
DISCLAIMER: I take no responsibility for the damage of your phone or SIM card, the revocation of your mobile account, any criminal charges placed against you, your family or your friends, or any other adverse effects that may result from the reading of this document. Do so at entirely your own risk. This document is provided for information/education purposes only!

ACKNOWLEDGEMENT

Thanks to Vladimir and many others who have contributed to this guide. Without them this guide would not exist :)

INTRODUCTION

This method (Oz-Vlad method) would enable an activated iPhone (using the jailbreak method) to do the followings via your mobile carrier PROVIDED THAT YOUR MOBILE CARRIER'S SIM (SUBSCRIBER IDENTITY MODULE) AUTHENTICATION KEY (Ki) IS COMP128V1 ENCRYPTED.

1. Make voice calls
2. Receive voice calls
3. Send SMS
4. Receive SMS
5. Transfer data via EDGE (depends on the availability of EDGE in your mobile network)

Please note that

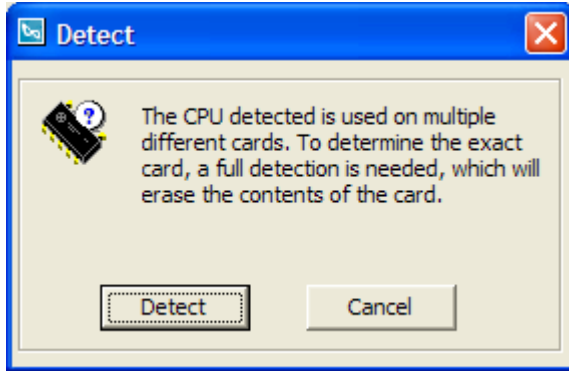
- this method requires some knowledge of PC operation and the purchase of relevant hardware. If you do not have either the time or the ability to do so please consult others (@ the Hackint0sh.org "Supersim and Simcloning solution" forum) who might be able to help you.
- I am almost certain that you could substitute some/all of the hardware as recommended below. But for the sake of simplicity the described method would only use those hardware that I have thoroughly tested and guaranteed to work.
- Mac users may not be able to use the method to "unlock" the phone function of their iPhone as the software used are PC-based.
- this method may not work with some mobile carriers that use COMP128V1 SIM card.

REQUIRED HARDWARE/SOFTWARE

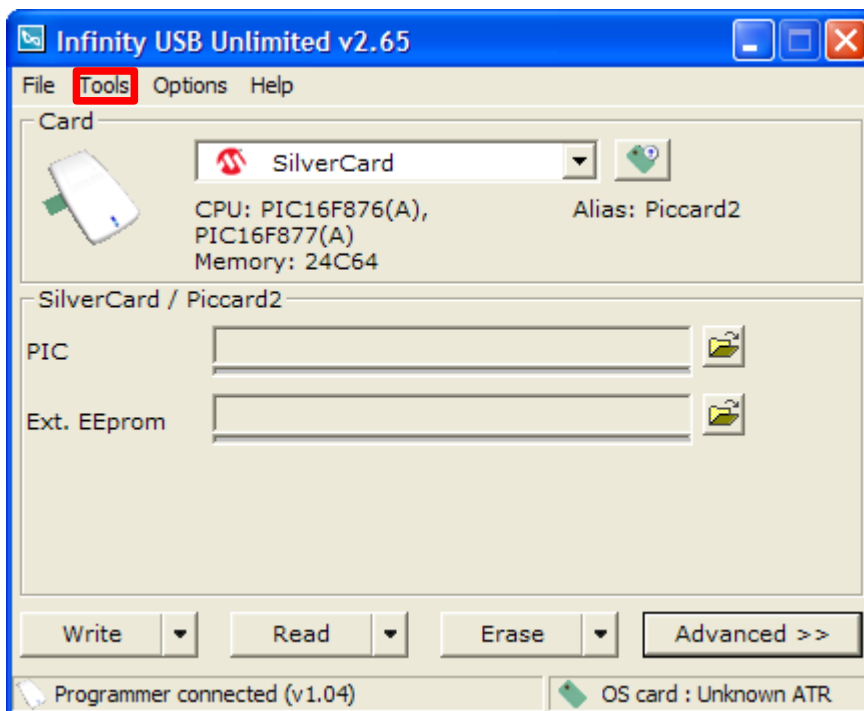
1. An iPhone (of course!!)
2. A valid COMP128v1 Subscriber Identity Module (SIM) card of your mobile carrier (ie. A SIM card that is legitimately obtained from and actively subscribed to your mobile carrier)
3. An AT&T SIM card
4. A "SilverCard". This is a PVC card with embedded Microchip® PIC16F876/77 microcontroller and 24C64 EEPROM (You can purchase it as a full size smart card and cut the sim yourself, or buy it pre-cut)
5. A wb_electronics Infinity USB Unlimited smartcard programmer (<http://www.infinityusb.com/default.asp?show=productsdetail&ProductID=11>)
6. Woron Scan 1.09 (download from: <http://download.mobile01.com/attach/200501/mobile01-bd0f08a256ab9a75bb0b415485dcc081.zip>)
7. SIM-EMU 6.01 (download from: http://simemu.gsmhosting.net/SIM_EMU_6.01_CFG_v2.1.zip)
8. Infinity USB Unlimited Programming software (current version 2.65: <http://www.infinityusb.com/default.asp?show=download&DownloadID=24>)
9. SimScan v2.01 (download from: http://users.net.yu/~dejan/download/sim_scan.zip)
10. Vlad's FLASH and EEPROM files: (download from: http://rapidshare.com/files/48485013/SIM_EMU_6.01_iphone_u1.rar.html)

