Course: CompSci 4C03
Name: Jatin Chowdhary
Mac ID: Chowdhaj
Date: April 12th, 2021

Assignment #6: Wireless Trace Analysis

MacSecure Trace

1) Can you guess what is the vendor (manufacture) of the APs for MacSecure?

Yes, I estimate that the vendor/manufacture of the AP for MacSecure is Cisco. This is because in the Wireshark output, I can see that frames are sent from *Cisco_50:0d:30* to the mobile device, *Apple_18:af:01*. Refer to the figure below for more information. Furthermore, since the mobile device is broadcasting and isn't connected to an AP, all nearby APs are Cisco, based on the Wireshark packet-listing window.

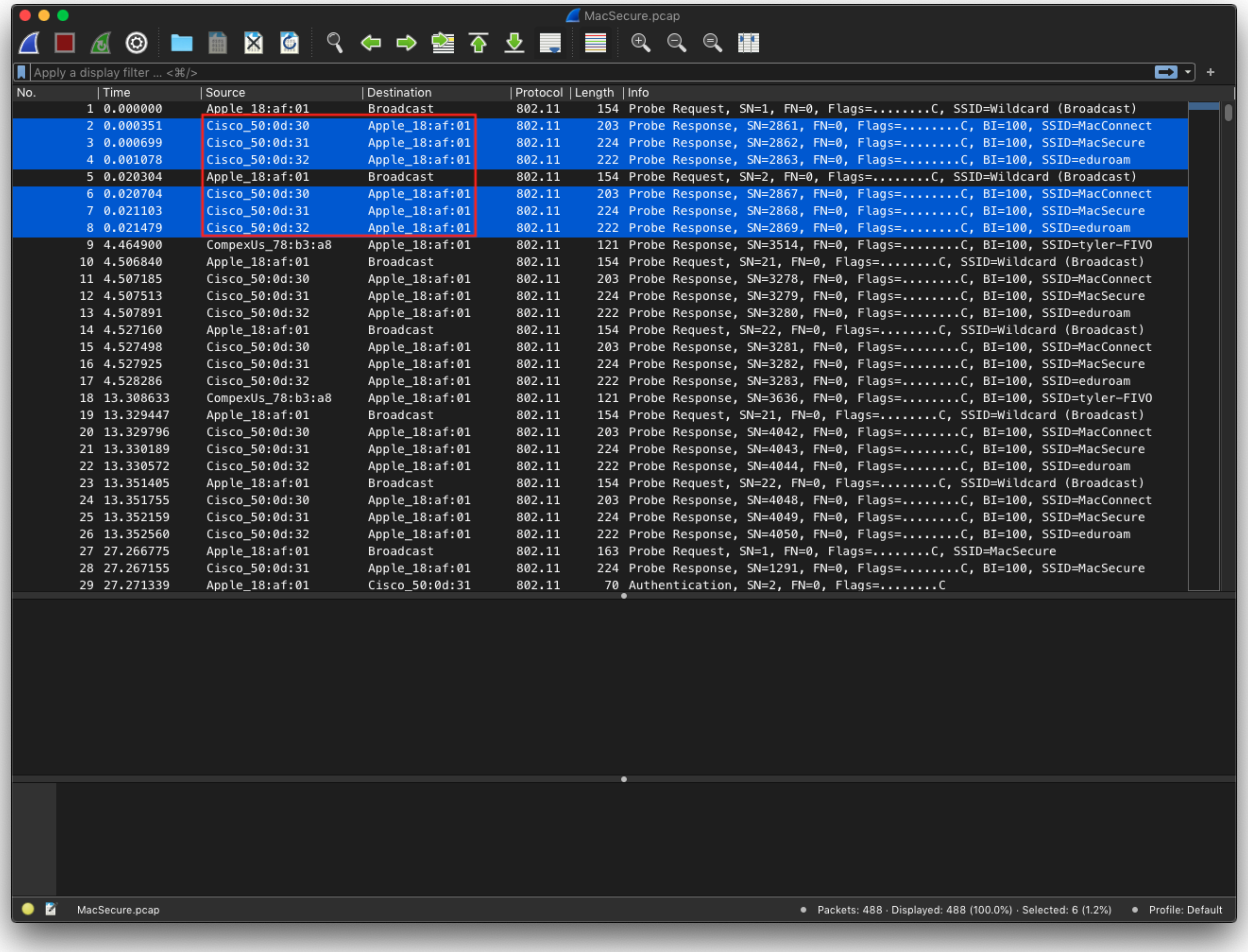

Figure 1: The red box highlights frames sent from an AP to the mobile device. Since we know the MAC address of the mobile device, we can assume that the other device is an AP. Thus, Cisco is the vendor of the APs. Furthermore, packets sent from the mobile device are a broadcast. This means that they are sent to all devices.

2) What is the type of the first frame (at time 0.0)? Why is the SSID set to “Broadcast”?

The first frame, at time 0.0, is of type *Probe Request*. This is evident in the figure below. The SSID is set to *Broadcast* because the mobile device is probing nearby Access Points, to determine what is available to connect to. The frame is not sent to a particular destination, it is sent to whomever can receive the frame and process it appropriately. Thus, the value in the Destination field for the mobile device is *Broadcast*.

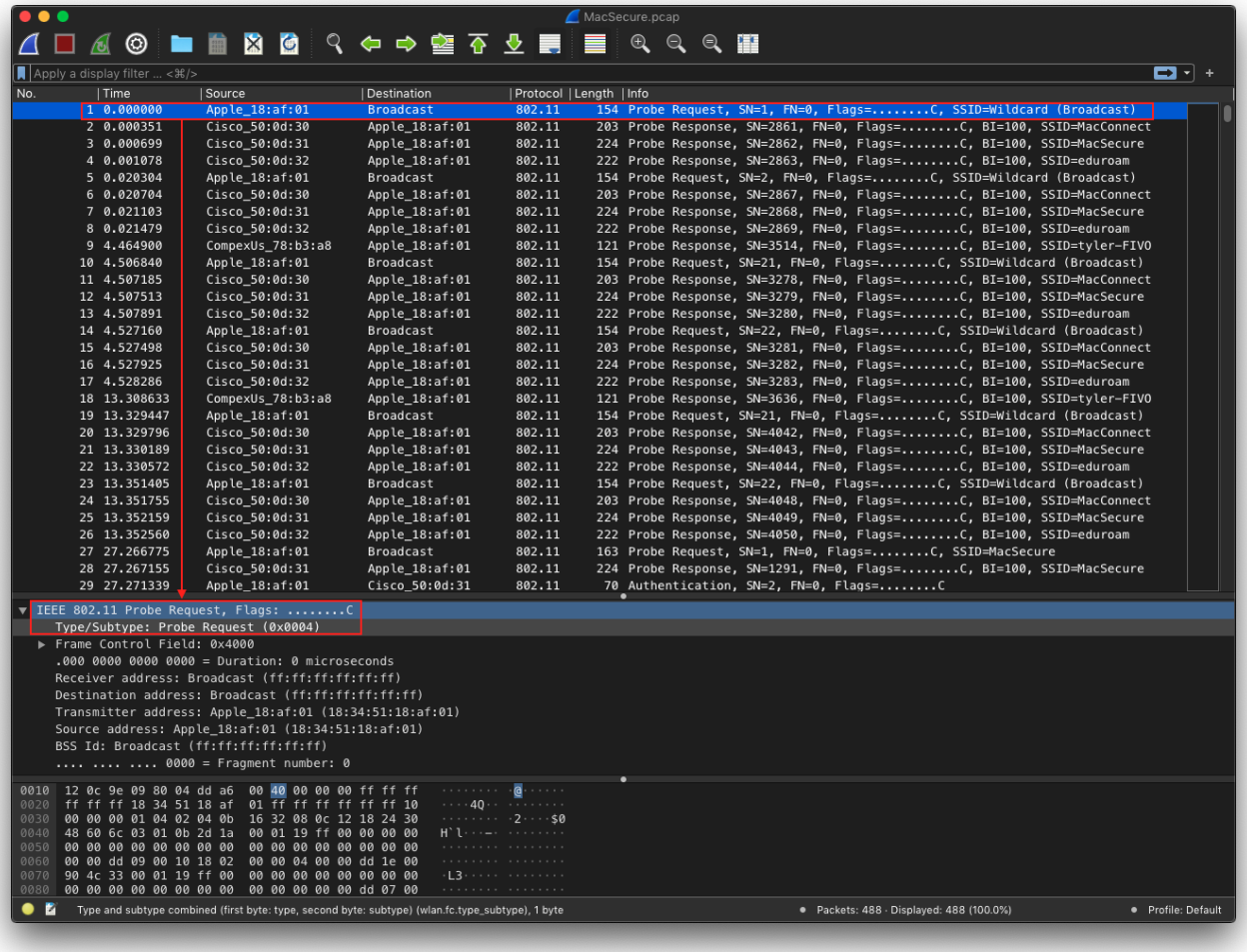

Figure 2: The red box at the bottom highlights key information in the packet-listing window. The highlighted information shows that the type of the first frame is a Probe Request.

3) What are the types of the frames numbered 2, 3, 4? What information is contained in the Radiotap header, and the IEEE 802.11 wireless LAN management frame?

The frames 2, 3, and 4 are *Probe Response* frames; as shown in figure 3. These frames are in response to the first frame, which is a *Probe Request* frame sent from the mobile device. The *Radiotap Header* contains (meta) data about the wireless signal between the mobile device and the access point. This information is, but not limited to, *Antenna signal*, *Antenna noise*, *Channel frequency*, *Channel flags*, *Data rate*, etc. This is shown in figure 4.
The *IEEE 802.11 Wireless Management* frame contains information about the access point itself. It is broken into two categories: *Fixed* and *Tagged parameters*. These contain information such as: device's name, information about the vendor, *parameters, SSID parameter set*, *Supported Rates*, etc. This is shown in figure 5.

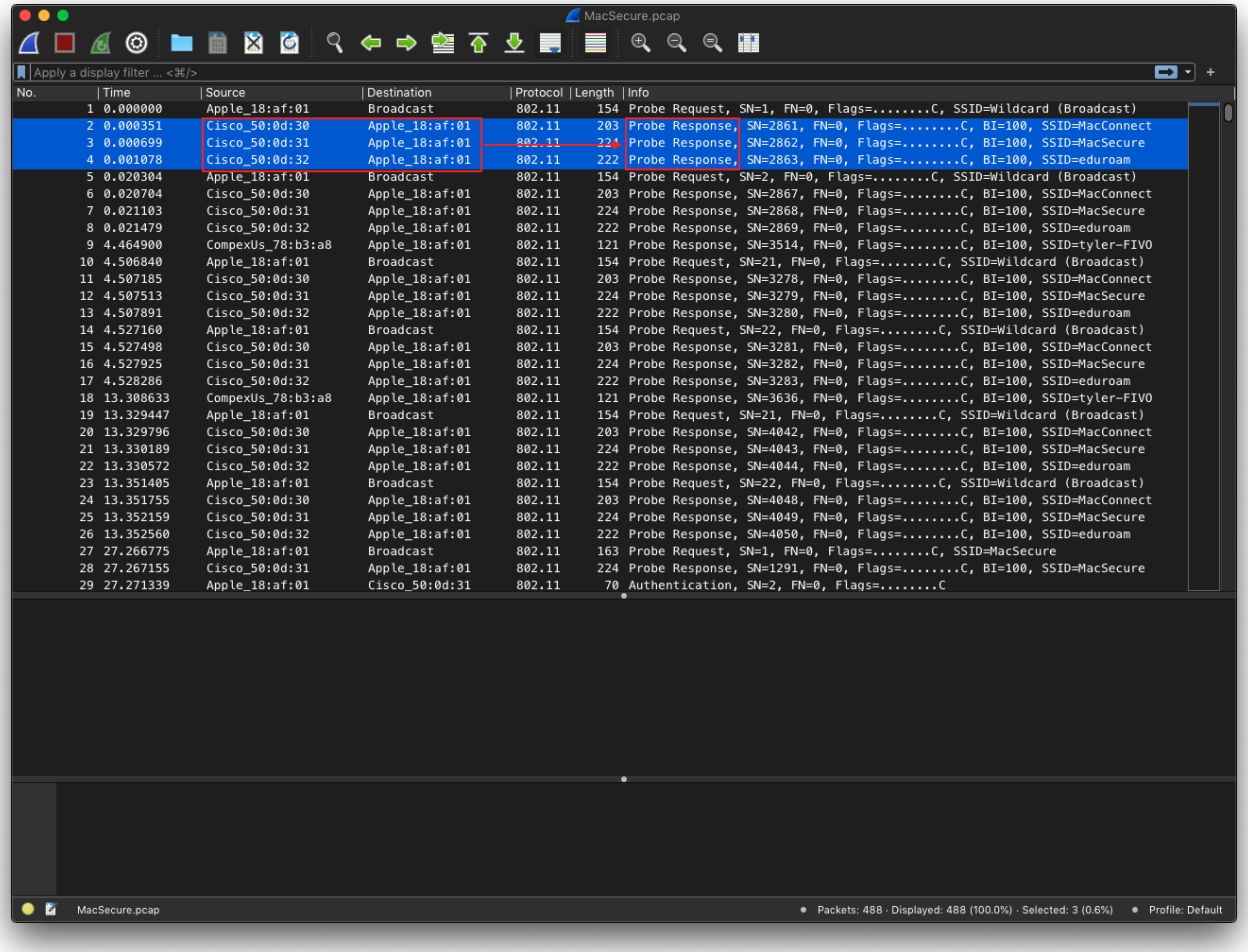

Figure 3: This figure highlights information about the type of Packets 2, 3, and 4. The red box on the right side highlights the type of these frames; they are Probe Response frames.

