

How to activate, jailbreak and unlock 1.1.4 firmware with PwnageTool (3.9 / 4.6 bootloader)

intel Mac

PwnageTool is the latest program from the iPhone Dev Team. It will allow you to jailbreak, activate and unlock your iPhone using the safest methods yet. Instead of using a dedicated program to hack into the firmware already on the iPhone, iTunes itself is now used to restore your iPhone with the hacks already included in the firmware. PwnageTool is based on an exploit found in the lower levels of the iPhone and iPod Touch bootloaders. This allows for the execution of unsigned code. To learn more [read here, and here.](#)

Thanks go out to: asap18, bgm, Bugout, bushing, chris, dinopio, drudge, Fred_, ghost_000, gray, kroo, MuscleNerd, NerveGas, netkas, np101137, planetbeing, pr3d4t0r, pumpkin, pytey, roxfan, sam, Turbo, w___, wizzdaz, and Zf.

Before I get into this tutorial, please do not email with your personal scenario about your iPhone and if this will work or not. There is no way I can possibly know everything. **This is what worked for me.** [Here is a great FAQ for PwnageTool at Hackint0sh.](#) The iPhone I used was running 1.1.4 firmware with 04.02.13_G baseband and was unlocked via iNdependence. It also had the 4.6 bootloader. When I restored it, the unlock was gone. I then tried using iLiberty+ (version 1.5) and it would not unlock the iPhone. It did however downgrade the bootloader to 3.9 fake blank. I tried this twice. It did everything but unlock the iPhone. Enter PwnageTool after a fresh restore via DFU mode.

Attention

You should read my [Warning to all iPhone owners](#) page before proceeding.

Step 1.

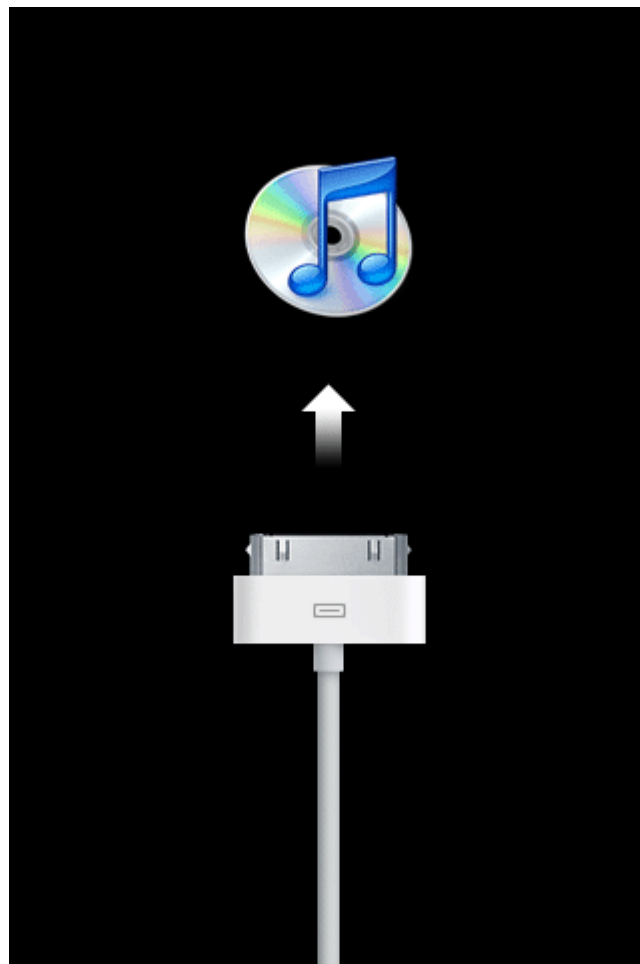
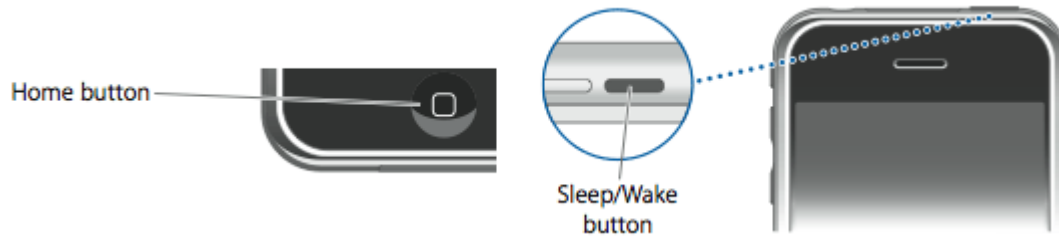
[Download PwnageTool version 1.1 here.](#)

Step 2.

[Download the 1.1.4 firmware here.](#)

Step 3.

Put your iPhone in restore mode (not DFU) by plugging it in to your Mac, and holding the Sleep/Wake and Home buttons until the Apple logo appears (about 20 seconds). Release the Sleep/Wake button, and continue holding the Home button until the connect to iTunes graphic is displayed.

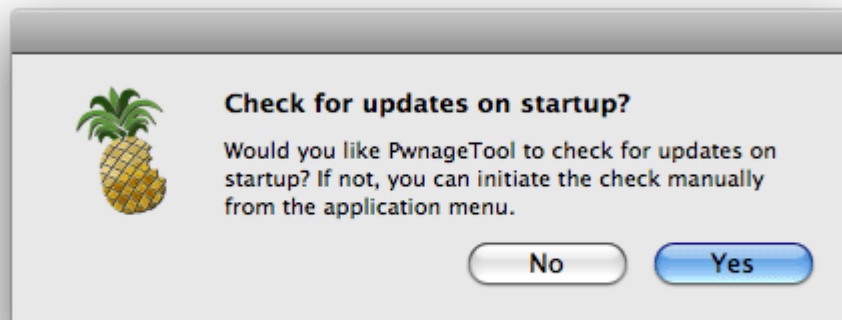


Step 4.

