The Iphone SIM Lock: An IR Technique

Boring Disclaimer Stuff: This document is not designed to be legal guidance, advice, or opinion and any of the opinions, techniques, or procedures contained in this document should be discussed with a legal professional (like a lawyer) for legal admissability and/or legal integrity prior to utilization. Furthermore, any attempt to reproduce any of the tactics, techniques, or procedures contained within this document are done without the knowledge, consent, guidance, or support of the author.

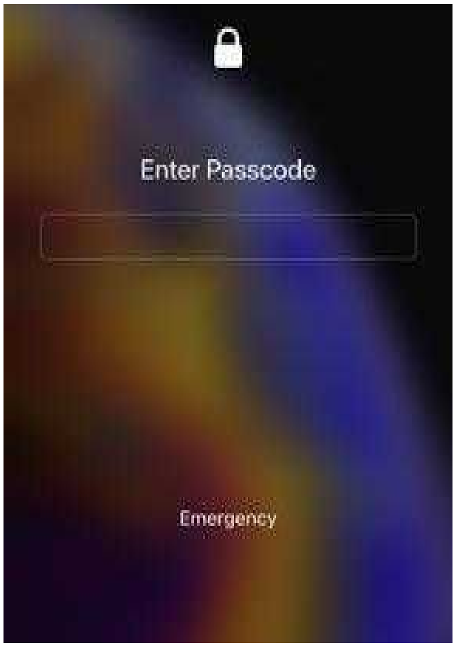
It has come to my attention that a number of professional do not know how to respond to or investigate incidents that happen on cellular devices. Although I am not a forensics expert I do have limited specific knowledge that may be benneficial for discussion amongst those whom are, or are aspiring to be, dfir and or forensics experts. In this article I will cover the use case where an IPhone is believed to be compromised in a persisten way or in a way that permits recompromise fairly easily (such as poorly written app or a trojan for example). The assumption here being that restarting the cellular device does not remove the threat (persistence through a poorly written app or an actual persistent exploit). The first thing area covered is how to enable the SIM Lock on an Iphone. Then this article will demonstrate how to restart the IPhone and access the contents without unlocking the SIM. Lastly, this article will demonstrate some limitations that are placed on a device that has a locked SIM and why this technique may be of practical use.

Caveats

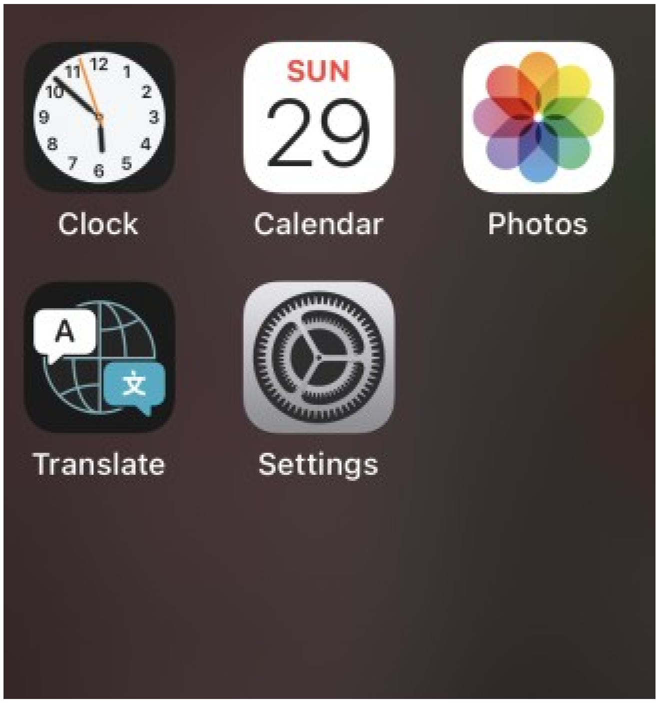
Having a locked SIM does not prevent data from being transmitted through bluetooth, NFC, or WiFi. Having a locked SIM only has the potential to act as a cellular firewall and may only prevent cellular based communications. As technology and standards changes having a locked SIM may become less reliable as a cellular signal firewall.

