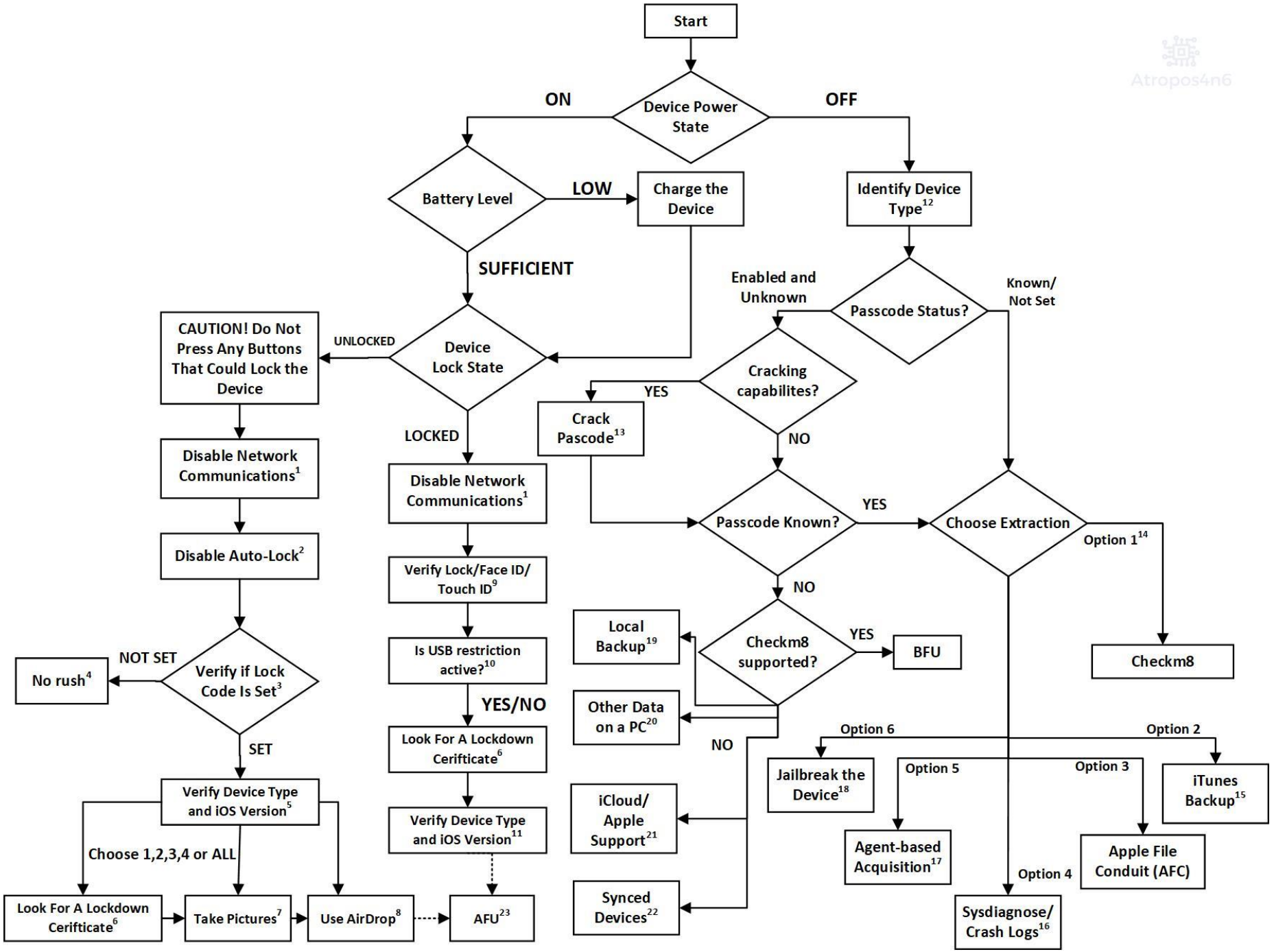
Atropos4n6

iOS Acquisition Guide



Atropos4n6

Introduction

This guide was created by atropos4n6 (https://www.atropos4n6.com/). It is solely based on the work, research and insights provided by Mattia Epifani (@mattiaep). Mr. Epifani generously shared all of these tips and tricks with the DFIR community at his latest public talk (the talk took place at the BelkaDay 2021 Event (https://belkasoft.com/forms/belkaday_europe_2021).

