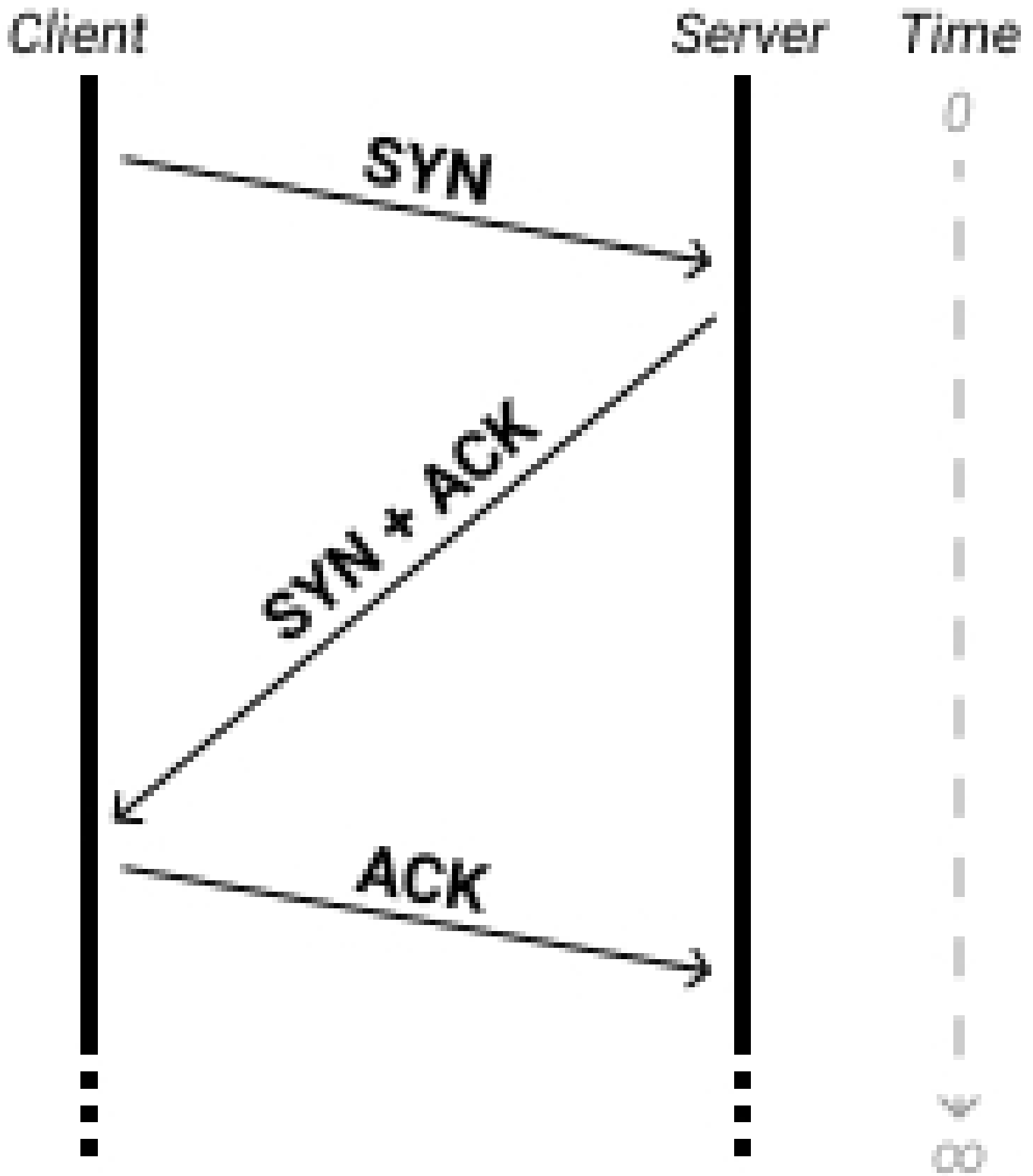

Client
Server
FIN
ACK
FIN
ACK

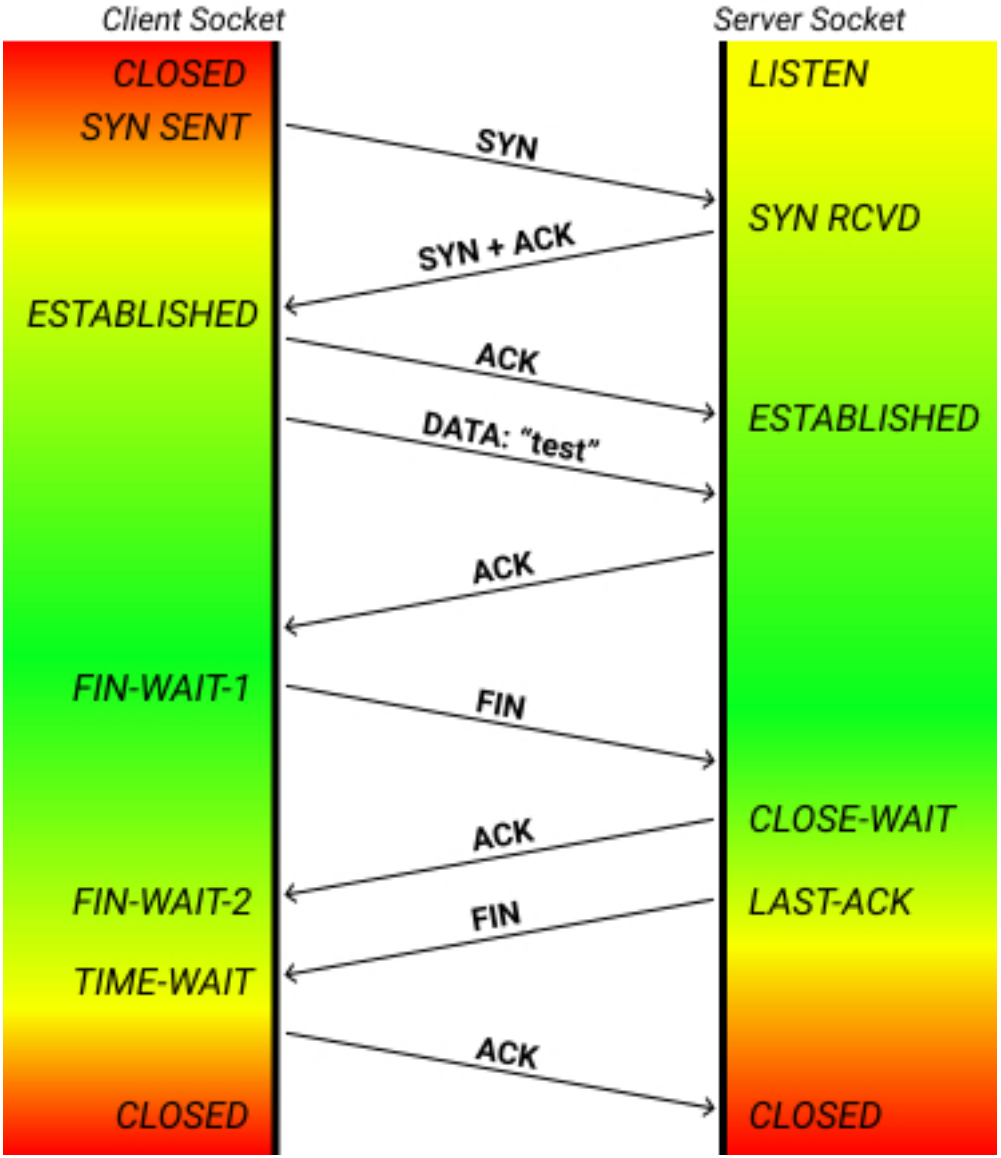

12 Bits
Reserved
Reserved
Reserved
NS
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
Network congestion monitoring
TCP Connection Lifecycle