How to Enable a SIM Lock on an IPhone

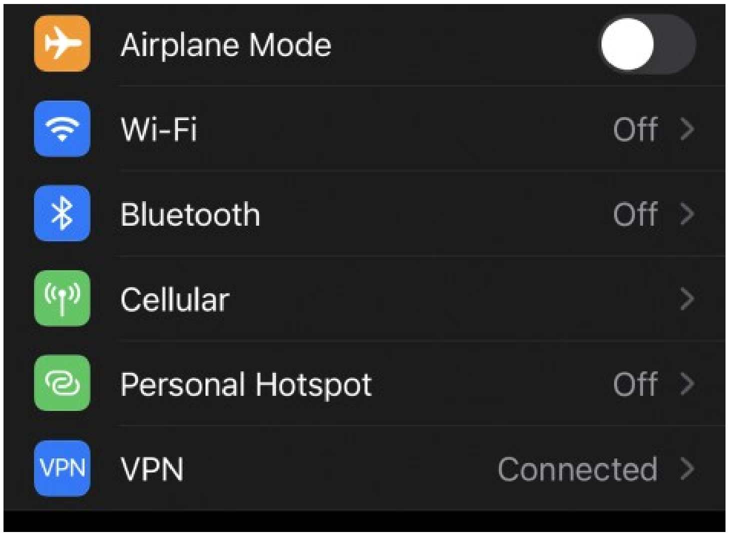
1. Enter your phone’s password



2. Open the “Settings” app



3. Select the “Cellular” menu item



Airplane Mode

Wi-Fi Off

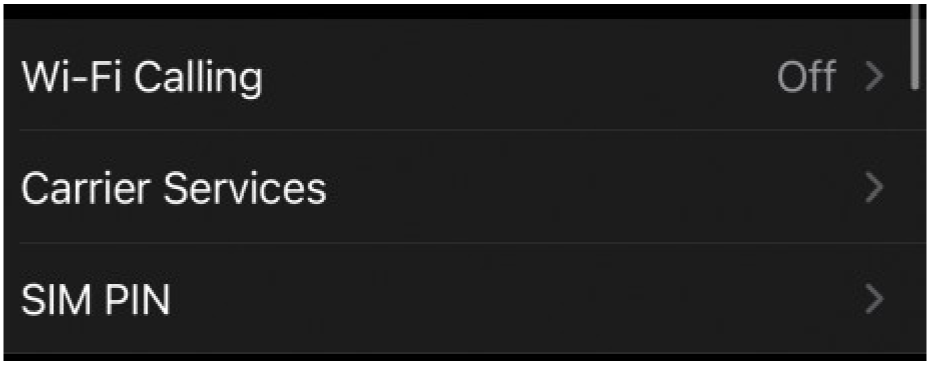
Bluetooth Off

Cellular

Personal Hotspot Off

VPN Connected

4. Press the “SIM PIN” line item

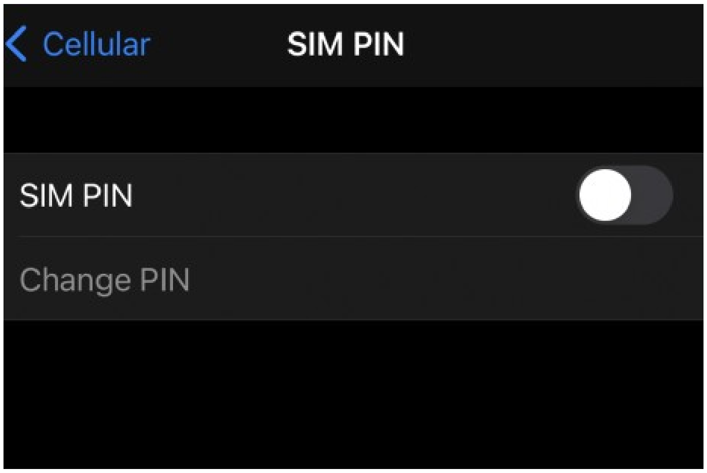


Wi-Fi Calling Off

Carrier Services

SIM PIN

5. Toggle the “SIM PIN” selctor so it appears green



