
ATTACK
DEFENSE
by PentesterAcademy

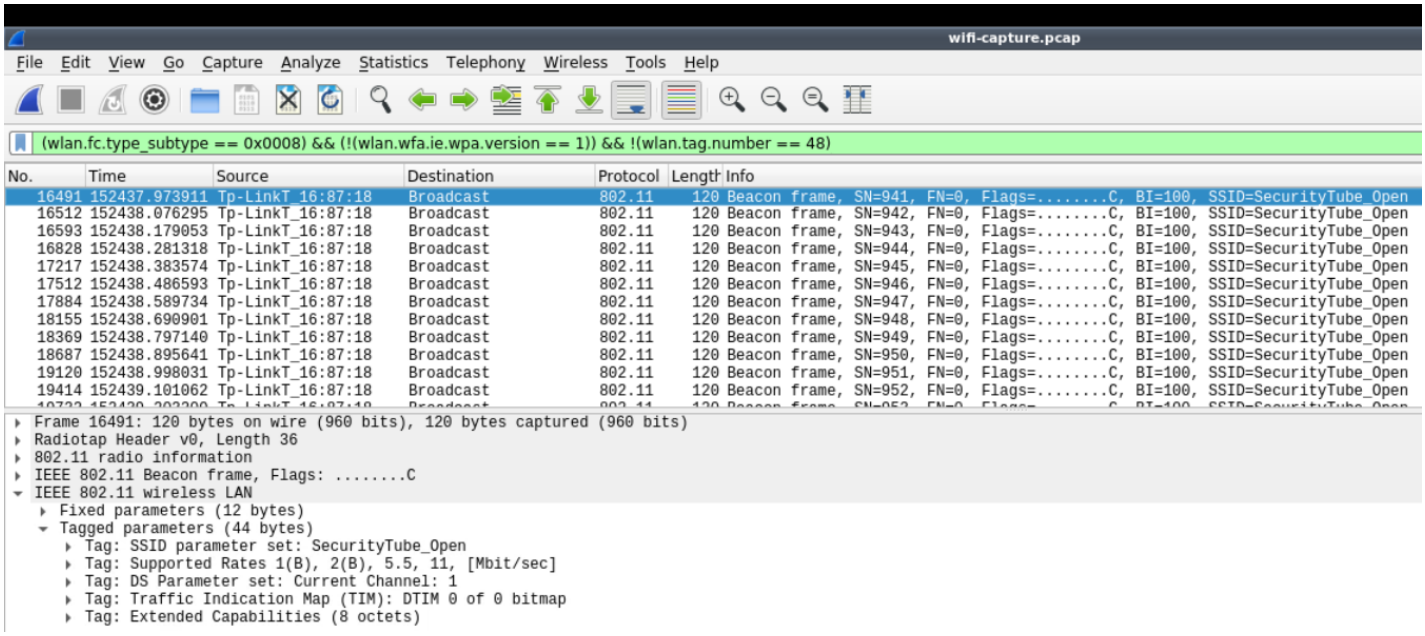
Name	WiFi Security: Traffic Analysis I
URL	https://www.attackdefense.com/challengedetails?cid=1141
Type	WiFi Pentesting: Traffic Analysis

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

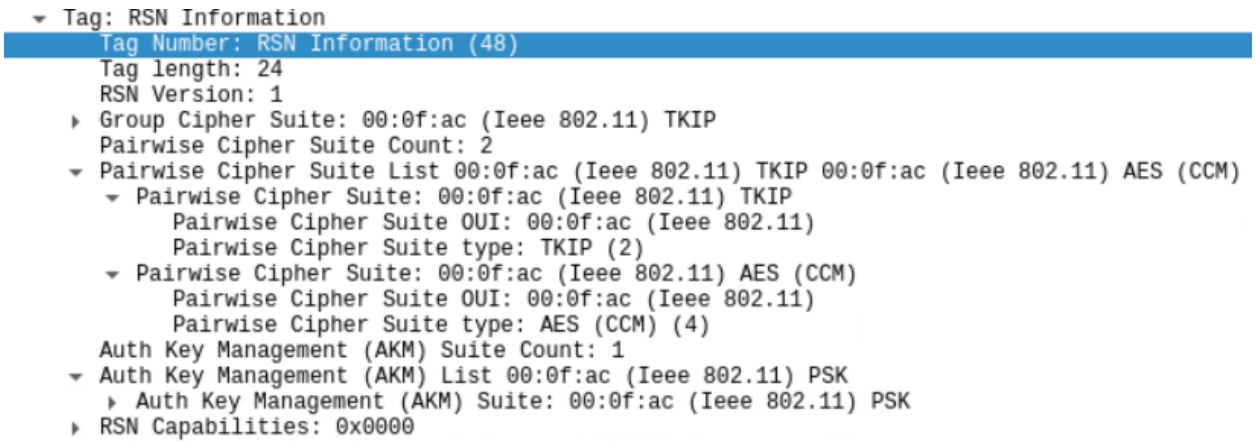
Q1. What is the name of the Open (No Security) SSID present in the packet dump?

