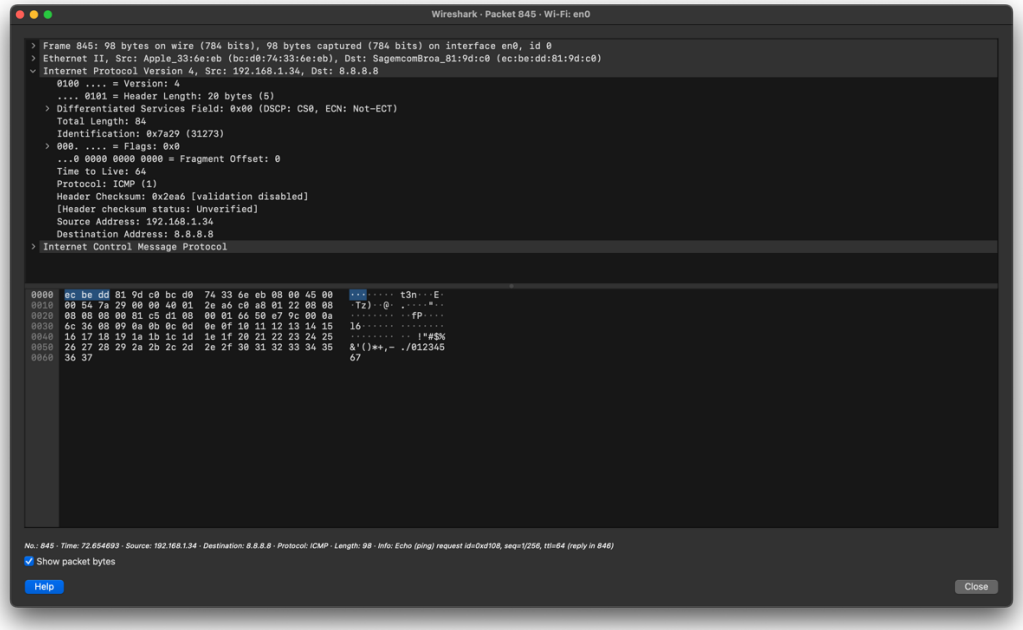
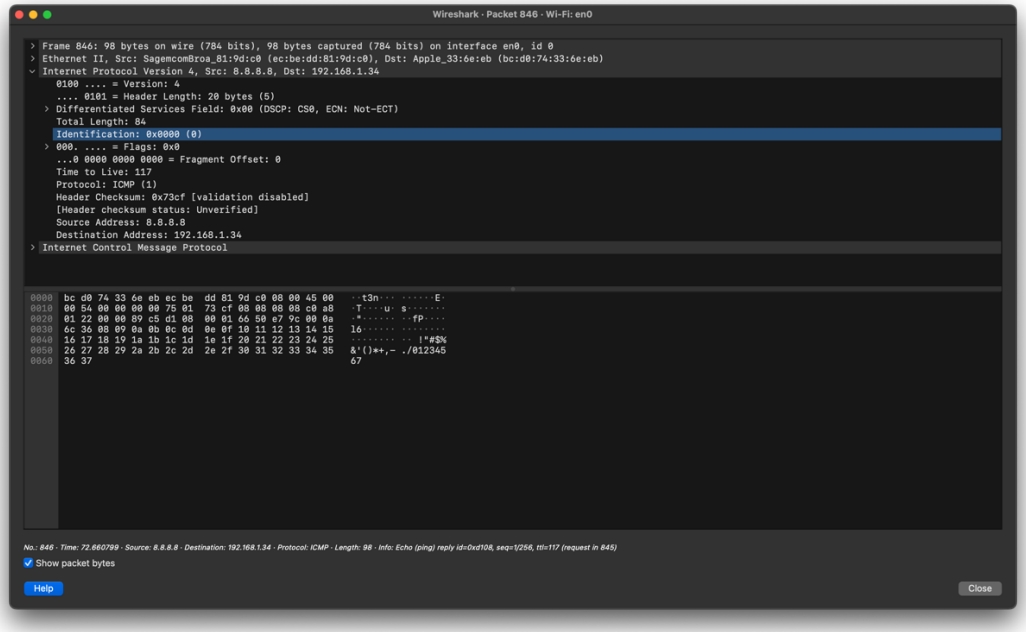
Exercise 11

ICMP – Wireshark

Command used: ping 8.8.8.8
Request:



Reply:

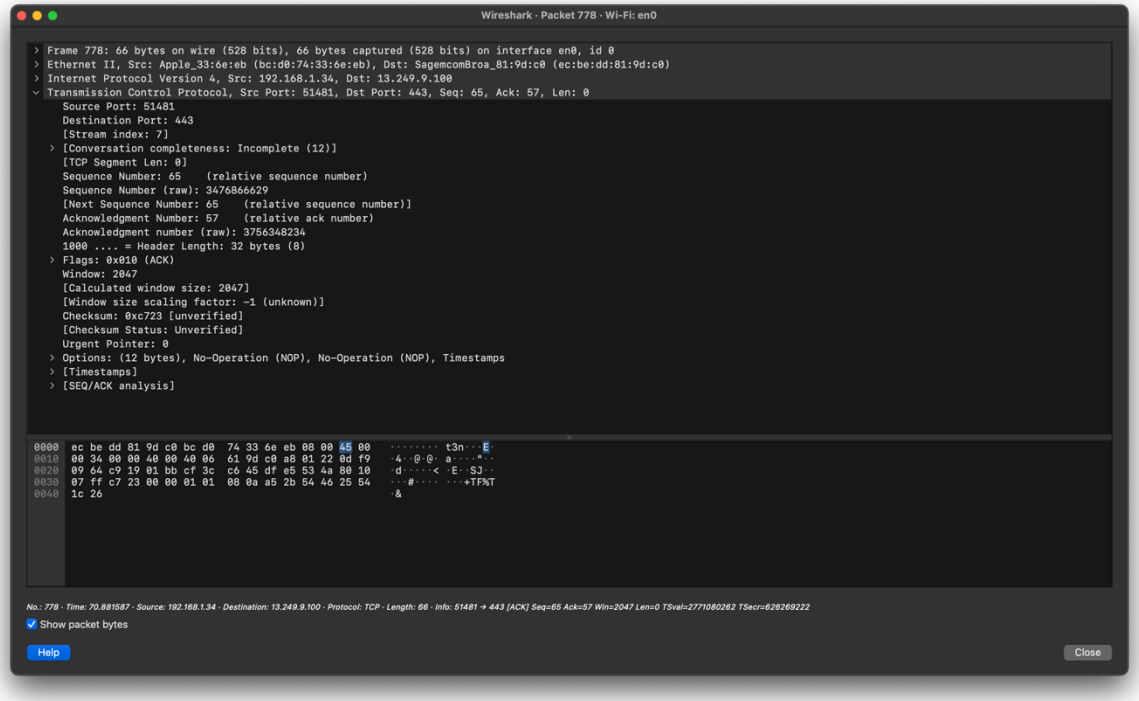


Observations:

1. The Version field gives the version of the Internet Protocol used. In this case, it's 4, therefore it's an IPv4 packet.
2. TTL gives the maximum number of hops that the packet can travel before being discarded. In this case, it is 64 for the request and 117 for the reply
3. The 'Protocol: ICMP (1)' field identifies the protocol encapsulated in the IP packet's payload. In this case the value is 1, therefore the payload contains an ICMP packet.

Exercise 13

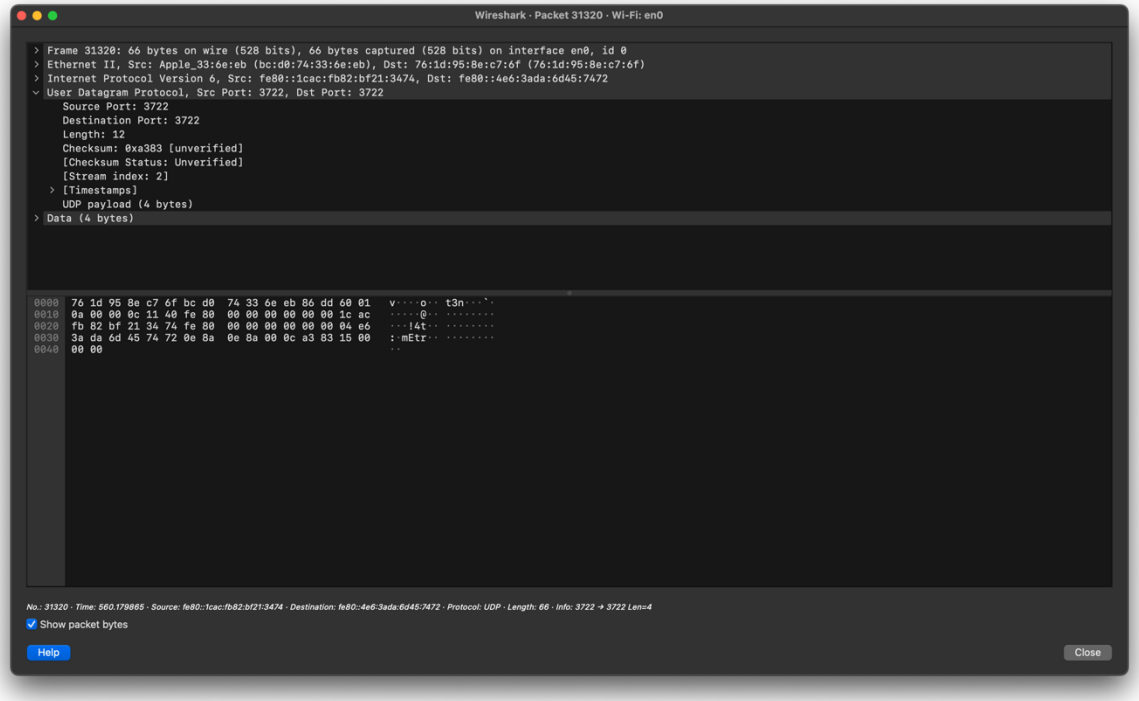
TCP – Wireshark



Observations:

1. Destination port is 443, which corresponds to HTTPS
2. The sequence number of first octet in the segment (in this case, it is 3476866629) indicates that the first byte of data in this segment is the 2476866629th byte of the data stream (because 3476866629 - 1000000000 = 2476866629).
3. The relative sequence number (in this case, 65) is a number used by wireshark for easier interpretation.
4. Acknowledgment Number (3765483824) indicates that the sender has received all bytes up to this number minus one.
5. Header length = 32 bytes (8 * 4 = 32 bytes, as the header length field is in 4-byte words).

UDP – Wireshark



Observations:

1. The source port is equal to the destination port (3722)
2. The checksum value is 0xa383, but it's marked as unverified, therefore it hasn't been verified by the receiving system