Hacking Wifi Networks On Windows

Kevin

This is my first e-book and it shows you how easy a Wireless network using WEP protocol for security can be cracked on a Windows operating system with just two tools and some patience .The Book contains detailed instructions with screenshots for each step so that anybody can understand .

Zweep Books

Skype:Superhero619

+91 9176295852

M4DH4CK3R

7/9/2011

Kevin

Digitally signed by Kevin
DN: cn=Kevin, o=Zweep,
ou=Books,
email=kvyn.14@gmail.com, c=IN
Date: 2011.09.07 15:02:03
+05'30'

CONTENTS

Introduction:

Many Windows users here are struggling to hack Wi-Fi networks because most of the tutorials are based on Backtrack and other Linux Tools. I'm just sharing the method to Crack Wi-Fi networks using WEP security protocol. It takes about 5-6 hours if the password is weak a high signal of the Wi-Fi network you are going to hack and you have sometimes 10-12 for more complicated passwords and if the Wi-Fi signal of the Network is weak .The time taken also changes if the Wi-Fi network you are going to hack has many other clients already accessing it that is if the real user is already using Wi-Fi from his laptop then it will be a lot faster.

The contents of this book are for testing your own Wi-Fi network . The Author is not responsible for anything that happens due to the knowledge gained from this book .

Flaw in WEP:

Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

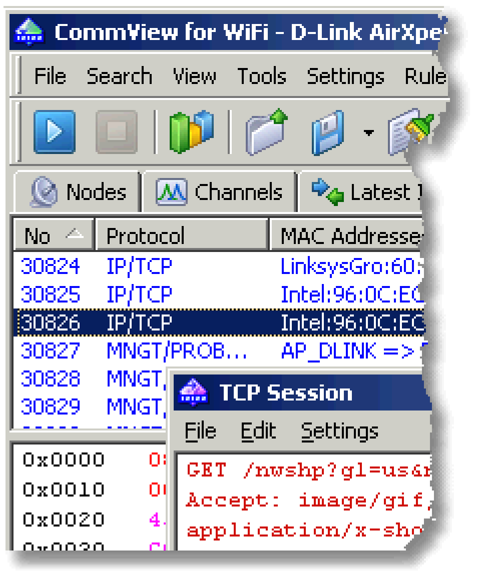
Depending on the amount of network traffic, and thus the number of packets available for inspection, a successful key recovery could take as little as one minute. If an insufficient number of packets are being sent, there are ways for an attacker to send packets on the network and thereby stimulate reply packets which can then be inspected to find the key. The attack was soon implemented, and automated tools have since been released. It is possible to perform the attack with a personal computer, off-the-shelf hardware and freely available software such as aircrack-ng to crack *any*WEP key in minutes.

Generic weaknesses of WEP:

- the use of WEP was optional, resulting in many installations never even activating it, and
- WEP did not include **a key management protocol**, relying instead on a single **shared key** among users.

TOOLS REQUIRED:

1. Commview for Wi-Fi:


CommView for WiFi - D-Link AirXpe
File Search View Tools Settings Rule
Nodes
Channels
Latest I
TCP Session
File Edit Settings

```
No   Protocol      MAC Addresse
30824 IP/TCP       LinksysGro:60:
30825 IP/TCP       Intel:96:0C:EC
30826 IP/TCP       Intel:96:0C:EC
30827 MNGT/PROB... AP_DLINK =>
30828 MNGT,
30829 MNGT,
```

```
GET /nwshp?gl=us&r
Accept: image/gif,
application/x-sho
```

Commview for **Wi-Fi** is a powerful **wireless network monitor and analyzer** for 802.11 a/b/g/n networks. Loaded with many user-friendly features, CommView for Wi-Fi combines performance and flexibility with an ease of use unmatched in the industry.

CommView for Wi-Fi captures every packet on the air to display important information such as the list of **access points** and **stations**, per-node and per-channel **statistics**, **signal strength**, a list of packets and network **connections**, protocol distribution **charts**, etc. By providing this information, CommView for Wi-Fi can help you view and examine packets, pinpoint network problems, and troubleshoot software and hardware.

You will use this tool for capturing the packets sent and received through the Access Point you are going to test .The more packets you capture the better chances of cracking the password .You will need more than 1,00,000 minimum packets to crack the password .The packets will be captured in the .ncp format . You will use this tool to convert the .ncp to .cap.

