

UFED July 2023 Version 7.66



## Contents

1. What's new?	2
1.1. Cellebrite YouTube video channel	2
2. Introduction	10
2.1. Overview	10
2.2. System requirements	11
2.3. Extraction types	12
2.4. Accessories	13
2.4.1. Cellebrite UFED Device Adapter with USB 3.0	14
2.4.2. Multi SIM Adapter	16
2.4.3. Using cables and tips	17
2.5. Supported devices	17
2.6. Cellebrite YouTube channel	18
3. Getting started	19
3.1. Installing Cellebrite UFED	20
3.2. View Release Notes in-application	23
3.3. Activating the license	25
3.3.1. Licensing procedure	26
3.3.2. Using a dongle license	32
3.3.3. Using a software license	36
3.3.4. Using a network dongle	39
3.3.5. Online activation of new license from Loader	40
3.3.6. Update software license with one click	41
3.4. Working with UFED	42
3.4.1. Starting the application	42

3.4.2. Home screen	43
3.4.3. Autodetecting a device	
3.4.4. Searching for a device	
3.4.5. Case details	51
3.4.6. Investigation notes	51
3.4.7. User predefined filter	59
3.4.8. Manual selection	61
3.4.9. Application taskbar	
3.4.10. Creating a Support ticket	
3. Smart flow	66
3.5. Android Live consent-based collection	72
4. Password extraction	74
4.1. Extracting the user lock	74
4.1.1. The extracted passwords folder	
4.2. Disabling or re-enabling the user lock	
4.3. Removing the screen lock	79
5. Logical extraction	82
5.1. Advanced logical Android extraction	82
5.1.1. The extracted data folder	88
5.2. Advanced logical iOS extraction	89
5.2.1. Encrypted iTunes backup	92
5.3. Logical (Partial)	
5.4. Logical extraction via Bluetooth	96
5.5. Faster transfer and verification of logical collection output	100
5.5.1. Enabling the zip feature	100
6. File system extractions	102

6.1. Performing a FULL file system extraction	102
6.1.1. iOS: Animated DFU instructions	
6.1.2. The file system extraction folder	106
6.1.3. Unlocked Huawei Kirin devices	106
6.1.4. smartStopping an extraction	107
6.2. Performing a SELECTIVE file extraction	110
6.2.1. To extract data using Selective file system extraction:	
6.2.2. Enhanced selective extraction	
6.2.3. Selective extraction by file (Android / iOS)	112
6.3. Android backup	117
6.3.1. Extracted apps	121
6.4. Android backup APK downgrade	122
6.4.1. Installing the latest APK version	
7. Physical extraction	128
7. Physical extraction      7.1. Performing a physical extraction	
7. Physical extraction         7.1. Performing a physical extraction         7.1.1. The Physical extraction folder	
7. Physical extraction         7.1. Performing a physical extraction         7.1.1. The Physical extraction folder         7.2. ADB rooted	
7. Physical extraction         7.1. Performing a physical extraction         7.1.1. The Physical extraction folder         7.2. ADB rooted         7.3. Advanced ADB	
7. Physical extraction         7.1. Performing a physical extraction         7.1.1. The Physical extraction folder         7.2. ADB rooted         7.3. Advanced ADB         7.3.1. Generic model	
7. Physical extraction         7.1. Performing a physical extraction         7.1.1. The Physical extraction folder         7.2. ADB rooted         7.3. Advanced ADB         7.3.1. Generic model         7.3.2. Errors and notifications	
7. Physical extraction         7.1. Performing a physical extraction         7.1.1. The Physical extraction folder         7.2. ADB rooted         7.3. Advanced ADB         7.3.1. Generic model         7.3.2. Errors and notifications         7.4. Boot loader (FW flashing)	
<ul> <li>7. Physical extraction</li></ul>	
7. Physical extraction         7.1. Performing a physical extraction         7.1.1. The Physical extraction folder         7.2. ADB rooted         7.3. Advanced ADB         7.3.1. Generic model         7.3.2. Errors and notifications         7.4. Boot loader (FW flashing)         7.5. Decrypting boot loader         7.6. Forensic recovery partition	
7. Physical extraction	
7. Physical extraction         7.1. Performing a physical extraction         7.1.1. The Physical extraction folder         7.2. ADB rooted         7.3. Advanced ADB         7.3.1. Generic model         7.3.2. Errors and notifications         7.4. Boot loader (FW flashing)         7.5. Decrypting boot loader         7.6. Forensic recovery partition         7.7. Smart ADB         8. Extracting Android devices	

8.1.1. Android debugging bridge method	168
8.1.2. Bootloader extraction	
8.1.3. smartStopping an extraction	
8.2. Technical terms	172
9. Drone extractions	173
10. Capture images and screenshots	
10.1. The Cellebrite UFED camera	174
10.2. Capturing images	175
10.3. Capturing screenshots	
11. SIM card functionality	
11.1. SIM data extraction	
11.1.1. Performing SIM data extraction	
11.2. Clone SIM	184
11.2.1. Cloning an existing SIM card ID	185
11.2.2. Entering SIM data manually	191
11.2.3. Creating a GSM test SIM	195
12. Device tools	196
12.1. Activate TomTom trip log	198
12.2. Android Debug Console	
12.3. Bluetooth scan	200
12.4. Disable iTunes encryption password	
12.5. Exit Android recovery mode	201
12.6. Exit iOS recovery mode	202
12.7. Exit Motorola Bootloop	203
12.8. Exit Odin mode	
12.9. Flash Cable 500 Firmware	

	12.10. LG EDL recovery	204
	12.11. Nokia WP8 recovery tool	204
	12.12. Remove Android extraction files	205
	12.13. Samsung Exynos Recovery	205
	12.14. Switch to CDMA offline mode	206
	12.15. Uninstall Windows mobile client	207
13	3. Settings	208
	13.1. General settings	209
	13.1.1. Changing the application interface language	213
	13.1.2. Changing the extraction location	216
	13.2. Report settings	217
	13.2.1. Managing report fields	221
	13.3. System settings	223
	13.4. License settings	224
	13.4.1. License not found	225
	13.4.2. Updating a dongle license online	228
	13.4.3. Updating a software license online	230
	13.5. Version details	233
	13.5.1. Connect a Cellebrite UFED device to Cellebrite Commander	234
	13.5.2. Updates and versions	235
	13.5.3. Importing settings and configuration files	237
	13.6. Activity Log	242
	13.6.1. Exporting metadata to Cellebrite Commander	242
	13.7. Users permissions	244
	13.7.1. Active Directory integration	245
	13.7.2. Enabling Active Directory in Cellebrite UFED application	253

13.7.3. Permission management	_ 254
14. Special cables	260
14.1. Device power-up cable	_ 260
14.2. Active extension cable	. 261
14.3. USB extension cable	_ 261
14.4. USB cable for Cellebrite UFED Device Adapter V2 PowerUP	_ 262
15. Index	_ 263

# Legal notices

Copyright © 2023 Cellebrite DI Ltd. All rights reserved.

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

- This document contains proprietary information belonging to Cellebrite DI Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of Cellebrite UFED.
- 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 DI 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.

# 2. Introduction

Cellebrite UFED is a new generation solution that empowers law enforcement, military, intelligence, personnel to capture critical forensic evidence from Android and iOS mobile devices.

## 2.1. Overview

Cellebrite UFED is a new generation solution that empowers law enforcement, military, intelligence, personnel to capture critical forensic evidence from Android and iOS mobile devices.

Cellebrite UFED enables you to:

- Perform physical, file system, and logical extraction of device data and passwords.
   Capabilities may vary, based on the Cellebrite UFED product purchased Cellebrite UFED Logical or Cellebrite UFED Ultimate.
- \* Extract vital data such as call logs, phonebook entries, text messages (SMS), pictures, videos, audio files, locations, app data, ESN IMEI, ICCID and IMSI information and more, from a wide range of mobile devices.
- \* Extract data from the widest selection of operating systems, such as Apple iOS, Blackberry, Android, Symbian, Microsoft Mobile, and Palm OS. You can also extract data from feature phones and drones.
- Ione the SIM ID, which allows you to extract phone data while preventing the mobile device from connecting to the network. It can also help if the SIM card is missing.
- \* Extract the data from a mobile device either by a cable-based connection (serial or USB) or a Bluetooth wireless connection. The tips and cable kit consists of four master cables and various tips.

The extracted data can be saved and then generated in the form of clear and concise reports.

Cellebrite's industry-expertise provides reliability and ease-of-use, and ensures the broadest support for mobile devices, including updates for newly released models before they are available to the market.



This manual is also relevant for Cellebrite Responder users.

## 2.2. System requirements

ĒÌ)

PC	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher		
Operating system	Microsoft Windows 11, 64-bit: UFED & Responder require v.7.56 and higher Microsoft Windows 10, 64-bit		
Memory (RAM)	<b>Required</b> 32 GB	Minimum 8 GB	
Space requirements	1.5 GB of free disk space for installation		
Additional requirements	Microsoft .NET version 4.5 or higher		
Permissions	If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, you must have administrative rights over the computer.		

This specification is for a PC running both Cellebrite UFED and the Physical Analyzer application as the decoding operations of Physical Analyzer require the higher specification. For a standalone PC running Cellebrite UFED an ATOM-based chipset (or equivalent) is sufficient.

## 2.3. Extraction types

Cellebrite UFED includes a range of data extraction types.



The available extraction types and methods may vary between devices depending on their manufacturer, operating system, and chipset.

Extraction types available in Cellebrite UFED products

Extraction types	Cellebrite UFED Logical	Cellebrite UFED Ultimate
Logical / Advanced Logical Extraction	Yes	Yes
File System Extraction	Not available	Yes
Physical Extraction	Not available	Yes
Capture Images and Screenshots	Yes	Yes
Chat capture	Yes	Yes

Extraction type descriptions:

- \* Logical extraction: Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.
- \* **File system extraction**: Extracts files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.
- Physical extraction: Extracts a physical bit-for-bit image of the flash memory of a device, including the unallocated space using advanced methods. Unallocated space is the area of the flash memory that is no longer tracked by the file system, which may contain images, videos, files, and more.
- Capture images and screenshots: Take pictures or videos of a device using the Cellebrite UFED camera. You can also capture internal screenshots directly from the connected device.
- <sup>\*</sup> **Chat capture**: Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third-party application data (available for Android only).

ð

For more information about the extraction types that are available, see the Performing extractions data sheet.

## 2.4. Accessories

The Cellebrite UFED kit includes connection cables and tips. These are used to connect mobile devices to Cellebrite UFED.



Cellebrite UFED Cables and tips

The Cellebrite UFED Ultimate kit contains tips and cables for logical, file system, and physical extractions.

The Cellebrite UFED Logical kit contains tips and cables for Logical Extraction only.

## 2.4.1. Cellebrite UFED Device Adapter with USB 3.0

The Cellebrite UFED kit contains a device adapter that attaches to your PC's USB ports. Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition, there are LEDs for power and Bluetooth.

Depending on when you received your kit, there are two types of device adapters: Cellebrite UFED Device Adapter with USB 3.0 (latest version) and Cellebrite UFED Device Adapter with USB 2.0 (previous version). This document provides more information about the Cellebrite UFED Device Adapter with USB 3.0.







This device adapter has the following connectors:

- » GPIO port (for future use)
- \* USB 3.0 port
- \* RJ45 port
- \* DC In power supply (Input 5.3V 3.7A)
- \* 2 USB connection cables labeled POWER and DATA.

#### To connect the Cellebrite UFED Device Adapter with USB 3.0:

- 1. Connect the DATA cable to a USB port on the computer.
- 2. Then connect the POWER cable to a second USB port on the computer.



Use the following procedure, if the computer is mounted in a difficult to access or distant location.

# To connect the Cellebrite UFED Device Adapter with USB 3.0 using extension cables:

- 1. Connect the Active Extension cable<sup>1</sup> to the DATA connection cable.
- 2. Connect the other end of this extension cable to a USB port on the PC.
- 3. Connect a standard USB extension cable to the POWER connection cable.
- 4. Connect the other end of this extension cable to a USB port on the PC.



#### 2.4.1.0.1. Using the External power supply

The external power supply is NOT required for the smooth operation of the Cellebrite UFED Device Adapter V3, but is provided for those cases where additional power output is required. The external power supply provides an output of approximately 5.3V 2.7A.

#### 2.4.2. Multi SIM Adapter

A Multi SIM Adapter supports Micro, Nano and standard SIM cards.

We recommend that you connect the Multi SIM Adapter to an available USB port on your computer, not to the USB port on the Cellebrite UFED Device Adapter.



<sup>1</sup>This cable is 150 cm in length and allows for the easy and accessible placement of the UFED Device Adapter with USB 3.0.

## 2.4.3. Using cables and tips

The cables and tips include various adapter cables (the number of cables depends on the Cellebrite UFED product and kit purchased). Each cable has a letter and name. For example, A Adapter – USB.



Single cable

For easy recognition, the tips are color coded and numbered; the color represents the vendor.



*Cellebrite UFED tip (example)* 

Before each extraction, the required cable and tip number and color is specified in the **Source** area of the Select Content Types screen.

## 2.5. Supported devices

There are various electronic devices that Cellebrite UFED supports. These include:

- \* Mobile devices: Mobile devices such as phones and tablets are the most widely supported.
- \* SIM cards Extract SIM card data (logical extraction) or clone a SIM card.
- Mass storage: Extract data from SD cards, removable drives, modems, etc via logical, physical, or file system extractions.
- » Drones: Extract data from drones via physical orfile system extractions.

To find out more about devices that are supported in Cellebrite UFED and which data extraction capabilities are available for each, use one of the following:

- <sup>\*</sup> The Cellebrite UFED <version no> Supported Phone List file is delivered with every Cellebrite UFED software version update. The Microsoft Excel file contains two worksheets:
  - <sup>\*</sup> The **Cellebrite UFED Logical** sheet lists the mobile devices supported for logical extraction.
  - <sup>\*</sup> The **Cellebrite UFED Physical** sheet lists the mobile devices supported for physical, file system, and password extractions.
- " UFED Phone Detective (devices supported for logical extraction only).
- \* Cellebrite UFED Supported Devices document in MyCellebrite.

## 2.6. Cellebrite YouTube channel

For your convenience, a selection of useful videos demonstrating typical workflows and common procedures are available at <u>youtubAxon Evidence/cellebriteufed</u>.

# 3. Getting started

This section includes the following:

3.1. Installing Cellebrite UFED	20
3.2. View Release Notes in-application	23
3.3. Activating the license	25
3.4. Working with UFED	42

## 3.1. Installing Cellebrite UFED

#### To install Cellebrite UFED:

1. Start the Cellebrite UFED installation wizard. The following window appears.

饡 Cellebrite Setup		—		X
	Setup is loading			>
	<		>	~
	Destination folder	_		
	C:\Users\JONATH~1\AppData\Local\Temp\RarSFX0	~	Browse	
	Installation progress			
	Install		Cancel	

2. Click Install. The License Agreement window appears.

🕞 Setup - UFED 4PC —		×
License Agreement Please read the following important information before continuing.	¢	Cellebrite
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.		
IMPORTANT: PLEASE READ THIS END USER	^	
LICENSE AGREEMENT CAREFULLY.		
USING CELLEBRITE-SUPPLIED SOFTWARE (AS PART		
OF A PRODUCT OR STANDALONE) CONSTITUTES		
EXPRESS ACCEPTANCE OF THIS AGREEMENT.		
CELLEBRITE IS WILLING TO LICENSE SOFTWARE TO	2~	
● I accept the agreement		
○ I do not accept the agreement		
Next >	Can	cel

3. Select I accept the agreement, and click Next. The Select Destination Location window appears.

🔂 Setup - UFED 4PC				×
Select Destination Location Where should UFED 4PC be installed?				C Cellebrite
Setup will install UFED 4PC into the following folder.				
To continue, click Next. If you would like to select a different folder,	click	Brow	se.	
C:\Program Files (x86)\Cellebrite Mobile Synchronization\UFED 4PC		Brov	vse	
At least 2,235.6 MB of free disk space is required.				
< Back Next	t >		C	ancel

4. Select the folder where you want the application installed, and click **Next** to continue. The Select Additional Tasks window appears.

🔀 Setup - UFED 4PC			×
Select Additional Tasks Which additional tasks should be performed?		¢	Cellebrite
Select the additional tasks you would like Setup to perform while inst then dick Next.	alling UFI	ED 4PC,	
Create a desktop icon			
Run on startup			
< Back Nex	t >	Car	ncel

5. Select the additional tasks you want the install wizard to perform, and then click **Next**. The Ready to Install window appears.

