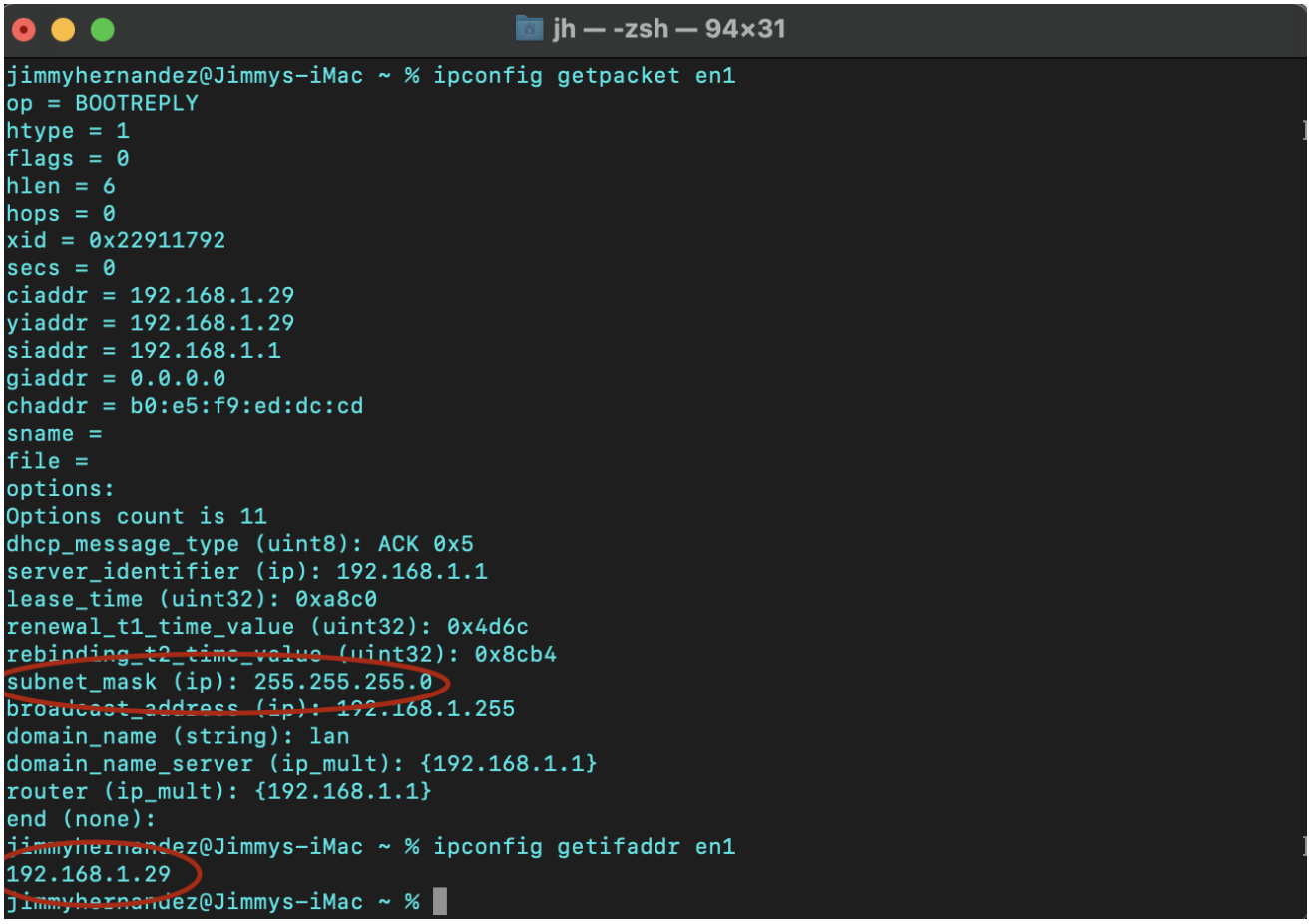
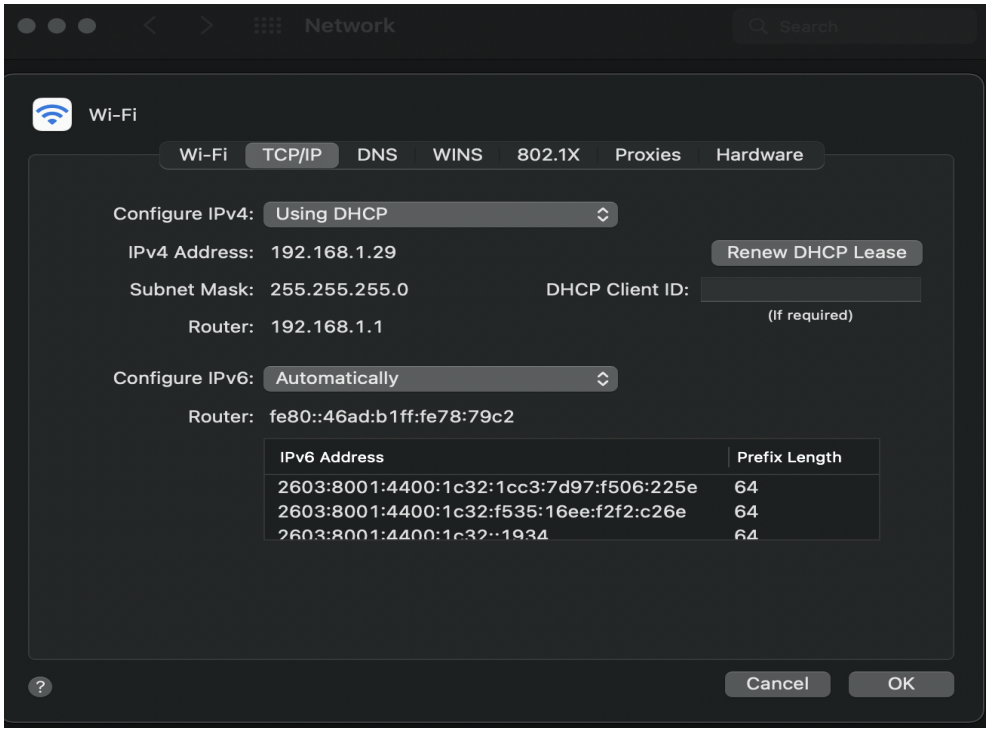
Jimmy Hernandez
CS 4771
March 12, 2022

Lab 5: Lab 4 Decoding Ethernet Frames

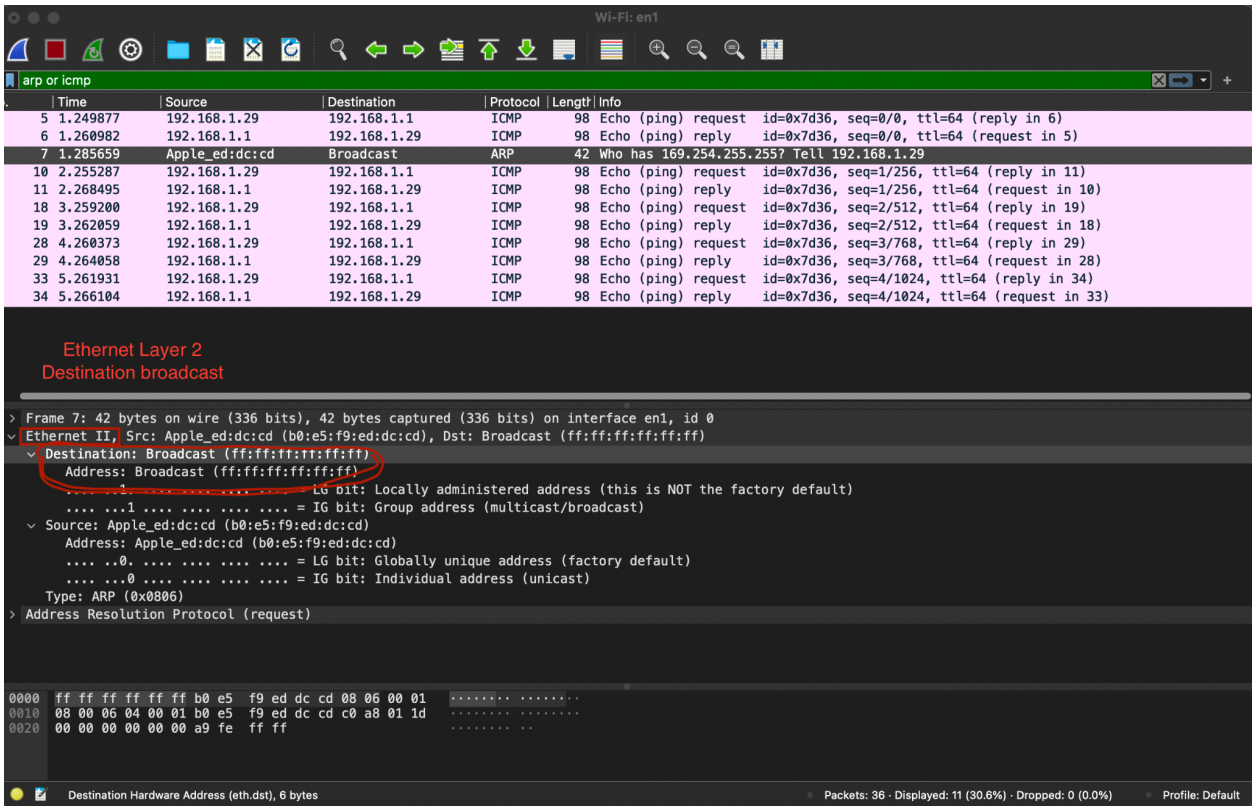
1. (2.5 pts) Turn on your sniffer and begin capturing IP version4 network traffic (Note: you may need to generate network traffic)

a. What is the IP address and subnet mask of your computer? Submit a screenshot that displays these values.

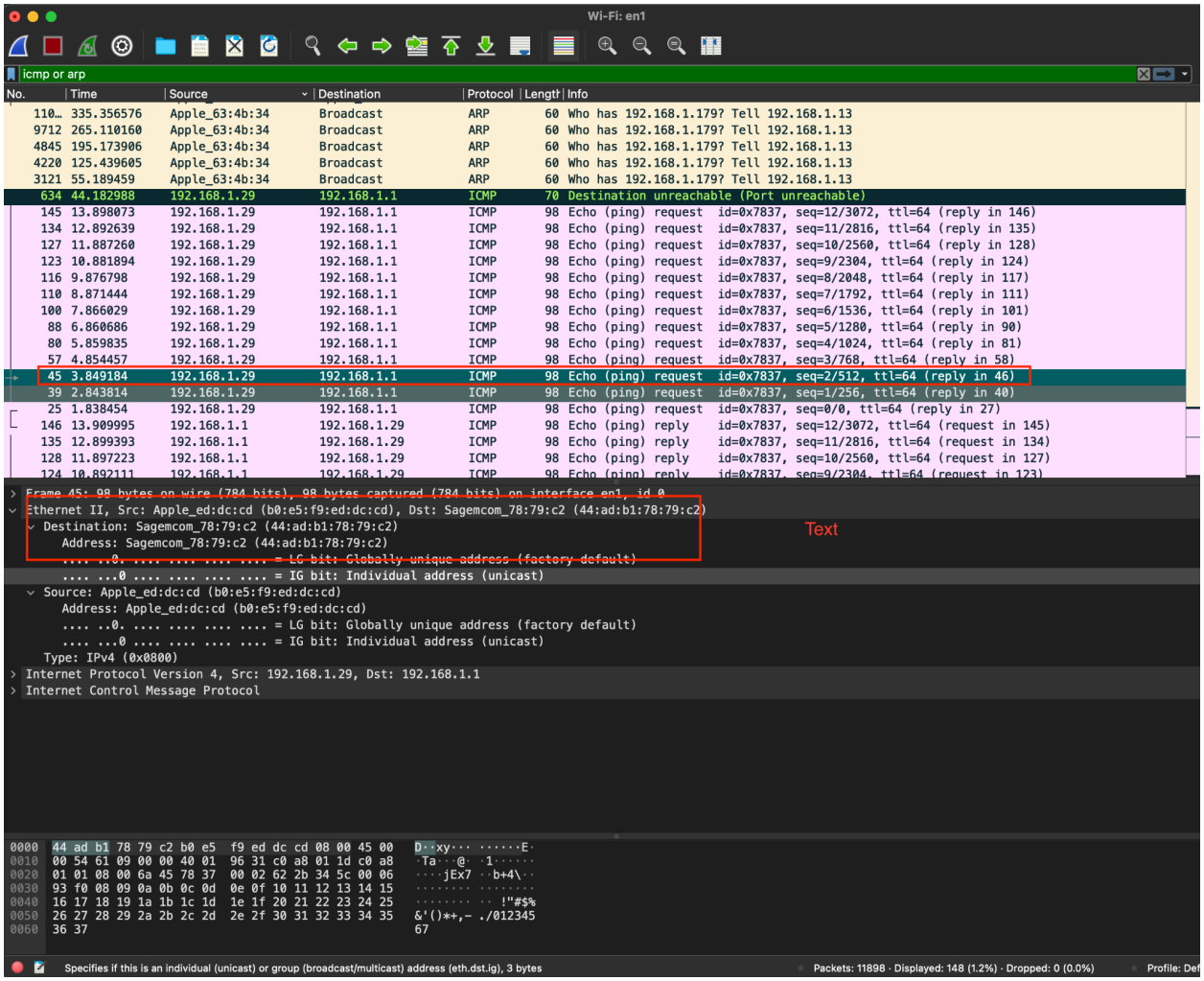




b. What is the layer-2 destination Ethernet address of broadcast (not unicast) traffic? Submit screenshot with this value circled.

