

# How to Crack a Wep Protected Wi Fi With Airoway and Wifislax

Want to ensure that your home network is secure from intruders? You can hack your own network with free tools to test the strength of your encryption. Using these tools to hack into a network that does not belong to you is illegal. Follow...

Method 1 of 2:

## Starting WiFislax



**Obtain and burn WiFiSlax.** WiFiSlax is an operating system that you will be loading from a CD. It contains the tools necessary to crack WEP encryption on wireless networks. This only works with WEP encryption, not WPA/WPA2. WiFiSlax is available for free from the developer's website.

1. Burn the .iso file that you downloaded to a blank CD. You can use any freeware image burning software to do this. Open the burning software, and select Burn Image. Browse for the .iso file that you downloaded.

**MAINTENANCE VERSION 4.10.1**

Posted on

This version comes to correct a problem with specific equipment froze when trying to use the monitor mode with RT3070 chipset

It has been updated and reconfigured the kernel.

It also has been updated sista during these weeks.

Here the list of changes from 4.10 wifislax -> wifislax 4.10.1

**Wifislax-4.10.1 Changelog \*\*\*\*\***

4.10.1-rc2 wifislax \*\*\*\*\*

20/01/2015

01 - Updated smtube-14.12.0 -> 15.1

01/18/2015

01 - Included wxheditor\_updater

02 - Updated firmware system

03 - Updated package libtool-2.4.2 - 2.4.4 >>


04 - Updated gcc-4.8.3 package -> 4.8.4


05 - Updated gcc-g++ package - 4.8.3 - 4.8.4 >>

06 - Updated freetype-2.5.3 package -> 2.5.5

07 - Updated wxsvg-1.5.2 package -> 1.5.3

08 - Updated list known patterns to version 20150119





Facebook

A 3511 personas les gusta Noticias seguridadwireless.net.

Play in social Facebook

**IMPORTANT LINKS**

- Feed seguridadwireless
- Feed / RSS entries
- Forum seguridadwireless
- Isbotigadelaescatedral
- Live cd Wifislax
- Wireless Security
- Wireless Android
- www.ciudadewireless.com

wikiHow

2.

**Check your computer's hardware.** In order to run this crack, you will need the IPW3945 chipset. To find out if your computer possesses the chipset, open the command line by clicking Start and then entering CMD into the Search or Run box. Once you have access to the command line, type "ipconfig /all". Look for "Intel PRO/Wireless 3945ABG Network Connection". This is a common chipset on many laptops.

1. In other operating systems like Linux-based ones, you can download programs like **hardinfo** to obtain a complete list of the hardware of your computer



**Wifislax**  
Slackware Based System

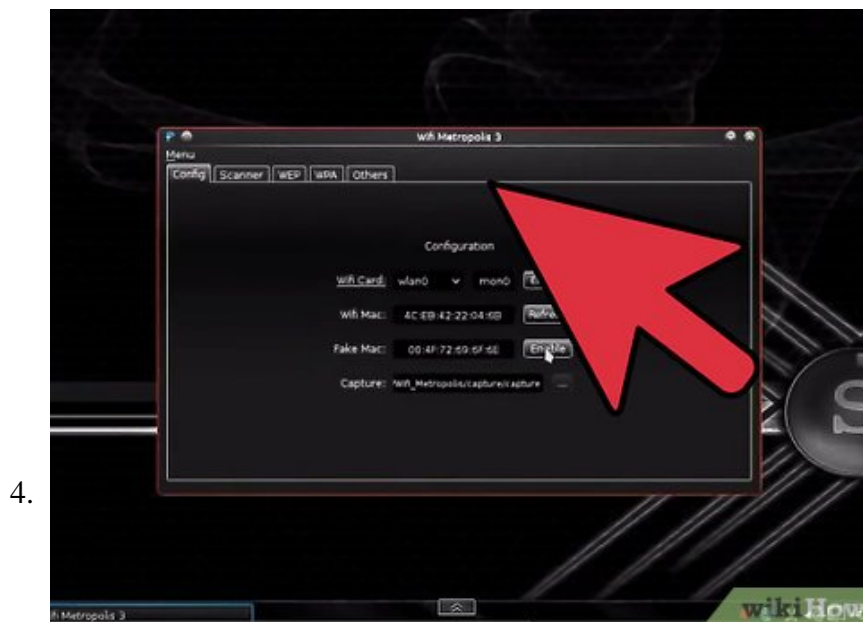
wikiHow

3.

**Set your computer to boot from CD.** In order to use WiFiSlax, you will need to make sure that your computer can boot from the CD drive. TO do this, reboot the computer and open the BIOS menu. You can access the BIOS menu when you see the computer manufacturer's logo. The key you need to press will be displayed on the screen. It is typically F2, F10, F12 or Del.

