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).

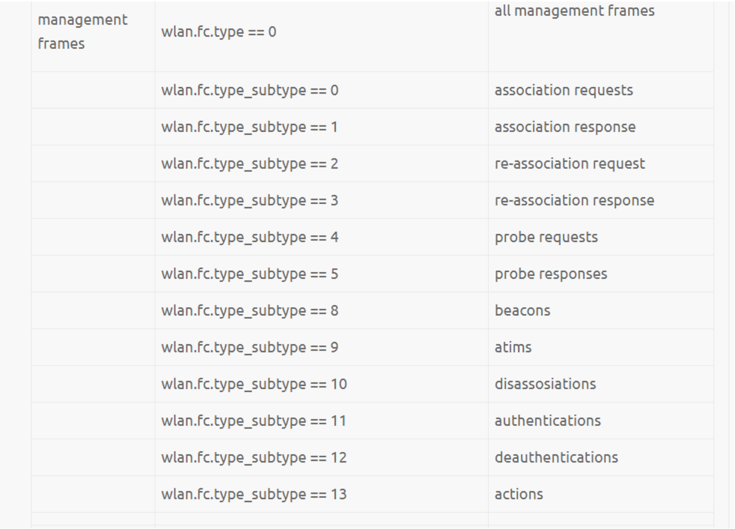
Exercise Resolution:

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:

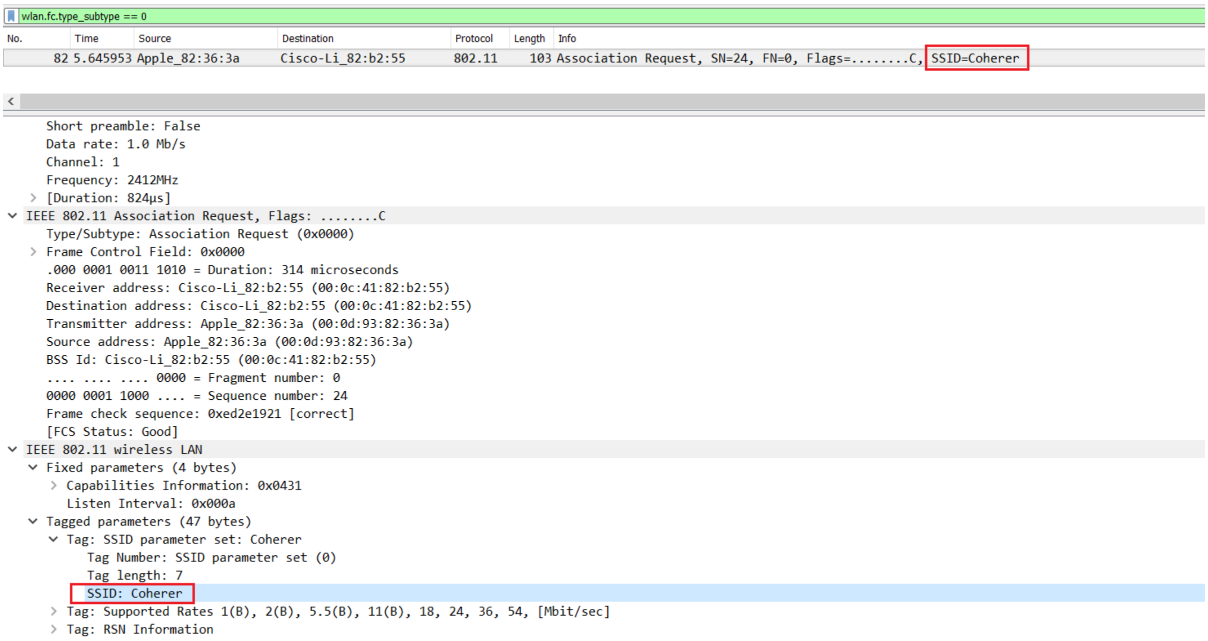
https://www.wifi-professionals.com/2019/03/wireshark-display-filters



