The Ultimate Guide to Spy on somebody is in every everybody's pocket ! The Modern Engineering marvel aka Mobile Phone's are everybody's need. People often (mostly) do their confidential talks over cell phone's, But only some know how easy it is to eavesdrop them. There are some tricks and hacks to do that, but the most powerful way is to clone their SIM Card. The Subscriber Identity Card aka SIM Card is the transmitter of signal to the mobile and tower, And you can do It easily.

First off a little introduction about SIM CARD:

Our sim cards contain two secret codes or keys called (imsi value and ki value) which enables the operator to know the mobile number and authenticate the customer ,these codes are related to our mobile numbers which the operators store in their vast data base,it is based on these secret keys that enables the billing to be made to that customer. now what we do in sim cloning is extract these two secret codes from the sim and programme it into a new blank smart card often known as wafer, since the operator authentication on sims is based on these values,it enables us to fool the operators in thinking that its the original sim,this authentication is a big flaw concerning GSM technology.

So What Can You Do When You Clone SIM card ?

Well There are many things to do when you clone a SIM Card, You can secretly spy on the victims calls and data transfers, make him mobile bill go crazy, send messages and make calls from his number, All without touching the victims Cell Phone.

First A Little Knowledge Of SIM Hacking :-

Not every SIM Card is clone-able, There are two types of SIM Card :

COMP128v1: The most popular and clone-able version of SIM Cards, Distributed widely till 2004 in USA (2007 In ASIA Countries), Of the number of victim is older than 2004 in USA or 2007 in Asia, Chances are you can clone it pretty easily.

COMP128v2: The newer SIM's, Capable of better 3G Reception, Video Call Support, New and Secure firmware, Complex Design, Very (I mean very fu*king very) Hard. If the SIM is bought after 2004, it is probably this version

Things Required :-

1). Blank SIM Programmable Cards : **CLICK HERE**

2). A SIM Firmware Writer : **CLICK HERE**

Or You Can Also Make Your Own Sim Writer

Make your own SIM Writer : CLICK HERE

3). Software For Reading : Woron Scan :- **CLICK HERE (MediaFire)**

4). The Victim's SIM For 15 minutes to 30 Minutes !

Lets Begin The Work :

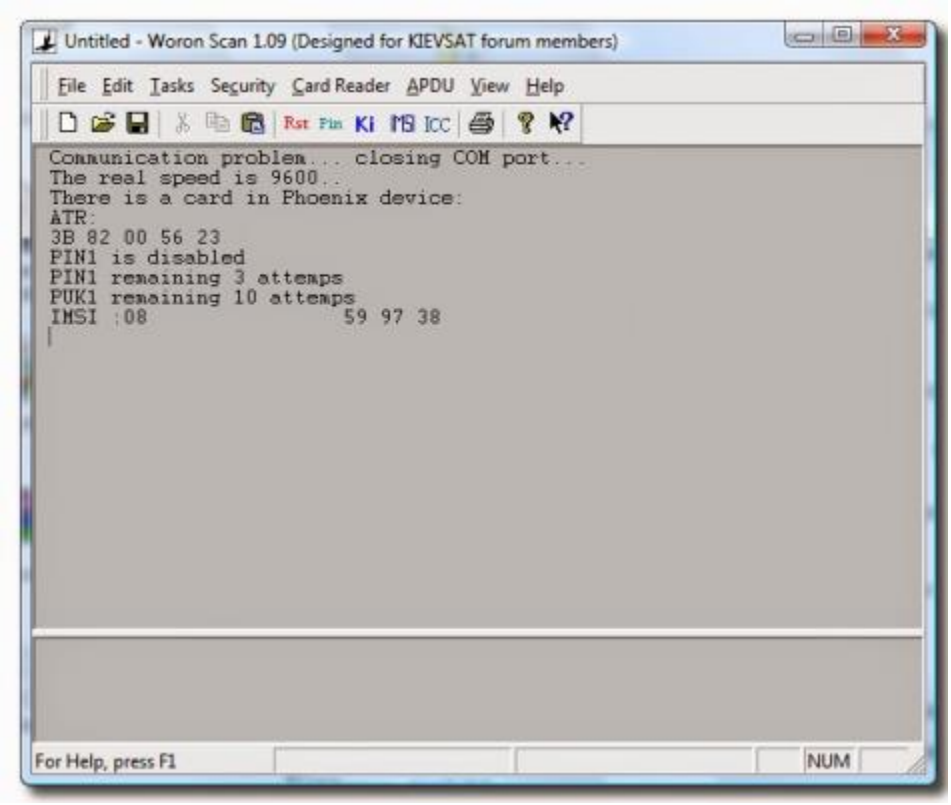
NOTE: THIS IS ONLY FOR EDUCATION PURPOSES, AND FOR SAFETY PURPOSE. WE ARE NOT RESPONSIBLE ANY HARM DONE BY YOU.