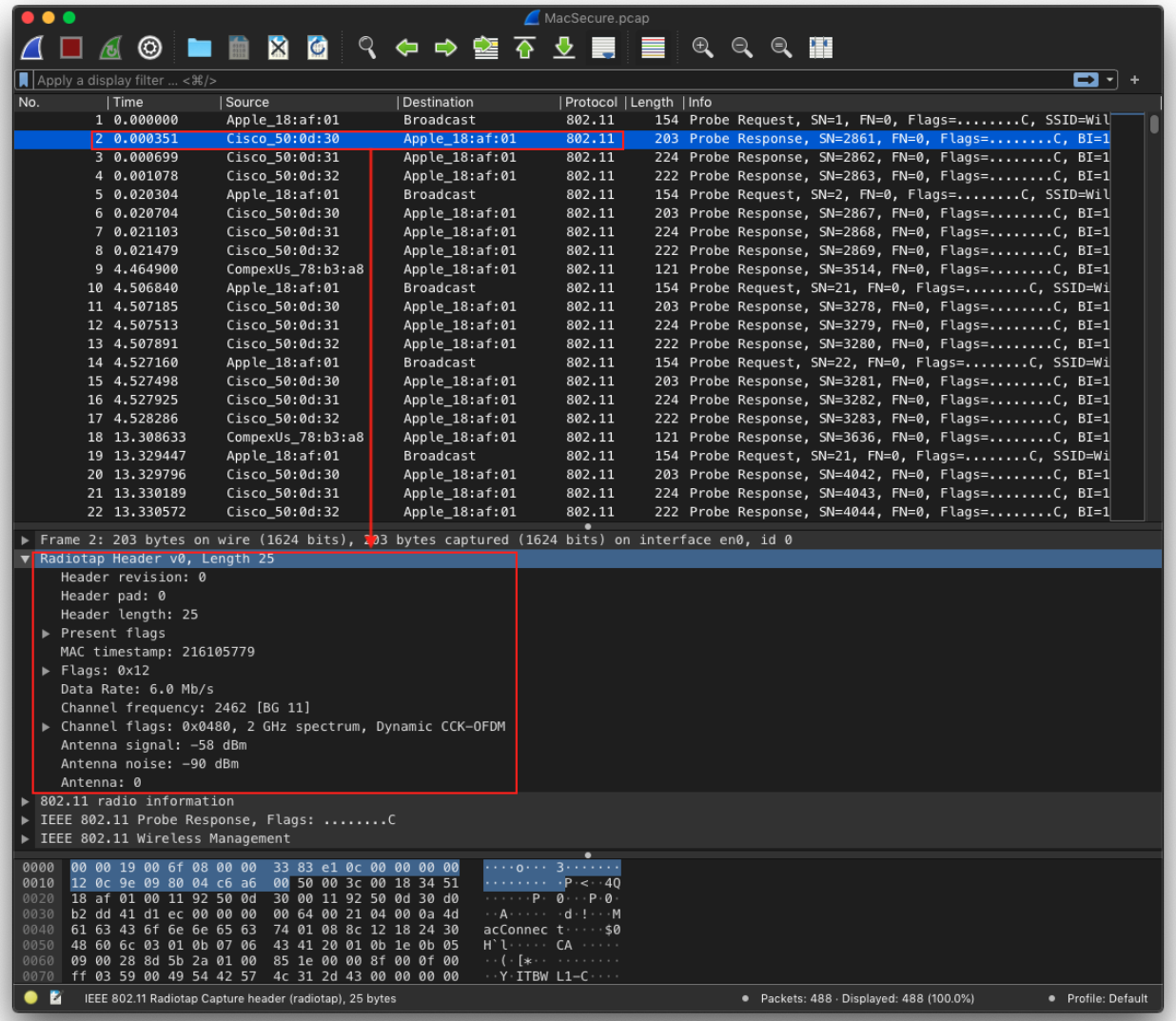

Figure 4: This figure shows that the Radiotap Header contains (meta) data about the wireless signal between the mobile device and the access point. The information in the figure above pertains to Frame 2. The red box at the bottom highlights the information in the Radiotap Header.

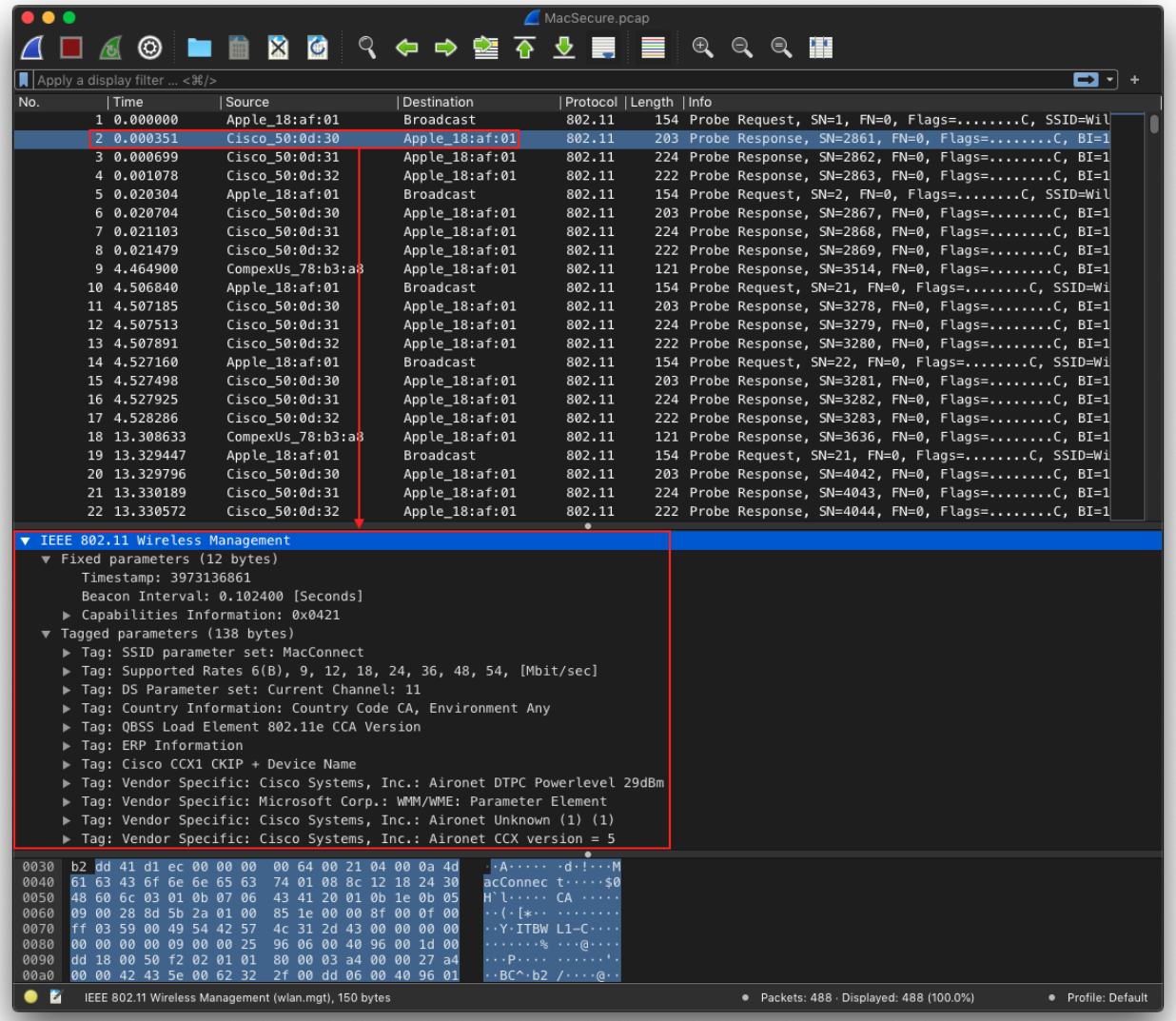

Figure 5: This figure shows that the IEEE 802.11 Wireless Management frame contains data about the access point, information such as device name, vendor information, capabilities, etc. The information in the figure above pertains to Frame 2. The red box at the bottom highlights the information in the IEEE 802.11 Wireless Management.

4) Explain the frames 29 and 30.

Frames 29 and 30 are Authentication messages that correspond to the mobile device and the access point colloquially known as *MacSecure*. Frame 29 is sent from the mobile device to the access point. This frame tells the AP that authentication algorithm *Open System* will be used; this is demonstrated in figure 6. Frame 30 is sent from the access point to the mobile device. This frame *is like an ACK* to the previous frame, and tells the mobile device that it is ready to use *Open System*, and it starts the initial phase of the connection process. This is shown in figure 7. In short, frame 30 is more like a success message.

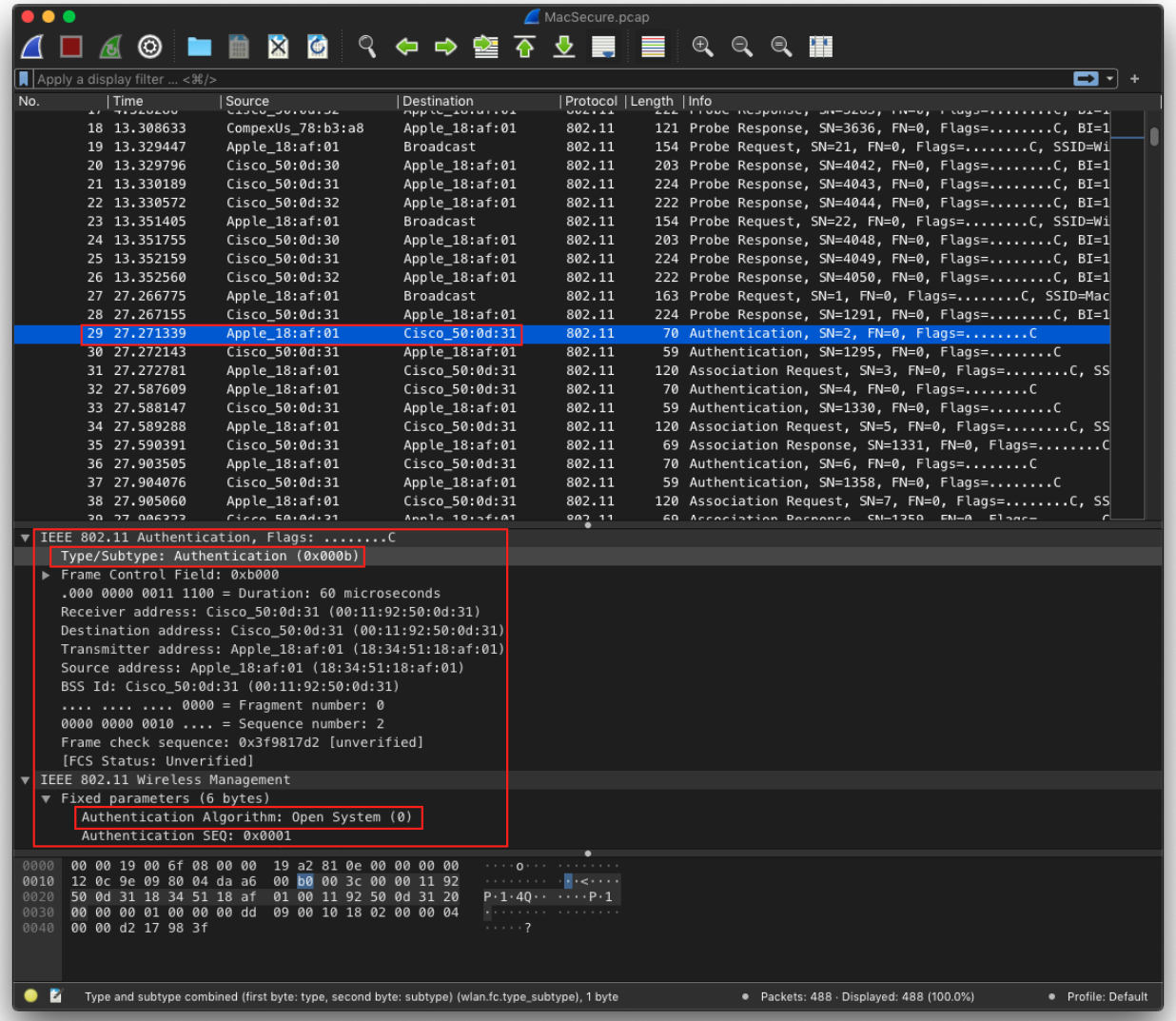

Figure 6: This figure shows that frame 29 is sent from the mobile device to the access point known as MacSecure. This frame is an authentication frame that tells the AP that the device wants to connect to it. In the red box at the bottom of the figure, you can see that the type of the frame is Authentication, and it uses the Open System algorithm.