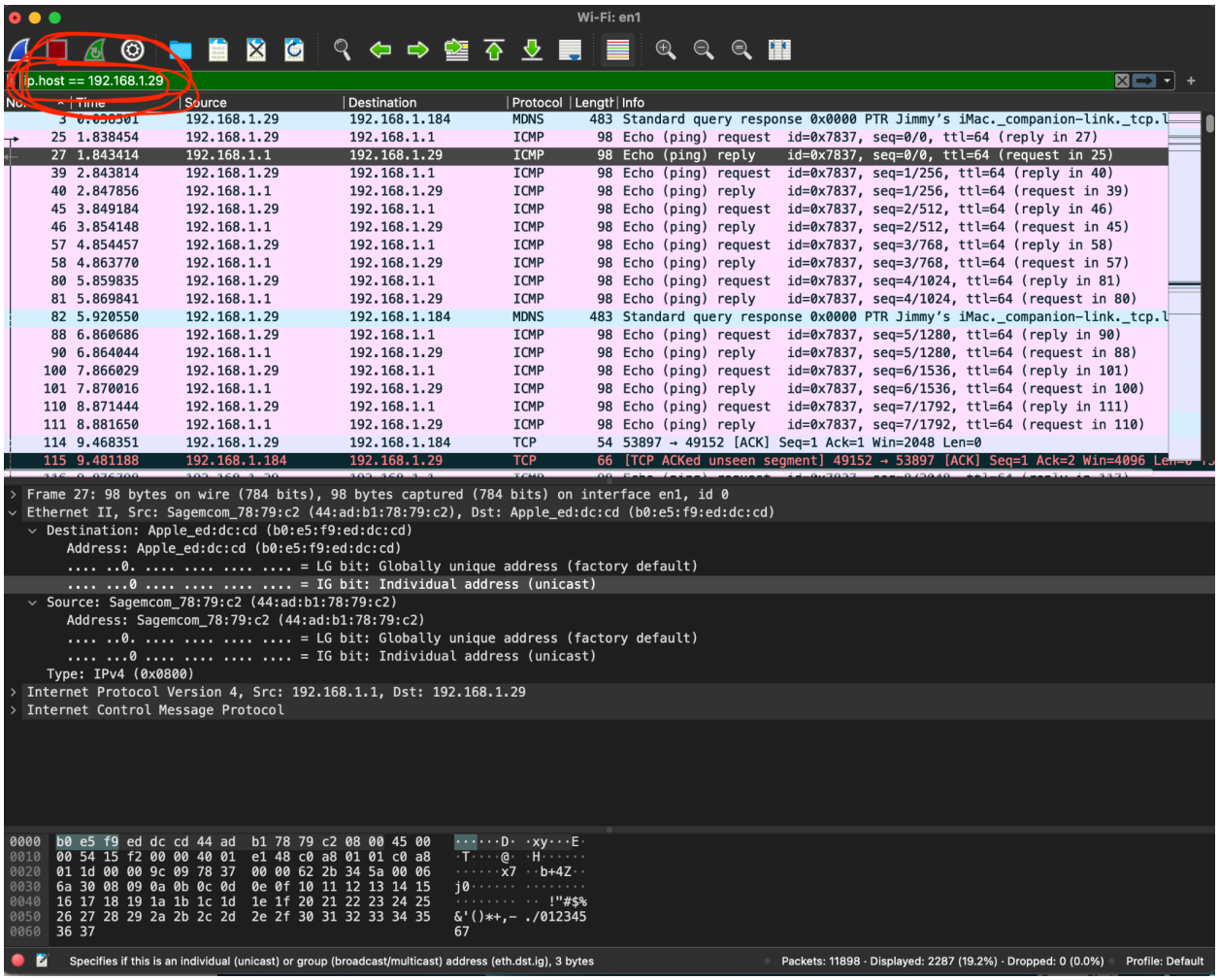


c. What is the layer-3 destination IP address of broadcast traffic that has an IP (not ARP) header? Submit screenshot with this value circled

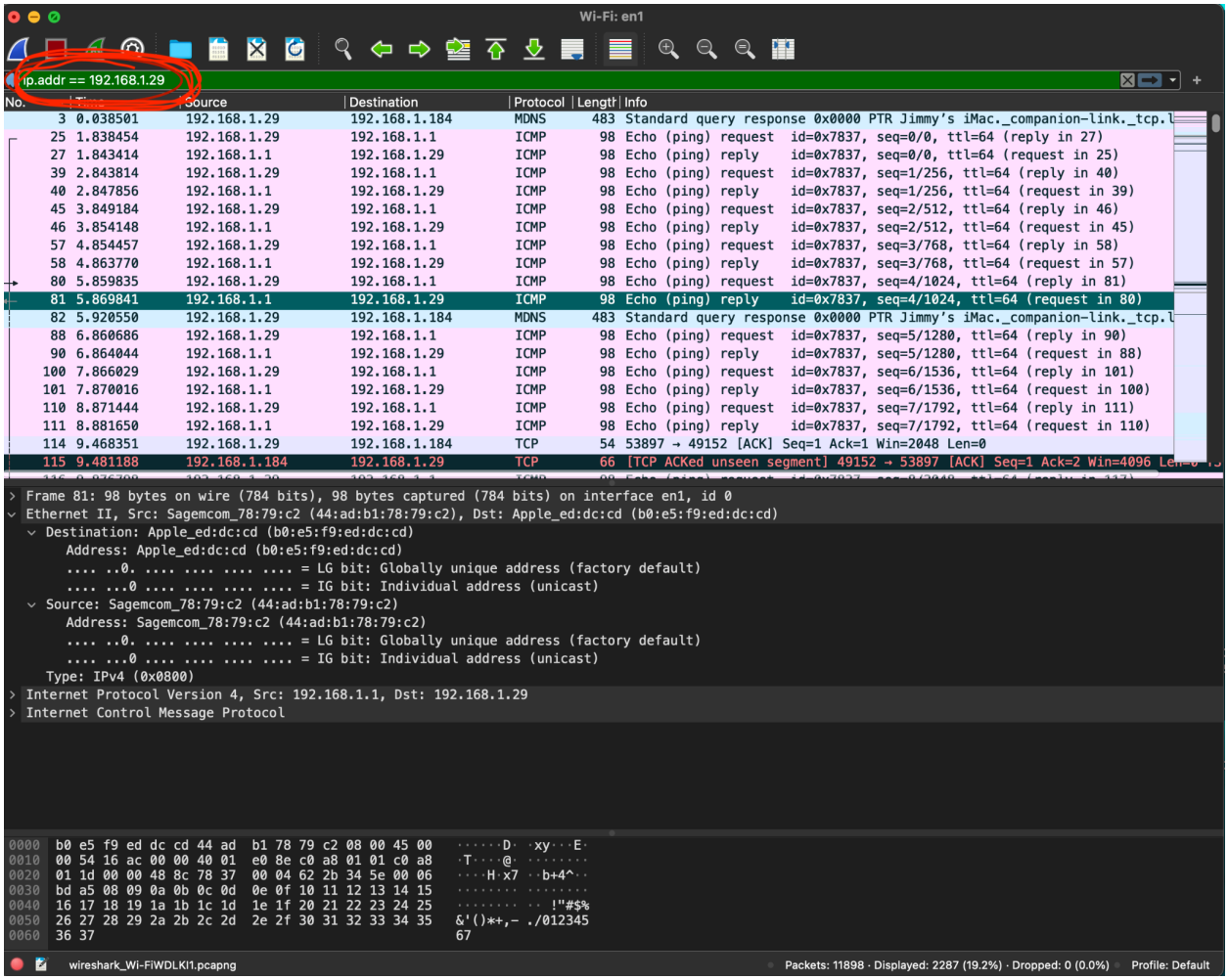


No. 45 shows a header with and IP address with the destination IP address broadcast circled in red in the lower half of the picture.

d. What filtering rule can you use on your sniffer so that it will display only Ethernet frames that contain your computer's IP address? Submit a screenshot with this filter in effect.



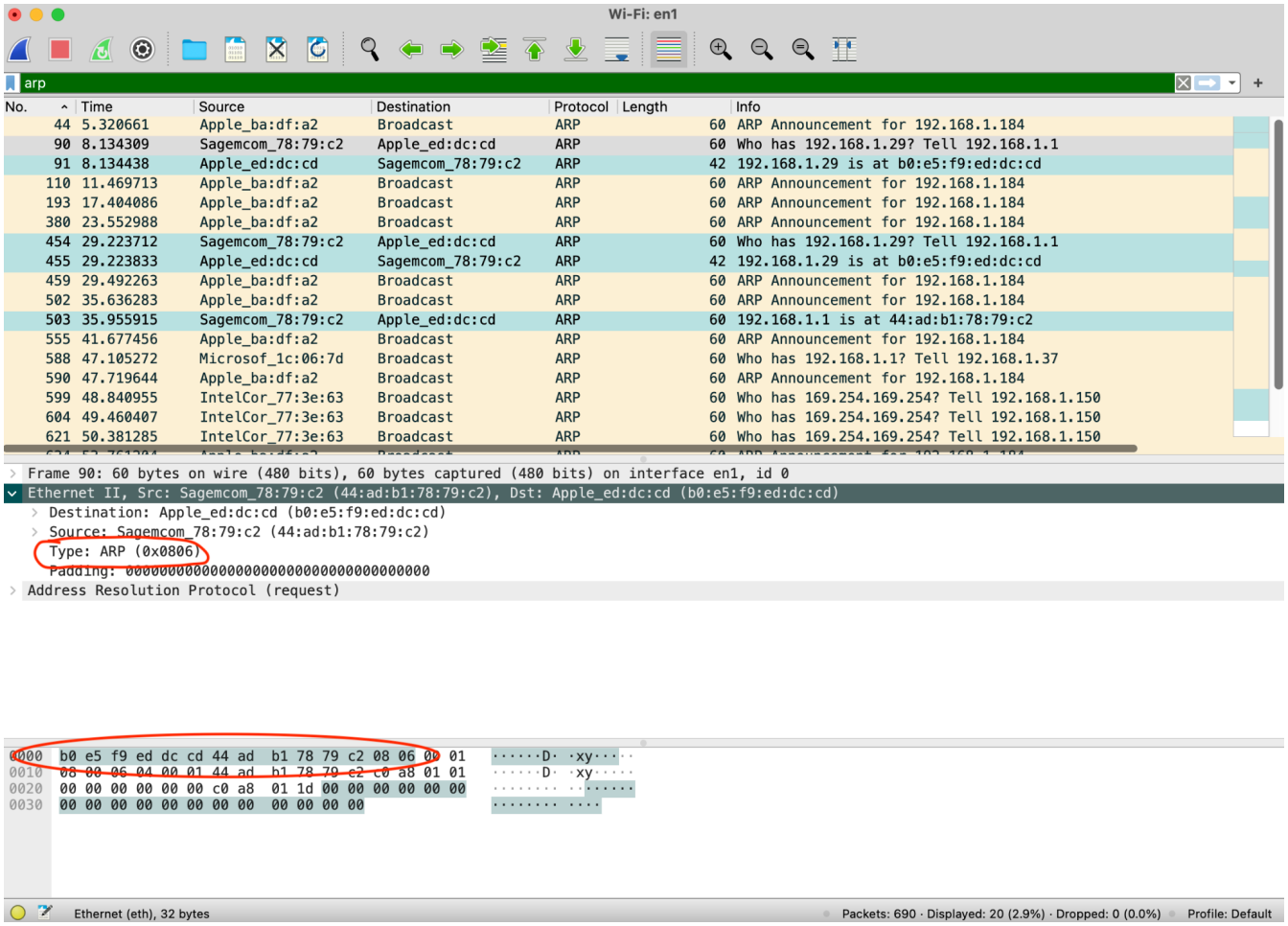
e. What filtering rule can you use on your sniffer so that it will display only Ethernet frames that contain your computer's Ethernet address in the Ethernet frame header? Submit a screenshot with this filter in effect.



