**What is Evil Twin Attack and How it works?[6]**

An evil twin is a fake Wi-Fi access point used to steal passwords, either by monitoring connections or by phishing.  Fake access points are set up by configuring a wireless card to act as an access point, giving it the same SSID and BSSID as a nearby Wi-Fi network.

**Process of Evil Twin Attack**

1) Scan the networks.

2) Select network.

3) Capture handshake (can be used without handshake)

4) We choose one of several web interfaces tailored for me (thanks to the collaboration of the users)

5) Mounts one FakeAP imitating the original

6) A DHCP server is created on FakeAP

7) It creates a DNS server to redirect all requests to the Host

8) The web server with the selected interface is launched

9) The mechanism is launched to check the validity of the passwords that will be introduced

10) It deauthentificate all users of the network, hoping to connect to FakeAP and enter the password.

11)   The attack will stop after the correct password checking

Requirements To hack Wifi Password Without using Wordlist

1)   Laptop

2)   WifiSlax (Operating System)

3)   Linset (Mostly Inbuilt)

4)   Pendrive or Flash Drive (2gb or higher)

5) Universal USB Installer

Software Requirements for Linset

[Aircrack-ng](https://www.darknet.org.uk/2007/10/aircrack-ng-wep-and-wpa-psk-key-cracking-program/), Aireplay-ng, Airmon-ng, Airodump-ng, Awk, Curl, Dhcpd, Hostapd, Iwconfig, Lighttpd, Macchanger, Mdk3, Php5-cgi, Pyrit, Python, Unzip, Xterm

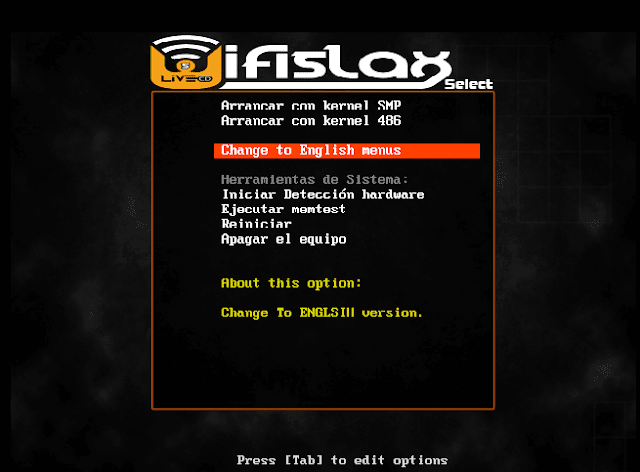
As it’s a BASH script, there’s quite a list of external apps required to perform evil twin attack successfully, like Linset.

How To hack Wifi Using Evil Twin Attack Using Linset

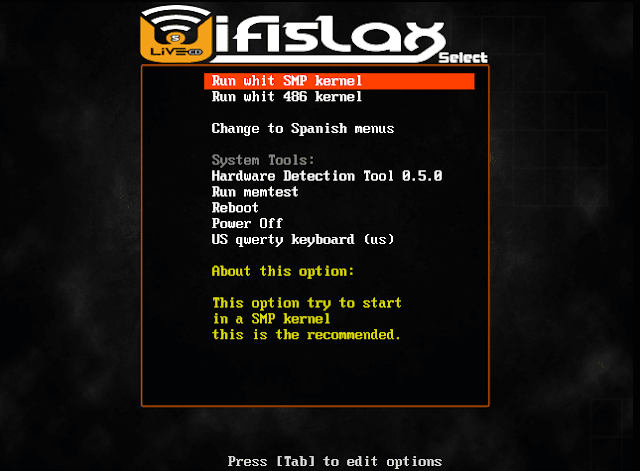
Step 1: Install WifiSlax in Flash Drive or Pendrive using universal usb installer

Step 2: Start WifiSlax

1. Click on “Change To English Menu”

[](https://2.bp.blogspot.com/-u73OW4tjerw/WPzgrgyKYlI/AAAAAAAAEj0/OUDuJuKpVG017T5q9tcl0_KTJbjNkhc7wCLcB/s1600/start%2Bwifislax.png)

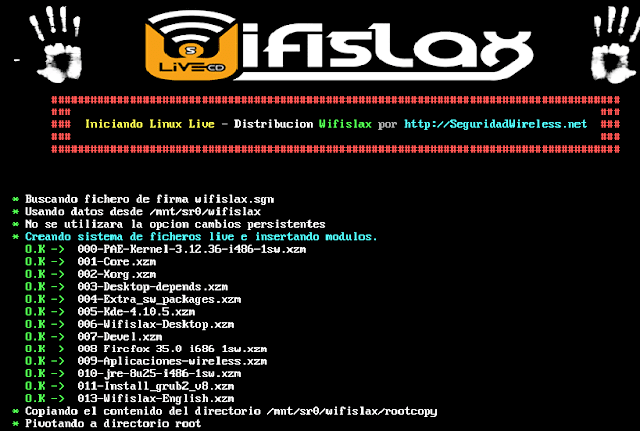
2)   Click on “Run with SMP Kernel”