The main mission in cloning a SIM Card is to get KI and IMSI codes, these codes are the identifier of the SIM Card, and help you register your mobile to the network.

1). Plug in the SIM Reader, Install the software, get the vic's SIM.

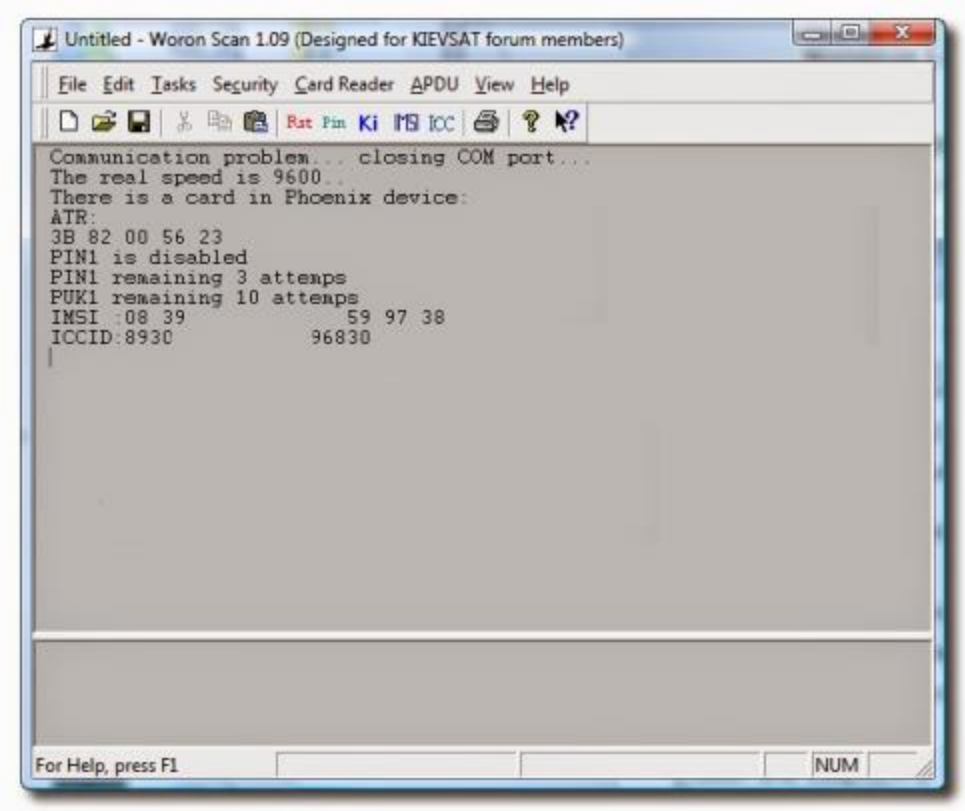
2). Configure the Software as shown in the below pictures :

3). First Run The IMSI Search :



