



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



TU AYUDA EN
CIBERSEGURIDAD



INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDEX

1. Practical Exercise	3
2. Research Exercise	7

FIGURES INDEX

Figure 1: WireShark filters	3
Figure 2: SSID identified	4
Figure 3: Filter for "Association Resquest"	4
Figure 4: Subtype 11 filter	4
Figure 5: Request phase connection.....	4
Figure 6: Handshake flow.....	5
Figure 7: EAPOL filter	5
Figure 8: Type of encryption used	6
Figure 9: Loop to build a key dictionary	7
Figure 10: Execution command.....	7
Figure 11: Key found	7
Figure 12: Known key to decode traffic.....	8
Figure 13: Decode traffic	8

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	disassociations
	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".

wlan.fc.type_subtype == 0						
No.	Time	Source	Destination	Protocol	Length	Info
82	5.645953	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID=Coherer


```

Short preamble: False
Data rate: 1.0 Mb/s
Channel: 1
Frequency: 2412MHz
> [Duration: 824µs]
▼ IEEE 802.11 Association Request, Flags: .....C
  Type/Subtype: Association Request (0x0000)
  > Frame Control Field: 0x0000
    .000 0001 0011 1010 = Duration: 314 microseconds
  Receiver address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
  Destination address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
  Transmitter address: Apple_82:36:3a (00:0d:93:82:36:3a)
  Source address: Apple_82:36:3a (00:0d:93:82:36:3a)
  BSS Id: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)
  .... .. 0000 = Fragment number: 0
  0000 0001 1000 .... = Sequence number: 24
  Frame check sequence: 0xed2e1921 [correct]
  [FCS Status: Good]
▼ IEEE 802.11 wireless LAN
  > Fixed parameters (4 bytes)
    > Capabilities Information: 0x0431
      Listen Interval: 0x000a
  > Tagged parameters (47 bytes)
    > Tag: SSID parameter set: Coherer
      Tag Number: SSID parameter set (0)
      Tag length: 7
      SSID: Coherer
    > Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    > Tag: RSN Information
  
```

Figure 2: SSID identified

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

wlan.fc.type_subtype == 0 or wlan.fc.type_subtype == 1						
No.	Time	Source	Destination	Protocol	Length	Info
82	5.645953	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID=Coherer
84	5.647953	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	82	Association Response, SN=4042, FN=0, Flags=.....C

Figure 3: Filter for "Association Resquest"

Similarly, authentication frames can be obtained with subtype 11:

wlan.fc.type_subtype == 11						
No.	Time	Source	Destination	Protocol	Length	Info
78	5.643955	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	58	Authentication, SN=23, FN=0, Flags=.....C
80	5.644958	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	66	Authentication, SN=4041, FN=0, Flags=.....C

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.

78	5.643955	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	58	Authentication, SN=23, FN=0, Flags=.....C
79	5.644038	Apple_82:36:3a	Apple_82:36:3a (00:0d:93:82:36:3a)	802.11	38	Acknowledgement, Flags=.....C
80	5.644958	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	66	Authentication, SN=4041, FN=0, Flags=.....C
81	5.645039	Cisco-Li_82:b2:55	Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)	802.11	38	Acknowledgement, Flags=.....C
82	5.645953	Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103	Association Request, SN=24, FN=0, Flags=.....C, SSID=Coherer
83	5.646955	Apple_82:36:3a	Apple_82:36:3a (00:0d:93:82:36:3a)	802.11	38	Acknowledgement, Flags=.....C
84	5.647953	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	82	Association Response, SN=4042, FN=0, Flags=.....C

Figure 5: Request phase connection

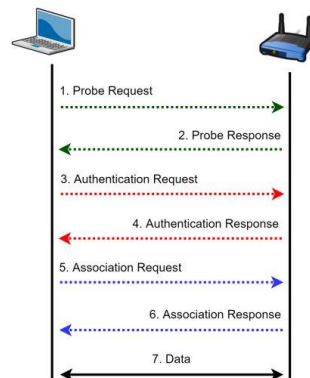


Figure 6: Handshake flow

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.

