Gasser Ahmed

[gasser18@vt.edu](mailto:gasser18@vt.edu)

ECE 5484, Project 4

Section 1 – Objectives:

Reinforce the understanding of the TCP/IP protocol suite by using Wireshark network protocol analyzer to examine details of TCP, UDP, and IP protocols from the TCP/IP protocol suite.

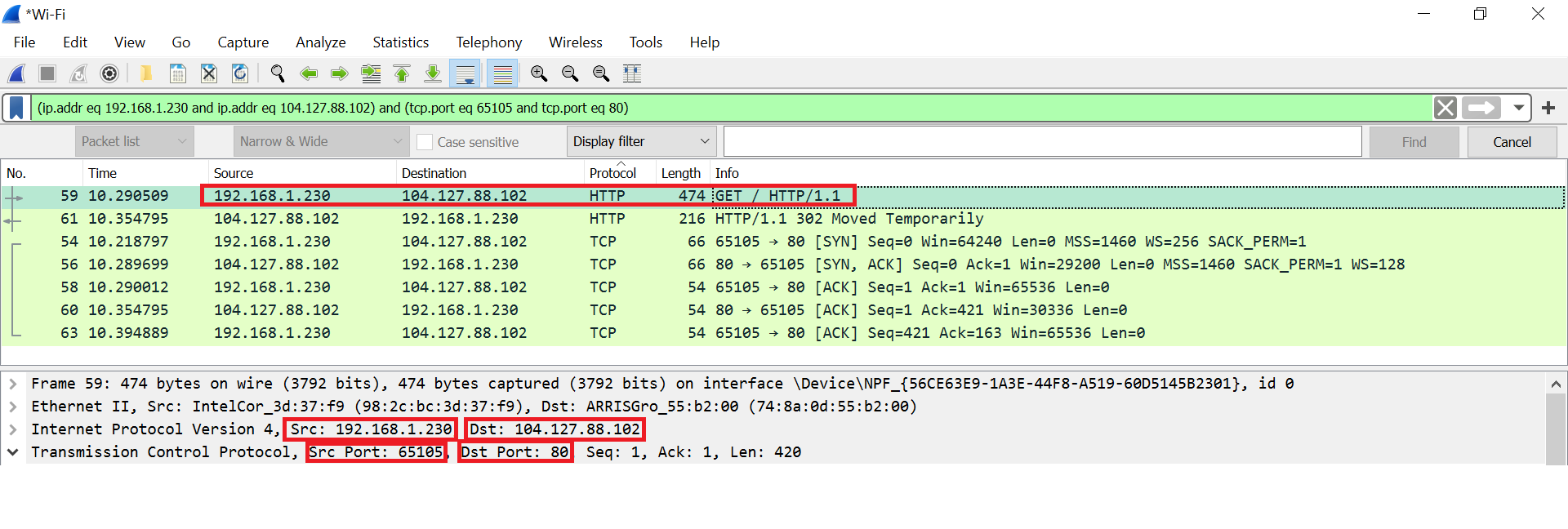
By following the steps below:

1. Capture and analyze TCP segments.
2. Capture and analyze UDP datagrams.
3. Capture and analyze IP datagrams.

Section 2 – Questions:

2.1. TCP:

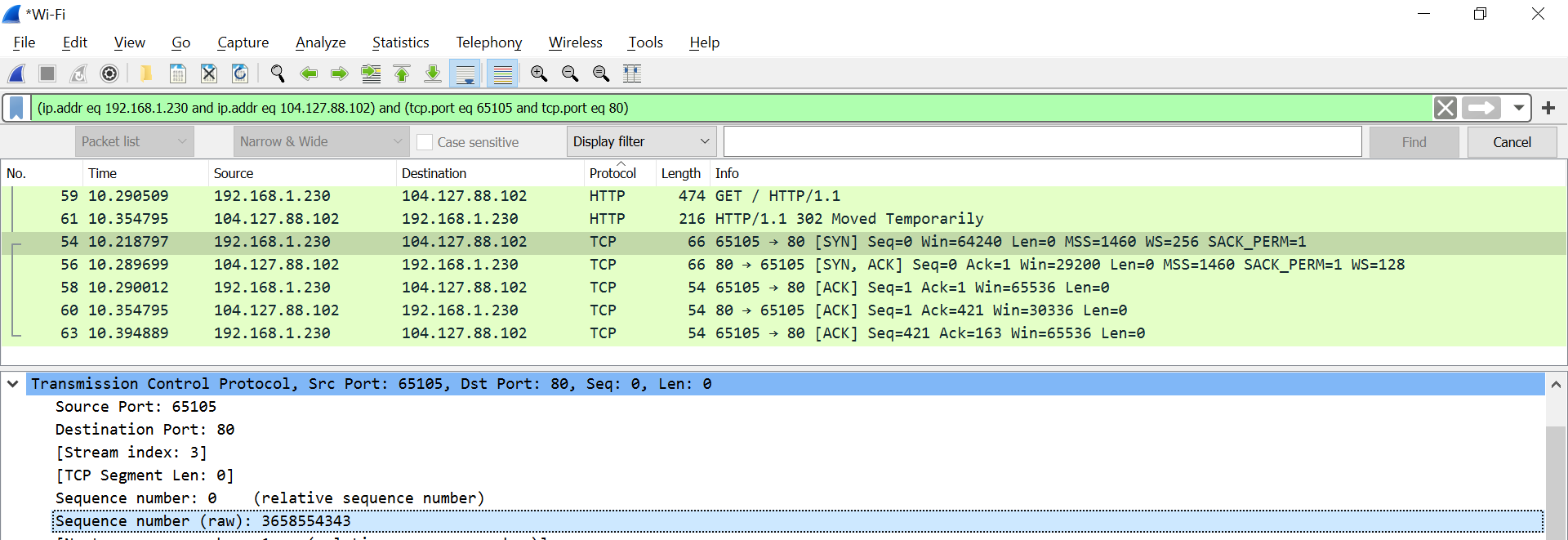
1. What is the IP address of the client? 192.168.1.230
2. What is the port number used on the client for the TCP session with the server? 65105
3. What is the IP address of the server? 104.127.88.102
4. What is the port number used by the server for the TCP session with the client? 80



1. What is the sequence number of the TCP SYN segment that is used to initiate the TCP connection between the client computer and the server?