NOTE: Some Wi-Fi cards are supported by Commview only in Windows 7 so i suggest you install Windows 7 in your Virtual Machine if your Wi-Fi card isn't supported.

Download Link: http://www.tamos.com/download/main/ca.php

2. Aircrack-Ng GUI:

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

You will use this tool to crack the password of the Access Point using the .cap files you obtained from the Commview application.

NOTE:

1. You need to run this as administrator.

2. Your Antivirus Might Detect it as a virus. It is a false positive.

Download Link: http://www.aircrack-ng.org/

The Testing Process:

STEP 1:

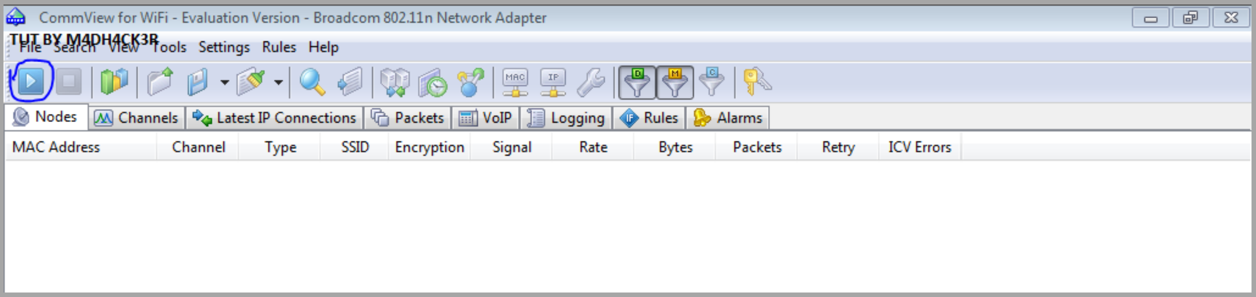
1. Install CommView for Wi-Fi. It doesn't matter whether you install it in VoIP mode or Standard mode. I used VoIP.

It automatically installs the necessary drivers. Allow it to install.

NOTE: You will not be able to connect to any Network using Wi-Fi when using CommView.

STEP 2:

2. Click on the PLAY ICON in the Left First.

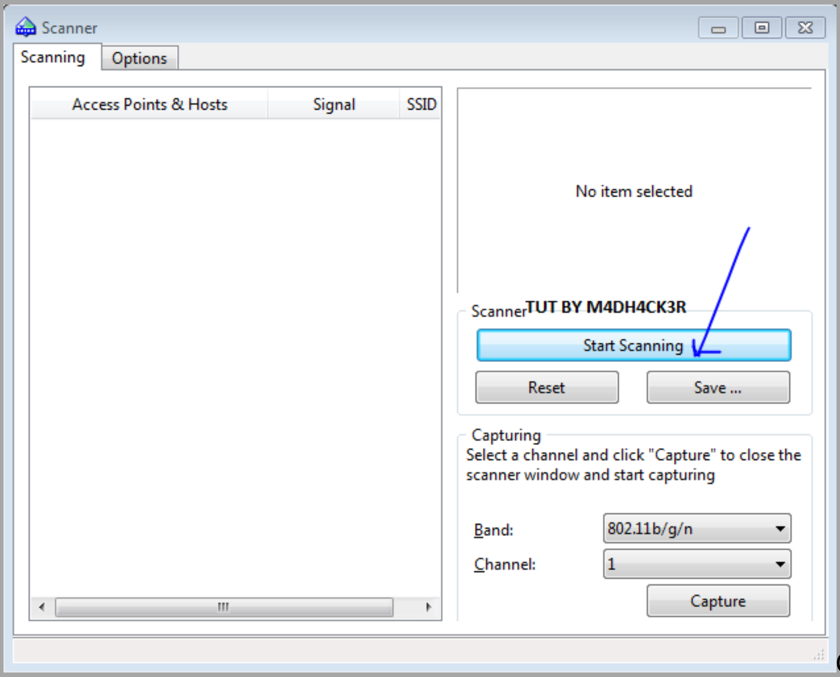


CommView for WiFi - Evaluation Version - Broadcom 802.11n Network Adapter

TUT BY M4DH4CK3R

MAC Address	Channel	Type	SSID	Encryption	Signal	Rate	Bytes	Packets	Retry	ICV Errors

STEP 3 (Choosing the Network (a)): A new window should pop up now.



