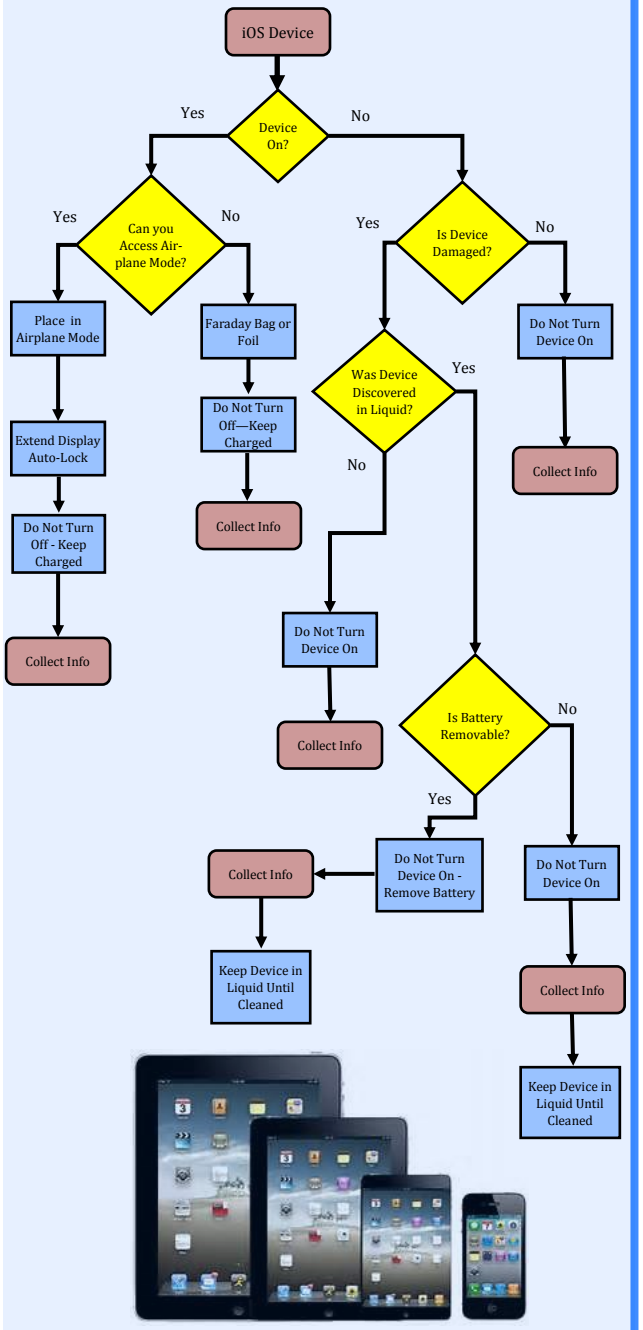
iOS Flowchart



* Collect Info = Model #, iOS Version and/or Mobile Carrier, etc.

The information contained within this brochure has been produced through review of several documents including: SWGDE Best Practices for Mobile Phone Forensics V2-0; NIST Guidelines – Mobile Device Forensics 800-101 May 2014; SWGDE Best Practices for Collection of Damaged Mobile Devices V1-1, as well as coordination with the FBI's Operational Technology Division (OTD), Digital Forensic Analysis Section (DFAS).

Things to Remember

- Follow your agencies Digital Evidence Procedures.
- Ensure you have appropriate Legal Authority.
- Once locked, or turned off, a device may become inaccessible.
- If unsure or uncomfortable handling a mobile device, contact your digital forensic personnel for assistance at:

- Secure and seize secondary devices, i.e., computers, laptops, etc. that device may be syncing or paired with along with charging cables.
- A Faraday Bag or foil is not foolproof and plugging a charging cable into a power source outside the Faraday Bag acts as an antenna unless the Faraday Bag is equipped with a shielded power/USB line.

National Domestic Communications Assistance Center

Technical Resource Group (TRG)
(855) 306-3222

Version #: 1.0

National Domestic Communications Assistance Center

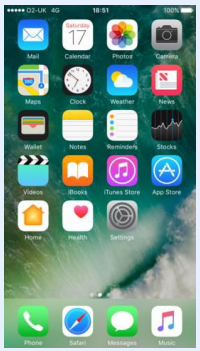
Best Practices for the Collection / Seizure of Mobile Devices for Investigators

This brochure provides Investigators and First Responders with best practices for the preservation of digital evidence when seizing Android and iOS mobile devices.

Summary

The purpose of this document is to provide a basic overview of the best practices for preserving evidence when seizing particular types of mobile devices. This document is not meant to be all encompassing. Specific extenuating circumstances may warrant a deviation from the procedures outlined herein. In most circumstances subjects should never be allowed to handle a device or be provided access to any evidence. Many mobile devices have factory reset codes that clear the contents of the device to original factory conditions. Factory resets may be performed remotely requiring proper precautions such as network isolation to ensure that evidence is not modified or destroyed.

iOS



iOS 10 running on an iPhone 7.

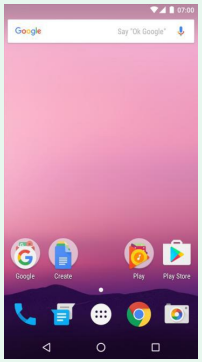
iOS is a mobile operating system created and developed by Apple Inc. exclusively for its mobile hardware, including the iPhone, iPad, and iPod Touch. The following steps should be taken to preserve evidence on an iOS device.