No.	Time	Source	Destination	Protocol	Length	Info
87	5.649953	Cisco-Li_82:b2:55	Apple_82:36:3a	EAPOL	181	Key (Message 1 of 4)
89	5.650959	Apple_82:36:3a	Cisco-Li_82:b2:55	EAPOL	181	Key (Message 2 of 4)
92	5.655957	Cisco-Li_82:b2:55	Apple_82:36:3a	EAPOL	239	Key (Message 3 of 4)
94	5.655973	Apple_82:36:3a	Cisco-Li_82:b2:55	EAPOL	159	Key (Message 4 of 4)


```

> Frame 87: 181 bytes on wire (1448 bits), 181 bytes captured (1448 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Data, Flags: .....F.C
> Logical-Link Control
▼ 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
  ▼ Key Information: 0x008a
    .... 010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
    .... 1.. = Key Type: Pairwise Key
    .... .00 = Key Index: 0
    .... .0.. = Install: Not set
    .... 1.. = Key ACK: Set
    .... .0.. = Key MIC: Not set
    .... .0.. = Secure: Not set
    .... .0.. = Error: Not set
    .... 0.. = Request: Not set
    .... .0.. = Encrypted Key Data: Not set
    .... .0.. = SMK Message: Not set
    
```

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.

No.	Time	Source	Destination	Protocol	Length	Info
95	5.656951	Cisco-Li_82:b2:55	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
96	5.734961	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4045, FN=0, Flags=.....C, BI=100, SSID=Coherer
97	5.837942	Cisco-Li_82:b2:55	Broadcast	802.11	168	Beacon frame, SN=4046, FN=0, Flags=.....C, BI=100, SSID=Coherer
98	5.842998	Apple_82:36:3a (00:0d...	Apple_82:36:3a (00:0d...	802.11	38	Clear-to-send, Flags=.....C
99	5.844024	Apple_82:36:3a	Broadcast	802.11	404	Data, SN=27, FN=0, Flags=p.....TC
100	5.844051	Apple_82:36:3a (00:0d...	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
101	5.845998	Cisco-Li_82:b2:55 (00...	Cisco-Li_82:b2:55 (00...	802.11	38	Clear-to-send, Flags=.....C
102	5.846994	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	652	Data, SN=4047, FN=0, Flags=p.....F.C
103	5.848122	Cisco-Li_82:b2:55 (00...	Cisco-Li_82:b2:55 (00...	802.11	38	Acknowledgement, Flags=.....C
104	5.875944	Apple_82:36:3a (00:0d...	Apple_82:36:3a (00:0d...	802.11	38	Clear-to-send, Flags=.....C
105	5.876920	Apple_82:36:3a	IPv6mcast-ff:82:36:3a	802.11	148	Data, SN=28, FN=0, Flags=p.....TC
106	5.876930	Apple_82:36:3a (00:0d...	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
107	5.889920	Apple_82:36:3a (00:0d...	Apple_82:36:3a (00:0d...	802.11	38	Clear-to-send, Flags=.....C
108	5.890916	Apple_82:36:3a	AppleTalk-broadcast-a...	802.11	104	Data, SN=29, FN=0, Flags=p.....TC
109	5.890934	Apple_82:36:3a (00:0d...	Apple_82:36:3a (00:0d...	802.11	38	Acknowledgement, Flags=.....C
802.11 radio information						
IEEE 802.11 Data, Flags: .p.....TC						
Type/Subtype: Data (0x0020)						
Frame Control Field: 0x0041						
.000 0000 0010 1100 = Duration: 44 microseconds						
Receiver address: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)						
Transmitter address: Apple_82:36:3a (00:0d:93:82:36:3a)						
Destination address: AppleTalk-broadcast-address (09:00:07:ff:ff:ff)						
Source address: Apple_82:36:3a (00:0d:93:82:36:3a)						
BSS Id: Cisco-Li_82:b2:55 (00:0c:41:82:b2:55)						
STA address: Apple_82:36:3a (00:0d:93:82:36:3a)						
.... .. 0000 = Fragment number: 0						
0000 0001 1101 = Sequence number: 29						
Frame check sequence: 0xcc9df85f [correct]						
FCS Status: Good						
CMP parameters						
CMP Ext. Initialization Vector: 0x000000000003						
Key Index: 0						

