How to hack your neighbor's Wifi

Exploration of WPA-PSK + Evil Twin

Andrew Schwartz, CIS446, 4.10.24

What is Wifi?

- Wi-fi is a wireless networking technology that uses radio waves to provide wireless high-speed internet and network connections based on the IEEE802.11 family of standards.

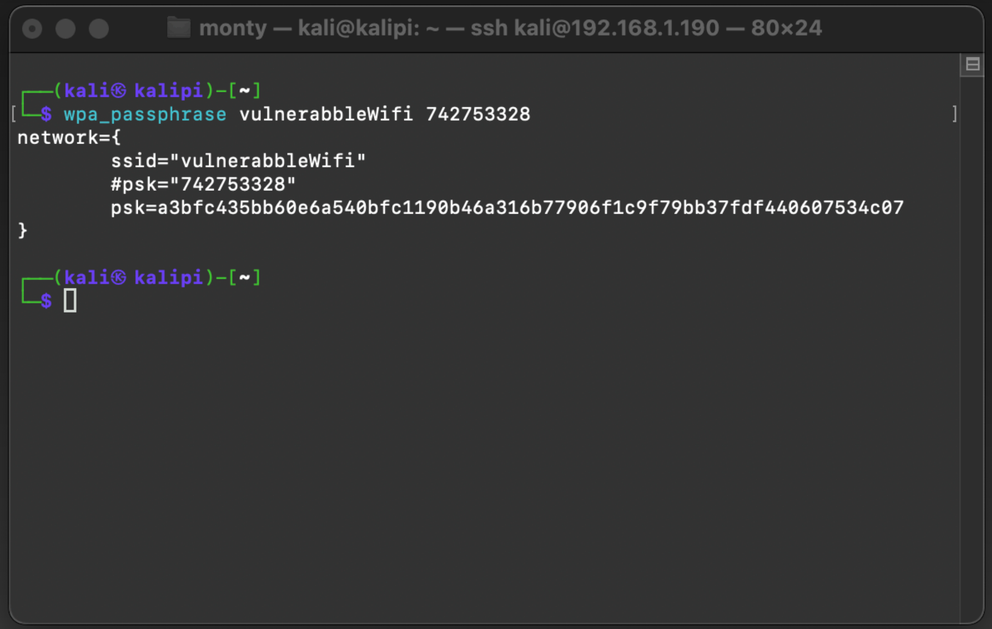
What is Wifi security?

- Wifi security comes in many levels, from the old insecure ways of WEP to the new more secure ways of WPA3.
- Wifi is naturally insecure because of the medium used to transmit data, anyone in the area has the ability to access traffic unlike physical wires like ethernet.
- We will be talking about Wifi Protected Access - Pre-Shared Key

WPA-PSK

The wifi you know

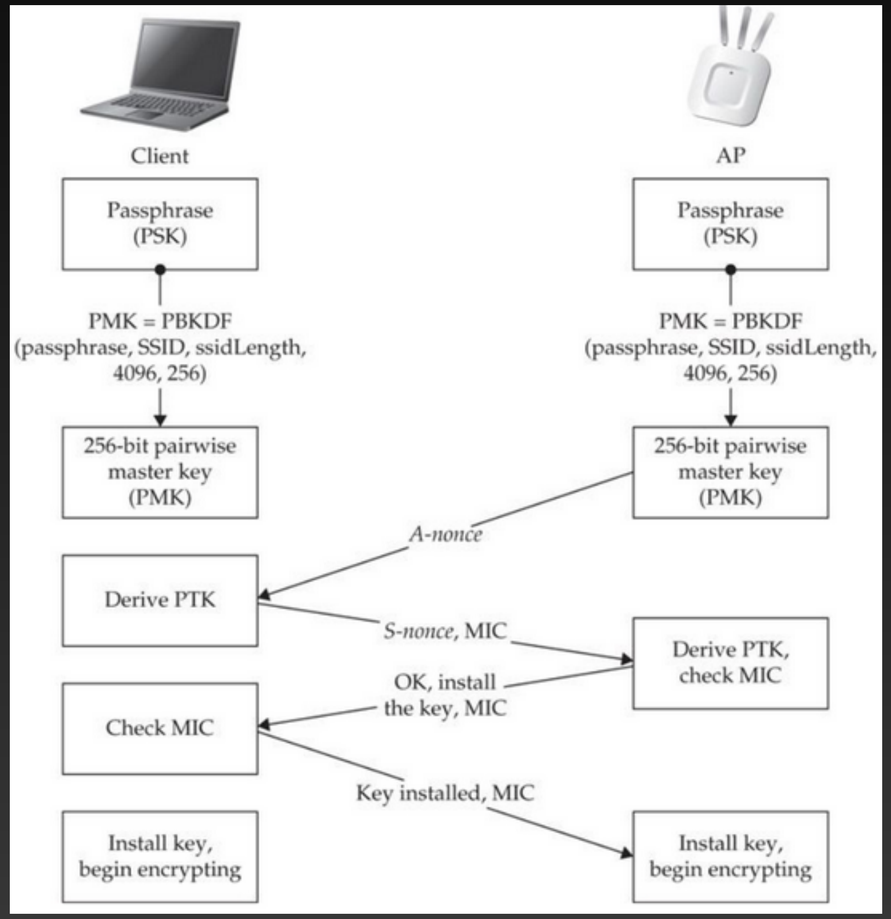
- The type of wifi that you are most familiar with, the “what’s the wifi password?” type of wifi with minimum security.
- The PSK part of the security is the essentially the Wifi password itself. The client and AP generate this PSK.