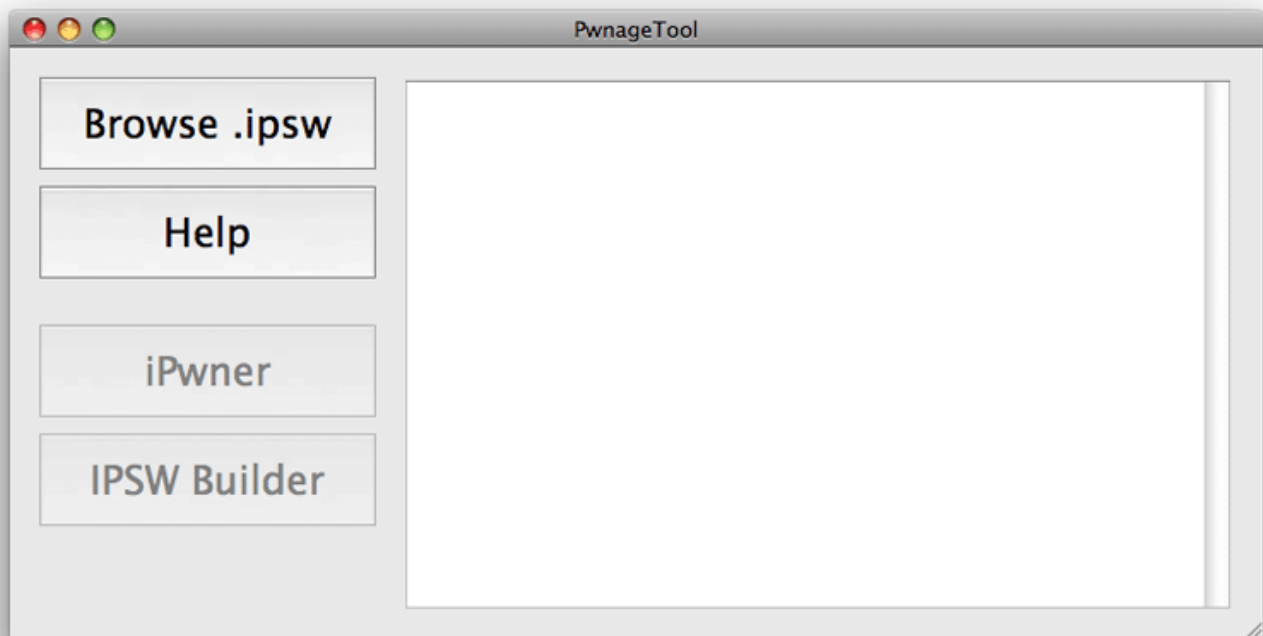
Unzip the PwnageTool zip file you downloaded earlier, and launch the program.



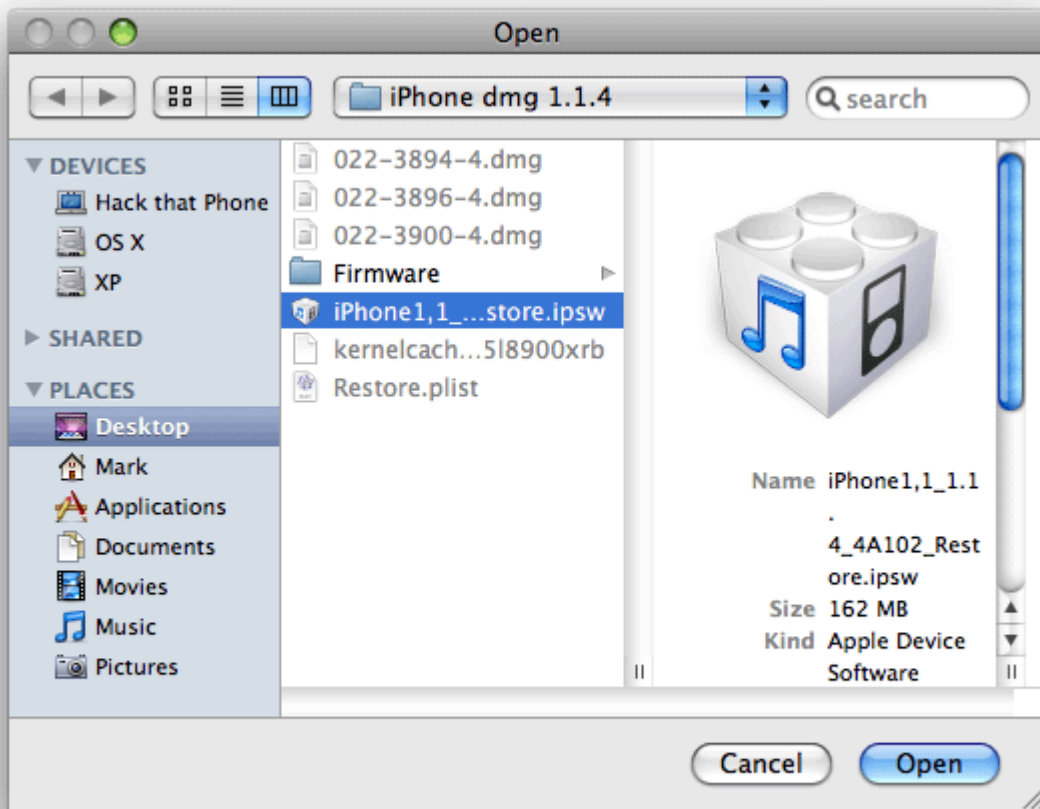
You'll be prompted to check for updates to PwnageTool automatically.