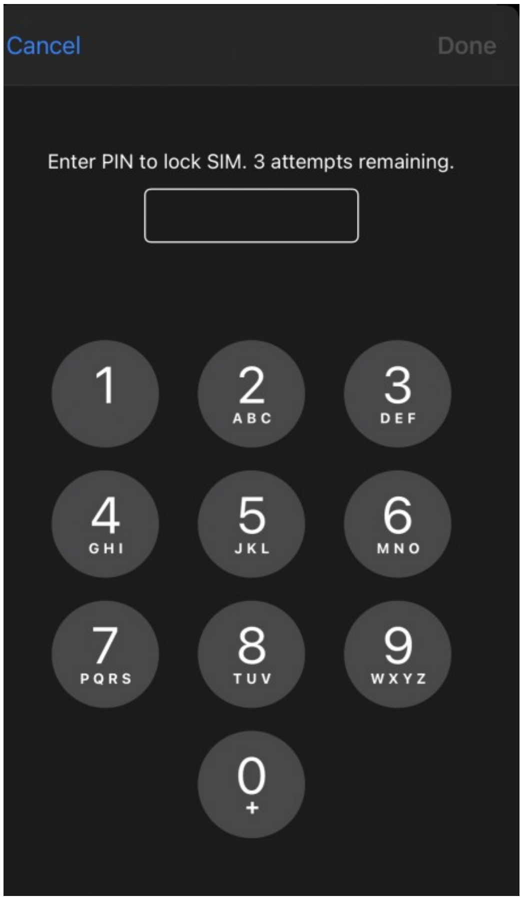
SIM PIN

SIM PIN

Change PIN

6. Enter your selected secret

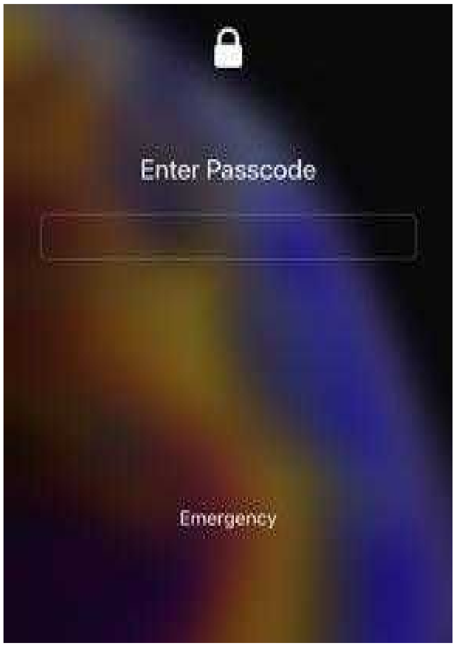
   Warning: If you forget your SIM PIN you will need to contact your service provider to retrieve the PUK Code to unlock your device. In the case of a corporate device an administrator may be required to retrieve the PUK Code on your behalf.



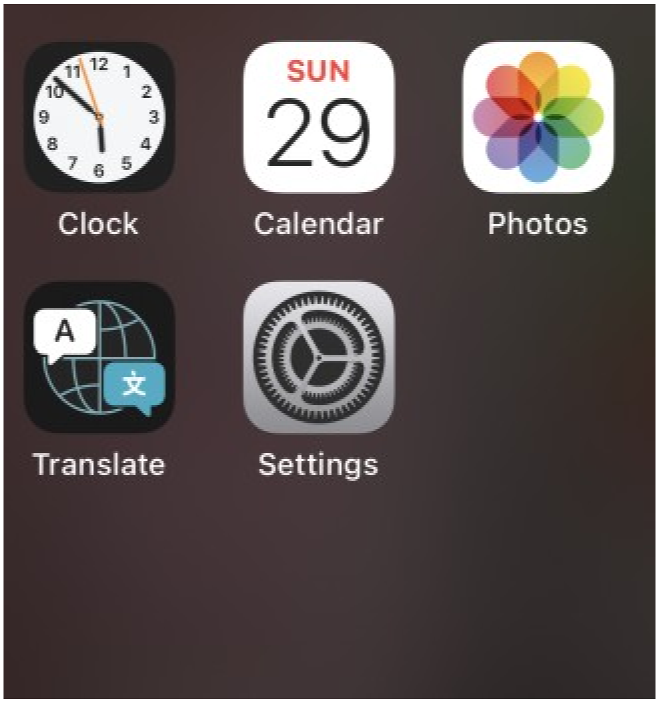
Enter PIN to lock SIM. 3 attempts remaining.