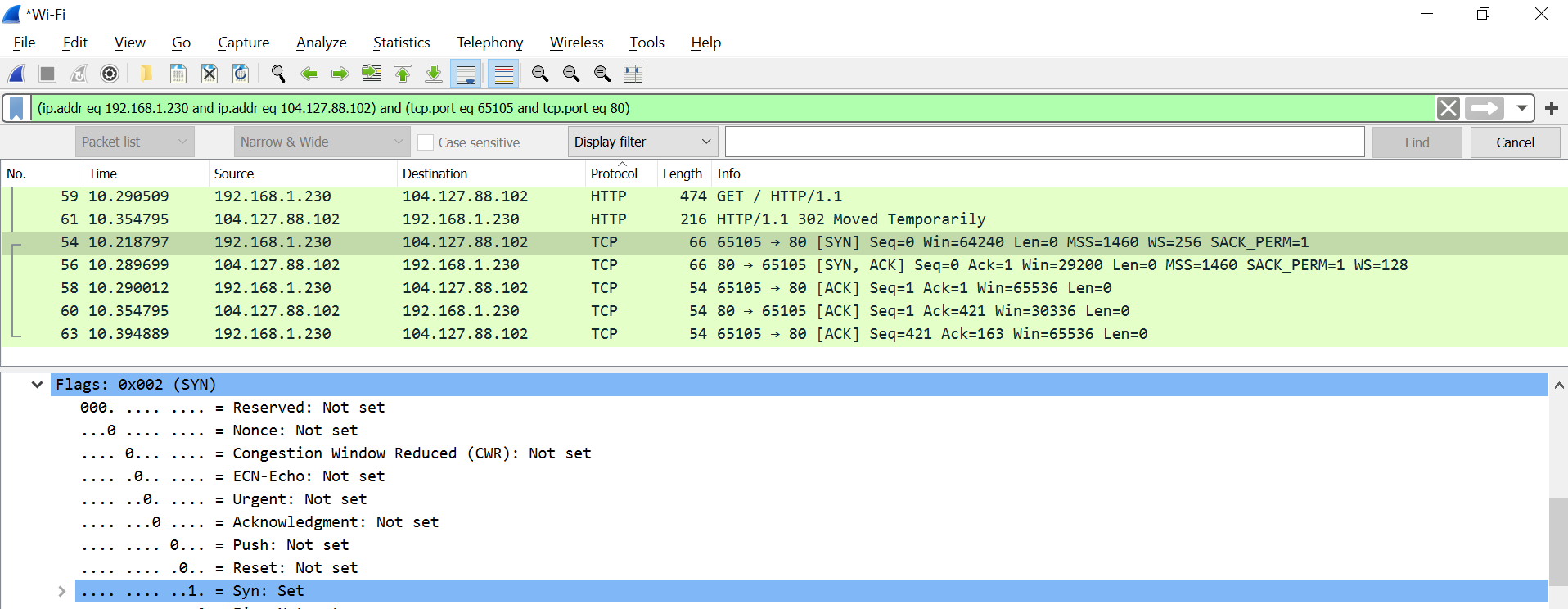
Absolute (raw) sequence number: 3658554343

Relative sequence number: 0



1. What field and value in that field in the TCP segment identifies the segment as a SYN segment?

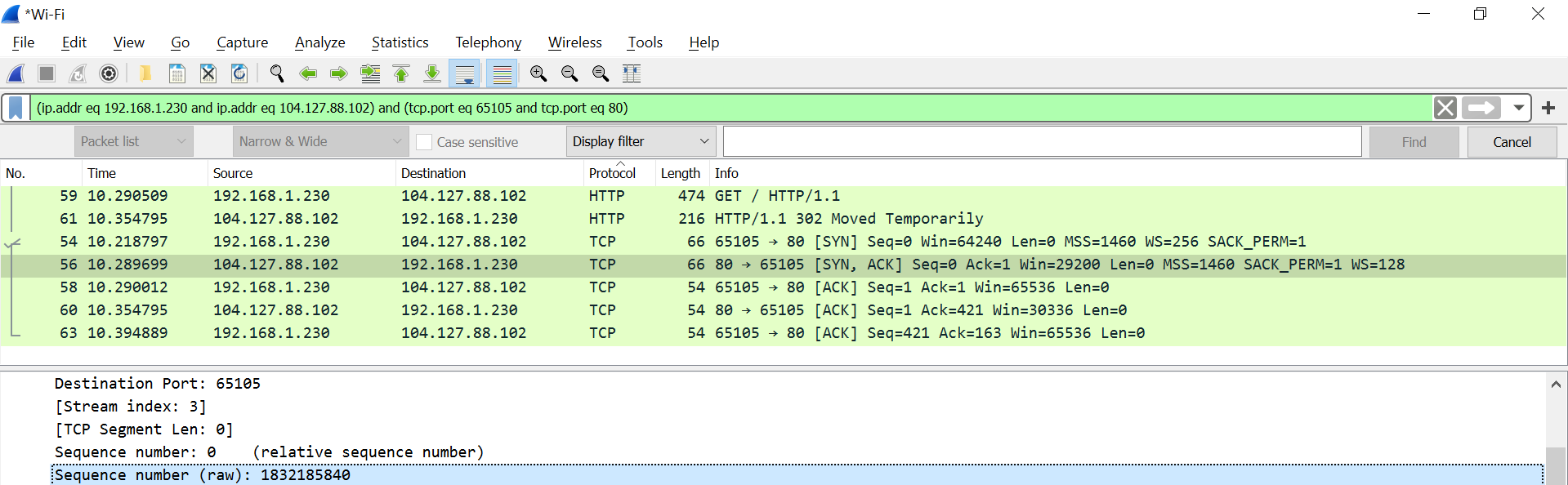
Field: Syn (tcp.flags.syn) , value: Set (1) (under Flags)



1. What is the sequence number of the SYN/ACK segment sent by the server to the client in reply to the SYN from the client?