1. In the BIOS screen, navigate to the Boot menu. Set the first boot device as the CD/DVD drive. This is sometimes labeled as an optical drive. Setting it first will make the computer try to boot from the

CD before it loads the operating system from the hard drive like it normally would.

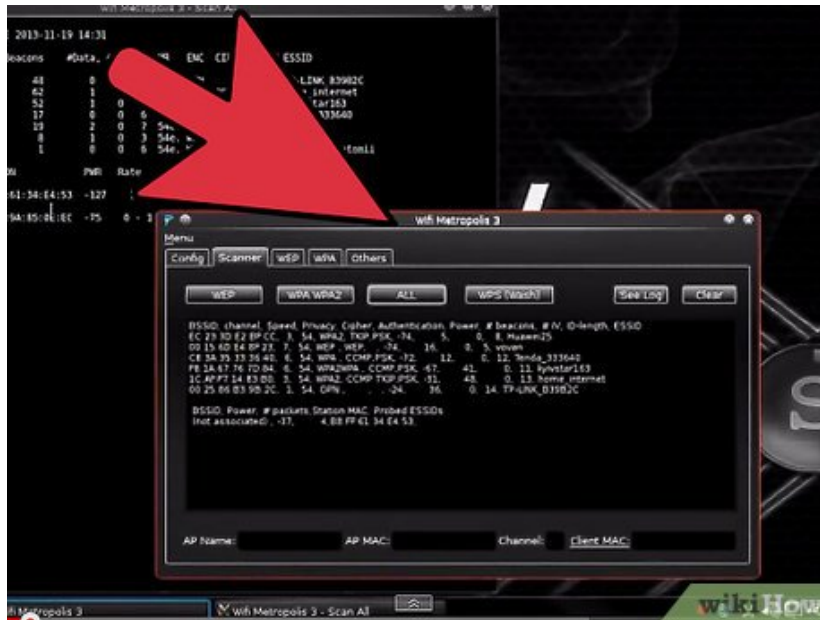


**Run WiFiSlax.** After adjusting your BIOS settings and rebooting your computer, press a key when prompted to boot from the CD. When presented with the first menu, select No PCMCIA and then press Enter.

1. Log in with the credentials:
  1. *User:* root
  2. *Password:* toor
2. Enter the command "startx" to start WiFiSlax with a graphic interface.

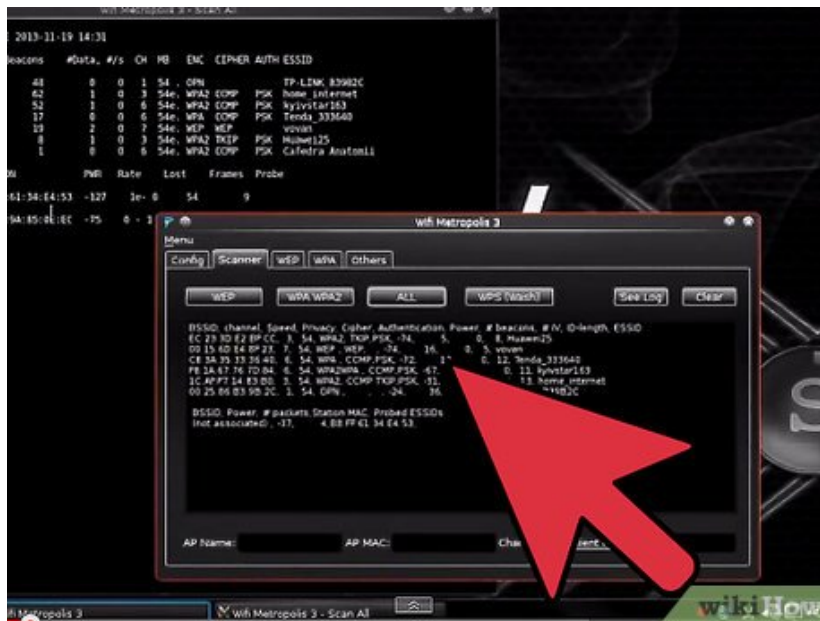
Method 2 of 2:

## Cracking the WEP



1.

