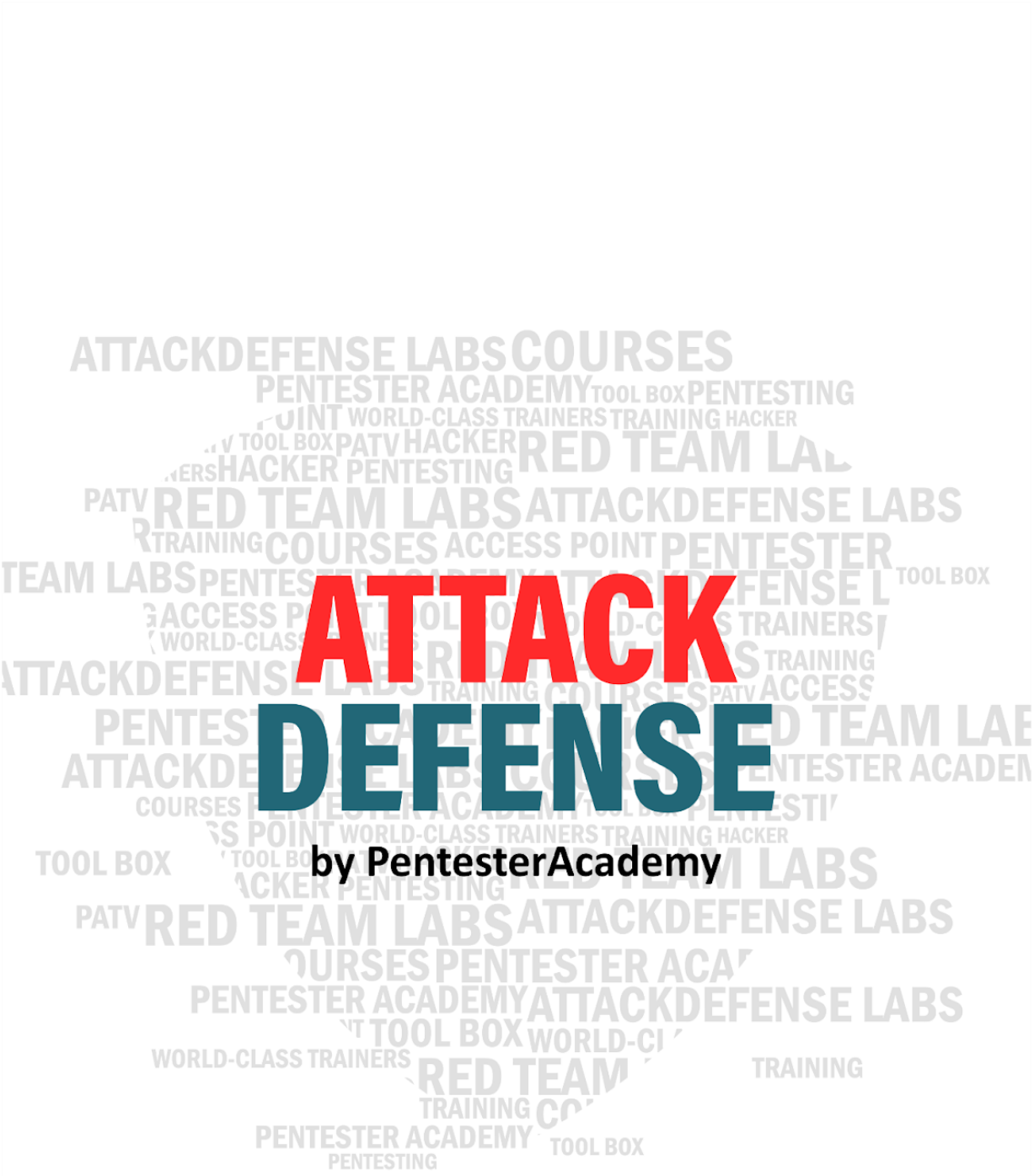

ATTACK
DEFENSE
by PentesterAcademy

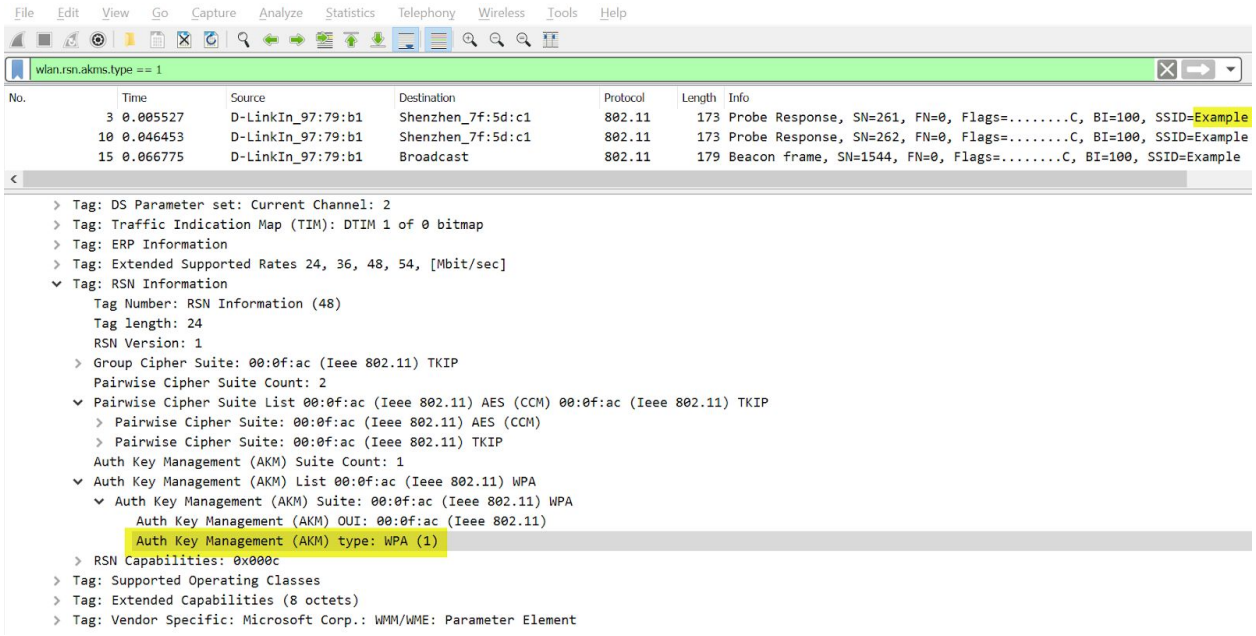
Name	WiFi Security: Traffic Analysis III
URL	https://www.attackdefense.com/challengedetails?cid=1142
Type	WiFi Pentesting: Traffic Analysis

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 SSID which is using WPA/WPA2-Enterprise security scheme?