🐻 Setup - UFED 4PC —		×
Ready to Install Setup is now ready to begin installing UFED 4PC on your computer.		Cellebrite
Click Install to continue with the installation, or click Back if you want to review change any settings.	N Or	
Destination location: C:\Program Files (x86)\Cellebrite Mobile Synchronization\UFED 4PC		^
Additional tasks: Create a desktop icon		
<	>	
< Back Install	C	ancel

6. Click Install. The following window appears.

🖑 Setup - UFED 4PC —		×
Android backup APK downgrade New APK for apps		Cellebrite
A new APK version is available for the following apps: Baidu, ChatON, Evernote, FireChat, Gmail/Inbox, Hangouts, Keep Safe (Ki Messenger, Ping Chat, QQ browser, QQ messenger, Signal Private Messer TextSecure, Tango, Text Free Ultra Texting, Text Me, TextNow, TextPlus, TigerText, Tinder, Viber, Vkontakte, Voxer, Whisper, Yandex Mail.	i Safe), Kik iger / Threema,	¢.
To download the APK, go to my.cellebrite.com > Downloads and search f under the product (UFED Touch2/UFED Touch/UFED 4PC/UFED InField) S section. Install via Settings > Version > File	or the APK oftware	C
	_	

 Click the APK Download link to go to <u>MyCellebrite</u> and search for and download the new APK under the Cellebrite UFED Software section. The new APK enables Android backup APK downgrade support for additional app versions.



Install the APK via **Settings** > **Version** > **File** after completing the Cellebrite UFED installation process.

8. Click Next. The following window appears.



9. Select Yes, restart the computer now, and click Finish to restart the computer.

You must now activate the license to use Cellebrite UFED. Proceed to <u>Activating the license (on page 25)</u>.

### 3.2. View Release Notes in-application

You can now review Release Notes from within the applications.

The release notes display automatically after the first launch of the installed application. In addition, you can find the release notes at any time by clicking as follows:



#### "?" > "Release Notes".

Cellebrite UFE	9.754.0.706		-	o x
	C Cellebrite   UFED			
			×	
	Improved serviceability, reduce logs size			
	You can new reduce the log size when opening a support ticket by sending only the last session logs.		11	
	Expert All: Exports logs for all sessions, including the current session.			
	Export last _ Exports all log from the last session (or the current session - whichever is session = 0 = 2 = 0 = 0			
	< 5/9 >			
	Version 7.54.0.106 () 3:23:05 PM	] 3/22/	2022	

## 3.3. Activating the license

Activate Cellebrite UFED in one of the following ways:

- \* Using a dongle license (on page 32)
- \* Using a software license (on page 36)
- \* Using a network dongle (on page 39)
- \* Using an online license
- \* Online activation of new License from loader

Ð

ÊÌ

Check your Cellebrite UFED kit to verify the method to use.

If you are using Cellebrite UFED for the first time or a license is not found, see License not found (on page 225).

#### 3.3.1. Licensing procedure

Manage licenses for your Cellebrite deployment with Cellebrite Commander. License management via Cellebrite Commander is supported for the following:

- <sup>\*</sup> Cellebrite Physical Analyzer (PA),
- <sup>\*</sup> Cellebrite Logical Analyzer (LA)
- <sup>\*</sup> Cellebrite Responder
- <sup>\*</sup> Cellebrite UFED
- <sup>°</sup> Cellebrite UFED Touch

The following process must be performed for <u>each</u> UFED unit in order to upload a new or renewal license via Commander.

- 1. Connect the UFED unit to Commander. Connecting a device to Commander
- 2. Launch the Commander screen selection.
  - a. Select I'm using Commander.

Cellebrite UFED 7.58.0.93		 - 🗆 ×
Cellebrite product lic	ense	
A license for this product was r Are you using Cellebrite Comm	not found. ander?	
l'm using Commander	I'm not using Commander	
Learn more about Cellebrite Co	bmmander	~
? Help \ Sales		Close

- b. Choose the license type you are using.
- c. When using a dongle, choose **Dongle**.(When more than one dongle is attached to the UFED there is a drop-down list of dongles.

Choose the dongle containing the device license from the drop-down list.)

Cellebrite UFED 7.58.0.93		-	
Cellebrite product license			
Connect to your Cellebrite Commander server			~
	▼ 🖍	CONNECT	
Use Specific Dongle 321454807 Vour display name in Cellebrite Commander: (opt	tional)		
-			$\sim$
③ Help	Back	Close	

#### 3. UFED will

- a. Display No license (for that UFED device) in the dialog.
- b. Automatically upload a C2V of the device's Dongle ID to Commander.
- c. Query Commander for a license until the Commander admin loads a valid license to the UFED device/dongle.

#### 4. **Commander** will:

a. Enter the state "waiting\_for\_admin".

Devices													
District Select district	- Station		-										
Quick serial search													
						Export C2V   B	View and	modify   / Charg	je device as	isignment   🗑 Delete	- at 1	mport devices & lice	enses
Device type	Ŧ	Serial number	Ŧ	Туре	Ŧ	Name	Ŧ	Code	Ŧ	Activation status	Ŧ	From	3
Device		1234		Not assigned		Not assigned		Not assigned		License applied			
Dongle		534025752		Not assigned		Not assigned		Not assigned		License waiting for admin			
Device		7056054		Not assigned		Not assigned		Not assigned		License applied			

5. When you have done the steps above for all unlicensed devices, go to Commander and click **Export** devices & C2V

This sends the C2Vs of all the devices to your account in MyCommunity.

6. Log in to Cellebrite's MyCommunity.

#### 7. Go to **Products & Licenses**.

<i>My</i> Cellebrite	HOME PRODUCTS & LICENSES	SUPPORT ADVANCED SERVICES STORE MORE
♦ Products & Licenses		٩
Products Licenses Try our products Wallets	Q. Search for serial	+ Start a trial + Register Device
Update your products with latest versions and add-on	s. Cellebrite Commander	Cellebrite License Tools
Downland latest version Tapdated 24 May 221	Dewritoed latest version (updated 31 Aug 22)	Download latest version lapdeted 21 Nov 211
Cellebrite Physical Analyzer See Licenses	Cellobrite Physical Analyzer Ultra See Licenses	Cellebrite Premium-as-a-Service See Licenses
Downland latest version lupdated 28 Sept 221	Download latest version (updated 05 Jul 22)	Download latest version lupdated 07 Sept

- 8. Select Cellebrite Commander.
  - a. Click the down arrow in the Cellebrite Commander product selection box.
     Note: You must have already purchased a Commander license for this option to be available.



#### 9. Click Download managed licenses.

Cellebrite Commander Downloa	ads	( Download managed licenses )
		🗄 Download latest generated CMS
7.24 7.23 7.21.2		
Released: 31/08/22		
What's new in Cellebrite Commander Version 7.24 • Complex dongle support to upgrade license distrit • Commander is integrated with User Management • UFED permissions settings have been updated with	ution for managed endpoints. Server v 9.0.4. h additional extraction options in role (	definitions
✓ Software Version		
31/08/22 Cellebrite Commander - 7.24 - Installation TAR	Version hash: MDS- d5b54b847aee27e793701f85	🕹 Download
	<b>SHA256</b> - ff4af570316014caea92e2dbebcd3b 848c1c13f7a0b92af8f	od8811809271773a
31/08/22 Cellebrite Commander - 7.24 - Installation ZIP	Version hash: MD5- 0c61f5d8e09917494ed6a42e	📩 Download
	<b>SHA256</b> - 8505e9bb97a442a0a939df548b69a 052dea55e1a186cfd48	#2a19470f88af11d

10. Select the serial numbers of all of the devices to be managed by this Commander.

#### 11. Click **Download**.

A zip file containing licenses for all the devices checked above is downloaded to your computer.

Manage	ed Licenses Downloads	
C, Search	n	
	Serial Number	Product Labels
	7206060	Cellebrite Commander for UFED Touch
	1273036809	Cellebrite Commander for UFED 4PC; Cellebrite Commander for Physical Analyzer
	473031921	Cellebrite Commander for UFED 4PC; Cellebrite Commander for Physical Analyzer
	1837593435	Cellebrite Commander for UFED 4PC; Cellebrite Commander for Physical Analyzer
	785010232	Cellebrite Commander for UFED 4PC; Cellebrite Commander for Physical Analyzer
		Download
Upl	oad your Zip file e	stracted from the commander
	Upload ZIP file	
	7.24[12899].zip	1
		Cancel Submit

12. In Commander:

#### a. Click Import devices & licenses.

			-		Help		mmander Admin -
A Dashboard	Devices						
B Product monitoring	District Select district - Station	Select station	×				
Software management >	Quick serial search					_	
Configurations	B	Export C2V   🖹 Vie	ew and modify   🧷 🤇	Change device assignm	ient   🏐 Delete 🕹 Import devi	ces & licenses Change st	atus 👻   All devices 👻
≣ SOPs >	Device type =	Serial n 💼	Туре 😨	Name 😨	Code = Activati	T From T	Status \Xi
≛t User management >	Dongle	091	District	155: arge	155 I argi	01/12/2021	Enabled
	PC Activation Code	0A:	Unit	26th District	26th	11/08/2022	Enabled
Devices	Dongle	101	District	Default District	911	29/11/2021	Enabled
X Offline management	Dongle	10:	District	zopa	123456	25/11/2021	Enabled
	Dongle	10:	Station	123456	963	02/12/2021	Enabled
	Dongle	10:	Not assigned	Not assigned	Not assigned		Enabled
Import devi	ices & licenses					_	×
Select File	s drop files her	e to uplo	ad				
						C	lose

#### 13. This message displays in **MyCellebrite**:



14. Select the license file that MyCellebrite downloaded to your computer and when the green check mark displays, click **Done**.



15. The devices are now licensed and managed by Commander.

## 3.3.2. Using a dongle license

Use the Cellebrite UFED dongle provided with your Cellebrite UFED kit. The dongle contains licenses for all the applications purchased.



#### To use Cellebrite UFED with a dongle:

- 1. Go to <u>community.cellebrite.com</u> and log in with your credentials (or create an account).
- 2. Go to **Products & Licenses > Register Device** and enter a name for the device, the serial number, and the Dongle ID as displayed on the dongle.

Register New Device	
* Device name	
UFED Dongle1	
* Serial number	
000000000	
* UFED/Dongle ID	
0000	
Cellebrite product license registration	
To start working with UER, registration of your UEB lonnes donge on MG elebrite is required (make sure you have an internet connection): 1. (Colo http://www.colebrite.com 2. (Create a new account or sign in using your existing account credentials. 1. Under tek My Photoschi tah registre your UEB donge. Dongle texis Copy 4. Download the license file and upload it by clicking the Copy Load license file Click Load licen. and upload the license.	
Testo	
	Next

3. Click **Next**. The following window appears.

Device Registration completed
Download license for device Serial number: 11to activate your product Download License
Register UFED Product / Dongle" Serial number " 121221220 Device/Dongle ID FB22 Figure figure f
Done Register Another Device

- 4. Click **Download License** from the Device Registration Completed window to download the license key (or click **See licenses** in the Products tab and then from the menu on the right select **Download license**).
- 5. Download and install the Cellebrite UFED application.
- 6. Start the Cellebrite UFED application and connect the dongle to a USB port on your computer. The following window appears.

Cellebrite product license
To start working with UFED, registration of your UFED license dongle on MyCellebrite is required (make sure you have an internet connection): 1. Go to <u>https://community.cellebrite.com</u> 2. Create a new account or sign in using your existing account credentials. 3. Under 'Products & licenses' tab, click 'Register device'. 4. Download the license file and upload it by clicking the "Load license file" link below.
Dongle serial: 8668 Copy Dongle ID: c1 Copy Dongle Type: Max
Load license file
③ Help  ☐ Sales

7. In the Cellebrite product license window, click **Load license file** and upload the license key.

Congratulations, your Cellebrite UFED application is now ready!

#### If a license dongle is not found:

1. When a license dongle is not found, the Cellebrite product license window appears.

<b>Cellebrite product</b> Select your license type:	license	
Dongle	Software	
⑦ Help 🕁 Sales		Close

2. Click **Dongle**. If you connected the dongle to a USB port on your computer, and it still does not work, contact <a href="mailto:support@cellebritAxonEvidence">support@cellebritAxonEvidence</a>.

You can now activate your Dongle or Software license online. Our "Cellebrite License Loader" application, which can be accessed by all users on the Cellebrite Community portal, now offers an activation process with an internet connection. To activate the license, install the License Loader on any computer and activate it with one click.

## 3.3.3. Using a software license

Use the PC activation code provided with your product kit to download a software license.



#### To use Cellebrite UFED with a software license:

1. Go to the required product link and sign in to your MyCellebrite account:

**Cellebrite UFED**: <u>community.cellebritAxon Evidence/ufed4pc</u>

(If you do not have an account, click **Register now** and create a user. Then go back to the product link).

You are directed to the product activation window.

- 2. Click **Download Cellebrite UFED** and save the file to a PC.
- 3. Extract the zip file, click the installation file and install the software using the Setup Wizard. Restart the PC if required.
- 4. Repeat step 1 and go to the product link.
- 5. In the Activation Code field, enter the Activation code provided with your product kit.

Activation Code
Activation Code

6. Obtain your Computer ID (do not close the MyCellebrite page while performing this step).

a. Start the application. The Cellebrite product licensing window appears.

Cellebrite product Select your license type:	license	
Dongle	Software	
⑦ Help   Sales		Close

b. Click **Software**. The following window appears.

Iready have a license file?	
Load license file	
leed to download	your software license?
leed to download So to MyCellebrite	your software license?
leed to download So to MyCellebrite	your software license?
leed to download So to MyCellebrite Computer ID: 4VB	your software license? -DH4-ZGR-YMT-VE3-W2Z-M3M Copy
leed to download So to MyCellebrite Computer ID: 4VB	your software license? -DH4-ZGR-YMT-VE3-W2Z-M3M Copy

- c. Click **Copy** to copy the Computer ID displayed in the window.
- 7. In MyCellebrite paste the copied Computer ID.

Computer IL	)		

8. Click **Generate License** to download the application license key to your PC. The license key is also sent to your registered MyCellebrite email address.
9. In the application, click **Load license file** in the Cellebrite product license window, then locate and select the license file, or click **Load from the web** to download the license file from MyCellebrite.

Congratulations, your Cellebrite UFED application is now ready!

## 3.3.3.1. Software license distribution by Commander

License updates for end points using software licenses can now be distributed from Commander 7.22. Until now thihs was possible only for dongle licenses.

License distribution via Commander can be done only for updates, new licenses should be activated manually on the end point before the first use. When working in offline mode, the license should be applied manually (as before). License distribution for offline mode will be supported in the next version

3.3.3.1.1.

# 3.3.4. Using a network dongle

The network dongle is connected to your organization's network and contains licenses for all the applications purchased.



### To use Cellebrite UFED with a network dongle:

\* Start the application. If the network dongle is connected to the network, the application starts and you can start working immediately.

## If a network dongle is not found:

1. If the network dongle is not recognized, the Cellebrite product licensing window appears.

#### Cellebrite product license

Select your license type:



?	Help	, ∖⊒	Sa	les
---	------	------	----	-----

Close

2. Click **Network**.

	If a dongle was not found on the network. Make sure that you have an Internet connection and that a dongle is connected to the network. Then click <b>Refresh</b> to search for a network dongle again.
_	
	If you click <b>Refresh</b> twice, a new window appears where you can manually connect to the network dongle. Click <b>Advanced</b> and then enter the IP address (or host name).
ß	If there is only one network dongle, it is selected automatically. If there are multiple network dongles, select the required Dongle Serial number.

### Congratulations, your Cellebrite UFED application is now ready!

## 3.3.5. Online activation of new license from Loader

license for this product wa ease select your license typ	as not found. pe:
Dongle	Software
<u> </u>	
V	
	CANCEL

Go to Start > Cellebrite License Loader > Cellebrite License Loader.

Select Dongle or Software.

For software licenses:

<sup>\*</sup> In the next screen, activate the license online.

Activation Code

Valid Email address

<sup>\*</sup> Press "Online activate"

You receive a license request with:

Activation Code, Email and C2V

<sup>\*</sup> Select Dongle license

You can activate the license online.

<sup>\*</sup> Fill in the following:

Dongle Serial ID (on the stick)

Press "Online activate"

You receive a license request:

Dongle Serial ID and C2V

If the Activation Code or Dongle Serial ID are valid, the loader activates the license.

## 3.3.6. Update software license with one click

You can now update your software license with one click.

#### To update your software license:

<sup>\*</sup> Go online and click Update. The license file is downloaded and applied automatically.

#### Cellebrite product license

To get or renew a license, use either the manual (offline) procedure or the automatic (online) procedure.						
Computer ID: Corpy this link						
1. Generate C2V file Click generate to create computer ID file (*.C2V)	2. Upload C2V file Go to MyCellebrite and upload the (*.C2V) file community.cellebrite.com	<b>3. Load license file</b> Load the file (*.zip) from MyCellebrite				
GENERATE		LOAD				

Online UPDATE

# 3.4. Working with UFED

This section includes the following:

Starting the application (below)

Home screen (on the facing page)

Autodetecting a device (on page 44)

Searching for a device (on page 46)

Case details (on page 51)

User predefined filter (on page 59)

Manual selection (on page 61)

Application taskbar (on page 62)

# 3.4.1. Starting the application

\* Double-click the Cellebrite UFED icon to open the application.