THE STEPS

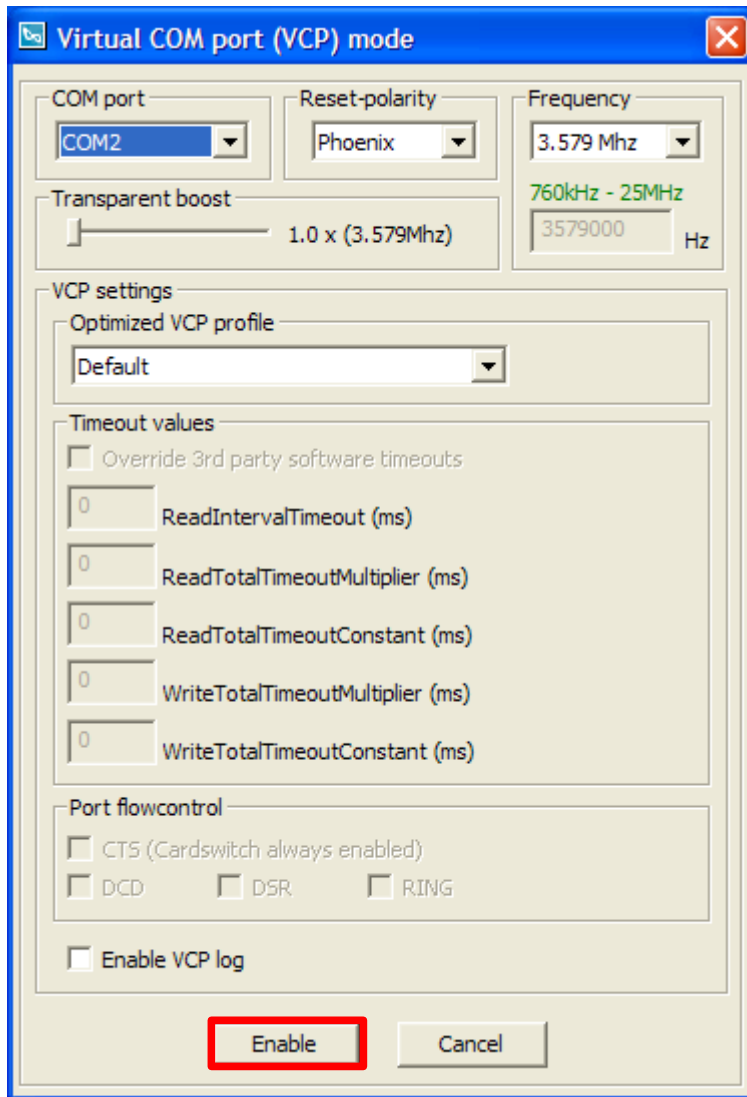
1. Install Woron Scan 1.09, SimScan v2.01, SIM-EMU 6.01 and Infinity USB Unlimited Programming software (IUUP software)
2. Put Vlad's Flash and EEPROM into a folder of your choice (eg. C:\vladhex)
3. Insert your mobile carrier's SIM into the Infinity USB Unlimited smartcard programmer (IUUP)
4. Plug the IUUP into one of your PC's USB ports. Install drivers as instructed.
5. Run the IUUP software. You will see this, click "Cancel". (If the software ask you to upgrade, please do so)



6. Now you are looking at the main window of the IUUP software. Click the menu item "Tools" and select "Virtual COM Port (VCP) mode"