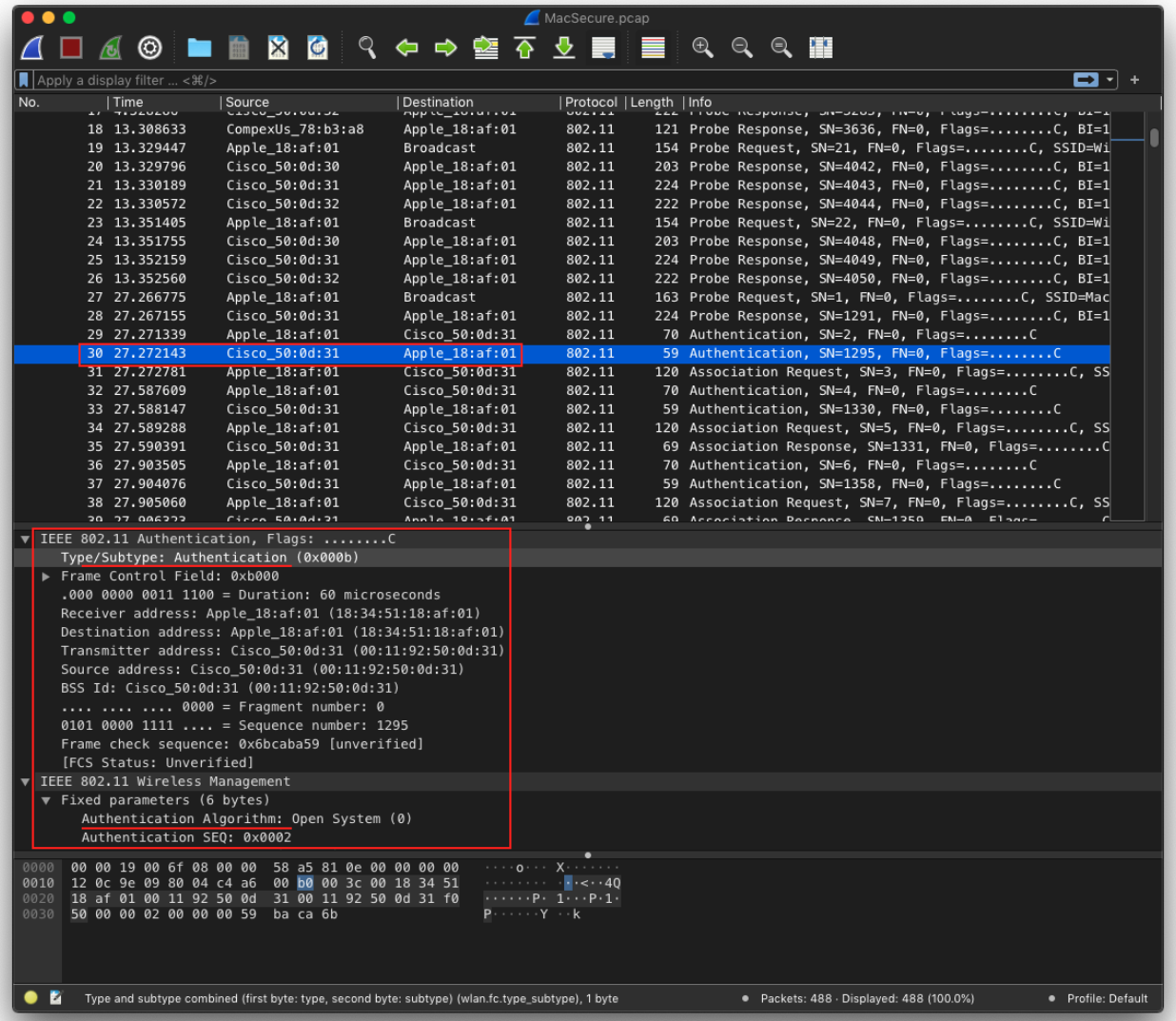

Figure 7: This figure shows that frame 30 is sent from the access point known as MacSecure to the mobile device. This frame is a response to frame 29 that was previously sent from the mobile device to the AP. This frame starts off the beginning of the connection phase between the two devices. This frame is an authentication frame that tells the mobile device that connection can be started. In the red box at the bottom of the figure, you can see that the type of the frame is Authentication, and it uses the Open System algorithm.

5) Which channel does the AP operate that the mobile is associated with?

The AP operates on *channel 11*. This is the channel that the mobile device is associated with. This is demonstrated in the figures below; both figures show that both devices operate on *channel 11*. Figure 8 shows that the mobile device operates on *channel 11*, and figure 9 shows that the AP also operates on *channel 11*, when communicating with the mobile device. Futhermore, both figures show that the frequency of *channel 11* is 2462Mhz, and the *PHY type* is 802.11g.

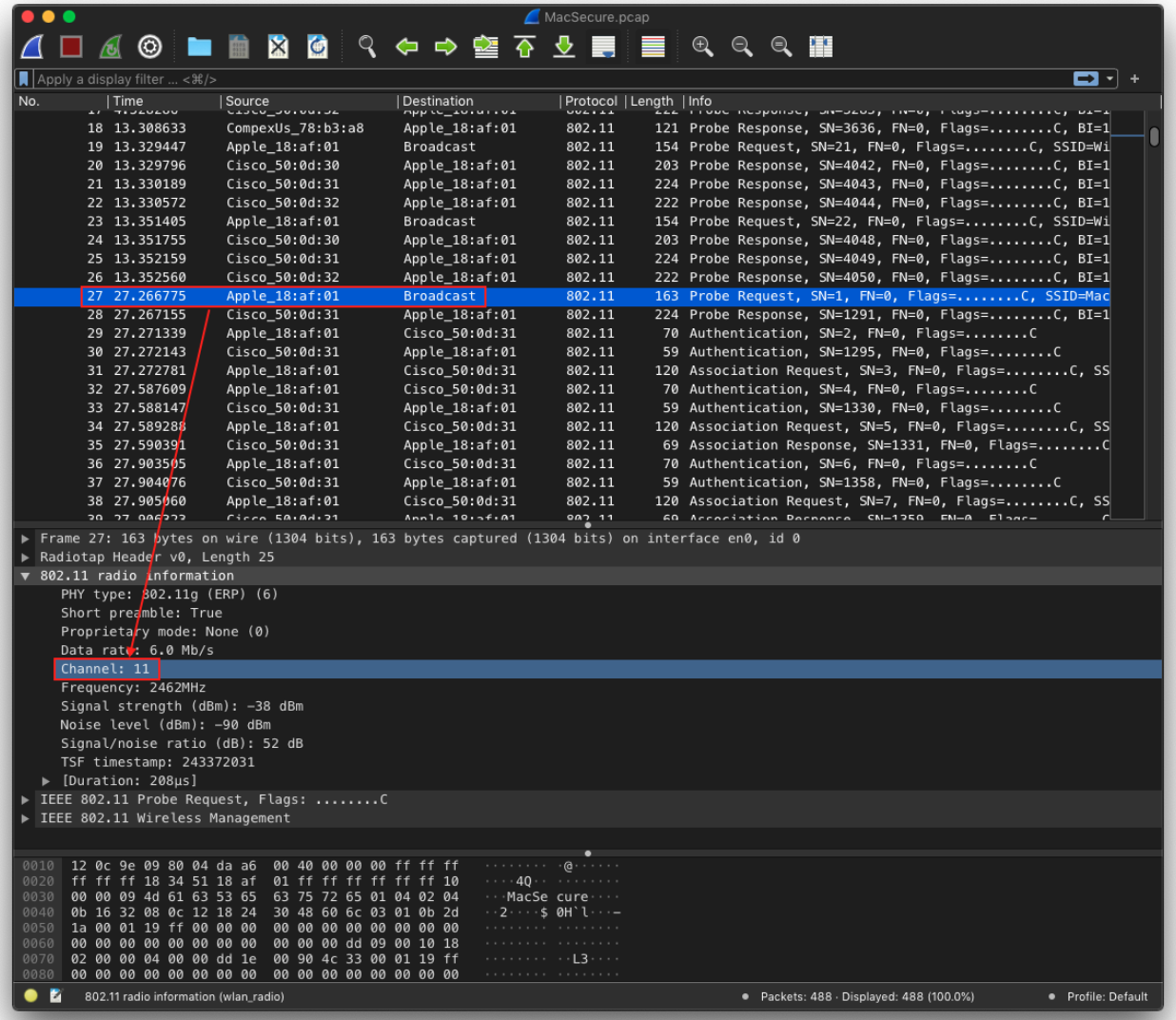

Figure 8: This figure shows that the mobile device operates on channel 11, when communicating with the access point, MacSecure. The red box at the bottom highlights this information.

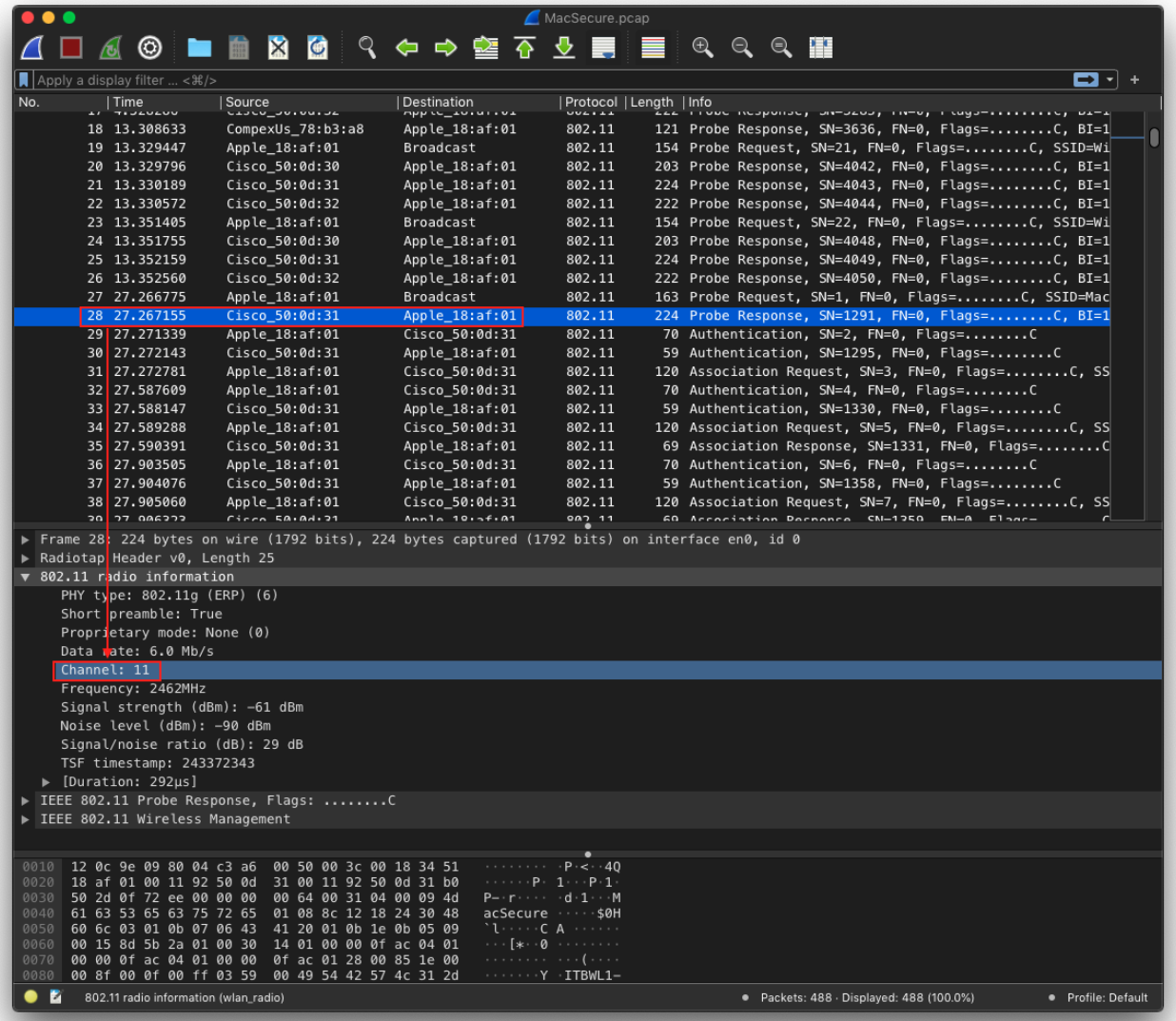

Figure 9: This figure shows that the access point (MacSecure) operates on channel 11, when communicating with the mobile device. This is shown in the red box at the bottom of the figure.

6) Between frame 31 – 44, how many association requests have been sent from the mobile device?

Between frames 31 and 44, 4 association requests are sent from the mobile device to the access point. This is shown in the figure below.