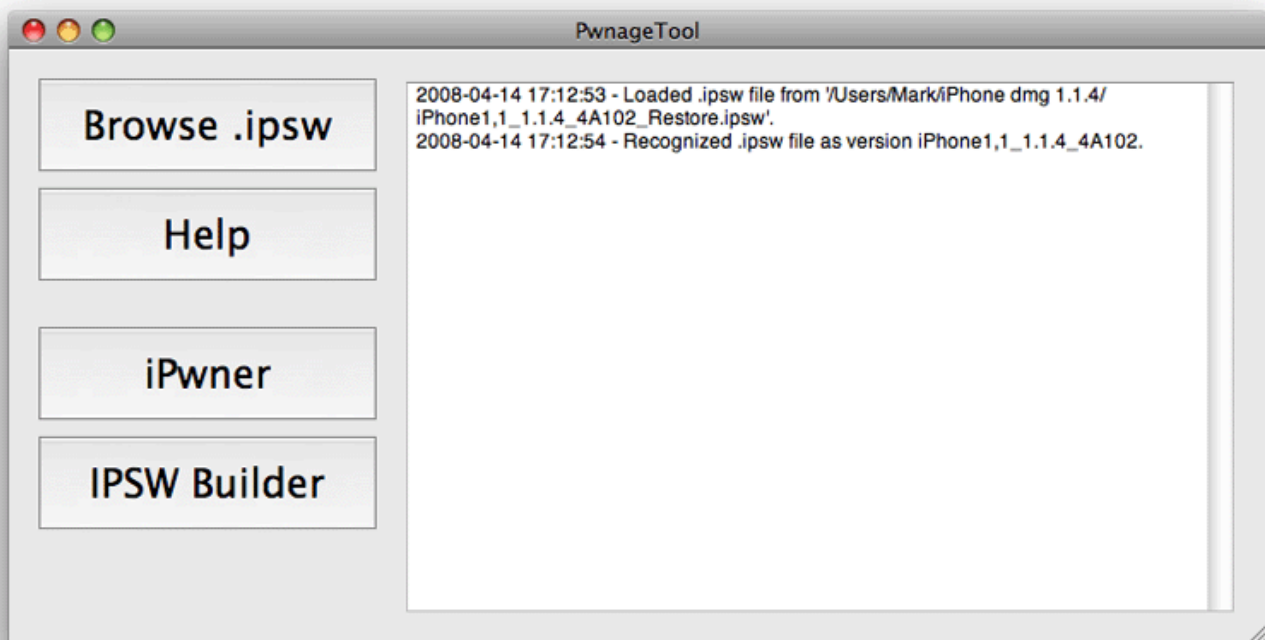
Click the Browse .ipsw button.



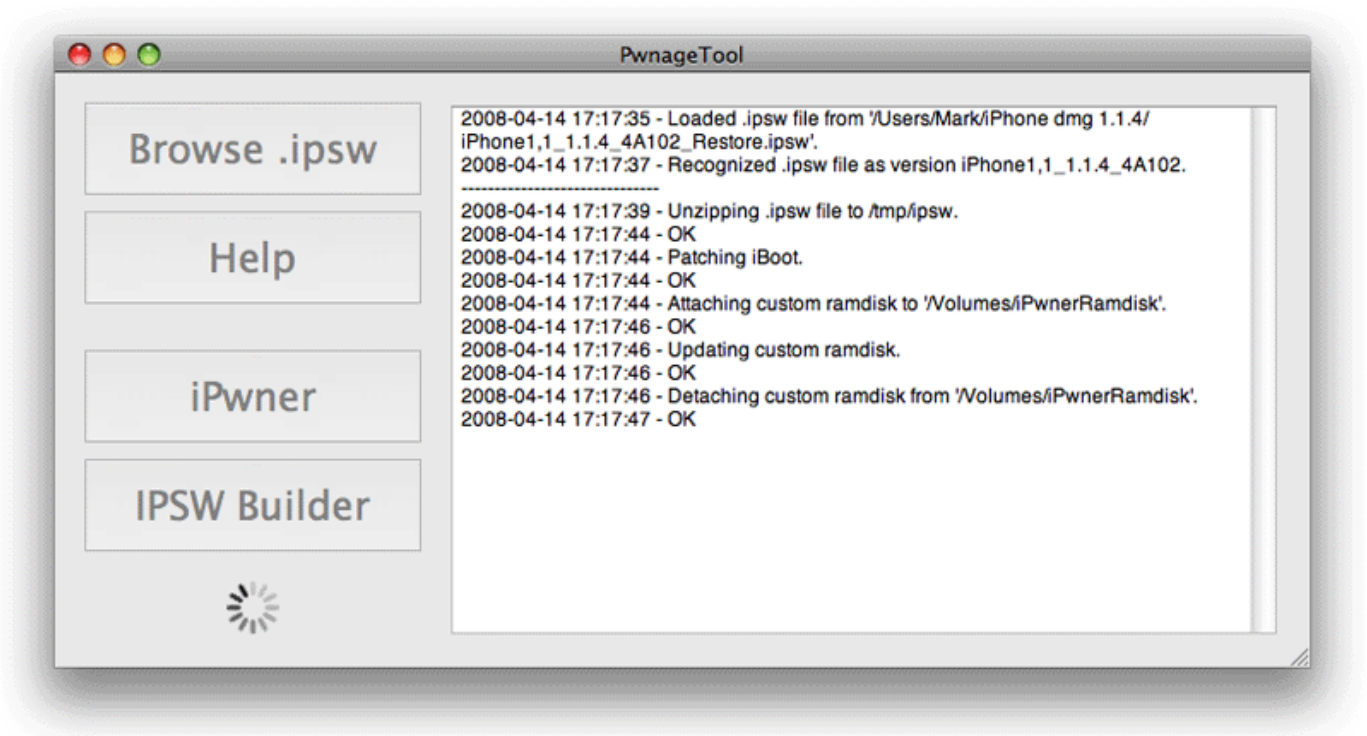
A file browser window will open. Navigate to where your 1.1.4 ipsw file is. Select it, and click Open.



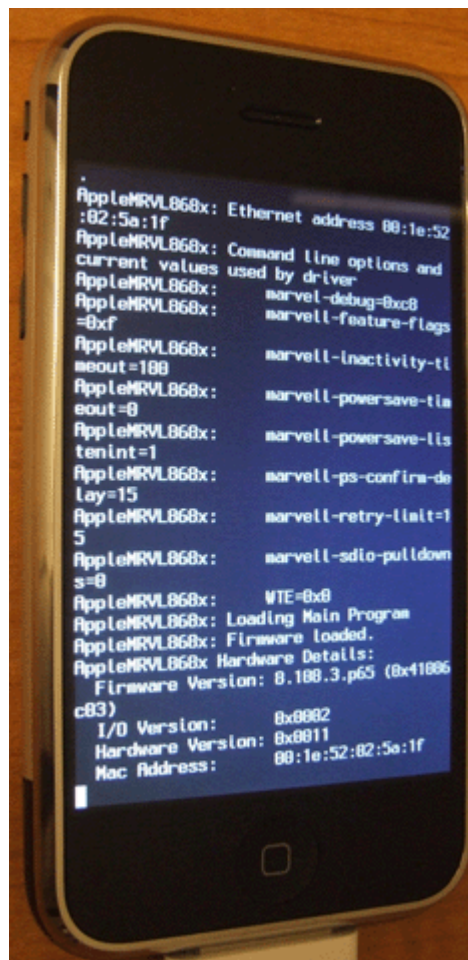
You should see similar output in a few seconds.