A. SecurityTube_Open

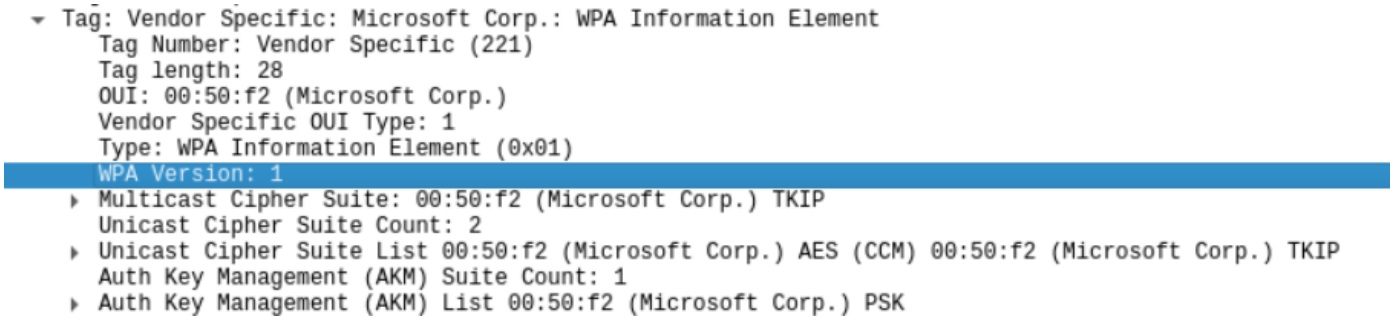
Filter: (wlan.fc.type_subtype == 0x0008) && (!(wlan.wfa.ie.wpa.version == 1)) && !(wlan.tag.number == 48)



Here tag 48 refers to RSN IE.



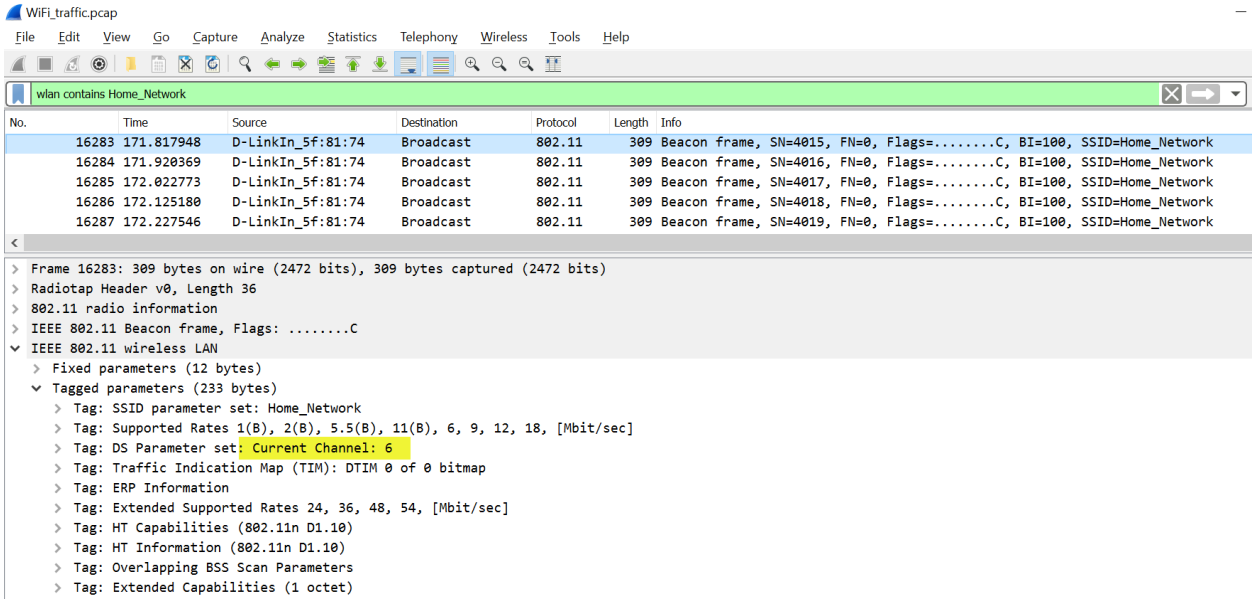
And, wlan.wfa.ie.wpa.version == 1 is to filter put a vendor IE



Q2. The SSID 'Home_Network' is operating on which channel?

