GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Webinar 7 "Public wifi security"

Exercises

017 TU AYUDA EN CIBERSEGURIDAD
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDEX

FIGURES INDEX

1. PRACTICAL EXERCISE

The objective of the exercise is to investigate the content of a .pcap file which contains 802.11 frames as a result of the connectivity of a certain device to an access point. Users should investigate its content and answer the following questions:

- What is the name (SSID) of the AP to which the client connects?
- It identifies the association and authentication frames exchanged between the AP and the client.
- It locates the 4-step handshake and indicates what type of encryption has been used (TKIP or CCMP).

Exercise Resolution:

Users should review the phases involved in connecting a station to a PA. A good resource for this exercise is: https://www.aircrack-ng.org/doku.php?id=wpa_capture.

The name of the SSID used by the client can be easily obtained by filtering the management frames related to the "Probe requests" or directly observing the association frames.

Some filters of interest from Wireshark for the 802.11 protocol can be found in the following resource:

https://www.wifi-professionals.com/2019/03/wireshark-display-filters

management frames	wlan.fc.type == 0	all management frames
	wlan.fc.type_subtype == 0	association requests
	wlan.fc.type_subtype == 1	association response
	wlan.fc.type_subtype == 2	re-association request
	wlan.fc.type_subtype == 3	re-association response
	wlan.fc.type_subtype == 4	probe requests
	wlan.fc.type_subtype == 5	probe responses
	wlan.fc.type_subtype == 8	beacons
	wlan.fc.type_subtype == 9	atims
	wlan.fc.type_subtype == 10	disassosiations
	wlan.fc.type_subtype == 11	authentications
	wlan.fc.type_subtype == 12	deauthentications
	wlan.fc.type_subtype == 13	actions

Figure 1: WireShark filters

By setting up filters related to "probe request" and/or "association requests" we quickly get the answer to the first question. The requested SSID is "Coherer".

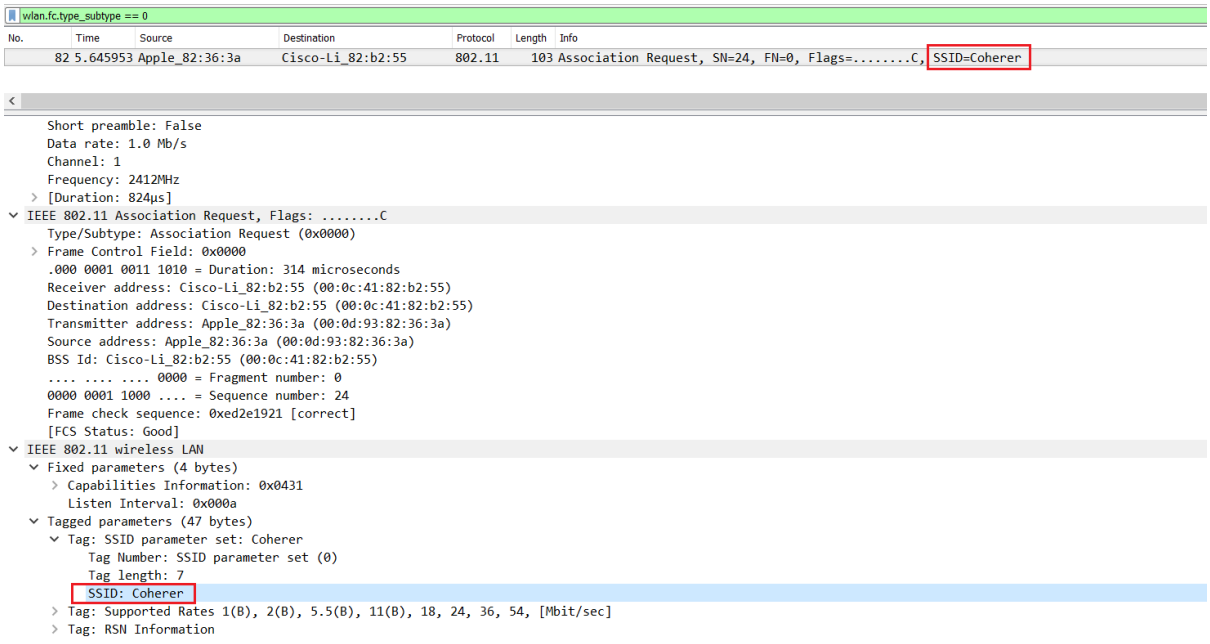

Figure 2: SSID identified

The "Association Request" and the AP ("Association Response") can be obtained by setting the following filter.