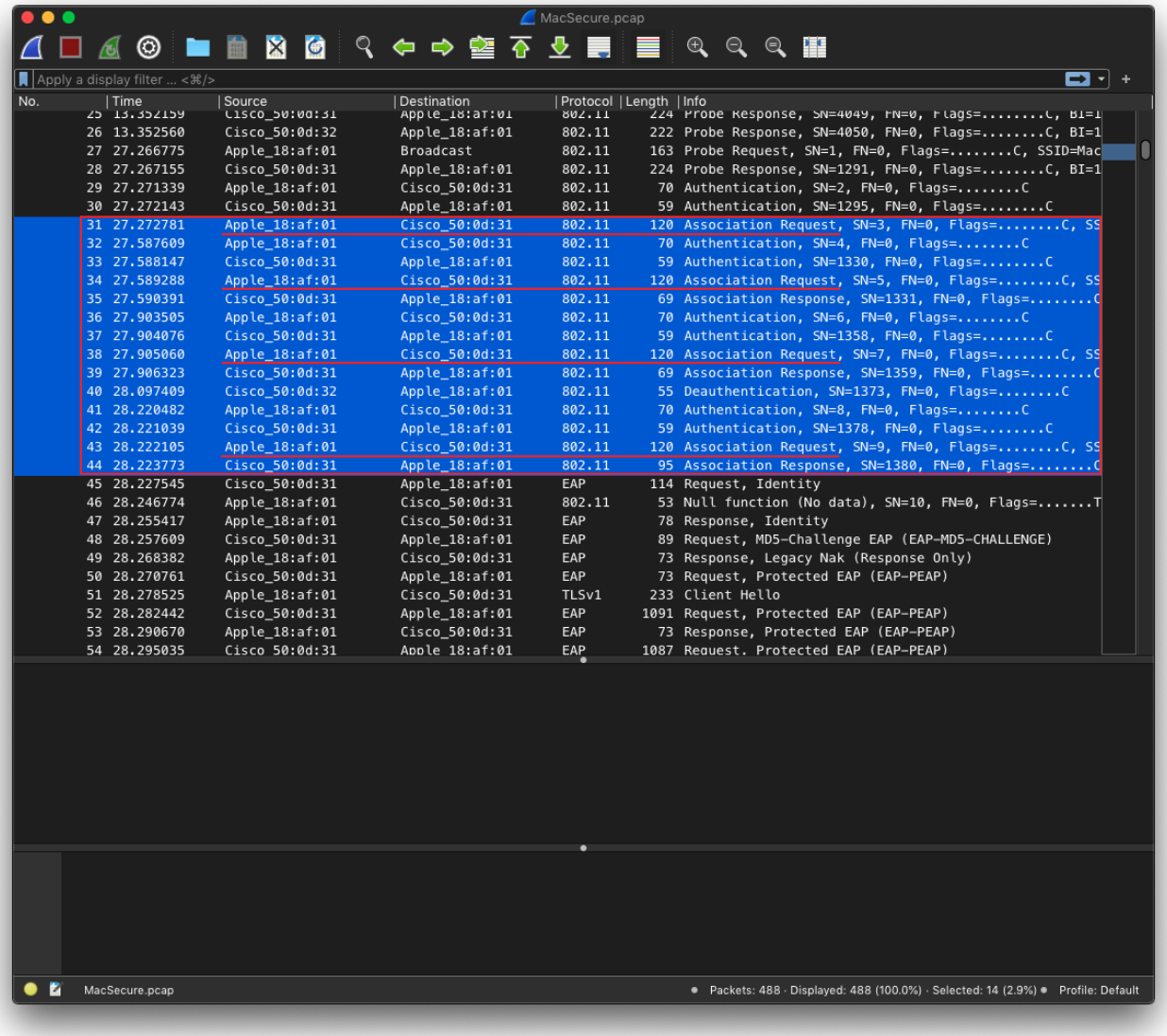

Figure 10: This figure highlights all frames between 31 and 44, inclusive. Each frame that is an association request, sent from the mobile device to the access point, is underlined in red. There are 4 of these types of frames in total.

7) Which extended authentication protocol(s) (EAP) is used by MacSecure (e.g., EAP-TTLS/MSCHAPv2, EAP-TTLS, etc.)

The access point, MacSecure, is using *EAP-MD5-CHALLENGE* and *EAP-TLS*, to authenticate the user credentials that are entered and sent by the mobile device. This is shown in the figure below.

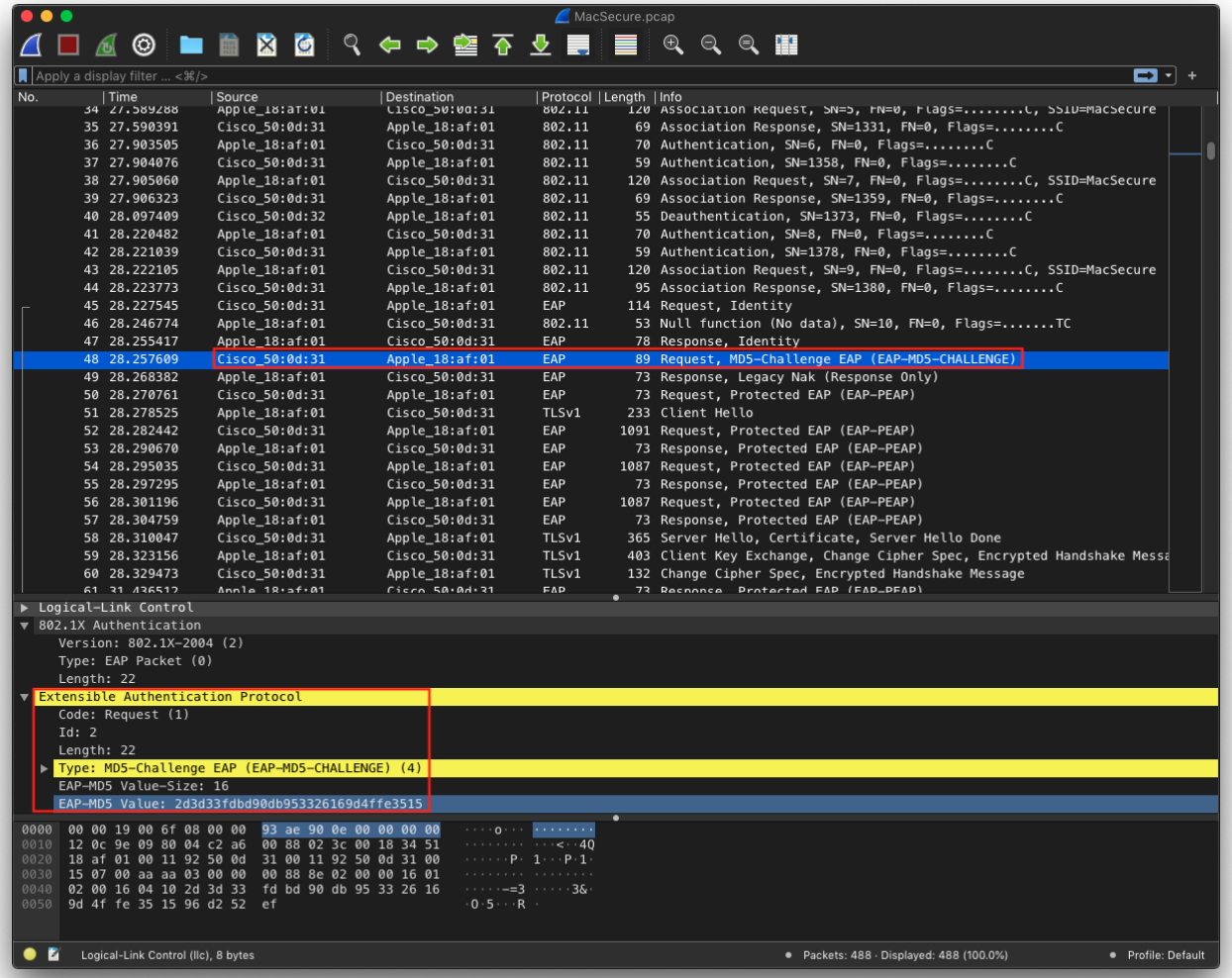

Figure 11: This figure shows that EAP-MD5 is used by the access point, MacSecure. It uses EAP-MD5 to authenticate the credentials sent by the mobile device. The red box at the bottom of the figure displays all of this information.

8) Which EAP is used in authenticating the mobile device?

EAP-TLS is used in authenticating the mobile device. This is shown in the figure below.

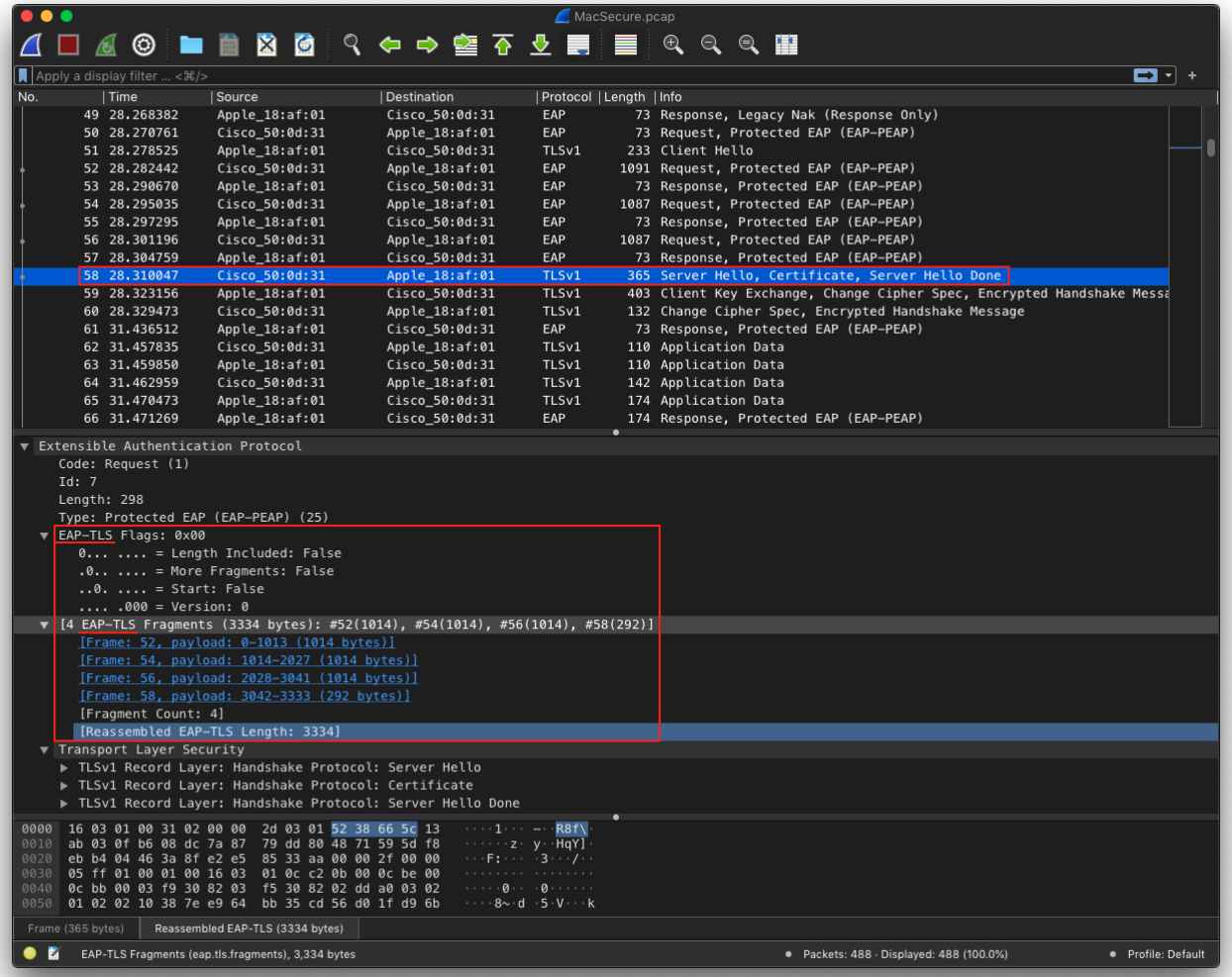

Figure 12: This figure shows EAP-TLS is used to authenticate the mobile device. The red box at the bottom demonstrates this, because EAP-TLS is used to encrypt the handshake message.

9) Frame 71 indicates the success of authentication via 802.11X. Which frames correspond to the 4-way handshake for establishing pair-wise transient key? What are the nonces used by the AP and the mobile devices in the 4-way exchange?