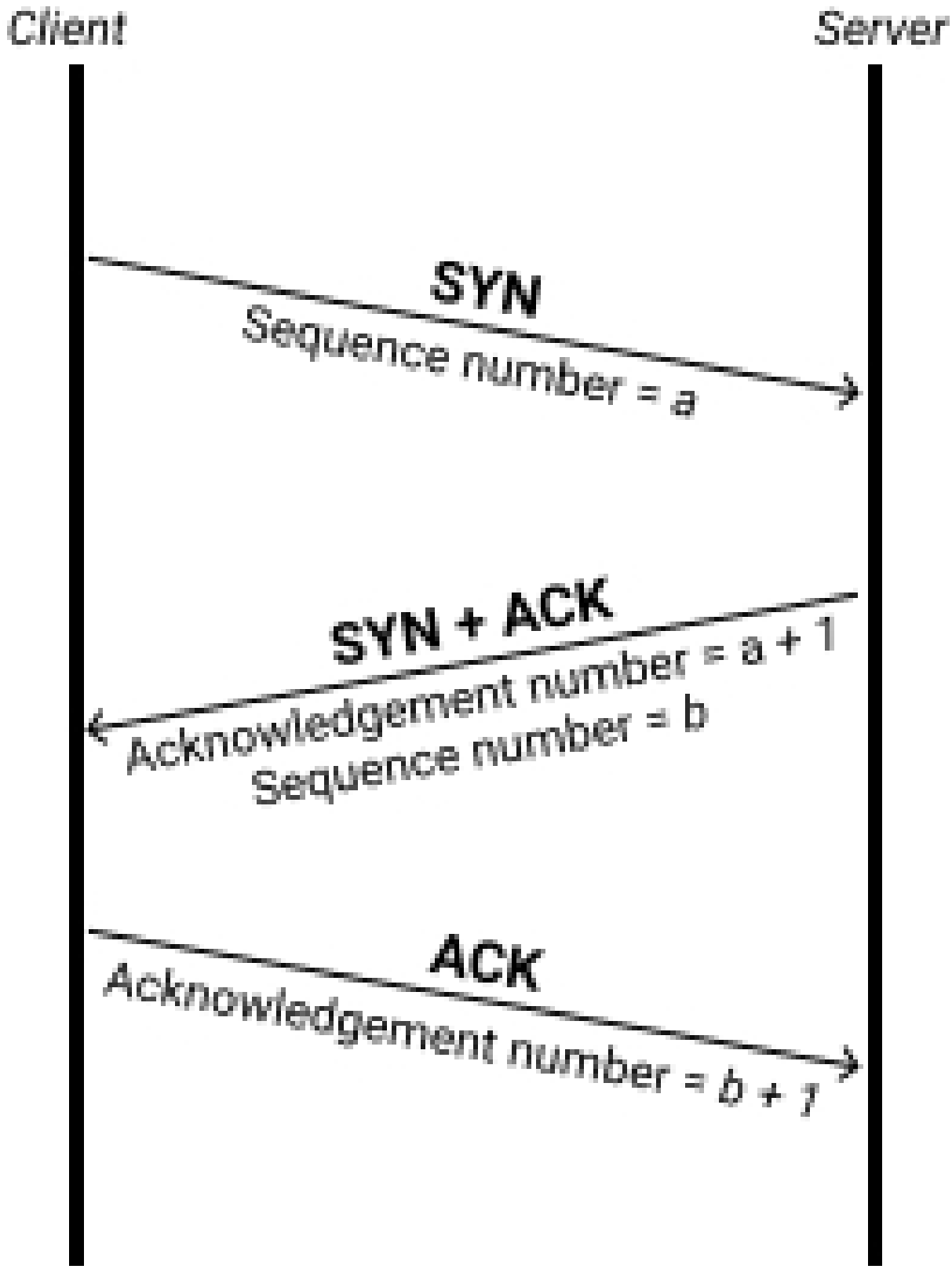

. . .
TCP Header
Data Payload
. . .
32 Bits
Begins at bit #:
1
33
65
97
129
161
Source Port
Destination Port
Sequence Number
Acknowledgement Number
Data Offset
Control Flags
Window Size
Checksum
Urgent Pointer
Options
...

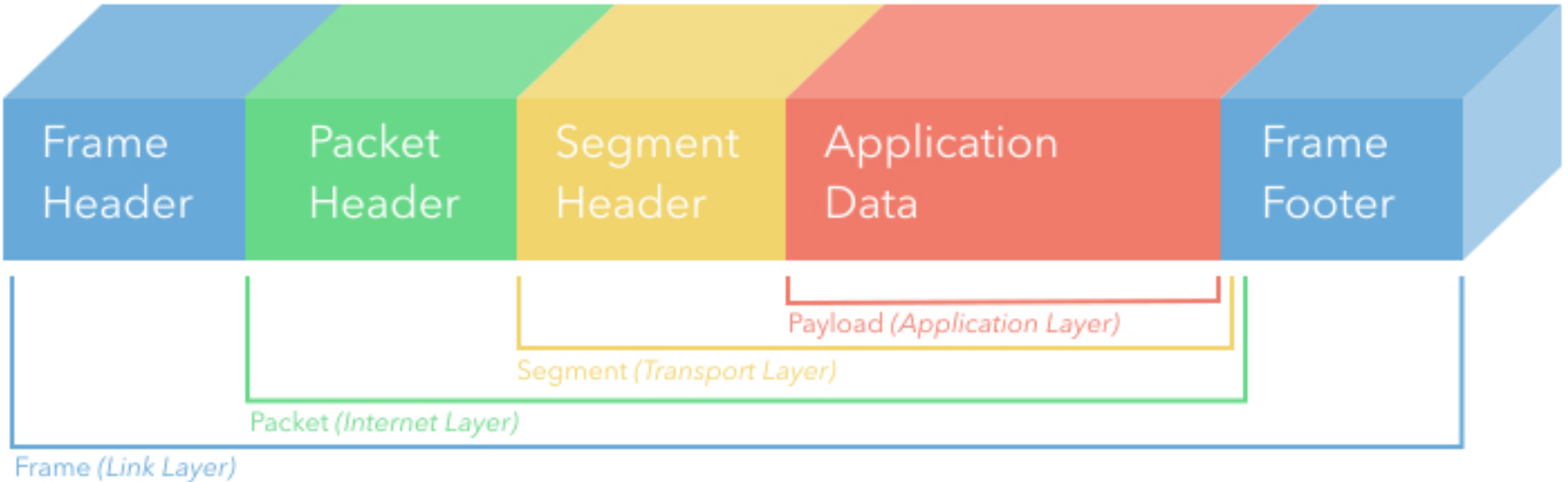

a/A 5G
8:04 PM
99%
Messages
Client
Details
I'm sending you some fruits, starting with #1:
#1: Apple
#2: Pear
#3: Banana
Got it! I'm ready for #4