This guide was created in order to help DFIR practitioners, LEA officers and researchers to choose which is the best way to go when acquisition of an iOS device is needed. Be safe and keep forensicating.

DISCLAIMER Notice

The creation of this guide was not sponsored by any forensic software company or any other third-party entity. Mattia Epifani is a well-known both independent and tool-agnostic researcher. Atropos4n6 is also a tool-agnostic researcher. Both Mr. Epifani and atropos4n6 do not have any personal or any kind of profit out of it.

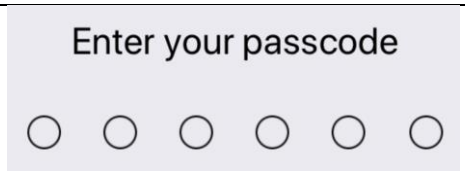
By sharing this guide, an effort is being made to help DFIR community and contribute back to it. Any reference to a particular forensic software or utility (either commercial or open-source) is made for demonstration purposes only and by no means does it suggest any software preferences of either Mr. Epifani or atropos4n6. Thank you.

For which iOS Devices is this Guide valid?

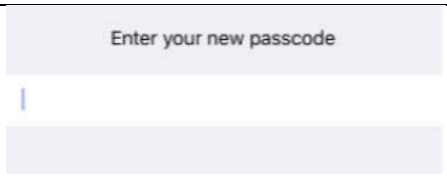
This guide is valid for devices starting from iPhone 4S up to the latest (March 2021).

Guide Sidenotes

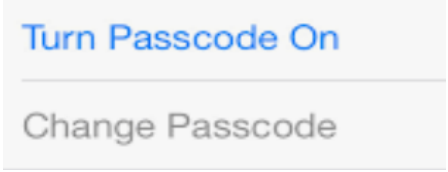
1: Enable Airplane Mode and disable WiFi, Mobile Data and Bluetooth. These settings can be unreachable if the device is locked (if the device is locked, scroll down the lock screen to check if you have access to these settings).
2: Navigate to *Settings-> Display & Brightness-> Auto-Lock-> Never*.
3: Navigate to *Settings->Face ID & Passcode*. If the options of the following Pictures 1 or 2 appear, this indicates that a passcode is set. If option of Picture 3 appears, this indicates that a passcode is not set.



Picture 1



Picture 2

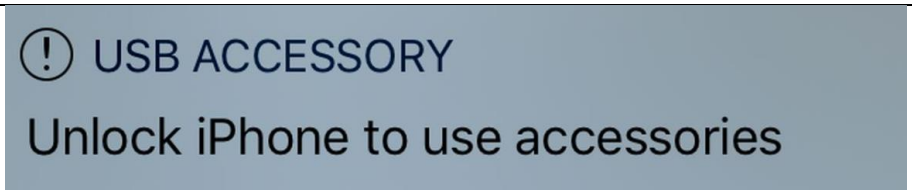


Picture 3

4: Since no passcode is set you can power off the device safely and acquire its data at your lab or you can acquire its data on the spot. Your call.
5: This will help you determine your acquisition options (checkm8, etc.). At this phase you cannot create a pair with a PC, as this requires the passcode. So, you cannot create the pairing and cannot acquire the device yet!
6: If another PC or Mac is found on the scene which is powered on, you can search for its latest lockdown certificate, as this file could **potentially** (under certain conditions) allow you to pair your workstation with the device and acquire/backup it.
The lockdown certificate's filename is ***Device_UDID.plist***
Lockdown Certificate's Path:
Windows: *C:\Program Data\Apple\Lockdown* Win 7/8/10
Mac: */private/var/db/lockdown* Mac OS X
Limitations:
-Lockdown certificate can be expired
-**Lockdown certificate cannot be used:**

- **in freshly/ restarted device (BFU status)**
- **after some hours since the last time the user unlocked the device with the passcode**

If you found a valid lockdown certificate you may try and use it with the forensic software of choice (if it supports such a function). This way you can make an iTunes Backup of the device. Be aware that if you do not choose to encrypt the iTunes backup with a password, then some of the device data will be left out of it (e.g. health data).
7: Take as many pictures of the screen as possible, by browsing through the various applications.
8: This method is a risky one. It is risky as it requires to enable some communications of the device (WiFi). You need to enable WiFi on the device and connect it to a WiFi AP that you control and is **NOT** connected to the Internet. So, what you should do is to connect both the device and your PC (e.g. Macbook) to the AP and then you may be able to transfer files from the device to your PC, without neither the need of "pairing" nor the passcode. This way you can potentially transfer media from the device (manually).
9: If Face ID or Touch ID are set, maybe you can ask the suspect to unlock the device (jurisdiction dependent action). Be careful not to bruteforce the password, as after a number of wrong attempts it will return to BFU state.
10: If you connect the device to a PC or/and you see the following message (Picture 4) on the lock screen, then USB restriction is active.