7. Leave all settings as is. Click "Enable" at the bottom of the window.

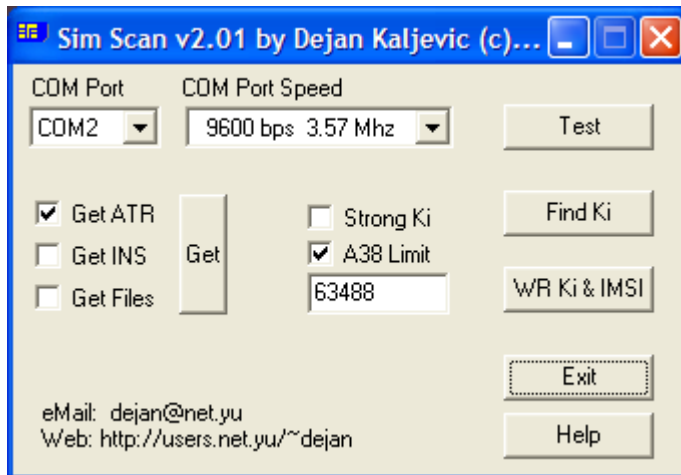


8. You will hear a sound to tell you that the VCP mode is enabled. Also, on

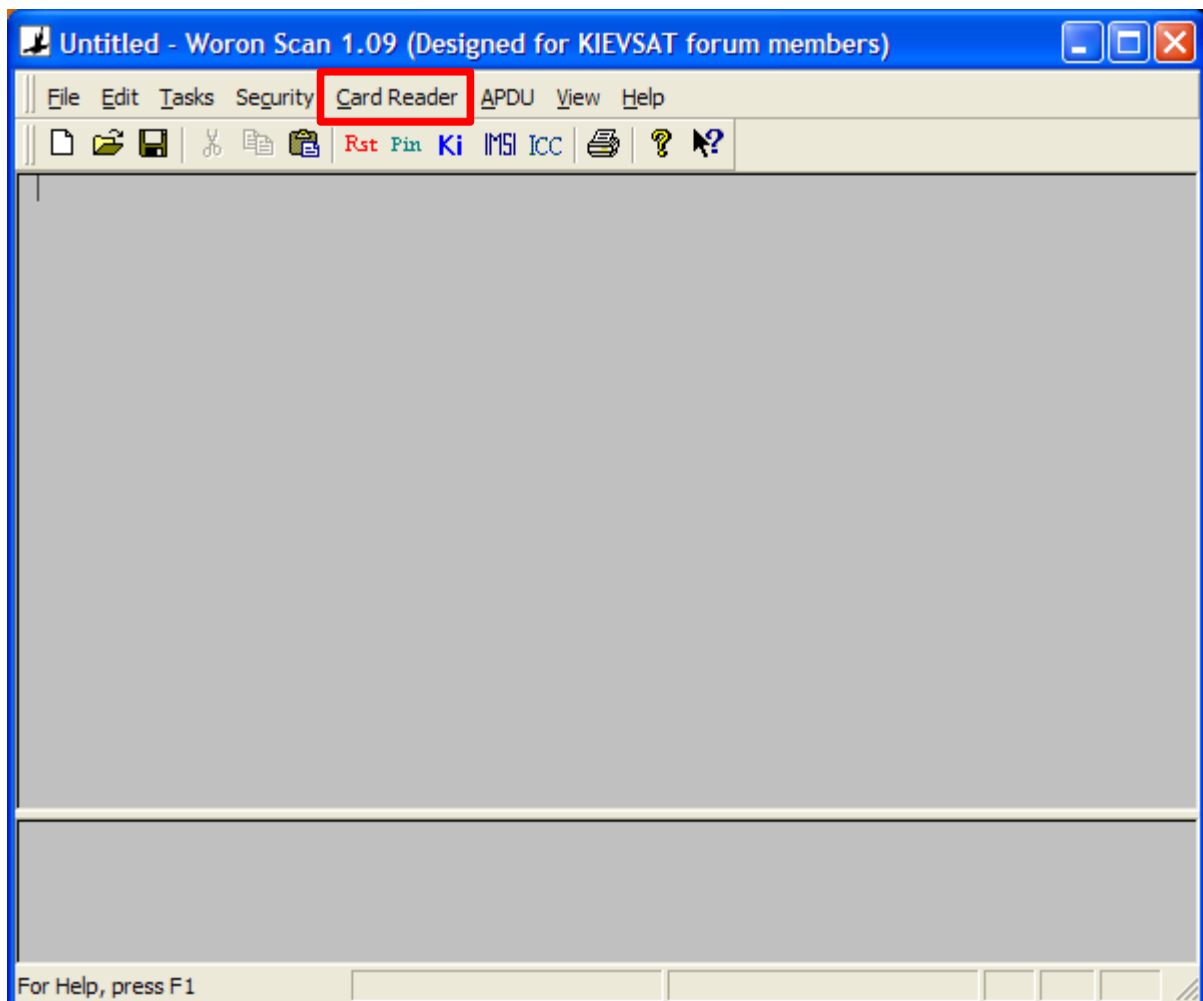


the right hand side of the taskbar you will see an icon like this . When you hover your mouse over it, the line "Infinity USB Unlimited - COMx (ready)" will be shown.

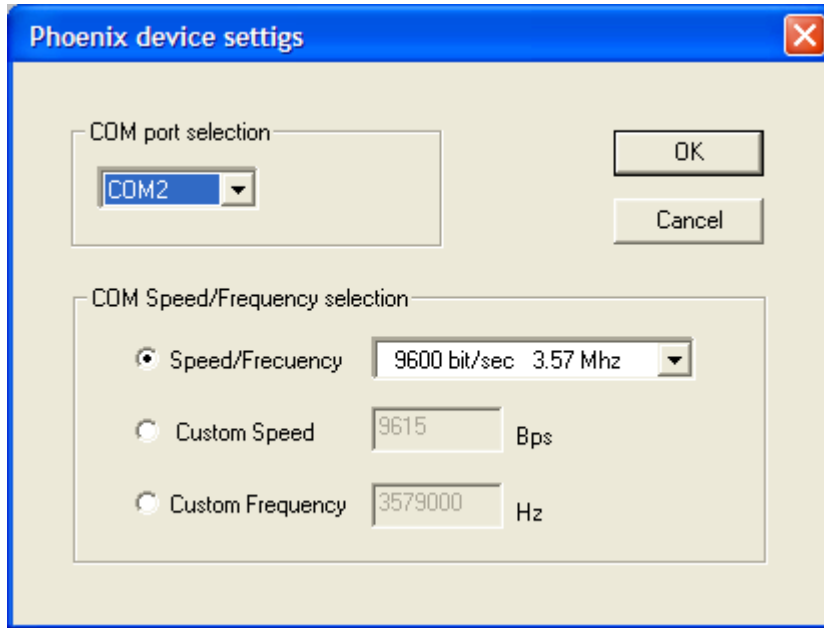
9. Run SimScan v2.01. You will see the window on the left. Make sure the COM Port and COM Port Speed is set to the same settings in the IUUP software (in my case it's COM2, 9600 bps 3.57 Mhz). Then click "Test" and then "OK". Quit SimScan v2.01.