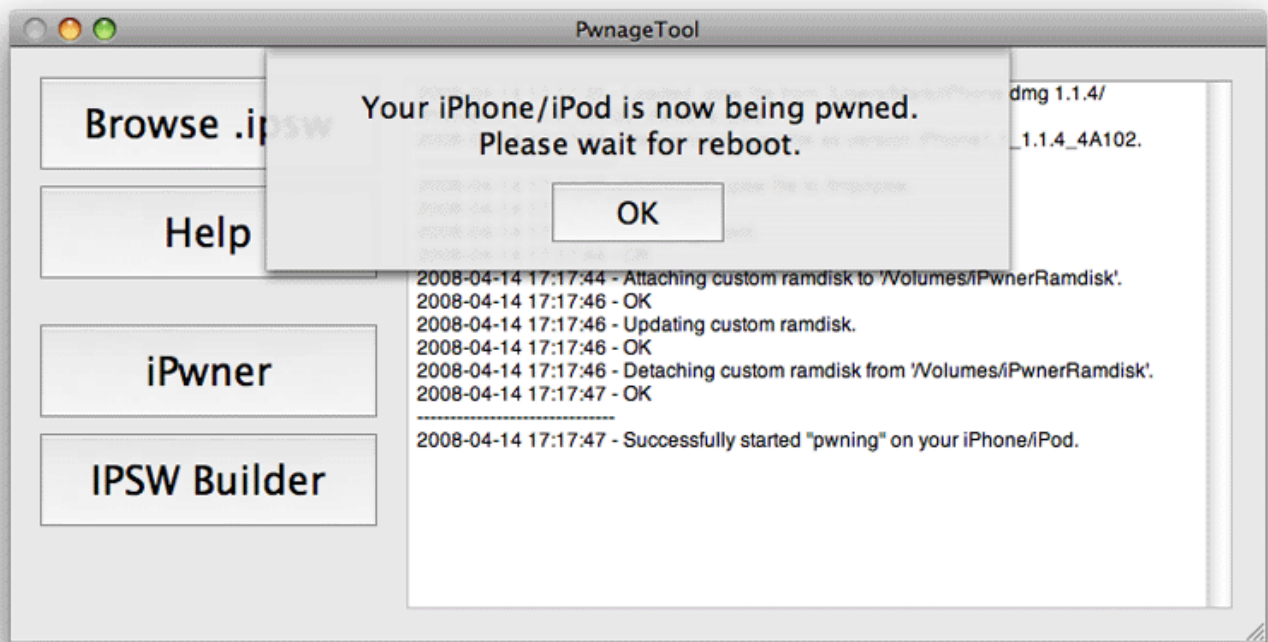
Click the iPwner button and more text will appear in the program window.



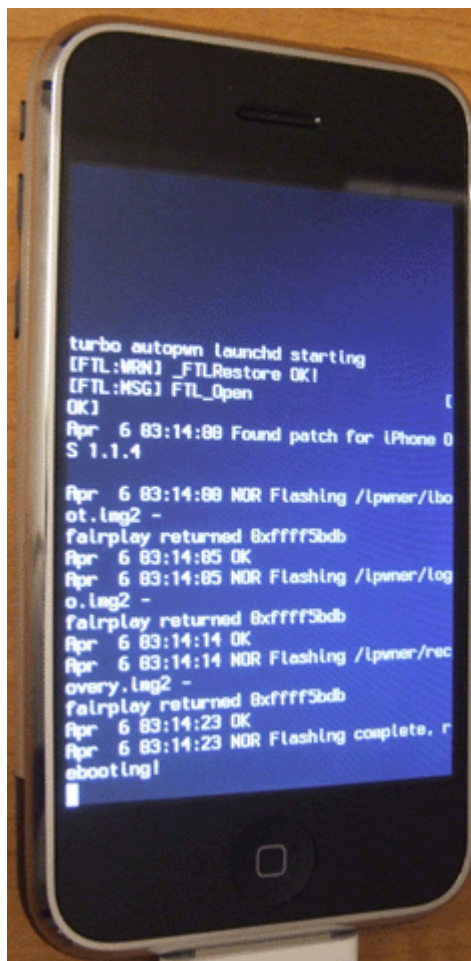
Text will now scroll on the iPhone screen.



A drop down message will appear.



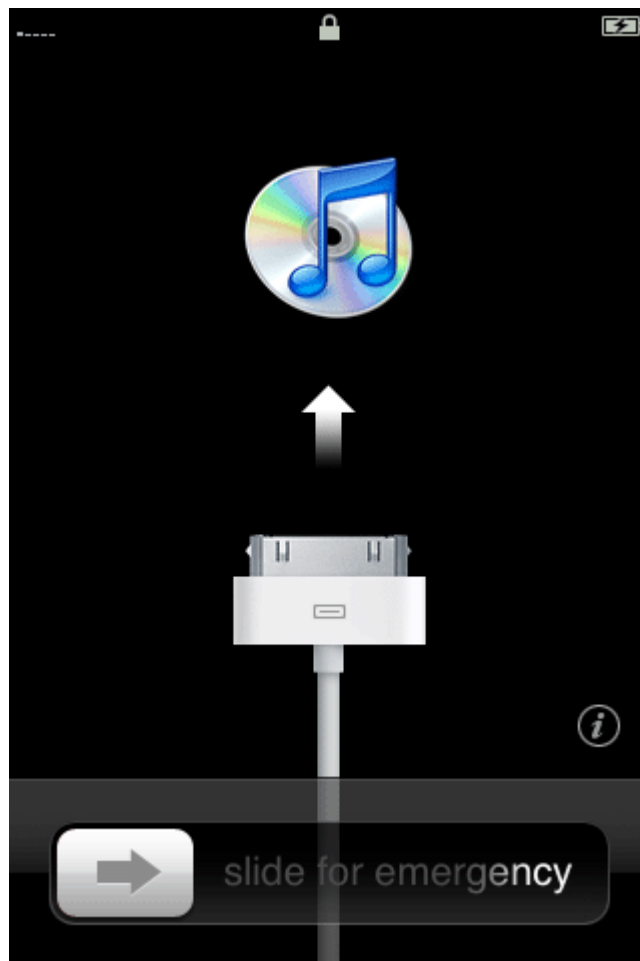
Code will slowly scroll up the iPhone's screen.