WPA-PSK Handshaking

Client and AP establish keys

Client

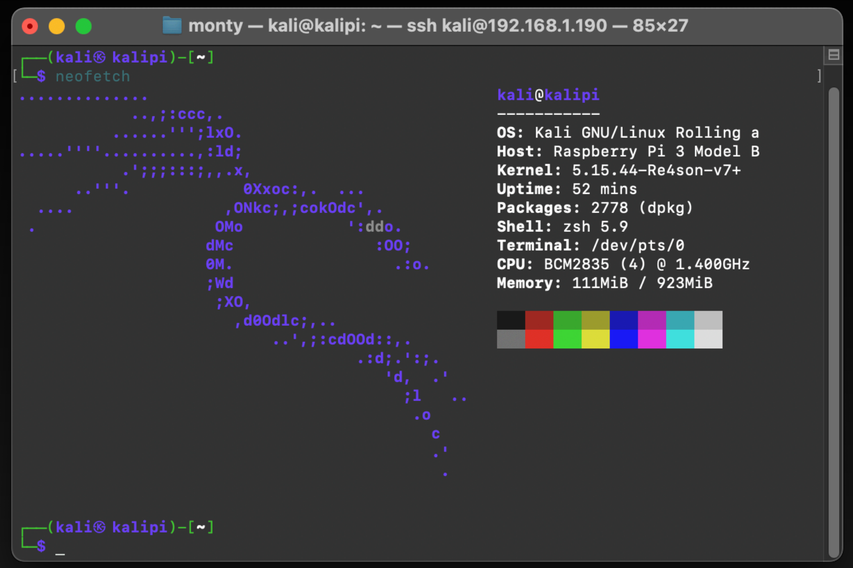


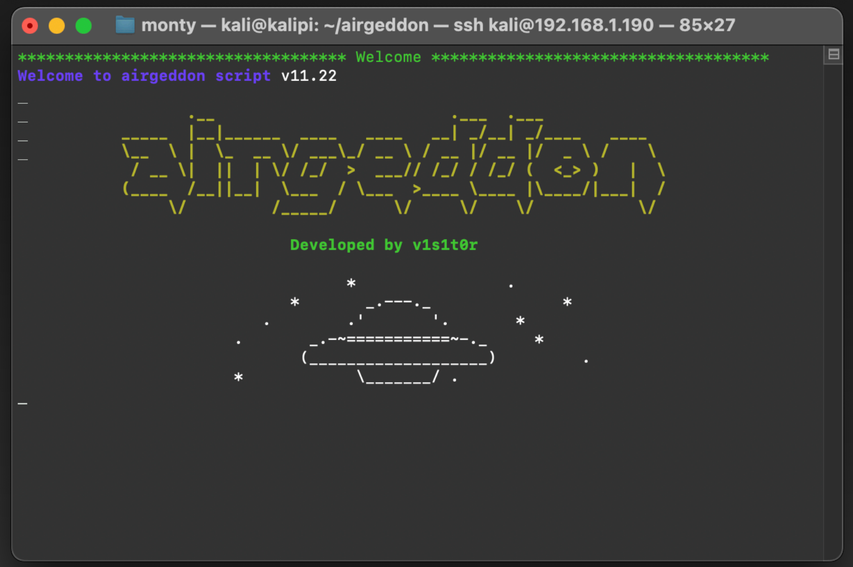
Access Point (router)

