



Fort Worth Police Department



Digital Forensic Lab

Topic: Apple iPhone Passcode Work-Around

Date: February 26, 2008

Author: Troy Lawrence

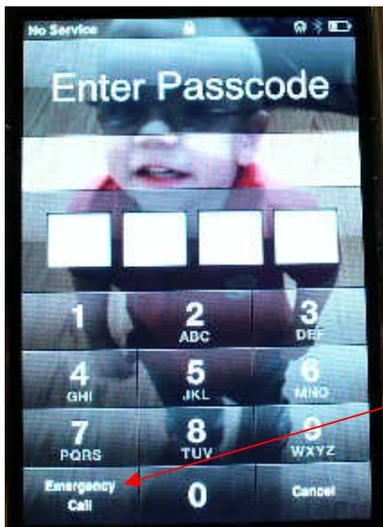
If you encounter an Apple iPhone where the phone is locked with a Passcode, keep in mind the hand set only allows 5 Passcode attempts before locking out phone.

This work-around is limited to iPhones with firmware versions 1.1.2 and earlier. The work-around was disabled on version 1.1.3 in February 2008.

Data can be retrieved from the SIM card as well as from the phone handset. To remove the SIM card, place a paperclip in the hole at the top of the phone. Force must be applied to get the SIM holder to pop-up. The SIM card will be inside a plastic tray and can be easily removed. Process the SIM card as normal.



To access the locked handset, follow these instructions:



From the keypad, press the “Emergency Call” button.

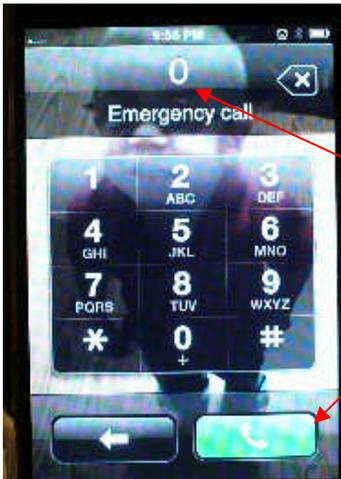


Type **##301#** followed by the green [phone] button.



Delete the previous entry by hitting the delete key six times.

(The delete key has an "X" in the middle)



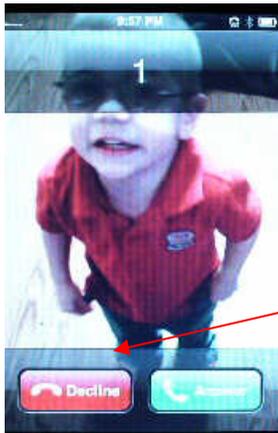
Type the number **0** followed by the green [phone] button.



Answer the call by pressing the green [Answer] button.



End the call by pressing the red [End Call] button.



Press the [Decline] button.



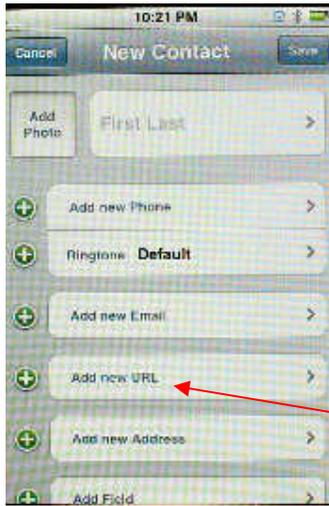
This will place you in the “Contacts” screen where you can view the “Favorites”, “Recents”, “Contacts”, “Keypad”, and “Voicemail”.

(The current view is “Contacts”)

“My Number” is located here.



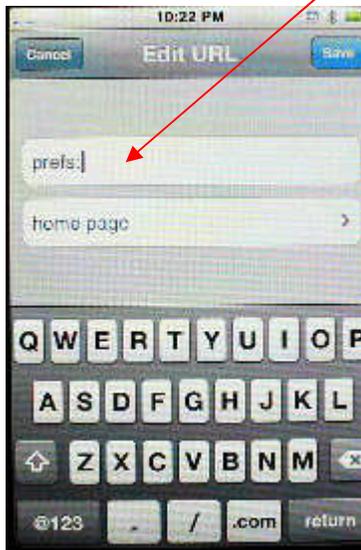
In the “Contacts” tab, press the [+] button at the top to create a new contact.



In the “Add new URL” tab,

Enter “**prefs:**”

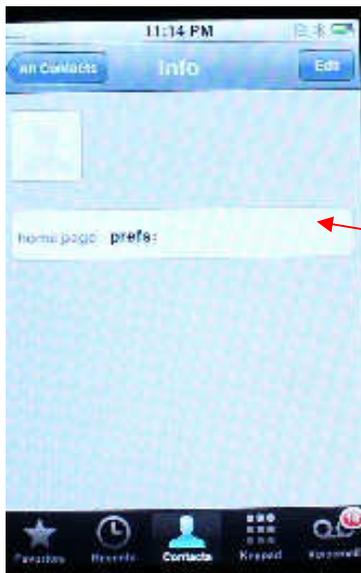
Press the [save] button.





Enter the [All Contacts] button to take you back to the “Contacts” screen.