# 3.4.2. Home screen

The home screen groups the extraction data into distinct areas: Mobile device, SIM card and USB device or Memory card. In addition, users can directly operate the camera for immediate image capturing or access the device tools. All extraction functionality is driven by **automatic** identification of the device, by **searching** for the device or by **manually** selecting the vendor and model. Cellebrite UFED determines what functions are available for the specific device and displays the relevant functions.



# 3.4.3. Autodetecting a device

#### To use Autodetect to locate the mobile device:

1. Connect the mobile device to the Cellebrite UFED unit.

DETECT DEVICE		<u>ن</u> (۲
CONNECT PHONE TO AUTO DETEC		
ABORT	BACK CONSOLE	AUTO DETECT SKIP

2. Select Auto Detect at the bottom of the screen.

If the connected device is recognized by the system the following window appears.



If multiple matches are found, the following window appears.

DETECT DEVICE					0	Ċ
SELECT YOUR DEVI	CE				EXTRACTION F	LOW
Samsung GSM SM-6900 Galaxy SS	DR4 Samsung	GSM SM-G900R4 Salaxy SS	Samsung CDMA SM- G900R4 Galaxy S5	Samsur G900F	g CDMA 5M- 4 Galaxy SS	
ABORT		ВАСК	CONSOLE		BROWSE DE	VICES

- 3. Select the relevant device.
- 4. Alternatively, click **Browse Devices** to manually search for the device.



Click the **Console** button to access device information using the Android Debug Console. For more information, refer to the *Performing extractions* manual.

5. If the connected device cannot be recognized by the system, a message prompts you to try the following steps or tap Find device manually.

Auto detect didn't find the device	
2 Android only:	
Turn on USB Debug and enable Media Device mode (MTP)         3         Wait 5 seconds and reconnect the device (Auto detect will start)	
Tried the steps, and the device wasn't found?	
FIND DEVICE MANUALLY CONSOLE	

6. If the device still cannot be found, tap **Browse Devices** or **Console**.

# 3.4.4. Searching for a device

### To search for the mobile device:

1. Narrow the list by vendor, recently used, etc. or begin typing in the search field in the top bar to search for a device or model. As you type, the list of devices is reduced to match your search criteria.



You can also search for a device by its IMEI value, which is used to uniquely identify devices. The IMEI value is usually found printed inside the battery compartment of the device, or dial \*#06# from the phone keypad. Enter the value in the search field, using a minimum of four digits up to the full number. If the IMEI value is recognized, matching devices are displayed.

2. Select the device model type from the list.

Ē

Having selected the device, Cellebrite UFED determines what extraction functions are available for

this combination and presents those functions:

Cellebrite Responder 7.38.0.133					- 0 ×
	SELECT EXTRACTION TYPE			ى 💿 🖄 📀	
	Cable A with black tip T-1	30F Galaxy S7 00			
	0	0	0	0	
	Advanced Logical	Disable/Re-Enable User Lock	File system	Physical	
	<b>₽</b>				
Na		Lock Bypass	Selective Lock Bypass	Lock Bypass	
les -	0	0			
	Screenshot	Chat Capture			
udance	Ē.	Ę			
	_				
	ABORT			FINISH	

Lock Bypass is displayed for both physical and file system extraction methods that can bypass the user lock of the device.

#### 3.4.4.1. Device wizard - Beta

The new search capability enables users to view all supported extraction methods available for a particular mobile device, even before connecting to it.

For Android devices,, you can input device properties such as chipset, OS, OS version etc. Each property added increases the number of methods available for devices that have been tested by Cellebrite, and the number of methods available for devices that have not yet been tested but which have a high probability of success based on the device properties.



SEARCH DEVICE	Beta de la constante de la cons		⊙ ≡
Search device	O-Device specification		O Applicable method
Search device by name	, model or vendor not listed, click "Next" to search by device specifications only.	Q 	
ABORT		ВАСК	NEXT

DEVICE SPECIFICATION Beta			⊙ ≡
Search device	Device specification		O Applicable methods
Chipset	os		
OS version	Kernel version		
Type OS version	4.19.87 Security patch date	·	
Select encryption type	Select date		Samsung Galaxy S20 SM-G980F
ABORT		ВАСК	NEXT



## 3.4.4.2. TAC search

If you cannot find the Android device which you are looking for after performing a TAC number search, a window appears. This window appears if Cellebrite UFED does not support the device directly, but there are applicable generic options available for the device.

To retrieve device information and view generic extraction options:

1. Enter the complete 8-digit TAC number. The following window appears.



The window includes the vendor, operating system and device name.

2. Click **See recommended extractions**. A window appears with the generic extraction options for the device.



Ð

If you enter a partial TAC number (with less than 8-digits) or the device is not supported by Cellebrite UFED then the following window appears.

3568588	×	Search By: Name, Model,	Chipset, IMEI, TAC, Manufactor	0	Ċ
All	Vendors	Generic profiles	Recently used		
It appears that th	nis device is not s	supported by UFEI	). Enter the complete 8-digit	TAC to retrieve d	levice
	infori	mation and extract	non recommendations.		
ABORT				BACK	

# 3.4.5. Case details

The Case details feature enables you to enter case details when performing an extraction or using the Cellebrite UFED camera. This feature is not enabled by default.

### To enable the case details feature:

\* Select Include Case details screen under Settings > General.

### To specify the case details:

1. On the Home screen, select an extraction type or Cellebrite UFED camera. The following window appears.

CASE DETAILS		0	ወ
NEW CASE			
Case ID *			
	Use details from last case:		
Seized by *	Case ID: 4455 Soized by:		
Crime type *	John Smith		
· · · · · · · · · · · · · · · · · · ·	<b>Crime type:</b> Armed Robbery		
Device owner *	Device owner: Suspect		
	USE LAST DETAILS		
ABORT	ВАСК	CONTINU	JE

2. Use the current case information, or enter and select the case information and then click **Continue**.

# 3.4.6. Investigation notes

The Investigation notes feature enables you to add notes during the data extraction process. You can include observations or report any issues encountered during the process.

## To enable or disable the feature:

1. Select **Settings > General**. The following window appears.

«	General	System	License	Version 🚿
Ca T Su	Show device restart alerts able and Tip Mode: Tip T upport Notification: Use offline maps Extraction folder name acco	ording to case details		
Ex III Vi	Show investigation notes Disc catalog ID amination tool: nField viewer Choose additional logo Save report automatically deo quality: ow Enable device info (Advance)	ed logical)		
			SAVE	CANCEL

- 2. Select or clear **Show investigation notes**.
- 3. Click Save.

## 3.4.6.1. Using the feature

You can add pictures, screenshots and text that are relevant to your investigation to create an audit trail of actions taken and decisions made.

1. Start an extraction and click **Notes**. The Investigation notes window appears.

Investigation notes	0	Ċ
🙆 🗘 т		
Add pictures, screenshots and text that are relevant to your investigation.		
	Use details from last case: Case ID: 447500-2019 Seized by: Cpt. J Smith Crime type: Narcotics Device owner:	
	Suspect USE LAST DETAILS	
		E

To close the window, click the Cellebrite UFED interface outside of the Investigation notes window.

2. Add text, screenshots and pictures that are relevant to your investigation. The investigation notes are available as part of the extracted data or report. See <u>Accessing the extraction</u> notes file (on page 58).

See the following procedures to add text, screenshots and pictures:

To add text notes: (on the next page)

To add screenhots: (on page 55)

To add pictures: (on page 56)

## To add text notes:

1. In the Investigation notes window click Text ( $\square$ ). The following window appears.

S	Save

- 2. Enter the required text and tap **Save**.
- 3. The text is added to the Investigation notes panel and it includes the date, time, and stage of the extraction process.

Investigation Case ID: 4475	notes <b>00-2019</b>						
Ø	5		Т				
Today 13:26:16 Detect device X Auto detect was not used. Manually selcted the correct device.							
Today 13: Skip Conse this case	25:14 nt form. N	Ageno ot releva	nt to	×			
Today 13: Start invest	23:26 igation	Case	details	×			

To remove a note click Delete (X).

## To add screenhots:

1. In the Investigation notes window click Screenshot (

nsert text					
Your note h	ere				
	DEVICE DETECTED			00	
	YOUR DEVICE'S INFO				
r	Samsung 65M GT-8205 Samsung 65M GT-8205 Samsung 63kay Maga 63 Cable A web black typ 7-100	Device properties Mudat Sommang GAD GT H205 Summaing Galaxy Mega Device annues GT H205 GE Andread 4.2 Objecti mean#IR06 Rooted: No	Security patch: MCD Appo 17		
				CONTINUE	
<u>a e</u>	N &	120			
		(	Close		Save

- 2. Enter the required text and tap **Save**.
- 3. The screen capture is added to the Investigation notes panel and it includes the date, time, and stage of the extraction process.



## To add pictures:

1. In the Investigation notes window click Picture (<sup>()</sup>). The following window appears if a camera is not connected.

Insert text		
Your note here		
ـلــم		
0		
Camera not connected	Close	Save

2. Connect a camera to Cellebrite UFED.

Insert text	
Your note here	
IPEVO Point 2 View ▼ Close	

3. Select the required camera to use.

4. Click Camera () to take a picture. If required, tap Refresh () to take a new picture,

or click Rotate 🖄 to rotate the picture.

- 5. Enter the required text and tap **Save**.
- 6. The picture is added to the Investigation notes panel and it includes the date, time, and stage of the extraction process.



## 3.4.6.1.1. Accessing the extraction notes file

Ē

After completing the extraction, the investigation notes are displayed as an ExtractionNotes.pdf file in the Notes folder when the report or extraction is saved.

In Cellebrite UFED, the PDF file is only created when you click **Finish**.



Summary		
Notes (4)		
1/4		
Time stamp	2/23/2020 4:26:14 PM (GMT+2)	
Application state	Detect device	
Camera note		<u>Click to enlarge</u>
2/4		
Time stamp	2/23/2020 4:26:23 PM (GMT+2)	
Application state	Detect device	
Screenshot note	test	Click to enlarge
Example Investigation	notes	

# 3.4.7. User predefined filter

The User predefined filter provides the ability to extract and view only a portion of the device content, based on time range or specific subject information (person, email, phone). This can be useful when:

- \* The agency has a warrant to extract data from a specific time window, and is not allowed to view additional data that is not covered by the warrant.
- » The user wishes to save time and get to the relevant data ASAP.

The most time consuming phase during a device extraction is transferring the data from the mobile device to the extraction tool. Timeframe filtering is performed on the device (when technically supported), and can reduce the extraction time. Another advantage is the reduced amount of data that the agent must browse through to find the evidence.

#### To enable the User predefined filter:

\* Select Allow user predefined filter under Settings > General.

### To specify the timeframe and parties for the extraction:

1. Identify the device and select an extraction type. The following window appears.

ADD FILTERS	0	Ċ
LG CDMA VS988 G6 using USB cable 170 or Original Cable		
When? Select a timeframe for the extraction:  Unimited 1 year 1 month 1 week 1 day 1 hour Which events? Include or exclude or exclu		
Enter keywords or numbers		ADD
ABORT BACK	NEXT	•

The extraction is based on the Cellebrite UFED unit's date and time. When selecting a time frame, also consider the device's time zone.

The timeframe option is not applicable to file system extractions.

- 2. Select the required time frame. The less time selected, the quicker the extraction.
- 3. Enter keywords or numbers that you would like to include.



Selective extraction by party: Similar to the time frame, the ability to extract and review only data relevant to a specific party (number or device).



Partial numbers are matched by the application, and names are matched irrespective to the capitalization.

4. Click Next.

# 3.4.8. Manual selection

### To manually select the vendor and model:

1. Click Mobile device and then click Skip.

You can then select **All**, **Vendor**, **Generic profiles**, or **Recently used**. As displayed next, the Vendor screen enables you to select the device vendor.



2. After choosing the Vendor, the application presents the Select Model screen where the specific model of the device is chosen.



Having chosen the **Vendor** and the **Model**, Cellebrite UFED determines what extraction functions are available for this combination and presents those functions.

# 3.4.9. Application taskbar

The application taskbar is located at the top of the screen.

?	
	ပံ Exit
	Export logs
	Settings
Mass storage	

Application taskbar icons and descriptions

lcon	Description
?	Click to select Online help or Extraction flows document.
	Click the menu icon to access the following:
	» 🕐 Exit
	* Export logs
	* Settings

## 3.4.9.1. Export last session logs

Click on the options icon (hamburger) and select Export.

**Export All:** Exports logs for all sessions, including the current session.

Export lastExports all logs from the last session (or the current session - whichever issession:latest).



# 3.4.10. Creating a Support ticket

UFED enables opening Support tickets directly from the application. It is not necessary to go to the Cellebrite Community site or to email / phone the Support team in order to do so.

## 3.4.10.1. Support ticket issues

Support tickets regarding the following issues can be opened directly from the UFED interface:

- <sup>\*</sup> Installation/Upgrade
- <sup>»</sup> License
- <sup>\*</sup> Phone Support Status
- <sup>»</sup> Application
- <sup>\*</sup> Android
- iOS
- ° SIM
- » Mass Storage
- <sup>»</sup> Drone
- Device tools
- Other

### Procedure

1. From any UFED screen, click (the information icon) **? > Report and Issue > Open new ticket**.

Cellebrite UFED 7.62.0.32					-		×
Cellebrite UFED					?	=	
Mobile device	SIM card	Quick	Open nev Transfer t copy	Mass stor v ticket icket files	Releas Extract Help Report	e Notes tion Flov an Issue	/
Device tools							
Version 7.62.0.32						2/01/20	23

2. The **Support ticket** screen displays.

Support ticket	×
Subject' Email*	
Please choose	r enail
Full name Device more	del
Enter full name Enter you	r emàil
Brief description of issue	
Write hene	
No files attach The	image could not be found
ATTACH FILE	rintscreen
Severity LOW HIGH CRITICAL	
Share last logs VEW LOGS	

- 3. In the Support ticket screen, do the following:
- a. Enter your email (required field) and select the Subject (required field) from the drop down menu.
- b. Enter your name and the device model.
- C. Enter a brief description of the problem.
- d. To share the last log files, select the option "Share last logs".
- e. To select files that are relevant to the Support request, click **Attach File**. The file names of the selected files display in the small display pane.
- f. To share the current screen, select the option "Share printscreen". The image displays in the display area above the option and to the right of the file list.

- g. Select the severity of the problem (Low, High, Critical).
- h. Click SEND to send the Support ticket to the Cellebrite Support team

A notice will be sent to the user with a message stating that a Support ticket was opened and will include the Ticket (case) number.



#### 3.4.10.2. Transfer files

Frequently, transferring files that you attach to a support ticket are large and transferring them to Cellebrite Support requires an extended period of time. Cellebrite UFED enables you to continue working while it transfers the files in the background.

# Viewing Transfer file status

To view the status of all your tickets and their associated files *after* you have created a Support ticket, do this:

1. From any UFED screen, click (the information icon) **? > Report and Issue > transfer files**.

Cellebrite UFED 7.62.0.32					-		×
Cellebrite UFED					?		
Mobile device	SIM card		Release Notes Mass stor Help Open new ticket Transfer ticket files		/		
	UFED camera	Quick	сору	(	Drone	)	
Device tools							
Version 7.62.0.32			L 12:	03:39		2/01/20	23

2. The **Ticket file transfer** screen displays and shows all tickets:

Cellebr	ite UFED 7.62.0.32				- 🗆 ×
снос	DSE ACTION			<b>6</b>	⊘ ≡
	Ticket file transfer				×
	Ticket number	Subject	Device model	Status	
	00228306	Phone Support Status	Galaxy3000	Ocompleted	
	00228307	Phone Support Status	Galaxy3000	Completed	
	ABORT				ВАСК

# 3. Smart flow

Smart flow is an automated flow that shortens the time to evidence by shortening the extraction process. It is an alternative flow for performing a full file system, physical, or selective, exploit-based extraction, without the need to select a specific phone profile, extraction type, method, etc.

Smart flow is relevant only for:

- <sup>\*</sup> Unlocked Android devices (see <u>Android extraction methods (on page 168)</u>). Locked devices will be added in the future.
- <sup>\*</sup> An exploit based flow to get full file system or selective by app token extraction.

The flow is simple flow – connect the phone, start the relevant exploit based on the connected device, display device info and optional extraction types.

Smart flow automatically tries the compatible method based on the connected device. If the flow fails, it will try another method that may work.

Smart flow

#### 1. Open UFED

Cellebrite   UFED 4PC			¢ 🤊 🙂
Welcome, Anna!			
Mobile device	SIM card		Mass storage
	UFED camera	Quick copy	Drone
Device tools			
Version: 7.58.0.1		() 12	:38 PM   🔅 Feb 21, 2022

2. Select the device. The following screen displays.

				<b>\$</b> ()
Connect Device	O Select Target Path	O OS Access	O Extraction	O Extraction Summary
DO THE FOLLOWING	STEPS BEFORE CONNE	CTING THE DEVICE		
		Android Devices 1. Open settings 2. Enable developer opti number" 7 times. 3. Enable USB debugging 4. Enable stay awake (if a 5. Set USB connection to 6. Connect your device <b>IOS devices</b> 1. Disable auto-lock	ions > Go to About/Infr available) o enable file transfer (N	ormation > Tap the "Build MTP/Media)
ABORT				BACK

- 3. In "Choose action", select "Smart Flow".
- 4. Follow the on-screen directions before connecting the device.