No item selected

Select a channel and click "Capture" to close the scanner window and start capturing

Band: 802.11b/g/n

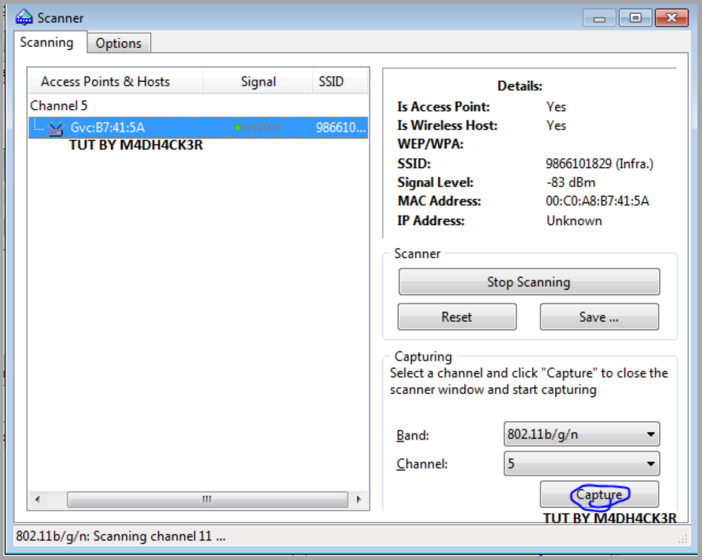
Channel: 1

Click on Start Scanning.

STEP 4 (Choosing the Network (b)) :

Click on the Wi-Fi network you want to hack in the Right Column and Click on CAPTURE.

NOTE: This tutorial is only for WEP protected networks.



Channel 5

Gvc:B7:41:5A 986610...

Details:

Is Access Point: Yes

Is Wireless Host: Yes

WEP/WPA:

SSID: 9866101829 (Infra.)

Signal Level: -83 dBm

MAC Address: 00:C0:A8:B7:41:5A

IP Address: Unknown

Select a channel and click "Capture" to close the scanner window and start capturing

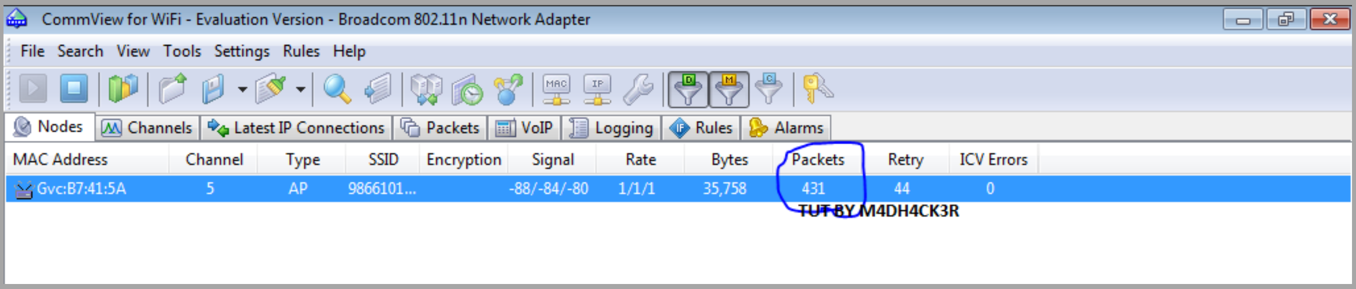
Band: 802.11b/g/n

Channel: 5

802.11b/g/n: Scanning channel 11 ...

STEP 5 (Capturing the Packets):

The windows should close now and you should see that CommView has started Capturing Packets.