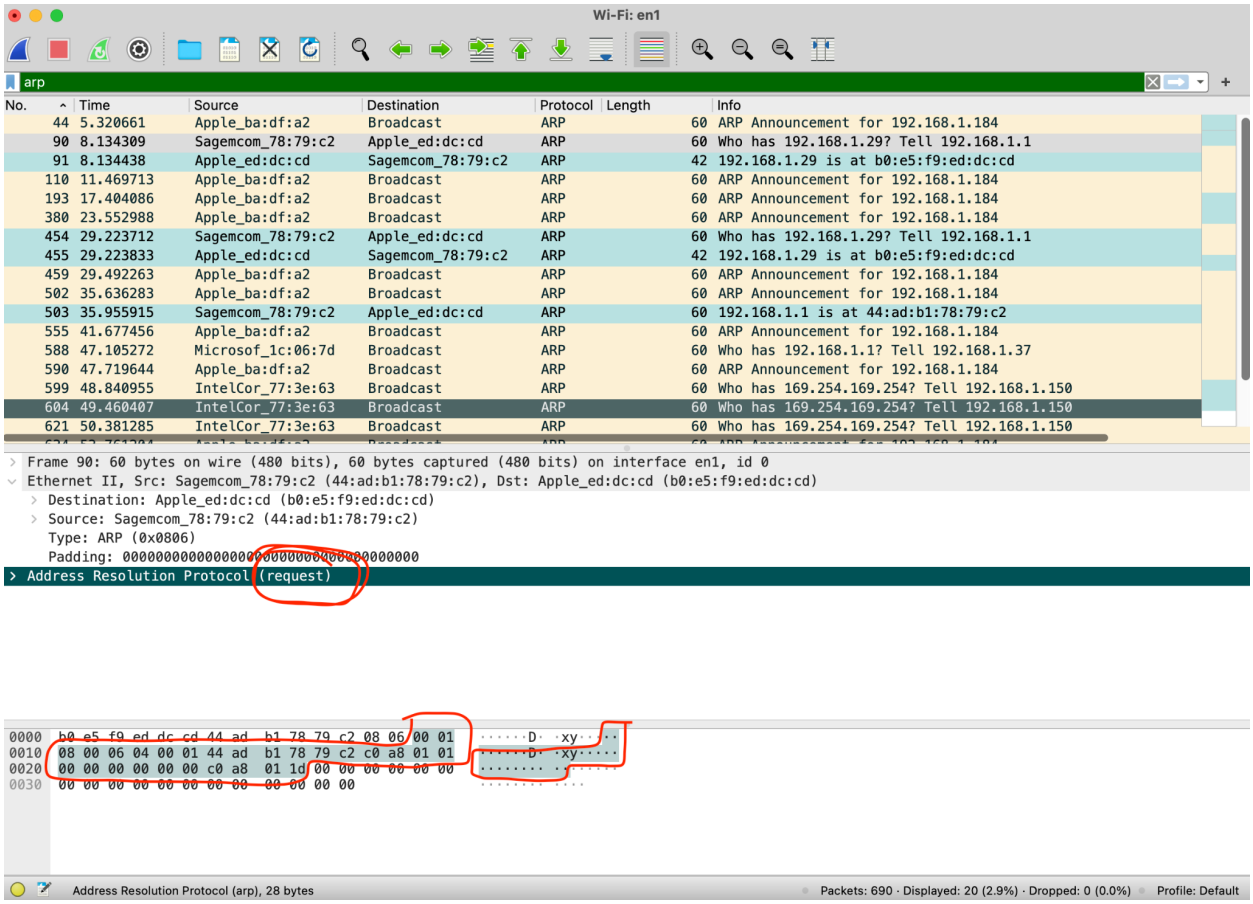
2. (2 pts) Capture and decode an ARP request and the corresponding ARP reply packet. You may need to initially clear your ARP cache (arp –d) in command prompt window (cmd.exe) before generating an ARP packet.

a. What is the hexadecimal value the field in Ethernet frame header that is used to identify that the packet is an ARP packet? Submit screenshot with this value circled.

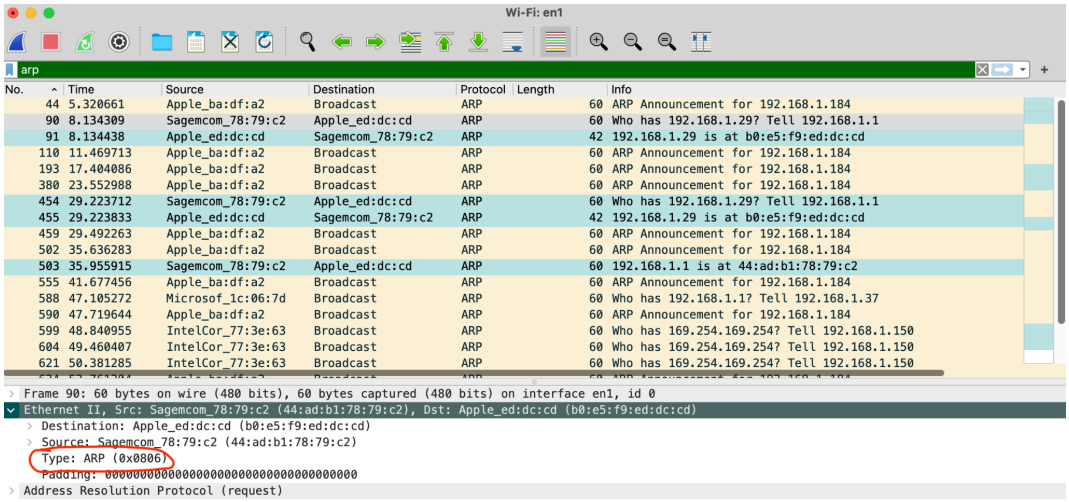
I believe the “08 06” is what declares the following bytes that come before is what declares what kind of type it is because when arp is clicked it only highlights those numbers but assuming you want the hexadecimal value too it would be everything that comes before it.

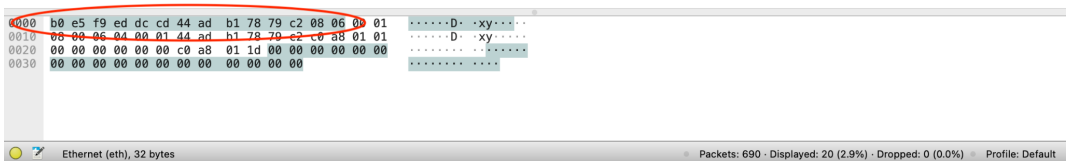


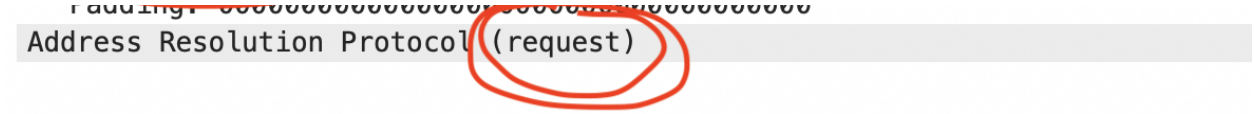
b. Turn in screenshots which show the decoded ARP request and ARP reply packets. First image is a request with the decoded bytes at the bottom.