[](https://1.bp.blogspot.com/-1YQjn_azjbE/WPzg06D46II/AAAAAAAAEkA/gscofkP0lF8wQ7-bzEzNIsdaHaGflCSPQCLcB/s1600/2-min.png)

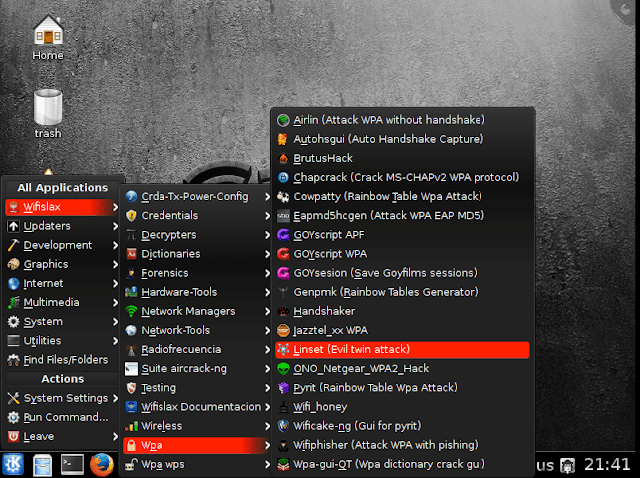
3)   Click on “WifiSlax with KDE Desktop”

[](https://2.bp.blogspot.com/-tfSST4U7qAI/WPzg0mkJFVI/AAAAAAAAEj8/HMQiUPrznbYuXsxGNxszec9zfnDD4t3CACEw/s1600/3-min.png)

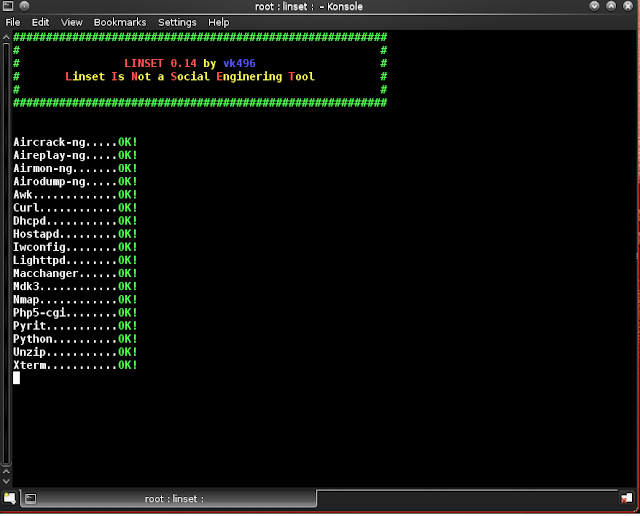
4)   That’s it WifiSlax will start now

[](https://3.bp.blogspot.com/-is8HyG2ogdo/WPzg0oepjmI/AAAAAAAAEj4/XCcEfJB8smEMTHyo4R8dAEhY8OCCHytIwCEw/s1600/4-min.png)

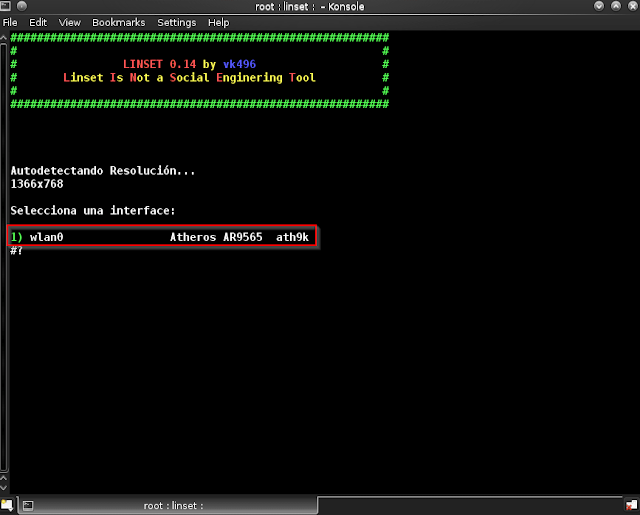
Step 3: Go to WifiSlax à WPA à Linset (Evil Twin Attack)

[](https://2.bp.blogspot.com/-VW_QXJ9Y5jw/WPzg1qatgRI/AAAAAAAAEkI/koxybTdA4Pc3em0SvrLkVqoq6WYtnFwVQCEw/s1600/5-min.png)