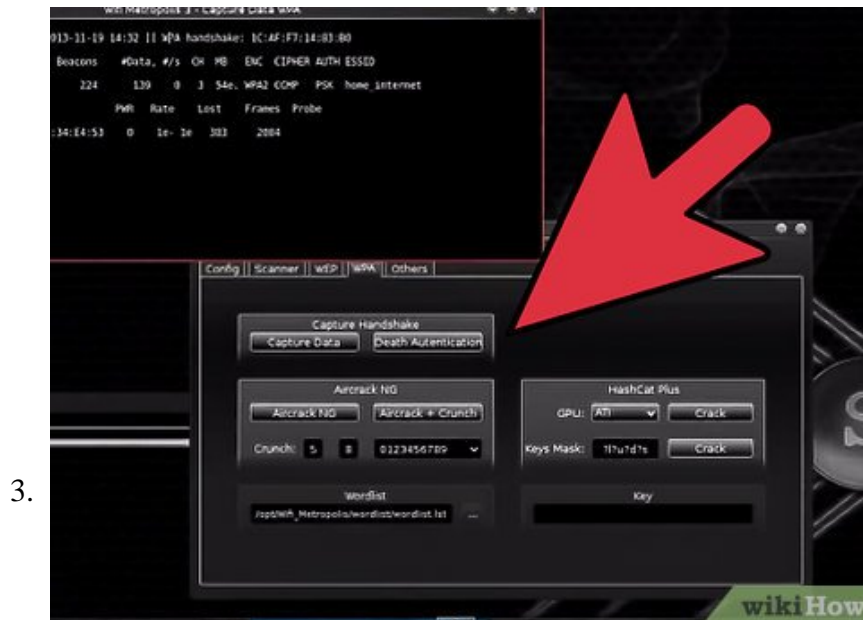
**Start the scanning process.** Click the Start menu, and navigate to WiFislax > Asistencia chipset > Asistencia Intel pro wireless > Cargar ipw3945 inyección - ipwray-ng. This will put your network card into wifi0 mode, which is the monitor mode.



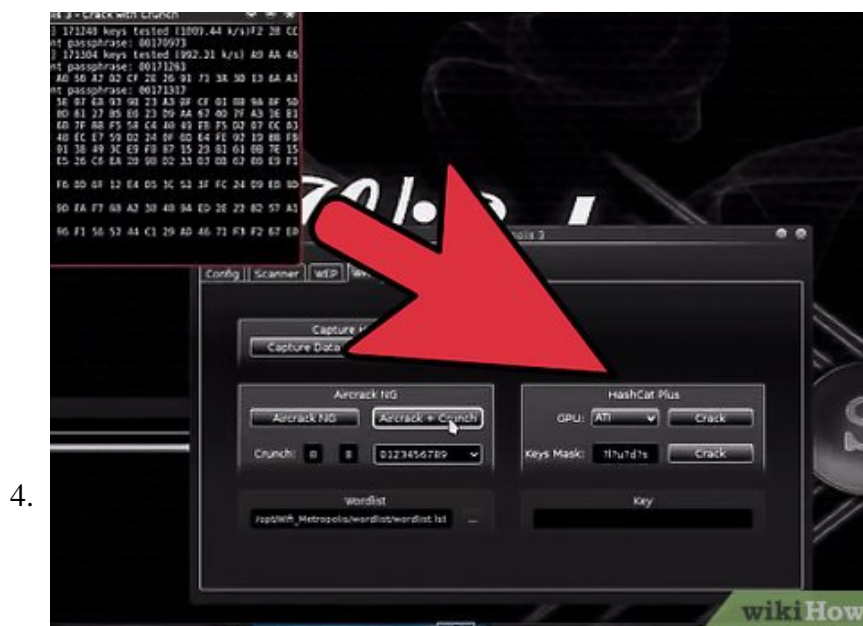
2.

**Enter the command "airodump-ng wifi0".** This will display all of the WiFi data that your card collected while in monitor mode.

1. You will need to make note of the BSSID with the most beacons. The BSSID is the name of the network, and the number of beacons indicates signal strength. The more beacons you have, the easier it will be to crack. Make note of the channel (CH) that the network occupies.



**Open Airoway.** Click Start, and then navigate to WiFiSlax > Herramientas Wireless > Airoway. This will open multiple windows with command lines.



**Select the channel.** In the Airoway Command window, select the channel of the BSSID that you want to crack. Press Enter to begin the cracking process. Select the access point that you want to crack by pressing the associated number.

1. Once you've selected the access point, a new menu will open. Select option 2 to associate a MAC address and then option 3 to replay live ARPs (this will speed the crack process up).

5.



**Wait for packets to accumulate.** Once the process has begun, you will need to wait a few moments as the program collects packets. The more packets you have, the greater chance you have at cracking the WEP.

1. When the Data category in the Scan window reaches between 20,000-30,000 press 8 on the keyboard to crack the key.

6.



**Copy the key.** If the attack was successful, the key will be displayed in the bottom-right window. It will be listed next to the words KEY FOUND. Make sure that the Decrypted Correctly value is at 100%, or else the key will not work.

1. The key will be displayed both in hexadecimal and ASCII format. The ASCII key is the one typically entered in when connecting to the network.

You finished reading the article "**How to Crack a Wep Protected Wi Fi With Airoway and Wifislax**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