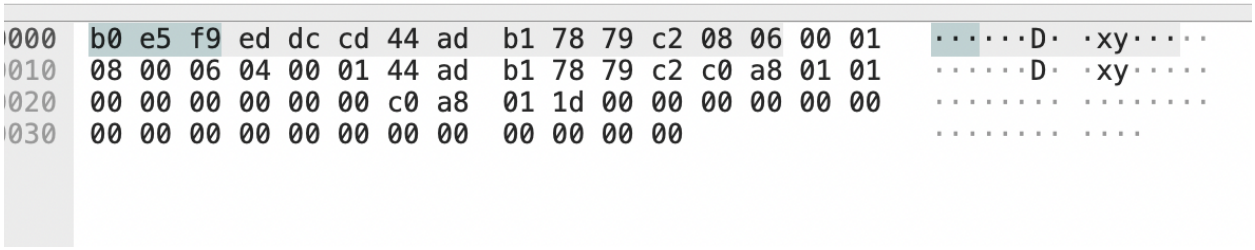


The second image is a reply with the decoded bytes at the bottom



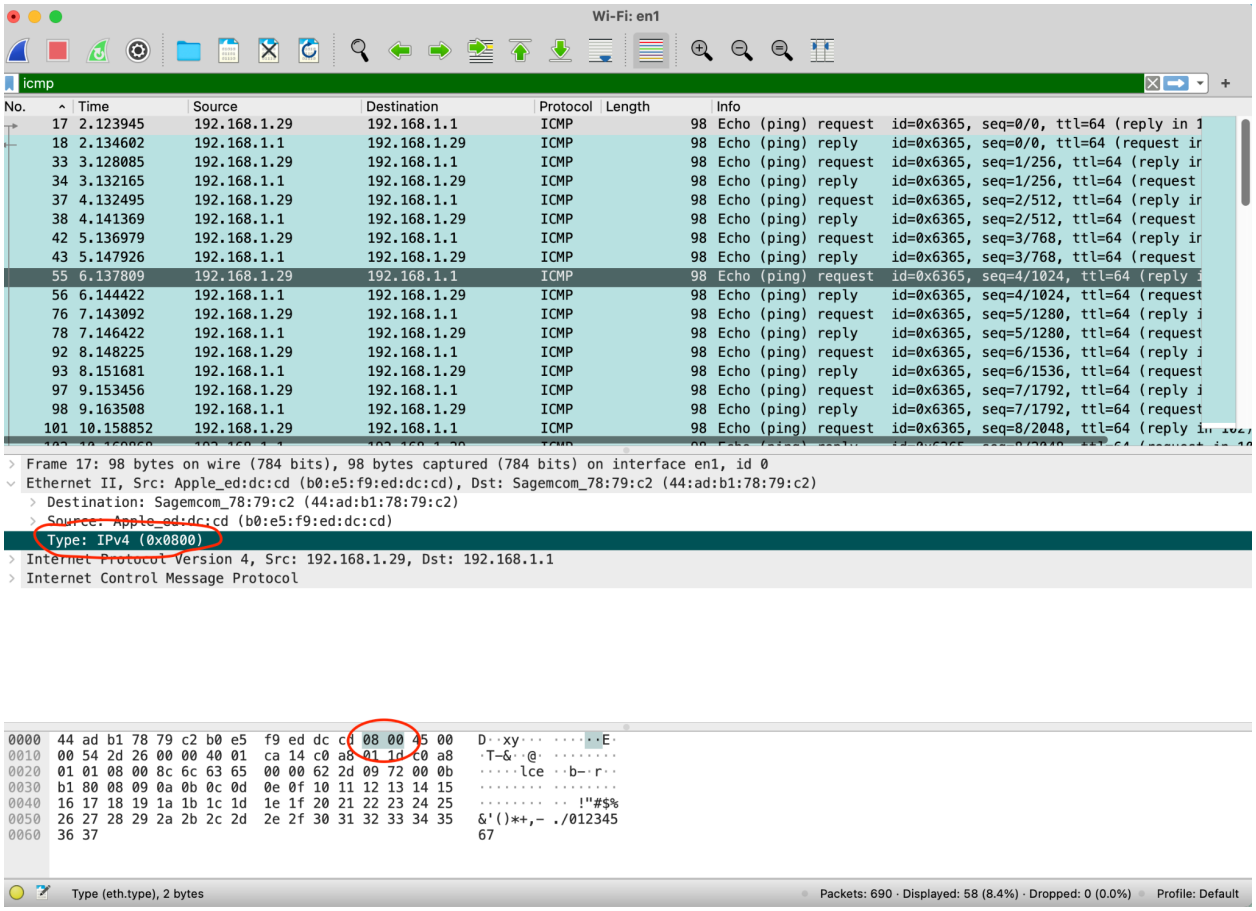




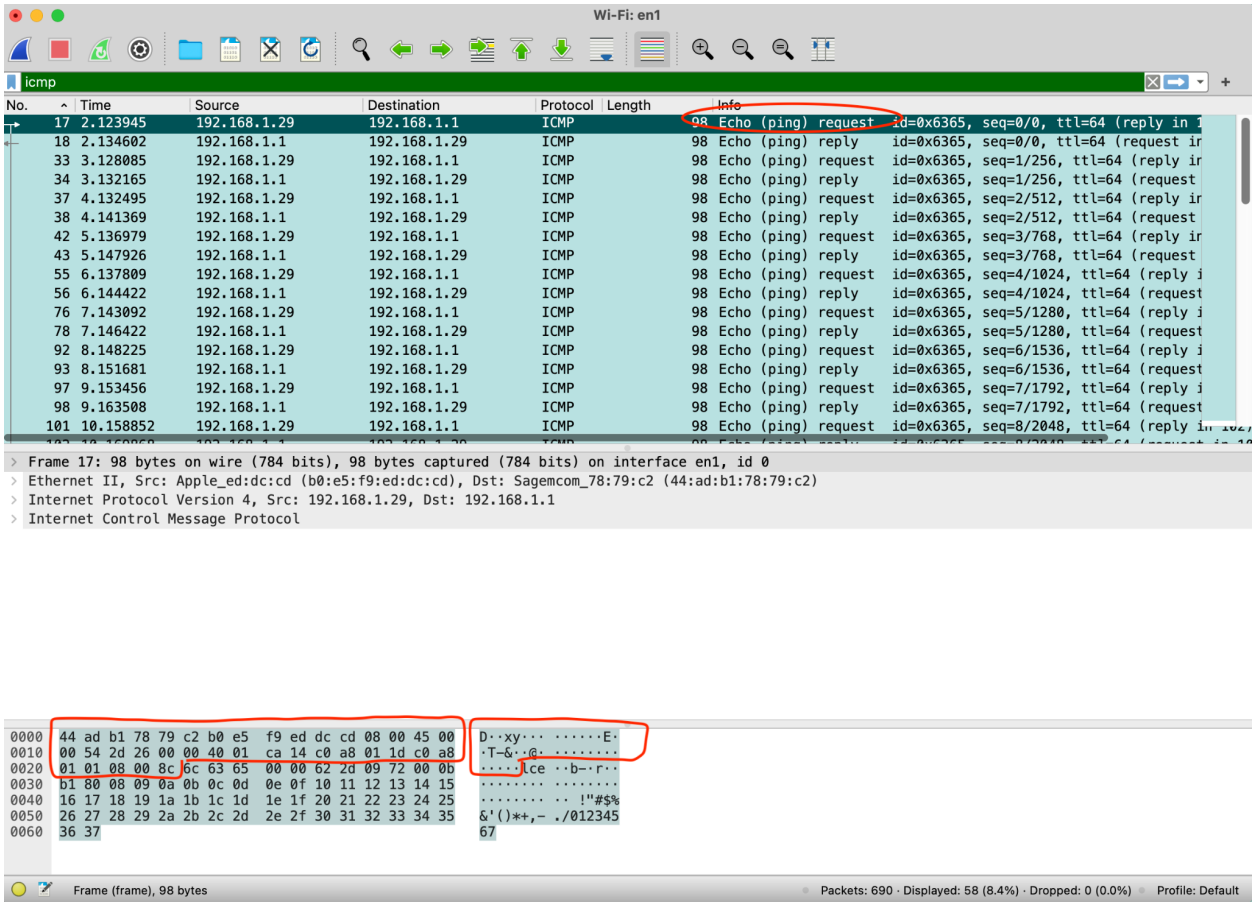


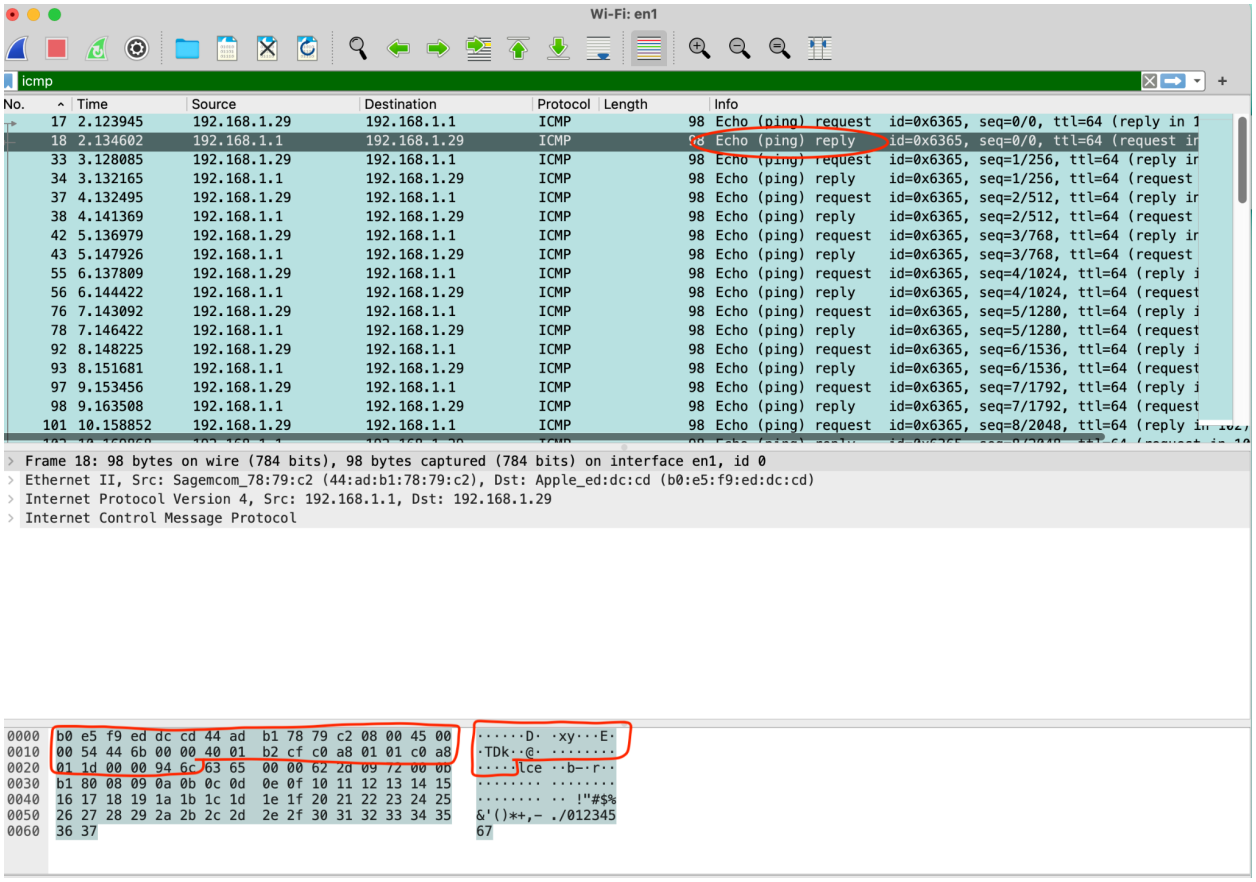
3. (2 pts) Capture and decode an IP version4 ICMP echo request and the corresponding ICMP echo reply packet by running the ping command.

a. What is the decimal value of the protocol field in IP header that is used to indicate that the packet is an ICMP packet? Submit screenshot with this value circled.



b. Turn in screenshots which show the decoded ICMP echo request and ICMP echo reply packets.


Wi-Fi: en1
icmp
No. Time Source Destination Protocol Length Info
17 2.123945 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=0/0, ttl=64 (reply in 1
18 2.134602 192.168.1.1 192.168.1.29 ICMP 98 Echo (ping) reply id=0x6365, seq=0/0, ttl=64 (request ir
33 3.128085 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=1/256, ttl=64 (reply ir
34 3.132165 192.168.1.1 192.168.1.29 ICMP 98 Echo (ping) reply id=0x6365, seq=1/256, ttl=64 (request
37 4.132495 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=2/512, ttl=64 (reply ir
38 4.141369 192.168.1.1 192.168.1.29 ICMP 98 Echo (ping) reply id=0x6365, seq=2/512, ttl=64 (request
42 5.136979 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=3/768, ttl=64 (reply ir
43 5.147926 192.168.1.1 192.168.1.29 ICMP 98 Echo (ping) reply id=0x6365, seq=3/768, ttl=64 (request
55 6.137809 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=4/1024, ttl=64 (reply i
56 6.144422 192.168.1.1 192.168.1.29 ICMP 98 Echo (ping) reply id=0x6365, seq=4/1024, ttl=64 (request
76 7.143092 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=5/1280, ttl=64 (reply i
78 7.146422 192.168.1.1 192.168.1.29 ICMP 98 Echo (ping) reply id=0x6365, seq=5/1280, ttl=64 (request
92 8.148225 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=6/1536, ttl=64 (reply i
93 8.151681 192.168.1.1 192.168.1.29 ICMP 98 Echo (ping) reply id=0x6365, seq=6/1536, ttl=64 (request
97 9.153456 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=7/1792, ttl=64 (reply i
98 9.163508 192.168.1.1 192.168.1.29 ICMP 98 Echo (ping) reply id=0x6365, seq=7/1792, ttl=64 (request
101 10.158852 192.168.1.29 192.168.1.1 ICMP 98 Echo (ping) request id=0x6365, seq=8/2048, ttl=64 (reply i
Frame 17: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface en1, id 0
Ethernet II, Src: Apple_ed:dc:cd (b0:e5:f9:ed:dc:cd), Dst: Sagemcom_78:79:c2 (44:ad:b1:78:79:c2)
Internet Protocol Version 4, Src: 192.168.1.29, Dst: 192.168.1.1
Internet Control Message Protocol
0000 44 ad b1 78 79 c2 b0 e5 f9 ed dc cd 08 00 45 00 D··xy··· ·····E·
0010 00 54 2d 26 00 00 40 01 ca 14 c0 a8 01 1d c0 a8 ·T-&··@· ····
0020 01 01 08 00 8c 6c 63 65 00 00 62 2d 09 72 00 0b ·····lce ··b-·r··
0030 b1 80 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 ····· ····
0040 16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25 ····· ·· !"#$%
0050 26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35 &'()*+,- ./012345
0060 36 37 67
Frame (frame), 98 bytes
Packets: 690 · Displayed: 58 (8.4%) · Dropped: 0 (0.0%)
Profile: Default

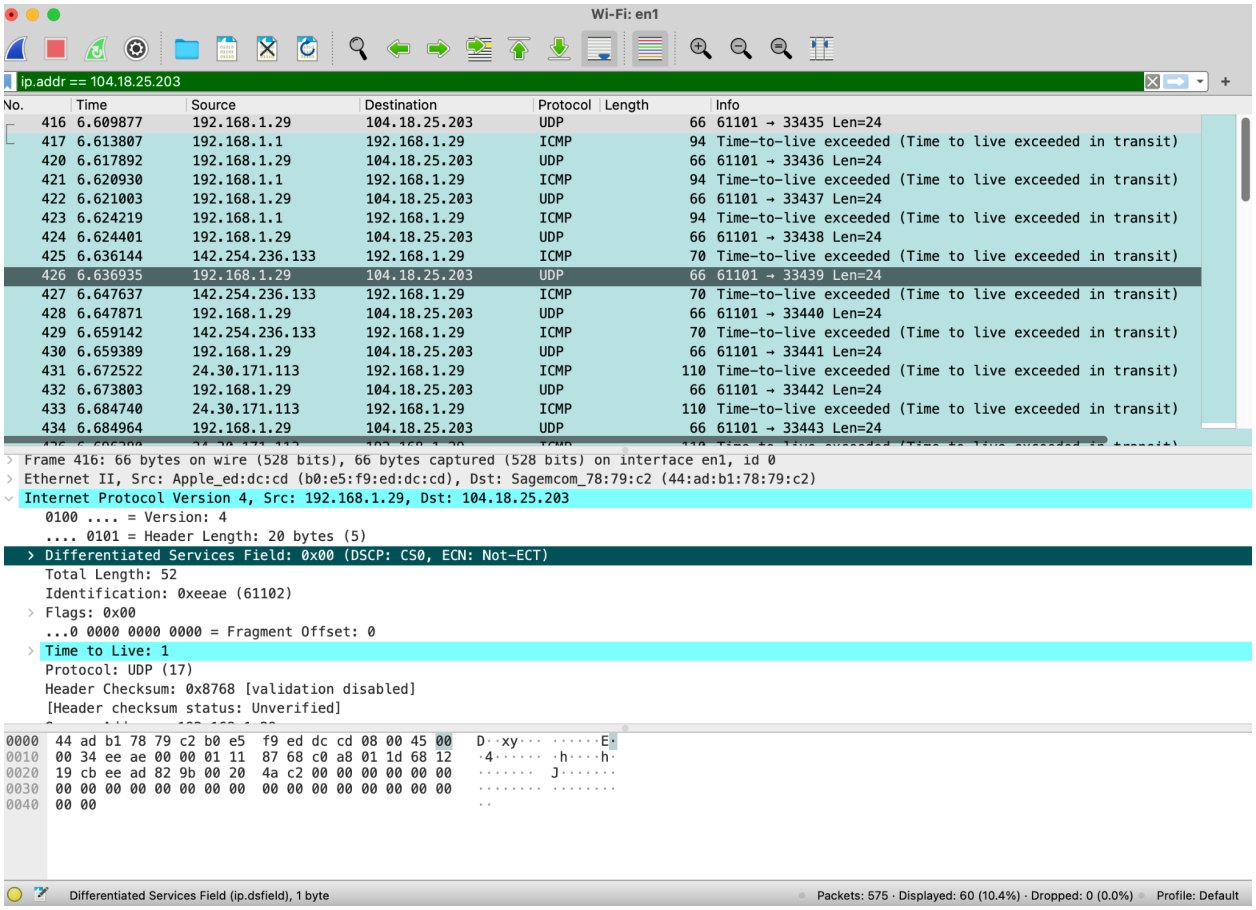


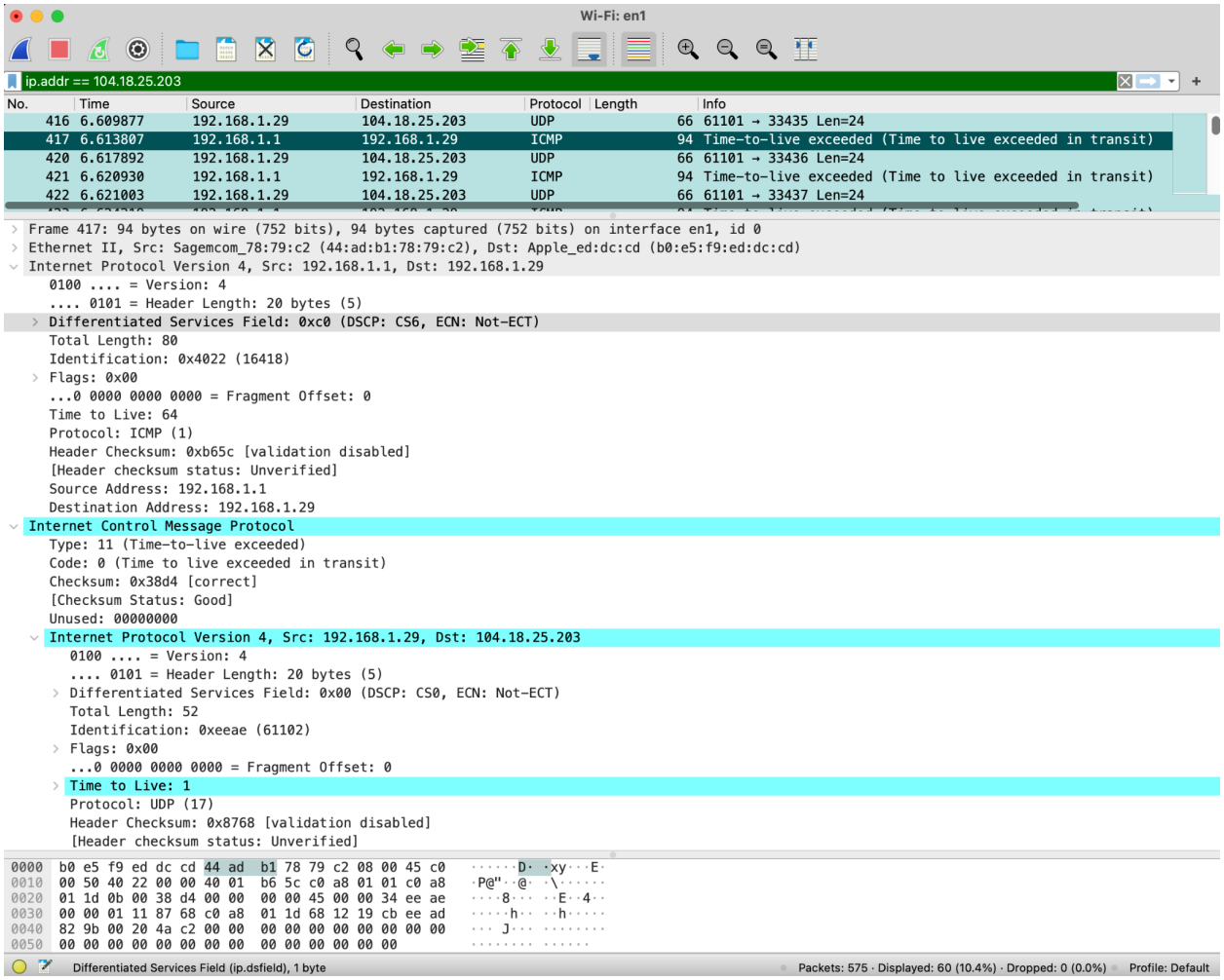
4. (1.5 pts) On your Windows computer, capture and decode packets generated by a tracert command from your computer to www.calstatela.edu.

a. How does the tracert command running on the Windows client computer modify the value in the TTL field to cause the routers to reply with ICMP messages?