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

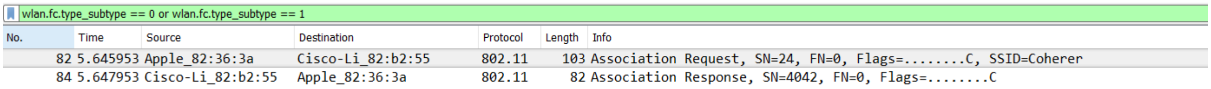
By setting up filters related to "probe request" and/or "association requests" we quickly get the answer to the first question. The requested SSID is "Coherer".



```
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

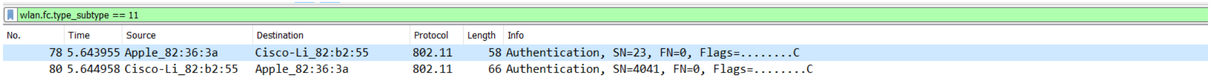
The "Association Request" and the AP ("Association Response") can be obtained by setting the following filter.



```
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"

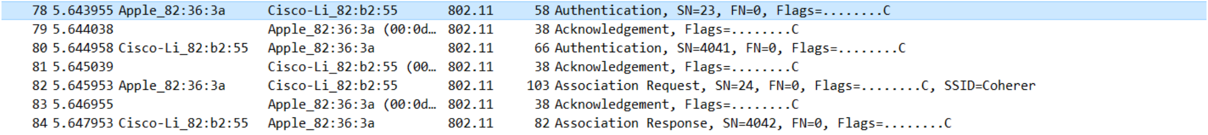
Similarly, authentication frames can be obtained with subtype 11:



```
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 (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

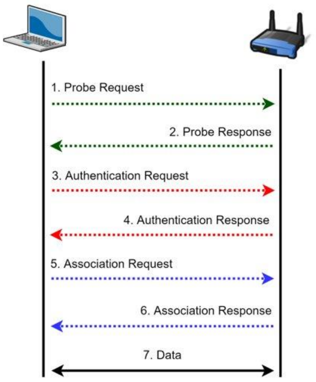
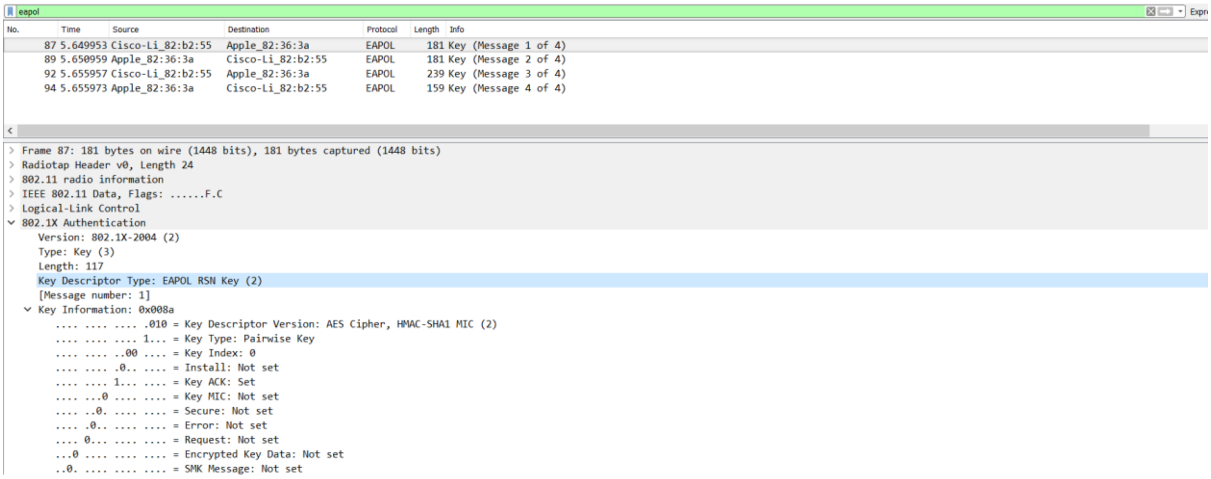


Figure 6: Handshake flow

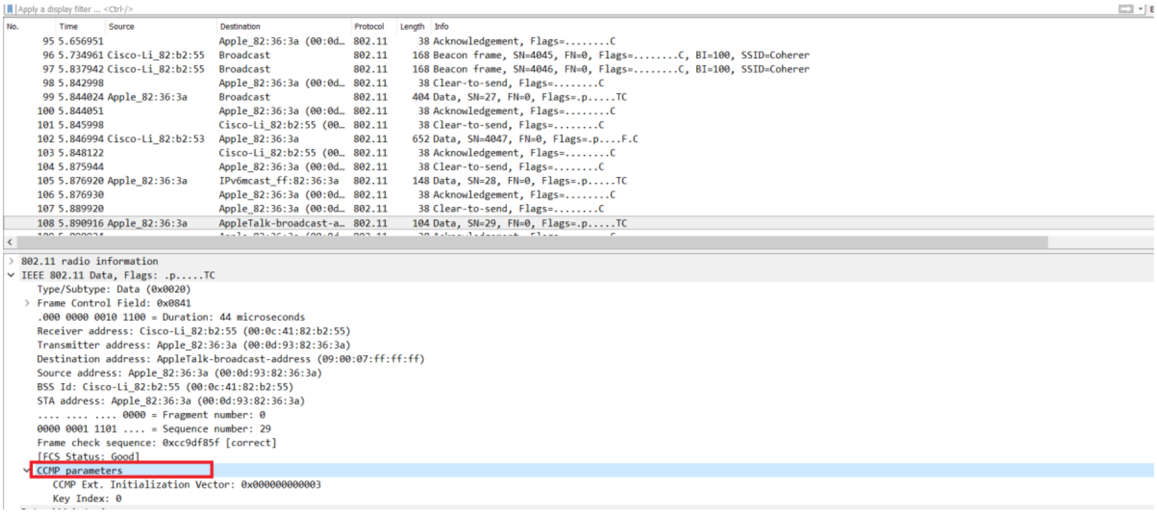
On the third point, two questions are asked. The first one asks to identify the 4-step handshake. To do this we can use the "EAPOL" filter which will show us the 4 frames responsible for the negotiation. Note that the AP oversees initiating it.