The frames 72, 73, 74, and 75 correspond to the 4-way handshake for establishing pair-wise transient keys. This is shown in figure 13, below. The nonces used by the AP and the mobile device in the 4-way exchange are:

Device	Nonce	Frame #	Message	Figure
Cisco (AP)	8e5a38648b923b518e60a2c401dc2f96ae075499cd1cbbc8c621ce26b70cea38	72	1 of 4	14
Mobile Device	d366366499b732449224224f24ffd8058059fa6f5903c819819f19fc603701ba	73	2 of 4	15
Cisco (AP)	8e5a38648b923b518e60a2c401dc2f96ae075499cd1cbbc8c621ce26b70cea38	74	3 of 4	16
Mobile Device	00000000000000000000000000000000000000000000000000000000000000000000000000000000	75	4 of 4	17

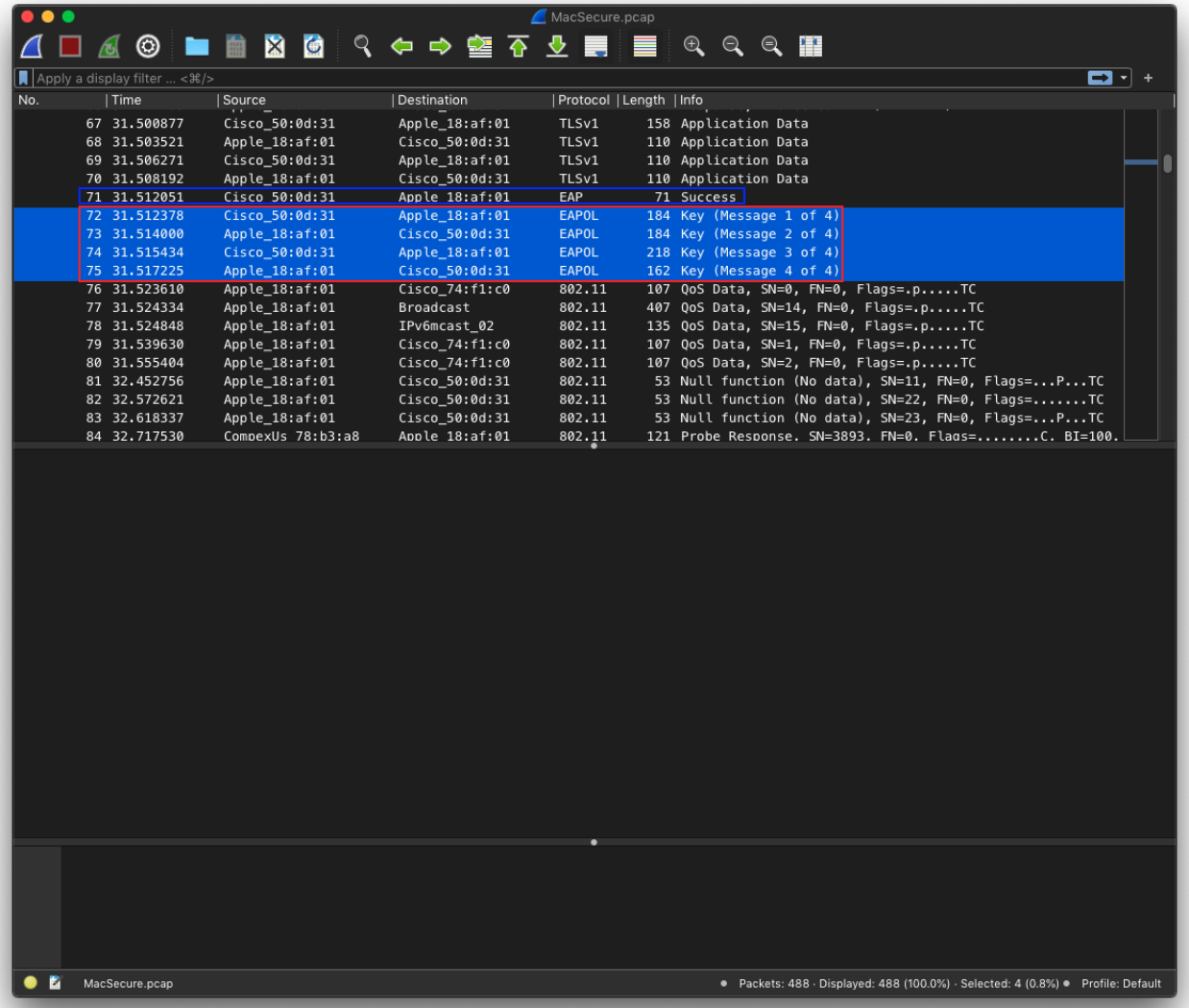

Figure 13: This figure highlights the 4 frames responsible for the 4-way handshake for establishing pair-wise transient keys

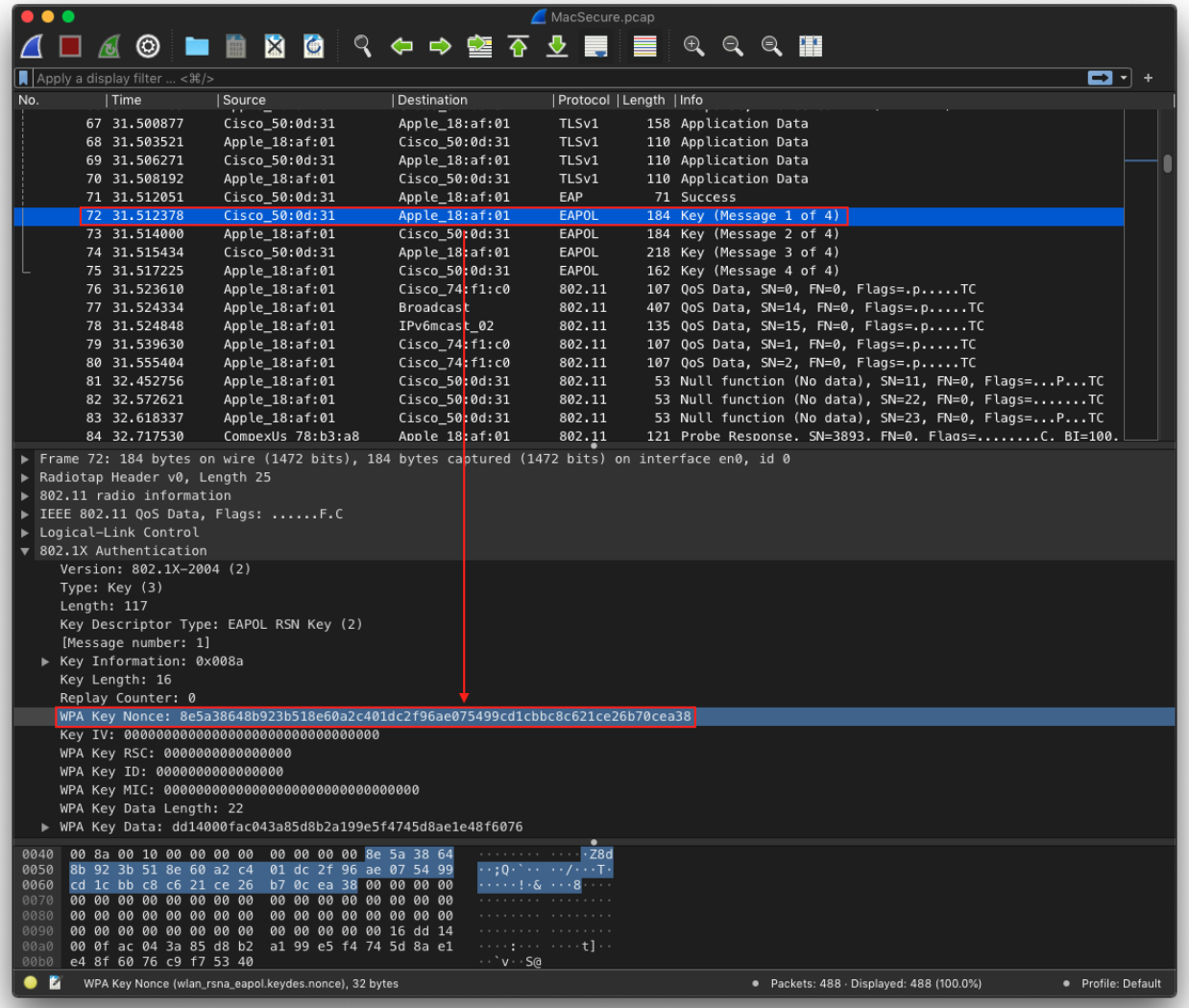

Figure 14: This figure highlights Frame 72, which is the first message in the 4 way handshake. Its respective WPA Nonce is highlighted at the bottom in a red box.

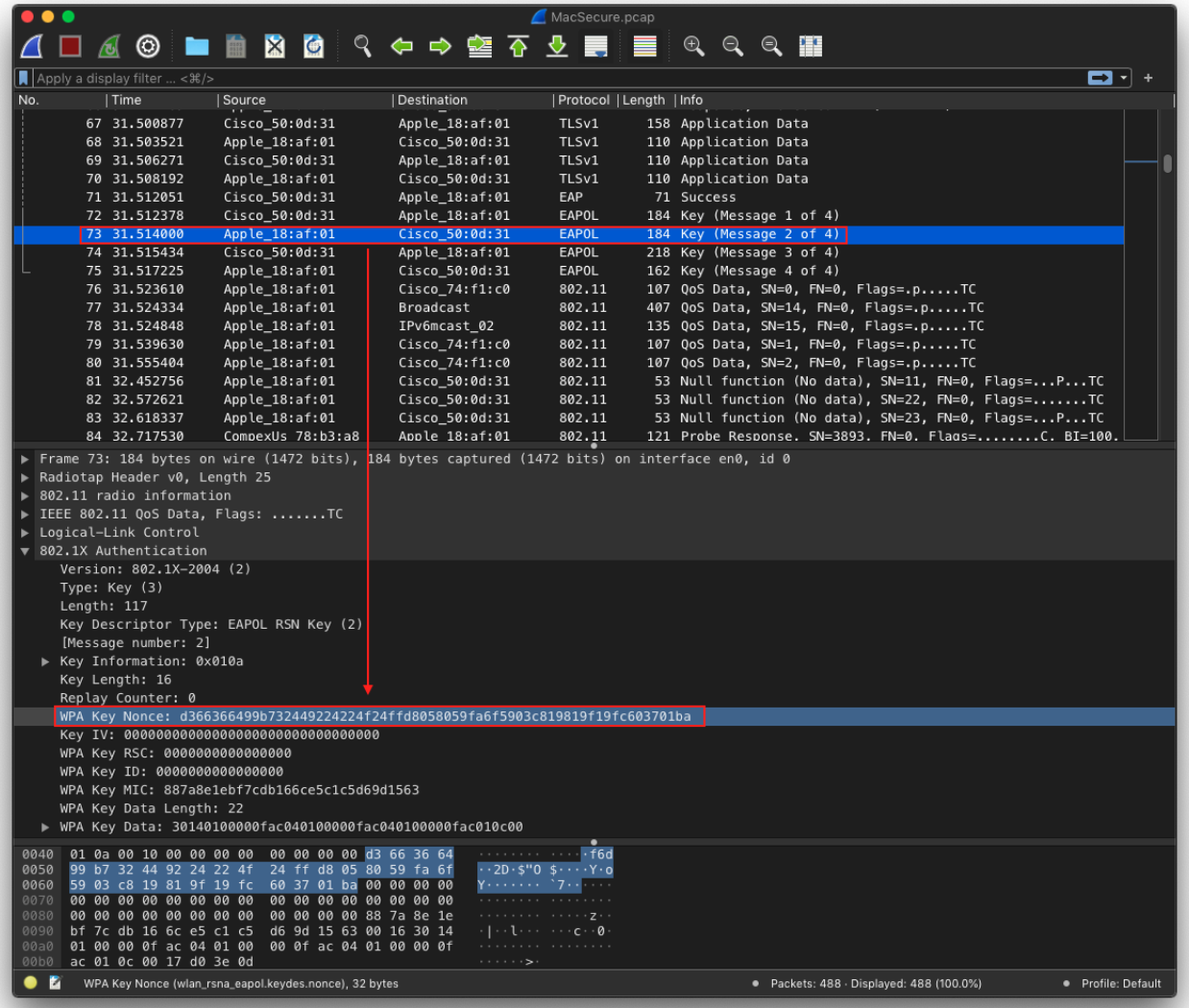

Figure 15: This figure highlights Frame 73, which is the second message in the 4 way handshake. Its respective WPA Nonce is highlighted at the bottom in a red box.

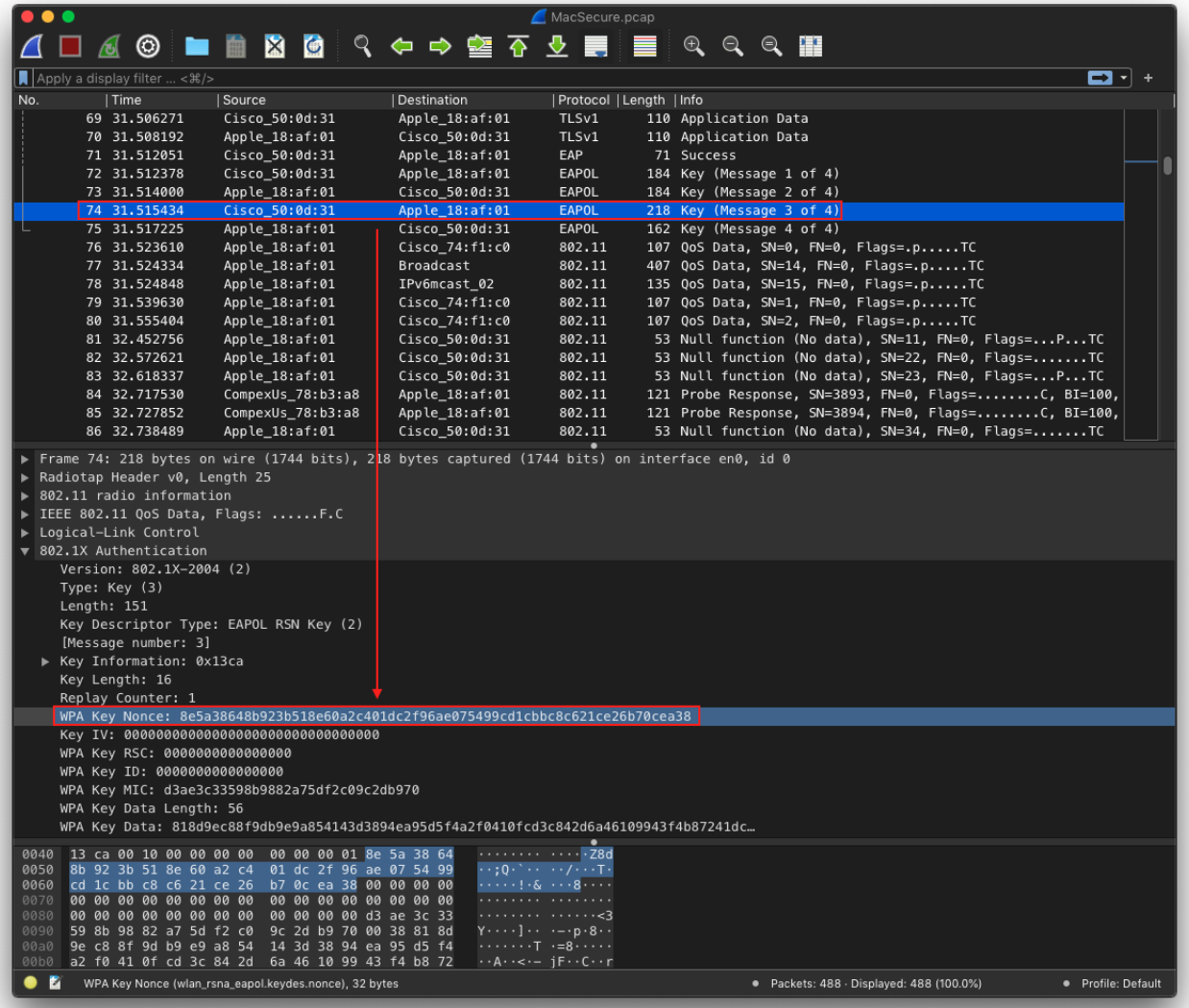

Figure 16: This figure highlights Frame 74, which is the third message in the 4 way handshake. Its respective WPA Nonce is highlighted at the bottom in a red box.