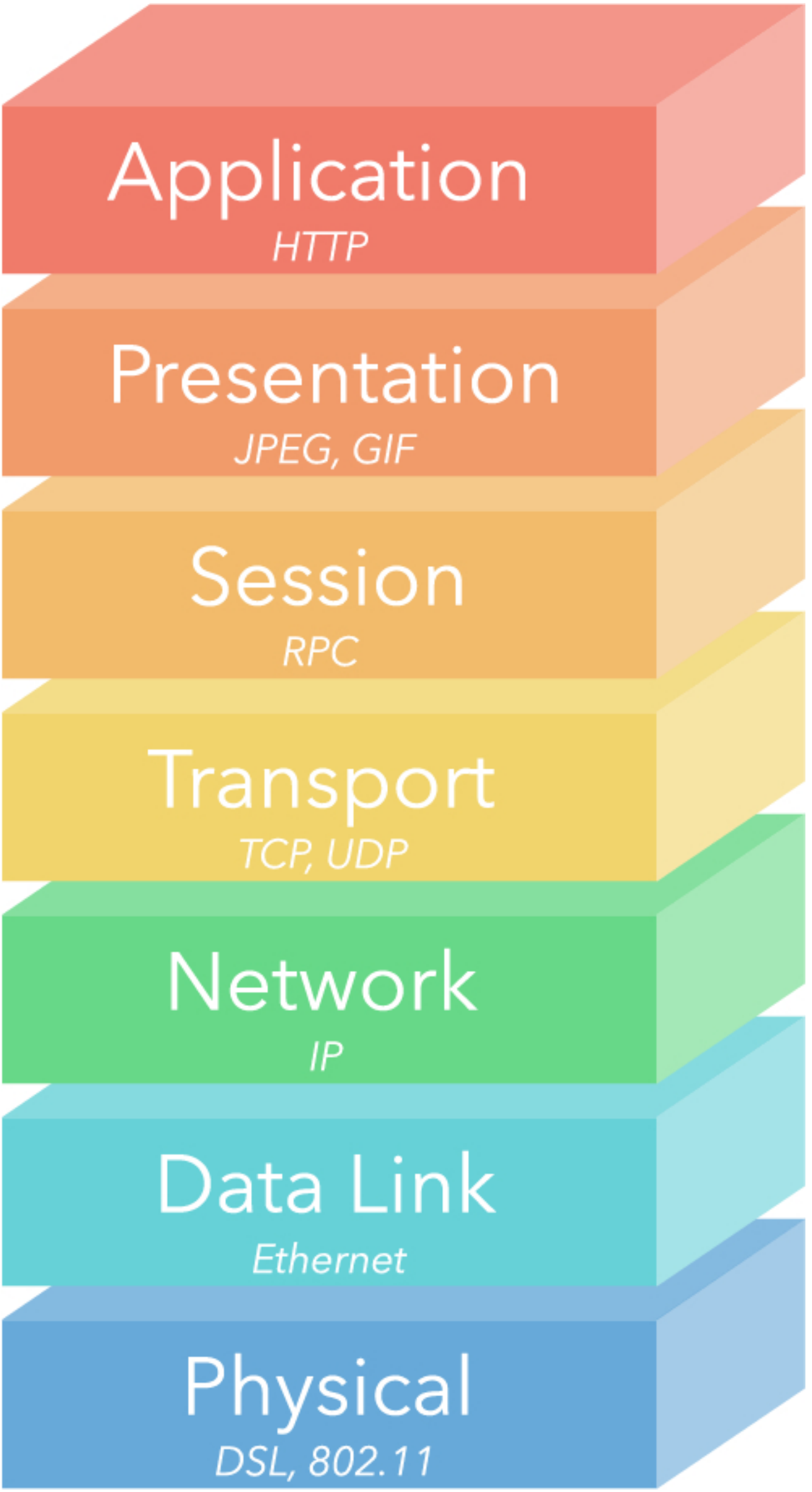

Client
Server
Time
0
SYN
SYN + ACK
ACK
∞

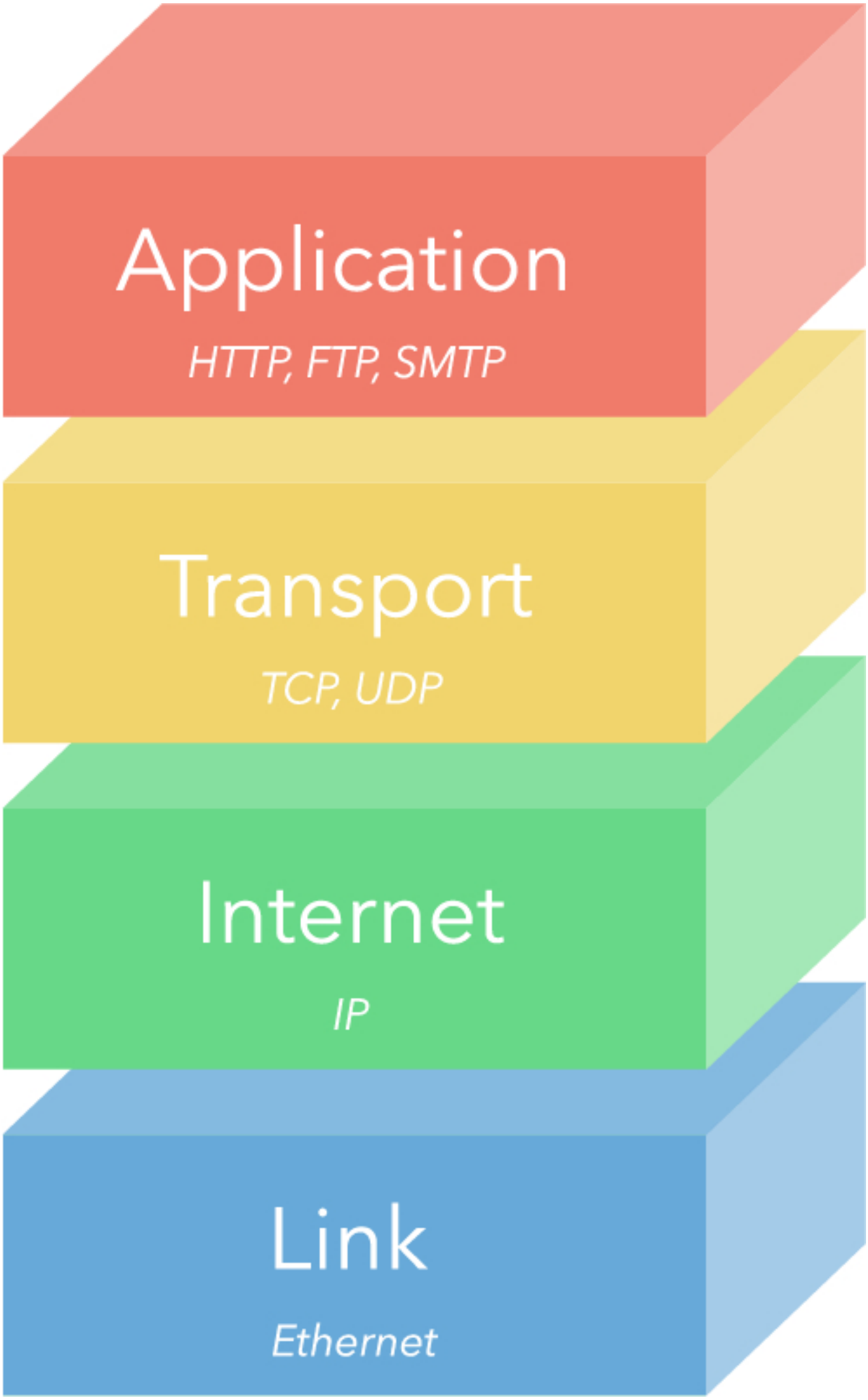

Client
Server
Time
0
SYN
SYN + ACK
ACK
∞

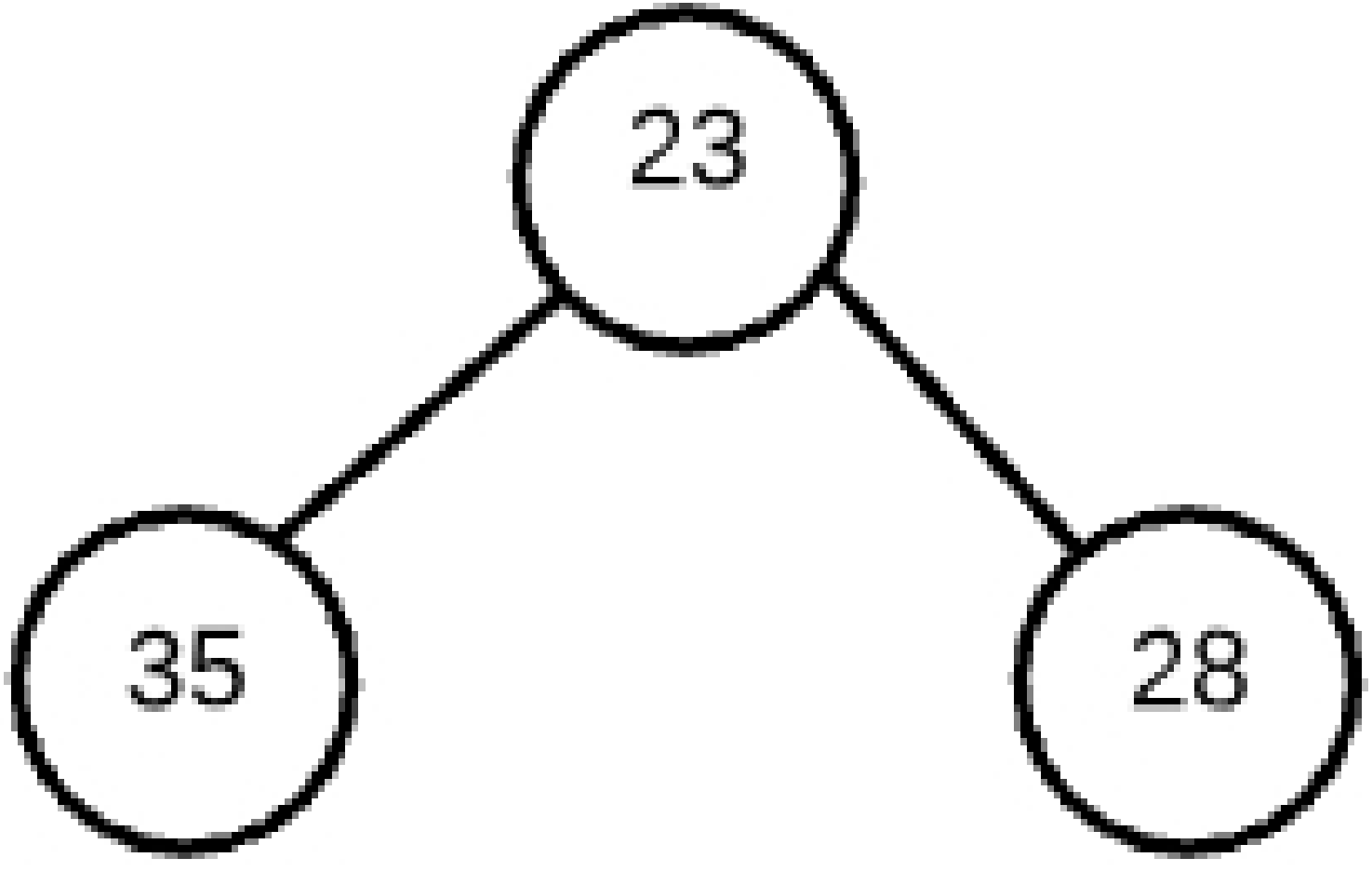

Client Socket
Server Socket
CLOSED
SYN SENT
LISTEN
SYN
SYN RCVD
SYN + ACK
ESTABLISHED
ACK
ESTABLISHED
DATA: "test"
ACK
FIN-WAIT-1
FIN
CLOSE-WAIT
ACK
FIN-WAIT-2
LAST-ACK
FIN
TIME-WAIT
ACK