Absolute (raw) sequence number: 1832185840

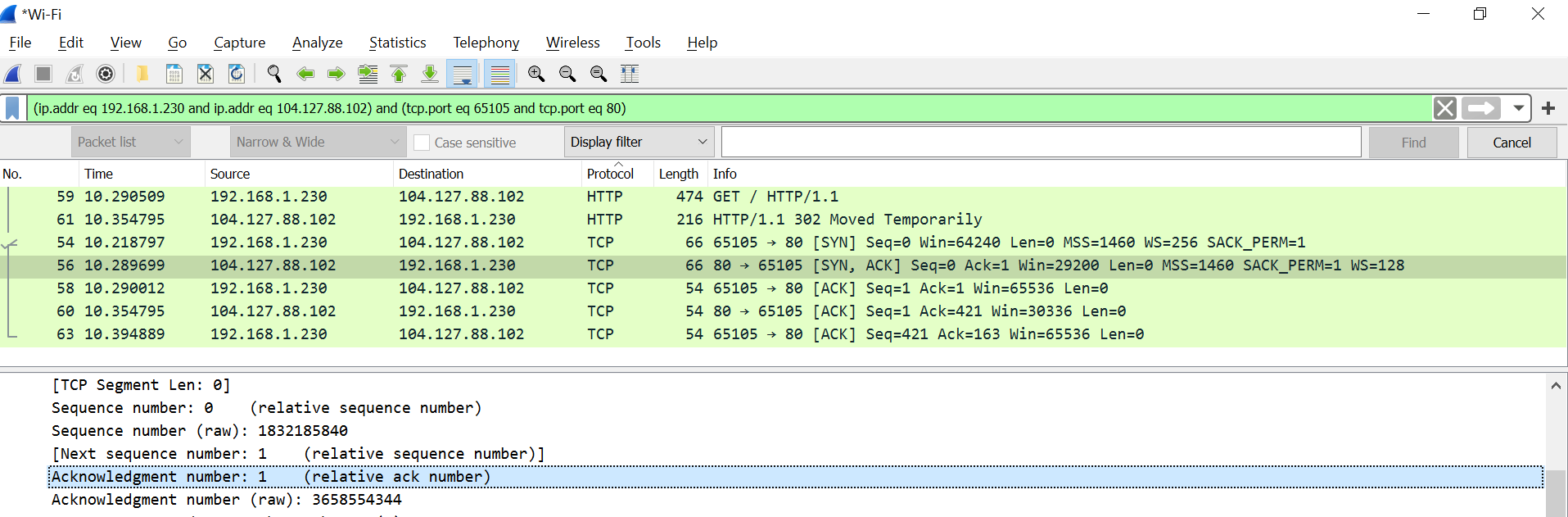
Relative sequence number: 0



1. What is the value of the acknowledgement number in the SYN/ACK segment sent by the server to the client?

Absolute (raw) ack number: 3658554344

Relative ack number: 1



1. What does this acknowledgment number indicate?

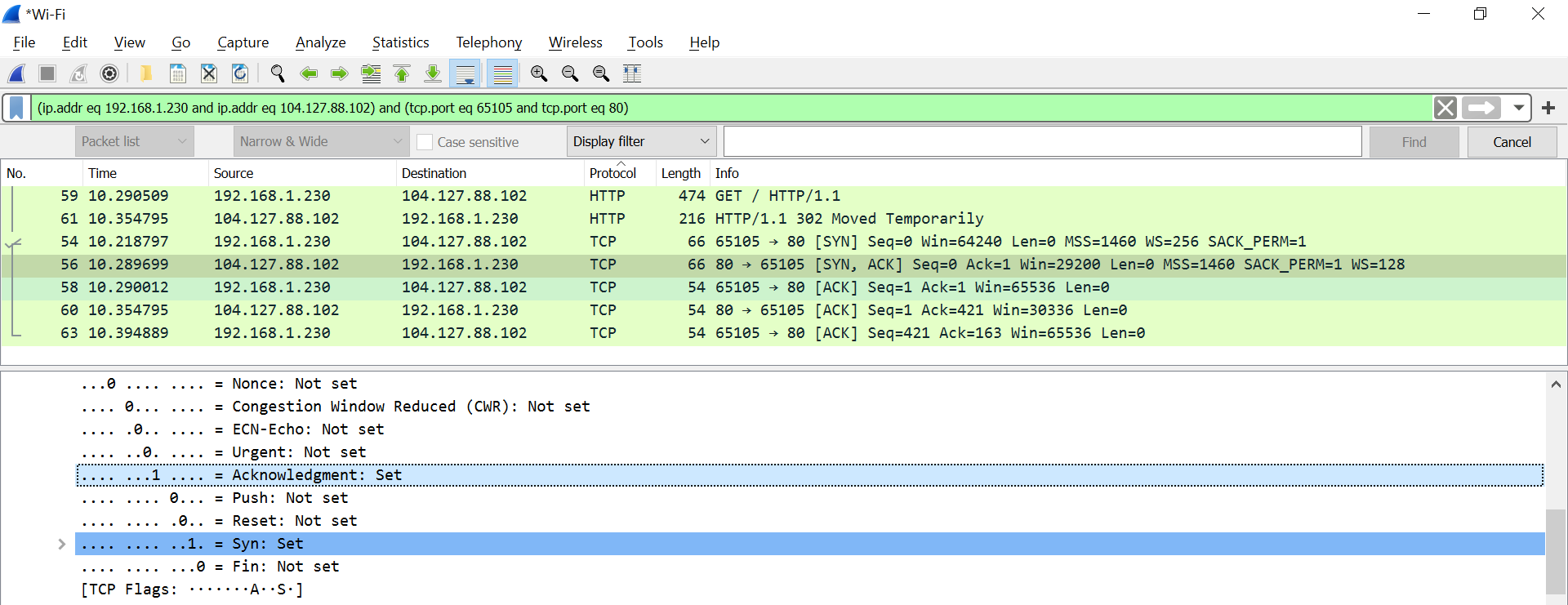
The acknowledgement number is set to 1 to indicate the receipt of the client's SYN flag in packet #1. It also indicates that the sequence number of the next byte the receiver expects to receive is 1.

1. What field in the TCP segment and value in that field identifies the segment as a SYN/ACK segment?

Under flags:

Field: Acknowledgment (tcp.flags.ack), value: Set (1)

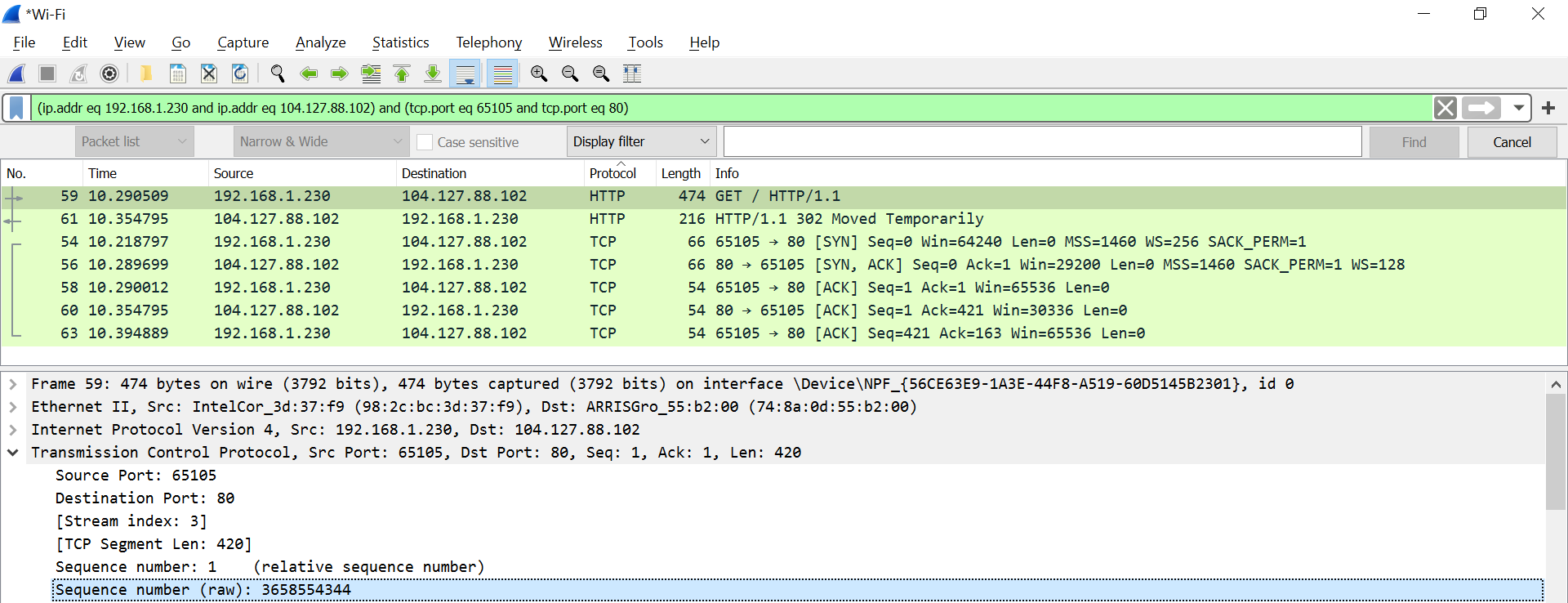
Field: Syn (tcp.flags.syn) , value: Set (1)