The iPhone will reboot with the PwnageTool logo instead of the silver Apple.



The slide for emergency screen returned. At least it did for me.



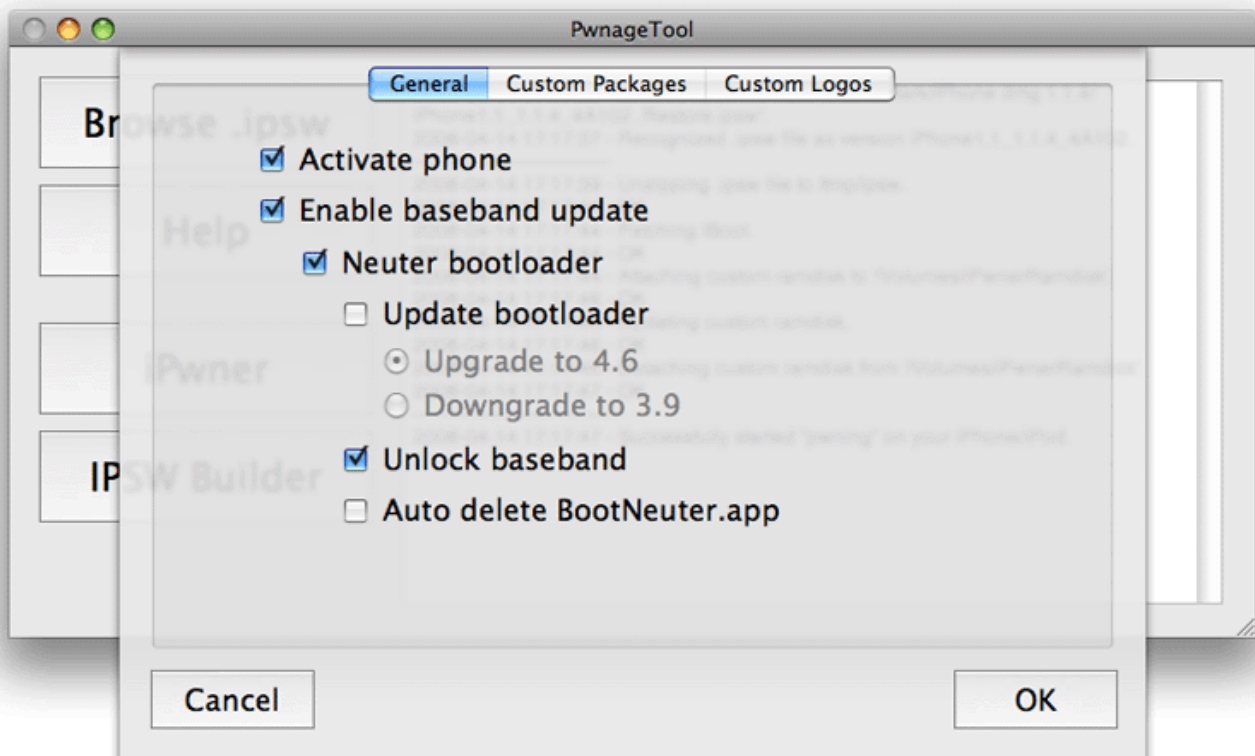
The status area of PwnageTool continued to report: "Successfully started "pwning" on your iPhone/iPod." It should say: "Successfully "pwned" your iPhone/iTouch."

I manually put the iPhone back into restore mode (wait for the pineapple graphic to appear this time, not the Apple). The Steve Jobs "surprise" graphic appeared (it replaces the connect to iTunes graphic).



Step 5.

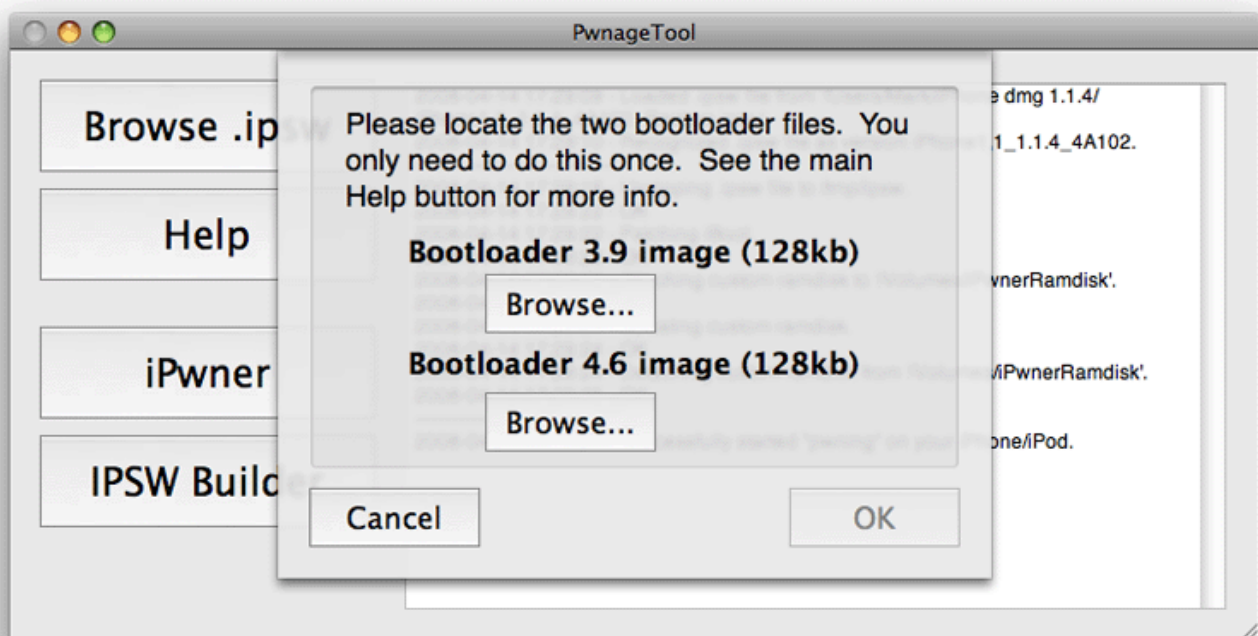
Click the IPSW Builder button. An options screen will appear. I checked the box "Enable baseband update" since I needed to unlock. Doing this auto checks the "Neuter bootloader" and "Unlock baseband" features. Click OK.