CLOSED
CLOSED

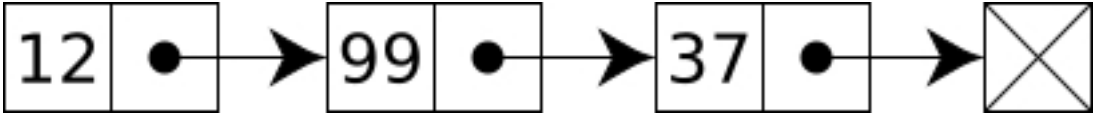

Client
Server
SYN
Sequence number = a
SYN + ACK
Acknowledgement number = a + 1
Sequence number = b
ACK
Acknowledgement number = b + 1

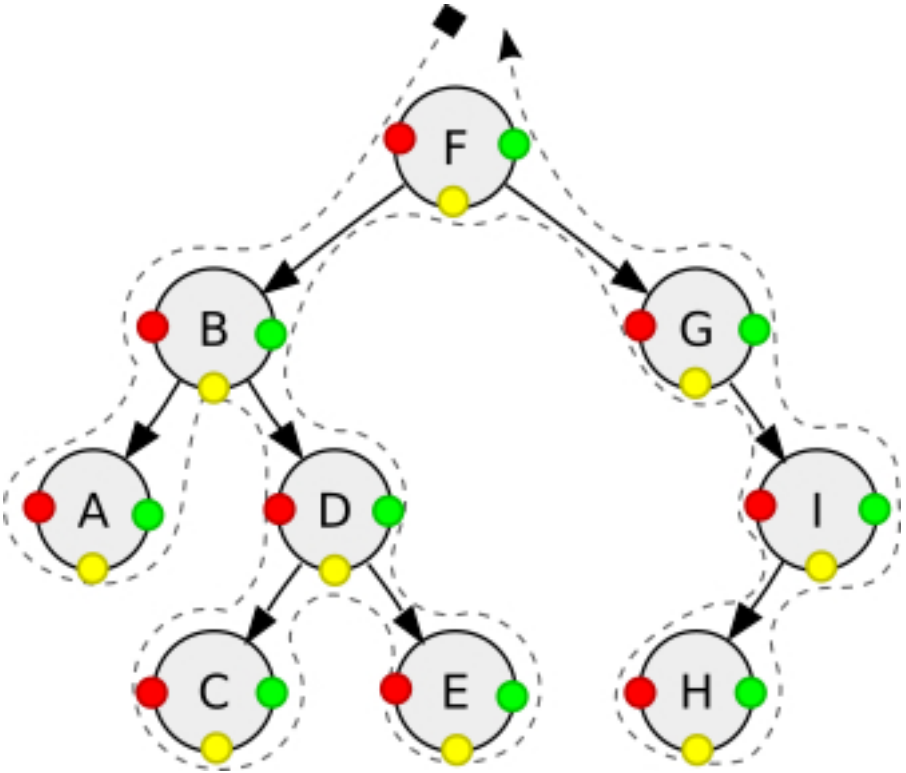

Frame Header
Packet Header
Segment Header
Application Data
Frame Footer
Payload (Application Layer)
Segment (Transport Layer)
Packet (Internet Layer)
Frame (Link Layer)