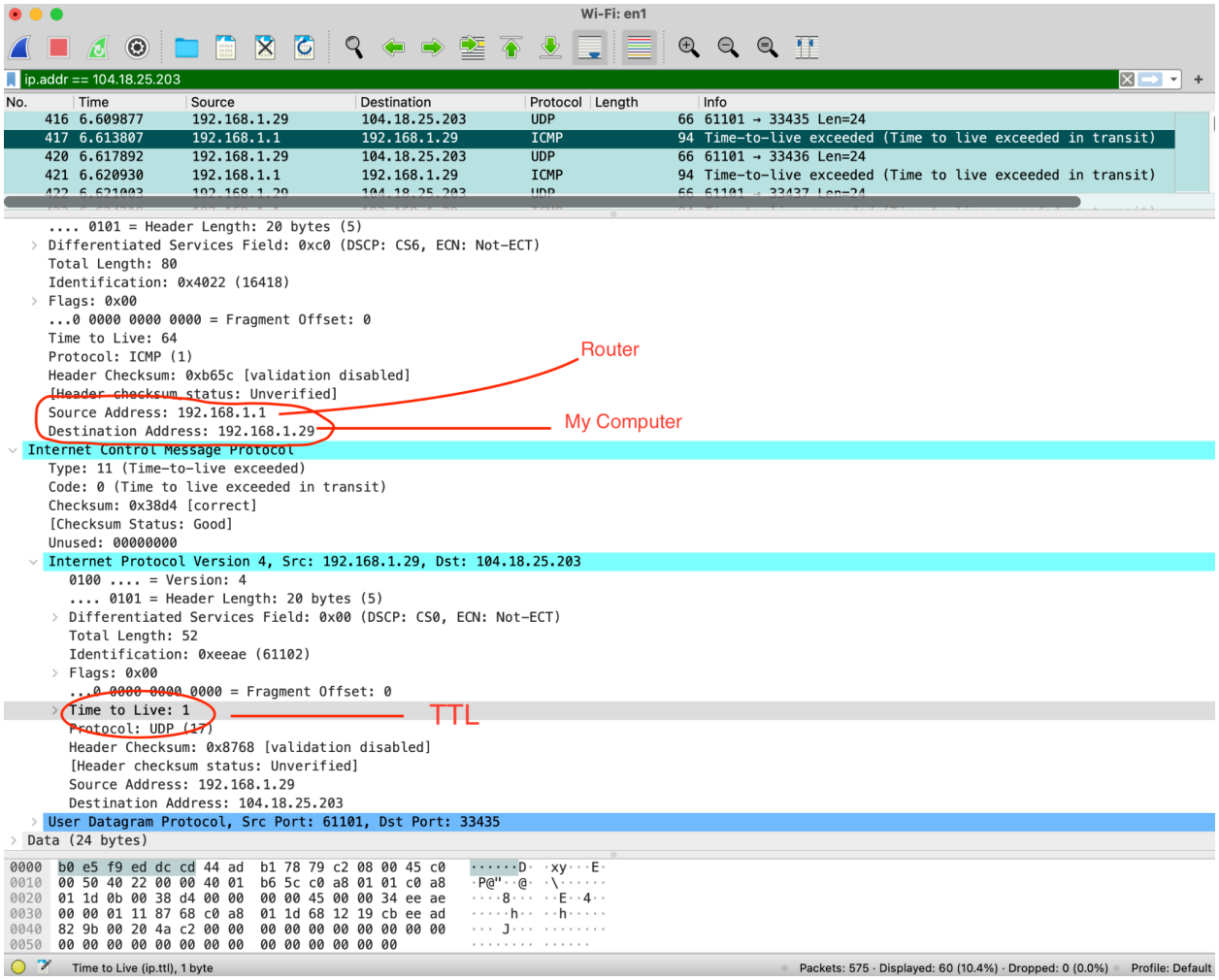
It modifies the value (TTL = 1) in the TTL field to reply with a message that it has exceeded the time to live between the two its destination from its source. When the packet reaches its time to live the router replies back with a message that it has exceeded its time to live.

b. Provide screenshots of decoded packets to support your answer in 4a.

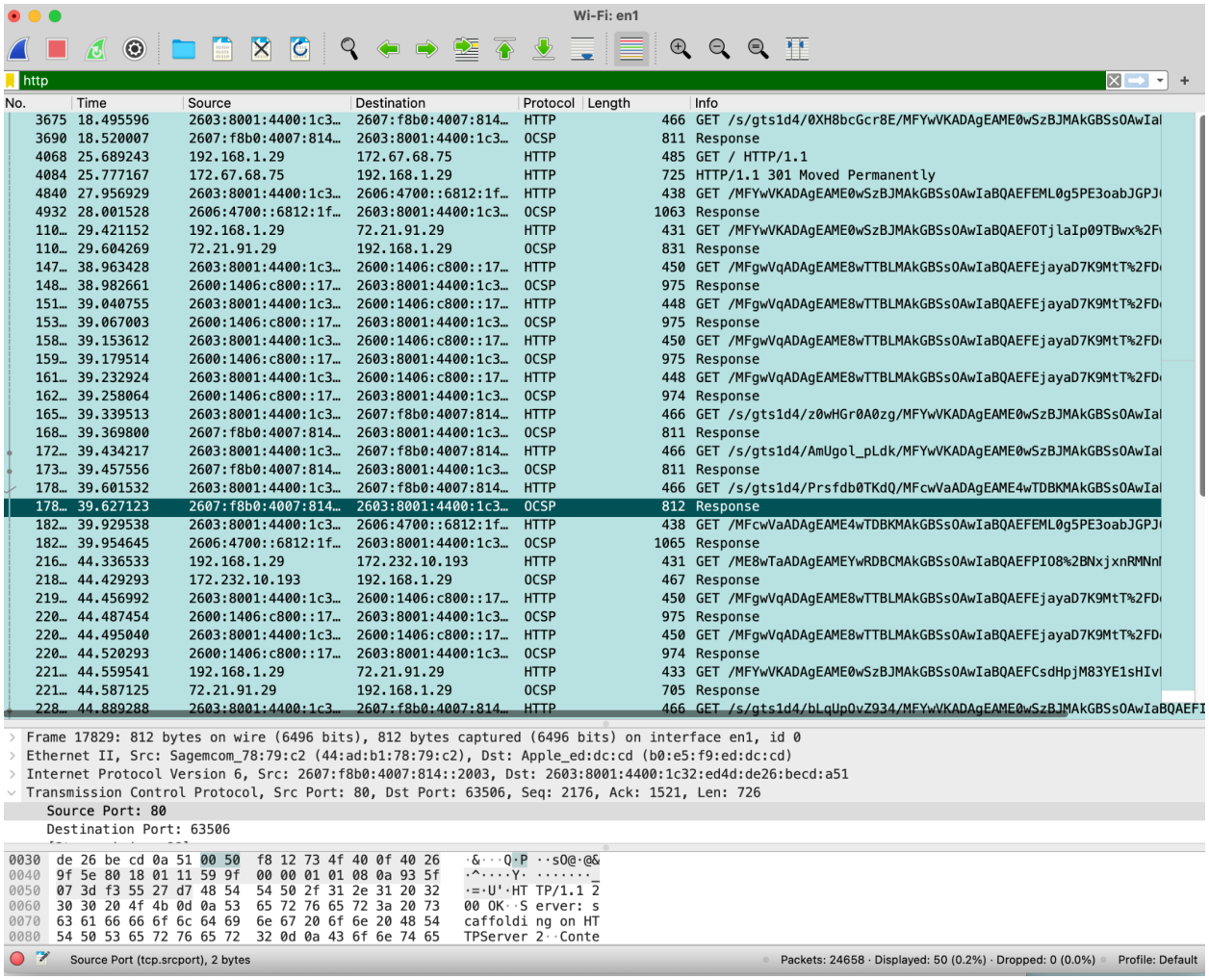

Wi-Fi: en1
ip.addr == 104.18.25.203
No. Time Source Destination Protocol Length Info
416 6.609877 192.168.1.29 104.18.25.203 UDP 66 61101 → 33435 Len=24
417 6.613807 192.168.1.1 192.168.1.29 ICMP 94 Time-to-live exceeded (Time to live exceeded in transit)
420 6.617892 192.168.1.29 104.18.25.203 UDP 66 61101 → 33436 Len=24
421 6.620930 192.168.1.1 192.168.1.29 ICMP 94 Time-to-live exceeded (Time to live exceeded in transit)
422 6.621003 192.168.1.29 104.18.25.203 UDP 66 61101 → 33437 Len=24
423 6.624219 192.168.1.1 192.168.1.29 ICMP 94 Time-to-live exceeded (Time to live exceeded in transit)
424 6.624401 192.168.1.29 104.18.25.203 UDP 66 61101 → 33438 Len=24
425 6.636144 142.254.236.133 192.168.1.29 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
426 6.636935 192.168.1.29 104.18.25.203 UDP 66 61101 → 33439 Len=24
427 6.647637 142.254.236.133 192.168.1.29 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
428 6.647871 192.168.1.29 104.18.25.203 UDP 66 61101 → 33440 Len=24
429 6.659142 142.254.236.133 192.168.1.29 ICMP 70 Time-to-live exceeded (Time to live exceeded in transit)
430 6.659389 192.168.1.29 104.18.25.203 UDP 66 61101 → 33441 Len=24
431 6.672522 24.30.171.113 192.168.1.29 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
432 6.673803 192.168.1.29 104.18.25.203 UDP 66 61101 → 33442 Len=24
433 6.684740 24.30.171.113 192.168.1.29 ICMP 110 Time-to-live exceeded (Time to live exceeded in transit)
434 6.684964 192.168.1.29 104.18.25.203 UDP 66 61101 → 33443 Len=24
Frame 416: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface en1, id 0
Ethernet II, Src: Apple_ed:dc:cd (b0:e5:f9:ed:dc:cd), Dst: Sagemcom_78:79:c2 (44:ad:b1:78:79:c2)
Internet Protocol Version 4, Src: 192.168.1.29, Dst: 104.18.25.203
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 52
Identification: 0xeeae (61102)
Flags: 0x00
...0 0000 0000 0000 = Fragment Offset: 0
Time to Live: 1
Protocol: UDP (17)
Header Checksum: 0x8768 [validation disabled]
[Header checksum status: Unverified]
0000 44 ad b1 78 79 c2 b0 e5 f9 ed dc cd 08 00 45 00
0010 00 34 ee ae 00 00 01 11 87 68 c0 a8 01 1d 68 12
0020 19 cb ee ad 82 9b 00 20 4a c2 00 00 00 00 00 00
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040 00 00
Differentiated Services Field (ip.dsfield), 1 byte
Packets: 575 · Displayed: 60 (10.4%) · Dropped: 0 (0.0%)
Profile: Default



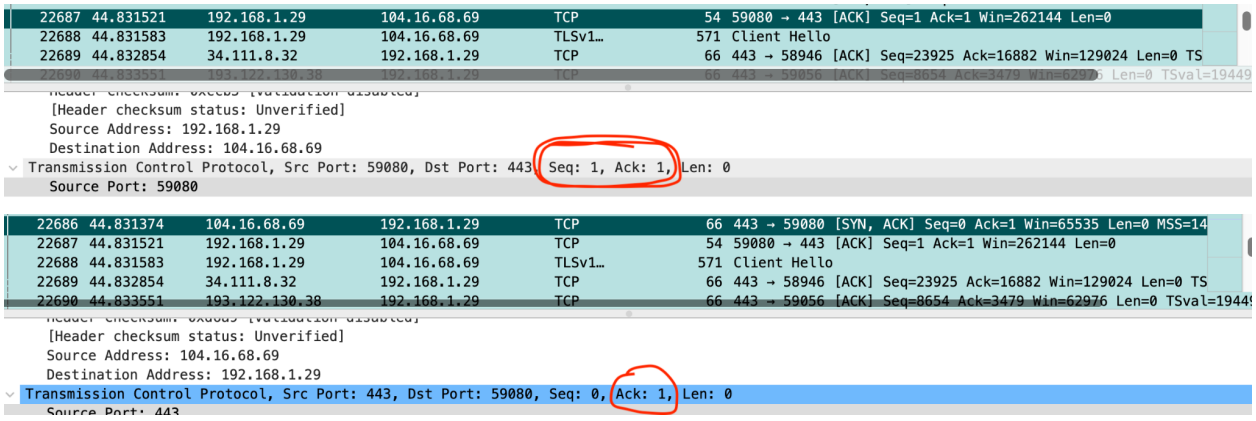
c. Turn in a screenshot which shows a decoded ICMP TTL exceeded packet that was generated and sent back from a router to your computer.