Restarting an IPhone without unlocking the SIM

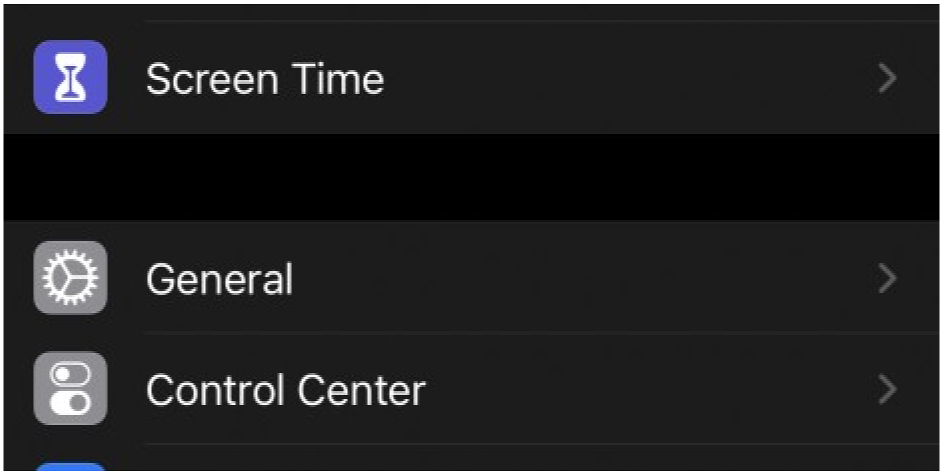
1. Enter your phone’s password



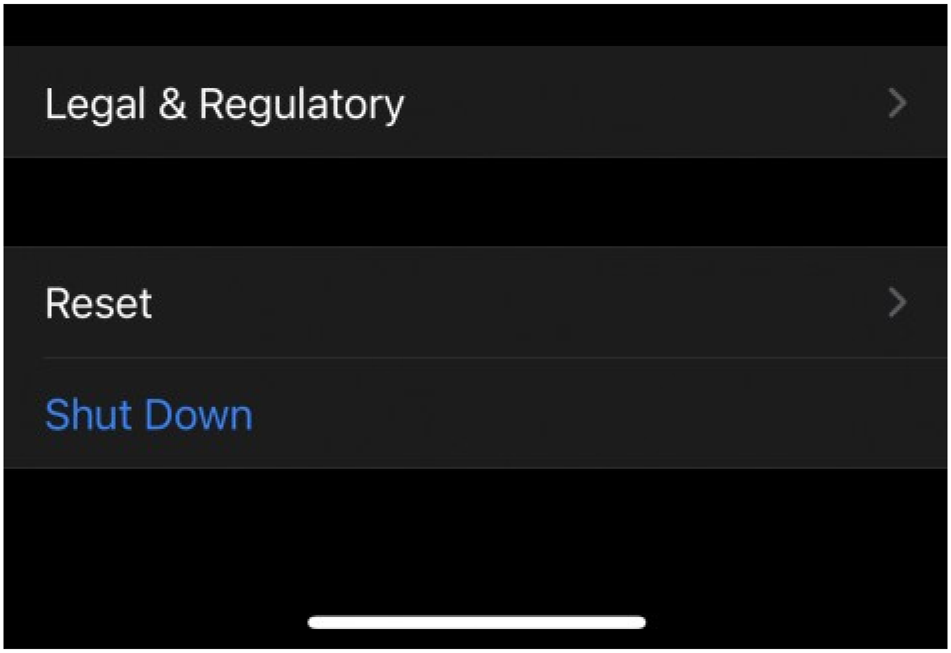
2. Open the “Settings” app



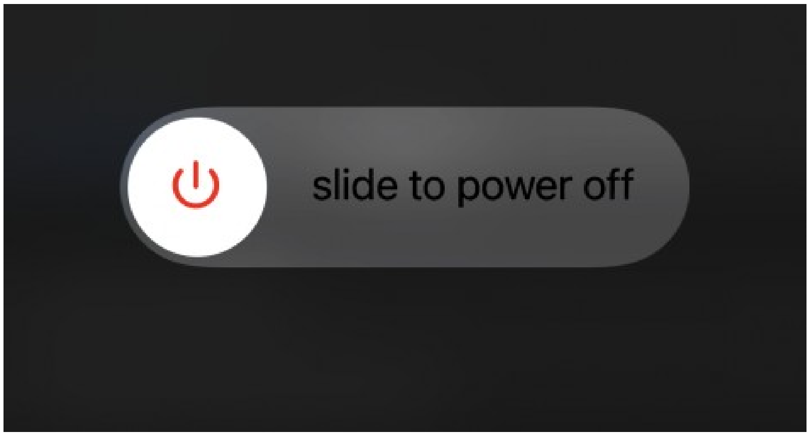
3. Select the “General” menu item



4. Scroll to the bottom of the menu and press “Shut Down”



