

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**











### 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"	1
	. –
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 encyption 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
0	







### **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: <u>https://www.aircrack-ng.org/doku.php?id=wpa\_capture</u>.

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".







w 📕	wlan.fc.type_subtype == 0									
No.	Time	Source	Destination	Protocol	Length Info					
	82 5.64595	3 Apple_82:36:3a	Cisco-Li_82:b2:55	802.11	103 Association	Request, SN=2	24, FN=0,	Flags=C,	SSID=Coherer	
<										
	Short pream	ble: False								
	Data rate:	1.0 Mb/s								
	Channel: 1									
	Frequency:	2412MHz								
	> [Duration:	824µs]								
~ 1	EEE 802.11 As	sociation Request,	Flags:C							
	Type/Subtyp	e: Association Reque	est (0x0000)							
	> Frame Contr	ol Field: 0x0000								
	.000 0001 0	011 1010 = Duration	: 314 microseconds							
	Receiver ad	dress: Cisco-Li_82:	b2:55 (00:0c:41:82:b2:55	)						
	Destination	address: Cisco-Li_8	82:b2:55 (00:0c:41:82:b2	:55)						
	Transmitter	address: Apple_82:	36:3a (00:0d:93:82:36:3a	)						
	Source addr	ess: Apple_82:36:3a	(00:0d:93:82:36:3a)							
	BSS Id: Cis	co-Li_82:b2:55 (00:0	0c:41:82:b2:55)							
		0000 = Fragment	number: 0							
	0000 0001 1	000 = Sequence	number: 24							
	Frame check	sequence: 0xed2e192	21 [correct]							
	[FCS Status	: Good]								
~ ]	EEE 802.11 wi	reless LAN								
	✓ Fixed param	eters (4 bytes)								
	> Capabili	ties Information: 0>	x0431							
	Listen I	nterval: 0x000a								
	✓ Tagged para	meters (47 bytes)								
	✓ Tag: SSI	D parameter set: Cor	herer							
	Tag N	umber: SSID paramete	er set (0)							
	lag 1	engtn: /								
	SSID:	Conerer		24 26	5 A 5 M 1 4 / 3					
	> Tag: Sup	ported kates 1(B), 2	2(8), 5.5(8), 11(8), 18,	24, 36,	54, [MDit/sec]					
	> rag: KSN	TUTOLMACTON								

#### Figure 2: SSID identified

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

wian.fc.type_subtype == 0 or wian.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	wian,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	1 58 Authentication, SN=23, FN=0, Flags=C						
	80 5.644958	Cisco-Li_82:b2:55	Apple_82:36:3a	802.11	1 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 (00:0d	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 (00	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 (00:0d	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.

eapol						Expr
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)	
<						
> Fram	e 87: 181	bytes on wire (1448	bits), 181 bytes captur	ed (1448	bits)	
> Radi	otap Heade	r v0, Length 24				
> 802.	11 radio i	nformation				
> IEEE	802.11 Da	ta, Flags:F.(	C			
> Logi	cal-Link C	ontrol				
✓ 802.	1X Authent	ication				
v	ersion: 80	2.1X-2004 (2)				
T	ype: Key (	3)				
L	ength: 11/		H (3)			
K	ey Descrip	COP Type: EAPOL KSN	Key (2)			
	lessage nui	nber: Ij				
- K	ey intorma	010 - Kov Do	scripton Version: AES C	inhan W	NC_SUA1 MTC (2)	
		1 - Key De	ne. Dainwise Key	aprier, in	ar-sint rite (z)	
		00 = Key Tr	dex: 0			
		.0 = Instal	1: Not set			
		1 = Kev AC	K: Set			
		= Key MI	C: Not set			
	0.	= Secure	: Not set			
		= Error:	Not set			
	0	= Reques	t: Not set			
	0	= Encryp	ted Key Data: Not set			
	0	= SMK Me	ssage: 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.