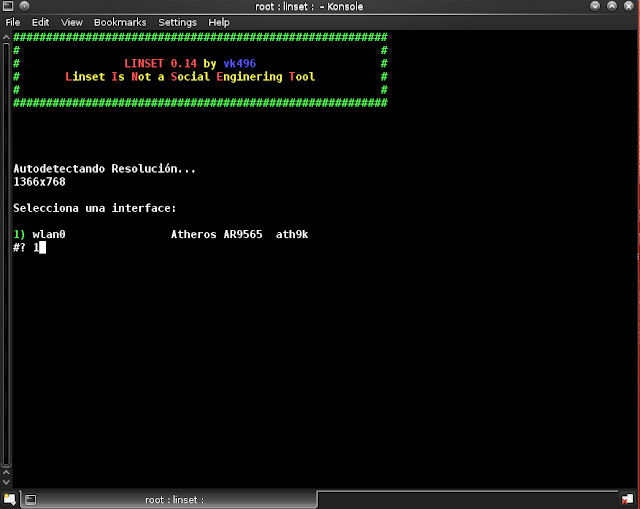
Step 4: Linset will Start required Tolls

[](https://3.bp.blogspot.com/-N4hd-dbpFJM/WPzhguyTihI/AAAAAAAAEkU/2ZIgi5SZuUExbOLqGs30yrQuEHmPVvLZACLcB/s1600/snapshot1-min.png)

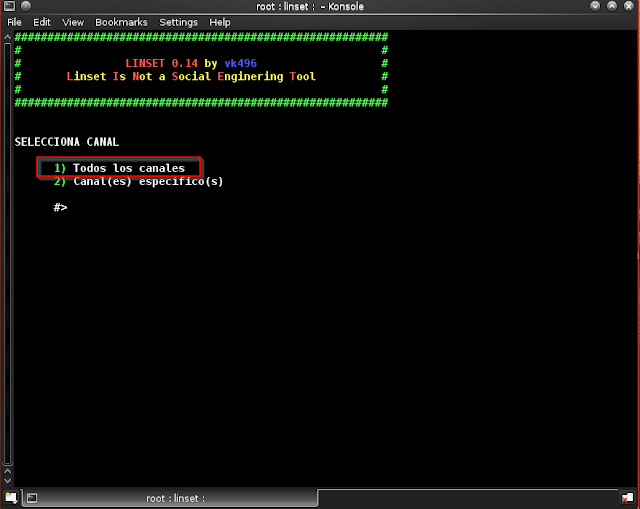
Step 5: Select Wlan0

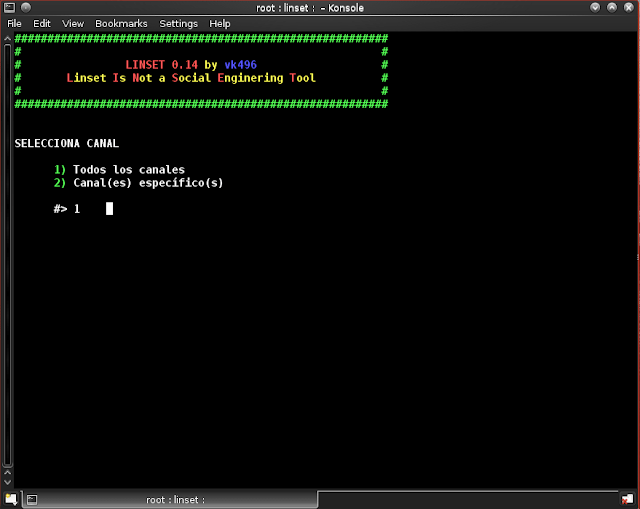
[](https://1.bp.blogspot.com/-RyfEX2yrvZU/WPzhkm6qQOI/AAAAAAAAElM/Zp3TFUdJpMY1y7T5rWTVoE4kE57RJsHhgCLcB/s1600/snapshot3-min.png)

Step 6: type “1” to select Wlan0

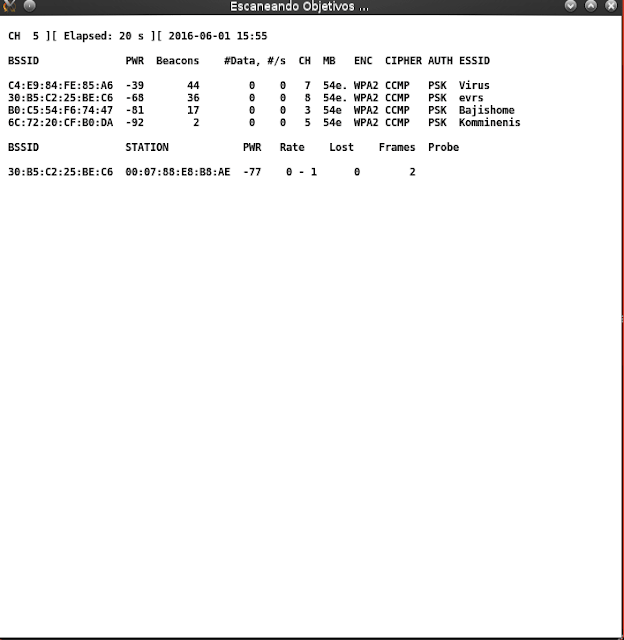
[](https://4.bp.blogspot.com/-zUawT3QVJvE/WPzhk1JlAWI/AAAAAAAAElI/kmPt_wNpyN080e9QrLBrQmx2rrK-l-lKwCEw/s1600/snapshot4-min.png)

Step 7: Enter “1” to select “todos los canales” which means select all channels. We need to search all channels to get all the networks available near you. If you want to hack a particular network whose channel number you know already, select 2 and proceed.