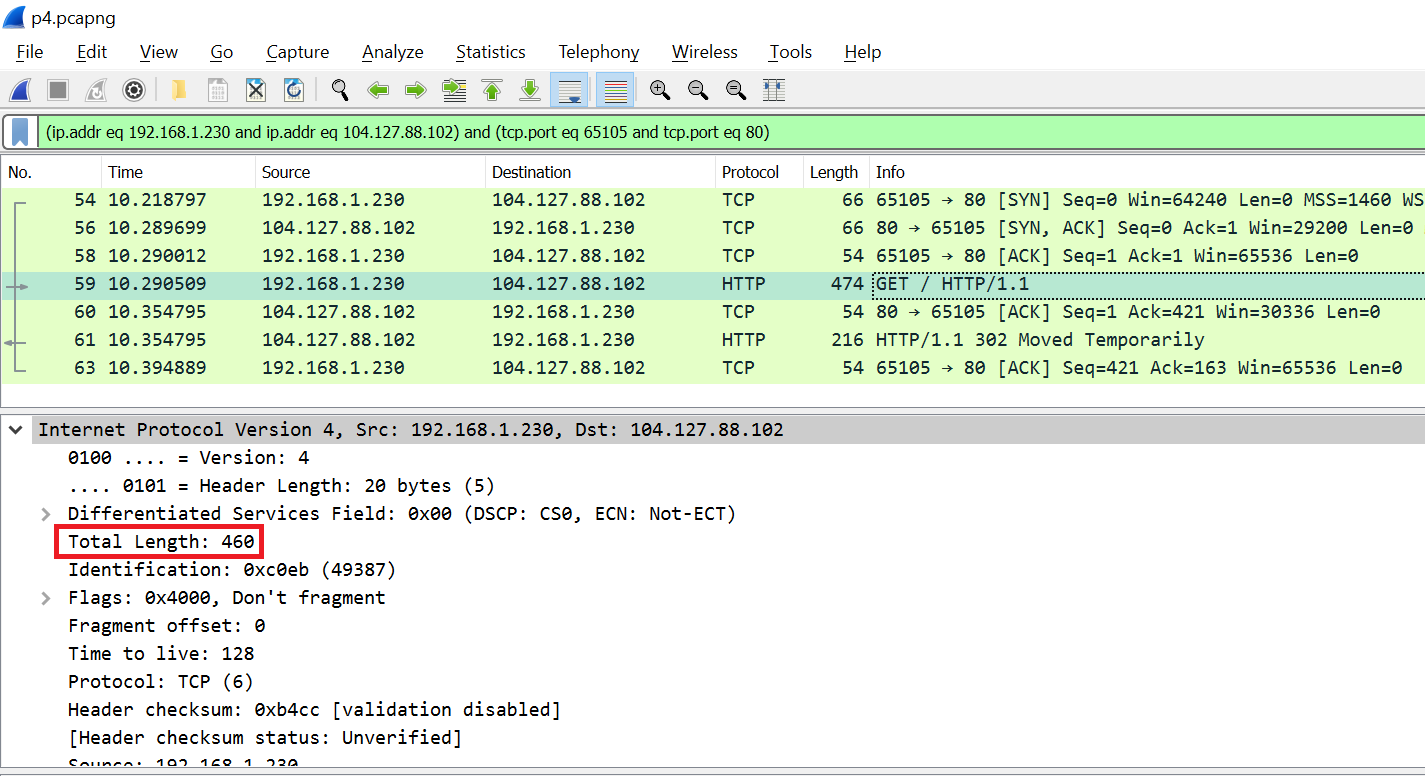
1. Locate the first GET message sent to the server. What is the sequence number of this message?

Absolute (raw) sequence number: 3658554344

Relative sequence number: 1



1. What is the total length of the HTTP request containing the GET? 460 bytes



1. Yes, the acknowledgment number agrees with what I would expect which is 421 (figure 13.a). Since the sequence number of the previous segment (figure 13.b) was 1 and its TCP segment length (TCP payload) was 420, so the acknowledgment number of the current segment should be 1 (previous seq #) + 420 (previous segment’s TCP payload) = 421