A. 6

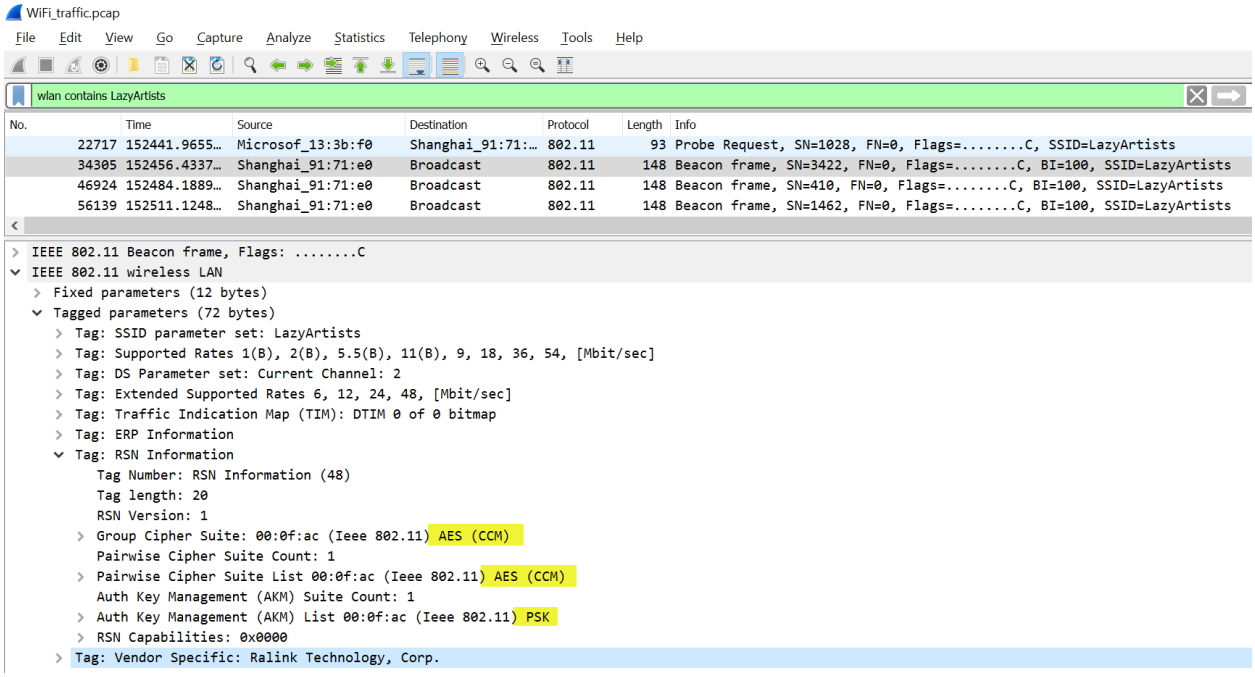
Filter: wlan contains Home_Network



Q3. Which security mechanism is configured for SSID 'LazyArtists'? Your options are: OPEN, WPA-PSK, WPA2-PSK.