A. Example

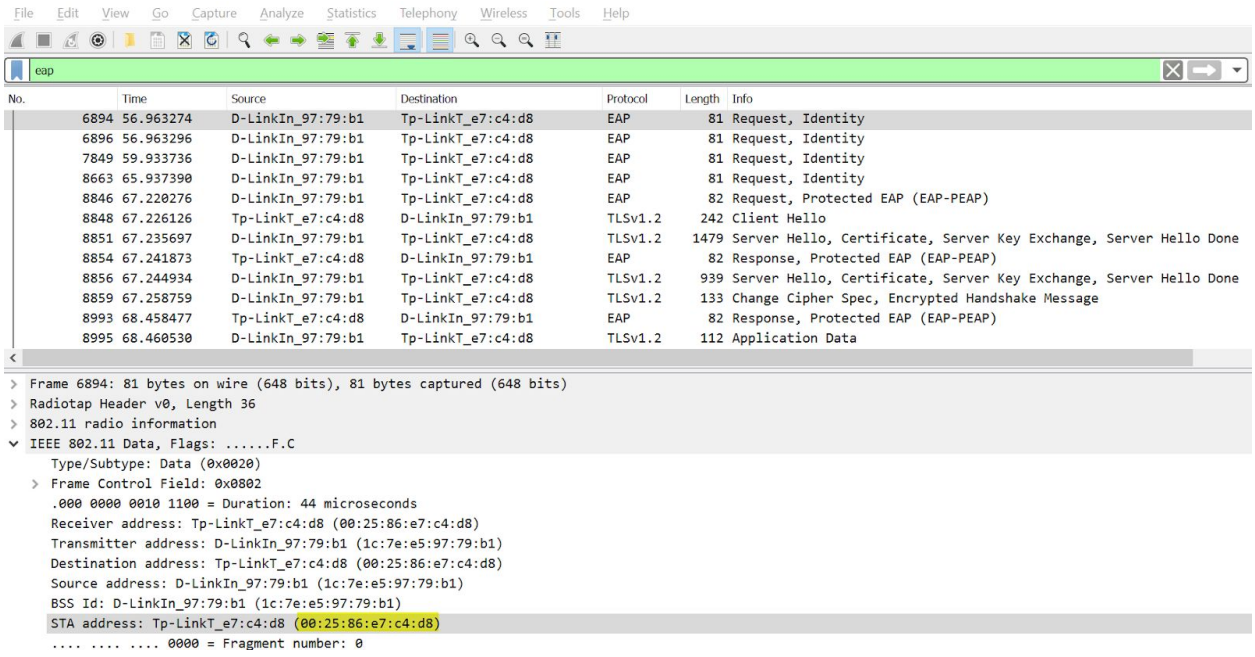
Filter: wlan.rsn.akms.type == 1



Q2. A device tried to connect to the SSID mentioned in Q1. What is the MAC address of that device?

A. 00:25:86:e7:c4:d8

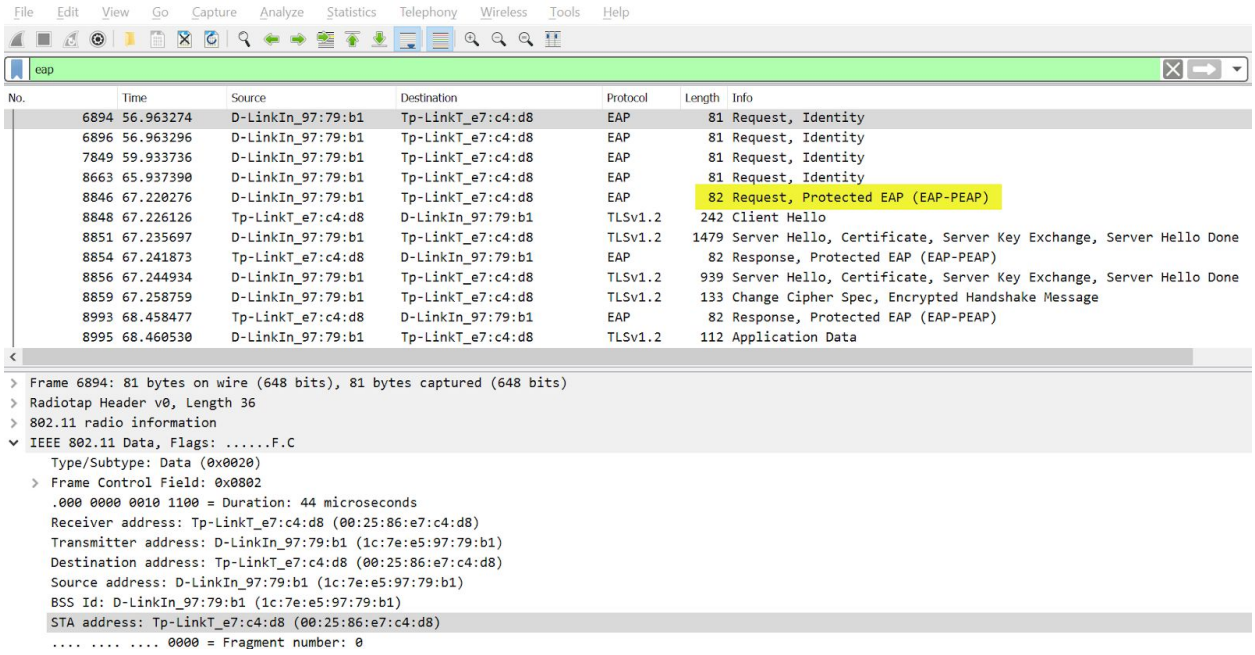
Filter: eap



Q3. What kind of EAP (Extended Authentication Protocol) is used by the SSID? Provide answer in form of abbreviation.