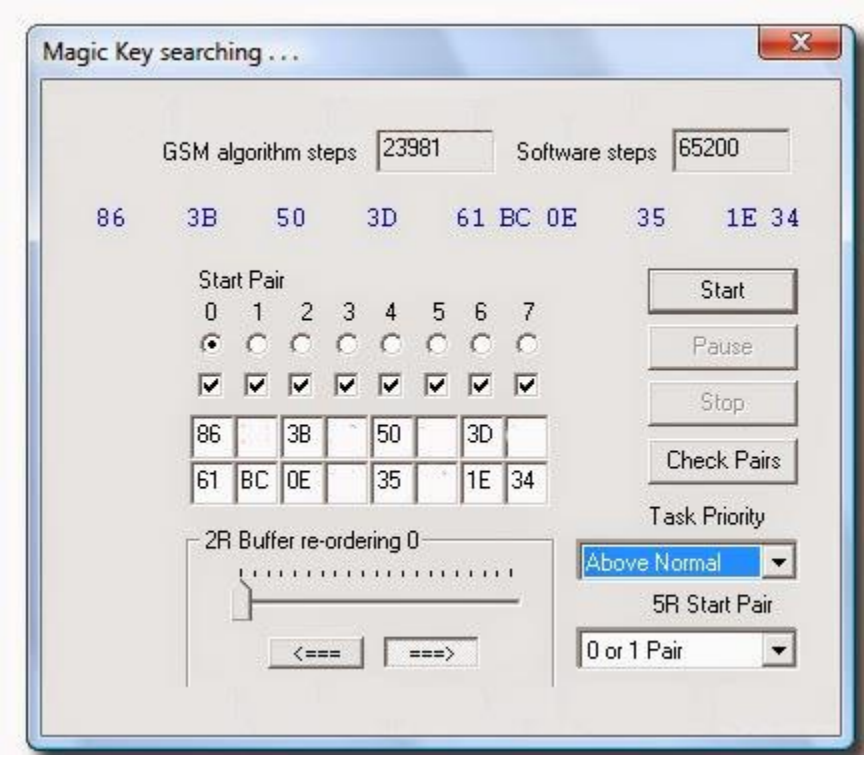
note IMSI number

When the results come, write them down. Then start the ICC Search :



note down value too

Write down the ICC Number too, Now run the KI Search, This may take some time :



After 45 Minutes, IF you don't Get the First Value, The Sim IS Un-cloneable !

Now remove the Vic's SIM And give it back to him.
4). Download SIM-EMU, A software to write settings on Blank SIM Card.

Now insert the blank SIM and wait for it to detect.

5). Run SIM-EMU and click the configure tab,
Enter the ALL the Info Gathered from the Woron Scan Process: IMSI, KI, ICC.

The Setup Menu

For the rest Info :

For ADN/SMS/FDN# (ADN= Abbreviated Dialing No. / SMS = No. of SMSes stored on SIM / FDN = Fixed Dialing No.) Enter: 140 / 10 / 4 OR if the Program has suggested values, let it remain as it is.

The Phone Number should be in International Format, EG: For India +91(the international code) 9999999999 (the number)

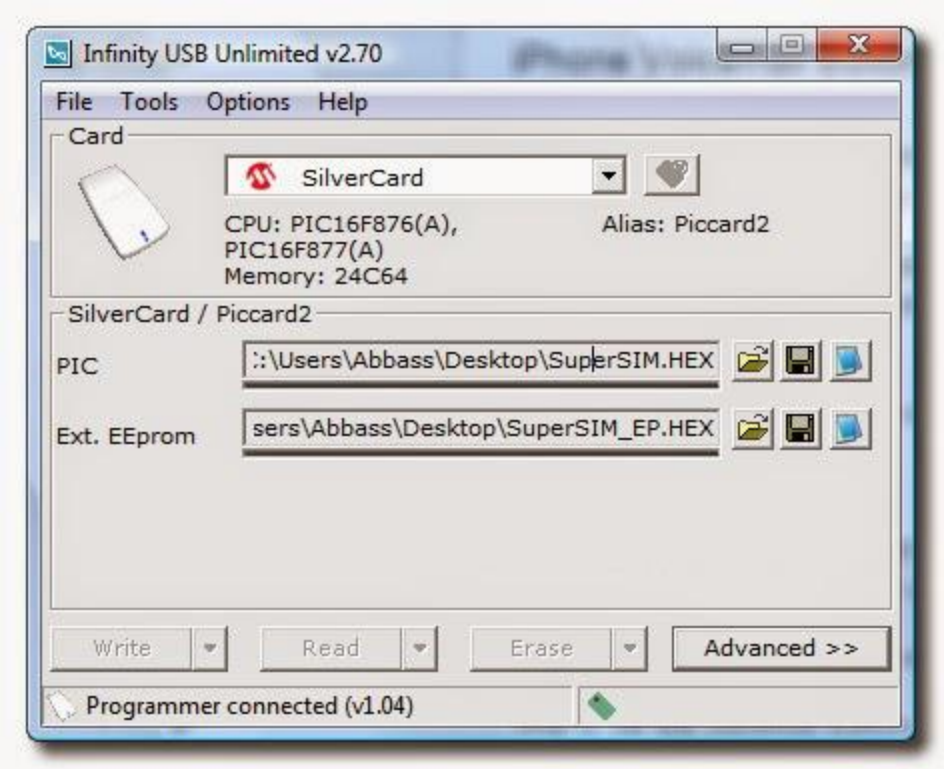
6). Let The Writing Begin, Select the Write To Disk button and Name the File: SuperSIM.HEX.