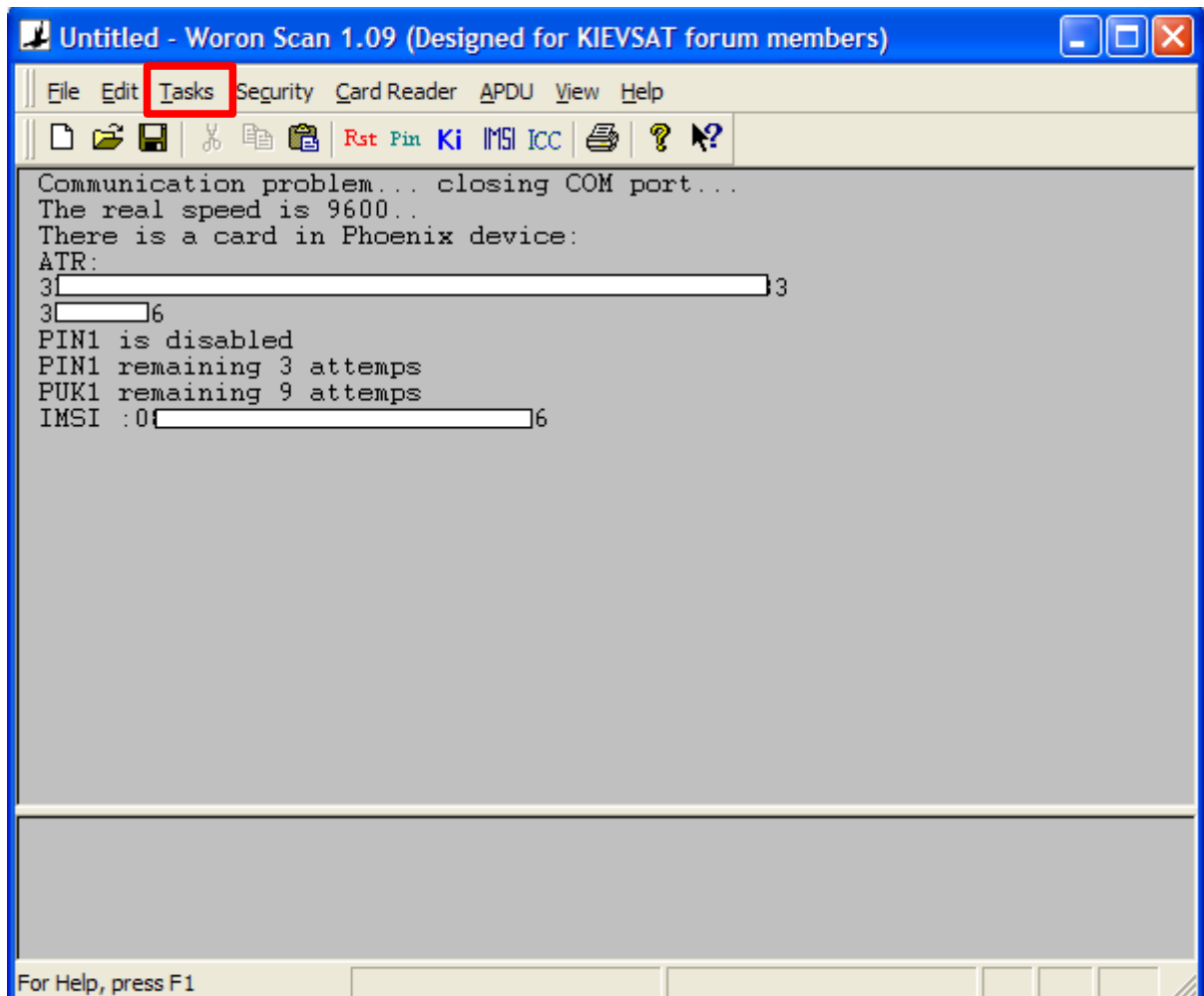
10. Run Woron Scan 1.09. You will see this window. Click the menu item "Card Reader" and select "Phoenix Card".



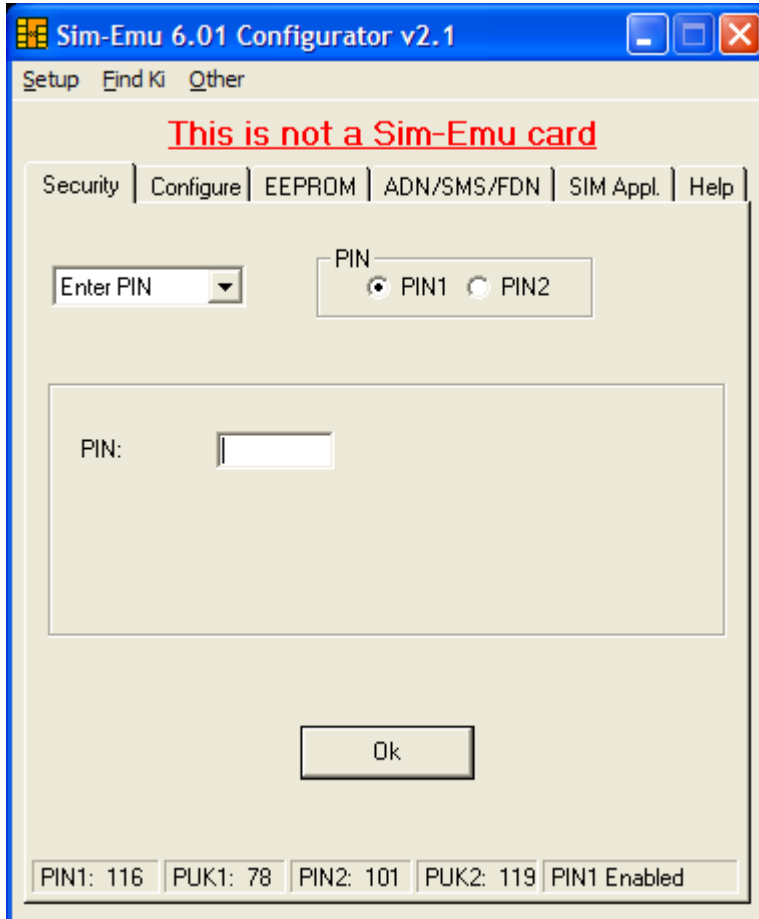
11. Click "Settings" within the dropdown and the following window will appear.



