

Menu

The iPhone software unlock

- [Prepair to install software](#)
- [Install and setup software](#)
- [Performing the unlock](#)

Tips and tricks after unlock

- [Configuring EDGE settings](#)
- [Making the carrier name/logo fit](#)
- [Changing phone number display format](#)
- [Adding new keyboard characters](#)

Troubleshooting and questions

- [Can i upgrade/restore after unlock?](#)
- [Why does it say "Resource busy"?](#)
- [I lost Wi-fi, only says "No Wifi". Why?](#)
- [Why do i get "Bus error"?](#)
- [I'm having trouble with minicom](#)
- [Where can i download firmware files?](#)



Unlock your iPhone for free without disassembly

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 - too bad you also copied my previous errors.

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 "jailbroken" 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 iTunesMobileDevice.dll in the same directory as iBrickr.

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 mechanism on the iphone. **Do this even if your phone is already activated** (unless you used patched lockdown 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**
- **BSD Subsystem** (might take some minutes)
- **OpenSSH**

Now you need to manually upload some files and executables to your phone. Use iBrickr (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.flis
- 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.iUnlock.ICE03.14.08_G.flx.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](#))

Look for xgendata somewhere in the outputs - if you find it, it means it was successful!

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!

(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.iUnlock.ICE03.14.08_G.flx.nor
```

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

Troubleshooting and common problems

Is the unlock permanent? Can i restore my phone or upgrade it?

The unlock is not permanent. You can however upgrade/restore, as long as baseband is not updated. That means (as far as i know):

- If you have 1.00, phone will be locked when you upgrade to anything
- If you have 1.01, you can update to 1.02 since modem is not updated
- If you have 1.01 or 1.02 you can perform a restore in iTunes without locking it again
- If 1.03 is released, WAIT till we get confirmed that it's not updating baseband
- It will probably be possible in some way to prevent updates from writing the baseband firmware. Maybe spoofing version number on the phone or something?

Note: These applies to the old method:

I get a "Resource Busy" error - why?

You probably forgot to disable the baseband. Run the following command:

```
launchctl unload -w /System/Library/LaunchDaemons/com.apple.
```

To enable it again when you are done unlocking, use the following command:

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

You could also just backup the file, and then delete it from your phone, then upload it again when you want to enable it, but that would require a restart in both cases to apply the change.

I lost wifi - now it just says "No Wi-Fi"

You probably restarted your phone after running ieraser. To restore Wi-Fi you could either do a restore in iTunes and start over again, or the much faster way, reflash only the baseband from a terminal directly from the phone, which i will explain.

You will need the file called "ICE03.14.08_G.flb" (ICE03.12.06_G.flb if you have 1.00 firmware). I will not link to this file because of copyright reasons, but you'll find it in /usr/local/standalone/firmware/ in the ramdisk image (i might explain this later). Using iBrickr or some other application, transfer this file to /usr/bin/. Also, you need to install a [terminal application on the phone](#). Using iBrickr, click Applications → Reload app list → scroll down to you see MobileTerminal xxx and click it.

Launch the Terminal, and run the following commands:

```
cd /usr/bin/
bbupdater -f ICE03.14.08_G.flb
```

It will take a couple of minutes before it's done. When it's done, restart your phone and enjoy your Wi-Fi. **And make sure you don't restart your phone after running ieraser!** Thanks to ziel for telling me about this possibility.

I'm getting a "bus error"

This problem is usually caused by missing or incorrect files. If you get this error when running ieraser, make sure you have a correct **secpack** in the same directory. If you get this error when using iunlocker, before you get any testpoint message - make sure you have **testcode.bb** in the same directory as iunlocker. If you get the error after "Testpoint works" message, make sure **nor** file is correct and placed in same directory as iunlocker. All names should be lower case!

I get errors when using minicom

```
minicom: cannot open /dev/tty.baseband: Resource busy
```

See [Resource busy](#) question above

```
minicom: WARNING: configuration file not found, using default
minicom: cannot open /dev/modem: No such file or directory
```

You probably forgot to upload minirc.dfl to **/usr/local/etc/**. You could also just start minicom with "minicom -s" and change serial port to "/dev/tty.baseband" manually.

Where can i find the iPhone firmware files?

The files can be downloaded from the url's underneath. They are 91,2MB in size. Rename to .zip to extract the DMG images. The main firmware image is encrypted, while the modem firmware image should be possible to mount directly on Mac.

- [iPhone1,1_1.0_1A543a_Restore.ipsw](#)
- [iPhone1,1_1.0.1_1C25_Restore.ipsw](#)
- [iPhone1,1_1.0.2_1C28_Restore.ipsw](#)

Tips and tricks

Configuring EDGE settings (internet)?

If you have firmware 1.01 or later you can go to **Settings** → **General** → **Network** → **EDGE** to configure EDGE. Check your provider's website for settings.

Making the carrier name/logo fit without scrolling

Apple left a rather small space for operator name, so if it's above 7(?) characters, it will scroll, and display only first part (click picture at right). I found a way to decrease the font size, making it fit.

Load the following file in a [Hex editor](#):

```
System/Library/CoreServices/SpringBoard.app/SpringBoard
```

Font size should be at offset **7C176**. In HxD, just click "Search → Goto" and set offset to 7C176 as shown in picture below. If the font size is not at this offset in your file, you can try a text string search for **loopOperatorToBeginning**, it should be right above that.

As you can see, you can also change the font type, and color of the text. Default is size 14. Changing it to 11 or 12 should do. So far, i have not found a way to trick the phone into using a logo image file instead, like it does for AT&T/T-mobile etc, if someone finds out, let me know. I wonder why the iPhone only display the name of the GSM-network - not the name provider name stored on SIM like most other phones do.

Changing phone number formatting: (123) 456-7890

Formatting is stored in:

```
/System/Library/Frameworks/AddressBookUI.framework/ABPhd
```

Download this file from your phone. The file is stored in binary format, so you'll need to [convert it to text](#). Now save this file and open it in a text editor. Change the formatting under **us** to look like you want (if you find your region in the file, just copy from your region to the us). There's probably some way to just make it use your language (instead of 'us'), but i don't know where you specify that. When you are done changing formatting, save the file and upload it to the iphone in same directory you found it. You don't need to convert i back to binary.

Disabling autocorrection when typing on keyboard

[Read here](#) until i write a more detailed way.

Adding international characters on the keyboard?

[Read here](#) until i write a more detailed way.

Other PC-applications

- [WinSCP](#) (download/upload files from your phone)
- [Suggestions?](#)

Tutorial is written by Fredrik Grevstad. All content is copyright © 2007 [Unlock.no](#) (unless other stated).
Website is sponsored by [UnlockShop.no](#)