GOBIERNO DE ESPAÑA GE ESPAÑA GOBIERNO DE ASUNTOS ECONÔMICOS YTRANSFORMACIÓN DIGITAL	secretaria de estado de digitalización e inteligencia artificial	\$in <b>cib</b> e_	TU AVUDA EN CIBERSEGURIDAD
Annhy a direction filter of the last			
Interpolynamic         Cuty / Park         Source         Destination           96.         Time         Source         Apple_82:36:3a (00:0d.           96.5.7.566951         Apple_82:36:3a (00:0d.         Source           96.5.7.34661 Cisco-Li, 82:b2:55         Broadcast         Broadcast           97.8.37942 Cisco-Li, 82:b2:55         Broadcast         Broadcast           99.5.844024 Apple_82:36:3a         Broadcast         Broadcast           100.5.844024         Apple_82:36:3a (00:0d.         Cisco-Li, 82:b2:55 (00           102.5.844094         Sisco-Li, 82:b2:253         Apple_82:36:3a           103.5.848122         Cisco-Li, 82:b2:55 (00         Apple_82:36:3a (00:0d.           104.5.875944         Apple_82:36:3a (40:0d.         Apple_82:36:3a (40:0d.           105.5.876939         Apple_82:36:3a (40:0d.         Apple_82:36:3a (40:0d.           105.5.876930         Apple_82:36:3a (40:0d.         Apple_82:36:3a (40:0d.           105.5.876930         Apple_82:36:3a (40:0d.         Apple_82:36:3a (40:0d.           108.5.89920         Apple_82:36:3a (40:0d.         Apple_82:36:3a (40:0d.           108.5.89920         Apple_82:36:3a (40:0d.         Apple_82:36:3a (40:0d.           108.5.89920         Apple_82:36:3a (40:0d.         Apple182:36:3a (40:0d.	Protocol         Langh         Info           802.11         38 Acknowledgement, Flags=         802.11           802.11         168 Beacon frame, SH-4045, FH-0, F         802.11           802.11         168 Beacon frame, SH-4046, FH-0, F         802.11           802.11         168 Beacon frame, SH-4045, FH-0, F         802.11           802.11         34 Clear-to-send, Flags=         602.11           802.11         36 Acknowledgement, Flags=         602.11           802.111         30 Acknowledgement, Flags=	.C lags=C, BI=100, SSID=Coherer lags=C, BI=100, SSID=Coherer TC .C F.C .C TC .C	
> 802.11 radio information > 802.11 radio information > 1EEE 802.11 Data, Flags: .pTC Type/Subtye: Data (08020) > Frame Control Field: 0x0801 .000 0000 0010 1100 = Duration: 44 microseconds Receiver address: (cio-Li, 82:b2:55 (00:06:41:82:b2:55) Transmitter address: Apple 82:36:31 (00:04):93:82:36:30 Destination address: Apple 82:36:31 (00:04):93:82:36:30 Source address: Apple 82:36:31 (00:04):93:82:36:30 	) } :07:ff:ff:ff)		









## 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.



Figure 9: Loop to build a key dictionary

Subsequently, aircrack-ng has been executed as follows:



#### 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	[00:00:00] 264/511 keys tested (2096.50 k/s)								
Time left: 0 second	51.66%								
	KEY FOUND! [ Induction ]								
Master Key : A2 2A	88 FC F0 CA AA CD A9 A9 F5 86 33 FF 35 E8 99 01 D9 C1 0B A5 E0 2E FD F8 CB 5D 73 0C E7 BC								
Transient Key : Bl	CD 79 27 16 76 29 03 F7 23 42 4C D7 D1 65 11								
82 15	A6 44 13 3B FA 4E 0B 75 D9 6D 23 08 35 84 33 79 8D 51 1B EA E0 02 83 13 C8 AB 32 F1 2C 7E								
СВ	71 C8 93 48 26 69 DA AF 0E 92 23 FE 1C 0A ED								
EAPOL HMAC : A4 root@kali:/media/sf_Share	62 A7 02 9A D5 BA 30 B6 AF 0D F3 91 98 8E 45 #								