```
eapol
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
v 802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
  v 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                     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…   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…   802.11    38 Acknowledgement, Flags=........C
101 5.845998                     Cisco-Li_82:b2:55 (00…   802.11    38 Clear-to-send, Flags=........C
102 5.846994 Cisco-Li_82:b2:53   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…   802.11    38 Acknowledgement, Flags=........C
104 5.875944                     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…   802.11    38 Acknowledgement, Flags=........C
107 5.889920                     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
```

```
> 802.11 radio information
v IEEE 802.11 Data, Flags: .p.....TC
    Type/Subtype: Data (0x0020)
  > Frame Control Field: 0x0841
    .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]
  v CCMP parameters
      CCMP Ext. Initialization Vector: 0x000000000003
      Key Index: 0
```

Figure 8: Type of encryption used

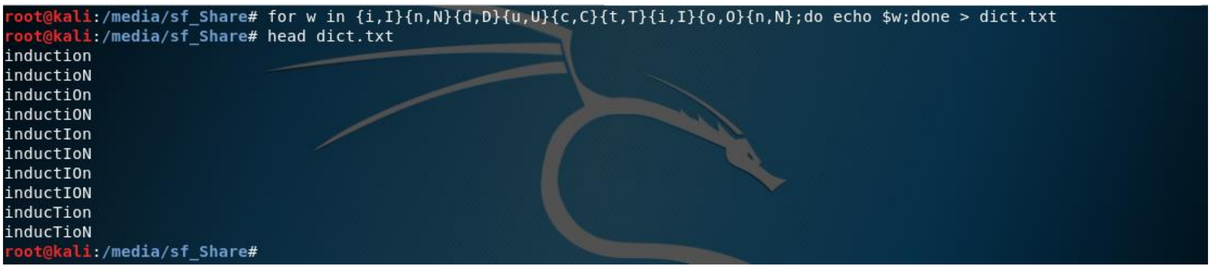
2. RESEARCH EXERCISE

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:

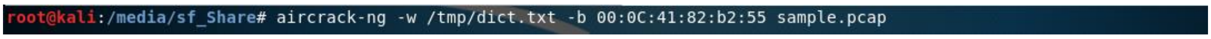
The *aircrack-ng* tool suite has been mentioned several times in the course. Students should investigate how to apply brute force using one of its tools. A dictionary of words using "induction" and its variations in upper and lower case has been created as a result of the clue.