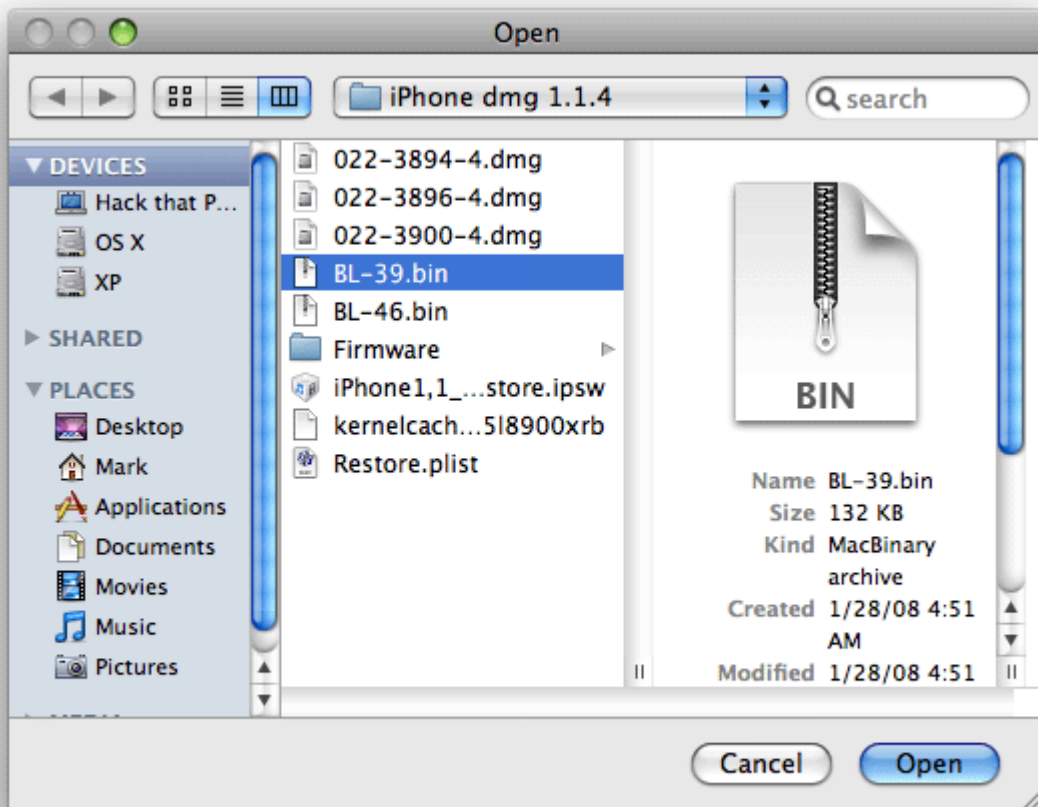
Here's my custom boot logo. If you'd like to see some other custom boot and recovery graphics [check out this page](#).



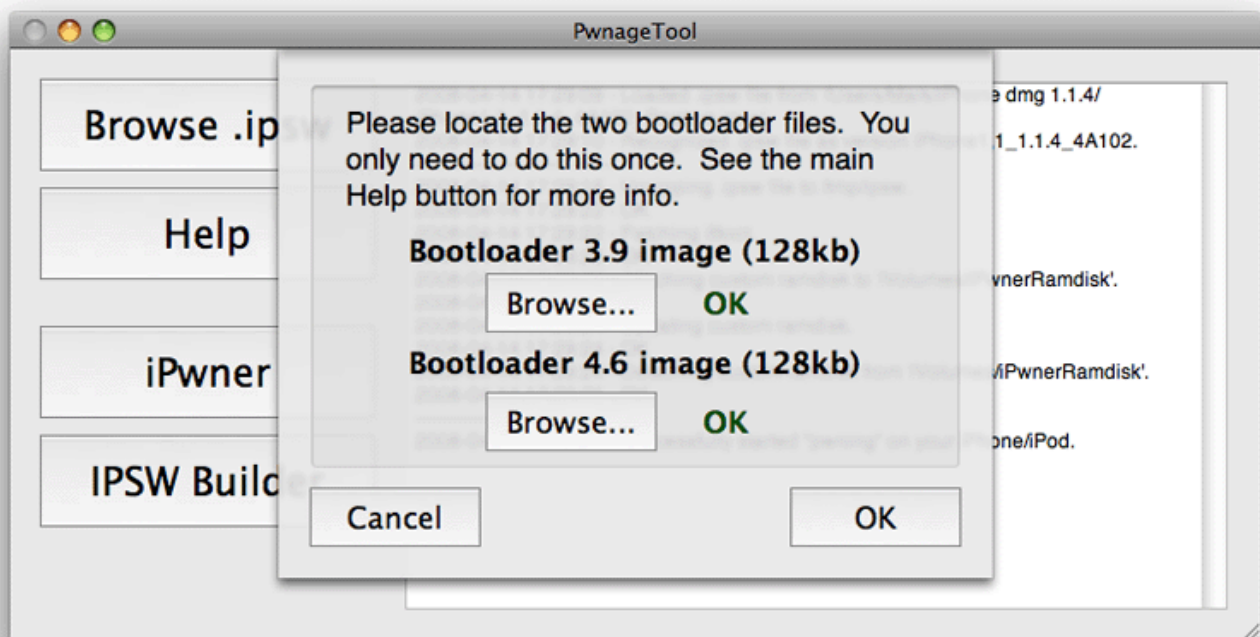
You will now be prompted to locate the 3.9 and 4.6 bootloader bin files. [Download them here](#). Decompress the rar.