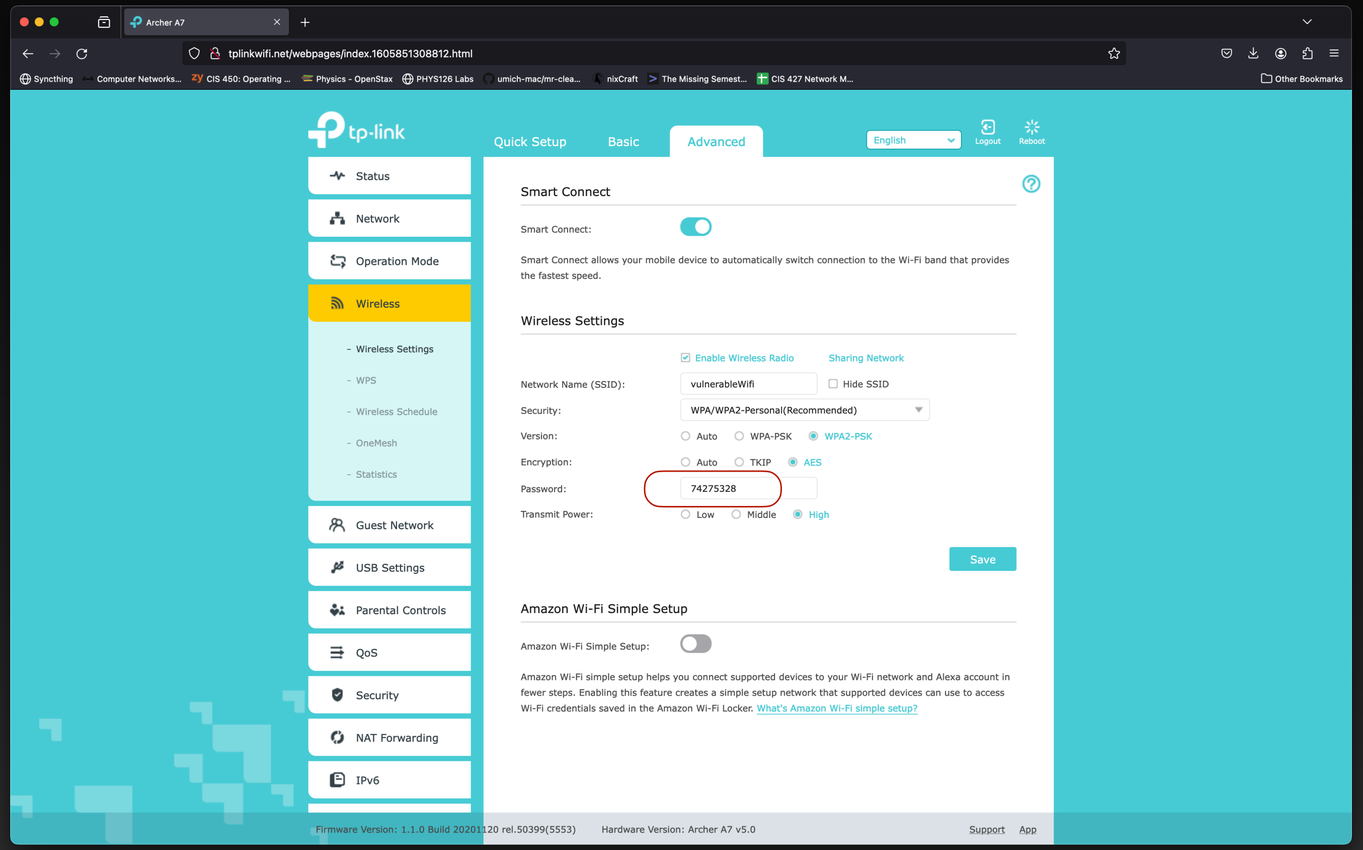
Demo

- Hardware:
  - Rpi 3B+
  - Alfa Networks Wifi Adapter AWUS036ACM (in monitor mode)
  - TP-Link Archer A7 Wifi Router
- Software:
  - Kali Linux Arm and related tools
  - Airgeddon (https://github.com/v1s1t0r1sh3r3/airgeddon)
  - TP-Link proprietary router OS


tp-link
AC1750







*remember the password

Side Note about Monitor Mode

- Monitor mode, or RFMON (Radio Frequency MONitor) mode, allows a computer with a wireless network interface controller (WNIC) to monitor all traffic received on a wireless channel.

- WNIC’s can have many different modes, but are usually in managed mode. Other modes include ad-hoc mode (mesh network), master mode (act as an AP), and monitor mode (sniffing),

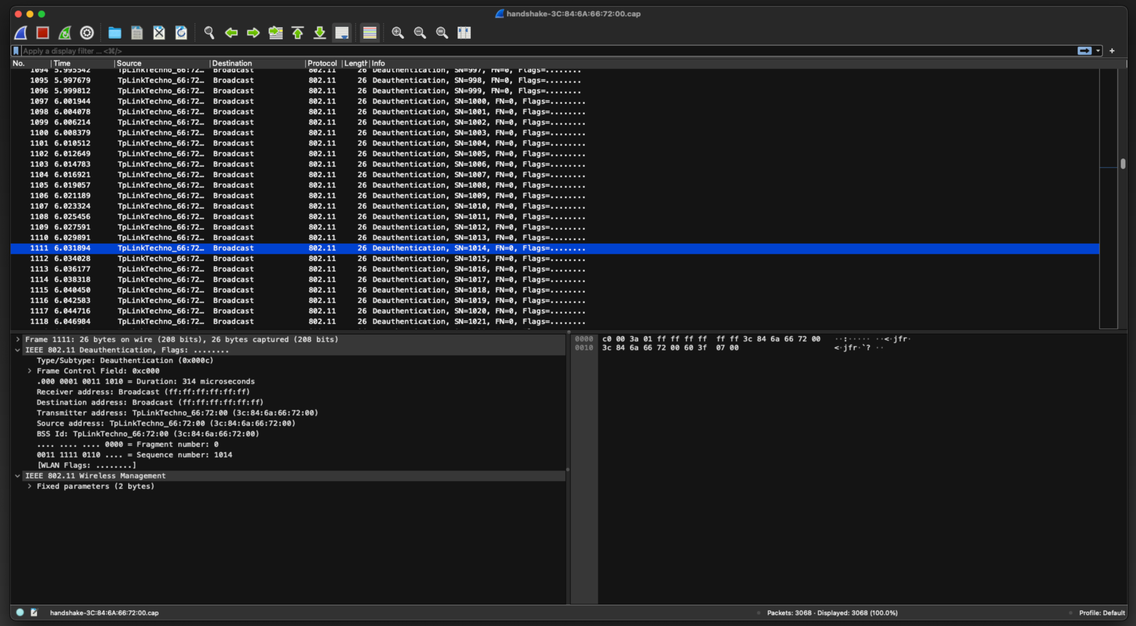
The Attack

Three parts:

1. The DeAuth
2. The Capture
3. The Crack

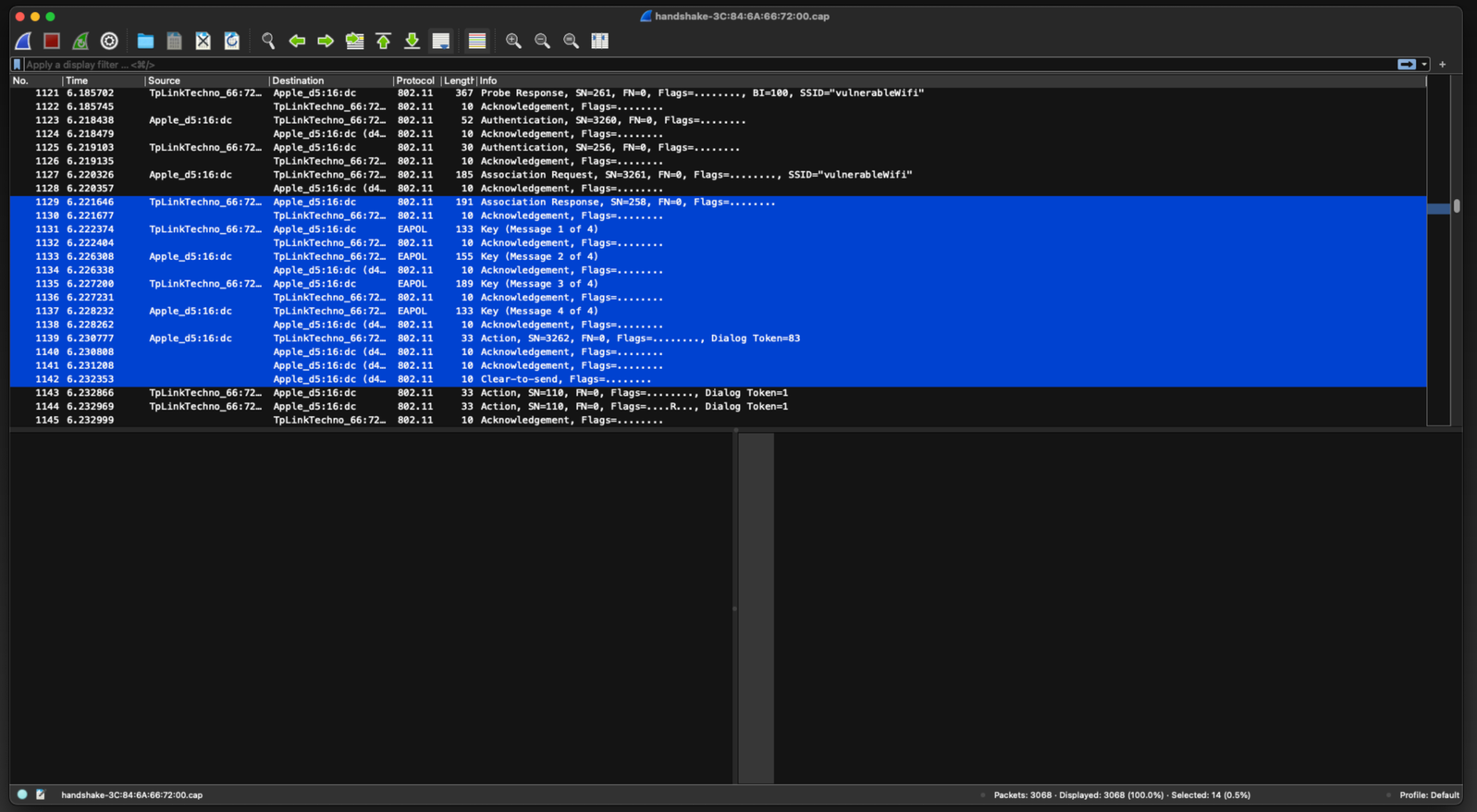
Part One: DeAuthentication

- User’s device (client) is connected to the wifi (AP) already but we (the attacker) need to capture the handshake to be able to crack it. As part of the 802.11 standard there are special DeAuthentication packets that clients may receive from the AP to reconnect to get a stronger signal, etc.
- We can get the AP to broadcast these DeAuthentication packets and get clients to disconnect.