```
root@kali:/media/sf_Share# for w in {i,I}{n,N}{d,D}{u,U}{c,C}{t,T}{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

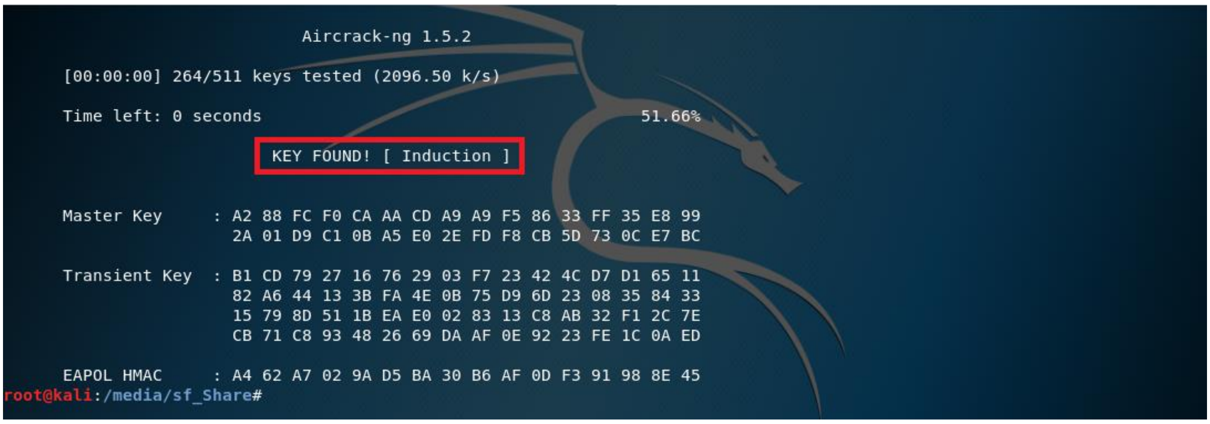
Subsequently, *aircrack-ng* has been executed as follows:



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

Figure 10: Execution command

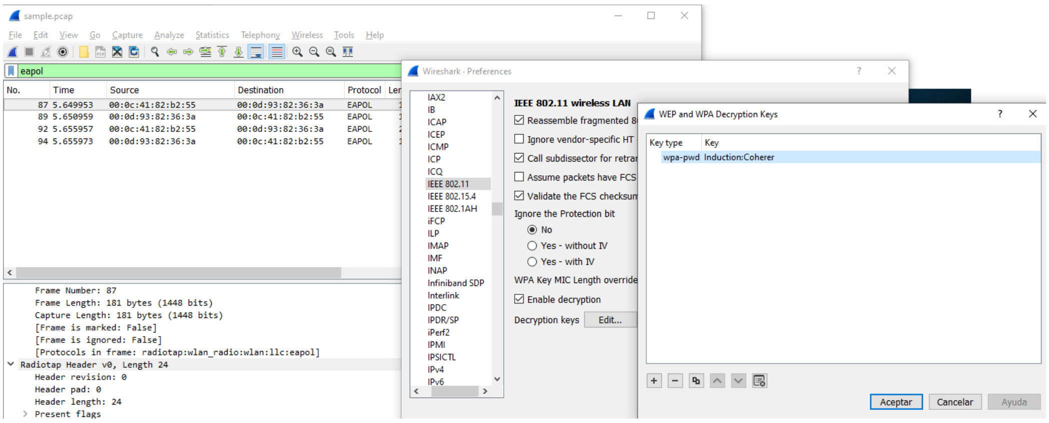
The MAC of the AP will be indicated with the -b parameter and the previously created dictionary with -w.



```
                              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")



sample.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Preferences
WEP and WPA Decryption Keys
Aceptar
Cancelar
Ayuda

eapol