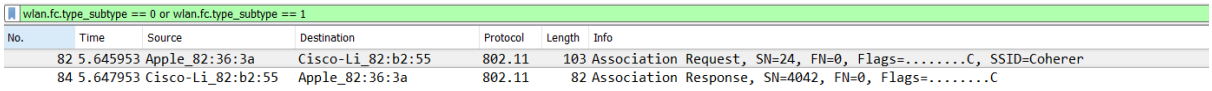

Figure 3: Filter for "Association Resquest"

Similarly, authentication frames can be obtained with subtype 11:

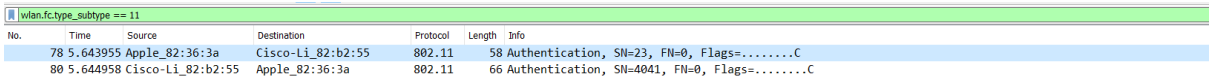

Figure 4: Subtype 11 filter

It can be seen, as described in the Webinar, that authentication frames precede association frames and that this phase is a requirement for connecting to a network.

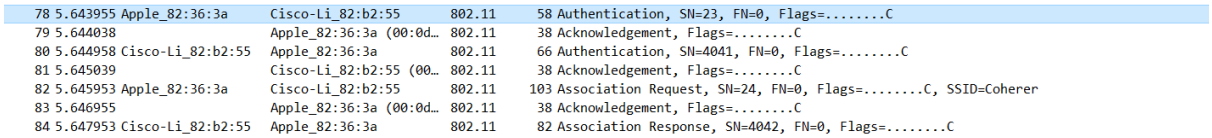

Figure 5: Request phase connection

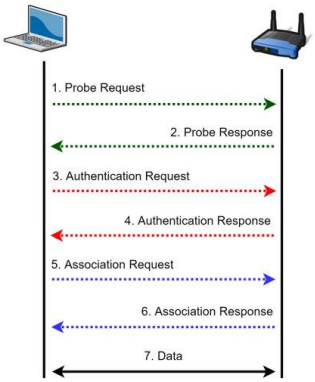

Figure 6: Handshake flow

On the third point, two questions are asked. The first one asks to identify the 4-step handshake. To do this we can use the "EAPOL" filter which will show us the 4 frames responsible for the negotiation. Note that the AP oversees initiating it.

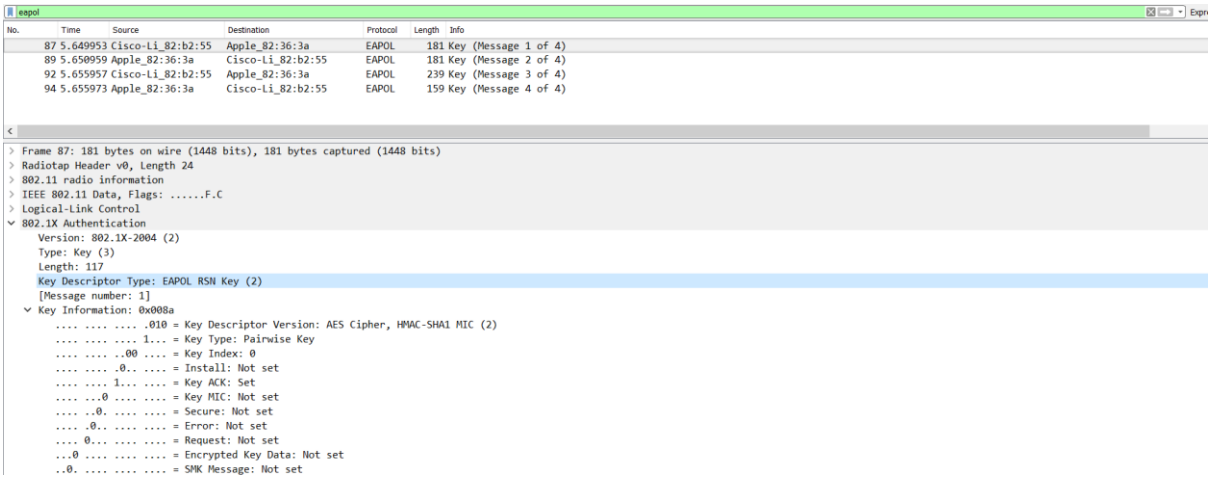

Figure 7: EAPOL filter

Regarding the second question (what type of encryption is used) as can be seen in the following frame (corresponding to the data exchanged between the AP and the station once it is authenticated and associated in the network), it is CCMP.