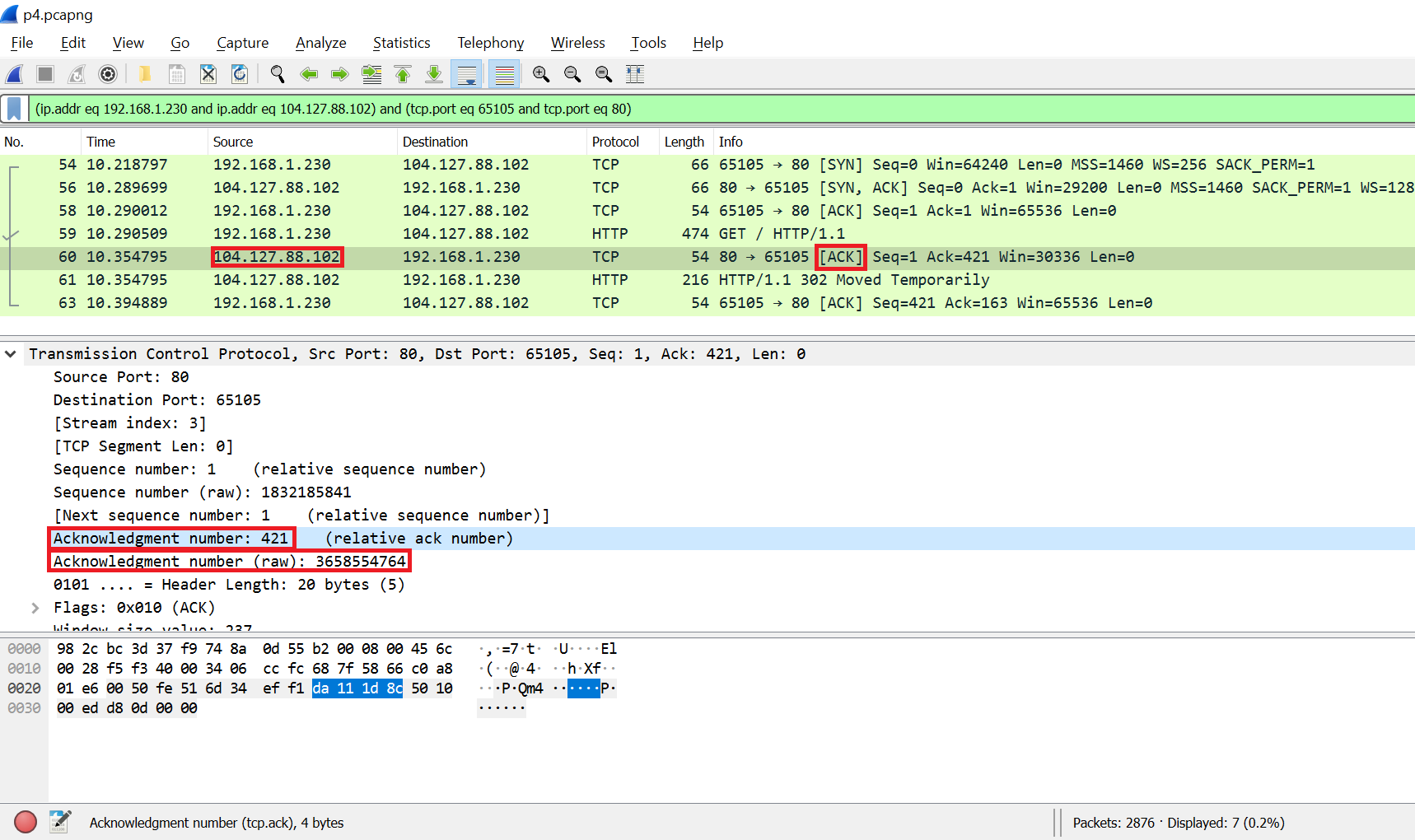


Figure 13.a

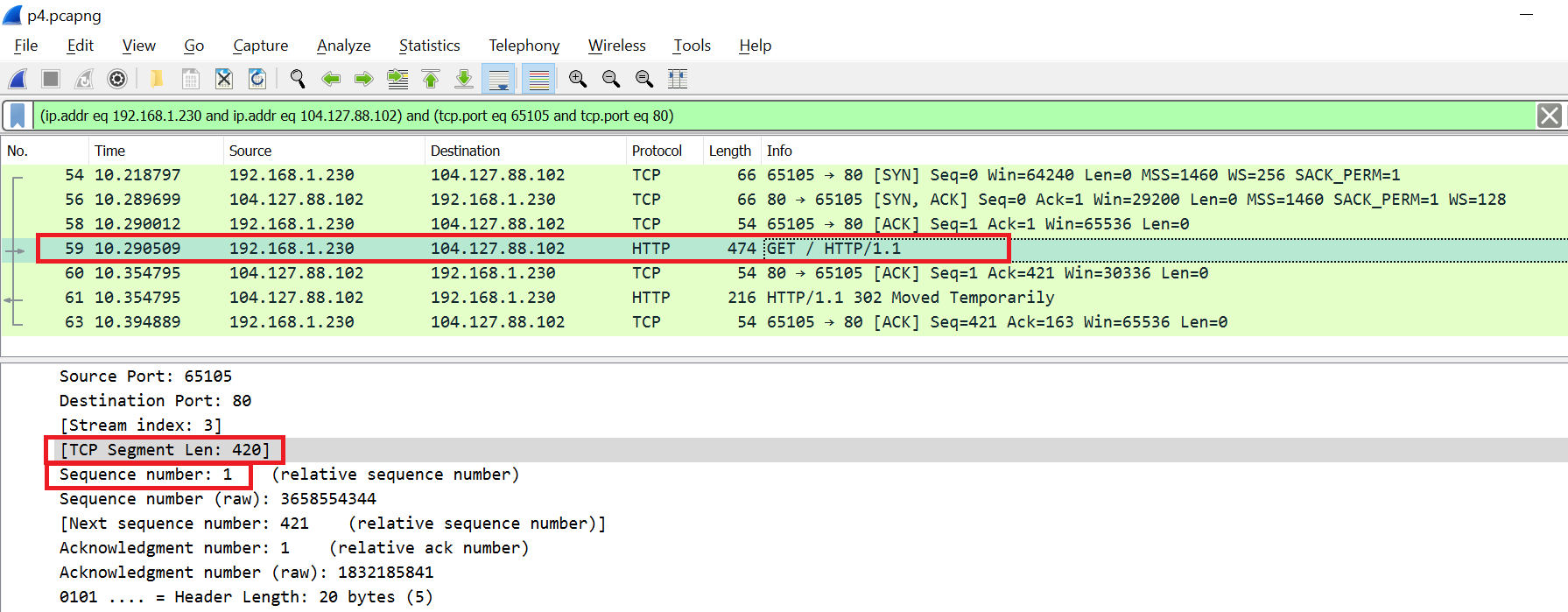
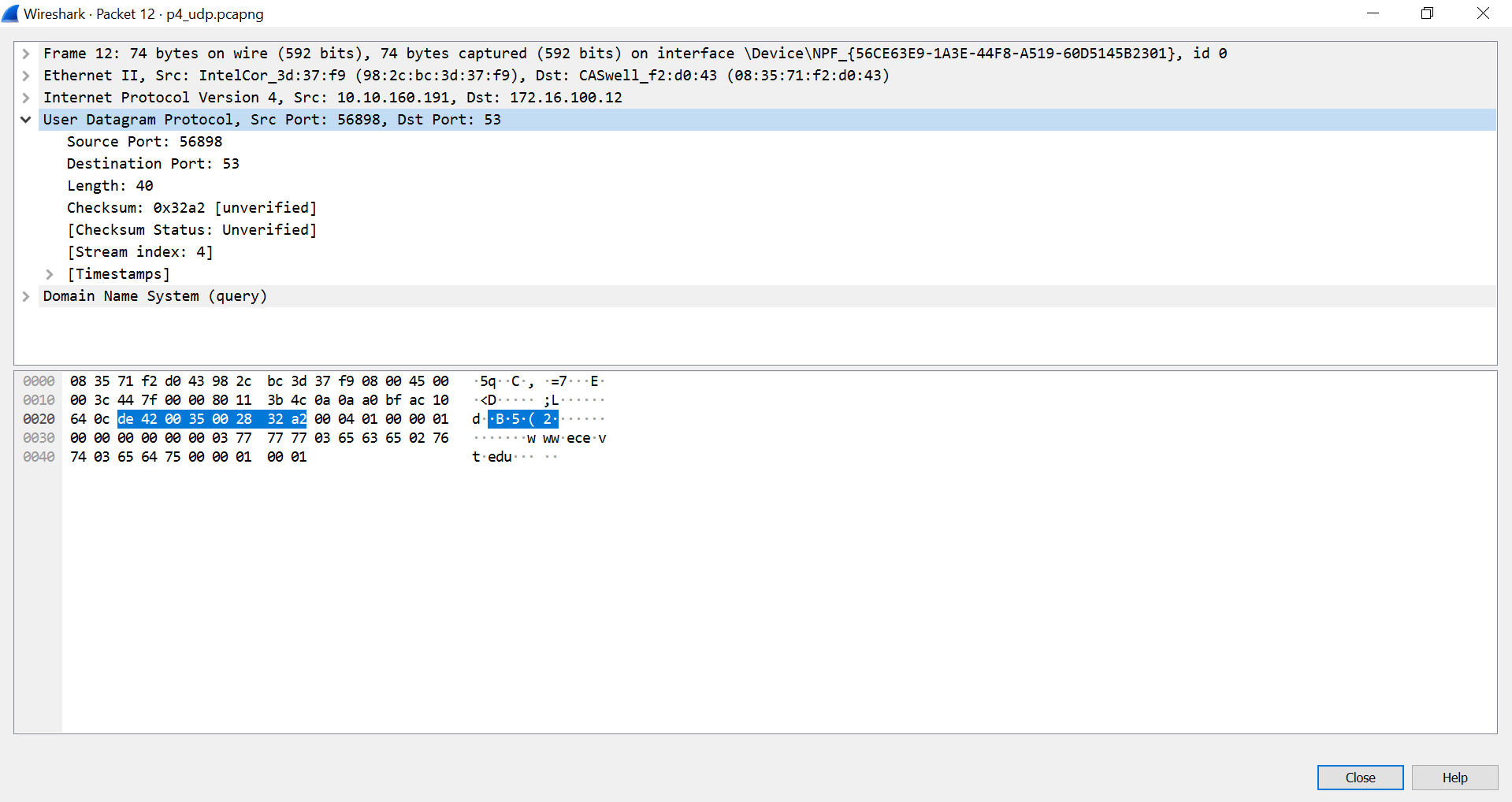


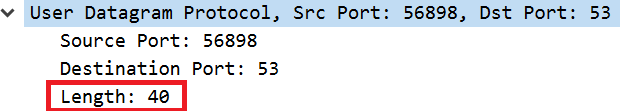
Figure 13.b

2.2. UDP:

1. The UDP header has a fixed length of 8 bytes. Each of these 4 header fields is 2 bytes long.
2. Source port, length: 2 bytes, value: 56898
3. Destination port, length: 2 bytes, value: 53
4. Length, length: 2 bytes, value: 40
5. Checksum, length: 2 bytes, value: 0x000032a2



1. The length field specifies the number of bytes in the UDP segment (header plus data). An explicit length value is needed since the size of the data field may differ from one UDP segment to the next.



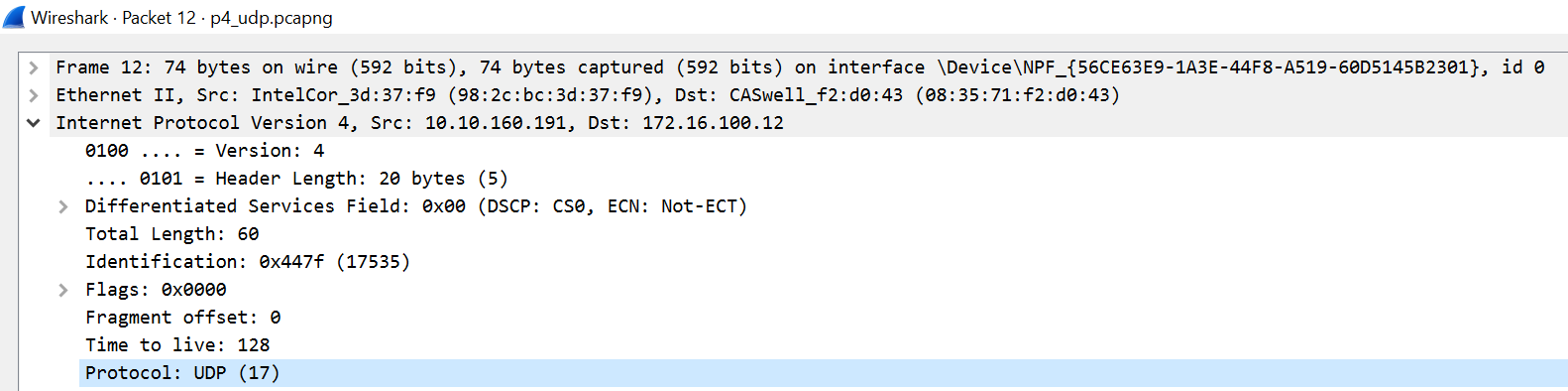
1. What is the maximum number of bytes that can be included in a UDP payload?