```
No.   Time      Source             Destination        Protocol
   87 5.649953  00:0c:41:82:b2:55  00:0d:93:82:36:3a  EAPOL
   89 5.650959  00:0d:93:82:36:3a  00:0c:41:82:b2:55  EAPOL
   92 5.655957  00:0c:41:82:b2:55  00:0d:93:82:36:3a  EAPOL
   94 5.655973  00:0d:93:82:36:3a  00:0c:41:82:b2:55  EAPOL

    Frame Number: 87
    Frame Length: 181 bytes (1448 bits)
    Capture Length: 181 bytes (1448 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: radiotap:wlan_radio:wlan:llc:eapol]
v Radiotap Header v0, Length 24
    Header revision: 0
    Header pad: 0
    Header length: 24
  > Present flags
```

IAX2, IB, ICAP, ICEP, ICMP, ICP, ICQ, IEEE 802.11, IEEE 802.15.4, IEEE 802.1AH, iFCP, ILP, IMAP, IMF, INAP, Infiniband SDP, Interlink, IPDC, IPDR/SP, iPerf2, IPMI, IPSICTL, IPv4, IPv6

IEEE 802.11 wireless LAN

☑ Reassemble fragmented 8
☐ Ignore vendor-specific HT
☑ Call subdissector for retrar
☐ Assume packets have FCS
☑ Validate the FCS checksum

Ignore the Protection bit
● No
○ Yes - without IV
○ Yes - with IV

WPA Key MIC Length override

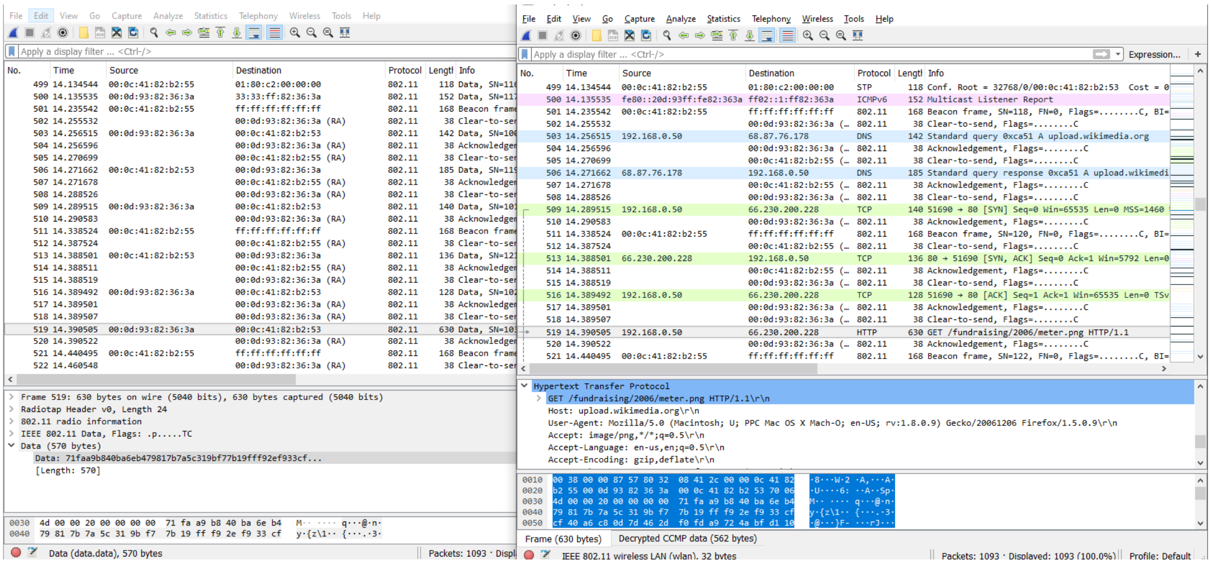
☑ Enable decryption

Decryption keys [Edit...]

Key type	Key
wpa-pwd	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).



File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time       Source             Destination             Protocol Lengtl Info
  499 14.134544  00:0c:41:82:b2:55  01:80:c2:00:00:00       802.11   118 Data, SN=116
  500 14.135535  00:0d:93:82:36:3a  33:33:ff:82:36:3a       802.11   152 Data, SN=117
  501 14.235542  00:0c:41:82:b2:55  ff:ff:ff:ff:ff:ff       802.11   168 Beacon frame
  502 14.255532                     00:0d:93:82:36:3a (RA)  802.11    38 Clear-to-ser
  503 14.256515  00:0d:93:82:36:3a  00:0c:41:82:b2:53       802.11   142 Data, SN=100
  504 14.256596                     00:0d:93:82:36:3a (RA)  802.11    38 Acknowledgem
  505 14.270699                     00:0c:41:82:b2:55 (RA)  802.11    38 Clear-to-ser
  506 14.271662  00:0c:41:82:b2:53  00:0d:93:82:36:3a       802.11   185 Data, SN=119
  507 14.271678                     00:0c:41:82:b2:55 (RA)  802.11    38 Acknowledgem
  508 14.288526                     00:0d:93:82:36:3a (RA)  802.11    38 Clear-to-ser
  509 14.289515  00:0d:93:82:36:3a  00:0c:41:82:b2:53       802.11   140 Data, SN=101
  510 14.290583                     00:0d:93:82:36:3a (RA)  802.11    38 Acknowledgem
  511 14.338524  00:0c:41:82:b2:55  ff:ff:ff:ff:ff:ff       802.11   168 Beacon frame