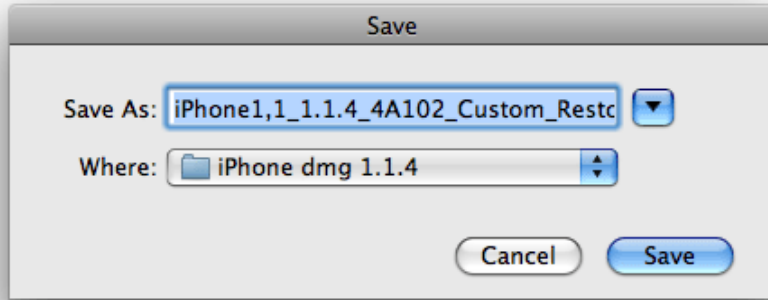
Click the Browse... buttons and navigate to each of the bootloader bin files, select them, and click Open.



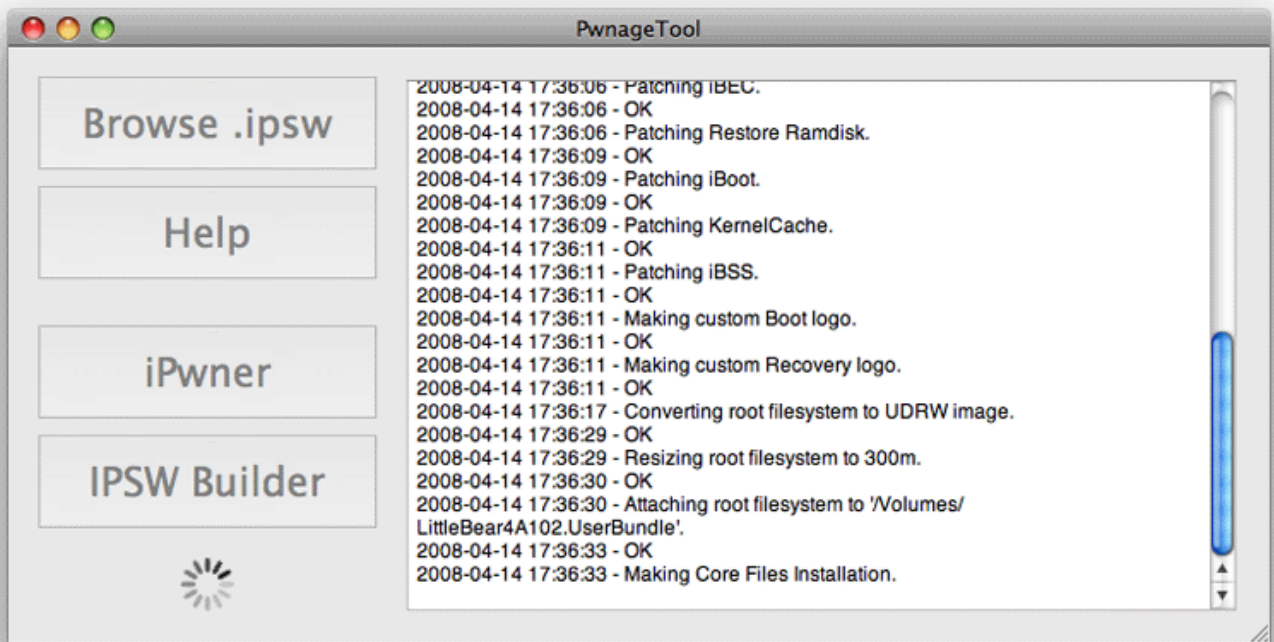
When you've loaded both bootloaders you should get an OK confirmation. Click OK.



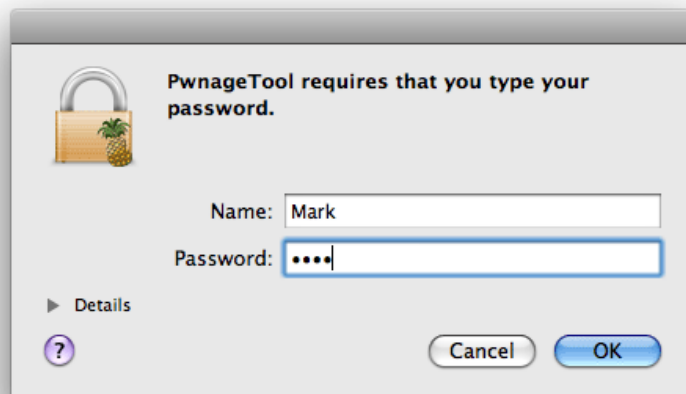
You can now name your custom firmware file. PwnageTool automatically adds the word "custom" to the original file name so you can tell it apart from your original ipsw. Click Save.



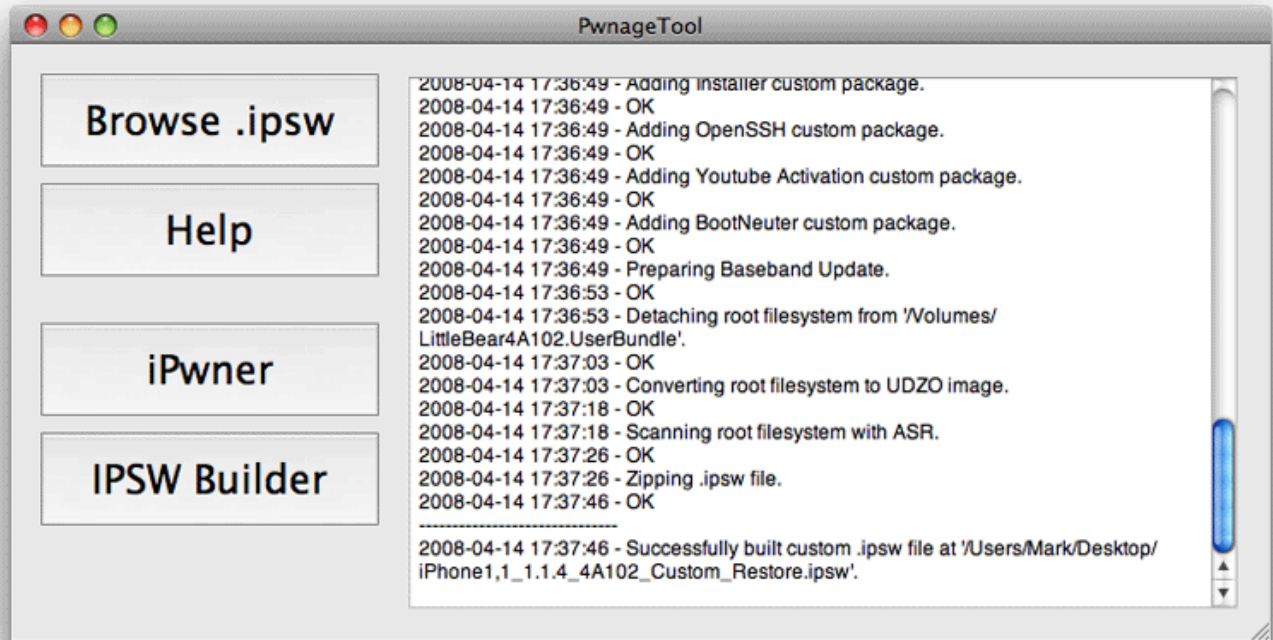
More text will appear in the status area of PwnageTool while your custom firmware is created.