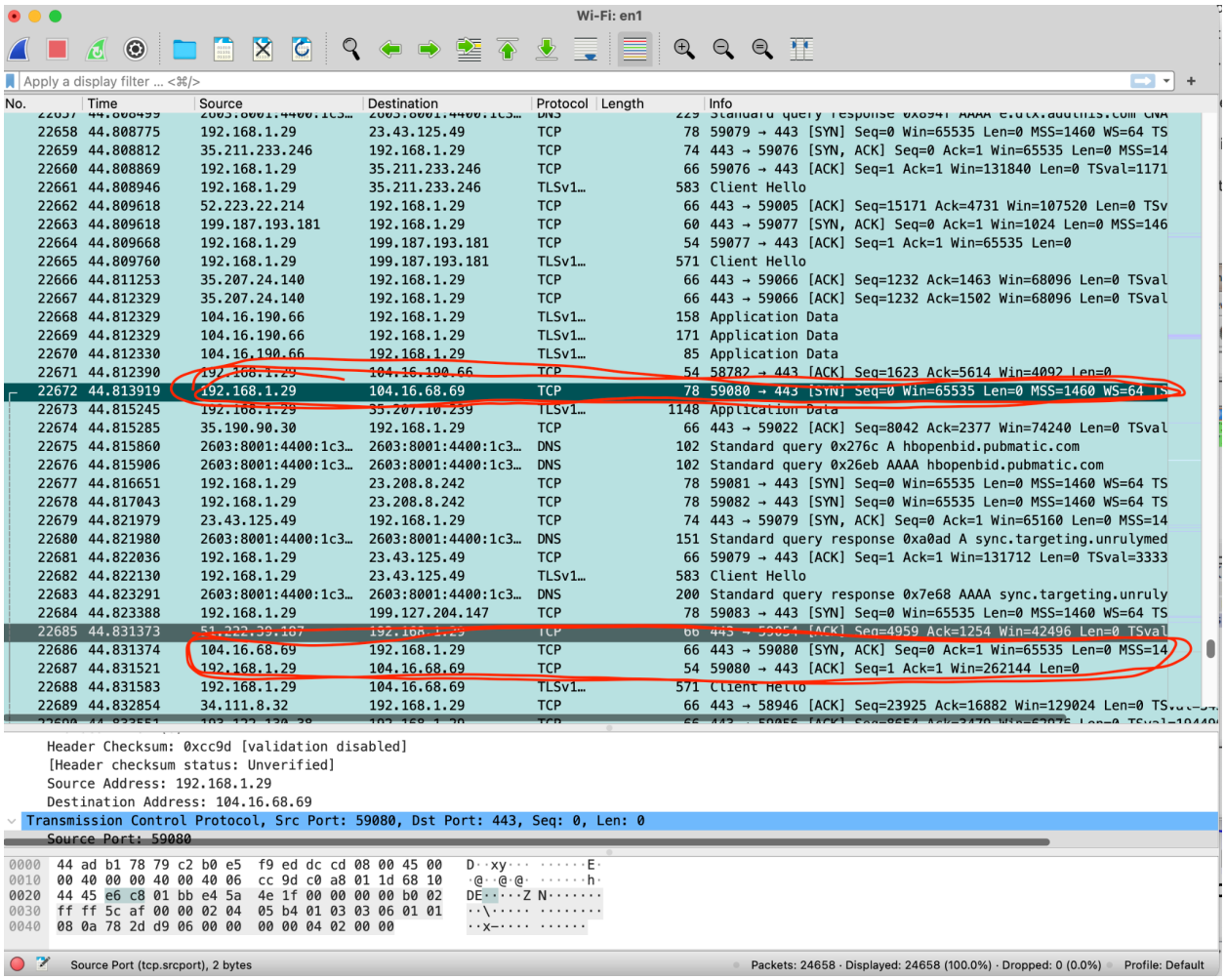


5. (2pts) Capture and decode packets associated with an entire http session. Provide screenshots to support your answers.

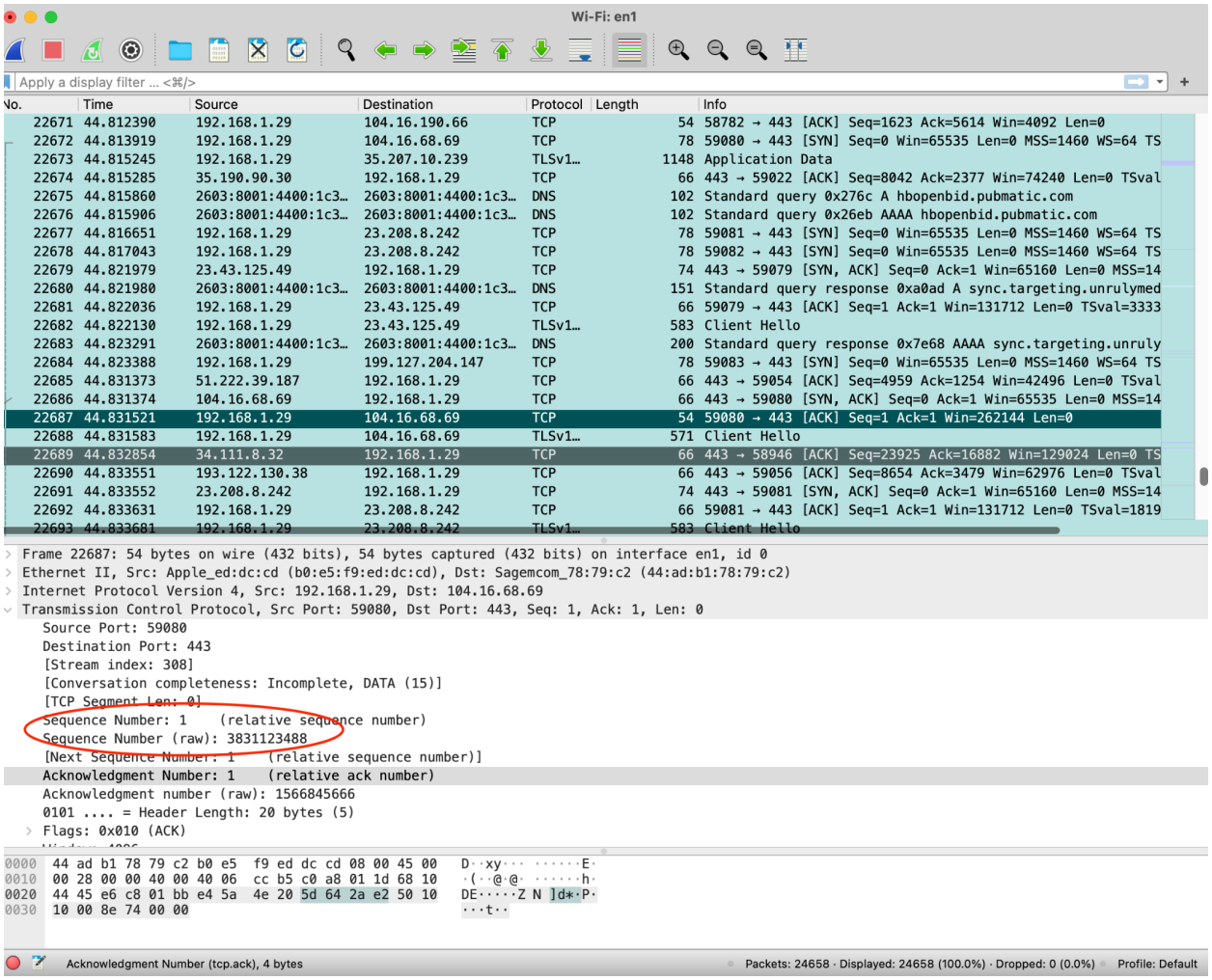


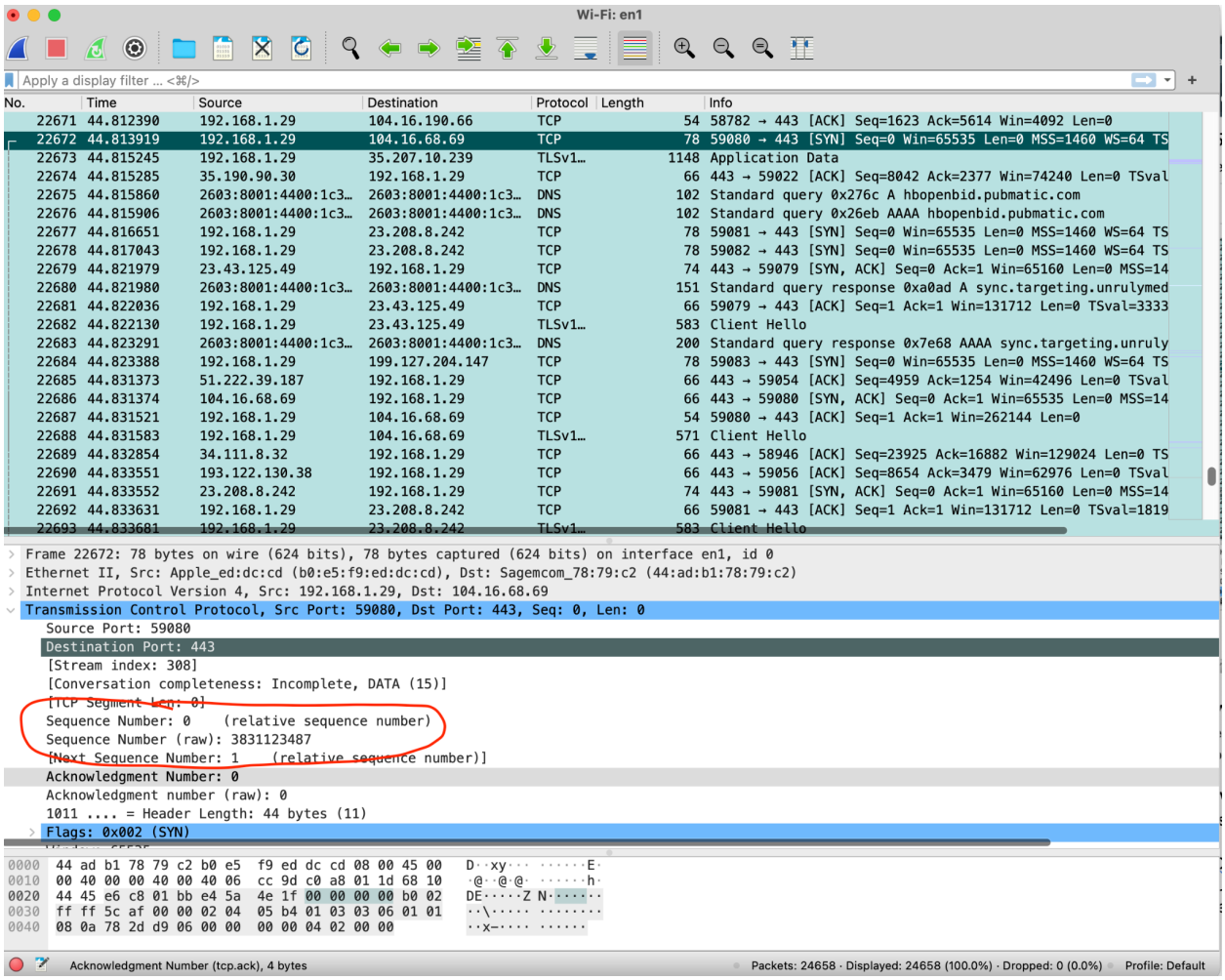
a. Circle and Identify the packets on a screenshot that comprise the 3-way handshake used during startup of the TCP connection. What TCP flags were set to 1 during the initial 3-way handshake?





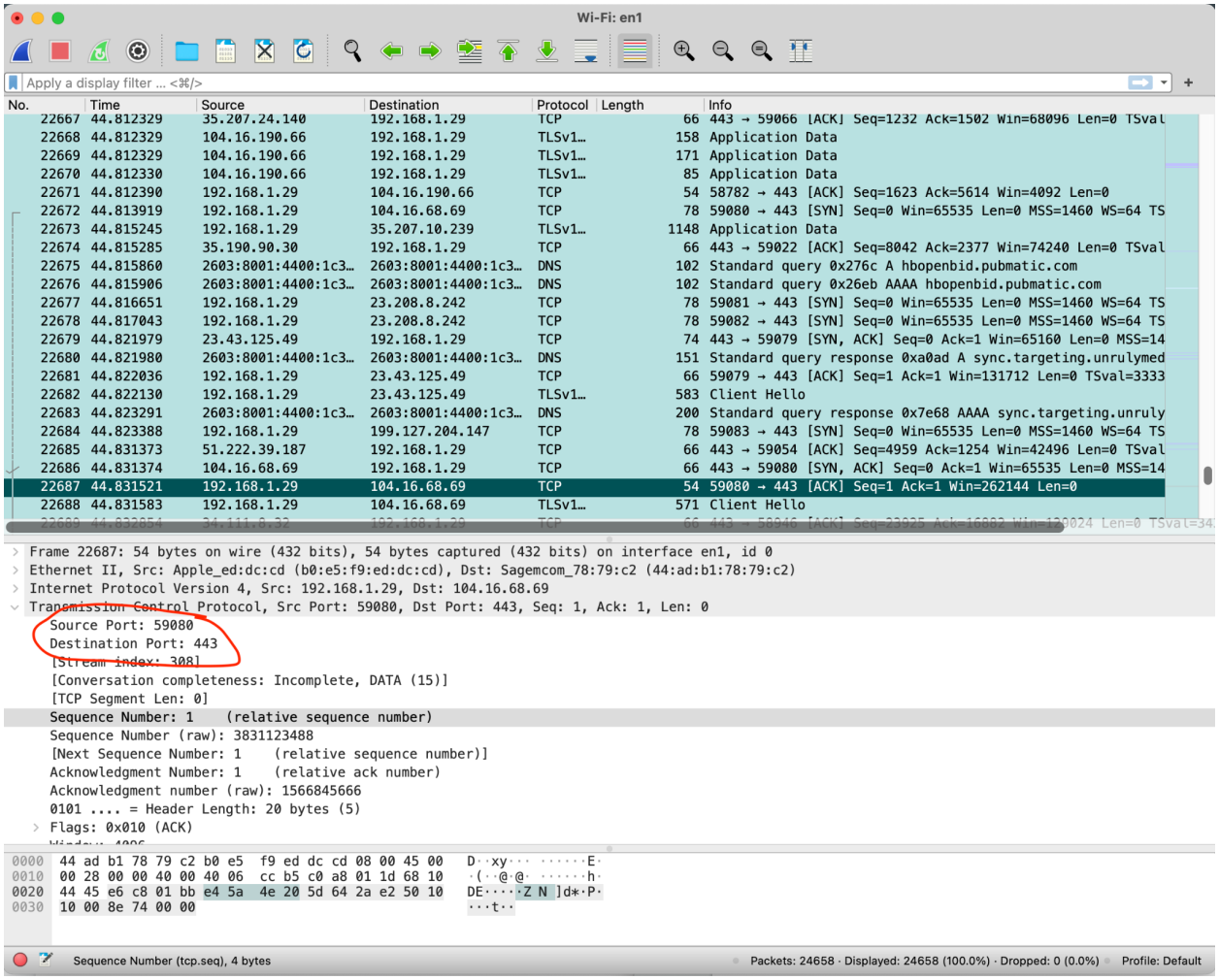
b. What were the absolute(raw) and relative values of the initial sequence numbers used by the http client and server? Submit screenshots with these values circled. There should be a total of 4 values circled.