A. WPA2-PSK

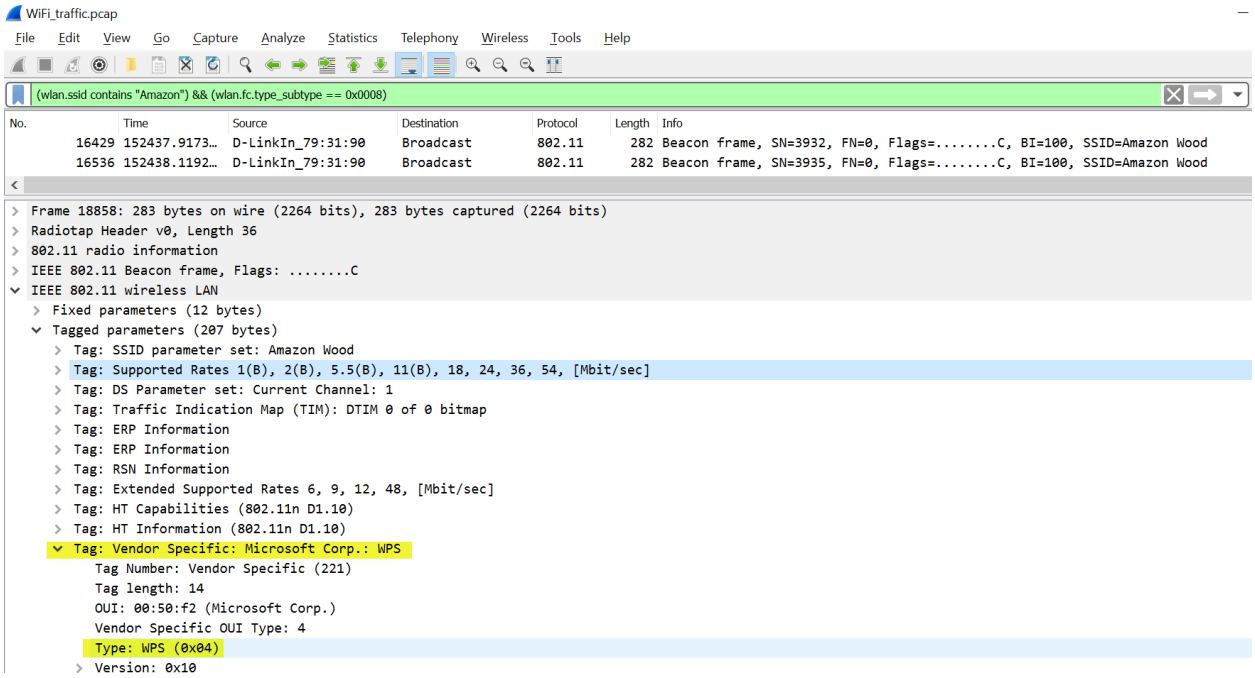
Filter: wlan contains LazyArtists



Q4. Is WiFi Protected Setup (WPS) enabled on SSID 'Amazon Wood'? State Yes or No.

A. Yes

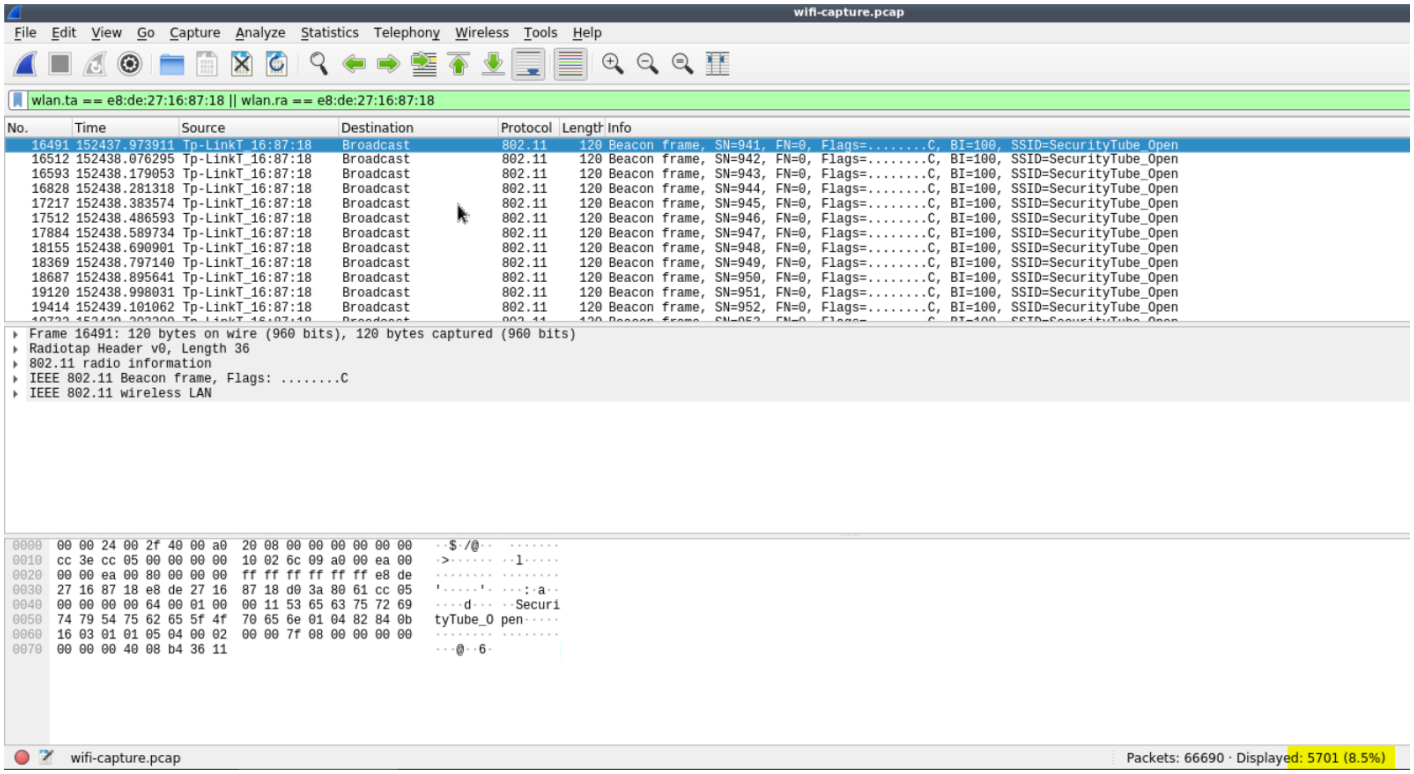
Filter: (wlan.ssid contains "Amazon") && (wlan.fc.type_subtype == 0x0008)