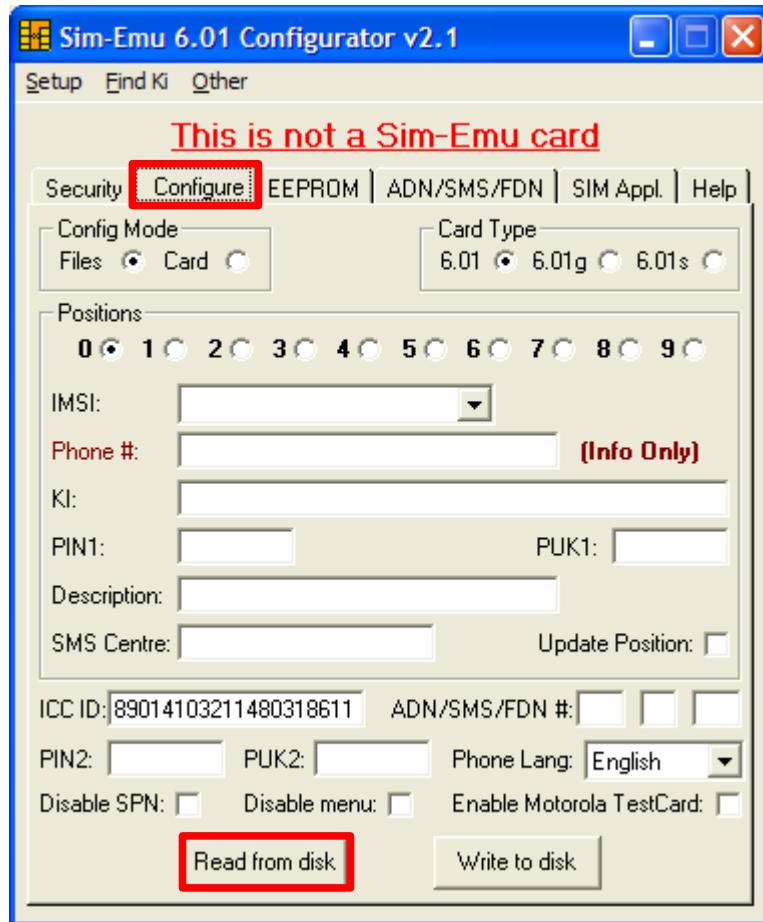
12. Make sure the COM port selection is the same as the settings in the IUUP software (in my case it's COM2). Also confirm the Speed/Frequency is correct (ie. 9600bit/sec 3.57Mhz). Click "OK"
13. Click the menu item "Tasks" and select "IMSI select". You will see the result as shown in the following window in a short moment. Note down the IMSI (IMSI-a).



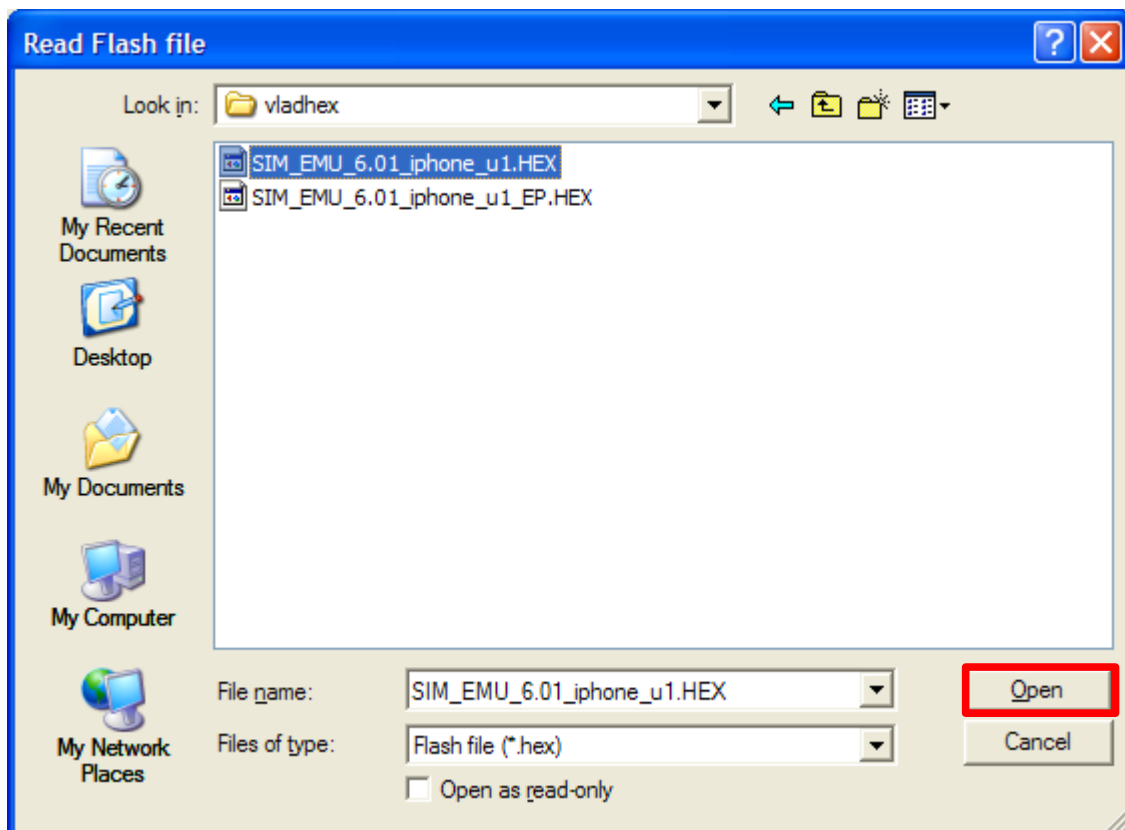
14. Do the same for "KI SEARCH" (Tasks>KI search). it might take a while to complete. Note down the KI.
15. Now remove your mobile carrier's SIM and put in the AT&T SIM. Click the menu item "Tasks" and select "IMSI select". You will get the AT&T IMSI (IMSI-b). Please note it down.
16. Quit Woron Scan 1.09 (click "NO" when you are asked to "Save changes to Untitled" as you have all the information required noted down already). Remove the AT&T SIM and put in the "SilverCard".
17. Run SIM-EMU 6.01 Configurator V2.1 (SIM-EMU). You will see the following window. (Please ignore the remark below the menu bar (in this case "This is not a Sim-Emu card"))