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")

	sample.pcap					-				
Ei	le <u>E</u> dit <u>V</u> iew <u>G</u> o	<u>Capture</u> Analyze Statistics	Telephony Wireless T	ools <u>H</u> elp						
	🔳 🖉 🕥 📙 🗄	🗙 🖸 । ९ 👄 👄 🖉 🖗	4 🗐 🗐 Q Q Q	11						
	eapol				Wireshark - Preferer	nces		? ×		
No	<ul> <li>Time</li> <li>87 5.649953</li> <li>89 5.650959</li> <li>92 5.655957</li> <li>94 5.655973</li> </ul>	Source 00:0c:41;02:42;55 00:0d:93:82:36:3a 00:0c:41;82:42;55 00:0d:93:82:36:3a	Destination 00:04:93:82:36:3a 00:0c:41:82:b2:55 00:0d:93:82:36:3a 00:0c:41:82:b2:55	Protocol Ler EAPOL 2 EAPOL 2 EAPOL 2 EAPOL 2	IAX2 IB ICAP ICCP	IEEE 802.11 wireless LAN     Reassemble fragmented 8     Ignore vendor-specific HT     Call subdissector for retrat     Assume packets have FCS     Validate the FCS checksum     Ignore the Protection bit	WEP and WPA Decryption Keys Key type Key wpa-poid induction:Coherer		?	×
<	Frame Number: Frame Length: Capture Lengt [Frame is mar [Frame is ign [Protocols in Header Header Header revisi Header pad: 0 Header length > Present flags	87 181 bytes (1448 bits) 1: 181 bytes (1448 bits) ced: False] frame: radiotap:wlan_rad: 0; Length 24 nn: 0 24	io:wlan:llc:eapol]		INAP Infiniband SDP Interlink IPDC IPDR/SP IPerf2 IPMI IPSICTL IPv4 IPv6 >	WPA Key MLC Length override	* • • • • •	Aceptar C2	ancelar Ayu	ıda

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).