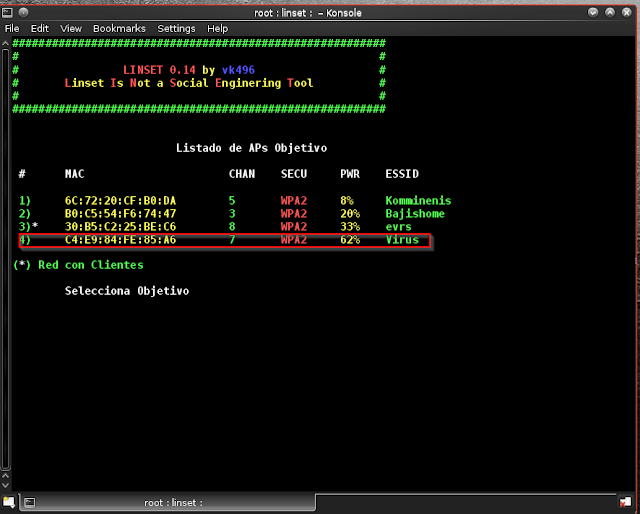
[](https://1.bp.blogspot.com/-z4epjWrFHS4/WPzhlLQkliI/AAAAAAAAElQ/MGb2-E-HmkwKZsjyiiBYWTDRcpMK34gzACEw/s1600/snapshot5-min.png)

[](https://3.bp.blogspot.com/-8RBk6DXQkIM/WPzhlRV-l3I/AAAAAAAAElY/kkyxlvyOoVQbf0kipaLOwP6WxjkafcWGACEw/s1600/snapshot6-min.png)

Step 8: All the Available networks will be shown now, wait for 2-3 mins to complete the search and click “CTRL +C” To stop the search

[](https://3.bp.blogspot.com/-WZusEv1bxbQ/WPzhleT-vKI/AAAAAAAAElU/tLZhHdFqJdU1VRZ0J5X1J8u2IMJ8koLigCEw/s1600/snapshot7-min.png)

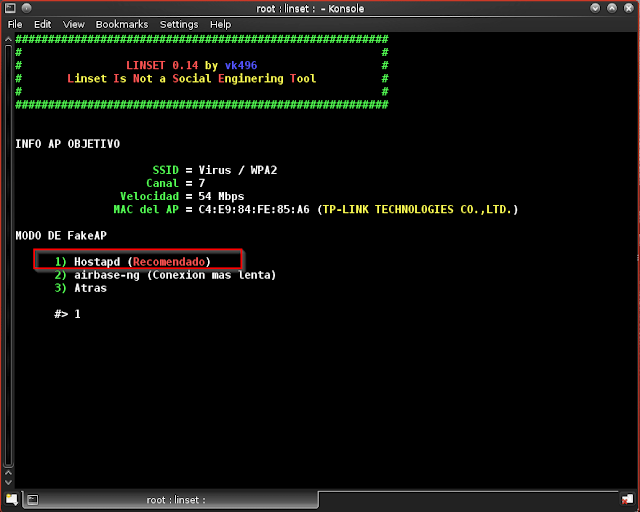
Step 9: Select the network that you want to hack from the list shown as in the below picture

[](https://3.bp.blogspot.com/-U6t7UHTYaB0/WPzhl4yeXuI/AAAAAAAAElc/B3L0WJRZvRwQ7ykoPROqBoDxdfqf4T5bwCEw/s1600/snapshot8-min.png)

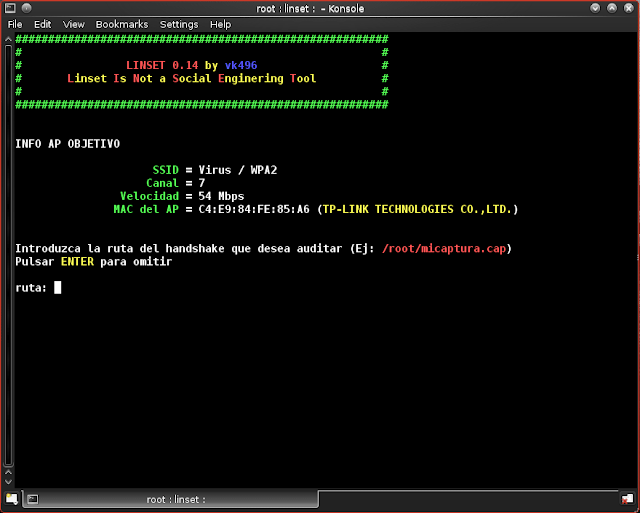
Step 10: Enter the number of the network that you want to hack.