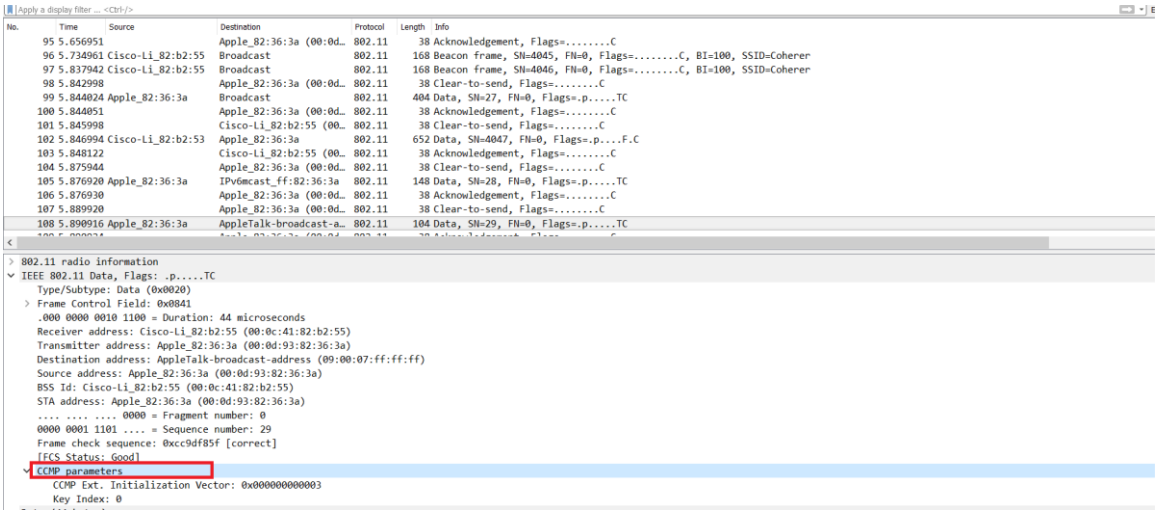

Figure 8: Type of encryption used

2. RESEARCH EXERCISE

As a result of the study of the previous .pcap the students will have to investigate how to crack the password in order to access the encrypted traffic of the .pcap. Remember that the .pcap contains the four-step handshake and is therefore susceptible to cracking if a weak password is used.

Hint: It is possible in this case that the password is "induction" either in upper/lower case or a combination of both.

Exercise Resolution:

The *aircrack-ng* tool suite has been mentioned several times in the course. Students should investigate how to apply brute force using one of its tools. A dictionary of words using "induction" and its variations in upper and lower case has been created as a result of the clue.

```
root@kali:/media/sf_Share# for w in {i,I}{n,N}{d,D}{u,U}{c,C}{t,T}{i,I}{o,O}{n,N};do echo $w;done > dict.txt
root@kali:/media/sf_Share# head dict.txt
induction
inductioN
inductiOn
inductiON
inductIon
inductIoN
inductIOn
inductION
inducTion
inducTioN
root@kali:/media/sf_Share#
```

Figure 9: Loop to build a key dictionary

Subsequently, *aircrack-ng* has been executed as follows:

```
root@kali:/media/sf_Share# aircrack-ng -w /tmp/dict.txt -b 00:0C:41:82:b2:55 sample.pcap
```

Figure 10: Execution command

The MAC of the AP will be indicated with the -b parameter and the previously created dictionary with -w.

```
                          Aircrack-ng 1.5.2

      [00:00:00] 264/511 keys tested (2096.50 k/s)

      Time left: 0 seconds                                      51.66%

                          KEY FOUND! [ Induction ]


      Master Key     : A2 88 FC F0 CA AA CD A9 A9 F5 86 33 FF 35 E8 99
                       2A 01 D9 C1 0B A5 E0 2E FD F8 CB 5D 73 0C E7 BC

      Transient Key  : B1 CD 79 27 16 76 29 03 F7 23 42 4C D7 D1 65 11
                       82 A6 44 13 3B FA 4E 0B 75 D9 6D 23 08 35 84 33
                       15 79 8D 51 1B EA E0 02 83 13 C8 AB 32 F1 2C 7E
                       CB 71 C8 93 48 26 69 DA AF 0E 92 23 FE 1C 0A ED

      EAPOL HMAC     : A4 62 A7 02 9A D5 BA 30 B6 AF 0D F3 91 98 8E 45
root@kali:/media/sf_Share#
```