Wait For The Conformation, Then Select OK.

A write EEPROM file window will appear. Name the EEPROM file SuperSIM_EP.HEX and click the Save button.

Now You Have 2 Files, Ready to be Flashed.

7). *Now We Flash the files on Blank SIM Card :*



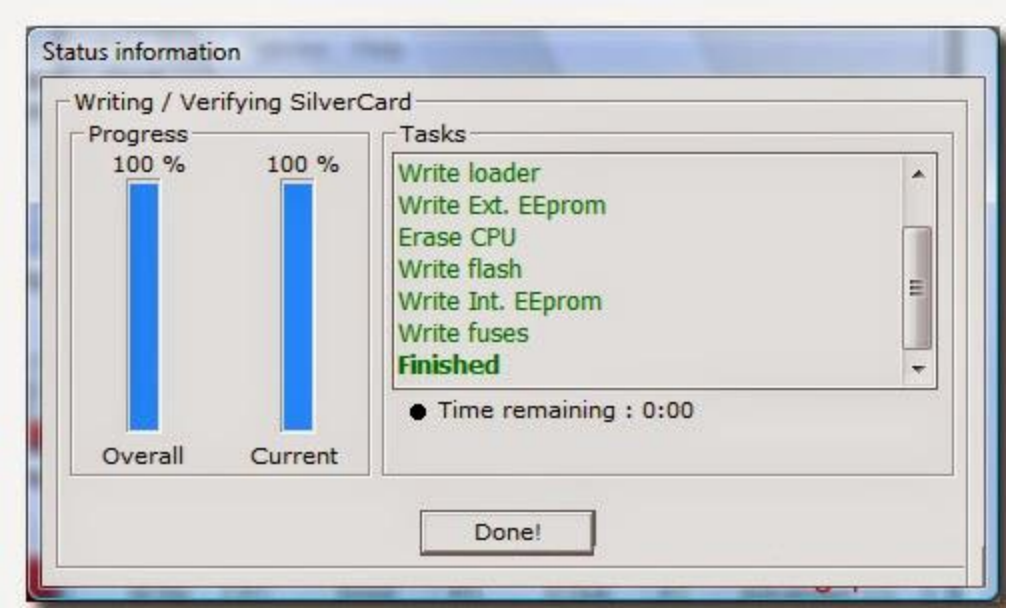
Install the card that came with the card writer, cause using any other software will fu*k up your card and your reader.

Our Card Readers Software was Infinity USB Unlimited, The interface can be changed in your software, but the functioning is the same.

Now Put the required files in the appropriate fields :

Flashing The Blank SIM.

8). Now run the writing task, Click on done when it has completed.



Congrats, You Have Cloned A SIM Card !

So here you have it, A Cloned SIM Card, Now when somebody calls the victim, Both of the mobiles will ring, same will happen in the case of SMS, But only one can pick up the call. Also don't do something big that will raise a red flag in Mobile Company. You are responsible for your own Shit.