

[illegible]

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

The image shows a Wireshark packet capture analysis. The filter bar at the top is set to `wlan.rsn.akms.type == 1`. The packet list shows three packets: a Probe Response (SN=261), another Probe Response (SN=262), and a Beacon frame (SN=1544). The details pane for the selected packet (15) shows the following structure:

- Tag: DS Parameter set: Current Channel: 2
- Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
- Tag: ERP Information
- Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
- Tag: RSN Information
 - Tag Number: RSN Information (48)
 - Tag length: 24
 - RSN Version: 1
 - Group Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
 - Pairwise Cipher Suite Count: 2
 - Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM) 00:0f:ac (Ieee 802.11) TKIP
 - Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
 - Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) TKIP
 - Auth Key Management (AKM) Suite Count: 1
 - Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA
 - Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) WPA
 - Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
 - Auth Key Management (AKM) type: WPA (1)
 - RSN Capabilities: 0x000c
- Tag: Supported Operating Classes
- Tag: Extended Capabilities (8 octets)
- Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

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

No.	Time	Source	Destination	Protocol	Length	Info
6894	56.963274	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
6896	56.963296	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
7849	59.933736	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
8663	65.937390	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
8846	67.220276	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	82	Request, Protected EAP (EAP-PEAP)
8848	67.226126	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	TLSv1.2	242	Client Hello
8851	67.235697	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	1479	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8854	67.241873	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	EAP	82	Response, Protected EAP (EAP-PEAP)
8856	67.244934	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	939	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8859	67.258759	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	133	Change Cipher Spec, Encrypted Handshake Message
8993	68.458477	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	EAP	82	Response, Protected EAP (EAP-PEAP)
8995	68.460530	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	112	Application Data

< Frame 6894: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
▼ IEEE 802.11 Data, Flags:F.C
Type/Subtype: Data (0x0020)
> Frame Control Field: 0x0802
 .000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Tp-LinkT_e7:c4:d8 (00:25:86:e7:c4:d8)
Transmitter address: D-LinkIn_97:79:b1 (1c:7e:e5:97:79:b1)
Destination address: Tp-LinkT_e7:c4:d8 (00:25:86:e7:c4:d8)
Source address: D-LinkIn_97:79:b1 (1c:7e:e5:97:79:b1)
BSS Id: D-LinkIn_97:79:b1 (1c:7e:e5:97:79:b1)
STA address: Tp-LinkT_e7:c4:d8 (00:25:86:e7:c4:d8)
 0000 = Fragment number: 0

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

A. PEAP

Filter: eap



No.	Time	Source	Destination	Protocol	Length	Info
6894	56.963274	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
6896	56.963296	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
7849	59.933736	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
8663	65.937390	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
8846	67.220276	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	82	Request, Protected EAP (EAP-PEAP)
8848	67.226126	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	TLSv1.2	242	Client Hello
8851	67.235697	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	1479	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8854	67.241873	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	EAP	82	Response, Protected EAP (EAP-PEAP)
8856	67.244934	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	939	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8859	67.258759	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	133	Change Cipher Spec, Encrypted Handshake Message
8993	68.458477	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	EAP	82	Response, Protected EAP (EAP-PEAP)
8995	68.460530	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	112	Application Data

> Frame 6894: 81 bytes on wire (648 bits), 81 bytes captured (648 bits)
> Radiotap Header v0, Length 36
> 802.11 radio information
▼ IEEE 802.11 Data, Flags:F.C
Type/Subtype: Data (0x0020)
> Frame Control Field: 0x0002
.000 0000 0010 1100 = Duration: 44 microseconds
Receiver address: Tp-LinkT_e7:c4:d8 (00:25:86:e7:c4:d8)
Transmitter address: D-LinkIn_97:79:b1 (1c:7e:e5:97:79:b1)
Destination address: Tp-LinkT_e7:c4:d8 (00:25:86:e7:c4:d8)
Source address: D-LinkIn_97:79:b1 (1c:7e:e5:97:79:b1)
BSS Id: D-LinkIn_97:79:b1 (1c:7e:e5:97:79:b1)
STA address: Tp-LinkT_e7:c4:d8 (00:25:86:e7:c4:d8)
.... 0000 = Fragment number: 0

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

No.	Time	Source	Destination	Protocol	Length	Info
6886	56.940082	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	EAPOL	77	Start
6894	56.963274	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
6896	56.963296	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
7849	59.933736	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
8663	65.937390	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	81	Request, Identity
8846	67.220276	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	EAP	82	Request, Protected EAP (EAP-PEAP)
8848	67.226126	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	TLSv1.2	242	Client Hello
8851	67.235697	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	1479	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8854	67.241873	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	EAP	82	Response, Protected EAP (EAP-PEAP)
8856	67.244934	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	939	Server Hello, Certificate, Server Key Exchange, Server Hello Done
8859	67.258759	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	133	Change Cipher Spec, Encrypted Handshake Message
8993	68.458477	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	EAP	82	Response, Protected EAP (EAP-PEAP)
8995	68.460530	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	112	Application Data
8997	68.463989	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	TLSv1.2	128	Application Data
9000	68.470252	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	140	Application Data
9002	68.476373	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	TLSv1.2	182	Application Data
9003	68.477862	Tp-LinkT_e7:c4:d8	D-LinkIn_97:79:b1	TLSv1.2	182	Application Data
9006	68.482723	D-LinkIn_97:79:b1	Tp-LinkT_e7:c4:d8	TLSv1.2	173	Application Data

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)

The image shows a Wireshark packet capture interface. The filter bar at the top contains the filter: (wlan.ta == 1c:7e:e5:97:79:b1) && (wlan.fc.type_subtype == 0x000c). The packet list shows a single packet, No. 18327, at Time 147.658224, from Source D-LinkIn_97:79:b1 to Destination Broadcast, Protocol 802.11, Length 66. The packet details pane shows the following information:

- Frame 18327: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
- Encapsulation type: IEEE 802.11 plus radiotap radio header (23)
- Arrival Time: Mar 14, 2018 11:16:49.520670000 Coordinated Universal Time
- [Time shift for this packet: 0.000000000 seconds]
- Epoch Time: 1521026209.520670000 seconds
- [Time delta from previous captured frame: 0.004072000 seconds]
- [Time delta from previous displayed frame: 0.000000000 seconds]
- [Time since reference or first frame: 147.658224000 seconds]
- Frame Number: 18327
- Frame Length: 66 bytes (528 bits)
- Capture Length: 66 bytes (528 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: radiotap:wlan_radio:wlan]
- > Radiotap Header v0, Length 36
- > 802.11 radio information
- > IEEE 802.11 Deauthentication, Flags:C
- > IEEE 802.11 wireless LAN

References:

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