Picture 4

11: If USB Restriction is not active, then even if the device is locked, you can use forensic software of choice (e.g. ideviceinfo) and retrieve some basic information about the phone. This will help you determine your acquisition options (checkm8, etc).
12: Either in the SIM tray or the back of the device (depending on the model), IMEI and device model can be found and will help you identify the device type and possibly determine your acquisition options (checkm8, etc.).
13: If you have access to such software services (e.g. like those provided by GrayKey Grayshift, Cellebrite CAS/Premium, Elcomsoft iOS Forensic Toolkit and more) you can use these services to obtain the passcode of the device.

14: The options listed start from the less intrusive (checkm8) to the most intrusive (Jailbreak). You can choose one or more. Be aware of each option's pros and cons.
15: Be aware that if you do not choose to encrypt the iTunes backup with a password, then some of the device data will be left out of it (e.g. health data).
16: This option will allow you to find traces of the installed applications. You will not find user data using this option, but will gain insights into the applications of the device. Firstly, you should generate the Sysdiagnose logs and afterwards you can proceed with generating the Crash Logs. More info on this can be found at https://www.for585.com/sysdiagnose and https://github.com/cheeky4n6monkey/iOS_sysdiagnose_forensic_scripts .
17: Agent-based acquisition is currently not supported by all forensic software solutions. Be sure to check if the software you use, support such an acquisition. If it does, you will also need an Apple developer's account (https://developer.apple.com/programs/whats-included/). Basically, what you do is to install an application on the device (a.k.a. *Agent*) which is singed with your account's credentials (Apple ID & Password). If you hold an enterprise account then you do not have to connect the device to the Internet. But you still have to connect the computer where the device is attached to the Internet. If you do not own an enterprise account, it is still possible but you will need to connect the device itself to the Internet (create and connect to an AP where only connections to apple services are permitted). This method is dependent to the iOS version, but not dependent to the hardware (a.k.a. device model) of the device. Using this method, you may still obtain a full file system acquisition even if checkm8 is not supported!
18: This is the most intrusive method of all. But if it is your only choice, you may have to consider it. If you are a LEA officer consider you legal jurisdictions. Jailbreak software can be found on the Internet (e.g. https://unc0ver.dev/).
19: If another PC or Mac is found on the scene, maybe you are able to locate Local Backups. The paths where you should look for local backups are shown below:
Windows:

- *Users*\<*username*>*AppData**Roaming**MobileSync**Backup*
- \Users\<*username*>*Apple**MobileSync**Backup*

Mac:

- */Users/<username>/Library/Application Support/MobileSync/Backup*

20: If another PC or Mac is found on the scene, maybe you are able to locate other kind of data (e.g. crash logs). For example, if in Windows, search under *C:\Program Data\AppleComputer/iTunes/* for the file *"iPodDevices.xml".* This file will typically be a list of devices that have been connected to that PC.
21: You can try to locate iCloud credentials to perform a cloud-based acquisition. Also, if you are a LEA officer you can contact Apple for Apple Support.
22: Try to locate other Apple devices that may have been synced with the user data. In an Apple ecosystem, a user may have a Mac, an Apple TV, an Apple smartwatch etc. and these devices may hold some valuable user data like Media files, contacts, messages and more. For example, an Apple TV may hold the user's iCloud credentials with which you can either perform a cloud-based acquisition or opt for Apple Support.
23: If the device is in AFU (After First Unlock) State, there is still a possibility that some of the forensic software solutions support the device's acquisition, e.g. via exploiting vulnerabilities (based on their research). As this option is under research, this is why different arrows were used. You should contact your forensic solution's support team to find out.
Some resources that may help with the analysis of the device:

- https://digital-forensics.sans.org/media/DFIR_FOR585_Digital_Poster.pdf
- https://www.sans.org/security-resources/posters/dfir/ios-third-party-apps-forensics-reference-guide-poster-300

Follow Mattia Epifani for more on iOS:
@mattiaep
https://www.realitynet.it/en/