5. Slide the power button on the screen to the right

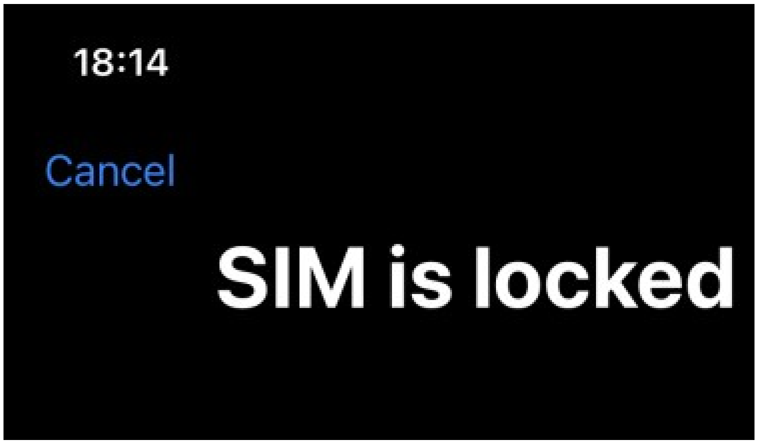


6. Hold the physical power button on the side of your phone until the logo appears

   Note: you should see a message indicating the SIM card is locked when the IPhone fully boots.

