iOS Extractions Cellebrite UFED

Cellebrite's data extraction processes

August 2018

Legal notices

This manual is delivered subject to the following conditions and restrictions:

- This manual contains proprietary information belonging to Cellebrite Mobile Synchronization Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the iOS extractions.
- No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

1. UFED iOS extraction

1.1. Logical extraction:

During Logical extraction UFED performs extraction according to the following:

Data Type	Method	Source
Call logs	AFC -> iTunes Backup fall back	CallHistory.storedata com.apple.imservice.iMessage.plist com.apple.imservice.SMS.plist
Messages	AFC -> iTunes Backup fall back	sms.db com.apple.imservice.iMessage.plist com.apple.imservice.SMS.plist
Phonebook	AFC -> iTunes Backup fall back	AddressBook.sqlitedb AddressBookImages.sqlitedb
Calendar	AFC -> iTunes Backup fall back	Calendar.sqlitedb NoteStore.sqlite /var/mobile/Containers/Shared/AppGroup/*/Media/*/Image.jpeg /var/mobile/Containers/Shared/AppGroup/*/Media/*/IMG_????.JPG /var/mobile/Containers/Shared/AppGroup/*/Media/*/*.MOV /var/mobile/Containers/Shared/AppGroup/*/Previews/*-1-2048x1536.png
Images	AFC Only	
Video	AFC Only	
Audio	AFC Only	
Browsing Data	AFC -> iTunes Backup fall back	/Safari
IM	AFC -> iTunes Backup fall back	
Emails	AFC -> iTunes Backup fall back	
Apps Data	iTunes backup + House	*/Application/* */Applications/* */Application Support/*

	arrest (up-to iOS 8) using Whitelist	*/Containers/Shared/AppGroup/* */SafeHarbor/* */Manifest.mbdb */Manifest.db */Manifest.plist

1.2. File System

UFED identifies if the device is encryption state (Encrypted or not) and iOS version.

Following File system extraction options are available:

1. **Full** – UFED performs AFC2, AFC, iTunes backup, file relay & house arrest (iOS 8 and below). in the same extractions. UFED tries to reduce duplications in the process.
2. **Backup** – UFED performs full iTunes backup with no whitelist.
3. **Data files** – UFED performs AFC2, AFC, file relay & house arrest (iOS 8 and below). If one of the three can't run it will skip it.
4. **Jailbreak** – If UFED identifies the device is Jailbroken it attempts to perform Full File system using AFC2.

2. Physical Analyzer iOS extraction

2.1. Physical Analyzer extraction methods

Physical Analyzer has three methods for file system:

1. **Method 1** – iTunes backup with no whitelist.
2. **Method 2** – AFC, file relay & house arrest (iOS 8 and below)
3. **Method 3** – Jailbroken devices, AFC2, attempts full file system

3. Physical Analyzer iOS extraction

The below table summarize the extraction methods in Cellebrite products

#	UFED	Physical Analyzer
1	Logical	No comparable method
2	FS Backup	Method 1
3	FS Data Files	Method 2
4	FS Full	No comparable method
5	Jailbreak (automatic)	Method 3

4. Terms

1. **AFC** – Apple file conduit, file transfer protocol between the device and computer. It allows transfer of specific data files (jailed).
2. **AFC2** – Apple file conduit 2, additional services like the above that gives accesses to the entire file system, this is available only in Jailbroken devices.
3. **File relay** – service that may provide data such as Bluetooth, accounts and others.
4. **House arrest** – service that provide accesses to App store applications folders and content (iOS 8 and below)
5. **Jailbreak** – state that allow the user full access and write permissions on the device. This can be done using external tools.