CommView for WiFi - Evaluation Version - Broadcom 802.11n Network Adapter
File Search View Tools Settings Rules Help
Nodes
Channels
Latest IP Connections
Packets
VoIP
Logging
Rules
Alarms
TUT BY M4DH4CK3R

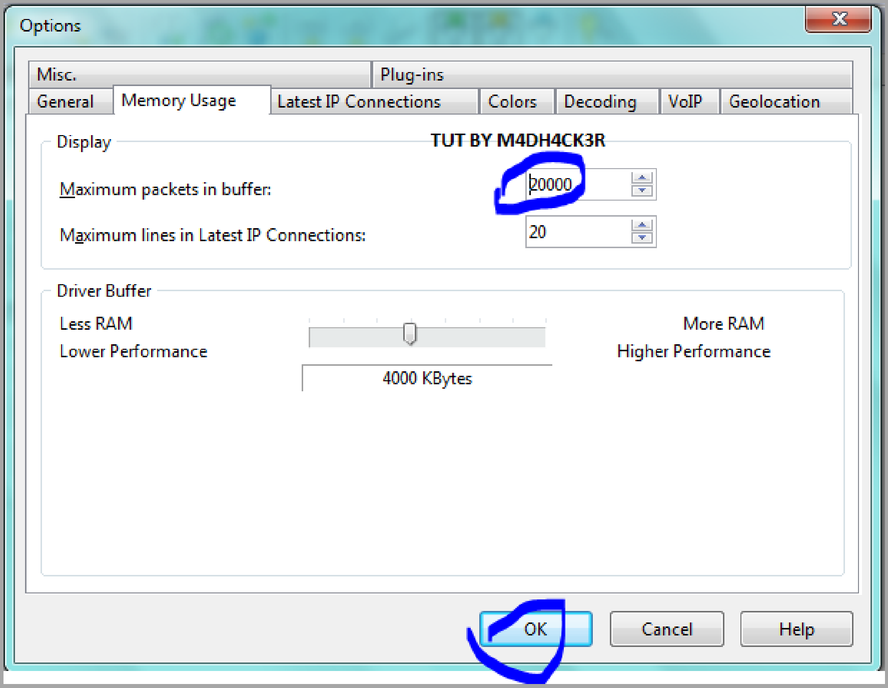
MAC Address	Channel	Type	SSID	Encryption	Signal	Rate	Bytes	Packets	Retry	ICV Errors
Gvc:B7:41:5A	5	AP	9866101...		-88/-84/-80	1/1/1	35,758	431	44	0

STEP 6 (Saving the Packets):

Now that the Packets are getting captured you need to save them.

Click on **Settings->Options->Memory Usage**

Change Maximum Packets in buffer to 20000



Maximum packets in buffer: 20000

Maximum lines in Latest IP Connections: 20

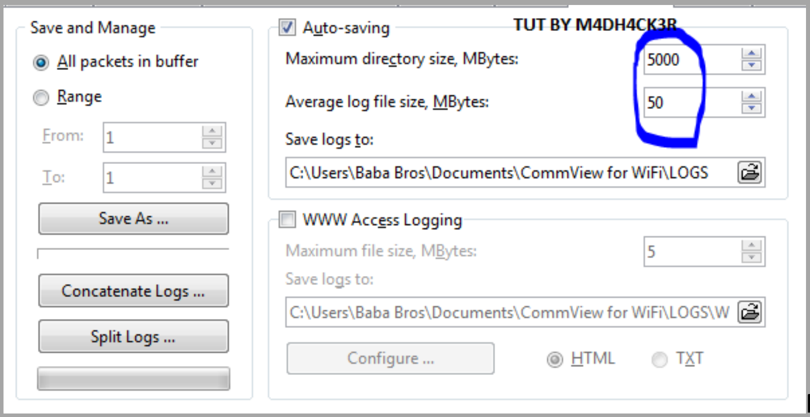
4000 KBytes

Click on the **LOGGING** Tab.

Check **AUTO-SAVING**

In the **Maximum Directory Size: 2000**

Average Log File Size: 20



● All packets in buffer

○ Range

From: 1

To: 1

☑ Auto-saving

Maximum directory size, MBytes: 5000

Average log file size, MBytes: 50

Save logs to: C:\Users\Baba Bros\Documents\CommView for WiFi\LOGS

□ WWW Access Logging

Maximum file size, MBytes: 5

Save logs to: C:\Users\Baba Bros\Documents\CommView for WiFi\LOGS\W

● HTML ○ TXT

Now CommView will automatically Start Saving packets in the .nap format at a size of 20MB each in the specified directory.

STEP 7 (Concatenating the Logs):

Since you are capturing a lot of logs you will need to concatenate them into once file.