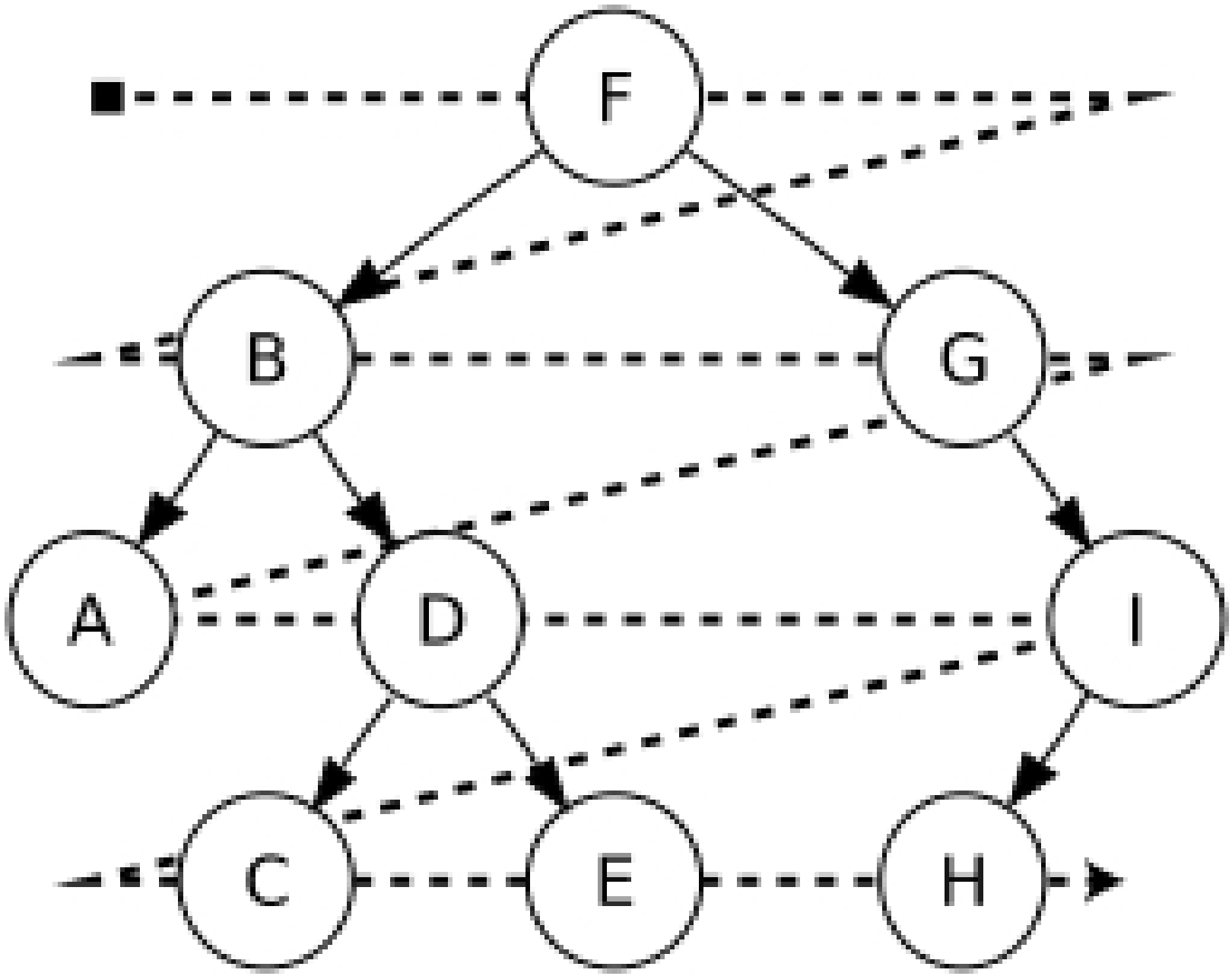

Application
HTTP
Presentation
JPEG, GIF
Session
RPC
Transport
TCP, UDP
Network
IP
Data Link
Ethernet
Physical
DSL, 802.11