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help	
🖌 🗏 🖉 🔍 🕒 🔄 🛠 🖄 🗣 🚸 😤 🗿 🔍 🔍 Q. Q. Q. X. 🖉 🖌 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉 🖉	
Apply a display filter < Ctrl-/>	Evoraccion +
No. Time Source Destination Protoci Lengt Into	
499 14.134544 00:0c:41:62:02:55 01:80:C2:00:00:00 STP 118 Conf. Root = 32768/0	1/00:0c:41:82:b2:53 Cost = 0
500 14.133535 00100195162136138 351351TT102130138 002.11 132 Data, SH=11 500 14.135535 fe80::200193ff:fe82:363a ff02::11ff82:363a ICMPv6 152 Multicast Listener R	report
501 44.235542 00:00:41:02:02:55 ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	;, FN=0, Flags=C, BI=
502 147.255532 00:0d:93:82:36:3a (	,=C
503 14-250515 00100195162136530 00100195162136530 0001014102102135 000.11 142 Units, 514100 503 14.256515 192.168.0.50 68.87.76.178 DNS 142 Standard query 0xca5	1 A upload.wikimedia.org
504 14.256596 00:0d:93:82:36:3a ( 802.11 38 Acknowledgement, Fla	igs=C
505 14.270699 00:0c:41:82:b2:55 ( 802.11 38 Clear-to-sent 505 14.270699 00:0c:41:82:b2:55 ( 802.11 38 Clear-to-sent, Flags	:=C ===
506 14.271652 00:00:14182102:53 00:00193:82:36:53 802.11 185 Uata, SH=11 506 14.271662 68.87.76.178 192.168.0.50 DNS 185 Standard query respo	mse 0xca51 A upload.wikimedi
507 14.2/16/8 00:00:41:82:b2:55 (m. 802.11 38 Acknowledgem 507 14.271678 00:00:41:82:b2:55 (m. 802.11 38 Acknowledgement, Fla	igs=C
508 14.288526 00:0d:93:82:36:3a ( 802.11 38 Clear-to-sent 508 14.288526 00:0d:93:82:36:3a ( 802.11 38 Clear-to-send, Flags	i=C
509 14.289515 00100193182136138 00100141402102153 800.11 140 URTA, SH=10 509 14.289515 192.168.0.50 66.230.200.228 TCP 140 51690 + 80 [SYN] Seq	=0 Win=65535 Len=0 MSS=1460
510 14.299583 00:00:93:82:36:3a (NA) 802.11 38 Acknowledgen 510 14.290583 00:0d:93:82:36:3a ( 802.11 38 Acknowledgenent, Fla	igs=C
511 14.338524 00:00:41:82:02:55 ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	1, FN=0, Flags=C, BI=
512 14.38/524 00:0c:41:82:b2:55 ( 802.11 38 Clear-to-sent 512 14.387524 00:0c:41:82:b2:55 ( 802.11 38 Clear-to-send, Flags	i=C
513 14.388501 00:0c:41:82:b2:53 00:0d:93:82:36:3a 802.11 136 Data, SN=12 513 14.388501 66.230.200.228 192.168.0.50 TCP 136 80 + 51690 [SYN, ACK	[] Seq=0 Ack=1 Win=5792 Len=0
514 14.388511 00:0c:41:82:b2:55 (RA) 802.11 38 Acknowledgen 514 14.388511 00:0c:41:82:b2:55 ( 802.11 38 Acknowledgement, Fla	igs=C
515 14.388519 00:0d:93:82:36:3a (RA) 802.11 38 Clear-to-sen 515 14.388519 00:0d:93:82:36:3a ( 802.11 38 Clear-to-send, Flags	;=C
516 14.389492 00:00193:82:36:38 00:00:41:82:82:38:41:42:82:36:38 00:00:41:82:82:38:41:42:82:38:42:38 00:00:41:82:38:42:38 00:00:41:82:38:42:38 00:00:41:82:38:42:38 00:00:41:82:38:42:38 00:00:41:82:38:42:38 00:00:41:82:38:42:38 00:00:41:82:38:42:38 00:00:41:82:38:42:38:42:38 00:00:41:82:38:42:3	=1 Ack=1 Win=65535 Len=0 TSv
517 14.389501 00:0d:93:82:36:3a (RA) 802.11 38 Acknowledgem 517 14.389501 00:0d:93:82:36:3a ( 802.11 38 Acknowledgement, Fla	igs=C
518 14.389507 00:0d:93:82:36:3a (RA) 802.11 38 Clear-to-sen 518 14.389507 00:0d:93:82:36:3a ( 802.11 38 Clear-to-send, Flags	;=C
519 14.399595 00:0d:93:82:36:3a 00:0c:41:82:b2:53 802.11 630 Data, SN=101 + 519 14.399595 192.168.0.50 66.230.200.228 HTTP 630 GET /fundraising/200	06/meter.png HTTP/1.1
520 14.390522 00:0d:93:82:36:3a ( 802.11 38 Acknowledgem 520 14.390522 00:0d:93:82:36:3a ( 802.11 38 Acknowledgement, Fla	igs=C
521 14.444495 00:0c:41:82:b2:55 ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:	!, FN=0, Flags=C, BI= ∨
522 14.460548 00:0d:93:82:36:3a (RA) 802.11 38 Clear-to-set <	>
V Hypertext Transfer Protocol	A
> Frame 519: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits) > 6ET /fundraising/2006/meter.png HTTP/1.1\r\n	
> Radiotap Header v0, Length 24 Host: upload.wikimedia.org\r\n	
> 802.11 radio information User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.9) Gecko/20061206 F	irefox/1.5.0.9\r\n
> IEEE 802.11 Data, Flags: .pTC Accept: image/png.*/*:q=0.5\r\n	
✓ Data (570 bytes) Accept-Language: en-us,en;q=0.5\r\n	
Data: 71faa9b840ba6eb479817b7a5c319bf77b19fff92ef933cf Accept-Encoding: gzip,deflate\r\n	
[Length: 570]	
0010 00 33 00 00 87 57 88 32 08 41 2c 00 00 c 41 82 -8	^
0030 4d 00 00 20 00 00 00 71 fa a9 b8 40 ba 6e b4 N····· q····B·n· 0056 cf 40 a5 c8 0d 7d 45 2d f0 fd a9 72 4a bf d1 10 - (B···) [-····]	
0040 79 81 7b 7a 5c 31 9b f7 7b 19 ff f9 2e f9 33 cf y-{z\1	
Traine (050 bytes)	

Figure 13: Decode traffic