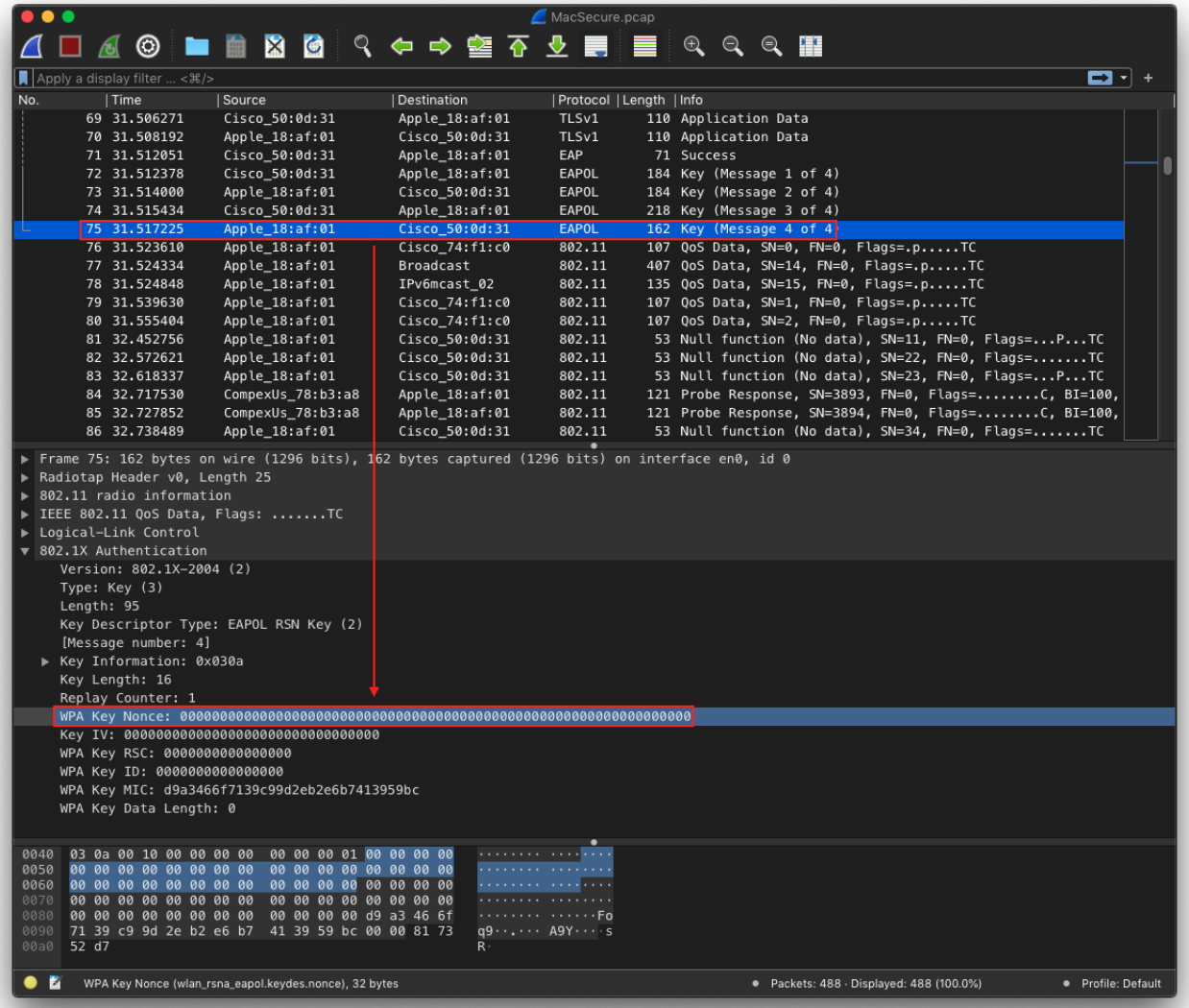

Figure 17: This figure highlights Frame 75, which is the last message in the 4 way handshake. Its respective WPA Nonce is highlighted at the bottom in a red box.

10) Why cannot we see DHCP message exchanges in the trace for address allocation?

We cannot see DHCP message exchanges in the trace for address allocation because once the authentication process has been established, the handshake has been completed, all subsequent messages exchanged between client (mobile device) and host (AP) are now encrypted. Therefore, we cannot see the DHCP messages. In fact, we cannot properly read any encrypted message sent between client and the access point.
No screenshot (or screenshots are) required for this question.

MacConnect Trace

1) Type “Bootp” in the filter field to display only DHCP related messages. A DHCP NAK message by the DHCP server is sent when a requested address is not available. From DHCP request message 77 – 101, what is the requested address by the mobile? What is the IP address allocated to the mobile eventually?

The requested address by the mobile device is *172.17.147.60*. This is shown in figure 18 and 19, below. After repeated requests, the mobile device is eventually allocated an IP address of *172.17.22.223*. This is shown in figure 20, below.

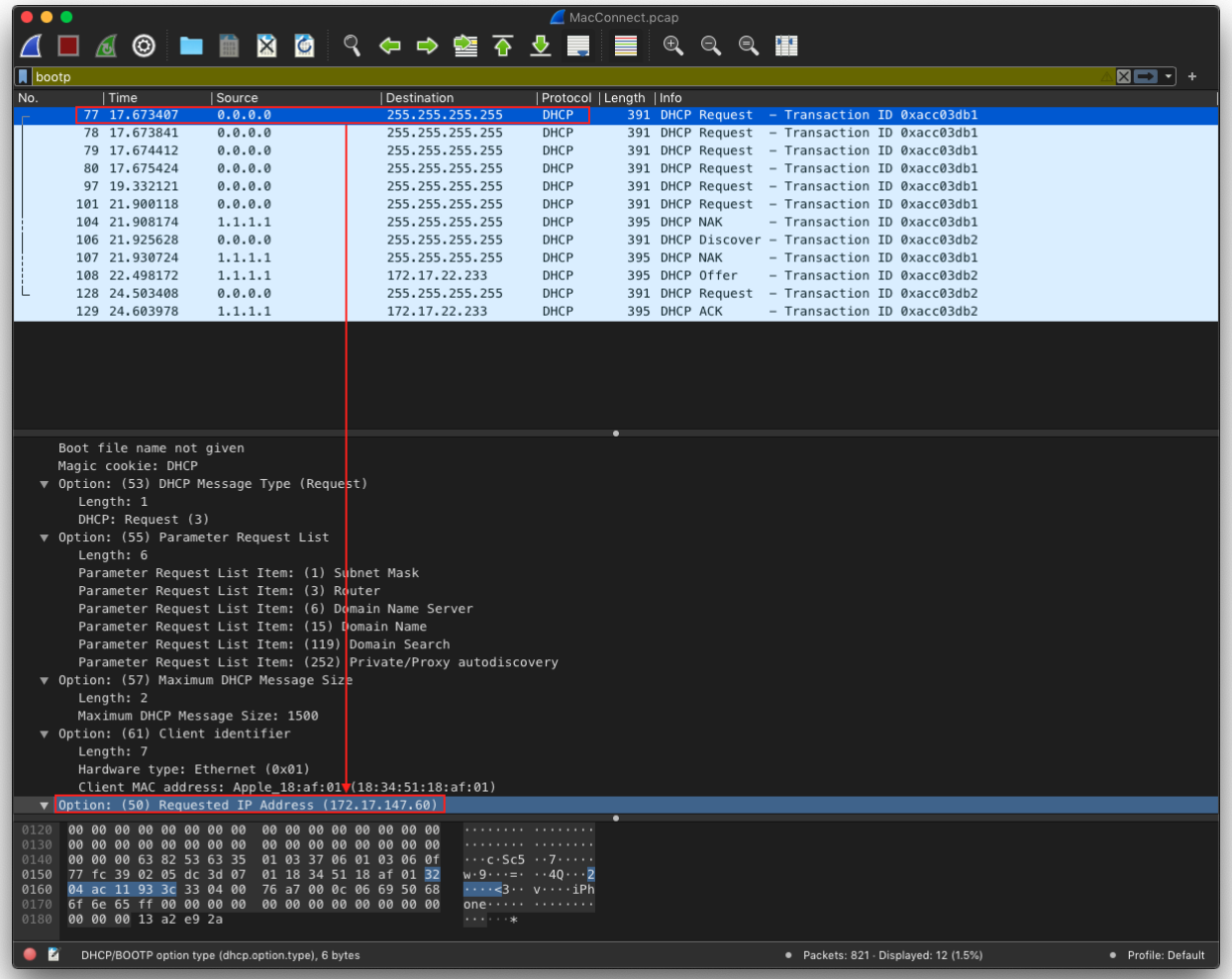

Figure 18: This figure shows that the 77th packet sent by the mobile device requests an IP address of 172.17.147.60. This is highlighted in red at the bottom of the figure.

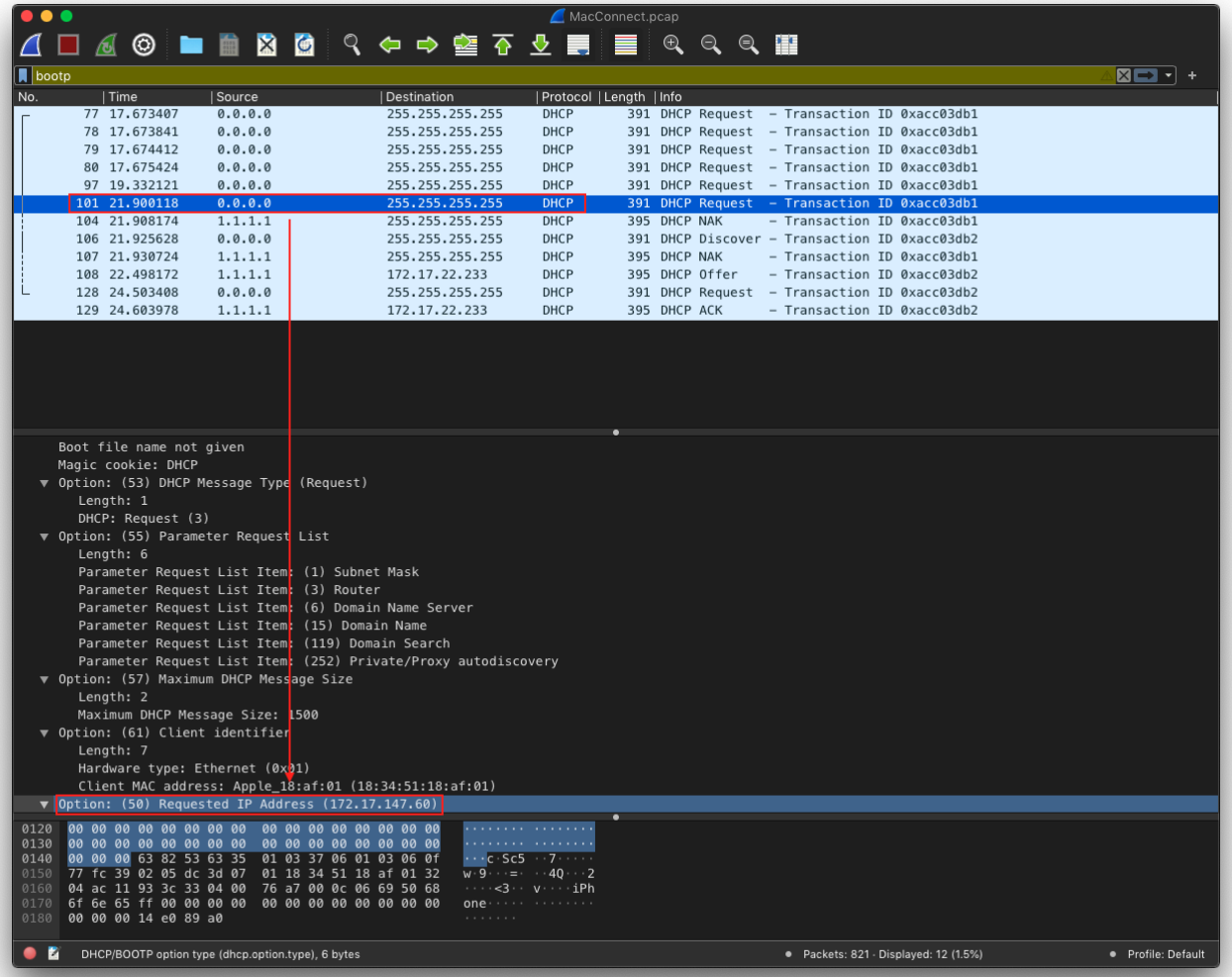

Figure 19: This figure shows that the 101st packet sent by the mobile device requests an IP address of 172.17.147.60. This highlighted in the red box at the bottom of the figure.