18. Click "Configure". You will see the following window. Click "Read from disk" at the bottom of the window.



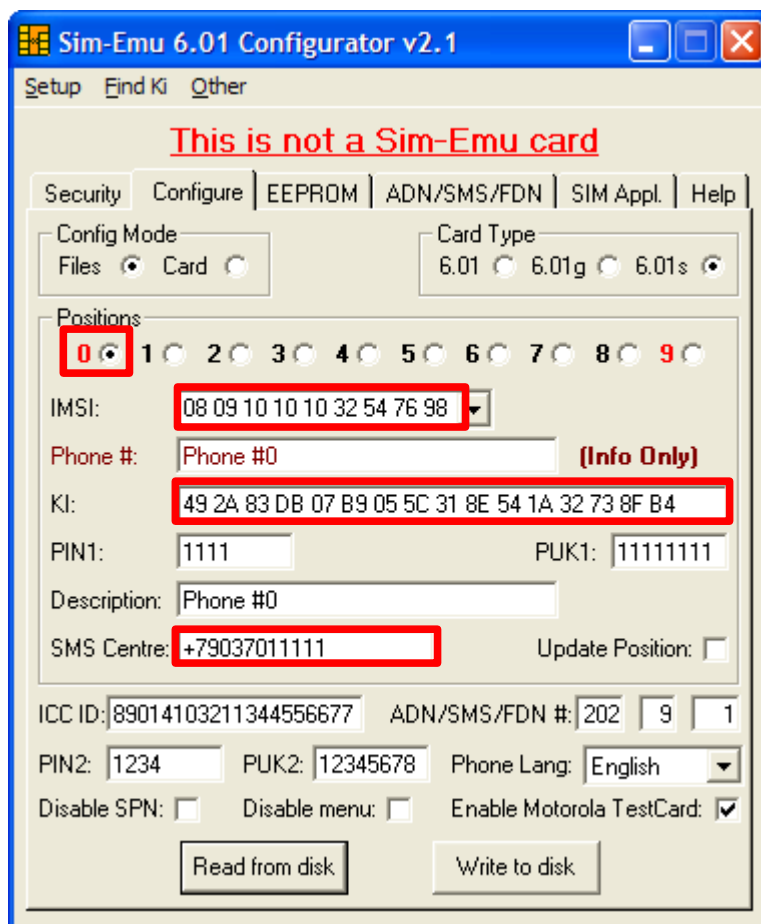
19. Select the folder (eg. `c:\vladhex`) where you put your Vlad's FLASH and EEPROM files, and select the FLASH file (in my case it's `SIM_EMU_6.01_iphone_u1.HEX`). Click "Open"



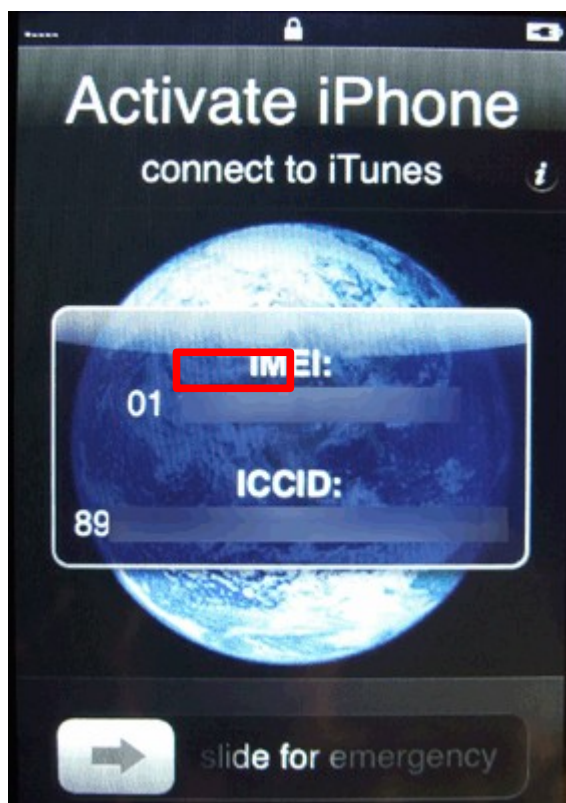
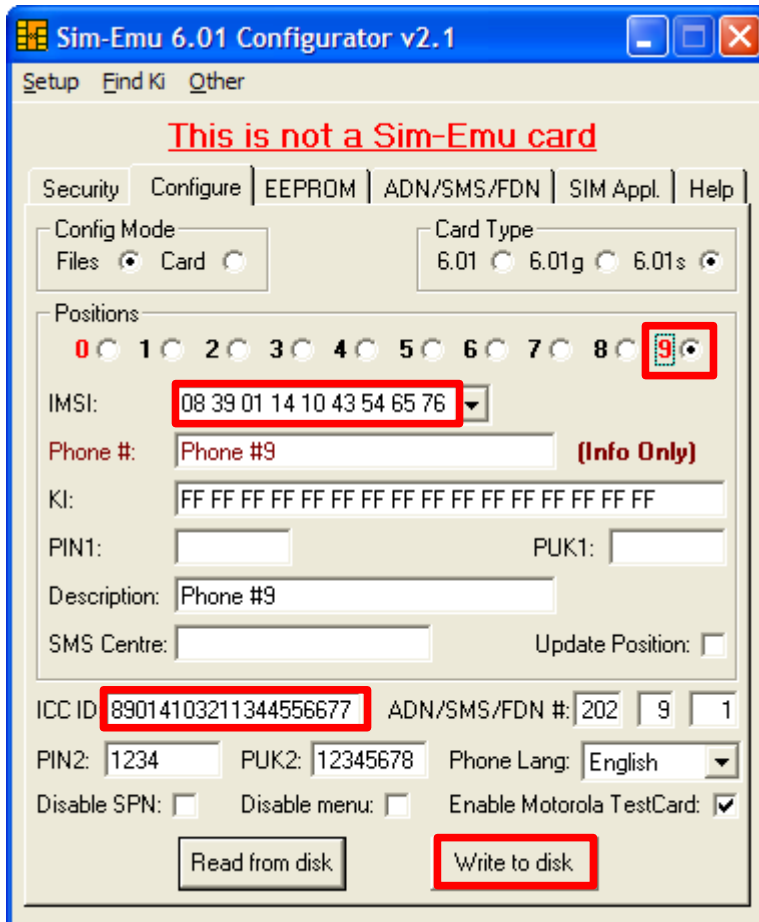
20. After you click "OPEN", the following window will be shown. Click "OK". Follow the rest of the instruction to open the EEPROM file (in my case it's SIM_EMU_6.01_iphone_u1_EP.HEX).