To do this go to Logging and click on **CONCATENATE LOGS**

Choose all the files that have been saved in your specified folder and concatenate them.

Now you will have one **.ncf** file.

STEP 8 (Converting .ncf to .cap):

Now that you have one file with all the packets you need to convert it into .cap file for AIRCRACK to crack.

Click on **File->Log Viewer->Load Commview Logs-> Choose the .ncf** file

Now **File->Export->Wire shark/TCP dump format.**

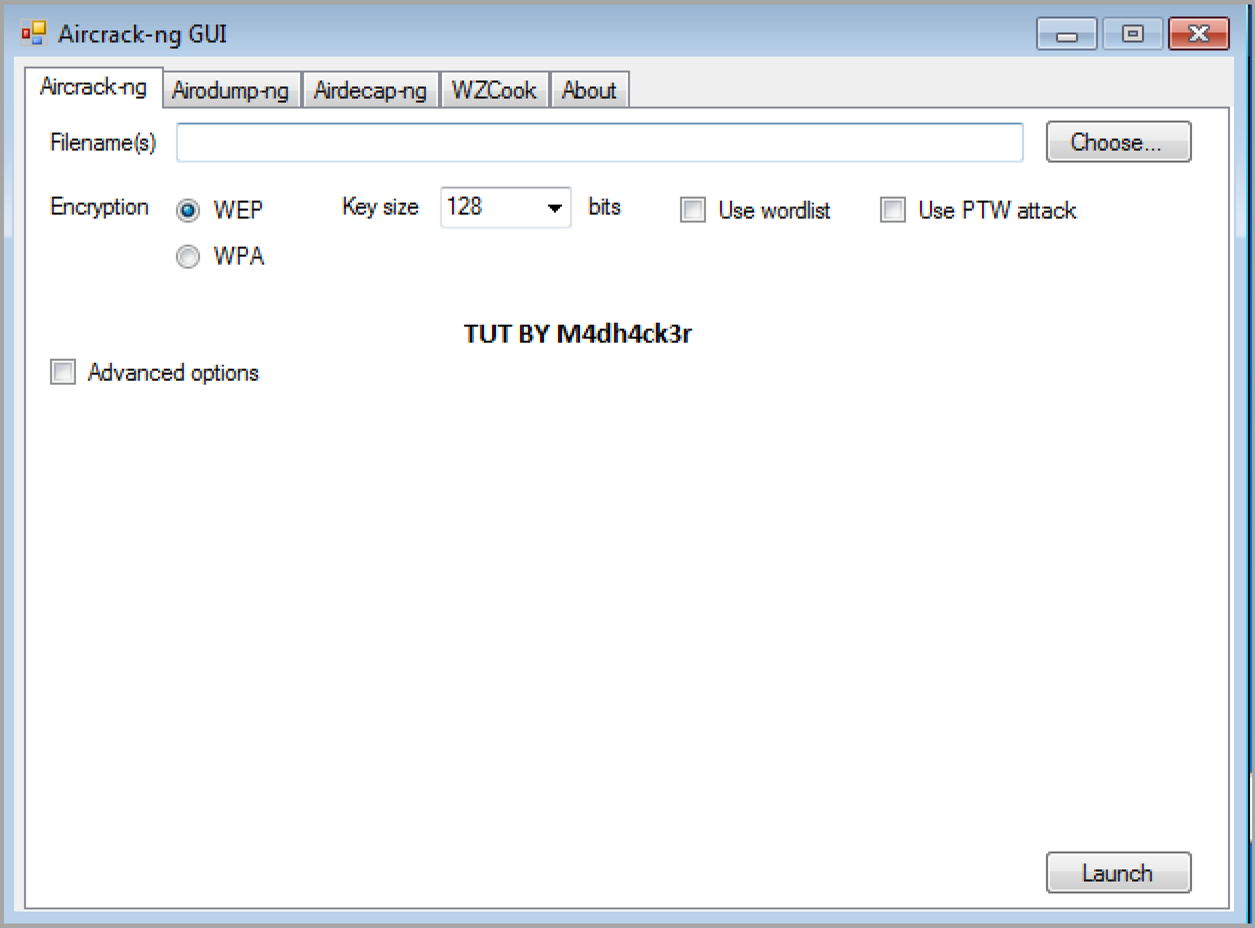
Aircrack:

Now that we have captured the ivs and stored it in a cap file. We are going to crack it using aircrack.