A. PEAP

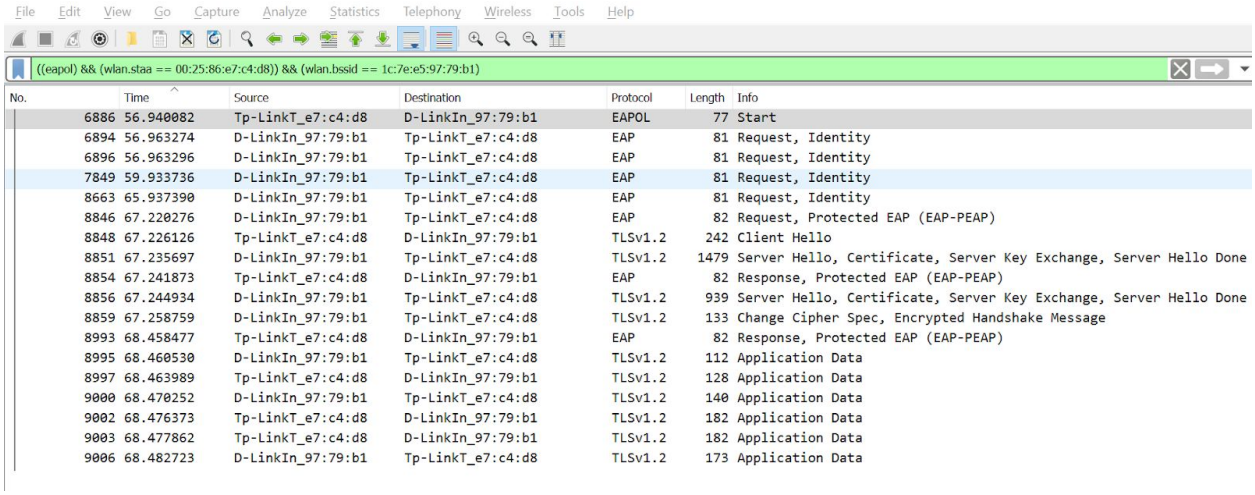
Filter: eap



Q4. A device tried to connect to the SSID mentioned in Q1. Was the connection attempt successful? State Yes or No.

A. No

Filter: eapol

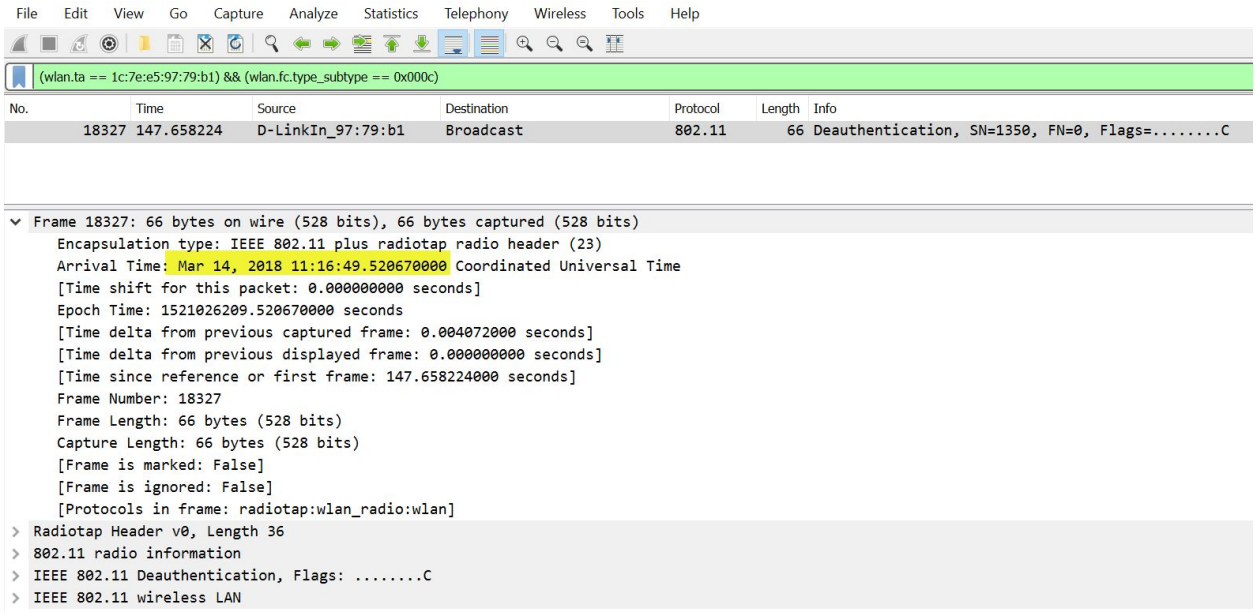


There were no 4-way handshake packets after the 802.1x packets which means that the device was not able to connect.

Q5. A deauthentication broadcast message was transmitted by the BSSID 1c:7e:e5:97:79:b1. Provide the time in UTC in DD/MM/YYYY HH:MM:SS format.

A. 14/03/2018 11:16:49

Filter: (wlan.ta == 1c:7e:e5:97:79:b1) && (wlan.fc.type_subtype == 0x000c)



References:

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