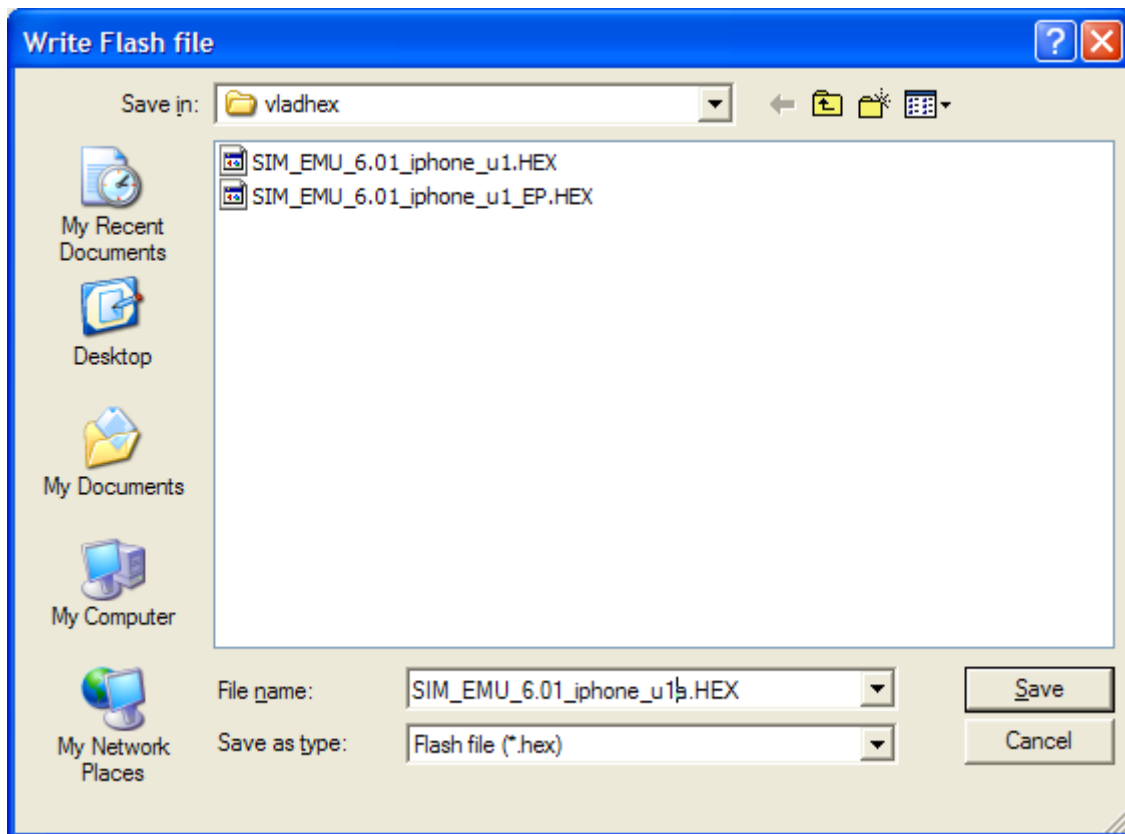
21. Now you have successfully read the FLASH and EEPROM files and the following window will be shown. Note you are in position 0 (zero). Enter your mobile carrier's IMSI (IMSI-a) and Ki. If you know your mobile carrier's SMS Centre (SMSC) number please enter it too. Leave the rest as is.




