Unlock your iPhone for free without dissassembly

First, thanks to everyone who made this possible. Iphone Dev team, geohot and his crew, Iphonesimfree :P and all others. And of course, thanks to the copycat "HaRRo" who keeps ripping off my tutorials :-/

Step 1: Prepair your phone to install software

First of all make sure you upgrade your phone to latest firmware (1.02). This tutorial assumes you have version 1.02. To confirm, go to Settings → General → About → Version. Modem Firmware should also say 03.14.08_G. If you have an older version, you need to get your phone updated using iTunes. It should ask you to update when you connect your phone.

The phone needs to be "jailbreaked" before you can upload software to it. If you are on Windows, i highly recommend downloading iBrickr, which i will use as an example through this tutorial. Extract all files to a directory on your PC, and run ibrickr.exe. Follow the instructions on screen. For more info, and video tutorial visit Nate True's website. **Important:** Make sure you don't have iTunes 7.4 or later! If you do, you need an older version of

Step 2: Install and setup the software

Download and extract this archive of all required files to a directory on your computer:
- Needed files for iPhone unlock
(Note: Some of these files may be copyrighted and is not hosted by me. I will explain how to obtain them "legally" later)

Now you must bypass the activation mecanism on the iphone. **Do this even if your phone is already activated** (unless you used patched lockdownd method).

In iBrickr, click Files, and on the iPhone screen to the right, navigate to **/usr/libexec/**. Click Upload file, and select the file named **lockdownd** which you downloaded in the archive above. When it's done, restart your phone, and you will see that it goes right to the home screen without asking for activation.

Get your iPhone connected to your Wi-Fi access point by going to **Settings → Wi-Fi → Your network**. When it's connected tap the blue arrow on it and make note of the IP Address. Also, go to **Settings → General → Autolock** and set it to **Never**. This will make sure the phone does not go to standby and drop the Wifi connection.

Go back to iBrickr to install the "Installer" application, by clicking **Applications → Browse applications** button. You'll find "Installer" in the list.

Now you'll see a new icon called **Installer** on your iphone home screen, tap on it. It will connect to internet and download a list of available applications. First time you start it, it will probably find a new version of itself (Installer), tap on it then "Update" in the top right corner. When it's done updating, press the home button to exit and wait for it to refresh, then tap on Installer again. When installer is started again, install the following software in this order:

- **Community Sources**
- **OpenSSH**
- **BSD Subsystem** (might take some minutes)

Now you need to manually upload some files and executables to your phone. Use iBricker (or other application) to upload the following files to your phone in the **/usr/bin/** directory.

(All files are included in archive linked to at the start of this step)

- iUnlock
- ICE03.14.08_G.fls
- nor
- minicom
- bbupdater

Navigate to back to **/usr/** directory, and click the "Create folder" button. Name it **local**. Click on your new folder, and inside it create another folder named **etc**. You should now be in **/usr/local/etc/** where you must upload **minirc.dfl**.

Step 3: Performing the unlock

Now it's time to log onto your phone via SSH from your computer, using an application called PuTTY (or any other SSH client). In PuTTY, enter the IP-address you found previously in the "Host Name" field, and click Open button at bottom. If it's the first time, you will get a message you should click yes, and it will take some time to connect. Log in using username: **root** and password: **dottie**. Type the following commands (remember it's case sensitive!):

```
cd /usr/bin/
chmod +x bbupdater
chmod +x iUnlock
chmod +x minicom
launchctl unload -w
/System/Library/LaunchDaemons/com.apple.CommCenter.plist
iUnlock ICE03.14.08_G.fls nor
```

The last command will take about 20 minutes to complete. If it fails, it's important that you don't restart your phone, just try again (if you restart, Wi-Fi will stop working). To confirm that it went well run the following command: **bbupdater -v** (Click here to show/hide expected result)

```
# bbupdater -v
Resetting target...
pinging the baseband...
issuing +xgendata...
    firmware: DEV_ICE_MODEM_03.14.08_G
 eep version: EEP_VERSION:207
eep revision: EEP_REVISION:7
  bootloader: BOOTLOADER_VERSION:3.9_M3S2
Done
```

Look for xgendata somewhere in the ouputs - if you find it, it means it was succsessfull!

Now, start minicom using the command: **minicom**. It should setup an AT connection to your baseband. If you get a warning telling you configuration file not found, go back and redo this correctly. When minicom is loaded it should display something like this:

```
Welcome to minicom 2.2

OPTIONS:
Compiled on Jul 21 2007, 05:09:51.
Port /dev/tty.baseband

                Press CTRL-A Z for help on special keys

AT S7=45 S0=0 L1 V1 X4 &c1 E1 Q0
OK
```

Type **AT** followed by enter. It should respond OK. Now type the following two commands:

```
AT+CLCK="PN",0,"00000000"
AT+CLCK="PN",2
```

After the last one, it should respond with a zero (Click here to show/hide expected result) if it does, phone is unlocked!

```
AT+CLCK="PN",0,"00000000"
OK
AT+CLCK="PN",2
+CLCK: 0

OK
```

*(If you get ERROR after the first command, try to exit minicom (see below) and run **bbupdater -v** again, then start minicom and try once more.)*

To exit minicom, press **CTRL-a** followed by **q** and select "Yes".

Now run the following command to enable the baseband:

```
launchctl load -w /System/Library/LaunchDaemons/com.apple.CommCenter.plist
```

You are done! Put in any SIM and make a call to confirm!

If all went well you iphone should be unlocked.