We will use the GUI version of aircrack.

Extract the Aircrack zip file you downloaded.

Go to the bin and open Aircrack Ng Gui.exe.



Filename(s)

Encryption ● WEP ○ WPA

Key size 128 bits

□ Use wordlist

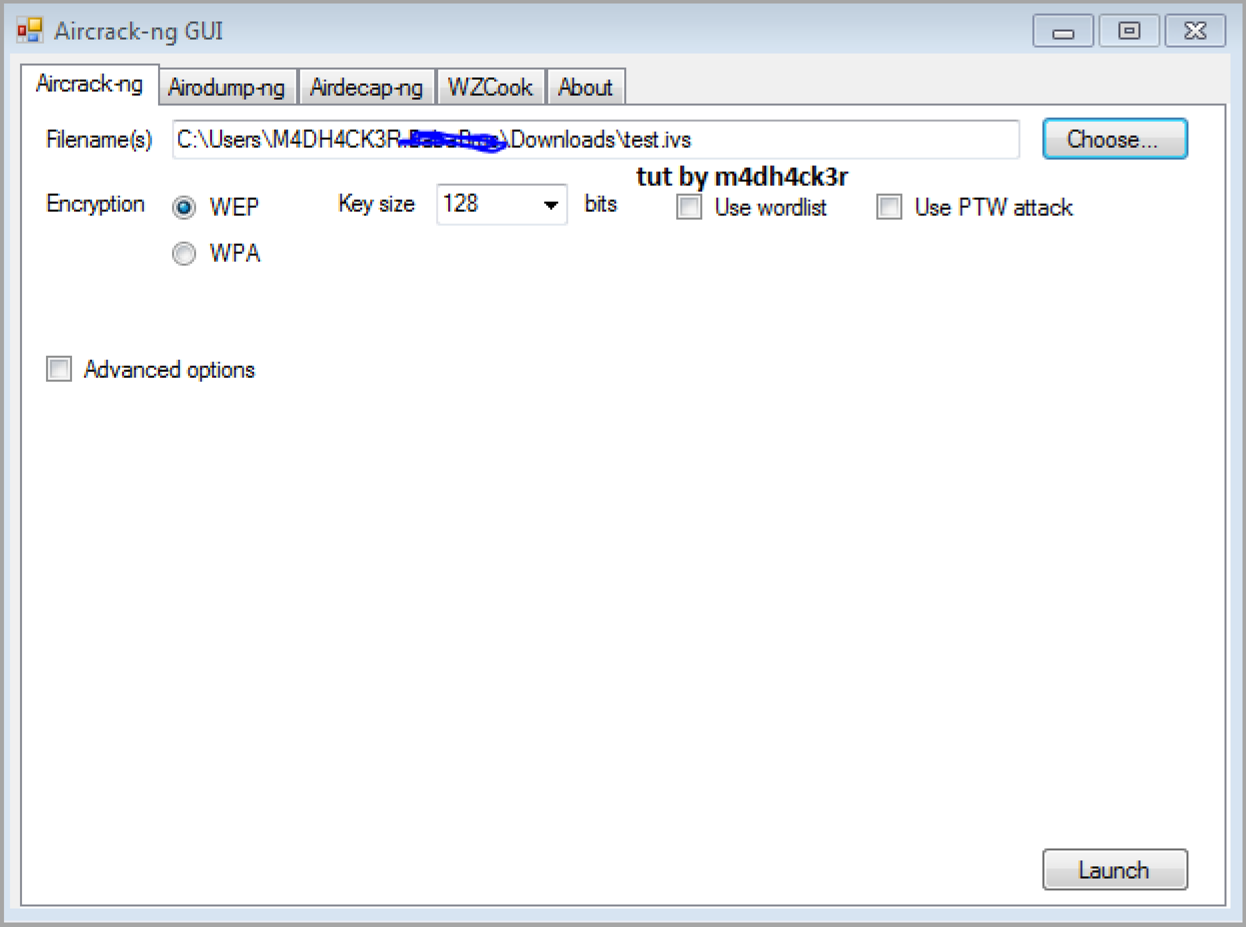
□ Use PTW attack

TUT BY M4dh4ck3r

□ Advanced options

STEP 2:

Choose the .cap file you got through CommView for Wi-Fi



Filename(s) C:\Users\M4DH4CK3R.[redacted]\Downloads\test.ivs

tut by m4dh4ck3r

Encryption ● WEP ○ WPA

Key size 128 bits

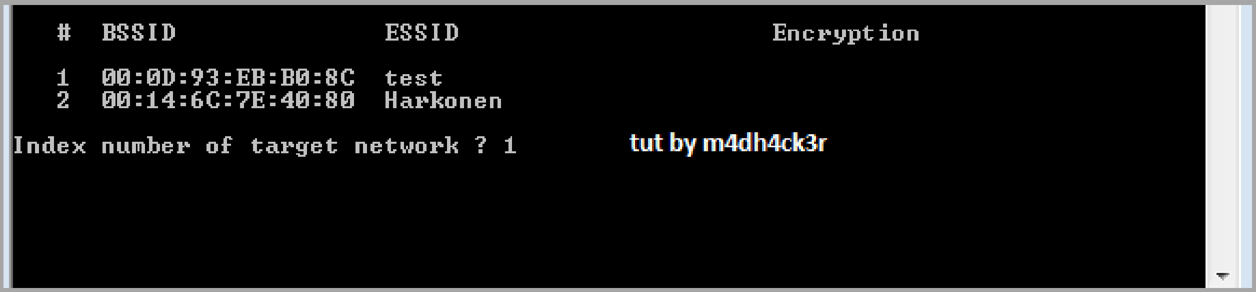
□ Use wordlist □ Use PTW attack

□ Advanced options

STEP 3:

Click on **Launch!**

You will get this screen in cmd



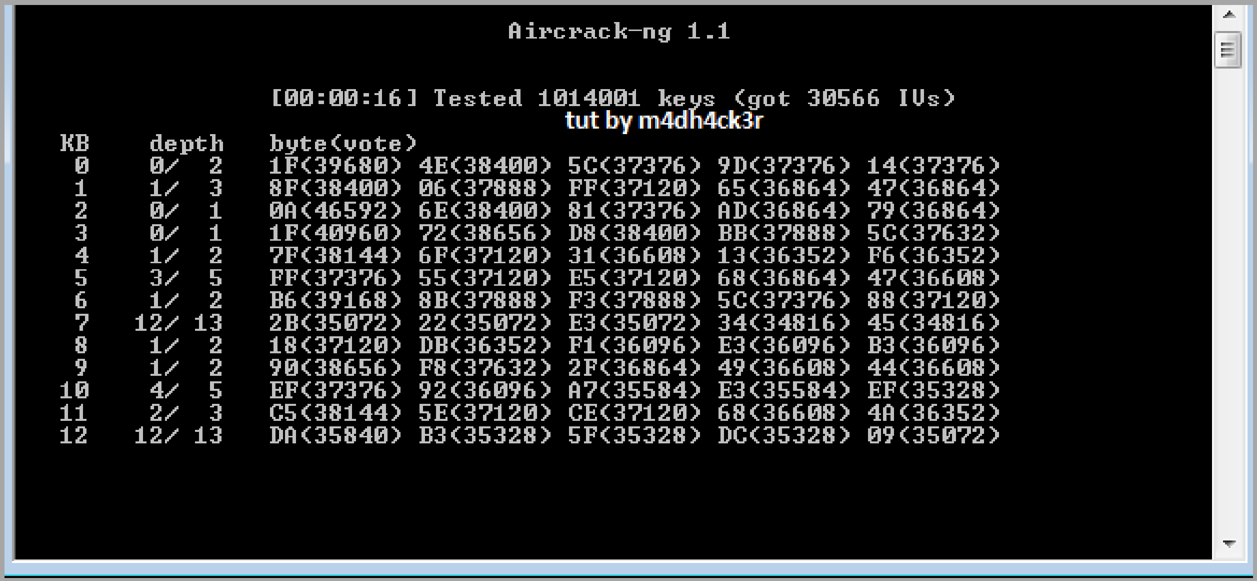
```
   #  BSSID              ESSID                     Encryption

   1  00:0D:93:EB:B0:8C  test
   2  00:14:6C:7E:40:80  Harkonen

Index number of target network ? 1
```