Touch the “No Name” contact entry you just created. This will open up the contact page you just created (see below).



Click on the “home page prefs:” button.



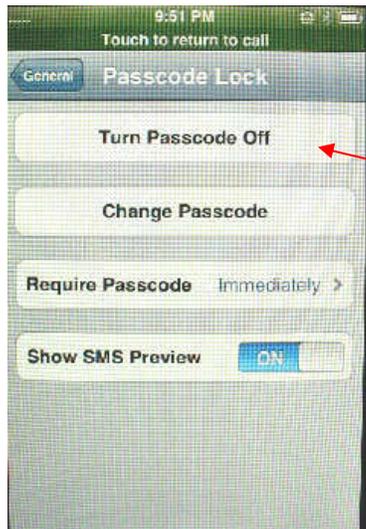
It will take you to the iPhone “Settings”.



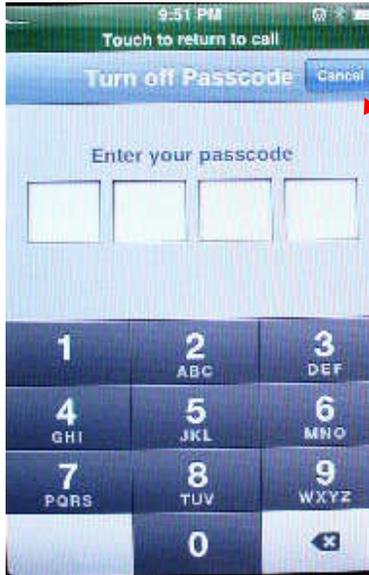
Click on the “General” tab.



Click on the "Passcode Lock" tab.



Click on "Turn Passcode Off" tab.



This will take you to a new screen where you enter the Passcode. You can enter this code as many times as you want and it won't lock you out.

Since there are 10,000 possible Passcodes, it is advisable to make one more modification.

Return to the "General" tab by clicking on [cancel].



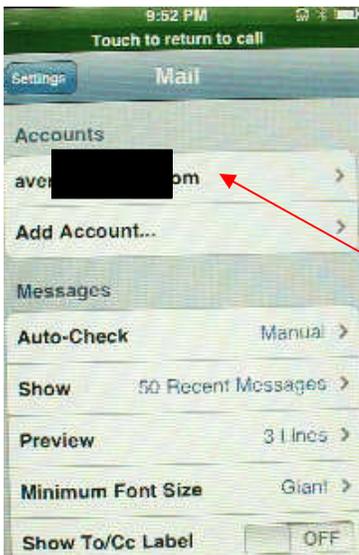
Click on "Auto-Lock" and reset it to "Never".

(This will keep the phone from timing out and giving you a black screen.)

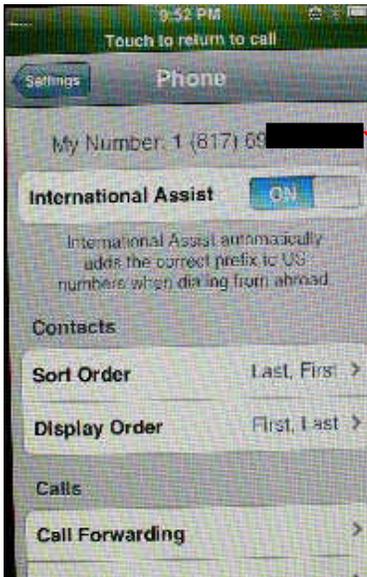
It is also recommended that you plug the phone into the iPhone power charger to maintain battery life as the screen will remain on and may drain the phone battery.



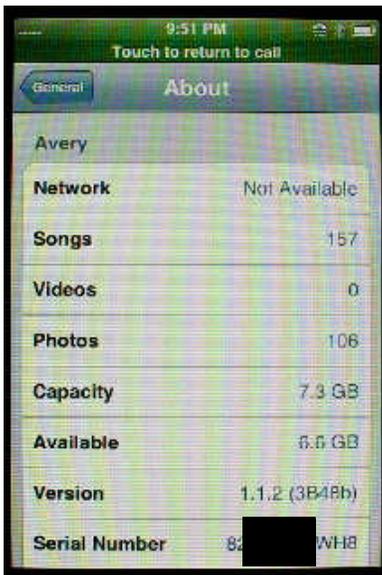
You have the ability to look at some of the pictures on this iPhone by clicking on the "Wallpaper" button in the "Settings" tab.



There may be additional information stored on the "Mail" button such as the e-mail address used by the phone owner.



The telephone number for the phone can be found in the “Phone” button of the “General” tab.



The phone serial number along with total number of songs, videos, and photos can be found in the “About” button of the “General” tab.



While this workaround will allow you to view different data areas of the cell phone, it will not allow you to download the information unless the Passcode is disabled. The screens can be photographed or copied manually. If you are able to guess the Passcode, or find it from a brute force attack, the contents of the phone can be copied using a fresh installation of iTunes.

Special thanks go to Mr. Curtis Thomas of the FBI's Forensic Electronic Device Analysis section for walking me through these steps. The screen shots came from an actual case and the pertinent information was redacted through the use of blackout boxes.