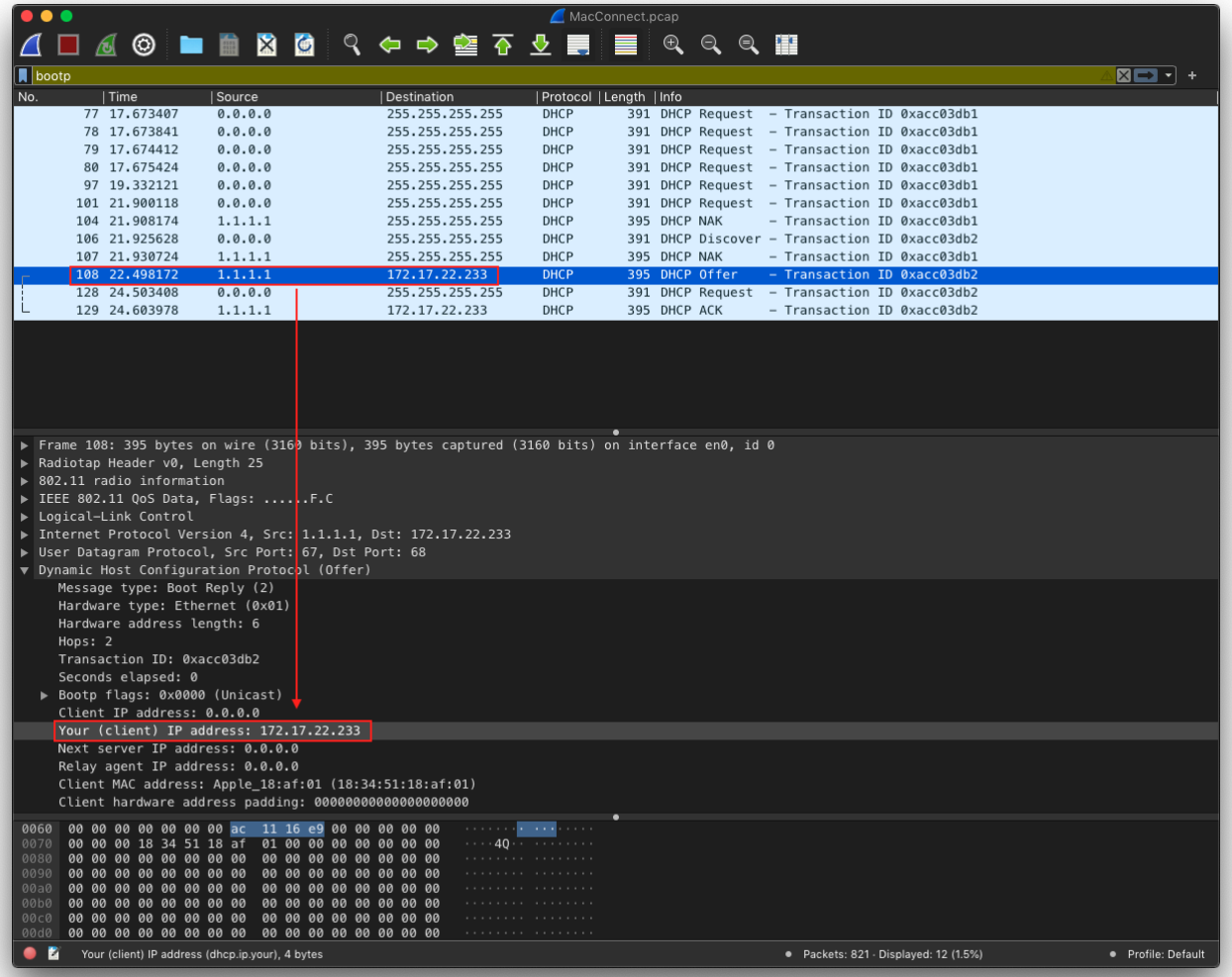

Figure 20: This figure shows that the mobile device is eventually allocated an IP address of 172.17.22.233. This is information is highlighted in red at the bottom of the figure.

2) What is the purpose of the gratuitous ARP in frame 136?

The gratuitous ARP in frame 136, shown in the figure below, is a way for the mobile device (client) to update its IP to MAC mapping to the entire network. The gratuitous ARP in frame 136 is not prompted by an ARP request, but sends one out anyways so the IP to MAC mapping is updated in the entire network. The purpose of an ARP, whether it is gratuitous or not, is to detect local IP address conflicts between devices, and to tell other devices on the network to update their IP to MAC mapping.

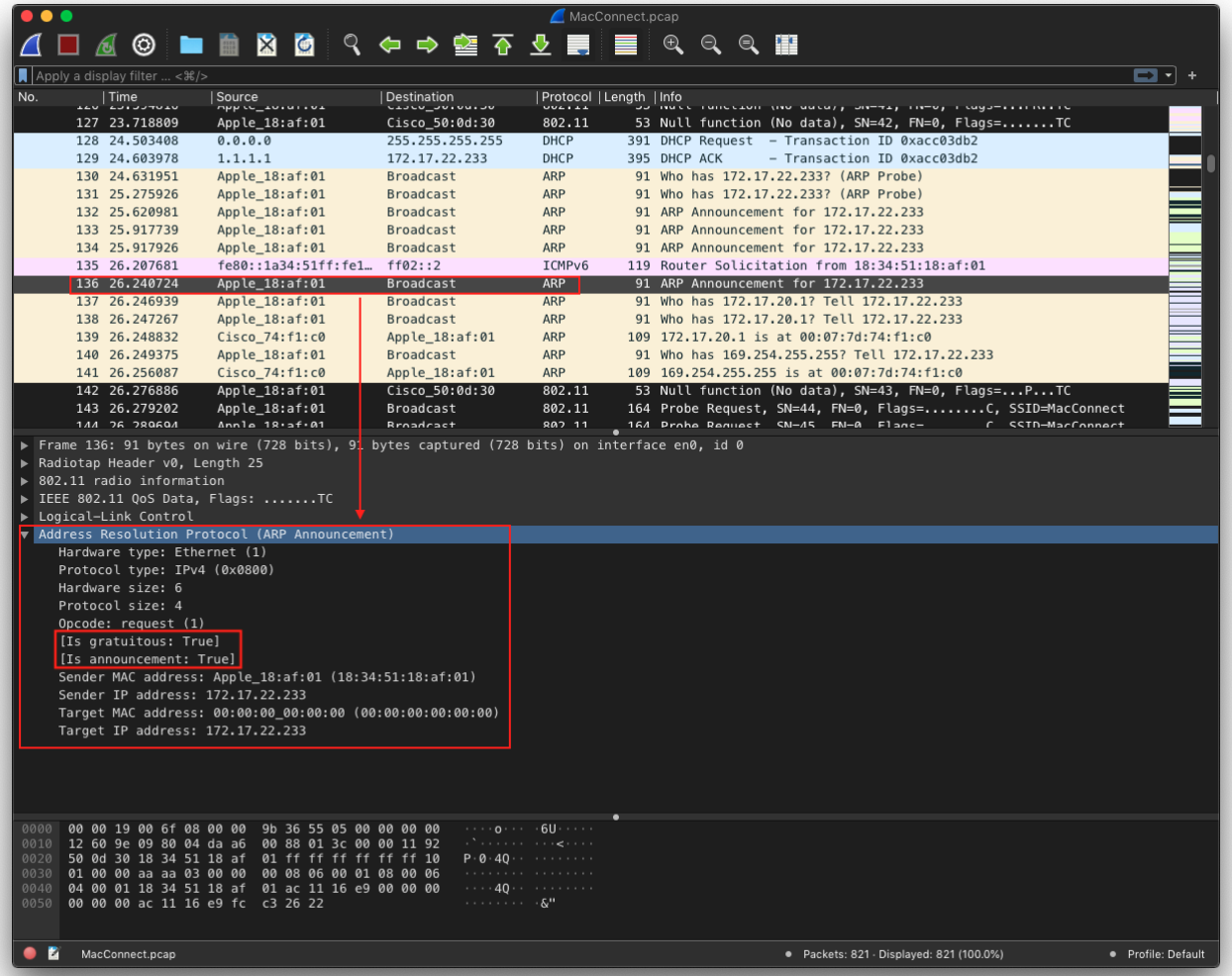

Figure 21: This figure highlights frame 136 and shows more details about the ARP in frame 136. In the red box at the bottom of the figure, you can see that this frame is a gratuitous announcement for the entire network to update their IP to MAC mapping.

3) Type “SSL” (or “ssl”) in the filter field to display SSL messages that are used to authenticate the user. From the frame 243 – 273, identify the type of messages exchanged and the values of the angle bracket (<>) in reference to Figure 1 that describes the connection setup process in SSL.

Frame #	SSL Client	SSL Server
243: Client Hello	**Client Hello** I want to establish secure connection. I support ***<Figure 22>*** version of SSL and ***<Figure 23>*** these ciphers	
250: Server Hello		**Server Hello** Ok, I initially accept request. I have chosen ***<Figure 24>*** version of SSL and ***<Figure 24>*** cipher suite
		Server’s Certificate (Optional)
		Server Key Exchange (Optional) Here is my public key (If I don’t have certificate)
257: Certificate		**Client Certificate Request (Optional)** I want to authenticate you. Send me your certificate signed by ***<Figure 25>*** CA
257: Server Hello Done		**Server Hello Done**
	Client’s Certificate (Optional)	
260: Client Key Exchange	**Client Key Exchange** I am sending you more parameters I will encrypt them by your public key	
	Certificate Verify (Optional) I will sign some information by using private key that corresponds to my certificate. Thus, you can be sure that I am the owner of the certificate	
262: Change Cipher Spec	**Change Cipher Spec** The next message from me will be encrypted	
263: Encrypted Handshake Message	**Client Finished (Encrypted)**	

267: Change Cipher Spec		**Change Cipher Spec** The next message from me will be encrypted
267: Encrypted Handshake Message		**Server Finished (Encrypted)**
269, 272, 272: Application Data	**Application's Data (Encrypted)**	**Application's Data (Encrypted)**

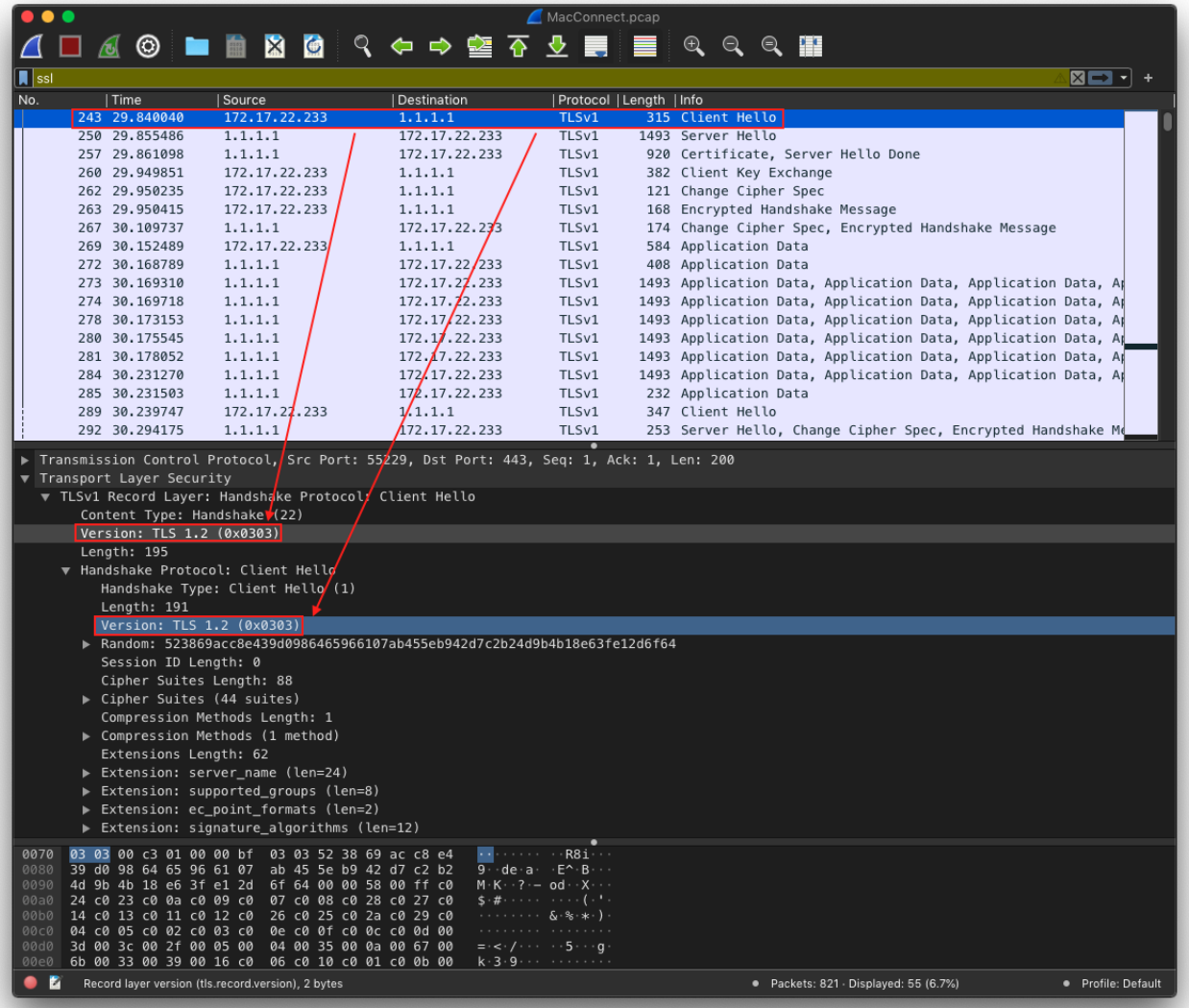

Figure 22: This figure shows information pertaining to frame 243. Frame 243 is Client Hello. The red boxes in the middle highlight the version of SSL that is supported by the client. In this case it is up to ***TLS 1.2****.*