5. Annex A - UFED and Physical Analyzer extractions

5.1. UFED iOS extraction types

Figure 1 iPhone 5c Extraction types

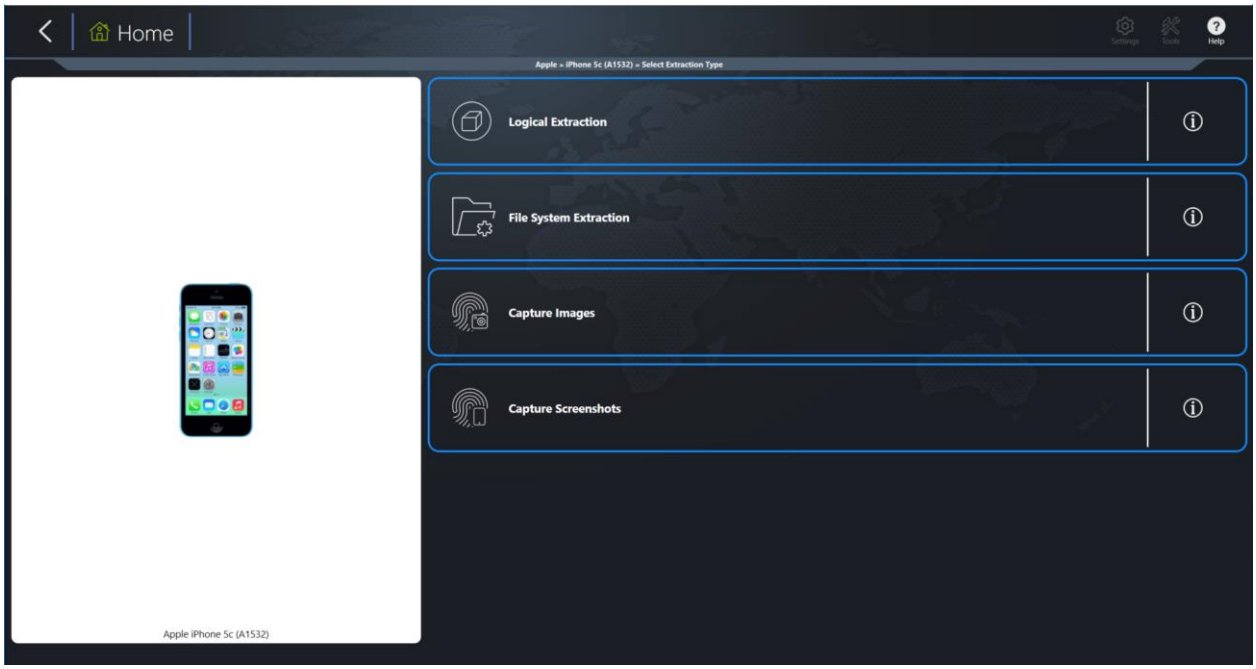
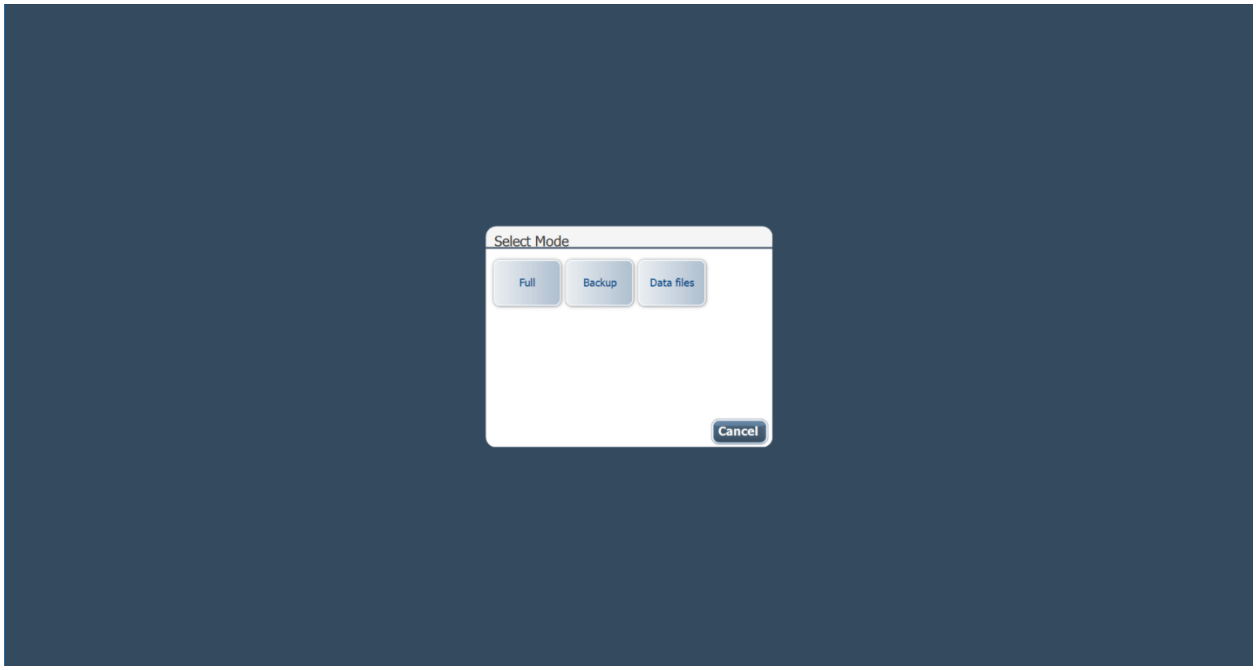