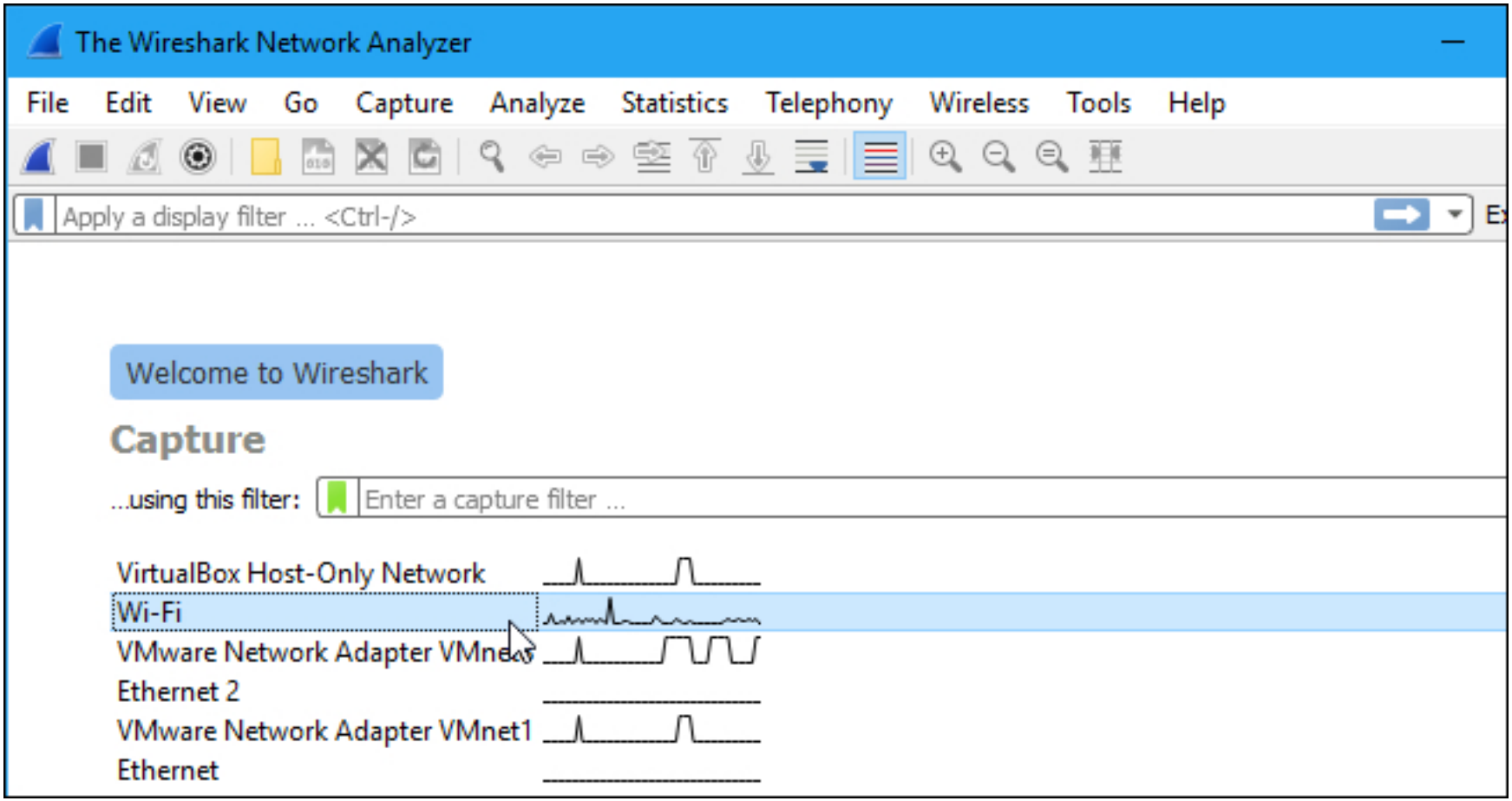

Application
HTTP, FTP, SMTP
Transport
TCP, UDP
Internet
IP
Link
Ethernet

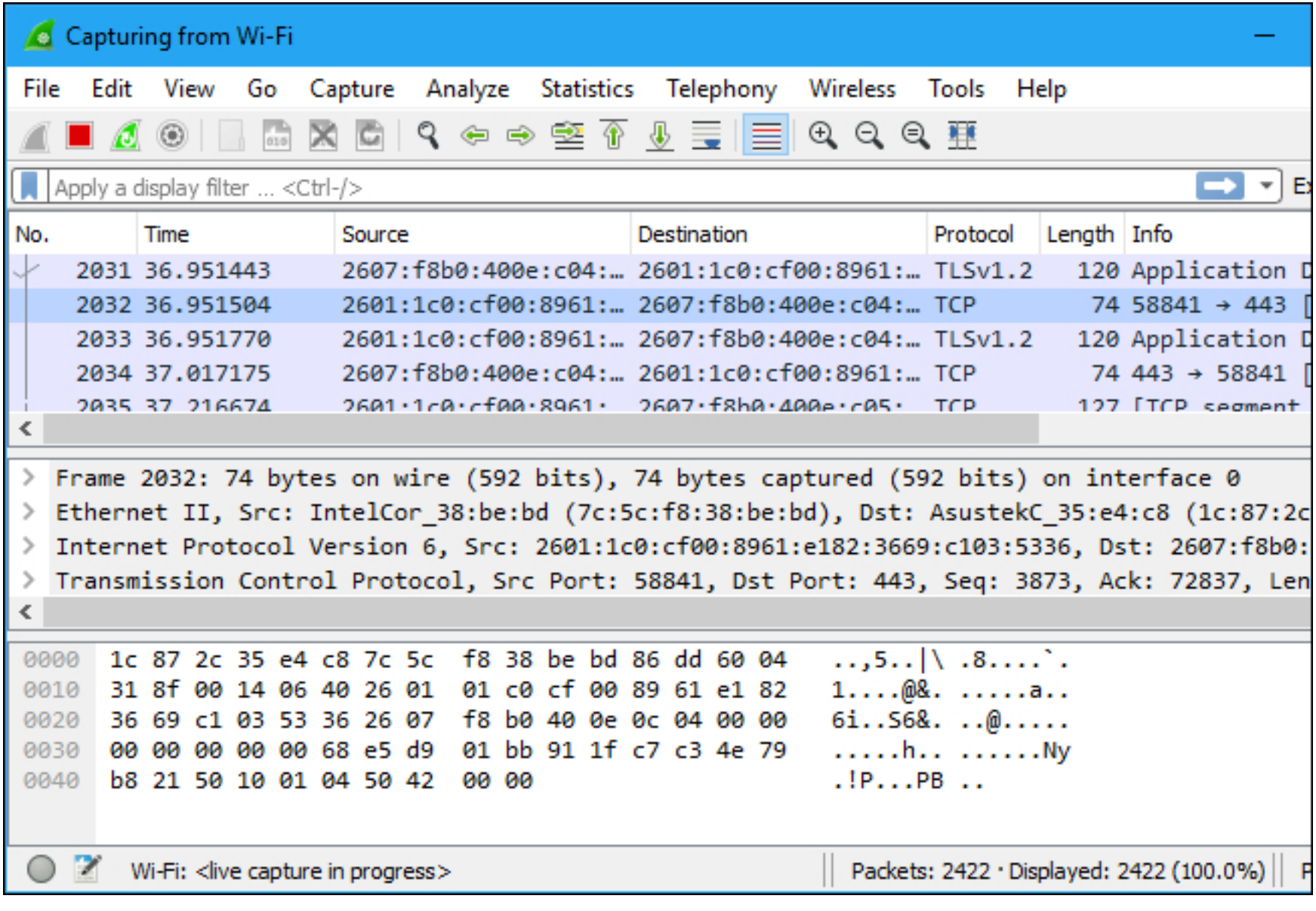

23
35
28

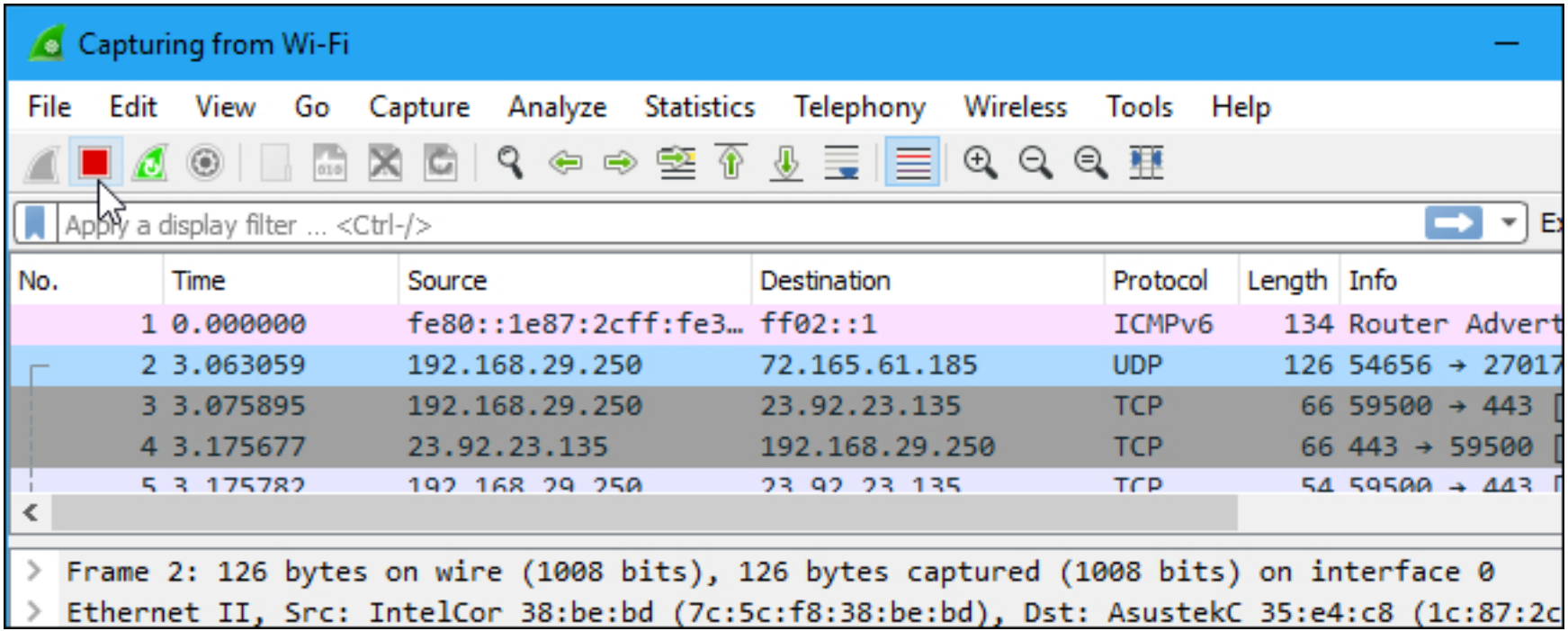

12
99
37

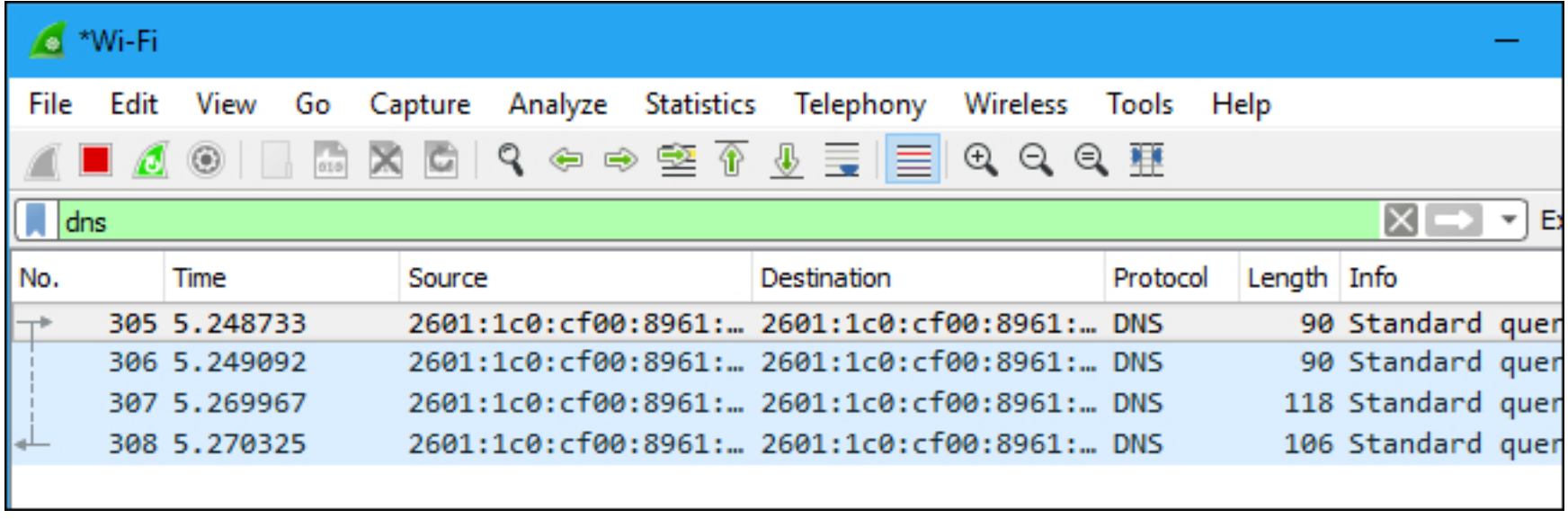

F
B
G
A
D
I
C
E
H

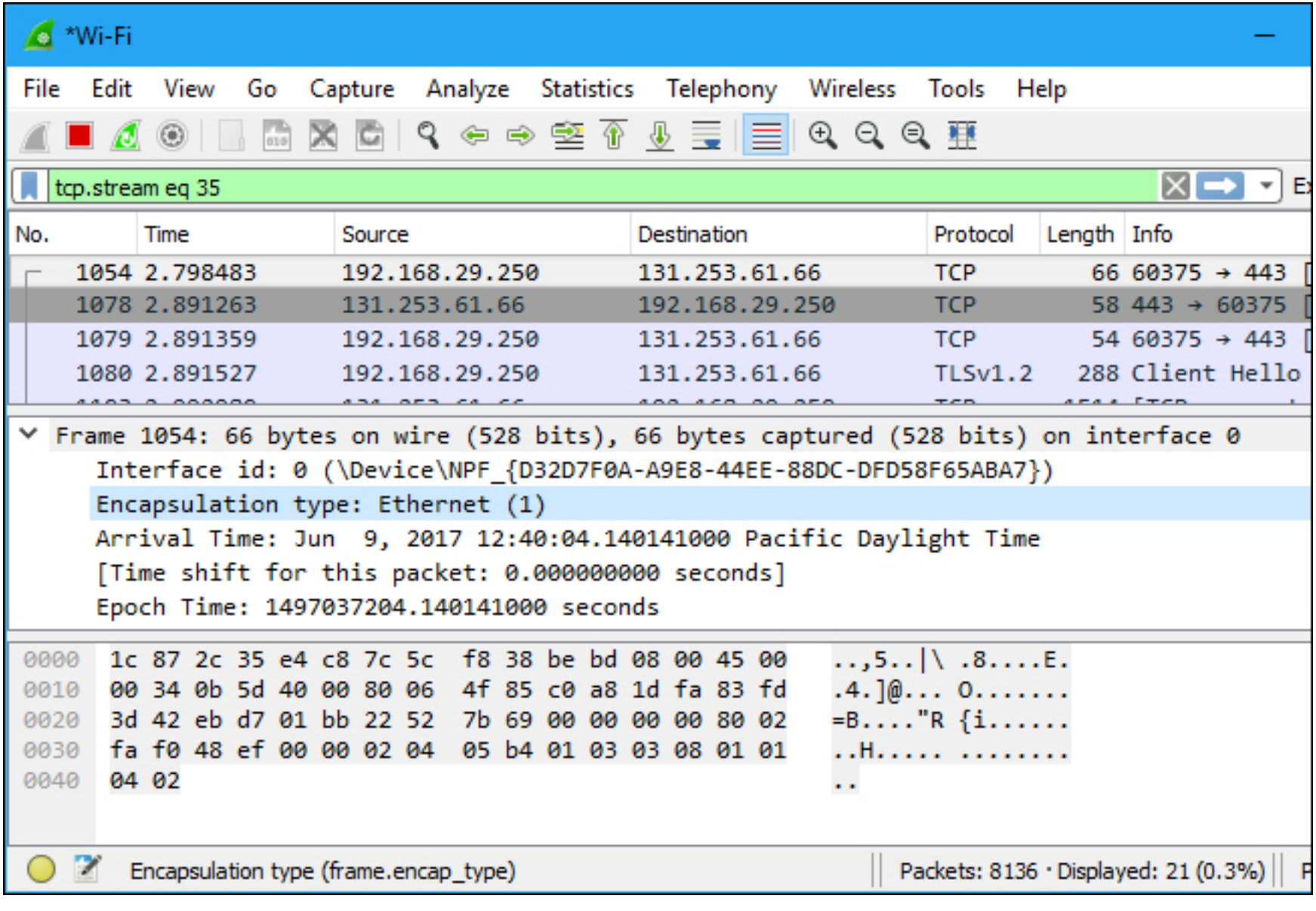

F
B
G
A
D
I
C
E
H

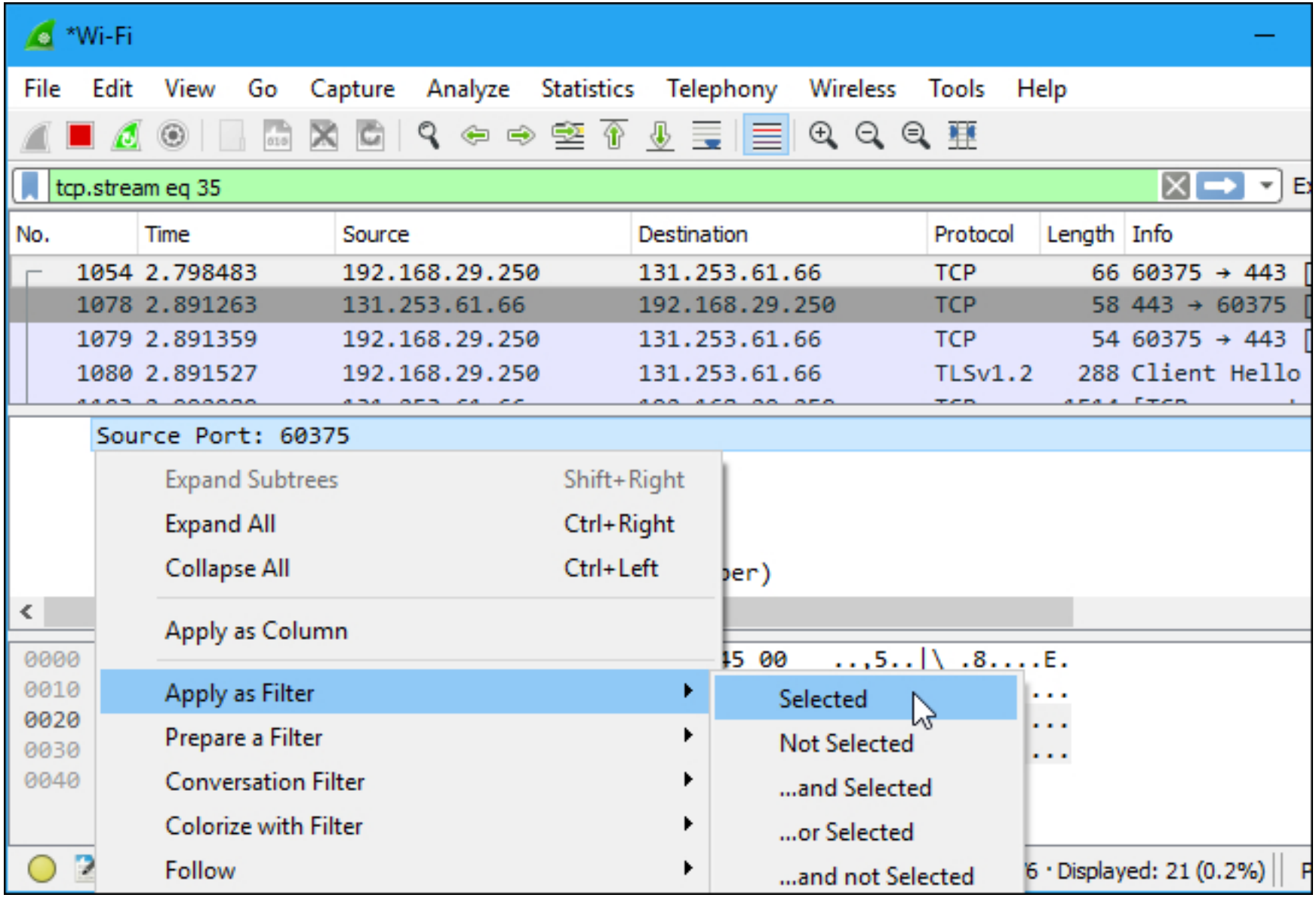

The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
VirtualBox Host-Only Network
Wi-Fi
VMware Network Adapter VMnet8
Ethernet 2
VMware Network Adapter VMnet1
Ethernet


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
2031 36.951443 2607:f8b0:400e:c04:… 2601:1c0:cf00:8961:… TLSv1.2 120 Application D
2032 36.951504 2601:1c0:cf00:8961:… 2607:f8b0:400e:c04:… TCP 74 58841 → 443 [
2033 36.951770 2601:1c0:cf00:8961:… 2607:f8b0:400e:c04:… TLSv1.2 120 Application D
2034 37.017175 2607:f8b0:400e:c04:… 2601:1c0:cf00:8961:… TCP 74 443 → 58841 [
Frame 2032: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: IntelCor_38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC_35:e4:c8 (1c:87:2c
Internet Protocol Version 6, Src: 2601:1c0:cf00:8961:e182:3669:c103:5336, Dst: 2607:f8b0:
Transmission Control Protocol, Src Port: 58841, Dst Port: 443, Seq: 3873, Ack: 72837, Len
0000 1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 86 dd 60 04 ..,5..|\ .8....`.
0010 31 8f 00 14 06 40 26 01 01 c0 cf 00 89 61 e1 82 1....@&. .....a..