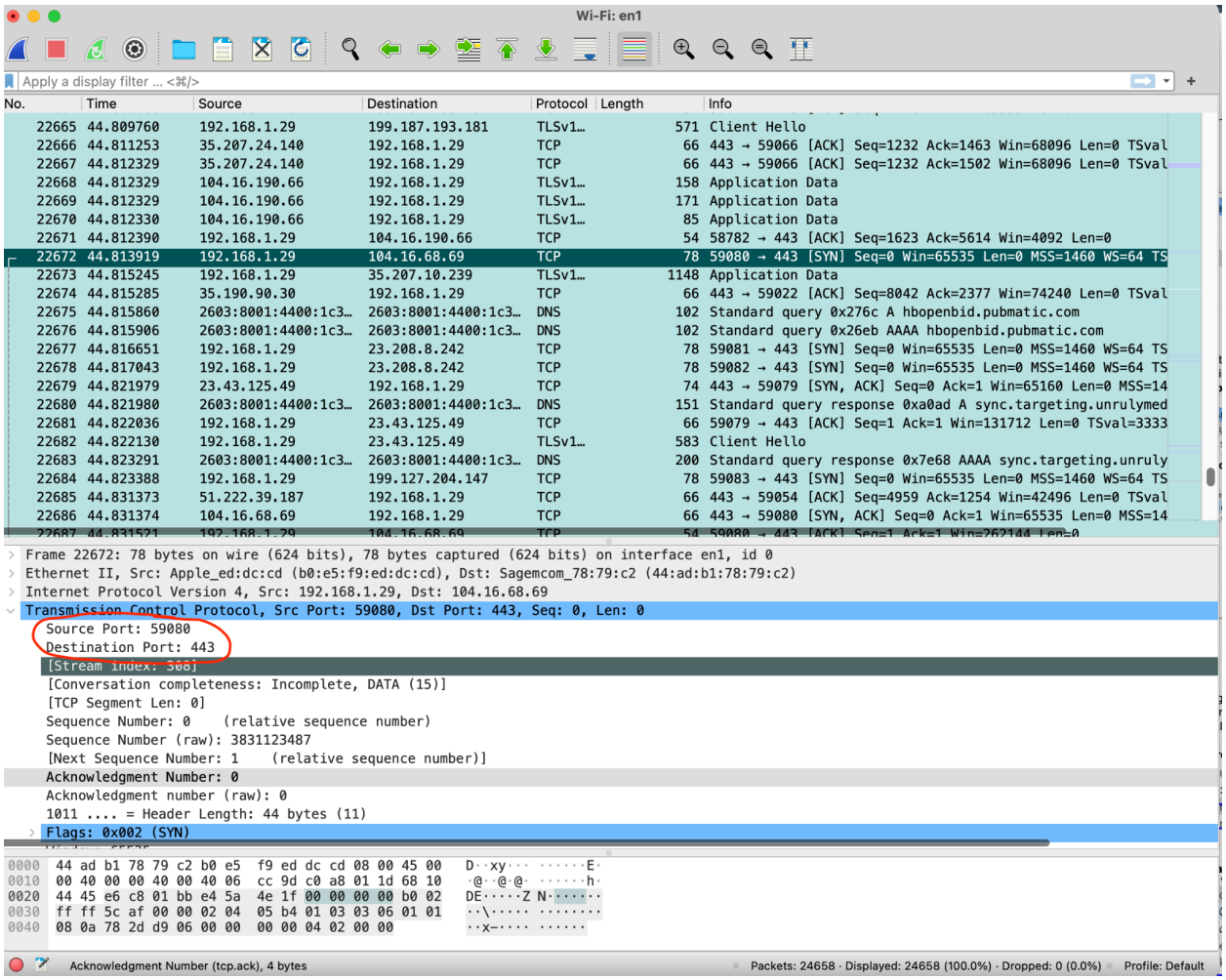

Wi-Fi: en1
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
22671 44.812390 192.168.1.29 104.16.190.66 TCP 54 58782 → 443 [ACK] Seq=1623 Ack=5614 Win=4092 Len=0
22672 44.813919 192.168.1.29 104.16.68.69 TCP 78 59080 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22673 44.815245 192.168.1.29 35.207.10.239 TLSv1… 1148 Application Data
22674 44.815285 35.190.90.30 192.168.1.29 TCP 66 443 → 59022 [ACK] Seq=8042 Ack=2377 Win=74240 Len=0 TSval
22675 44.815860 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 102 Standard query 0x276c A hbopenbid.pubmatic.com
22676 44.815906 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 102 Standard query 0x26eb AAAA hbopenbid.pubmatic.com
22677 44.816651 192.168.1.29 23.208.8.242 TCP 78 59081 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22678 44.817043 192.168.1.29 23.208.8.242 TCP 78 59082 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22679 44.821979 23.43.125.49 192.168.1.29 TCP 74 443 → 59079 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=14
22680 44.821980 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 151 Standard query response 0xa0ad A sync.targeting.unrulymed
22681 44.822036 192.168.1.29 23.43.125.49 TCP 66 59079 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=3333
22682 44.822130 192.168.1.29 23.43.125.49 TLSv1… 583 Client Hello
22683 44.823291 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 200 Standard query response 0x7e68 AAAA sync.targeting.unruly
22684 44.823388 192.168.1.29 199.127.204.147 TCP 78 59083 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22685 44.831373 51.222.39.187 192.168.1.29 TCP 66 443 → 59054 [ACK] Seq=4959 Ack=1254 Win=42496 Len=0 TSval
22686 44.831374 104.16.68.69 192.168.1.29 TCP 66 443 → 59080 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
22687 44.831521 192.168.1.29 104.16.68.69 TCP 54 59080 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
22688 44.831583 192.168.1.29 104.16.68.69 TLSv1… 571 Client Hello
22689 44.832854 34.111.8.32 192.168.1.29 TCP 66 443 → 58946 [ACK] Seq=23925 Ack=16882 Win=129024 Len=0 TS
22690 44.833551 193.122.130.38 192.168.1.29 TCP 66 443 → 59056 [ACK] Seq=8654 Ack=3479 Win=62976 Len=0 TSval
22691 44.833552 23.208.8.242 192.168.1.29 TCP 74 443 → 59081 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=14
22692 44.833631 192.168.1.29 23.208.8.242 TCP 66 59081 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=1819
22693 44.833681 192.168.1.29 23.208.8.242 TLSv1… 583 Client Hello
Frame 22687: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en1, id 0
Ethernet II, Src: Apple_ed:dc:cd (b0:e5:f9:ed:dc:cd), Dst: Sagemcom_78:79:c2 (44:ad:b1:78:79:c2)
Internet Protocol Version 4, Src: 192.168.1.29, Dst: 104.16.68.69
Transmission Control Protocol, Src Port: 59080, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
Source Port: 59080
Destination Port: 443
[Stream index: 308]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3831123488
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1566845666
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
0000 44 ad b1 78 79 c2 b0 e5 f9 ed dc cd 08 00 45 00 D··xy··· ·····E·
0010 00 28 00 00 40 00 40 06 cc b5 c0 a8 01 1d 68 10 ·(··@·@· ·····h·
0020 44 45 e6 c8 01 bb e4 5a 4e 20 5d 64 2a e2 50 10 DE·····Z N]d*·P·
0030 10 00 8e 74 00 00 ···t··
Acknowledgment Number (tcp.ack), 4 bytes
Packets: 24658 · Displayed: 24658 (100.0%) · Dropped: 0 (0.0%)
Profile: Default



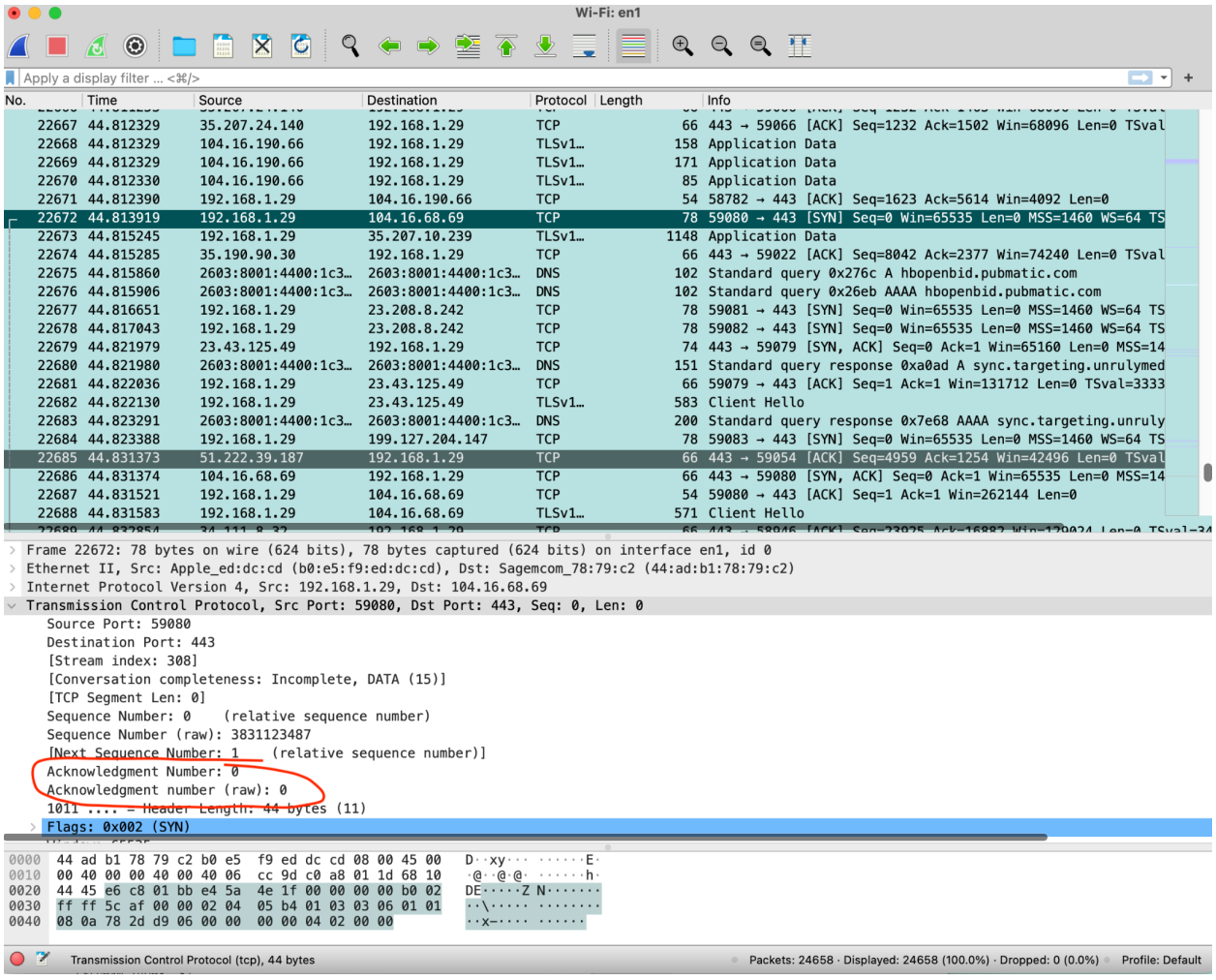
c. What tcp port numbers did the web client and server use? Submit screenshot with these two values circled.