The maximum number of bytes that can be included in a UDP payload is (2^16 – 1) bytes plus

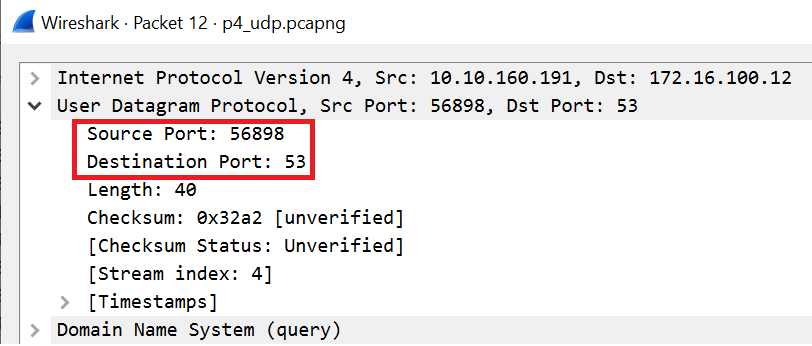
the header bytes. This gives 65535 bytes – 8 bytes = 65527 bytes.

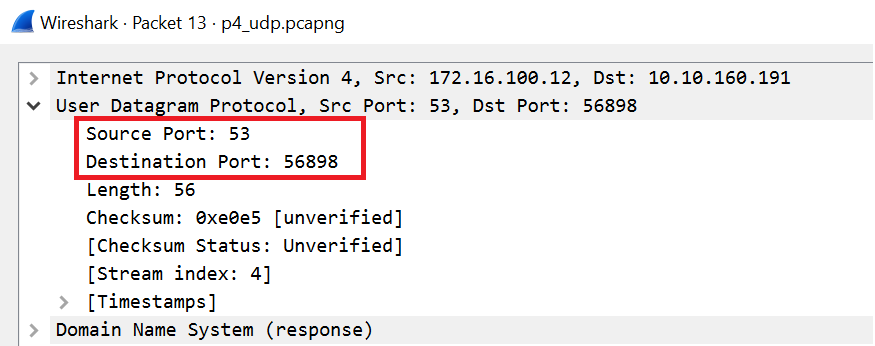
1. What is the protocol number associated with UDP?

17

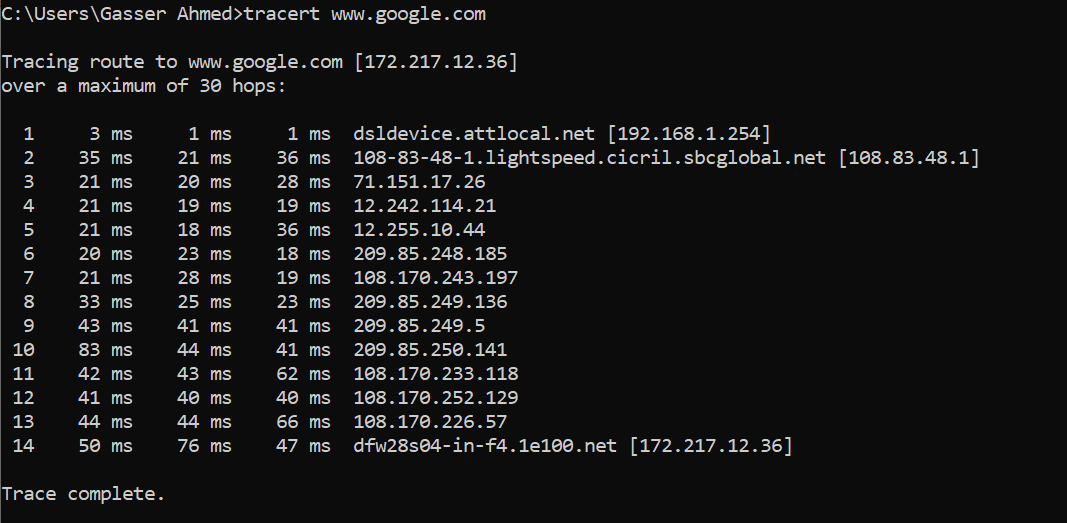


1. The source port of the UDP packet sent by the host is the same as the destination port of the reply packet, and conversely the destination port of the UDP packet sent by the host is the same as the source port of the reply packet.