tut by m4dh4ck3r

Choose the target network .Ex: 1 if test or 2 if harkonen and hit **Enter.**

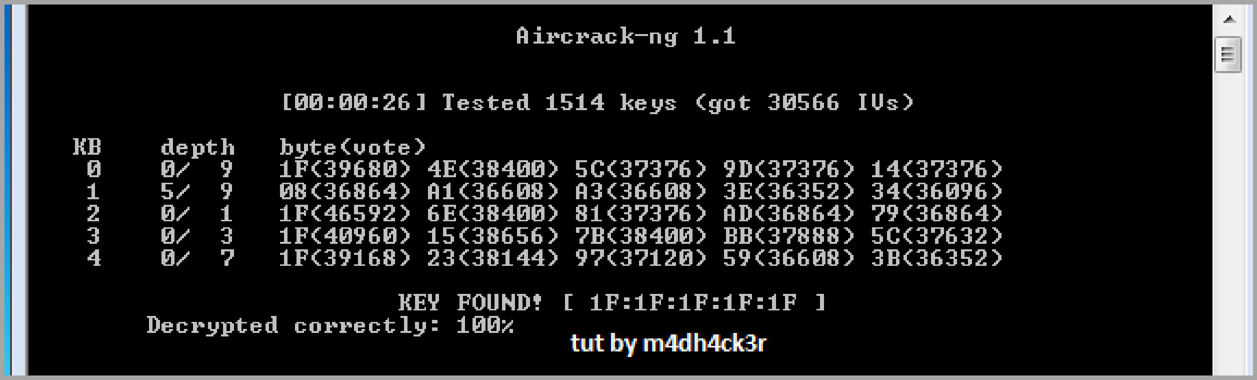
STEP 4:

Just wait while aircrack is cracking the password.



```
                              Aircrack-ng 1.1


                 [00:00:16] Tested 1014001 keys (got 30566 IVs)
                                  tut by m4dh4ck3r
   KB    depth   byte(vote)
    0    0/  2   1F(39680) 4E(38400) 5C(37376) 9D(37376) 14(37376)
    1    1/  3   8F(38400) 06(37888) FF(37120) 65(36864) 47(36864)
    2    0/  1   0A(46592) 6E(38400) 81(37376) AD(36864) 79(36864)
    3    0/  1   1F(40960) 72(38656) D8(38400) BB(37888) 5C(37632)
    4    1/  2   7F(38144) 6F(37120) 31(36608) 13(36352) F6(36352)
    5    3/  5   FF(37376) 55(37120) E5(37120) 68(36864) 47(36608)
    6    1/  2   B6(39168) 8B(37888) F3(37888) 5C(37376) 88(37120)
    7   12/ 13   2B(35072) 22(35072) E3(35072) 34(34816) 45(34816)
    8    1/  2   18(37120) DB(36352) F1(36096) E3(36096) B3(36096)
    9    1/  2   90(38656) F8(37632) 2F(36864) 49(36608) 44(36608)
   10    4/  5   EF(37376) 92(36096) A7(35584) E3(35584) EF(35328)
   11    2/  3   C5(38144) 5E(37120) CE(37120) 68(36608) 4A(36352)
   12   12/ 13   DA(35840) B3(35328) 5F(35328) DC(35328) 09(35072)
```

STEP 5:



```
                              Aircrack-ng 1.1


                 [00:00:26] Tested 1514 keys (got 30566 IVs)

   KB    depth   byte(vote)
    0    0/  9   1F(39680) 4E(38400) 5C(37376) 9D(37376) 14(37376)
    1    5/  9   08(36864) A1(36608) A3(36608) 3E(36352) 34(36096)
    2    0/  1   1F(46592) 6E(38400) 81(37376) AD(36864) 79(36864)
    3    0/  3   1F(40960) 15(38656) 7B(38400) BB(37888) 5C(37632)
    4    0/  7   1F(39168) 23(38144) 97(37120) 59(36608) 3B(36352)

                      KEY FOUND! [ 1F:1F:1F:1F:1F ]
        Decrypted correctly: 100%
                                  tut by m4dh4ck3r
```

Aircrack has successfully found the password.

Now Connect to the Wi-Fi network using the key.

Sources :

http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

http://www.aircrack-ng.org/

http://www.tamos.com/products/commwifi/