[](https://1.bp.blogspot.com/-kCsLdX-Mb0g/WPzhgtTF_rI/AAAAAAAAEkQ/5G_xQZB3V4gltu2gv8Ztgsq2hnl4DGZ3wCEw/s1600/snapshot10-min.png)

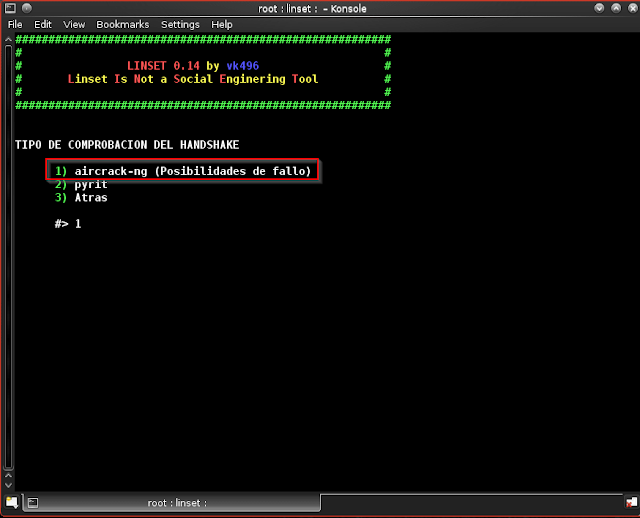
Step 11: Now we need to select hostpad, so type “1”

[](https://4.bp.blogspot.com/-CvMC3xY3Y_Y/WPzhgqP-FTI/AAAAAAAAEkM/Jg9regKsoPsJrBj90iEcXj-tdN6vQrg6QCEw/s1600/snapshot11-min.png)

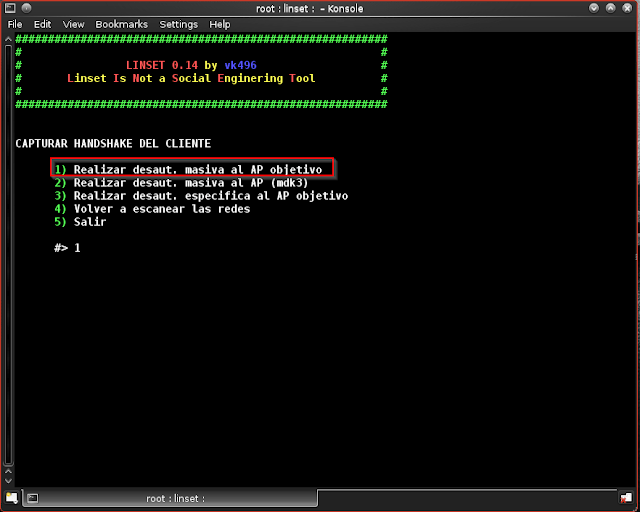
Step 12: we should enter the path of the handshake, by default it takes some root/micaprura.cap, so just Hit “Enter” without typing anything

[](https://4.bp.blogspot.com/-mFfVTCh_Qz0/WPzhhnrLZhI/AAAAAAAAEkY/--MpuZsoMkcyJOfKDBVPiStu6r1W07UqACEw/s1600/snapshot12-min.png)

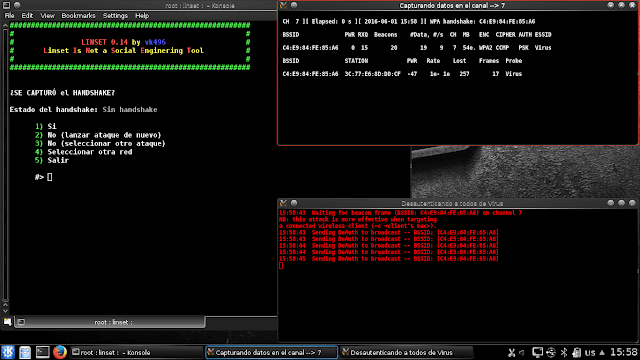
Step 13: we want to capture handshake using aircrack-ng, so enter “1”

[](https://1.bp.blogspot.com/-Dj2FNAPBilk/WPzhh1L01uI/AAAAAAAAEkg/wJRlvcfFkLE86kdimmSrlglH7AQNI1OnwCEw/s1600/snapshot13-min.png)