If the device is powered on, it may contain volatile encryption keys and should not be turned off. A power source should be connected as soon as possible to prevent the device from losing power. Be sure to seize the charging cable to keep power to the device.
You may also be able to adjust the Display Auto-Lock feature to extend the length of time before Auto-Lock is enabled.

Place the device in "Airplane Mode" (by swiping up from the bottom and selecting airplane mode) and verify that WiFi and Bluetooth are off. If you cannot put the device in "Airplane Mode", place device in a Faraday Bag or double wrap in aluminum foil to keep signals from potentially altering the device. Keep device charging if at all possible.

If the device is already off, and is not damaged, then do not turn it back on. If the device is submerged in liquid, or had liquid damage, remove it from the liquid only if you feel you can remove the battery (normally not possible with Apple products). Once the battery is removed, place the device back in the liquid. Collect basic information about the device including Model #, iOS Version and/or Mobile Carrier.

Android



Android 7.0 Nougat

Android is a Linux based mobile operating system developed by Google Inc. and has the largest install base of any mobile operating system. Unlike iOS, Android is available on devices manufactured by numerous companies and available in many different versions.

If the device is powered on, it may contain volatile encryption keys and should not be turned off. A power source should be connected as soon as possible to avoid the device losing power. Be sure to seize the charging cable to keep power to the device.

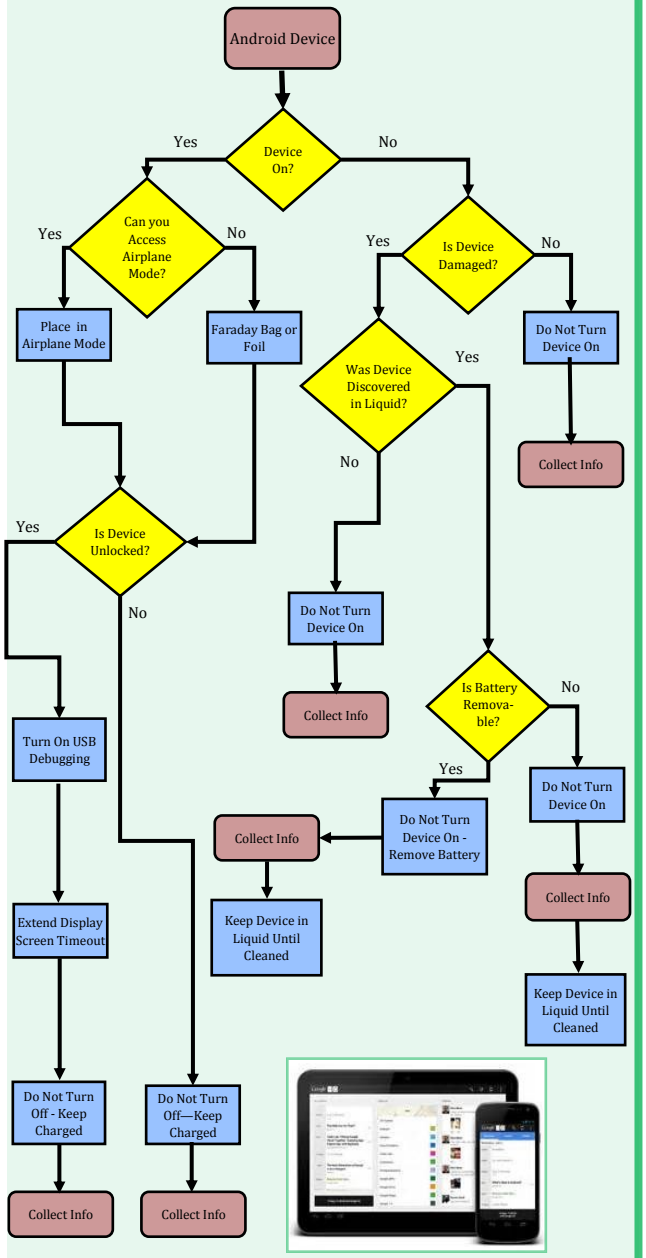
Place the device in "Airplane Mode" and verify that WiFi and Bluetooth are off. If you cannot put the device in "Airplane Mode", place device in a Faraday Bag or double wrap in aluminum foil to keep signals from potentially altering the device. Keep device charging if at all possible.

In order to give the best chance of accessing the evidence at a later date, if the device is unlocked, then turn on USB debugging if possible.
In Android versions 2.0 to 2.3, USB debugging is turned on by accessing the settings, under the "Applications". Within the "Development" menus there is an option to turn USB debugging on.
For versions 3.0 to 4.1, go to the settings menu and under "Developer options" there is be an option to turn it on.
In Android version 4.2 and above, the developer options screen is hidden. In order to turn on USB debugging go into the settings menu, and go to the "About phone" or "About tablet" menu where there should be a field showing the Android "build number". If the android build number is tapped seven times, developer mode is enabled and the "Developer options" menu will appear above the "About phone" menu. From there, USB debugging can be turned on.

You may also be able to adjust the Display Screen Timeout feature to extend the length of time before Auto-Lock is enabled.

If the device is already off and not damaged, do not turn it back on. If the device is submerged in liquid, or had liquid damage, remove it from the liquid only if you feel you can remove the battery (normally possible with Android devices). Once the battery is removed, place the device back in the liquid. Collect basic information about the device including Model #, Android OS Version and/or Mobile Carrier.

Android Flowchart



* Collect Info = Model #, Android OS Version and/or Mobile Carrier, etc.