During this process you will be prompted to enter your password.



The final bit of text will appear as the custom restore file is finalized. Close the PwnageTool once it has successfully completed. **Your iPhone should still be in recovery mode (displaying the Steve Jobs graphic).**



Step 6.

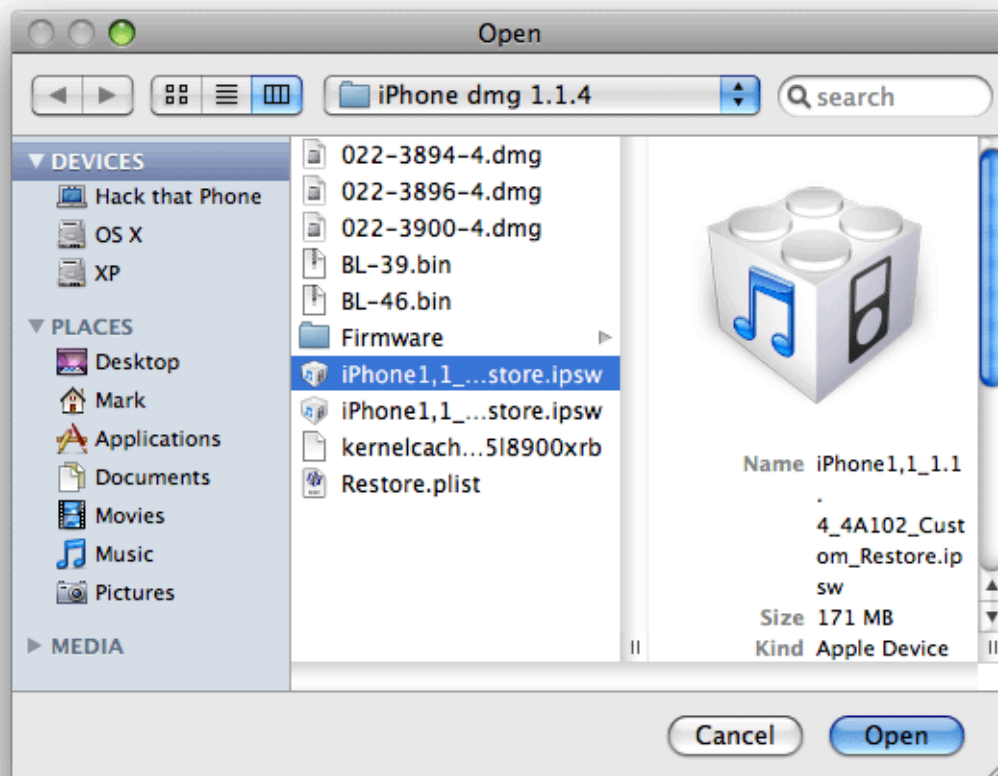
Launch iTunes and a pop up warning about recovery mode will appear.



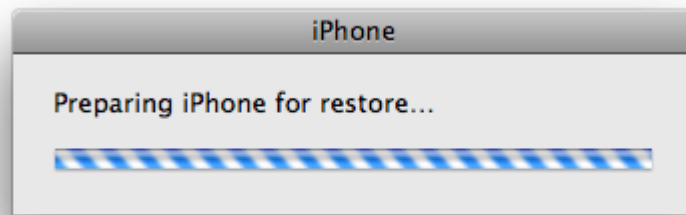
iTunes will look like this. Hold down your Option key and click Restore.



Navigate to where you saved your custom firmware restore file. Select it, and click Open.



Various status messages will display while the process continues.



The pineapple will reappear with the progress wheel.



After iTunes finishes restoring, the iPhone will reboot. If you chose to install BootNeuter (necessary for unlocking), then it will automatically start and unload the CommCenter process.

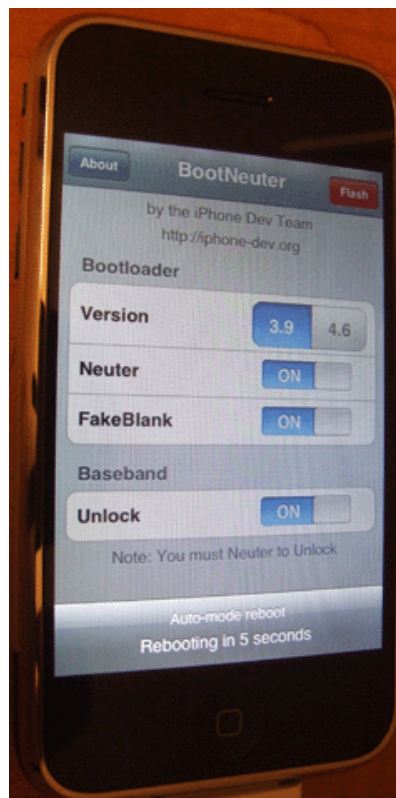
In the future, should you run BootNeuter again it will automatically unload the CommCenter process (you will lose your cellular signal). All you have to do is press the Home button to exit BootNetuer. Wait about 20 seconds and CommCenter will restart on its own (and your cellular signal will be restored). You may have to reboot the iPhone as your system sounds may be very low.

Several messages will display at the bottom of the program while it runs. Don't touch anything. This process will take several minutes to complete.



The next messages to appear are: "Flashing bootloader - do not interrupt!", "The bootloader was successfully flashed. Now flashing baseband." and "The bootloader and baseband were successfully flashed."

This is the final configuration of my BootNeuter program before it rebooted the iPhone.



The iPhone will reboot. You will then be at the SpringBoard with the Edit Home Screen pop up. Notice that BootNeuter and Installer are both installed already.