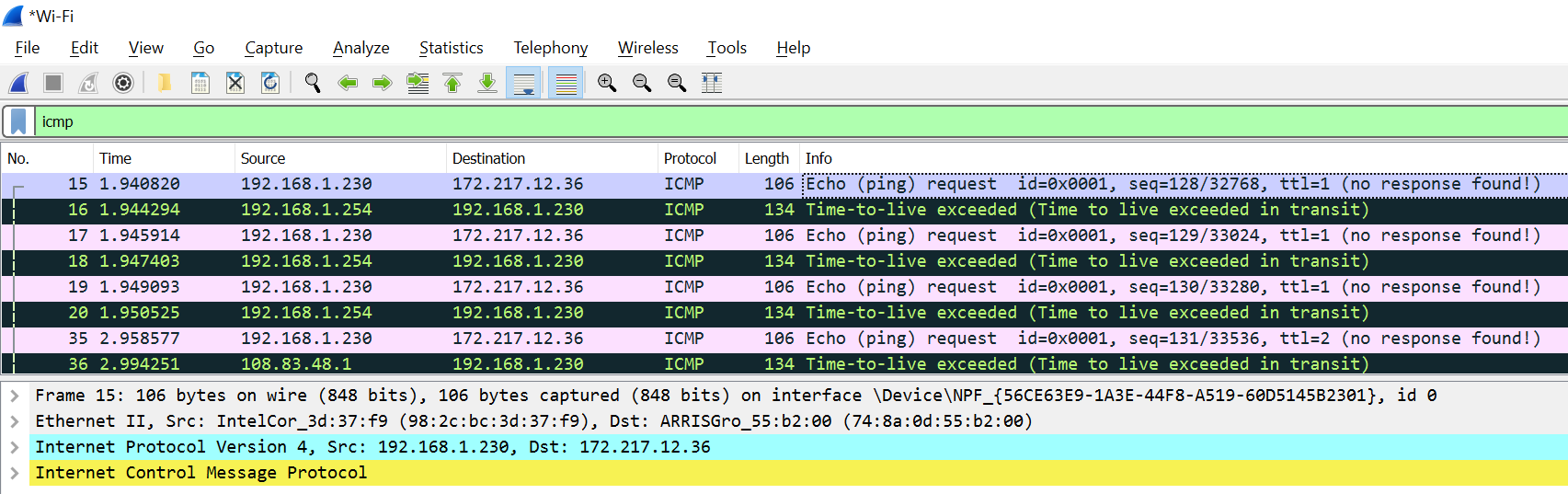


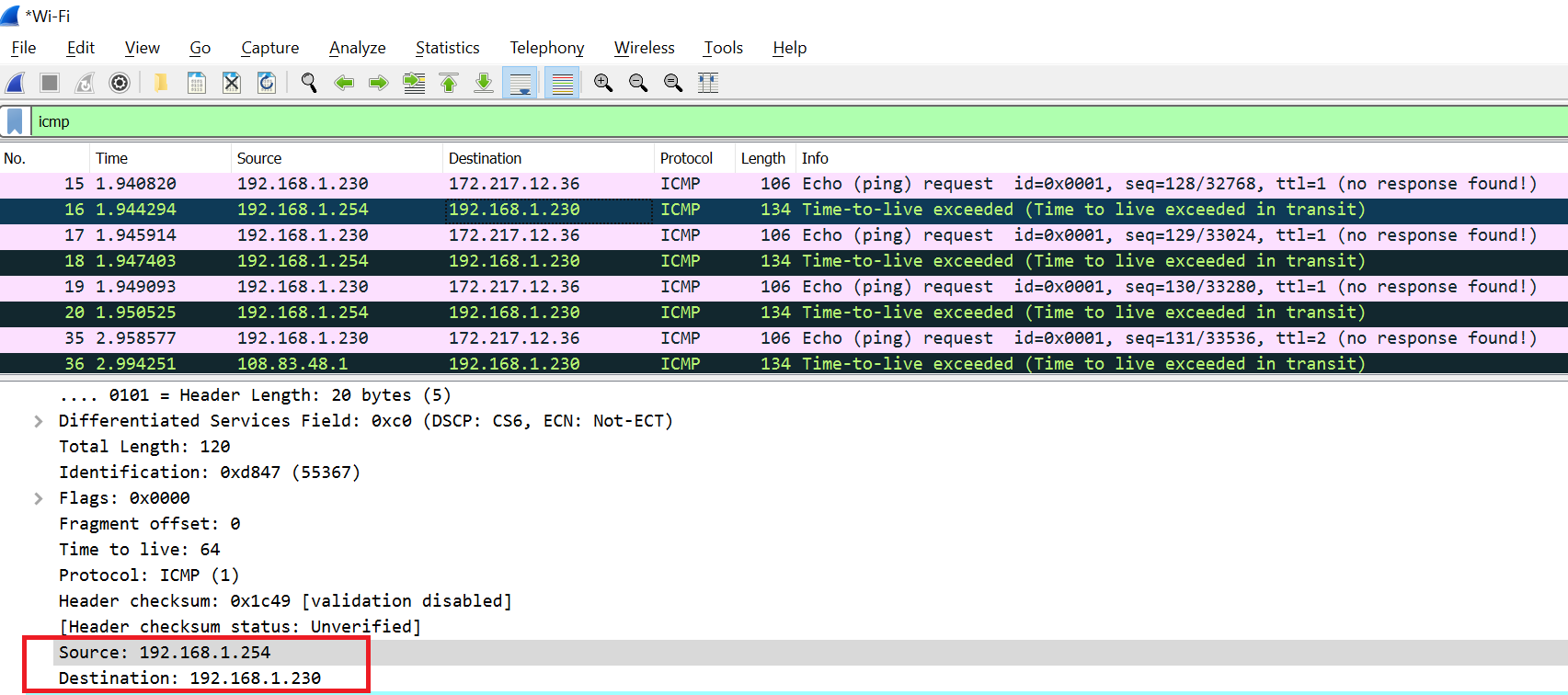


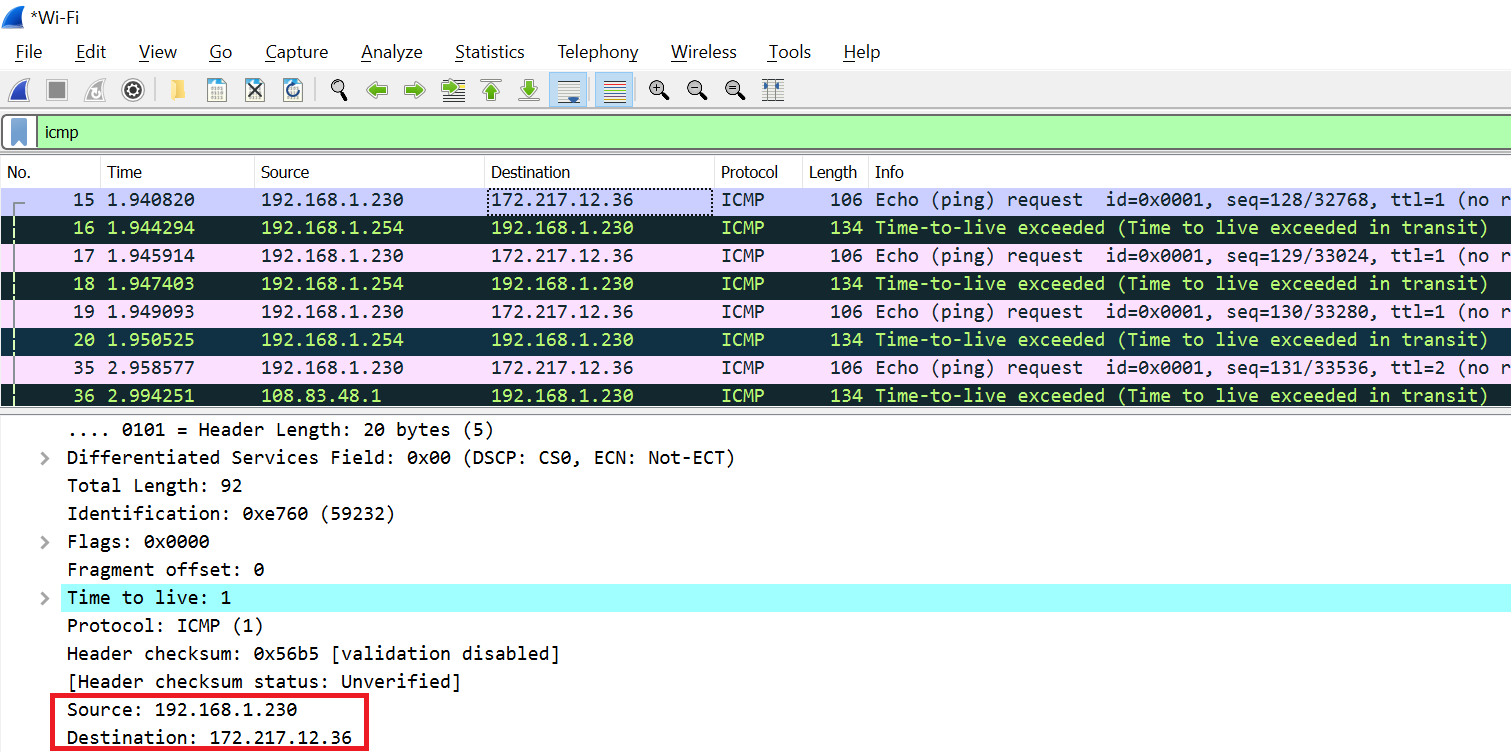
2.3. IP:



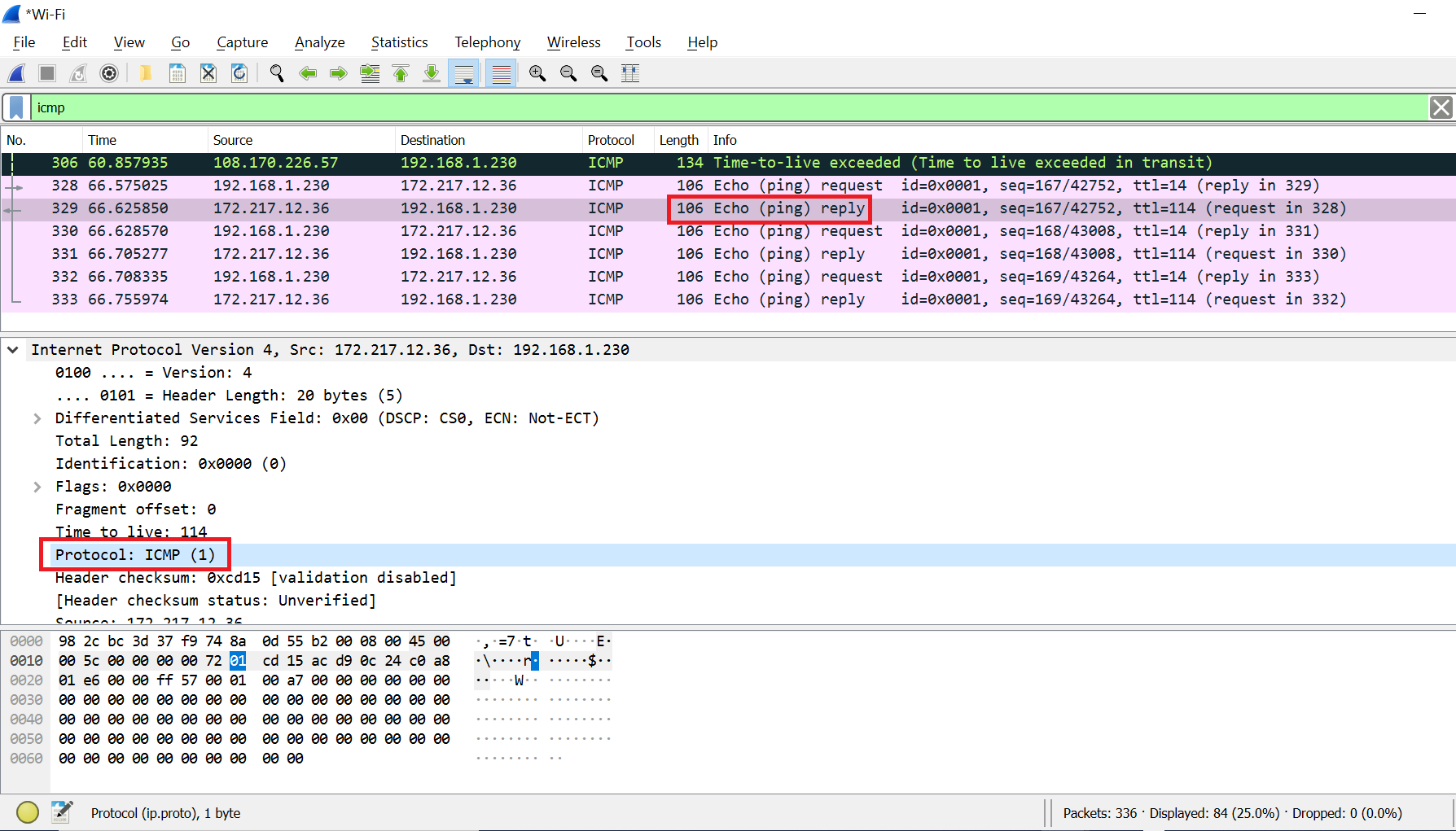
1. The traceroute (tracert) operation used ICMP



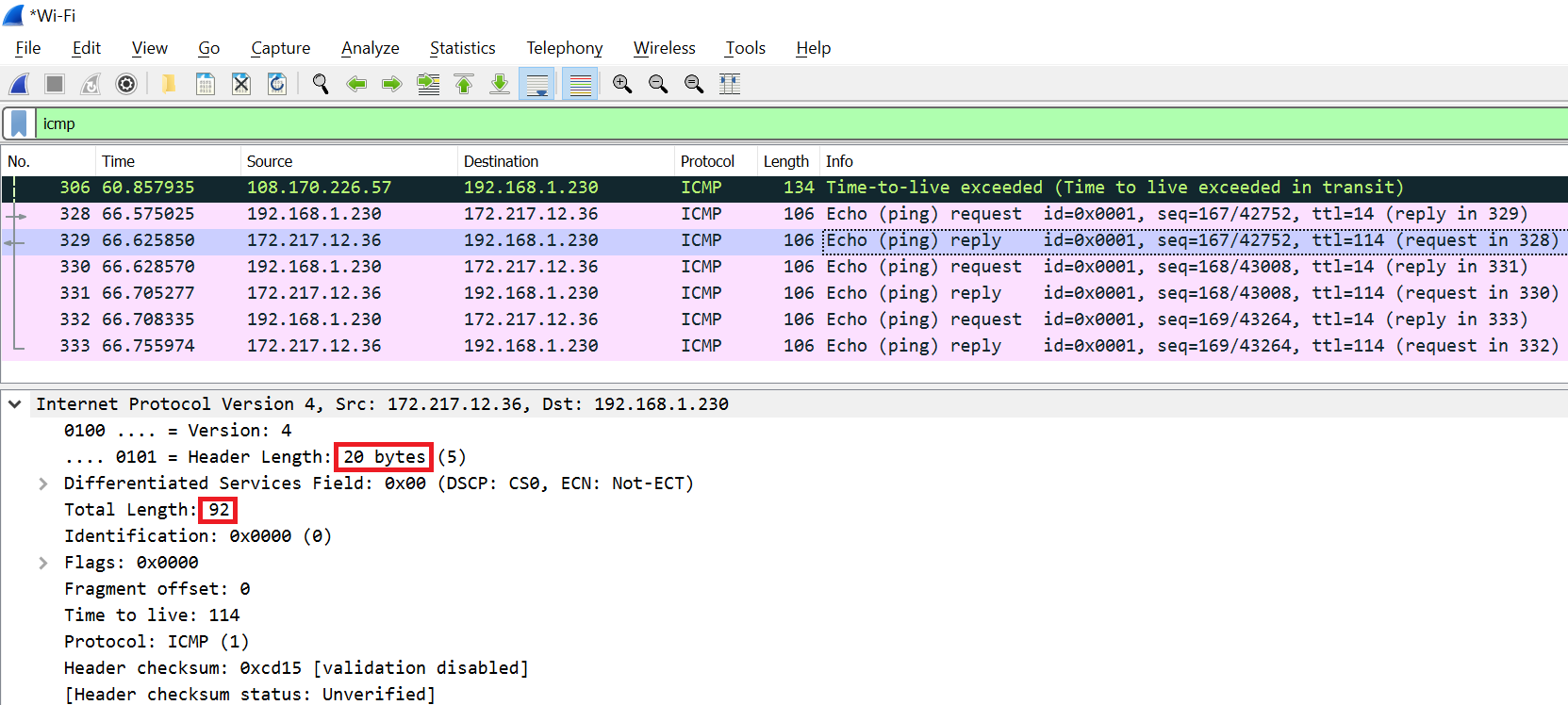
1. 192.168.1.254
2. No



1. ICMP (1)



1. The Protocol field in the IPv4 header contains a number indicating the type of data found in the payload portion of the datagram. It also provides a demultiplexing feature so that the IP protocol can be used to carry payloads of more than one protocol type.
2. 20 bytes



1. Number of bytes in the payload of the IP datagram = total length – header length

= 92 – 20 = 72 bytes

Section 3 – Conclusions:

After going through the TCP, UDP, and IP Capture and Analysis phases, I was able to become more familiar with Wireshark network analysis and have a better understanding how it works with different internet protocols. Also, using learning new commands like *nslookup* and *tracert* was very helpful in understanding those internet protocols. However, the nslookup part in the UDP section was a little tricky as it wasn’t giving me any response until I used a different network i.e. WiFi then it started to give me the expected results.

In general, the project clarified how different protocols work and behave. Lastly, the approximate number of hours I devoted to the project was about 12-16 hours.