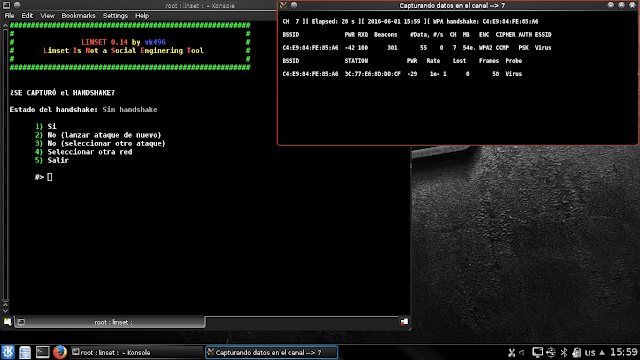
Step 14: we need to deactivate the process after the handshake is created, so select “realizar desaut. masiva al ap objetivo” that is option “1”

[](https://1.bp.blogspot.com/-NqvqdEp3jZs/WPzhhlorfII/AAAAAAAAEkc/73l0Fw8BT7Ug1M4KsGgLb4rEY2GCv1L_wCEw/s1600/snapshot14-min.png)

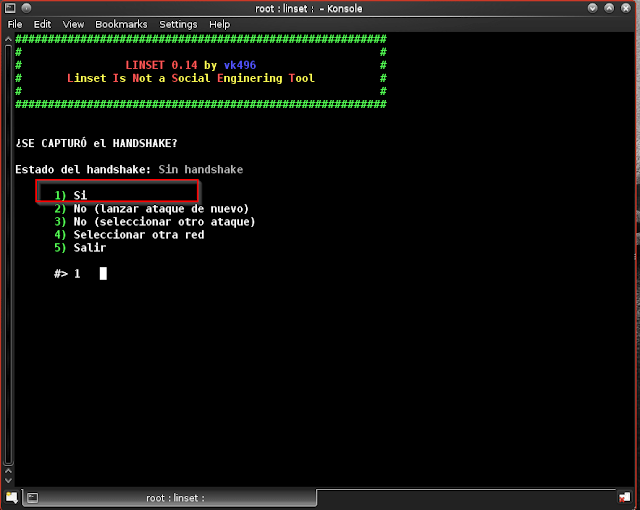
Step 15: Now Handshake capturing process will start, and 2 windows will open. We need to capture handshake compulsorily to proceed.

[](https://1.bp.blogspot.com/-sF0imwgxw9M/WPzhiLUH9VI/AAAAAAAAEkk/jkx5m8ZIOussR8RUIgiHg0HJn42yoqIlACEw/s1600/snapshot15-min.png)

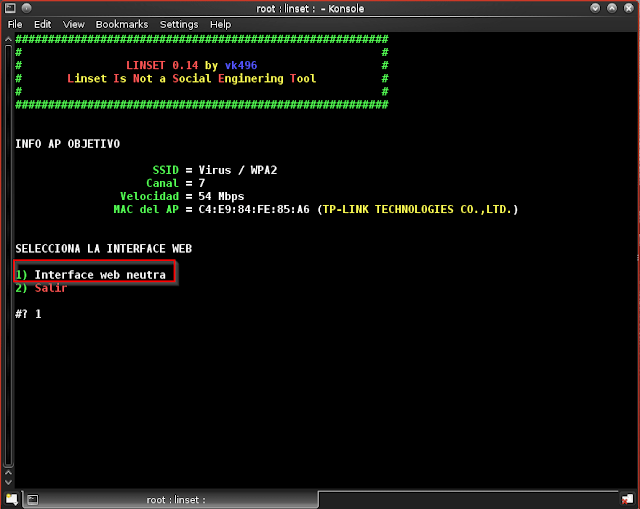
Step 16: After the Handshake is captured, close the de authentication box

[](https://2.bp.blogspot.com/-OIa0Y5n0Gok/WPzhiWaeiqI/AAAAAAAAEko/rw5MMPzYYiMwiYlS_Fcrd-0M81kIUXKCACEw/s1600/snapshot16-min.png)

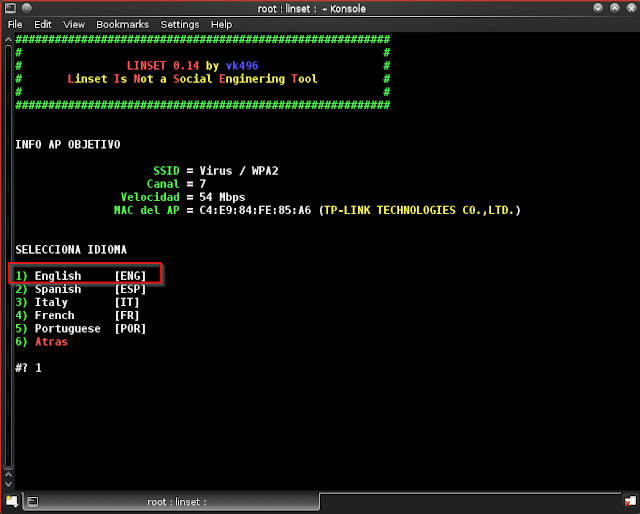
Step 17:  Select “Si” which means “Yes”. So, Enter “1”