Figure 2 File system extraction options



5.2. Physical Analyzer extraction types

Figure 3 Physical analyzer iOS extractions

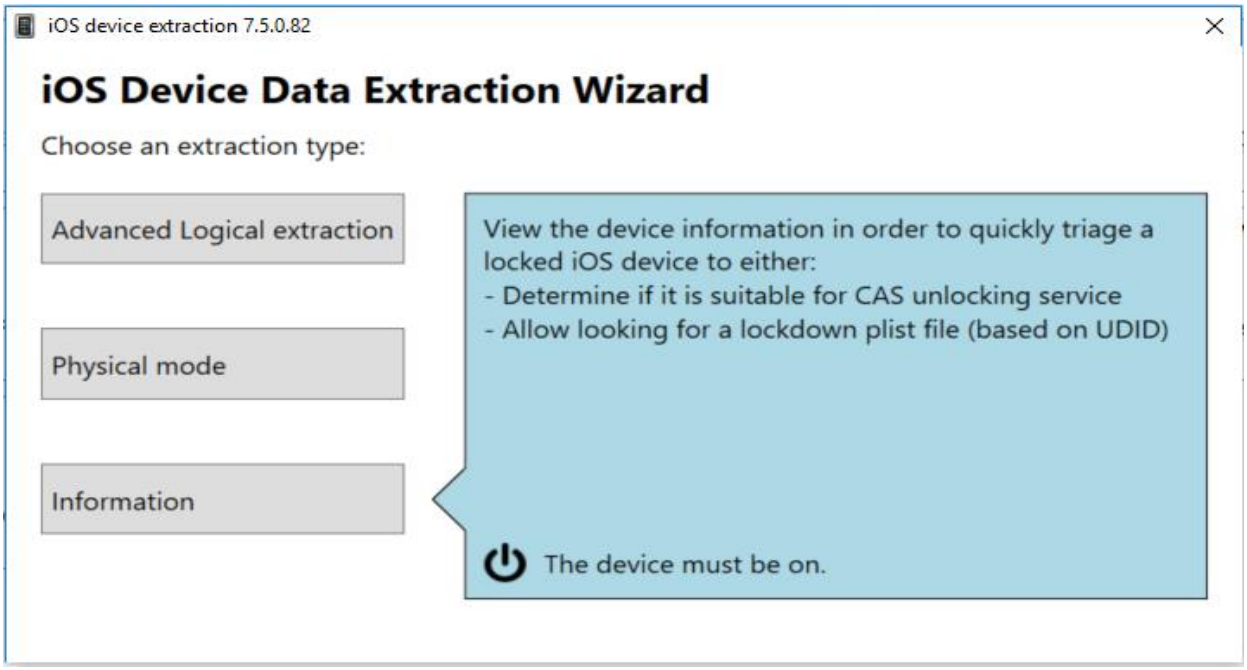


Figure 4 iOS methods