Q5. What is the total count of packets which were either transmitted or received by the device with MAC e8:de:27:16:87:18?

A: 5701

Filter: (wlan.ta == e8:de:27:16:87:18) || (wlan.ra == e8:de:27:16:87:18)

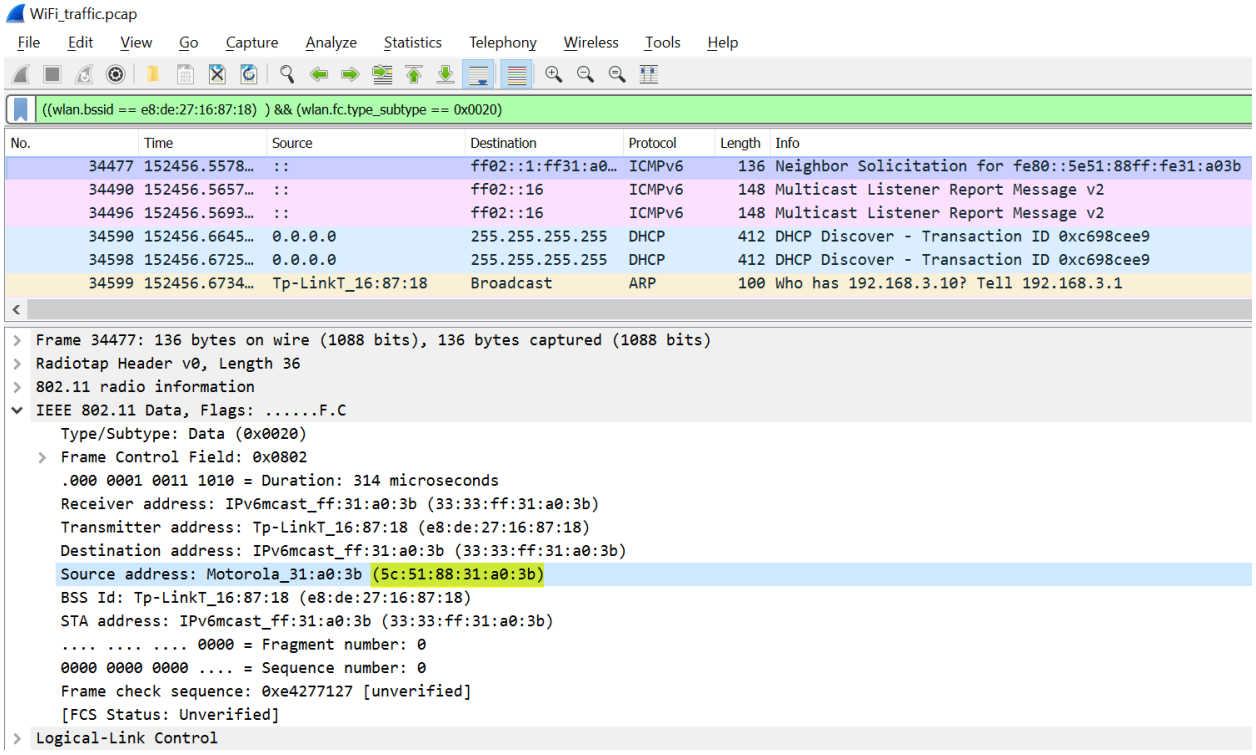


Q6. What is the MAC address of the station which exchanged data packets with SSID 'SecurityTube_Open'?