0020 36 69 c1 03 53 36 26 07 f8 b0 40 0e 0c 04 00 00 6i..S6&. ..@.....
0030 00 00 00 00 00 68 e5 d9 01 bb 91 1f c7 c3 4e 79 .....h.. ......Ny
0040 b8 21 50 10 01 04 50 42 00 00 .!P...PB ..
Wi-Fi: <live capture in progress>
Packets: 2422 · Displayed: 2422 (100.0%)


Capturing from Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 fe80::1e87:2cff:fe3… ff02::1 ICMPv6 134 Router Advert
2 3.063059 192.168.29.250 72.165.61.185 UDP 126 54656 → 27017
3 3.075895 192.168.29.250 23.92.23.135 TCP 66 59500 → 443
4 3.175677 23.92.23.135 192.168.29.250 TCP 66 443 → 59500
Frame 2: 126 bytes on wire (1008 bits), 126 bytes captured (1008 bits) on interface 0
Ethernet II, Src: IntelCor 38:be:bd (7c:5c:f8:38:be:bd), Dst: AsustekC 35:e4:c8 (1c:87:2c


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dns
No. Time Source Destination Protocol Length Info
305 5.248733 2601:1c0:cf00:8961:… 2601:1c0:cf00:8961:… DNS 90 Standard quer
306 5.249092 2601:1c0:cf00:8961:… 2601:1c0:cf00:8961:… DNS 90 Standard quer
307 5.269967 2601:1c0:cf00:8961:… 2601:1c0:cf00:8961:… DNS 118 Standard quer
308 5.270325 2601:1c0:cf00:8961:… 2601:1c0:cf00:8961:… DNS 106 Standard quer


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 35
No. Time Source Destination Protocol Length Info
1054 2.798483 192.168.29.250 131.253.61.66 TCP 66 60375 → 443
1078 2.891263 131.253.61.66 192.168.29.250 TCP 58 443 → 60375
1079 2.891359 192.168.29.250 131.253.61.66 TCP 54 60375 → 443