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}{l,L}{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
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**")

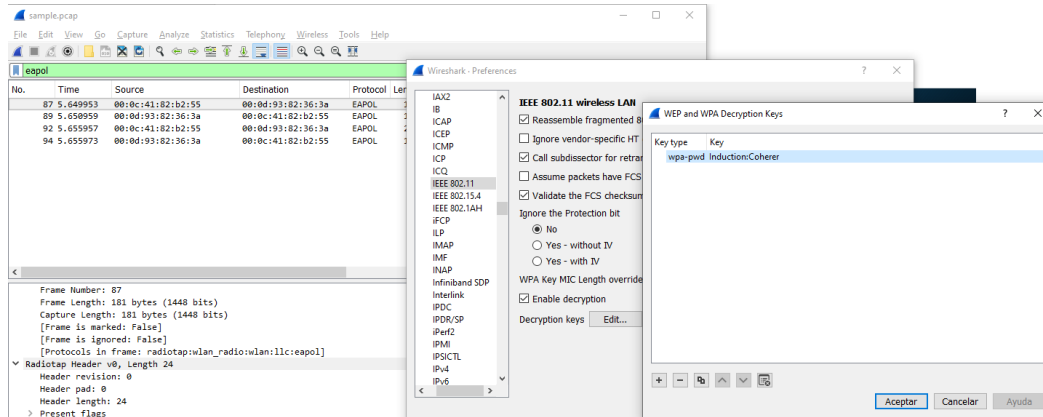


Figure 12: Known key to decode traffic

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).

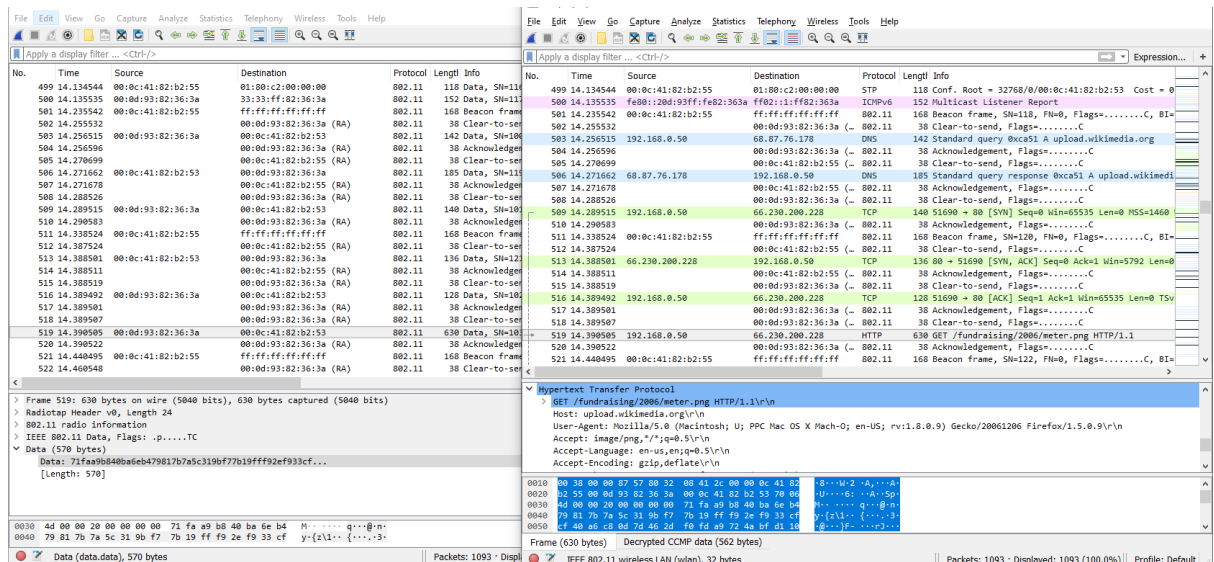


Figure 13: Decode traffic