				<b>O</b>	Ċ
•	•	o	o	o	
	Select Target Path	OS Access	Extraction	Extraction Summary	ary
CHINESE ANDR	OID MOBILE PHONE /ITH BLACK TIP T-100				
nect source device device.	to the USB port on the compu	ter. If the device is all	ready connected, discor	nect and then reconnect	nect
	Ext Select the destin	raction to local drive			
ABORT			BACK	NEXT	

- 5. Connect your device using the cable appropriate to your device.
- 6. UFED will select and attempt the best method.
- 7. From the Select Extraction screen, select the items to extract under "Insights from Installed Apps" or select VIEW ALL to see all items that can be extracted (and select the items to extract).

Model: LG G7 ThinQ LM-G710EMW	64GB	Rooted: No		Insights from I	nstalled Apps
Davies esmer		Cocurity Dat	eh.	Secure Wi	pe (1 Apps)
Jonathan's LG G7		Kirin 960	un.	Clean Mob	ile (1 Apps)
os:		Apps:		Unknown (	(165 Apps)
Android OS 7.1.2		197		Developer	Tools (13 Apps)
Chipset: Kirin 960		IMEI: 1234567890	123456	VIE	W ALL
Total used 32.8 GB (of 64 GB)	Pho	100	Anno	Other	21.2 CP /res
Videos	Pho	105	Apps	Other	31.2 GB 1100

8. The extraction will proceed.

Connect Device	Select Target Path		Extraction	O Extraction Summary
CHINESE ANDRI USING CABLE A W	OID MOBILE PHONE ITH BLACK TIP T-100			
Please wait, this can ta	ke a few minutes			
		Ę		
	4 out of 100		16%	
ABORT		STOP		

9. The following sceen displays when the extraction completes.



10. To extract using other, specific flows, see the Extraction sections below.

# 3.5. Android Live consent-based collection

This Smart-flow process is a unique, new industry-leading capability that provides the widest range of coverage for unlocked Android devices. This simplified flow automatically selects the appropriate "Live" access method for unlocked Android devices (such as Qualcomm Live, Exynos Live, etc.).

There is no need to select the device profile and method. Just connect the device - the relevant access method is automatically applied.

After gaining device access, users can select one of the extraction types presented.

Universal Live Android supports the most popular SoCs in the market: Qualcomm, MTK, Kirin, Unisoc (Spreadtrum), Exynos, and newly introduced SoC, JLQ (used in Xiaomi Poco C4).

This capability adds support to a wide range of devices that were not previously supported in the current "Live" methods, with no known SPL limitation.

Some of the supported devices are:

- <sup>»</sup> Samsung A12, A21, S22 Ultra (Exynos)
- <sup>\*</sup> All Google Pixel models (including Pixel 7 and 7 pro)
- <sup>»</sup> Xiaomi Redmi 9/9A/9C, Xiaomi Redmi K50, Xiaomi Redmi Note 11T [Pro Plus]

- <sup>\*</sup> Oppo A15, Oppo Reno8 Pro Plus 5G, Vivo S15 PR
- <sup>\*</sup> Moto G Pure, OnePlus 10R 5G, Honor 70 Pro Plus

We encourage you to use Smart flow for devices that are not included in this list.
# 4. Password extraction

It is common to encounter a device that is password protected. Passcodes include a 4-digit PIN, a complex alphanumeric passcode, or a pattern lock. UFED can identify and bypass some passcodes depending on the make and model of the device. To find out if the passcode can be identified or bypassed, refer to the <u>UFED Supported Devices</u> file.

### 4.1. Extracting the user lock

Extract the password, or user code or PIN, locking the device. The extracted password can be displayed on the screen or written to a USB flash drive or PC for archiving. The ability to extract passwords depends on the device's make and model, the type of passwords enabled on the device, and the password's length.

#### To extract a user lock on a mobile device:

1. Click Mobile device and identify the device, then click Extract User Lock.

SELECT EXTRACTION LOCATION

 Image: Constraint of the second sec

The Select Extraction Location screen appears.

- 2. Select **Display Only** or **Local Drive**.
- 3. Connect the source device to the USB port, or via the UFED Device Adapter.
- 4. Click **Continue**.

The Extraction in Progress screen appears.



At the end of the extraction process, the extracted passwords are displayed in the **Passwords** screen.

Passwords
User Code:
0000
ESN/MEID:
268435459304781538
Own Number:
MIN:
0123450000
CONTINUE

5. Click **Continue** to display a summary of the passwords extraction process.

The following screen appears.

EXTRACTION SUMMARY	?	டு
Extraction completed successfully		
Source: UN-161 Target: Display Only		
ADDITIONAL EXTRACTIONS	FINISH	1

6. Click Additional Extractions to add additional extraction types for the same device, or click Finish to end the process and return to the Home screen.

### 4.1.1. The extracted passwords folder

Ē)

At the end of the passwords extraction process, the extracted passwords are saved to a text file named Passwords.txt at the location you selected during the data extraction process.

The text file is located inside a folder named **Password** with the name of the selected device name and the extraction date. For example, **Passwords Iden i9** 2011\_06\_11 (001)

# 4.2. Disabling or re-enabling the user lock

You can disable and re-enable the user lock on a device:

- Disable the user lock: Disable the user lock (or password), which means that the device is no longer locked. Each device model has a slightly different process, depending on the device lock combination and how the model connects to UFED. When more than one method is available for the device, we recommend that you try both methods if one method is not successful. If you disable the user lock more than once, you cannot re-enable the original user lock. For a complete list of supported devices, refer to UFED Phone Detective or the UFED Supported Devices document in MyCellebrite.
- \* **Re-enable the user lock**: Re-enable the user lock on a device, after it was disabled by UFED. This enables you to return a device to its original state.

To re-enable the original user lock on the device, use the Re-Enable User Lock method and do not create a new user lock manually. If you create a new user lock, you cannot re-enable the original user lock.

UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: <u>https://www.cellebritAxon</u> <u>Evidence/en/services/advanced-unlocking-services/</u>

#### To disable (or re-enable) the user lock on the device:

1. Click **Mobile device** and identify the device, then click **Disable/Re-enable User Lock**. The following window appears.

SELECT MODE		<u></u> 0 (۲)					
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100							
Disable User Lock	Re-Enable User Lock						
ABORT		ВАСК					

2. Click **Disable User Lock** to remove the user lock from the device, or click **Re-Enable User Lock** to reenable the user lock on the device. The Waiting for Device screen appears.



3. Follow the instructions for the device and then click **Continue**.

If the device does not unlock, click **Abort**, and repeat the procedure. Make sure you are using the correct USB cable.

The Extraction completed successfully screen appears.

4. Click Finish.

## 4.3. Removing the screen lock

The Remove screen lock method disables the user lock from a wide range of Samsung Android devices for example Galaxy S7, S7 Edge, J7, J5, A7, and A5. This method works on both Qualcomm and Exynosbased devices.



UFED cannot re-enable the screen lock after running the process.

#### To remove the screen lock from a device:

1. Click **Mobile device** and identify the device, then click **Disable/Re-enable User Lock**. The following window appears.

SELECT MODE		?	Ċ
Samsung CDMA SCH-i. using Cable A with black t	545L Galaxy S4 ip T-100		
0	1		
Disable User Lock	Remove Screen Lock		
Lock Bypass	Lock Bypass		
ABORT		BACK	:

2. Click **Remove Screen Lock** to remove the screen lock from the device. The Waiting for Device window appears.

WAITING FOR DEVICE	0	Ċ	
Samsung CDMA SCH-i545L Galaxy S4 using Cable A with black tip T-100			
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.			
<ul> <li>SCH-I54SL Galaxy 54:</li> <li>Important: Devices with secure startup are not supported by this method.</li> <li>To allow device connection:</li> <li>Note: The device battery should be fully charged.</li> <li>1. Turn off the device.</li> <li>Press and hold the Volume down, Home and Power buttons until the device enters Download mode.</li> <li>3. Select "Continue" by pressing the Volume up button.</li> <li>4. Wait until the Download mode loga appears on the device screen, and then connect the device to the cable.</li> <li>5. Connect the cable to UFED 4PC.</li> <li>6. Select "Continue".</li> <li>1. Restart the device in Recovery mode: <ul> <li>a. Restart the device in Recovery mode:</li> <li>a. Restart the device displays the Recovery mode screen, release the Volume up, Home and Power buttons.</li> <li>c. Wait on the device displays the Recovery mode screen, release the Volume up, Home and Power buttons.</li> <li>c. Wait for the Recovery must be deligaded (this can take several minutes).</li> </ul> </li> <li>2. Select Power off, then press the Power button to turn off the device.</li> <li>Note: Use the Volume up and Volume down buttons to navigate the Recovery menu.</li> </ul>	id the Volume up, Hom	e and Pow	er
ABORT BACK	CONT	INUE	

3. Follow the instructions to place the device in Download mode, then click **Continue**. The following window appears.



4. UFED now tries to flash another image to the device. Follow the on-screen instructions until the device the device displays the Warning screen and Download mode again. Then click **Continue** in UFED. The following window appears.



5. Click **Continue**, then wait about one minute and restart the device again when instructed. The following window appears.



6. Restart the device for the changes to take effect and then click **Continue**. The following window appears.





The process completed successfully, but it may not work on all devices. If the process did not work, try a different method.

7. Click OK. The following window appears.



8. Click Finish.

# 5. Logical extraction

The Logical Extraction function enables you to extract various types of data, such as call logs, phonebook records, SMS text messages, calendar events, and multimedia files (images, videos, etc.). Save the extracted data from the source device to your PC or to a removable storage device, as desired. In most cases, a logical extraction is not possible for locked devices.

A logical extraction can also be used to extract data from many Android, BlackBerry, iOS, and Windows Phone apps. For an updated list of supported apps and versions for each platform go to **Help** > **Supported Apps** in Physical Analyzer or Logical Analyzer. Data extracted from these apps can be analyzed using Physical Analyzer or Logical Analyzer (although the data is not included in UFED HTML and XML reports).

The available types of extracted data may vary depending on the source device manufacturer and model. The supported data types are listed in the UFED Phone Detective or within the UFED Supported Devices.

## 5.1. Advanced logical Android extraction

The following procedure explains the Advanced logical extraction process for an example device. The procedure may vary depending on the selected device. This section shows only one of the many extraction types that can be performed.

#### To perform an Advanced logical extraction from a mobile device:

1. Click Mobile device and identify the device, then click Advanced Logical.



For information about using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location window appears.

SELECT EXTRACTION LOCATION	(?)	Ċ	
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100			
Extraction to Local Drive			
C:\Users\			
ABORT BACK	NEXT		

2. Use the current location or click the folder icon to change the target path and select a different location and then click **Next**. The Waiting for Device window appears.

WAITING FOR DEVICE				0	Ċ	
Samsung GSM GT-i9205 Samsung using Cable A with black tip T-100	g Galaxy Mega 6	5.3				
Connect the source device to the USB port on the com	nputer. If the device is	s already connected, di	sconnect and then reconnect	the device.		
Android 4.2 and Higher Android 4.0 - 4.1.2 Android 3.2 and Lower  1. Enable Developer options How to?  2. Enable Stay awake and USB debugging modes How to?						
3. Verify screen lock mode <u>How to?</u> 4. Enable MTP (after device is connected) <u>How to?</u>						
ABORT	BACK	CONSOLE		CONTINU	E	

Ē)

Click the **Console** button to access device information using the Android Debug Console. For more information, refer to the *Performing extractions* manual.

- 3. Select the correct cable and tip for the mobile device, and change the device settings according to the instructions.
- 4. Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

5. Click **Continue**. The following window appears if **Enable device preview info screen** is enabled under General settings.

	Device properties		
	Model: Samsung GSM SM-N950U Galaxy Note 8	Security patch: 2017-10-01	
	Device name: SM-N950U	IMEI: 358508080008220	
	OS: Android 7.1.1	<b>Аррs:</b> 0	
Samsung GSM SM-	Chipset: msm8998		
USB cable 170 or Original Cable	Rooted: No		
	Total used 24 GB (of 64 GB)		
	Pictures Videos Audio/Music Down	loads • Other • 40 GB free	
ABORT			CONTINUE

This window provides information about the device data before performing an Android extraction. It includes device properties such as model, device name, operating system, chipset, whether the device is rooted, date security patch installed, IMEA, the number of installed apps, and insights from installed apps.

Insights from installed apps allows the user to get a peek into the types of apps installed on the device before the extraction. This areas displays app categories and the number of apps in each.

Click View all to view all app insights by category.



To update the app categorization database, go to System settings.

On many devices, but not all, it also includes information about storage volume, data types, volume of storage per data type, and free data.

6. Click **Continue**. The following window appears.

SELECT CONTENT TYPE			<u>ن</u> (۲					
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100								
ি Extract from								
Device	😫 SIM	Memory Card						
Choose data types to	extract							
	දා sms	🕒 ммз	👬 Calendar					
Pictures	Audio/Music	🔛 Videos	Ringtones					
₽ <sub>₽</sub> Call Logs	Files		& IM					
ABORT		E	ACK NEXT					

- 7. Data can be extracted from the Device, SIM and Memory Card of the device. Select from which memory you want to extract.
- 8. Different data types can be extracted. Select which data types you want to extract. In the example above, music and ringtones are excluded and are not extracted.

When Files is selected, UFED performs ADB backup to enable user data to be extracted.

9. Click **Next**. The following window appears.

Extract Contacts						
Sel	ect the accounts for extracting contacts:	Contacts	Estimated time			
<u>~</u>	PHONE contacts	104	00:00:18			
<b>~</b>	GMAIL kat.cheme1610@gmail.com	1	00:00:01			
<b>~</b>	FACEBOOK messenger	1	00:00:01			
			Continue			

10. Select the required contacts to extract and click **Continue**. The extraction process starts.

SELECT CONTENT TYPE								0	ڻ ن	
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100										
🕝 Extract from										
	Please	select multim	nedia	types to e	extract					
Device	Multi	media types	Files	Size	Estimated tim	ne				
🗈 Choose data types to	☑ 🦉	Pictures	217	167 MB	00:01:45				🗹 All	
	2	Videos	17	105.9 MB	00:00:54	- 1	-	_		
🖉 Contacts 🗸	🛛 🎵	Audio/Music	15	5.7 MB	00:00:04	- 1		Calendar	~	
Pictures	<b>Z</b>	Ringtones	13	201.2 KB	00:00:01			Ringtones		
	Estimat	ed extraction ti	me:	00:02:44	L					
⊇ <sub>i</sub> , Call Logs 🗸 ✓	Estimat	ed size:		278.9 MB	5					
Browsing Data					OK Abo	ort				

11. Click **OK**. The following window appears.

SELECT CONTENT TY	PE					(?)	Ċ	
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100								
🕝 Extract from								
Device	g	SIM	📋 Memory Card	I.				
🖹 Choose data typ	es to extra	r					🗹 All	
A Contacts	<b>√</b> ₽	Please restart the ph	none and press Continu	ie. 🗸	👬 Cal	endar	~	
Pictures	✓ Jª		CONTINUE	~	Ĵ Rin	gtones	~	
₽ <sub>æ</sub> Call Logs	~	Apps Data	🚊 Email					

12. If required, restart the device then tap **Continue**. When the extraction is complete and if required, the Source Instructions window appears (this depends on the device model). The following window appears.



13. Follow the instructions to return the mobile device settings to the original settings, and then click **Continue**.

EXTRACTION SUM	MARY			0	Ċ
Extraction comple	ted successfully				
A Phonebook	106	ন্থ্রি sms	31		
Ср ммs		🖨 Email	NOT SUPPORTED		
<b>Д</b> ім	NOT SUPPORTED	👬 Calendar	0		
Pictures	217	🎜 Audio/Music	15		
🔛 Videos	17	Ringtones	13		
ව <sub>ු</sub> , Call Logs	8	E Browsing Data	NOT SUPPORTED		
User Dictionary	NOT SUPPORTED	BBB Apps Data	5,847 files		
_					
Open with UFED Phy	sical Analyzer				
Show in Folder					
OPEN	ADDITIONAL EXTR	ACTIONS		FINISH	

14. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

Selected Manufacturer:	Samsung GSM	
Selected Model:	GT-i9205 Samsung Galaxy Mega 6.3	
Detected Manufacturer:	samsung	
Detected Model:	GT-19205	
Revision:	4.4.2 KOT49H I9205XXUDOA1	
MEI:	357426050266879	
Extraction start date/time:	15/02/2017 11:58:56	
Extraction end date/time:	15/02/2017 12:14:59	
Phone Date/Time:	15/02/2017 11:59:21 (GMT+2)	
Connection Type:	USB Cable	
JFED Version:	Product Version: 6.1.0.13 , Internal Build: 4.5.2.13 UFED	
JFED S/N:	560AKCLQPHAIYYOKSFCNC	
or complete analysis and adv Generic Extraction Notes: ZZ – Extracted phone time stam	anced reporting, open in UFED Physical/Logical Analyzer.	