[](https://3.bp.blogspot.com/-tjaeXwF2zKI/WPzhitsdm8I/AAAAAAAAEks/hZqkd1XAN20k-tj_PKYIZL-R_duTb8PkACEw/s1600/snapshot17-min.png)

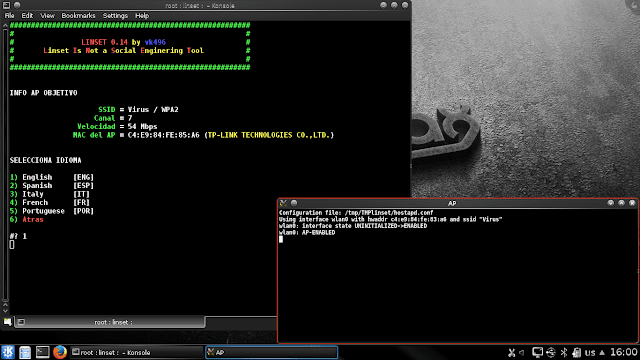
Step 18: Select “Interface Web Nutra”. So, Enter “1”

[](https://2.bp.blogspot.com/-ivmVkvyO7l4/WPzhi_pxyyI/AAAAAAAAEkw/DPB_Q3XKdSEIrwWtCOrMpPrstnbSdqRDQCEw/s1600/snapshot19-min.png)

Step 19: Select the Language.

[](https://2.bp.blogspot.com/-kzxN9xJVabo/WPzhjDH8OLI/AAAAAAAAEk0/Ujajnl9nMgswJULYGUwu5AIcIdEHLSIpQCEw/s1600/snapshot20-min.png)

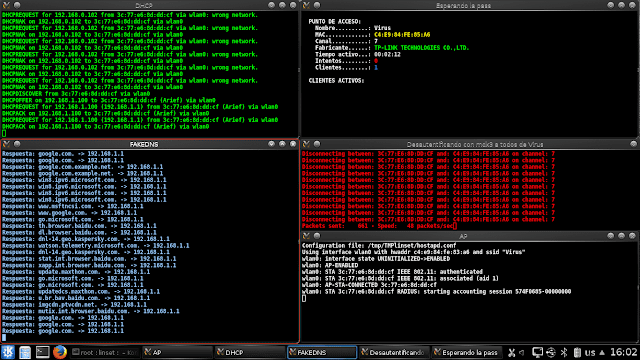
Step 20: Now the main process will start DHCP, fake dns, AP, deauth all, and wifi info dialog boxes will open. We wait until the client is connected to the network.

[](https://1.bp.blogspot.com/-0L7xNt0VfSA/WPzhjAetwEI/AAAAAAAAEk4/rVDwS2fXgccCqnlw8cifeB4L1qBm1wErQCEw/s1600/snapshot21-min.png)

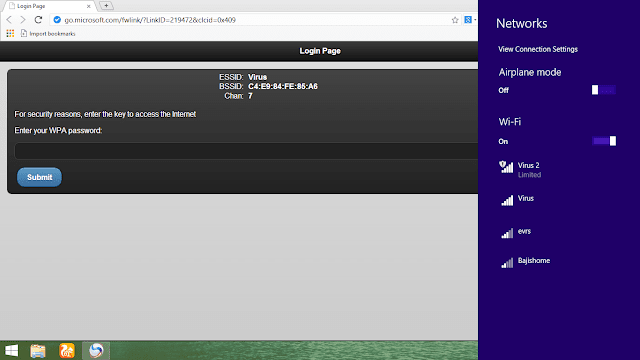
Step 21: Until we terminate the procedure, the victim cannot access their internet connection. They won't be able to receive any packets from our fake access point or false network signal because Dhcp and deauth will all prevent them from doing so.

A DOS attack is launched during this procedure, causing the victim to lose internet access and perceive it as having a "Limited Connection."

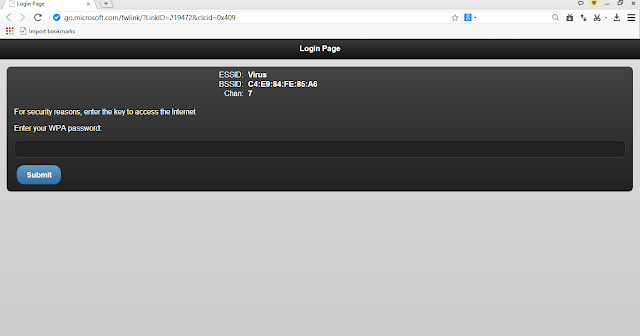
At this stage, you have the option to listen in on the victim. All of the websites they visit are visible to you, and FAKE DNS displays every single detail.