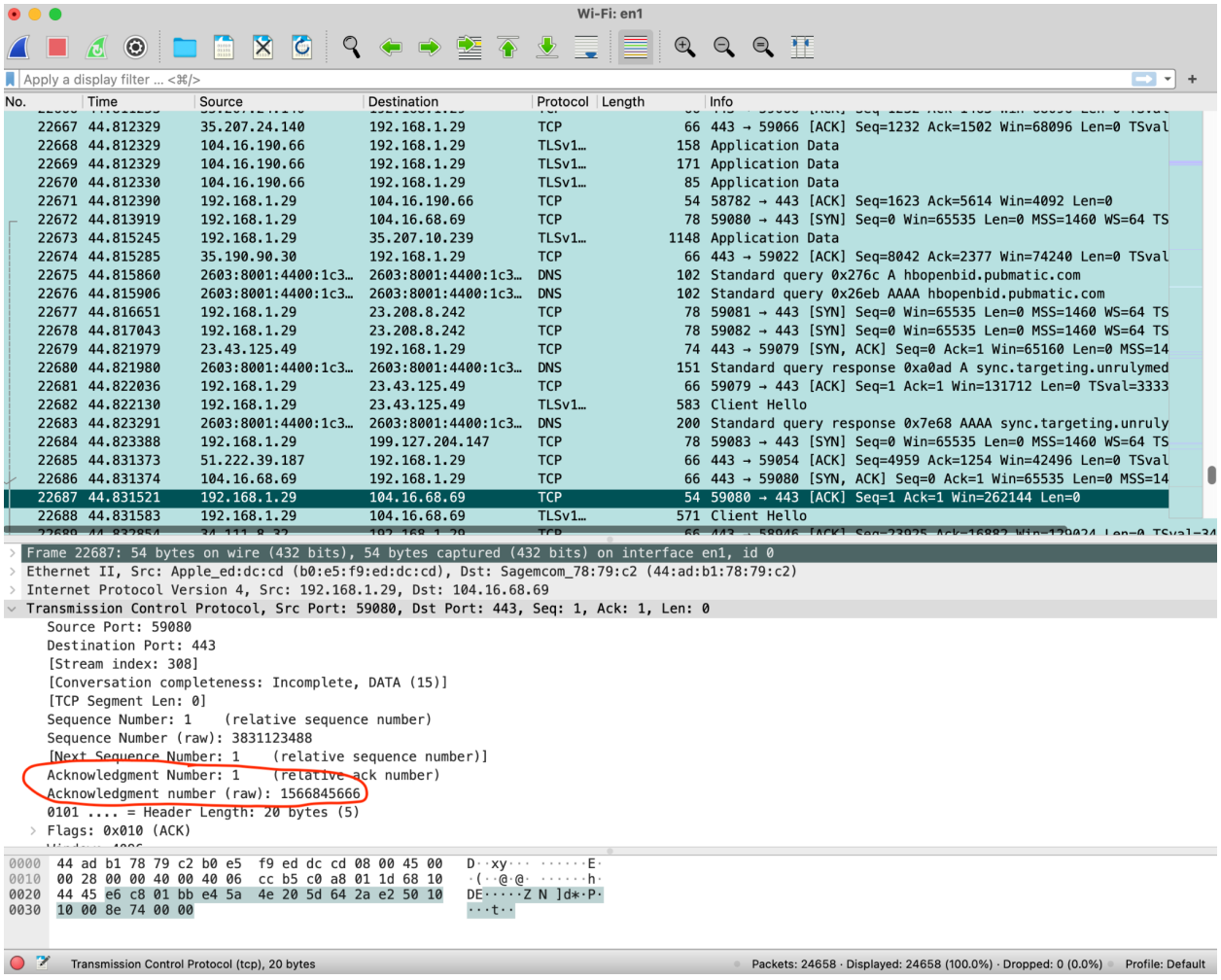
First image is from the client side and the second image is from the server side telling by their sequence numbers.


Wi-Fi: en1
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
22667 44.812329 35.207.24.140 192.168.1.29 TCP 66 443 → 59066 [ACK] Seq=1232 Ack=1502 Win=68096 Len=0 TSval
22668 44.812329 104.16.190.66 192.168.1.29 TLSv1… 158 Application Data
22669 44.812329 104.16.190.66 192.168.1.29 TLSv1… 171 Application Data
22670 44.812330 104.16.190.66 192.168.1.29 TLSv1… 85 Application Data
22671 44.812390 192.168.1.29 104.16.190.66 TCP 54 58782 → 443 [ACK] Seq=1623 Ack=5614 Win=4092 Len=0
22672 44.813919 192.168.1.29 104.16.68.69 TCP 78 59080 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22673 44.815245 192.168.1.29 35.207.10.239 TLSv1… 1148 Application Data
22674 44.815285 35.190.90.30 192.168.1.29 TCP 66 443 → 59022 [ACK] Seq=8042 Ack=2377 Win=74240 Len=0 TSval
22675 44.815860 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 102 Standard query 0x276c A hbopenbid.pubmatic.com
22676 44.815906 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 102 Standard query 0x26eb AAAA hbopenbid.pubmatic.com
22677 44.816651 192.168.1.29 23.208.8.242 TCP 78 59081 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22678 44.817043 192.168.1.29 23.208.8.242 TCP 78 59082 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22679 44.821979 23.43.125.49 192.168.1.29 TCP 74 443 → 59079 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=14
22680 44.821980 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 151 Standard query response 0xa0ad A sync.targeting.unrulymed
22681 44.822036 192.168.1.29 23.43.125.49 TCP 66 59079 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=3333
22682 44.822130 192.168.1.29 23.43.125.49 TLSv1… 583 Client Hello
22683 44.823291 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 200 Standard query response 0x7e68 AAAA sync.targeting.unruly
22684 44.823388 192.168.1.29 199.127.204.147 TCP 78 59083 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22685 44.831373 51.222.39.187 192.168.1.29 TCP 66 443 → 59054 [ACK] Seq=4959 Ack=1254 Win=42496 Len=0 TSval
22686 44.831374 104.16.68.69 192.168.1.29 TCP 66 443 → 59080 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
22687 44.831521 192.168.1.29 104.16.68.69 TCP 54 59080 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
22688 44.831583 192.168.1.29 104.16.68.69 TLSv1… 571 Client Hello
Frame 22687: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en1, id 0
Ethernet II, Src: Apple_ed:dc:cd (b0:e5:f9:ed:dc:cd), Dst: Sagemcom_78:79:c2 (44:ad:b1:78:79:c2)
Internet Protocol Version 4, Src: 192.168.1.29, Dst: 104.16.68.69
Transmission Control Protocol, Src Port: 59080, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
Source Port: 59080
Destination Port: 443
[Stream index: 308]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3831123488
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1566845666
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
0000 44 ad b1 78 79 c2 b0 e5 f9 ed dc cd 08 00 45 00 D··xy··· ·····E·
0010 00 28 00 00 40 00 40 06 cc b5 c0 a8 01 1d 68 10 ·(··@·@· ·····h·
0020 44 45 e6 c8 01 bb e4 5a 4e 20 5d 64 2a e2 50 10 DE·····Z N]d*·P·
0030 10 00 8e 74 00 00 ···t··
Sequence Number (tcp.seq), 4 bytes
Packets: 24658 · Displayed: 24658 (100.0%) · Dropped: 0 (0.0%)
Profile: Default



d. During teardown of the TCP connection, what were the absolute(raw) and relative values of the final acknowledgement numbers sent by the http client and server? Submit screenshots with these values circled. There should be a total of 4 values circled.


Wi-Fi: en1
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
22667 44.812329 35.207.24.140 192.168.1.29 TCP 66 443 → 59066 [ACK] Seq=1232 Ack=1502 Win=68096 Len=0 TSval
22668 44.812329 104.16.190.66 192.168.1.29 TLSv1… 158 Application Data
22669 44.812329 104.16.190.66 192.168.1.29 TLSv1… 171 Application Data
22670 44.812330 104.16.190.66 192.168.1.29 TLSv1… 85 Application Data
22671 44.812390 192.168.1.29 104.16.190.66 TCP 54 58782 → 443 [ACK] Seq=1623 Ack=5614 Win=4092 Len=0
22672 44.813919 192.168.1.29 104.16.68.69 TCP 78 59080 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22673 44.815245 192.168.1.29 35.207.10.239 TLSv1… 1148 Application Data
22674 44.815285 35.190.90.30 192.168.1.29 TCP 66 443 → 59022 [ACK] Seq=8042 Ack=2377 Win=74240 Len=0 TSval
22675 44.815860 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 102 Standard query 0x276c A hbopenbid.pubmatic.com
22676 44.815906 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 102 Standard query 0x26eb AAAA hbopenbid.pubmatic.com
22677 44.816651 192.168.1.29 23.208.8.242 TCP 78 59081 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22678 44.817043 192.168.1.29 23.208.8.242 TCP 78 59082 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22679 44.821979 23.43.125.49 192.168.1.29 TCP 74 443 → 59079 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=14
22680 44.821980 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 151 Standard query response 0xa0ad A sync.targeting.unrulymed
22681 44.822036 192.168.1.29 23.43.125.49 TCP 66 59079 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=3333
22682 44.822130 192.168.1.29 23.43.125.49 TLSv1… 583 Client Hello
22683 44.823291 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 200 Standard query response 0x7e68 AAAA sync.targeting.unruly
22684 44.823388 192.168.1.29 199.127.204.147 TCP 78 59083 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22685 44.831373 51.222.39.187 192.168.1.29 TCP 66 443 → 59054 [ACK] Seq=4959 Ack=1254 Win=42496 Len=0 TSval
22686 44.831374 104.16.68.69 192.168.1.29 TCP 66 443 → 59080 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
22687 44.831521 192.168.1.29 104.16.68.69 TCP 54 59080 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
22688 44.831583 192.168.1.29 104.16.68.69 TLSv1… 571 Client Hello
Frame 22672: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface en1, id 0
Ethernet II, Src: Apple_ed:dc:cd (b0:e5:f9:ed:dc:cd), Dst: Sagemcom_78:79:c2 (44:ad:b1:78:79:c2)
Internet Protocol Version 4, Src: 192.168.1.29, Dst: 104.16.68.69
Transmission Control Protocol, Src Port: 59080, Dst Port: 443, Seq: 0, Len: 0
Source Port: 59080
Destination Port: 443
[Stream index: 308]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 3831123487
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 0
Acknowledgment number (raw): 0
1011 .... = Header Length: 44 bytes (11)
Flags: 0x002 (SYN)
0000 44 ad b1 78 79 c2 b0 e5 f9 ed dc cd 08 00 45 00
0010 00 40 00 00 40 00 40 06 cc 9d c0 a8 01 1d 68 10
0020 44 45 e6 c8 01 bb e4 5a 4e 1f 00 00 00 00 b0 02
0030 ff ff 5c af 00 00 02 04 05 b4 01 03 03 06 01 01
0040 08 0a 78 2d d9 06 00 00 00 00 04 02 00 00
Transmission Control Protocol (tcp), 44 bytes
Packets: 24658 · Displayed: 24658 (100.0%) · Dropped: 0 (0.0%)
Profile: Default


Wi-Fi: en1
Apply a display filter ... <⌘/>
No. Time Source Destination Protocol Length Info
22667 44.812329 35.207.24.140 192.168.1.29 TCP 66 443 → 59066 [ACK] Seq=1232 Ack=1502 Win=68096 Len=0 TSval
22668 44.812329 104.16.190.66 192.168.1.29 TLSv1… 158 Application Data
22669 44.812329 104.16.190.66 192.168.1.29 TLSv1… 171 Application Data
22670 44.812330 104.16.190.66 192.168.1.29 TLSv1… 85 Application Data
22671 44.812390 192.168.1.29 104.16.190.66 TCP 54 58782 → 443 [ACK] Seq=1623 Ack=5614 Win=4092 Len=0
22672 44.813919 192.168.1.29 104.16.68.69 TCP 78 59080 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22673 44.815245 192.168.1.29 35.207.10.239 TLSv1… 1148 Application Data
22674 44.815285 35.190.90.30 192.168.1.29 TCP 66 443 → 59022 [ACK] Seq=8042 Ack=2377 Win=74240 Len=0 TSval
22675 44.815860 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 102 Standard query 0x276c A hbopenbid.pubmatic.com
22676 44.815906 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 102 Standard query 0x26eb AAAA hbopenbid.pubmatic.com
22677 44.816651 192.168.1.29 23.208.8.242 TCP 78 59081 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22678 44.817043 192.168.1.29 23.208.8.242 TCP 78 59082 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22679 44.821979 23.43.125.49 192.168.1.29 TCP 74 443 → 59079 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=14
22680 44.821980 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 151 Standard query response 0xa0ad A sync.targeting.unrulymed
22681 44.822036 192.168.1.29 23.43.125.49 TCP 66 59079 → 443 [ACK] Seq=1 Ack=1 Win=131712 Len=0 TSval=3333
22682 44.822130 192.168.1.29 23.43.125.49 TLSv1… 583 Client Hello
22683 44.823291 2603:8001:4400:1c3… 2603:8001:4400:1c3… DNS 200 Standard query response 0x7e68 AAAA sync.targeting.unruly
22684 44.823388 192.168.1.29 199.127.204.147 TCP 78 59083 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=64 TS
22685 44.831373 51.222.39.187 192.168.1.29 TCP 66 443 → 59054 [ACK] Seq=4959 Ack=1254 Win=42496 Len=0 TSval
22686 44.831374 104.16.68.69 192.168.1.29 TCP 66 443 → 59080 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=14
22687 44.831521 192.168.1.29 104.16.68.69 TCP 54 59080 → 443 [ACK] Seq=1 Ack=1 Win=262144 Len=0
22688 44.831583 192.168.1.29 104.16.68.69 TLSv1… 571 Client Hello
Frame 22687: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface en1, id 0
Ethernet II, Src: Apple_ed:dc:cd (b0:e5:f9:ed:dc:cd), Dst: Sagemcom_78:79:c2 (44:ad:b1:78:79:c2)
Internet Protocol Version 4, Src: 192.168.1.29, Dst: 104.16.68.69
Transmission Control Protocol, Src Port: 59080, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
Source Port: 59080
Destination Port: 443
[Stream index: 308]
[Conversation completeness: Incomplete, DATA (15)]
[TCP Segment Len: 0]
Sequence Number: 1 (relative sequence number)
Sequence Number (raw): 3831123488
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1566845666
0101 .... = Header Length: 20 bytes (5)
Flags: 0x010 (ACK)
0000 44 ad b1 78 79 c2 b0 e5 f9 ed dc cd 08 00 45 00
0010 00 28 00 00 40 00 40 06 cc b5 c0 a8 01 1d 68 10
0020 44 45 e6 c8 01 bb e4 5a 4e 20 5d 64 2a e2 50 10
0030 10 00 8e 74 00 00
Transmission Control Protocol (tcp), 20 bytes
Packets: 24658 · Displayed: 24658 (100.0%) · Dropped: 0 (0.0%)
Profile: Default