### 5.1.1. The extracted data folder

At the end of the data extraction process, the extracted data is saved in the location you selected.

The extracted data folder is named UFED with the selected device name, the IMEI / MEID information. and the extraction date. For example, UFED Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 2014\_11\_10 (0001)

The extracted data folder contains:

- » Multimedia files folders named Audio, Images, Ringtones, and Video folders, containing each of the respective type of media files.
- Phone extraction report files in HTML and XML formats. (One HTML report per content type)
- \* UFD file.

The XML file can be viewed by both Logical Analyzer and Physical Analyzer.

# 5.2. Advanced logical iOS extraction

The Advanced logical extraction uses other extraction protocols and can potentially extract additional data compared to the standard logical extraction.

Advanced logical extractions can be used to extract data from Android or iOS operating systems. The following example shows an Advanced logical iOS extraction.

#### To perform an advanced logical iOS extraction:

- 1. Click Mobile device and identify the device.
- 2. Click Advanced Logical.

For information about using optional timeframe and party filters, refer to the *Overview Guide*.

The following window appears.



- 3. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device.
- 4. Click Continue. The following window appears.



5. Unlock the device and select **Trust** on the device. The following window appears.



6. This window displays the device name, UDID, iOS version, and whether the backup is encrypted. Click OK. If the iTunes backup is not encrypted, the following message about data encryption appears. If the iTunes backup is encrypted, see <u>Encrypted iTunes backup (on page 92)</u>.

Attention		
To extract user credentials from an enabled (encryption is automatical extraction). Enable backup encryption? (UFED v "1234".)	iOS device, backup e ly disabled at the end will temporary set the	encryption should be d of a successful e password to
	NO	YES

 In the Attention window click Yes to enable backup encryption with the ability to extract additional information from the device, or click No if you do not require the additional information. The following window appears.

> You can encrypt the iOS file. This additional layer of security allows iOS to include more sensitive information not found on a standard iCloud or iTunes backup file, including login details for apps and email accounts and other services that may be in use. You can extract an iOS keychain (user credentials) using this extraction method. At the end of the extraction, the encryption is automatically reset. You can view the user credentials under the Passwords tree item in Physical Analyzer.

If the extraction was stopped and the device remains encrypted, see <u>Disable</u> <u>iTunes encryption password (on page 200)</u>.

EXTRACTION IN PROGRESS	?	Ċ
Apple iPhone 4 (A1349) using Cable A with black tip T-110		
Please wait, this can take some time		
/Facebook.app/Facebook		
ABORT		

After the extraction completes, the Extraction completed window appears.



8. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

### 5.2.1. Encrypted iTunes backup

During Advanced Logical Extraction, if iTunes backup encryption is already enabled, then the following window appears.

Source Encrypted Backup Pass	word			
iTunes backup encryption is enabled. To preserve the password for the decoding stage enter it below (or press "Skip" if not known). Note: If you cannot obtain the password (including brute-force attempts), contact Cellebrite CAIS to bypass the iTunes encryption.				
encryption.				
••••••				
Show Characters				

#### If you know the iTunes backup password:

- 1. Enter the password so that it is not required during the decoding stage (in Physical Analyzer).
- 2. Click OK and follow the on-screen instructions to complete the extraction.

If you do not know the iTunes backup password:

<sup>\*</sup> Click **Skip** and follow the on-screen instructions to complete the extraction.



If you have exhausted all options to obtain the password (including the bruteforce option), Cellebrite Services can provide a full file system extraction that bypasses the iTunes encryption.

# 5.3. Logical (Partial)

This is a quick extraction method that supports the largest number of devices. You can extract Call logs, Phone books, SMSs, Calendar events, Multimedia files, and file data. The available types of data may

vary depending on the source device's make and model. In most cases, a logical extraction is not possible for locked devices.

#### To perform Logical (Partial) extraction:

- 1. Click Mobile device and identify the device.
- 2. Click Logical (Partial) and then select where you want to save the extraction.



For information about using optional timeframe and party filters, refer to the

The Select Extraction Location window appears.

3. Use the current location or click the folder icon to change the target path and select a different location and then click **Next**. The Waiting for Device window appears.

WAITING FO	OR DEVICE							C	2	ር
Apple Cable A	iPhone 4 ( with black	(A1349) tip T-110								
Connect the sou	rce device to	the USB port	on the compute	r. If the device	is already connecte	ed, disconnect	and then recor	nnect the dev	vice.	
IOS 10 and Higher	IOS 5.0 - 9.3.5	IOS 3.0 - 4.3.5	IOS 2.x and Lower							
<ol> <li>Dealle Scient</li> <li>Connect the dealers</li> </ol>	vice to the unit	wtor								
ABORT					BACK		CONSOLE	СО	NTINUE	



The Console button is only supported on Android devices.

- 4. Select the correct cable and tip for the mobile device, and change the device settings according to the instructions.
- 5. Connect the source device to a USB port. If the device is already connected, disconnect and then reconnect the device.
- 6. Click **Continue**. The following window appears.

SELECT CONTENT TYPE			<sup>(1)</sup> (1)
Apple iPhone 4 (A134 Cable A with black tip T-	49) 110		
🖄 Extract from			
Device			
Choose data types to	extract		All
	து sms	<b>С</b> ммs	🕄 Calendar
Pictures	Audio/Music	🔛 Videos	Ringtones
2, Call Logs	iies	🚖 Email	<i>2</i> , ім
E Browsing Data			
ABORT		BA	CK NEXT

7. Different data types can be extracted. Select which data types you want to extract. In the example above Ringtones are excluded and are not extracted.



When the **Files** button is selected, UFED performs an iTunes backup to extract user data.

8. Click **Next**. The following window appears.



9. Unlock the device and select **Trust** on the source device.

Multimedia types		Files	Size	Estimated time
🗹 🏹 Pictures		38	24.2 MB	00:00:10
🗹 🎬 Videos		3	7.2 MB	00:00:01
Estimated extraction time:	00:00:11			
Estimated size:	31.4 MB			
	OK			Abort

10. Select the multimedia types required and then click OK.

After the extraction completes, the Extraction completed window appears.

EXTRACTION SUN	IMARY				?	Ċ
Extraction comple	ted successfully					
A Contacts	715	ළි sm	S 3			
<b>[</b> р ммs	0	<u>ا</u> Em	ail O			
<i>2</i> த ім	0	Cal	endar O			
Pictures	38	Ja Aud	lio/Music 0			
Videos	3	م) Rin	gtones 0			
$\mathcal{D}_{p}$ Call Logs	4	E Bro	wsing Data CON	<b>NPLETED</b>		
🔐 User Dictionary	NOT SUPPORTED	### File	s 372	files		
OPE	N T	DDITIONAL EXTRACTIO	NS		FINISH	

11. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

# 5.4. Logical extraction via Bluetooth

This extraction method can be used to perform logical extraction via Bluetooth from any Android device. To use this extraction method, you must load a client onto the source device over the Bluetooth connection. When extracting data from a device via a Bluetooth connection, some content types (e.g., apps data, pictures, audio and music, video, and ringtones) and memory types (e.g., memory card or SIM card) are not supported. To extract multimedia content via Bluetooth, go to Smart Phones/PDAs > Android Bluetooth > Logical Extraction > Logical (Only Multimedia). Note that this method takes much longer.

Previously, the logical extraction via Bluetooth method was only available via the generic profile.

#### To perform a logical extraction via Bluetooth:

- 1. Click **Mobile device**, identify the device, select the extraction location, and then click **Logical**.
- 2. Select the extraction location. The following window appears.

WAITING FOR DEVICE	?	Ċ						
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100	Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100							
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.								
Android 4.2 and Higher       Android 4.0 - 4.1.2       Android 3.2 and Lower         1. Enable Developer options       How to?         2. Enable Stay awake and USB debugging modes       How to?         3. Verify screen lock mode       How to?         4. Enable MTP (after device is connected)       How to?								
ABORT BACK USE BLUETOOTH COM								

3. Click **Use Bluetooth**. The following window appears.



- 4. Click OK.
- 5. If required, connect the UFED device Adapter.

The following window appears.

SELECT CONTENT TYPE			ල <b>(</b> )
Smart Phones/PDAs using Bluetooth	Android Bluetooth		
🖻 Extract from			
Device			
Choose data types to	) extract		All
A Contacts	ନ୍ତ୍ର sms	<b>С</b> ммs	👬 Calendar
₽" Call Logs	Apps Data		
ABORT		BACK USE US	B CABLE NEXT

6. Select the required content types and then click Next.

Client Upload				
Uploading a client to the device Press 'Skip' if the client is already installed.				
SKIP	UPLOAD			

7. Click **Upload** to upload the client to the device or click **Skip** if you have already uploaded the client to the device. The following window appears.

Connect the device
Activate Bluetooth on the SOURCE phone and make it visible to other devices Android Bluetooth: Before connecting the phone, set phone's connection settings as follows: On an Android 4.0 and above, Select the checkbox: "Unknown sources" located under Menu → Settings → Security. On an Android 4.0 and under, Select the checkbox: "Unknown sources" located under Menu → Settings → Applications. Please turn on your Bluetooth connectivity. Make sure your Bluetooth connectivity. Makes ure gluetooth is set to discoverable ON. This phone needs a client in order to communicate with the application. The application has to upload the client to the phone prior to using it.
CONTINUE

8. Activate Bluetooth on the source device and make it visible to other devices. Follow the on-screen instructions to set the devices connections, then click **Continue**. The following window appears.

Bluetooth	Device Sele	ection			
JBL T110BT	QL-820NWB09 38	Galaxy Mega			
		_			
			REFRESH LIST	CANCEL	

9. Click the required device. The following window appears.



10. Press **Accept** on the device when the file transfer request is displayed (this is skipped if the client is already installed). The following window appears.



11. Follow the instructions to install the client on the source device, then click **Continue**.



- 12. Open (or start) the client on the source device and confirm the Bluetooth permission request on the device.
- 13. Click **Continue**. The following window appears.

Select the accounts for extra	acting contacts:	Contacts	Estimated time	
PHONE contacts		104	00:00:18	
GMAIL kat.cheme1610@gmail.com		1	00:00:01	
			Continue	

#### 14. Click Continue.

During the extraction process, the progress bar for the Source and then the Target is active.

When the extraction is complete and if required, the Source Instructions screen appears (this depends on the device model).



15. Click **Continue**. The following window appears.

EXTRACTION SUM	MARY			(?)	Ф	
Extraction completed successfully						
A Phonebook	105	ନ୍ଦି sms	31			
🕒 ммs	0	🖨 Email	NOT SUPPORTED			
<i>2</i> , ім	NOT SUPPORTED	📆 Calendar	0			
Pictures	NOT SUPPORTED	Ja Audio/Music	NOT SUPPORTED			
Videos	NOT SUPPORTED	Ringtones	NOT SUPPORTED			
$\mathcal{D}_{\hat{\boldsymbol{y}}}$ Call Logs	8	E Browsing Data	NOT SUPPORTED			
🛃 User Dictionary	NOT SUPPORTED	👯 Apps Data	NOT SUPPORTED			
Open Preview Repor	t					
Open with UFED Phy	sical Analyzer					
Show in Folder						
OPEN	ADDITIONAL EXTRA	ACTIONS		FINISH		

16. Click **Open Preview Report** to view an HTML preview report that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

# 5.5. Faster transfer and verification of logical collection output

Logical extraction output files can now be zipped for faster transfer. During the procedure, a hash of the zip is calculated automatically and is added to the UFD file.

### 5.5.1. Enabling the zip feature

To enable zipping the logical extraction output, go to *Settings > General tab > Zip logical extraction output* and mark the checkbox.

Logical extractions that were zipped can be opened in PA 7.52 and above. In older versions, open the extraction by manually unzipping it.



# 6. File system extractions

File system extractions (Full and Selective) enable you to perform extractions from a device.

UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: https://www.cellebritAxon Evidence/en/services/advanced-unlocking-services/

Lock Bypass is displayed if the file system extraction method can bypass the user lock of the device.

## 6.1. Performing a FULL file system extraction

1. Click **Mobile device** and identify the device, then click **File System**.

The Select Mode screen appears.

SELECT MODE			0	Ċ
Samsung GSM SM-J25 using Cable A with black ti				
File System Boot Loader (Recommended) Lock Bypass	Android Backup	1 Android Backup APK Downgrade		
ABORT			ВАСК	

2. Select ADB (for Android Backup, see Android backup (on page 117)).

For information about using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location screen appears.

PC UFED 4PC 0.0.1.1133		□ ×
SELECT EXTRACTION LOCATION	?	Ċ
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100		
Extraction to Local Drive C:\Users\jonathank\AppData\Local\My		
ABORT BACK	NEX	кт

3. Select a location. The following window appears.

WAITING FOR DEVICE	?	டு					
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100							
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.							
Android 4.2 and Higher 4.1.2 and Lower							
I. Enable Developer options <u>How to?</u> 2. Enable Stay awake and USB debugging modes <u>How to?</u> 3. Verify screen lock mode <u>How to?</u> 4. Connect the device to the unit.							
ABORT BACK	CONTIN	UE					

- 4. Select the correct cable and tip for the mobile device based on the information written in the screen.
- 5. Change the device settings according to the instructions
- 6. Connect the device.
- 7. Click **Continue**. The Extraction in Progress screen appears.

De UFED 4PC 0.0.1.1133						
EXTRACTION IN PROGRESS	© ()					
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100						
Please wait, this can take some time						
data/log/setupwizard.txt						
ABORT						

During the extraction process, the progress bar for the Source and then the Target is active.

For QCP and Samsung MTK devices, an estimation of the time the extraction will take is displayed.

When extraction is complete, the File System Extraction Summary screen appears.

EXTRACTION SUMMARY	0	Ċ
Extraction completed successfully		
Source: GT-i9205 Samsung Galaxy Mega 6.3 Target: Local Drive (FileSystem ADB 01)		
Open with UFED Physical Analyzer		
Show in Folder		
OPEN  ADDITIONAL EXTRACTIONS	FINISH	

8. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

### 6.1.1. iOS: Animated DFU instructions

iOS devices have a new animated instructional aid. The new aid displays the iPhone model and an interactive image with detailed instructions for carrying out the process.

a To ( Firr	place the iOS device in Device nware Update (DFU) mode:			
<b>1</b> . 2.	Hold both the Power button and the Volume Down button for 10 seconds. Release the Power button and continue to hold the Volume Down button for an additional 10 seconds.	<b>10</b>		
* For	illustration guide only	Restart	Abort	
To p Firm	lace the iOS device in Device ware Update (DFU) mode:			
1.	Hold both the Power button and the Volume Down button for 10 seconds.	$\bigcirc$		
2.	Release the Power button and continue to hold the Volume Down button for an additional 10 seconds.	$\odot$		
* For i	Ilustration guide only	Restart	Abort	

## 6.1.2. The file system extraction folder

At the end of the file system extraction process, the extracted data is saved in the location you selected previously (see **Performing a FULL file system extraction (on page 102)**).

The extracted data folder is named FileSystemDump with the selected device model and name and the extraction operation date. For example, FileSystemDump Nokia GSM Nokia 2626 2014\_03\_12 (001)

The extracted data folder contains:

- Zipped archive of the device file system containing files and folders in the same structure they were extracted.
- » UFD file containing the system extraction information, used by the Physical Analyzer application.
- \* PM file.

The File System extraction can be viewed using Physical Analyzer.

### 6.1.3. Unlocked Huawei Kirin devices

This new method enables you to do a full file system collection on unlocked Huawei Kirin devices.

- <sup>\*</sup> The **Huawei Live** method is located under file system extraction type in the **Android Kirin** generic profile and in several tested Huawei profiles.
- <sup>\*</sup> The method also appears as untested when connecting Huawei Kirin devices.





### 6.1.4. smartStopping an extraction

You can now stop Android File System extractions (not including Android Backup and APK downgrades) before they complete and save the (partial) extraction to that point.

- To stop an extraction in progress, clickthe STOP button in the screen labeled "Extraction in progress".
   A confirmation message displays.
- Click "Stop Extraction" (the exact wording might change).
   The extraction procedure will finish extracting the current file and stop.





The partial extraction can be opened in Physical Analyzer.

	EXTRACTION SUMMARY	0	é	0	≡
[	Extraction partially completed - stopped by user				
	Source: XT1754 Moto C Target: Local Drive (FileSystem MTK Live 01)				

A message stating that the extraction is partial and was stopped by the user displays in Physical Analyzer v7.54 and above.



To continue with the extraction and **not** stop the current extraction), click **Continue extraction** (the exact wording might change). The extraction continues uninterrupted.
# 6.2. Performing a SELECTIVE file extraction

Selective extractions are a subset of full file system extractions for both Android and iOS devices. A selective extraction extracts all app data from those files and folders (located under the root directory) that you <u>select</u>. The app data includes the folders and files associated with the app such as databases, APKs, images, and keys.