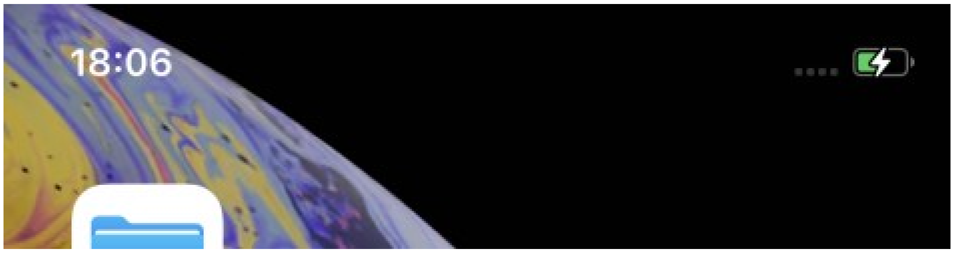
7. Enter your Phone’s password

8. Do Not Enter the SIM PIN: Select “Cancel” in the upper left corner of the screen



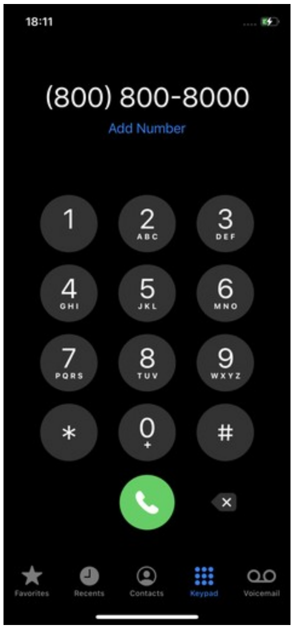
SIM is locked

9. Observe: you should seefour grey dots where the cellular signal strength indicator usually resides.



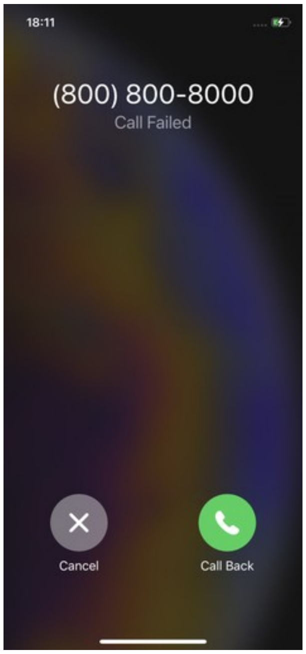
Limitation when the SIM is locked

1. When attempting to place a call the SIM Unlock screen appears. If the SIM PIN is not entered the call will fail. The cellular device can not use cellular signal for phone calls.



18:11

(800) 800-8000



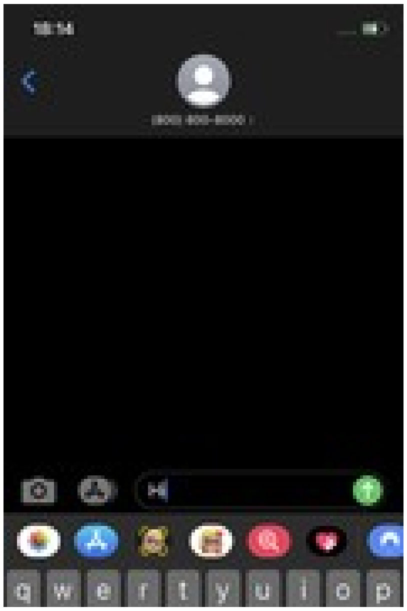
18:11

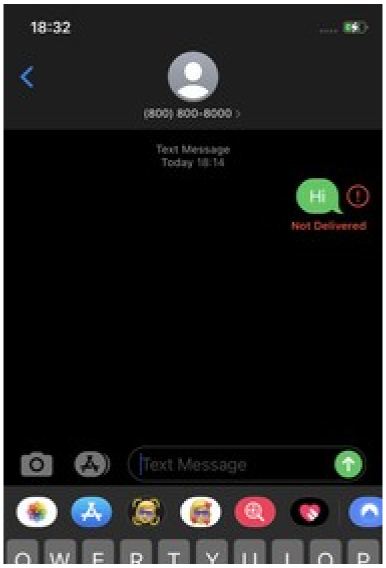
(800) 800-8000

Call Failed

2. All Apps that require cellular signal will be unable to establish a connection and shoulld present some form of error message.

3. Any text messages that are destined to the phone or sent from the phone will fail and any attempt to send a message will present the user with the SIM Unlock screen.





Text Message
Today 18:14

Hi

Not Delivered

4. While the SIM is locked the user has full access to all files saved on the device as well as the ability to remove (delete) apps. This can be useful in the event the user is trying to locate specific evidentiary artifacts, remove trojaned or malicious software, and/or reset certain configuration settings while preventing data from escaping the device through cellular signals.

Conclusions

While it can be standard practice to remove a SIM card during an investigation that technique is becoming far more complicated as manufacturers “seal” their cases or limit access to the SIM by placing it in a difficult to extract location. Using a SIM PIN is a quick and (possibly) efficient way to create a cellular firewall on a device that prohibits all trafic even on devices that have been substantially compromised. Locking the SIM is not a omni-signal firewall and other techniques must be used in conjuction to prevent remote communication over other wireless (or wired) signals such as BlueTooth, NFC, and WiFi; however, this technique does permit quick and effective IR capabilites such as ressetting configurations and removing unauthorized or malicious apps. When conducting any search of a cellular device or investigation of a potential incident always consult the legal department and the currently accepted standard practices and procedures to ensure compliance with any governing entities.

Thanks for reading
-Andrew