A: 5c:51:88:31:a0:3b

SSID SecurityTube_Open is hsoted on BSSID e8:de:27:16:87:18.

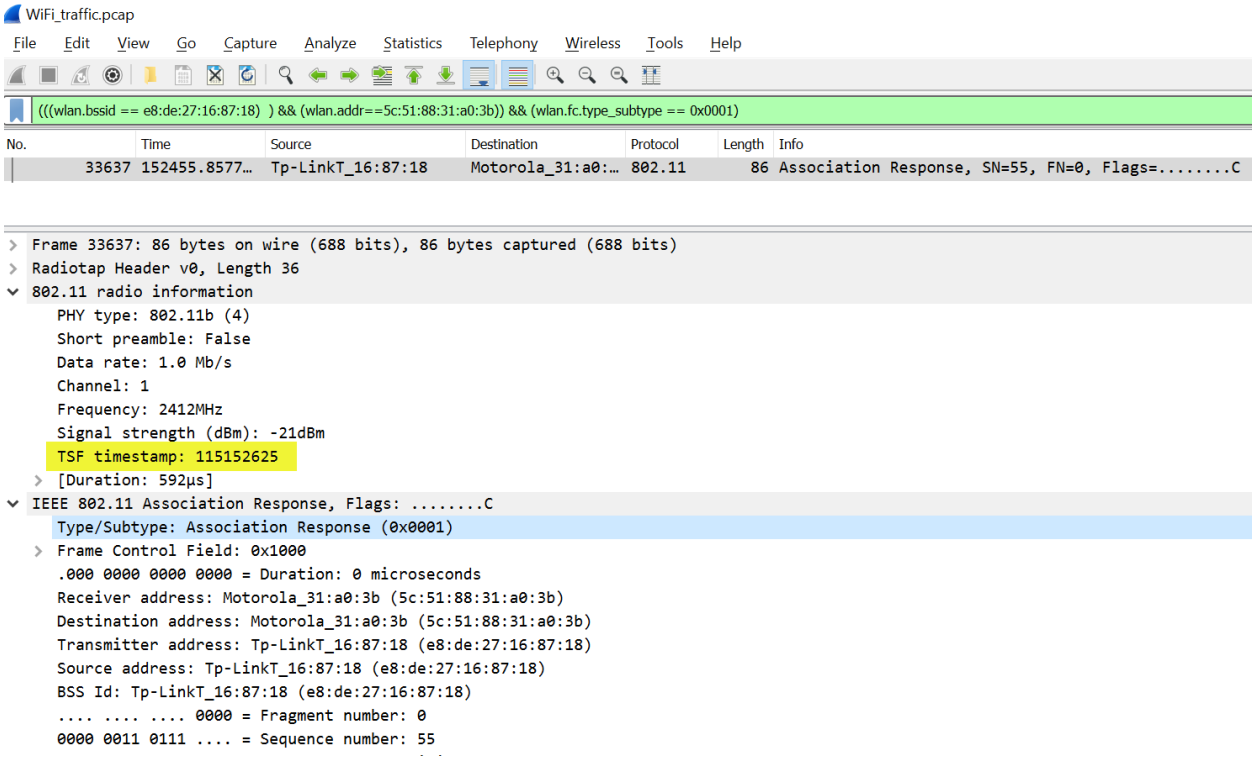
Filter: ((wlan.bssid == e8:de:27:16:87:18)) && (wlan.fc.type_subtype == 0x0020)



Q7. From the last question, we know that a station was connected to SSID 'SecurityTube_Open'. Provide TSF timestamp of the association response sent from the access point to this station.

A. 115152625

Filter: (((wlan.bssid == e8:de:27:16:87:18)) && (wlan.addr==5c:51:88:31:a0:3b)) && (wlan.fc.type_subtype == 0x0001)



References:

1. Wireshark (https://www.wireshark.org/)
2. Pentester Academy WiFi course (https://www.pentesteracademy.com/course?id=9)