A selective extraction takes less time to complete than a full file system extraction and enables you to select only the files that you require.

Selective extraction is currently supported for EDL Decrypting Bootloader, Samsung Qualcomm Decrypting Bootloader and Huawei Decrypting Bootloader methods. Other methods require that you perform a <u>Full File System Extraction</u>.

When te Selective file system method is available, an indication is made on the method(s) presented.



Selective extraction **does not extract data from unallocated space**. Use one of the Physical extraction methods instead.

## 6.2.1. To extract data using Selective file system extraction:

When performing an extraction method that supports Selective file system extractions, you can see the Selective file system button on the Device info screen.

1. Click Selective file system.

EXTRACTION IN PROGRE	SS			0	С С
YOUR DEVICE'S INFO					
	Device properties				
	Model: Huawei VKY-L29 P10 Plus		Security patch: 2017-03-01		
<sub>ල,</sub> ව ඉති -	Device name: VKY-L29		IMEI: 862940031051182		
	OS: Android 7.0		Apps: 215		
	Chipset: hi3660				
Huawei VKY-L29 P10 Plus	Rooted: No				
USB cable 170					
	Total used GB 5(of 16 GB				
	PicturesVideosAudio/Mu	isic Downloads Ot	ther	11 GB free	
ABORT		SELECTIVE FILE SYST		TEM TOKEN	S

2. Select the apps to extract. You can search for apps by category from the Select categories list.

Cellebrite UFED 7.60.0.358						- 0	3 X
DEV	/ICE DETECTED						
Q	Apple iPhone 8 Plus (A1897) USB cable 210 or Original Cable						
			Tot	al Items selecte	d: 401 (54.22 MB)		
0	- Name	*   Size	Туре	Created	Modified		
•	Applications	12,956 files, 209,942,440 KB					
•	🗌 📕 dev	85 files, 0 K8					
•	🗌 📜 Library	2,370 files, 177,330,631 KB					
•	💳 📜 private	24,038 files, 2,434,746,742 KB					
•	🔲 📜 sbin	15 files, 892,098 KB					
•	😑 📜 System	210,447 files, 7,567,369,724 KB					
•	🔲 📙 usr	1,023 files, 422,014,172 KB					
		0 KB	file	01/01/20 8:00:00 A.	01/01/20 8:00:00 A		
	etc	11 KB		01/01/20 8:00:00 A.	01/01/20 8:00:00 A		
	tmp	15 KB		01/01/20 8:00:00 A.	01/01/20 8:00:00 A		
	🗌 🗋 ver	11 KB		01/01/20 8:00:00 A.	01/01/20 8:00:00 A		
34	42,496 Items, 10.07 GB						
					EXTRACT		

- 3. Click Extract. The Extraction Summary window appears.
- 4. Click Open Preview Report to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click Open with Physical Analyzer to open the extraction in Physical Analyzer, click Show in Folder to open the folder where the UFD extraction file is located, click Additional Extractions to add additional extraction types for the same device, or click Finish to end the process and return to the Home screen.

# 6.2.2. Enhanced selective extraction

Application lists are now grouped by category when using "App categorization".

Users can select an entire category of applications with a single click for quick and easy "Select by Application". Enhanced selective extraction also enables standard selection of individual apps.

To use this feature, <u>Community portal</u> Settings.	download , under the	the "App "Add-or	o Categorization Df ns" section of the p	3" file from the _ product, and upload	it via
SELECT APPS TO EXTRACT			<b>\$</b> (U		
LG G7 THINQ LM-G710EMW ( USING CABLE A WITH BLACK TIP T-	54GB 100				
You can select specific apps to extract:					
Search apps	Q Multiple values	selected	2 apps selected All		
App name	Physical Analyzer	Last used	Category		
🗌 🕨 💮 Browser	No	Today			
🗌 👻 📮 Chat	Yes	Today			
🗌 😒 WhatsApp	Yes	Today	Chat		
🗆 🔼 Snapchat	Yes	Today	Chat		
🔲 👻 🏢 Entertainment	No	Today			
Youtube	No	04.12.18	Entertainment		
🗌 👻 🔒 Password manager	Yes	Yesterday			
1Password	Yes	13.09.18	Password manager		
🗌 🐣 TunnelBear	No	13.09.18	Password manager		

# 6.2.3. Selective extraction by file (Android / iOS)

Selective extraction by file (Android / iOS) enables users to traverse the file system and select specific folders and files to extract. All relevant metadata from the files is retained and the forensic integrity of the file remains intact. Additional search capabilities can be applied.

1. When performing an extraction method that supports Selective File System extractions, the Selective file system button displays on the Device info screen.

SELECT EXTRACT	TION TYPE					?	=
Samsung G USB cable 17	SM SM-G970F Ga 0 or Original Cable	alaxy S10e					
Advanced Log	gical Selectiv	File system	1 Physic	al (Rooted)		Camera	()
Screensho	ot	Chat Capture	0				
ABORT						ВАСК	
Cellebrite UFED 7.60.0.358	DEVICE DETECTED			凶	⊚ ≡		- 0 ×
	YOUR DEVICE'S INFO						
	Apple iPhone 8 Plus (A1897) USB cable 210 or Original Cable	Device properties Device owner: iPhone Device model: iPhone 8 Plus iOS version: 14.5.1 (1822/2) IME11: 356772087436568 IME12: -	ICCID: 89972010620040744325 Installed apps: 55	Insights from installed appe: You can get insights from inst applications. To upload the app categoriza the setting menu	talled		
		Total used 10 GB (of 64 G • Applications • Pictures	5B) - 54 GB free ● Videos ● Audio/Music ● C	Other			
	ABORT		FULL FI	ILE SYSTEM SELECTIVE F	ILE SYSTEM 🔻		

2. Click **SELECTIVE FILE SYSTEM > FILE**S to display the next image:

Cellebrite UFED 7.59.0.165						- 0
	EXTRACTION			0		
	YOUR DEVICE'S INFO					
		Device properties				
	LG GSM H930DS V30+ USB cable 170 or Original Cable	Model: LG GSM H930D5 V30+ Device name: LG H930 OS: 9 Chipset: mon8998 Rooted: No	Security patch: 2019-09-01 IMFE: 352676090371460 352676090371460 <b>App:</b> 382	Insights from install You can get insights applications. To upload the app ca the setting menu	nd apps: rom installed tegorization D8 go to	
ance		Total used 7 GB (of 128	GB) - 121 GB free			
		Pictures Videos A	udio/Music • Downloads •	Other		
				ounci		
				Apps Toke Phys Files	i ns ical	
[	ABORT		FULL		CTIVE FILE SYSTEM 🔻	
Xiaomi M1804 USB cable 170 or	1D2SG Mi A2 r Original Cable				Total Item	ns selected: 0 (0 B)
Name		*   Sia	te	Туре	Created	Modified
>		10	files, 382,899 KB			
> 📃 📜 cache		1 f	iles, 385 KB			
> 🗌 📜 cust		57	files, 427,955,043 KB			
> 📃 📜 data		12	527 files, 8,898,049,309 K	в		
> 📃 🧵 dsp		29	files, 8,859,716 KB			
> 📃 🧵 firmware		47	6 files, 102,360,885 KB			
🗸 🗌 📜 persist		66	files, 354,224 KB			
> 🗌 📜 alarm		1 f	iles, 49 KB			
V 🗌 📜 bluetoo	th	1 f	iles, 9 KB			
	t_nv	9 K	(B	bin	01/01/1970 0:00:24	01/01/1970 0:00:24
> 📃 📕 bms		1 f	iles, 100 KB			
24,484 Items, 12.10 G	βB					
						EXTRACT

#### 3. Select the folders and files to extract.

Search by file name <b>Q</b>			Total Items sele	ected: 22 (6.00 ME
🗕   Name	▲ Size	Туре	Created	Modified
V 😑 🗁 apex	1,860 files, 606,586,710 KB			
🗸 😑 🗁 com.android.adbd	23 files, 7,785,247 KB			
🗸 🔲 📁 bin	1 files, 1,497,464 KB			
adbd	1,497,464 KB	avi	01/01/1970 00:00	01/01/1970 00:00
🗸 🔽 🗁 etc	1 files, 181 KB			
🔽 📄 init	181 KB	rc	01/01/1970 00:00	01/01/1970 00:00
> 🔽 🖻 lib	9 files, 2,306,936 KB			
> 🔽 🗁 lib64	11 files, 3,980,448 KB			
apex_manifest	218 KB	pb	01/01/1970 00:00	01/01/1970 00:00
> 🦲 📼 com.android.adbd@301400200	23 files, 7,785,247 KB			
> 🦳 📁 com.android.apex.cts.shim	4 files, 39,725 KB			

4. To **select files by name**, enter the name (or partial name) into the text entry box at the top. The screen filters the selection and displays all files that contain the characters entered **and their path**.

add X				Total	Items selected: 22 (6.00 M
E Name	Size	Туре	Created	Modified	Path
0b3 <mark>add</mark> 97-887a-4b7a-9bf7-a4dfa6a5f	0 KB	cllevent	25/04/2022 09:36	25/04/2022 09:36	data\data\com.microsoft.appmana
1c2ad8e5-e2e1-409e-a31c- <mark>add</mark> 12d16	740 KB	cllevent	18/01/2022 01:29	18/01/2022 01:29	data\data\com.microsoft.appmana
2060b9fc- <mark>add</mark> a-4bf5-91c4-d93096e8d	. 0 КВ	cllevent	18/01/2022 01:39	18/01/2022 01:39	data\data\com.microsoft.appmana
24695913-d178-48d3-a7da-9654265 <mark>a</mark>	. 5,144 KB	cllevent	15/02/2022 13:04	15/02/2022 13:04	data\data\com.microsoft.appmana
2add47b6	2,679 KB	0	31/12/2008 15:00	31/12/2008 15:00	system\etc\security\cacerts\2add4
66ea7e1e-c0f5-4a17- <mark>add</mark> 0-b5d00c89	4,135 KB	cllevent	18/01/2022 01:31	18/01/2022 01:31	data\data\com.microsoft.appmana
6e1bacf8-1273-4f08- <mark>add</mark> b-d87bfbc09	5,144 KB	cllevent	15/02/2022 11:48	15/02/2022 11:48	data\data\com.microsoft.appmana
ace865b2-9154-4b48-add0-e34d3eed	. 6,754 KB	cllevent	03/03/2022 14:48	03/03/2022 14:48	data\data\com.microsoft.appmana
add	602,333 KB	pb	31/12/2008 15:00	31/12/2008 15:00	vendor\bin\add.pb
addb870e-d629-42ef-a45b-54deebc8	0 KB	cllevent	03/05/2022 13:18	03/05/2022 13:18	data\data\com.microsoft.appmana
additional_skipping_apk_list	241 KB	xml	31/12/2008 15:00	31/12/2008 15:00	system\etc\additional_skipping_ap

5. To view all files in the **same location** as any file displayed here, click the file path. The display files now displays the file that you clicked in its path (location) **AND** all files that are located in the **same** 

path/memory area and which are therefore likely to be associated with the file whose path you clicked.

😳 Cellebrite   UFI	ED			
Search by file name	٩		Total Items sele	ected: 22 (6.00 MB
- Name	▲ Size	Туре	Created	Modified
	1a0e68d1-49c1-4d53-926b-67ea8cae3 5,141 KB	cllevent	18/01/2022 01:12	18/01/2022 01:12
	1a32415d-31e3-4664-bab7-23ed50ae 5,144 KB	cllevent	13/12/2021 23:29	13/12/2021 23:29
	1a4437e7-2f2b-4173-95f4-b5542f804 0 KB	cllevent	18/01/2022 01:09	18/01/2022 01:09
	1a7fc686-839e-457f-afed-9378355e08 741 KB	cllevent	14/12/2021 01:27	14/12/2021 01:27
	1b0d1a22-6360-4d1b-8b75-e0afbf301 5,141 KB	cllevent	08/03/2022 15:37	08/03/2022 15:37
	1b160b5c-3359-4ef5-b830-645fb28f2c 5,141 KB	cllevent	15/02/2022 10:49	15/02/2022 10:49
	1bcb5ce8-24d8-4dc0-b1a0-01b1960bc 5,144 KB	cllevent	13/03/2022 15:50	13/03/2022 15:50
	1c06f79a-736a-4e20-81dc-27e252f68 0 KB	cllevent	15/12/2021 04:27	15/12/2021 04:27
	1c0d9f88-d189-4165-9e19-82eb618b0 5,141 KB	cllevent	07/03/2022 15:02	07/03/2022 15:02
	1c2ad8e5-e2e1-409e-a31c-add12d161 740 KB	cllevent	18/01/2022 01:29	18/01/2022 01:29
	1c4e2655-6d2d-4135-af31-b6898c26a 5,141 KB	cllevent	07/03/2022 13:59	07/03/2022 13:59
27,530 Items, 10.91 GB				
ABORT				EXTRACT

**Note**: In iOS, some files must **always** be selected as part of the extraction operation. Cellebrite pre-selects these files; they cannot be deselected.

a.) Your first click selects all the files.

b.) In iOS, a **second click returns the selections to the required files only** (see image above) - they remain selected always.

c.) When you move the mouse near the main checkbox, a tooltip displays with the following text:

*Cellebrite pre-selects some files that must be selected as part of the operation; these files cannot be deselected.* 

# 6.3. Android backup

The Android Backup feature communicates with a connected Android device and enables you to extract data from the device. The data that is extracted is dependent on the device's specific characteristics. Android backup supports Android devices with version 4.1 and higher.

Android Backup may provide less data then other methods, therefore, only use this feature when other file system methods such as ADB are not successful or when other file system methods are not available for the device (for example, if the Android version is not supported).

This feature is controlled under **Settings** > **General**.

### To extract data using Android backup:

1. Click **Mobile device** and identify the device, then click **File System**.

SELECT MODE			0	Ċ
Samsung GSM SM-J250 using Cable A with black tip	DF_DS Galaxy J2 2018 o T-100			
File System Boot Loader (Recommended) Lock Bypass	1 Android Backup	1 Android Backup APK Downgrade		
ABORT			ВАСК	

- 2. Click Android Backup.
- 3. Select the extraction location.

For information about using optional timeframe and party filters, refer to the *Overview Guide*.

4. Click **Continue**.

The Waiting for Device screen appears.



- 5. Connect the source device to the USB port. If the device is already connected, disconnect and then reconnect the device.
- 6. Click **Continue**. The following window appears.



7. Click **Continue** and if required select **Backup my data** on the device. The extraction begins.



The following screen appears.



8. Click **No** if you do not want to extract data from a shared location. Click **Yes** if you want to try extract data from a shared location. With a shared location, Cellebrite UFED extracts all the applications (native and non-native) that reside on the device, as well as data from the device's internal storage and memory card (images, videos, etc.), which takes additional time.

The following screen appears.

Device Instructions	
<b>GT-i9205 Samsung Galaxy Mega 6.3:</b> Please return the Screen timeout to its original settings: Menu (Apps) $\rightarrow$ Settings $\rightarrow$ My Device $\rightarrow$ Display $\rightarrow$ Screen timeout. or Menu (Apps) $\rightarrow$ Settings $\rightarrow$ Display $\rightarrow$ Screen timeout. or Menu (Apps) $\rightarrow$ Settings $\rightarrow$ Display $\rightarrow$ Sleep.	
	ОК

9. Follow the instructions and click OK.

When the extraction completes the Extraction summary window appears.

EXTRACTION SUMMARY	?	Ċ	
Extraction completed successfully			
Source: GT-i9205 Samsung Galaxy Mega 6.3 Target: Local Drive (FileSystem Android Backup 01)			
Open with UFED Physical Analyzer			
Extracted Apps			
OPEN   ADDITIONAL EXTRACTIONS	FINISH		

10. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

## 6.3.1. Extracted apps

The App information window can be displayed by clicking the **Extracted Apps** button after the File system Android backup extraction completes.

It displays the apps extraction status for the device. Apps that were extracted are listed under **Extracted**. These apps are decrypted in Physical Analyzer. Apps that could not be extracted are listed under **Not Extracted** and indicates the reason the apps were not extracted. The Notes indicate if another extraction method is applicable. Unrecognized apps and their status are listed under **Unrecognized**. This list contains files that could not be mapped by the system and exist for extraction results verification. To obtain more information about these files, we recommend that you do an Internet search for the file names.

App information			×
Extracted	Not Extracted	Unrecognized	
Name	Note		
Bluetooth	Yes		
Calendar (com.android.calendar)	Yes		
Chrome Browser - Google	Yes		
Contacts	Yes		
Screensaver	Yes		
Stock Email	Yes		
HTML Viewer	Yes		
Messaging	Yes		
Audio Equalizer	Yes		
Live Wallpaper (com.android.noisefield)	Yes		
Wallpaper	Yes		
Dialer	Yes		
Calendar Storage	Yes		
Download Manager	Yes		
Downloads	Yes		
Media Storage	Yes		
Settings Storage	Yes		
		MORE INFO	

# 6.4. Android backup APK downgrade

This method extracts application data using Android backup. It supports Android devices with version 4.1 and higher. During the process, the selected application version (\*.apk file) is temporary downgraded to an earlier version, so that the data can be extracted. The current version is restored at the end of the extraction process. The potential risk in this method relates to the downgrading and then restoration of the app version.