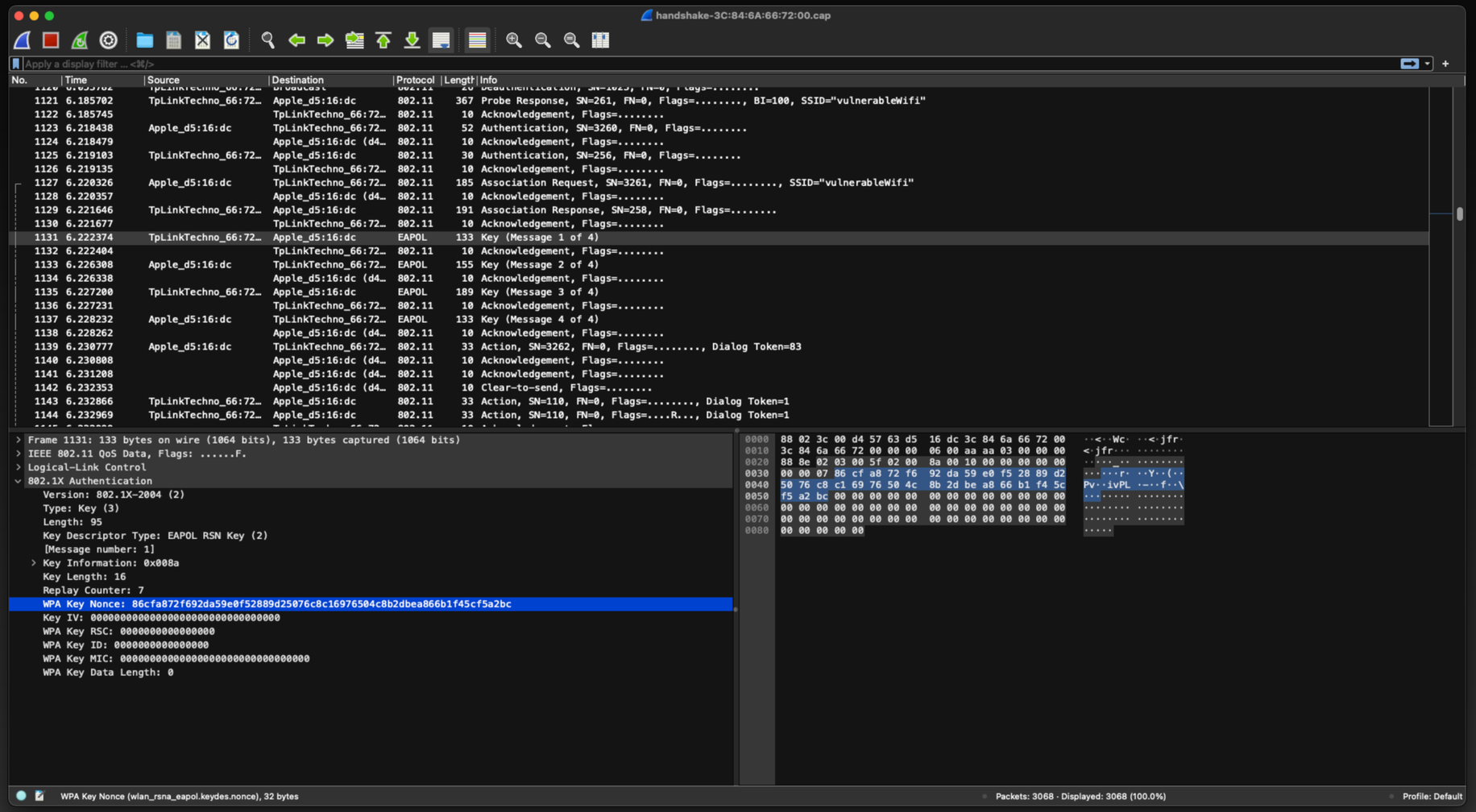


Part Two: The Capture

- Once the client has been DeAuthenticated, we listen for the handshake to take place, capturing all the traffic between the connecting client and the AP.



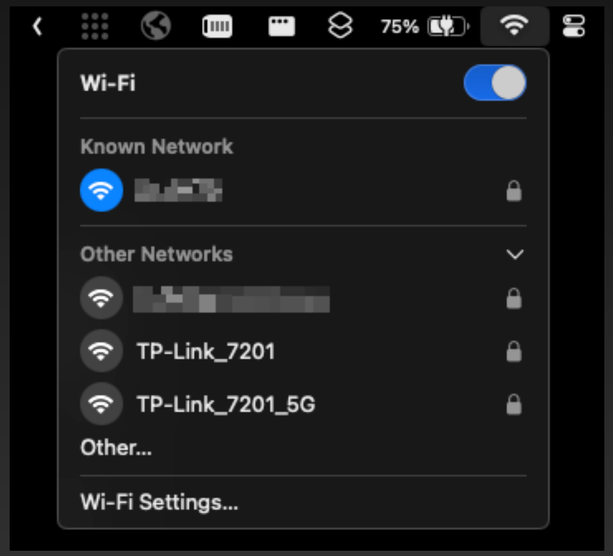
The Capture In Detail



AP sends nonce to Client

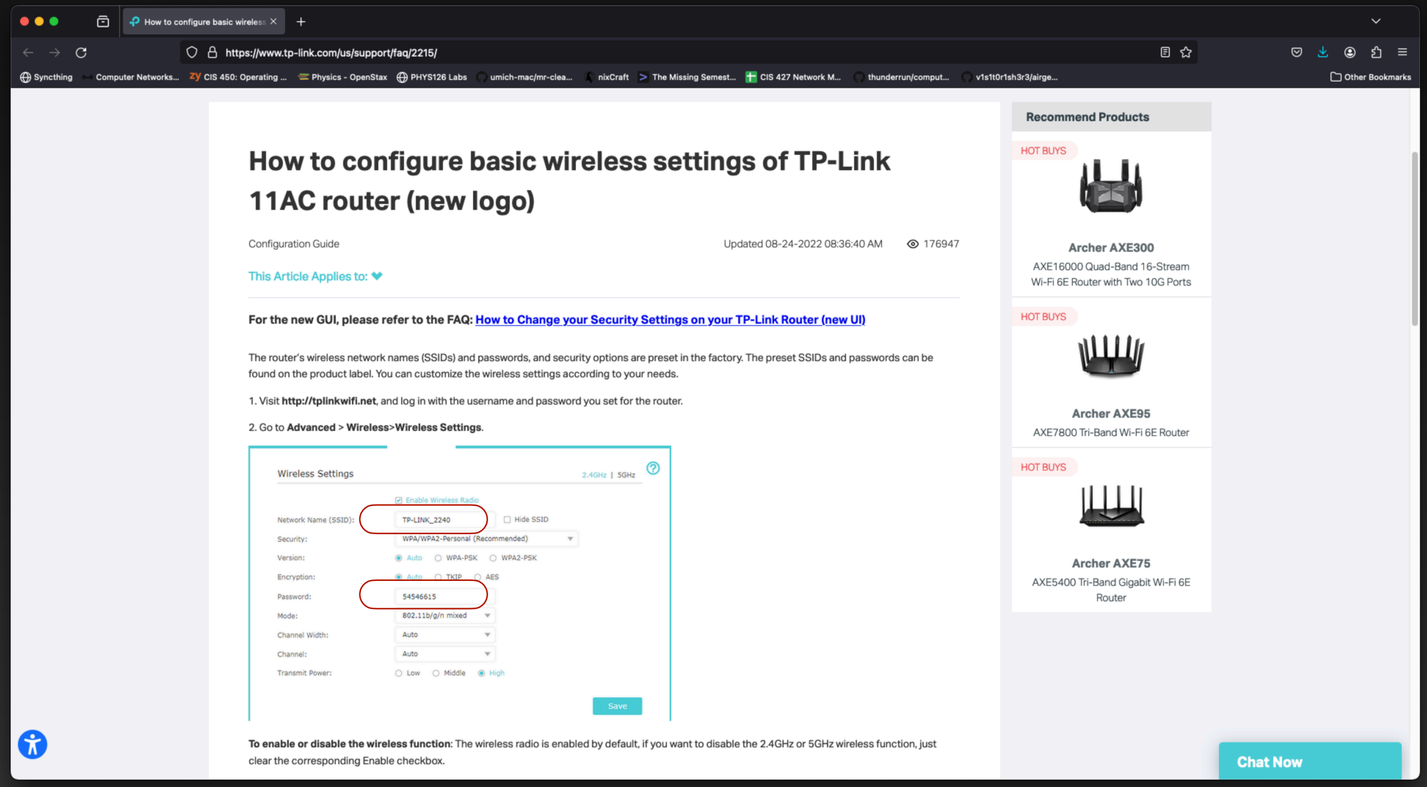
Part Three: The Crack

- As the smart attacker we are, we do some OSINT (open source intelligence) about our target wifi network. We see this as the default network SSID:

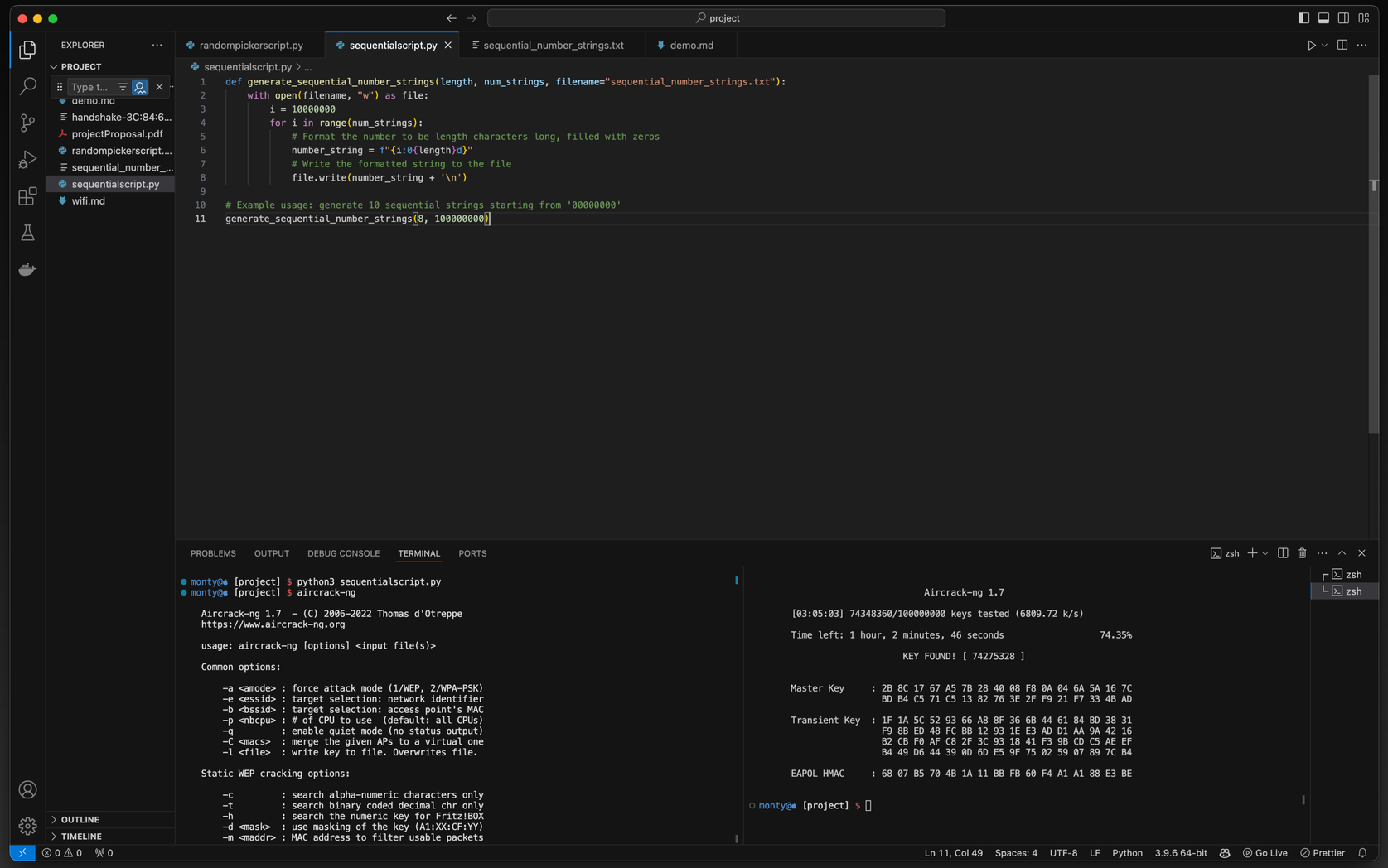


Part Three: The Crack

- So we know we are dealing with most likely a TP router. We look up online the what the default credentials look like. After about 1 minute of googling, we find:

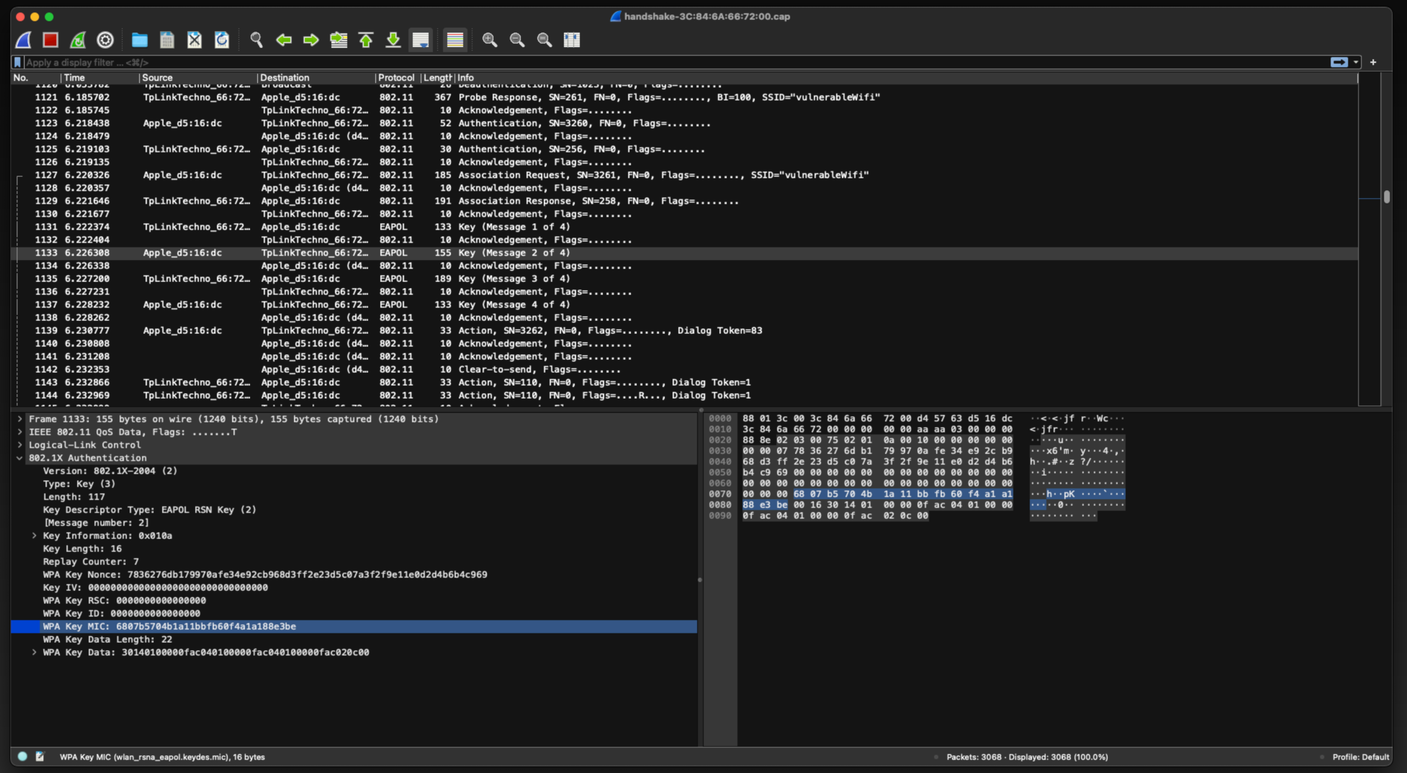


Part Three: The Crack



Part Three: The Crack

```
                                Aircrack-ng 1.7

  [03:05:03] 74348360/100000000 keys tested (6809.72 k/s)

  Time left: 1 hour, 2 minutes, 46 seconds                  74.35%

                          KEY FOUND! [ 74275328 ]


  Master Key     : 2B 8C 17 67 A5 7B 28 40 08 F8 0A 04 6A 5A 16 7C
                   BD B4 C5 71 C5 13 82 76 3E 2F F9 21 F7 33 4B AD

  Transient Key  : 1F 1A 5C 52 93 66 A8 8F 36 6B 44 61 84 BD 38 31
                   F9 8B ED 48 FC BB 12 93 1E E3 AD D1 AA 9A 42 16
                   B2 CB F0 AF C8 2F 3C 93 18 41 F3 9B CD C5 AE EF
                   B4 49 D6 44 39 0D 6D E5 9F 75 02 59 07 89 7C B4

  EAPOL HMAC     : 68 07 B5 70 4B 1A 11 BB FB 60 F4 A1 A1 88 E3 BE

○ monty@ [project] $
```



Congratulations!

You hacked your first Wifi Network.

How to Protect Yourself

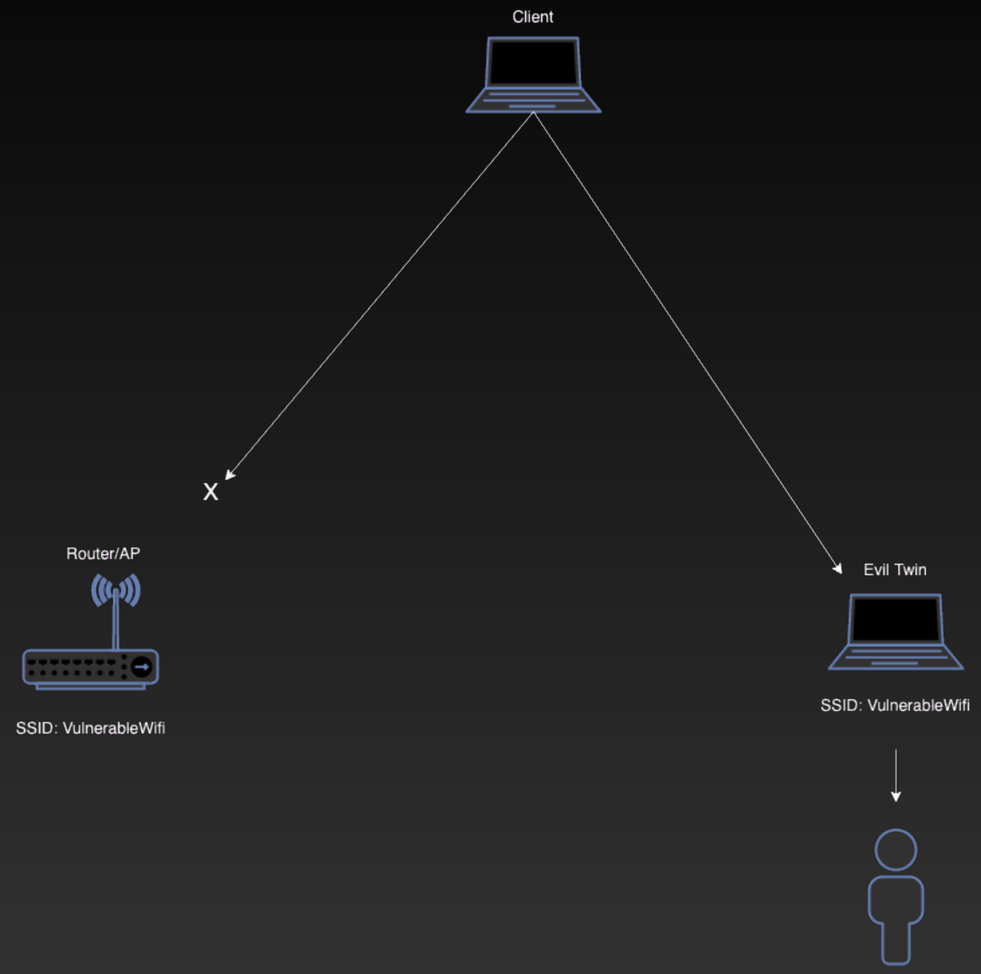
- Set longer and stronger (unique characters) passwords so the keyspace is very large from brute force attacks
- Set more random passwords, as to not hint as things about you
- Use higher security standards like WPA2 or WPA3 that use stronger encryption algorithms
- Don’t use public or untrusted wifi