  512 14.387524                     00:0c:41:82:b2:55 (RA)  802.11    38 Clear-to-ser
  513 14.388501  00:0c:41:82:b2:53  00:0d:93:82:36:3a       802.11   136 Data, SN=121
  514 14.388511                     00:0c:41:82:b2:55 (RA)  802.11    38 Acknowledgem
  515 14.388519                     00:0d:93:82:36:3a (RA)  802.11    38 Clear-to-ser
  516 14.389492  00:0d:93:82:36:3a  00:0c:41:82:b2:53       802.11   128 Data, SN=102
  517 14.389501                     00:0d:93:82:36:3a (RA)  802.11    38 Acknowledgem
  518 14.389507                     00:0d:93:82:36:3a (RA)  802.11    38 Clear-to-ser
  519 14.390505  00:0d:93:82:36:3a  00:0c:41:82:b2:53       802.11   630 Data, SN=103
  520 14.390522                     00:0d:93:82:36:3a (RA)  802.11    38 Acknowledgem
  521 14.440495  00:0c:41:82:b2:55  ff:ff:ff:ff:ff:ff       802.11   168 Beacon frame
  522 14.460548                     00:0d:93:82:36:3a (RA)  802.11    38 Clear-to-ser

> Frame 519: 630 bytes on wire (5040 bits), 630 bytes captured (5040 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
> IEEE 802.11 Data, Flags: .p.....TC
v Data (570 bytes)
    Data: 71faa9b840ba6eb479817b7a5c319bf77b19fff92ef933cf...
    [Length: 570]

0030  4d 00 00 20 00 00 00 00  71 fa a9 b8 40 ba 6e b4   M·· ···· q···@·n·
0040  79 81 7b 7a 5c 31 9b f7  7b 19 ff f9 2e f9 33 cf   y·{z\1·· {····.3·

Data (data.data), 570 bytes          Packets: 1093 · Displ
```

```
No.   Time       Source                     Destination          Protocol Lengtl Info
  499 14.134544  00:0c:41:82:b2:55          01:80:c2:00:00:00    STP      118 Conf. Root = 32768/0/00:0c:41:82:b2:53  Cost = 0
  500 14.135535  fe80::20d:93ff:fe82:363a   ff02::1:ff82:363a    ICMPv6   152 Multicast Listener Report
  501 14.235542  00:0c:41:82:b2:55          ff:ff:ff:ff:ff:ff    802.11   168 Beacon frame, SN=118, FN=0, Flags=........C, BI=
  502 14.255532                             00:0d:93:82:36:3a (… 802.11    38 Clear-to-send, Flags=........C
  503 14.256515  192.168.0.50               68.87.76.178         DNS      142 Standard query 0xca51 A upload.wikimedia.org
  504 14.256596                             00:0d:93:82:36:3a (… 802.11    38 Acknowledgement, Flags=........C
  505 14.270699                             00:0c:41:82:b2:55 (… 802.11    38 Clear-to-send, Flags=........C
  506 14.271662  68.87.76.178               192.168.0.50         DNS      185 Standard query response 0xca51 A upload.wikimedi