Only use the Android Backup APK Downgrade method as a last resort after other extraction methods have been exhausted (including JTAG and chip-off).

We recommend that you document the process during the extraction.

### To extract data using Android backup APK downgrade:

1. Click **Mobile device** and identify the device, then click **File System**. The following window appears.



2. Click Android Backup APK Downgrade. The following window appears.

Android Backup APK Downgra	ade			
The Android Backup APK Downgrade method should be used as a last resort after the other extraction methods have been exhausted (including JTAG and chip-off). Are you sure you want to continue?				
This method extracts application data using Android backup. During the process, the selected application (*.apk file) is temporarily downgraded to an earlier version, so that the data can be extracted. The current version is restored at the end of the extraction process. Some non-user data may be deleted during the downgrade.				
	CANCEL			

3. Click **Continue**.



For information about using optional timeframe and party filters, refer to the *Overview Guide*.

4. Select the target path and click **Next**. The Waiting for Device screen appears.



- 5. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device.
- 6. Follow the on-screen instructions for the device and then click **Continue**. The following screen appears.



You are notified when you are required to restart the device or to select **Backup my data** on the device. The following screen appears.

The following window appears.

elect apps:	
	Type to search Q
Dropbox	Facebook Mess LINE Telegram
Twitter	Wickr
Cancel	Select All Start

7. Select the required apps (or click **Select All**) and then click **Start**. The following window appears.

EXTRACTION IN PROGRESS	(?)	Ċ
Huawei EVA-L19 P9 using USB cable 170 or Original Cable		
Please wait, this can take some time		
Connecting		

8. Select **Backup my data** on the device. The following window appears.

Android backup				
Would you like to try data extraction from a shared location? The system will attempt to extract data from the device's internal storage and memory card and will take additional time.				
	NO	YES		

9. Click No if you do not want to extract data from a shared location. Click Yes if you want to try extract data from a shared location. With a shared location, Cellebrite UFED extracts all the applications (native and non-native) that reside on the device, as well as data from the device's internal storage and memory card (images, videos, etc.), which takes additional time.

If some app packages could not be backed up, this screen provides an indication of how many app packages were backed up successfully.

10. Click **Continue**. The following screen appears.



11. Follow the instructions and click OK. The Extraction summary window appears.



12. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

## 6.4.1. Installing the latest APK version

During the Android backup APK downgrade extraction the following notification appears if you have not installed the latest APK version. The new APK version enables support for additional apps.

ø	Setup - UFED 4PC —	
	Android backup APK downgrade New APK for apps	ं Cellebrite
	A new APK version is available for the following apps: Baidu, ChatON, Evernote, FireChat, Gmail/Inbox, Hangouts, Keep Safe (Kii Safe), Kik Messenger, Ping Chat, QQ browser, QQ messenger, Signal Private Messenger / TextSecure, Tango, Text Free Ultra Texting, Text Me, TextNow, TextPlus, Threema, TigerText, Tinder, Viber, Vkontakte, Voxer, Whisper, Yandex Mail. To download the APK, go to my.cellebrite.com > Downloads and search for the APK under the product (UFED Touch2/UFED Touch/UFED 4PC/UFED InField) Software section. Install via Settings > Version > File	
	APK Download Next >	

### To download and install the latest APK version:

- 1. Go to MyCellebrite and log in with your credentials (or create an account).
- 2. Click **Downloads**.
- 3. Search for the APK under the Cellebrite UFED Software.

cellebrite delivering mobile expertise				🖸 Go to Technical Support
	Home	My Products	Downloads	UFED Phone Detective
Downloads				
Search				
UFED				
La Software -				
Documentation				
Archive				
Release Notes				

- 4. Download the APK Downgrade Pack and save it on the computer or to a USB drive.
- 5. In Cellebrite UFED, install the APK via **Settings** > **Version** > **File**.

# 7. Physical extraction

The **Physical Extraction** function enables you to perform a physical bit-for-bit image of the source device memory to a removable storage device or PC.

UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: <u>https://www.cellebritAxon</u> <u>Evidence/en/services/advanced-unlocking-services/</u>

ð

Ē)

Lock Bypass is displayed if the physical extraction method can bypass the user lock of the device.

# 7.1. Performing a physical extraction

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears.

SELECT MODE		0	Ċ
Samsung GSM GT-i92 using Cable A with black	05 Samsung Galaxy Mega 6.3 tip T-100		
ADB	Boot Loader (Legacy)     Lock Bypass		
ABORT		ВАСК	

- 2. Click ADB or Boot Loader (Legacy).
  - \* ADB: Android Debug Bridge (ADB) is a built-in communication mechanism that allows device debugging. With this extraction method, you can perform a physical or file system extraction, provided that the device's USB debugging option is enabled. If the device is not already rooted, UFED attempts to temporarily gain the permissions required for the extraction. In some cases, data from a memory card is extracted; however, we recommend that you read the card with an external memory card reader.
  - Boot Loader: An extraction method that performs a physical extraction when the device is in bootloader mode. With this extraction, the operating system is not running, so the device cannot connect to the mobile network. It bypasses any user lock and is forensically sound. The bootloader extraction does not support extractions from a memory card.

For information about using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location screen appears.



3. Click Next.

Depending on whether or not the device requires the UFED Device Adapter, the Waiting for Device or Waiting for Device Adapter screen appears.

WAITING FOR DEVICE	?	Ċ			
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100					
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconne	ect the device.				
Android 4.2 and Higher 4.1.2 and Lower a Tutorial Video 1. Enable Developer options How to? 2. Enable Stay awake and USB debugging modes How to? 3. Verify screen lock mode How to? 4. Connect the device to the unt.					
ABORT BACK CONSOLE	CONTIN	UE			

- 4. Do the following:
  - a. Select the correct cable and tip for the mobile device based on the instruction on the screen.
  - b. Change the device settings according to the instructions.
  - c. Connect the device to the PC.

If the device requires the UFED Device Adapter to perform the extraction:

<sup>\*</sup> Connect the UFED Device Adapter to a USB port on the computer.

The source port on the UFED Device Adapter flashes.

- » Connect the device to the UFED Device Adapter.
- 5. Click **Continue**. The Extraction in Progress screen appears.

Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100
Please wait, this can take some time
bk0_mmcblk0.bin 1/1 Time Remaining: 00:14:01
ABORT

6. Follow any on-screen instructions.

For some devices, an estimation of the time the extraction will take is displayed: For example, Blackberry, Nokia BB5, QCP (SamM550, LgEmergency, LgP0), Android, (generic and SPF), SpreadTrum, Samsung GSM (MTK, LGInfinion, and BCM2133), and Palm.

When the extraction completes, the Extraction summary window appears.

EXTRACTION SUMMARY		0	ப
Extraction completed successful	ly		
Open with UFED Physical Analyzer	Source: GT-i9205 Samsung Galaxy Mega 6.3 Target: Local Drive (Physical ADB 01)		
Show in Polaer	ADDITIONAL EXTRACTIONS	FINISI	н

7. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where

Additional Extractions to add additional extraction types for the same device, or click Finish to end the process and return to the Home screen.

### If the system cannot connect to the device:

<sup>\*</sup> The following window appears with an error message.

Cannot connect to device (13) GT-i9205 Samsung Galaxy Mega 6.3: * If the device has an SD card slot, insert an SD card and restart the * Please disable "Stay awake" option if it was enabled. General recovery steps:	extraction.	
<ul> <li>Make sure the phone displays the main screen</li> <li>Check the cable number</li> <li>Check that the cable connectors are well cleaned</li> <li>Replace the connecting cable</li> </ul>		
To allow phone connection:		
Battery should be fully charged.		
<ol> <li>Power on the phone and wait until it's fully booted</li> <li>* Only unlocked phones are supported.</li> <li>Set up phone's connectivity as follows:</li> </ol>		
	ABORT	RETRY

\* Follow the instructions on the screen and click **Retry**.

### 7.1.1. The Physical extraction folder

At the end of the physical extraction process, the extracted data is saved in the location you selected during the physical extraction process.

The extracted data folder is named **Physical** with the selected device name and the extraction operation date. For example, **Physical Samsung GSM SGH-A711** 2011\_06\_12 (001)

The extracted data folder contains:

- \* Binary file of the device memory.
- » UFD file containing the system extraction information, used by the Physical Analyzer application.

The extraction information can be viewed using the Physical Analyzer. You can double click on the UDF file or open it via the GUI.

# 7.2. ADB rooted

The ADB method for Android rooted devices can be used when the physical extraction method is not supported. Using the ADB method, you can perform a physical extraction from rooted Android devices. This extraction method is for pre-rooted devices only, and does not root the device. To *root* a device means to gain administrative rights on the file system.

A device can be rooted as part of recovery partition or fully rooted following a rooting procedure. We recommend that you do not root the device; however, if there is no other option, use this method.

### To perform a physical extraction for a rooted Android device:

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears.

SELECT MODE			0	Ċ
Samsung GSM SM-G5 using Cable A with black t	30AZ Galaxy Grand Prime ip T-100			
Advanced ADB (Generic)	ADB (Rooted)	Boot Loader (Legacy)	EDL ADB	1
ABORT			BACK	(

2. Click ADB (Rooted).

For information about using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location screen appears.

SELECT EXTRACTION LOCATION	?	Ċ
Samsung GSM SM-G530AZ Galaxy Grand Prime using Cable A with black tip T-100		
Extraction to Local Drive		
C:\Users\jonathank\AppData\Local\My 📋		
ABORT BACK	NEXT	

3. Click **Next**. The following window appears.

Depending on whether or not the device requires the UFED Device Adapter, the Waiting for Device or Waiting for Device Adapter screen appears.

WAITING FOR DEVICE			?	Ċ		
Samsung GSM SM-G530AZ Galaxy Grand Prime using Cable A with black tip T-100						
Connect the source device to the USB port on the computer. If the device is a	Iready connected, disc	onnect and then reconnect the	e device.			
Android 4.2 and Higher 4.1.2 and Lower	B Tutorial Video					
1. Enable Developer options <u>How to?</u> 2. Enable Stay awake and USB debugging modes <u>How to?</u> 3. Verify screen lock mode <u>How to?</u> 4. Connect the device to the unt.						
ABORT	ВАСК	CONSOLE	CONTIN	UE		

- 4. Do the following:
  - a. Select the correct cable and tip for the mobile device based on the instruction on the screen.
  - b. Change the device settings according to the instructions.
  - c. Connect the device to the PC.

If the device requires the UFED Device Adapter to perform the extraction:

<sup>\*</sup> Connect the UFED Device Adapter to a USB port on the computer.

The source port on the UFED Device Adapter flashes.

- \* Connect the device to the UFED Device Adapter.
- 5. Click **Continue**.

The Extraction in Progress screen appears.

EXTRACTION IN PROGRESS	?	Ċ
Samsung GSM SM-G530AZ Galaxy Grand Prime using Cable A with black tip T-100		
Please wait, this can take some time		
blk0_mmcblk0.bin 1/1 Time Remaining: 00:15:01		
ABORT		

- 6. Follow any on-screen instructions.
- 7. When the extraction is complete, the Extraction summary screen appears.



8. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

# 7.3. Advanced ADB

Advanced ADB extraction enables physical extraction of data from additional devices. This method supports devices with Android operating systems up to version 7.1, on devices with a security patch level up to November 2016, including Galaxy S7, Galaxy Note 5, LG G5, V20, and Nexus devices.



Due to the widely fragmented variance in Android devices, exceptions may apply.

ð

To avoid any interruptions during the extraction, the device must be placed in Airplane mode.

### Before performing an Advanced ADB extraction:

- 1. Make sure the source device is fully charged.
- 2. Prepare a target storage device on which to save the extraction file. This target can be either a USB mass storage device (connected via OTG cable 501 or 508), or an SD memory card.
  - The target storage device must have FAT32, vFAT, or exFAT format and have sufficient space for the extraction.
  - <sup>\*</sup> If a USB drive is selected for the target storage, make sure you have an available OTG cable for the extraction: OTG cable 501 (micro USB connector) or cable 508 (type C connector).



If an SD card is selected for the target storage, place it in the Android device now.

The SD card must be blank and not contain any case evidence.

If the card port location is under the device's battery, restarting may relock a device that was locked before. Therefore, for devices with OTG support, we recommend using a USB drive for the target storage.

### To perform an Advanced ADB extraction:

SELECT EXTRACTION TYPE			0 U
Samsung GSM GT-i92 using Cable A with black	05 Samsung Galaxy Mega ( tip T-100	5.3	
Logical	Disable/Re-Enable User Lock	File system	Physical
Camera	Screenshot		
ABORT			ВАСК

1. From the Home screen, detect the relevant device automatically. The following window appears.

If the relevant model is not listed, browse manually for a generic Android model. See <u>Generic model (on page 144)</u>.

2. Click Physical.

The Select Mode screen appears.

3. Click Advanced ADB.



For information about using optional timeframe and party filters, refer to the *Overview Guide*.

- 4. Follow the instructions to set up device connectivity.
- 5. On the source device, perform the following steps:
  - a. On an Android OS 4.3 and above, Go to **Menu (Apps)** > **Settings (More)** > **Security** and clear the Verify apps setting. Approve any pop-ups that may appear.
  - b. Go to Menu (Apps) > Settings (More) > About (Software information) > More, and tap the Build number 7 times until developer options are enabled.
  - c. Go to **Development settings** and enable USB debugging.
  - d. Connect the source device to the cable described in UFED.
  - e. A notification is added to the notification dropdown. Allow MTP and PTP on the device.
- 6. On the UFED screen, click **Continue**. The following window appears.

Warning				
Before you select the target storage: If the target storage is an SD card, place it in the device now. Reminder: Restarting may re-lock the device. For this reason a USB drive is recommended for the target storage.				
If the target device is not recognized by the Android device click "Help with storage format"				
SD CARD WAS INSERTED	MASS STORAGE	HELP WITH STORAGE FORMAT		

7. Click the relevant target storage. The following window appears.





If requested, you should only approve the installation of apps.

UFED is installing the extraction app and attempting to temporarily gain the permissions required for the extraction. This stage can take approximately 20 minutes. During this process, the device screen appears.



When UFED has prepared the device, a window appears indicating that the device is ready for extraction. Disconnect the device from UFED and follow the instructions on the source device.

- 8. Click Continue.
- 9. Follow the instructions on the Android source device's screen. For a USB drive target, continue to the following step. For an SD card target, skip to the next step.
- 10. If a **USB drive target** was selected, the following screen appears.

۲		*	Ϋ́	ü	7:54
					1
OTG USB drive as target	was sele storage	ct	ed		
1. Disconnect the d and use the OTG ca the source device to	evice from U ble <sup>®</sup> to conn o the USB dri	IFE lect	D		
Micro US8 connects     S01.     US8 Type C connects	ctor - Use ca ector - Use ci	ble abl	e		
2. Select Continue.					
Cont					
Switch to	SD card				
Ab	ort				
< <	)	(			

- a. Follow the on-screen instructions:
  - i. Disconnect the device from UFED.
  - ii. Use the OTG cable to connect the source device to the USB drive.



- b. Skip the SD card step.
- 11. If an SD card target was selected, the following screen appears.

A 🛎		*12	B 7:54
			-
SD card	was selected storage	l as targe	t I
1. Disconr 2. Select ( ready.	nect the cable fro Continue if the de	om UFED. wice is	
Important not yet ins the device re-lock a before. To avoid a extraction	If the target SD erted and is loca 's battery, restart fevice that was k iny harm to the e failure switch to	o card is ated under ting may ocked vidence or USB drive.	
5	witch to USB dri	ve	
	Abort		
	V1.0.7		
$\bigtriangledown$	0		

- a. Follow the on-screen instructions:
  - i. Disconnect the device from UFED.
  - ii. If the target SD card is not yet inserted and is located under the device's battery, restarting may relock a device that was locked before. To avoid an extraction failure (for devices with OTG support), select **Switch to USB drive**.

Reminder: This target device requires a FAT32\*, vFAT, or exFAT format SD card with sufficient space for the extraction.



12. Select **Continue**. The reading process begins.



When the extraction is successfully completed, the following screen appears.



13. Select **Exit** to uninstall the extraction app without restarting the device, or select **Restart** to uninstall the extraction app and return the device to its normal functionality.



- 14. Return to UFED.
- 15. Follow the on-screen instructions on the source device. When the extraction completes click **Extraction failed**, **Extraction successful** or **Abort** to update the extraction Activity log.
- 16. Click the relevant extraction status to update the extraction Activity log.
- 17. Follow the instructions and click **Finish**.