1080 2.891527 192.168.29.250 131.253.61.66 TLSv1.2 288 Client Hello
Frame 1054: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Interface id: 0 (\Device\NPF_{D32D7F0A-A9E8-44EE-88DC-DFD58F65ABA7})
Encapsulation type: Ethernet (1)
Arrival Time: Jun 9, 2017 12:40:04.140141000 Pacific Daylight Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1497037204.140141000 seconds
0000 1c 87 2c 35 e4 c8 7c 5c f8 38 be bd 08 00 45 00 ..,5..|\ .8....E.
0010 00 34 0b 5d 40 00 80 06 4f 85 c0 a8 1d fa 83 fd .4.]@... O.....
0020 3d 42 eb d7 01 bb 22 52 7b 69 00 00 00 00 80 02 =B....."R {i.....
0030 fa f0 48 ef 00 00 02 04 05 b4 01 03 03 08 01 01 ..H..... ....
0040 04 02 ..
Encapsulation type (frame.encap_type)
Packets: 8136 · Displayed: 21 (0.3%)


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 35
No. Time Source Destination Protocol Length Info
1054 2.798483 192.168.29.250 131.253.61.66 TCP 66 60375 → 443
1078 2.891263 131.253.61.66 192.168.29.250 TCP 58 443 → 60375
1079 2.891359 192.168.29.250 131.253.61.66 TCP 54 60375 → 443
1080 2.891527 192.168.29.250 131.253.61.66 TLSv1.2 288 Client Hello
Source Port: 60375
Expand Subtrees Shift+Right
Expand All Ctrl+Right
Collapse All Ctrl+Left
Apply as Column
Apply as Filter
Prepare a Filter
Conversation Filter
Colorize with Filter
Follow
Selected
Not Selected
...and Selected
...or Selected
...and not Selected
0000
0010
0020
0030
0040
Displayed: 21 (0.2%)