Evil Twin Attack with Captive Portal

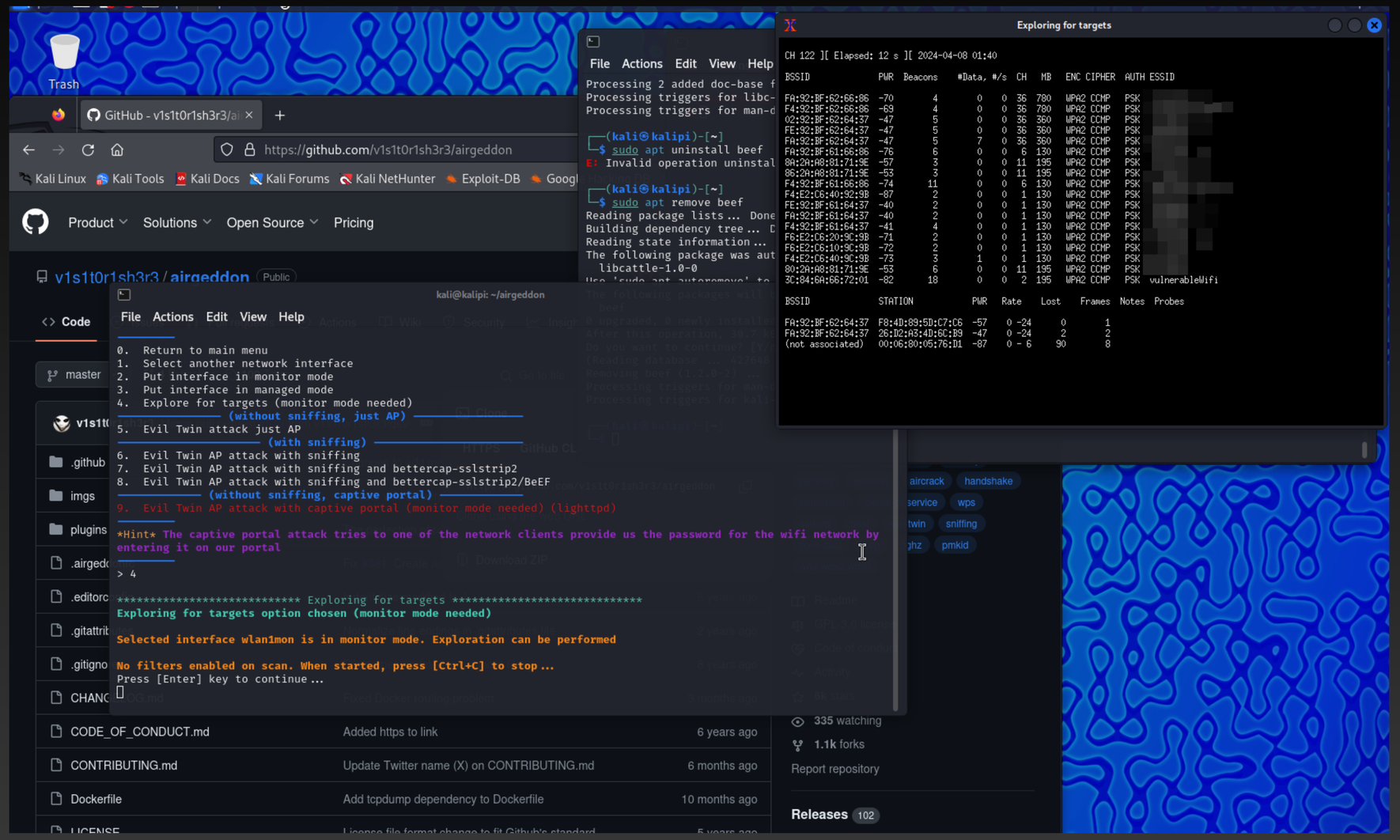
* if time permits

Basic Evil Twin

- A fake Wifi network is put up to connect to, which is actually the attacker.



Airgeddon Evil Twin Attack



Airgeddon searches for networks to attack

Thank you