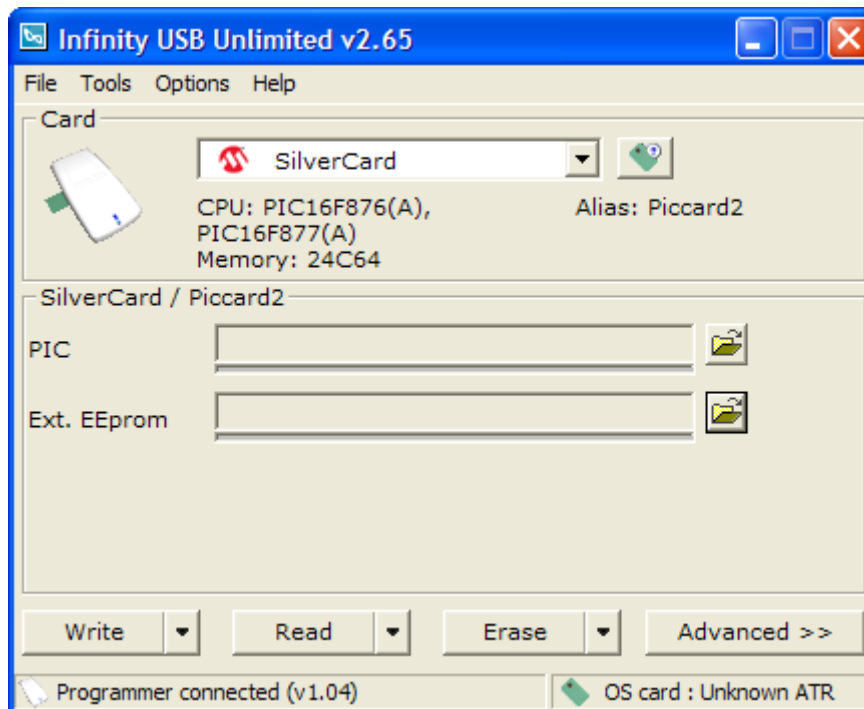
22. Click position 9 (nine). You will see the following window. Enter the AT&T IMSI (IMSI-b) and ICCID. Enter "1111" in PIN1 and "11111111" in PUK1. (Note: ICCID could be obtained by clicking the "i" button on the iPhone opening screen). Click "Write to disk".



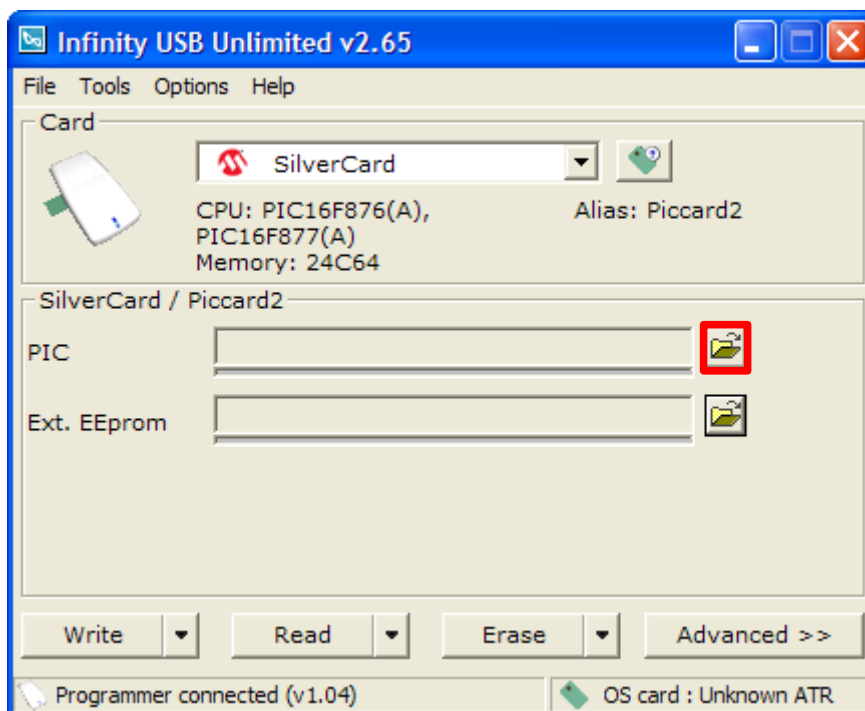
23. Save the information to a new Flash and EEPROM file. In my case it's called SIM_EMU_6.01_iphone_u1a.HEX and SIM_EMU_6.01_iphone_u1_EPa.HEX. After it's done quit SIM-EMU.



24. Right click on the Infinity USB VCP mode icon on the task bar  , and select "Exit VCP mode". You will see the following window.



25. Make sure in the Card section "SilverCard" is selected. Now click the "Open File" icon here next to PIC.



26. Select the modified Flash file (in my case it's SIM_EMU_6.01_iphone_ula.HEX) and Click "Open". Do the same for Ext. EEprom (use the modified EEPROM file (in my case it's SIM_EMU_6.01_iphone_ul_EPa.HEX). Click "Write" and wait for the process to complete. Quit IUUP software and remove the silver card from the IUUP.
27. Activate the iPhone by following the method here first (http://www.hacktheiphone.com/iphone_first_ten_steps_to_modding_mac.html) and then here second (http://www.hacktheiphone.com/iphone_using_cingular_for_windows.html).
28. Insert the silver card into the iPhone. It will ask for a PIN. Enter "1111" and click "OK".
29. Now wait for the iPhone to recognise your mobile network and establish the connection. If successful you will see your mobile carrier name next to the signal bar. Enjoy!!
30. In order to enable EDGE, first you need to make sure your mobile carrier support EDGE. Then you need to get the preferences.plist using iphoninterface from /var/root/Library/Preferences/SystemConfiguration/, make changes to APN/Username/Password, and put the modified preferences.plist back to the same directory. Reboot and enjoy!! (I have noted that the settings revert back to default (ie. AT&T APN/Username/Password) after sleep or reboot, not sure why).

ENDING WORDS

I hope you have fun enabling the phone function of your iPhone. If you get stuck at any step please let me know. Thanks everyone for your support.

Product names, brands, and other trademarks featured or referred to within this documentation are the property of their respective trademark holders. These trademark holders are not affiliated with the author of this documentation, and do not sponsor or endorse the materials contained within this documentation.