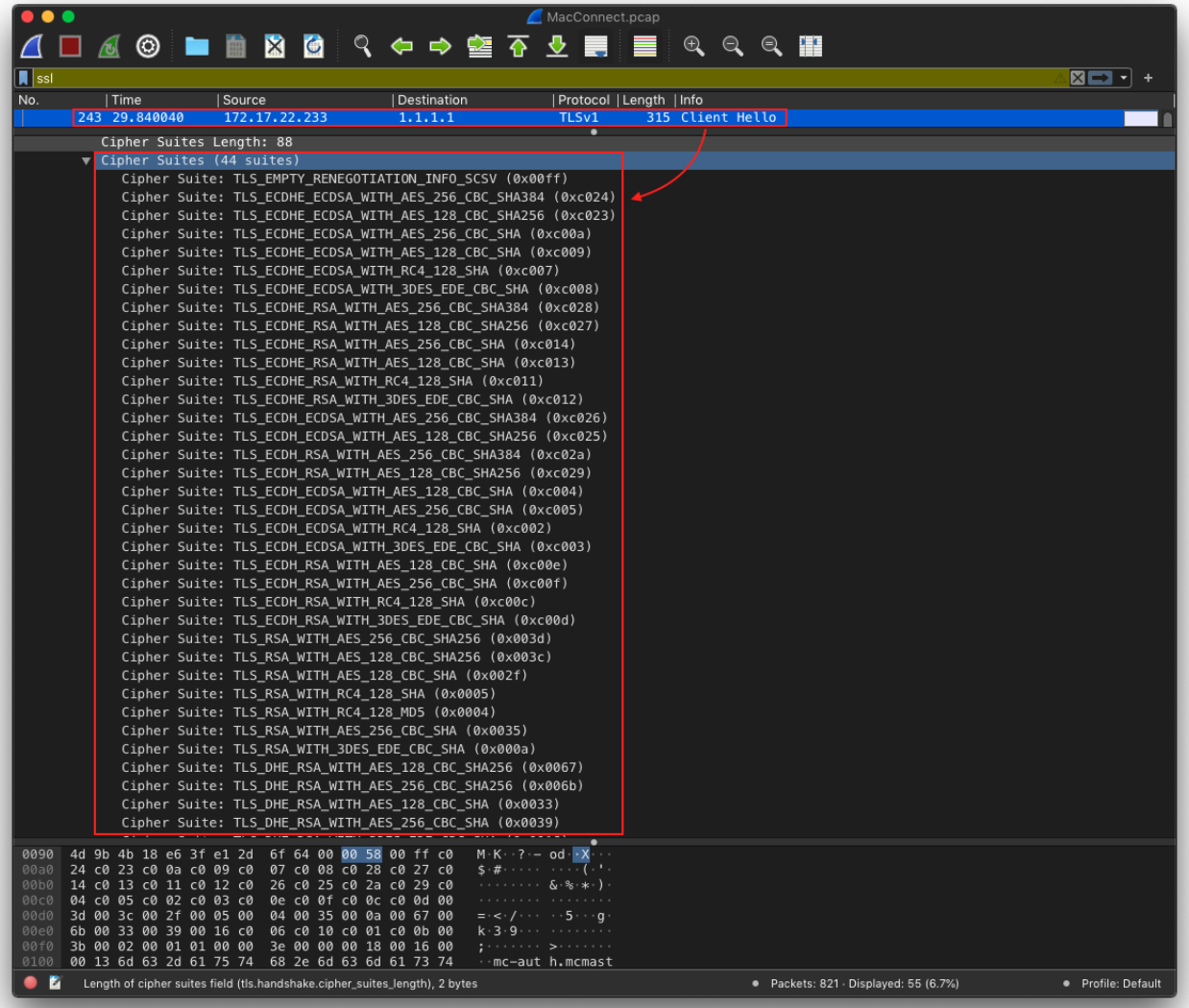

*Figure 23: This figure shows information pertaining to frame 243. Frame 243 is Client Hello. The huge red box in the middle highlights all the ciphers that are supported by the client. There are **44 cipher suites** in total, refer to the figure for them.*

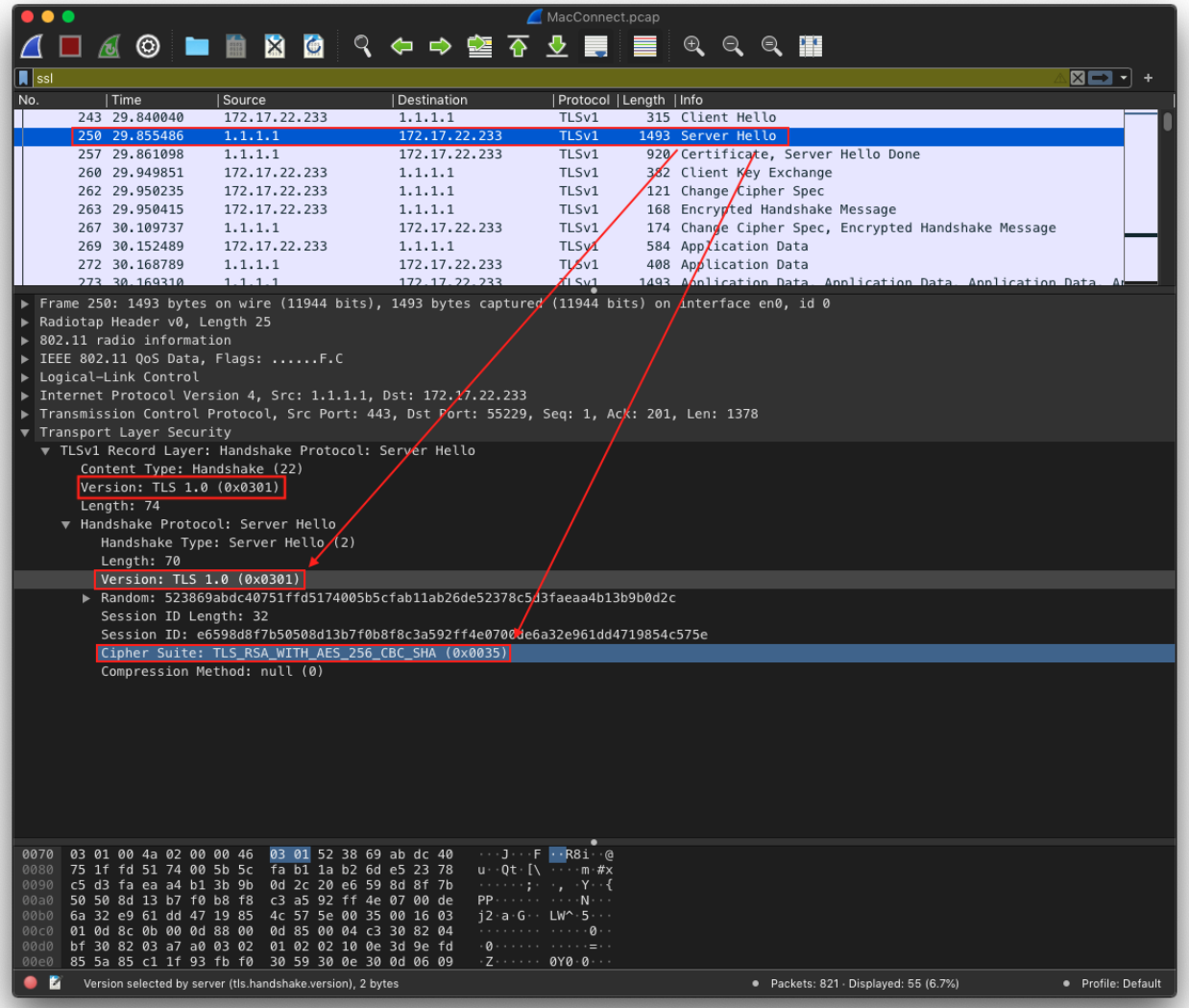

*Figure 24: This figure corresponds to frame 250. Frame 250 is Server Hello and contains information about the Server Hello response. The SSL Server has chosen to use SSL version **TLS 1.0**. This is evident by the two red boxes in the middle of the figure. The SSL Server has chosen to use the cipher suite: **TLS_RSA_WITH_AES_256_CBC_SHA**. This is evident by the red box at the bottom of the figure.*

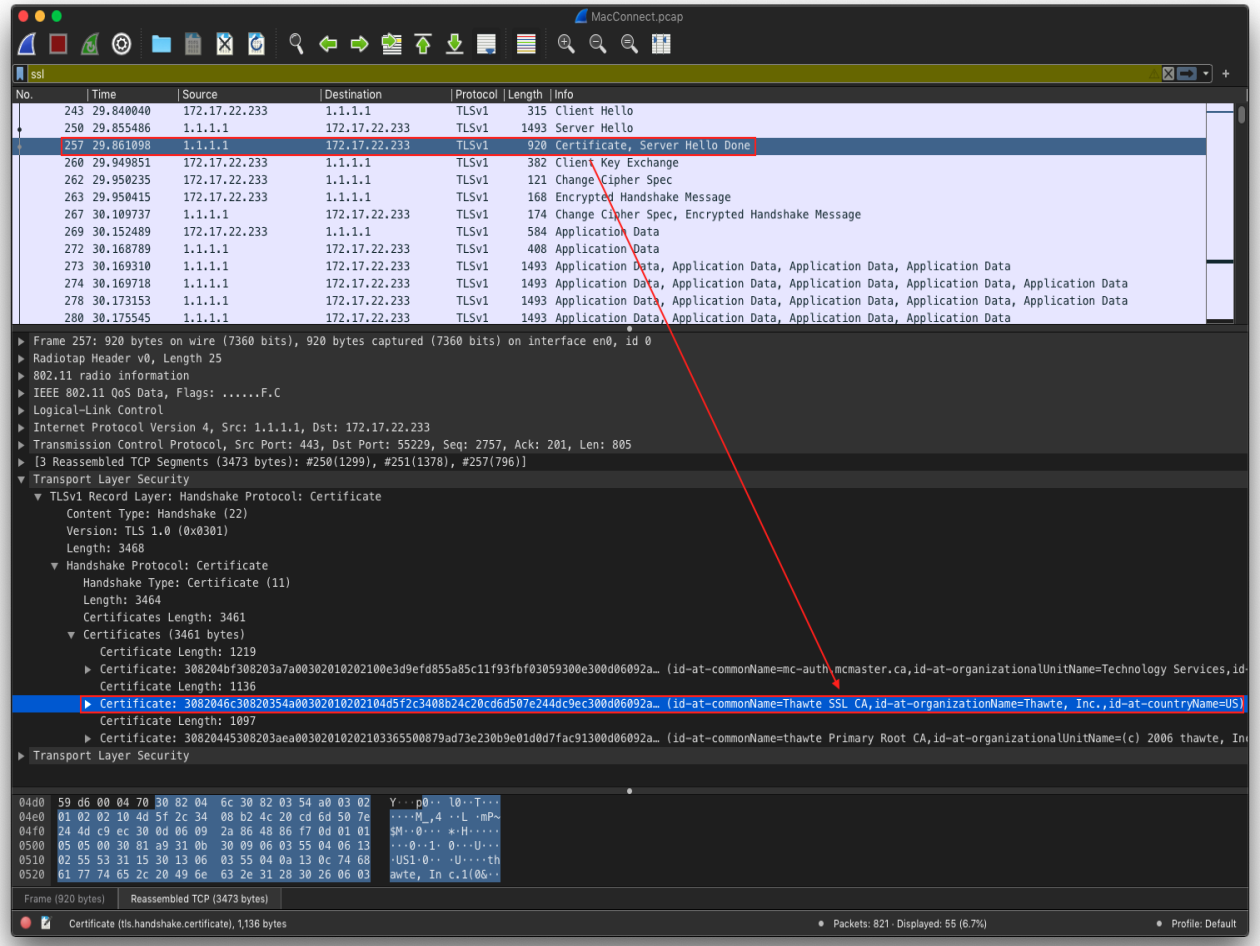

Figure 25: This figure corresponds to frame 257. Frame 257 pertains to the Certificate and Server Hello Done. The server wants to authenticate the client via a client certificate request. This frame tells the client to send the server its certificate signed by the entity: ***Thawte SSL CA***