  507 14.271678                             00:0c:41:82:b2:55 (… 802.11    38 Acknowledgement, Flags=........C
  508 14.288526                             00:0d:93:82:36:3a (… 802.11    38 Clear-to-send, Flags=........C
  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 14.290583                             00:0d:93:82:36:3a (… 802.11    38 Acknowledgement, Flags=........C
  511 14.338524  00:0c:41:82:b2:55          ff:ff:ff:ff:ff:ff    802.11   168 Beacon frame, SN=120, FN=0, Flags=........C, BI=
  512 14.387524                             00:0c:41:82:b2:55 (… 802.11    38 Clear-to-send, Flags=........C
  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 (… 802.11    38 Acknowledgement, Flags=........C
  515 14.388519                             00:0d:93:82:36:3a (… 802.11    38 Clear-to-send, Flags=........C
  516 14.389492  192.168.0.50               66.230.200.228       TCP      128 51690 → 80 [ACK] Seq=1 Ack=1 Win=65535 Len=0 TSv
  517 14.389501                             00:0d:93:82:36:3a (… 802.11    38 Acknowledgement, Flags=........C
  518 14.389507                             00:0d:93:82:36:3a (… 802.11    38 Clear-to-send, Flags=........C
  519 14.390505  192.168.0.50               66.230.200.228       HTTP     630 GET /fundraising/2006/meter.png HTTP/1.1
  520 14.390522                             00:0d:93:82:36:3a (… 802.11    38 Acknowledgement, Flags=........C
  521 14.440495  00:0c:41:82:b2:55          ff:ff:ff:ff:ff:ff    802.11   168 Beacon frame, SN=122, FN=0, Flags=........C, BI=

v Hypertext Transfer Protocol
  > GET /fundraising/2006/meter.png HTTP/1.1\r\n
    Host: upload.wikimedia.org\r\n
    User-Agent: Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-O; en-US; rv:1.8.0.9) Gecko/20061206 Firefox/1.5.0.9\r\n
    Accept: image/png,*/*;q=0.5\r\n
    Accept-Language: en-us,en;q=0.5\r\n
    Accept-Encoding: gzip,deflate\r\n

0010  00 38 00 00 87 57 80 32  08 41 2c 00 00 0c 41 82   ·8···W·2 ·A,···A·
0020  b2 55 00 0d 93 82 36 3a  00 0c 41 82 b2 53 70 06   ·U····6: ··A··Sp·
0030  4d 00 00 20 00 00 00 00  71 fa a9 b8 40 ba 6e b4   M·· ···· q···@·n·
0040  79 81 7b 7a 5c 31 9b f7  7b 19 ff f9 2e f9 33 cf   y·{z\1·· {····.3·
0050  cf 40 a6 c8 0d 7d 46 2d  f0 fd a9 72 4a bf d1 10   ·@···}F- ···rJ···

Frame (630 bytes)   Decrypted CCMP data (562 bytes)
IEEE 802.11 wireless LAN (wlan), 32 bytes     Packets: 1093 · Displayed: 1093 (100.0%)    Profile: Default
```

Figure 13: Decode traffic