[](https://2.bp.blogspot.com/-BvvnI9IzA3I/WPzhjkWQaUI/AAAAAAAAElA/IKDgDQpr5Q4JuG96dbA-haRvQYz0HFWAgCEw/s1600/snapshot23-min.png)

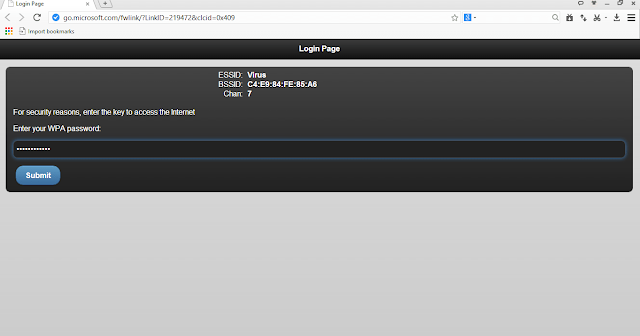
Now we see what happens when the process is started Original network gets disconnected and our newly created fake network with same name connects to victim’s network and a page pop’s up

[](https://4.bp.blogspot.com/-ojzM5StQXWM/WPzlDo24xFI/AAAAAAAAEl0/-Q986Yu36Sgewol4HZEOWGCUY04n60idgCLcB/s1600/1-min.png)

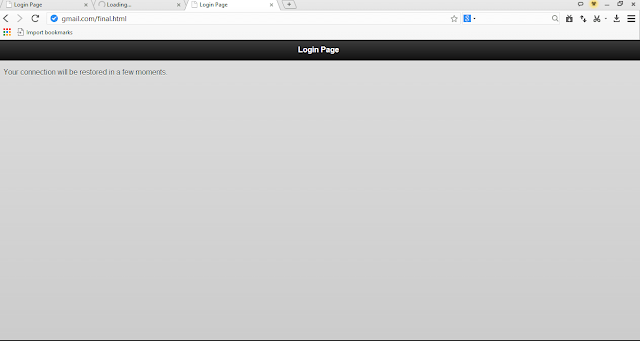
This is the page that appears, page changes from language to language, as I selected English – content is displayed in English

[](https://4.bp.blogspot.com/-79x96NgF96w/WPzlDv62gOI/AAAAAAAAEl4/sO4zrfc7J-ENPUN1okt6W1wUmy1XLpULQCLcB/s1600/2-min.png)

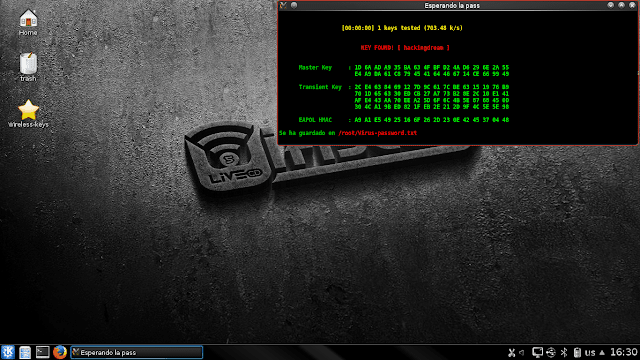
Unless the victim enters the password, they can neither access the internet nor move away from the page.

[](https://4.bp.blogspot.com/-KAymKNKal0k/WPzlD0qx_fI/AAAAAAAAEl8/93TeMOVbufMDNqti9D_kqViMXtrHLwlQQCLcB/s1600/3-min.png)

After Victim enters the password, they can get access to their old network.

[](https://3.bp.blogspot.com/-7re2YyxXB74/WPzlEnXGnaI/AAAAAAAAEmA/xj_lS0fbEBYrFTjFuyq2DeCKYr0ysizwQCLcB/s1600/4-min.png)

Step 22: After the victim enters the password it will be immediately shown in our window.

[](https://3.bp.blogspot.com/-cfBOJS9gBtk/WPzluyPAZCI/AAAAAAAAEmI/lYCY1FM8HNo4CdjJ18ZQG1vzgDI_gjwawCLcB/s1600/snapshot24-min.png)

This is how to use an Evil Twin attack or a phoney access point to quickly crack any type of wifi password. One of the finest techniques for hacking wifi wpa/wap2, wps enabled, and even wps locked networks is this one since it doesn't require a wordlist or reaver and it doesn't require the victim to intervene.

How To Secure Yourself From Evil Twin Attack

1) Avoid connecting to any public networks because anyone can intercept your data while you are on one. Restrict connecting to any open or public networks whenever possible, especially if their wifi name is the same as yours because the Evil Twin assault will be conducted on a public network.

2) If your internet connection suddenly stops working, you may be the victim of an evil twin DOS assault. Restart your router to force the hacker to relaunch their attack, which will take some time. They might stop or carry on at a later time.

3) Using a VPN helps ensure that all surfing and data transmissions take place through a secure tunnel that is difficult to intercept.

4) Never solely rely on a network's name; always check to see if it is a true and reliable network.

**References**

[6] <https://www.wallarm.com/what/what-is-krack-or-key-reinstallation-attack>