Figure 11: Key found

We will instantly get the password ("Induction"). Later, to decode the traffic from Wireshark we will go to "Edit->Preferences" and, within the IEEE 802.11 protocol, we will add the key in the following format: "wpa_key:SSID" (i.e.: "Induction:Coherer")

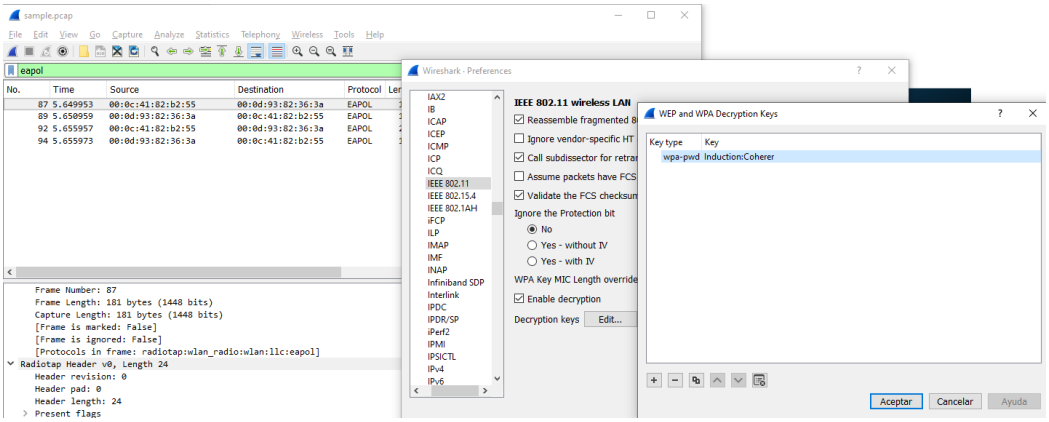

Figure 12: Known key to decode traffic

After accepting the dialog box we can access the encrypted information. In the following image you can see the capture before decoding (left image) and once decoded (right image). Note that it is already possible to access in clear the information sent by the client and the AP (for example, HTTP traffic).

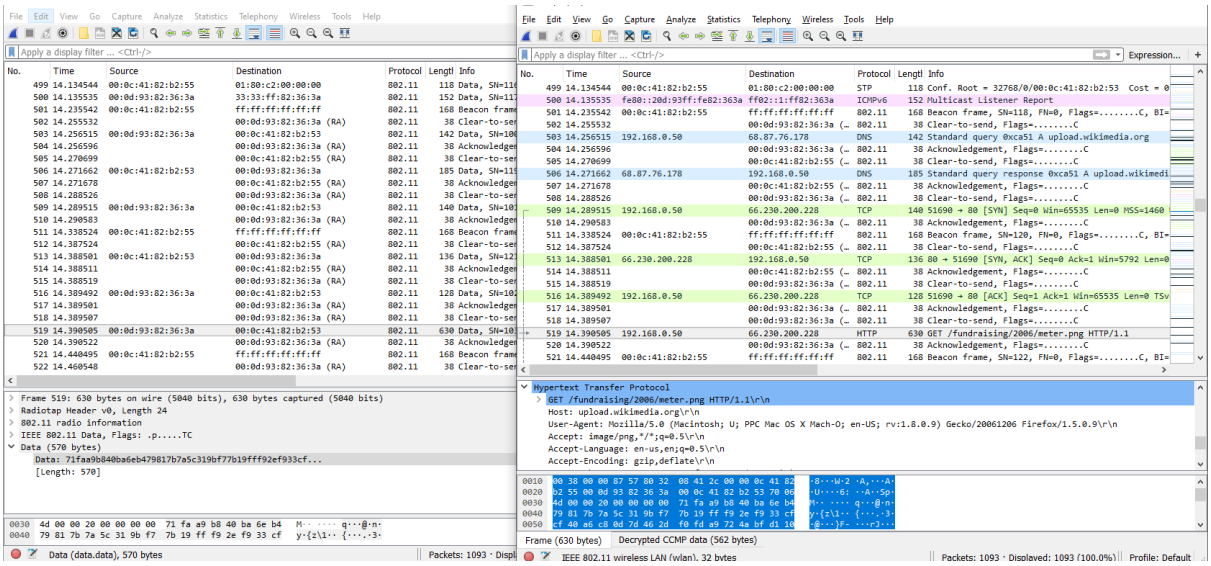

Figure 13: Decode traffic