# 7.3.1. Generic model

### To perform an Advanced ADB extraction:

1. From the Home screen, click Skip > Vendors (tab) and search for Smart Phones. The following window appears.



2. Click Smart Phones. The following window appears.

C UFED 4PC 0.0.1.1170			
Search in Smart Phones/PD/	As Q Search By: Name		<sup>(1)</sup> (1)
Smart Phones/PDAs Android	Smart Phones/PDAs Android Bluetooth	Smart Phones/PDAs Android Bluetooth Fast Phonebook	Smart Phones/PDAs BlackBerry BlackBerry
Smart Phones/PDAs BlackBerry 10 BlackBerry	Smart Phones/PDAs Coolsand	Smart Phones/PDAs Decrypting LG MTK	Smart Phones/PDAs Decrypting MTK
Smart Phones/PDAs Decrypting Qualcomm	Smart Phones/PDAs MS Pocket PC 2003 Windows Mobile	Smart Phones/PDAs MS SmartPhone 2003 Windows Mobile	Smart Phones/PDAs MS Windows Mobile 5 Windows Windows
ABORT			BACK

3. Click the relevant model. The following window appears.



- 4. Click Physical.
- 5. Continue with the extraction.
- 6. To continue, refer to Advanced ADB (on page 136).
## 7.3.2. Errors and notifications

### 7.3.2.1. Disk format error

#### **Storage Format**

To format the target storage you can use your Android device or your PC.

From the Android device: SD card - Insert the SD card in the relevant slot of the Android device now. USB drive - Connect the USB drive via the OTG cable to the Android device now.

Open the Android device notification drop-down and select the USB message or go to device portable storage settings and follow the instructions to

or go to device portable storage settings and follow the instructions to erase

and format the device.

From your PC:

Plug the target device into your Windows PC. Right-click the storage drive and select "Format...". In the format window, under File system, select exFat. Click "Start" and complete the format process.

STORAGE IS FORMATTED

If you receive this error message, follow the instructions listed in the error message.

To format the storage device from the Android device:

1. Open notification.



2. Select the **Corrupted USB drive** notification. The following screen appears.



3. Follow the instructions to erase and format the device. Upon completion, the following screen appears.



## To format the storage device from the PC:

1. Plug the hard drive into your Windows PC. Right-click on the D drive and select **Format** The following window appears.

Format My Passport (D:)	×
Capacity:	
465 GB	•
File system	
exFAT	•
Allocation unit size	
128 kilobytes	-
Volume label	
My Passport	
Format options Quick Format Create an MS-DOS startup disk	¢
Start	Close

- 2. Under File System, select exFAT.
- 3. Click **Start** and complete the format process.

### 7.3.2.1.1. Extraction aborted

If **Abort** was selected during the extraction process, the screen on the left appears. After some time (up to a few minutes) the screen on the right appears.



<sup>»</sup> Select **Exit** to uninstall the extraction app without restarting the device.

The device only returns to normal functionality after a restart.

Select **Restart** to uninstall the extraction app and return the device to its normal functionality.



Ē)

Restarting may relock a device that was locked before.

### 7.3.2.1.2. Extraction failed

If the extraction failed for any reason, the following screen appears with the failure reason.



<sup>»</sup> Select **Exit** to uninstall the extraction app without restarting the device.



The device only returns to normal functionality after restart.

Select **Restart** to uninstall the extraction app and return the device to its normal functionality.



Restarting may relock a device that was locked before.

# 7.4. Boot loader (FW flashing)

The Boot loader (FW flashing) extraction method uses boot loader reflashing, which enables a physical extraction while bypassing user lock (non-secure startup). This method is for Qualcomm-based Samsung Galaxy S7 devices running firmware version of Android 7.x. For a complete list of supported devices, refer to UFED Supported Devices document in <u>MyCellebrite</u>. This extraction does not support extractions from a memory card.

This Boot loader (FW flashing) extraction method requires the device's firmware to be flashed. In some cases the device may experience unexpected behavior and you must flash the original device firmware, which causes a device wipe. Before using this method, we recommend trying other Physical bootloader methods.

### To perform Boot loader (FW flashing):

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears.



2. Select Boot loader (FW Flashing).

For information about using optional timeframe and party filters, refer to the *Overview Guide*.

The following Select extraction location window appears.



3. Select the extraction location. Click **Next**. The Waiting for Device screen appears.

WAITING FOR DEVICE			0	Ċ
Samsung CDMA SM-G930V Galaxy S7 using Cable A with black tip T-100				
Connect the source device to the USB port on the computer. If the device is all	ready connected, dis	connect and then reconne	ect the device.	
<ul> <li>SM-6930V Galaxy 57:</li> <li>Note: This method is supported for devices running Android OS up to and including Android OS 80 and above is not supported and bootloop issues may occur. To allow device connection:</li> <li>Note: The device battery should be fully charged.</li> <li>1. Turn off the device.</li> <li>2. Press and hold the Volume down, Home and Power buttons until the device entt 3. Select "Continue" by pressing the Volume up button.</li> <li>4. Wait until the Download mode logo appears on the device screen, and then cont 5. Connect the cable to UFED 4PC.</li> <li>6. Select "Continue".</li> <li>If a password is required to turn the device off, remove and re-insert the battery. If the device does not have a removable battery, perform the following steps:</li> <li>I. Restart the device by pressing the Power and Volume down buttons. When the buttons.</li> <li>b. When the device displays the Recovery mode screen, release the Volume up, c. Wait for the Recovery menu to be displayed (this can take several minutes).</li> <li>J. Select Power off, then press the Power button to turn off the device.</li> <li>Note: Use the Volume up and Volume down buttons to navigate the Recovery menu</li> </ul>	g 7.1.1. ers Download mode. nect the device to the e device restarts, quid Home and Power but! nu.	: cable. :kly press and hold the Volu tons.	ime up, Home an	id Power
ABORT	BACK	CONSOLE		

- 4. Follow the on-screen instructions to place the device in Download mode, then connect the required cable to the device and UFED.
- 5. Click **Continue**. The following window appears.

Attention		
This method requires the device's f In some cases the device may expe need to flash the original device fir Before using this method, we recor methods.	irmware to be flashe rience unexpected b mware, which cause nmend trying other	ed. ehavior and you will s a device wipe. Physical bootloader
	ABORT	CONTINUE

6. Click **Continue** to flash the device's firmware. The following window appears.



- 7. Follow the on-screen instructions to place the device in Download mode again, then connect the required cable to the device and UFED.
- 8. Click **Continue**. The following window appears.

Attention
During device exploitation, UFED will temporarily corrupt the device's recovery partition (leaving the user data partition untouched). Upon success, UFED will immediately restore the recovery partition to its previous state, and follow to produce the physical extraction. In the unexpected case of failure, the device may be left in a state where it can operate and boot normally into Android, but without the capability to boot into recovery mode until the recovery partition is re-flashed with any original (carrier) or alternative (e.g. TWRP) recovery image. In such cases where restoring recovery capability is required, the operator is instructed to obtain a matching recovery image and flash it using the standard Odin tool. Continue extraction?
ABORT CONTINUE

9. Click **Continue**. The Extraction in Progress window appears.



10. Follow any on-screen instructions.

When the extraction completes, the Extraction completed successfully window appears.

11. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

# 7.5. Decrypting boot loader

This extraction method performs a physical extraction on encrypted Android devices with the following Qualcomm chipsets: 8909, 8916, 8939, 8952, and 8396. It performs the extraction when the device is in boot loader mode. It bypasses the user lock and is forensically sound.

#### To perform a Decrypting boot loader extraction:

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode window appears.

SELECT MODE			?	Ċ
Alcatel 6055U One Touch using Cable A with black tip	1 Idol 4 T-100			
Advanced ADB	ADB (Rooted)	Decrypting Boot Loader (Recommended) Lock Bypass		
ABORT			BACK	

2. Click Decrypting Boot Loader.

For information about using optional timeframe and party filters, refer to the *Overview Guide*.

The Select Extraction Location window appears.

3. Select the extraction location. Click **Next**. The Waiting for Device window appears.



4. Follow the on-screen instructions to place the device in the required mode. Click **Continue** when enabled.



5. Disconnect the device from UFED, enter the specified mode again (for example, key combination, EDL cable etc.) using the previous instructions, and then click **Continue**. The following window appears.

EXTRACTION IN PROGRESS	?	Ċ
Alcatel 6055U One Touch Idol 4 using Cable A with black tip T-100		
Please wait, this can take some time		
Connecting		

When the extraction completes, the Extraction completed successfully window appears.

6. Click Open Preview Report to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click Open with Physical Analyzer to open the extraction in Physical Analyzer, click Show in Folder to open the folder where the UFD extraction file is located, click Additional Extractions to add additional extraction types for the same device, or click Finish to end the process and return to the Home screen.

# 7.6. Forensic recovery partition

An extraction method that performs a physical extraction while the device is in recovery mode. UFED replaces the device's original recovery partition with Cellebrite's custom forensic recovery partition. The original recovery partition on the Android device can be considered as an alternative boot partition that may also change the user data, while Cellebrite's recovery partition does not affect any of the user data. This extraction method bypasses the user lock from several Samsung Android devices and is forensically sound. It does not support extractions from a memory or SIM card.

For a complete list of supported devices, refer to the UFED Phone Detective Mobile App or the UFED Supported Devices document in MyCellebrite.

We recommend that you use the Forensic recovery partition method when other physical extraction methods (e.g., Bootloader) are not successful, or not available (e.g., if the Android firmware version is not supported).

If the device does not start correctly after using this extraction method, use the Exit Android Recovery Mode device tool. See Exit Android recovery mode (on page 201).

#### To perform a forensic recovery partition extraction:

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears.

SELECT MODE			<sup>(1)</sup> (2)	
Samsung GSM SM-G9 using Cable A with black t	00H Galaxy S5 tip T-100			
Advanced ADB (Generic)	ADB (Rooted)	forensic Recovery Partition Lock Bypass		
ABORT			ВАСК	

2. Select Forensic Recovery Partition.



For information about using optional timeframe and party filters, refer to the *Overview Guide*.

#### The following screen appears.

	Samsung GSM » SM-G900H Galaxy SS » Physical Extraction » Select Extraction Location
Source	Target
Samsung GSM SM-	Current path:
G900H Galaxy S5 using Cable A with black tip T-100	S\Documents\My UFED Extractions Change target path
	Next

3. Click Next.

Depending on whether or not the device requires the UFED Device Adapter, the Waiting for Device or Waiting for Device Adapter screen appears.



The Waiting for Device screen appears.



4. Click **Continue**. The following warning is displayed.

Attention
This method replaces the recovery partition on the device in order to extract user data. For the recovery partition to function correctly, do not disconnect the device until the extraction completes. Warning: This method activates the Samsung KNOX warranty bit on the device. This permanently voids the warranty and prevents further access to data stored in KNOX containers.
CONTINUE ABORT

5. Click **Continue**. The device is placed in download mode. The following screen appears.

Attention		
Make sure that the device from which you are trying to extract data is identical to the model you selected in the UFED menu: SM-G900H		
Follow these steps to place the device in download mode:		
<ol> <li>Disconnect the device from UFED.</li> <li>Shut down the device.</li> <li>Press and hold the Volume down + displays the boot menu.</li> <li>Press the Volume up button.</li> <li>Connect the cable to the device.</li> <li>Connect the cable to UFED.</li> </ol>	PWR + Home buttons until the device	
	CONTINUE ABORT	

6. Click **Continue**. The following screen appears.



- 7. Click **Continue**. The following screen appears.
- 8. Follow the instructions to place the device in Download mode. Force it to restart by pressing the Power and Volume down buttons. When the device restarts, quickly press the Volume up, Home and Power buttons. Click **Continue** when **Downloading** appears on the device's screen (this can take a few minutes).

The Extraction in Progress screen appears.

70 UFED 4PC 0.0.1.1170	-	□ ×
EXTRACTION IN PROGRESS	?	Ċ
Samsung GSM SM-G900H Galaxy S5 using Cable A with black tip T-100		
Please wait, this can take some time		
Connecting		
ABORT		

9. Follow any on-screen instructions.

When the extraction completes, the Extraction completed successfully window appears.

10. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

# 7.7. Smart ADB

The Smart ADB extraction method enables you to perform physical extractions on Android devices that include the November 2016 security patch. This method is supported by OTG compatible devices, with OS versions 6.0 and above. Only security unlocked devices are supported.



On some devices, you may need to enable the OTG option.



We recommend that you place the device in Flight mode.

ð

If a specific device is not supported, we recommend that you use a similar model or any generic Advanced ADB profile.

#### To perform a Smart ADB extraction:

1. Click **Mobile device** and identify the device, then click **Physical**.

The Select Mode screen appears.

SELECT MODE		0 U
LG GSM LGMP450 Stylo 3 using Cable A with black tip	3 Plus T-100	
ADB (Rooted)	Smart ADB (Recommended)	
ABORT		ВАСК

2. Click Smart ADB.

For information about using optional timeframe and party filters, refer to the *Overview Guide*.

The Waiting for Device screen appears.



3. Follow the on-screen instructions then click **Continue**. The following window appears.

Attention
UFED will now try to flash another image to the device. Press and hold the Volume down, Power and Home (or Bixby) buttons, until the device displays the Warning screen. Then press Volume up and select "Continue" in UFED.
CONTINUE

4. Click **Continue**. The following window appears.

Process complete							
Disconnect the device and connect Cable No. 500 (side A) to UFED. Note: If required, this process flashes new firmware to the cable. You can also use "Tools" > "Flash Cable 500 Firmware".							
	ABORT	CONTINUE					

5. Disconnect the device and connect Cable No. 500 (side A) to UFED, then click **Continue**.

The initializing stage can take up to 30 minutes.
If required, this process flashes new firmware to the cable. You can also use the Flash Cable 500 Firmware (on page 204) tool.

The following window appears.



6. Connect Cable No. 501 (or other specified cable) to the device and the other end of the cable to Cable No. 500, then click **Continue**. The initialization process starts.

The following window appears.



7. Disconnect Cable No. 500 and reconnect the device using Cable No. 100 (or other specified cable). Click **Continue** to start the extraction. The following window appears.

EXTRACTION IN PROGRESS	0	Ċ
LG GSM LGL83BL Stylo 3 using Cable A with black tip T-100		
Please wait, this can take some time		

When the extraction completes, the Extraction completed successfully window appears. If Cellebrite UFED could not find a setting for the specific device, UFED can attempt other potential settings. This process requires user interaction and takes time to complete.

8. Click **Continue** to try the extraction with other settings. The following window appears.

Attention		
Completed attempt 1/3 with settin Retrying with current setting. Disconnect the cables, and connec	g number 1. t the device to UFED	) with Cable No. 100.
	ABORT	RETRY

9. Disconnect the cables and connect the device to UFED with Cable No. 100 (or specified cable), then click **Retry**.

When the extraction completes, the Extraction completed successfully window appears.

10. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

# 8. Extracting Android devices

This chapter covers the pros and cons of each Android extraction method, and provides answers to frequently asked questions about the extraction methods.

## 8.1. Android extraction methods

Many different devices run the Android operating system: phones, MP3 players, tablets, eBook Readers, and more.

There are two main extraction methods for Android devices:

- \* ADB debugging extraction using a built-in protocol that runs within the operating system. This method uses the Android Debugging Bridge (ADB), which is active when USB Debugging is enabled. Using this method, you can perform a physical or file system extraction on almost any Android device, provided that device USB debugging is enabled. All currently available Android OS versions are supported. For more information, see <u>Android debugging bridge method (below)</u>.
- Bootloader extraction extraction that takes place before the Android operating system starts running (several variations of this method are available). This method can be performed on locked devices. For more information, see <u>Bootloader extraction (on</u> <u>page 170)</u>.

## 8.1.1. Android debugging bridge method

#### Q: How does ADB work?

**A**: ADB is a built-in protocol within the Android operating system. Every Android-based device has this protocol, which enables developers to connect to an Android-based device and perform low-level commands used for development. Cellebrite utilizes this protocol to extract data from Android devices.

#### Q: Can ADB be used to extract any Android device?

A: In theory, data can be extracted from every Android device using ADB. However, there are some limitations:

- \* USB debugging must be enabled on the device
- » Access to the device must be with administrator permissions.

#### Q: How do I turn on USB debugging?

A: On most Android devices: go to Menu > Settings > Applications > Development and then click USB debugging.

#### Q: Does this method bypass the unlock password or pattern? Will I be able to retrieve the code?

A: Device USB debugging must be turned on before it is possible to attempt an extraction. For locked devices, you can perform an extraction if the user enabled USB debugging before locking the device.

For selected Android devices, you can perform a physical extraction, where there is greater support for extraction from locked devices (pattern lock, PIN, or password). Following a successful physical extraction, you can view the numeric password or pattern lock protecting the device in Physical Analyzer, and use it to unlock the device.

#### Q: How do I get Administrator (root) permissions on the device?

**A**: When USB debugging enabled, Cellebrite UFED automatically detects the Android OS version, and whether or not access is at administrator level. If it is not, Cellebrite UFED automatically gains root permissions.

You can gain access at administrator level manually using third-party tools, but gaining access this way may harm the integrity of the data on the device, or has the potential to render the device useless.

#### Q: I turned on USB debugging. What extraction types can I perform?

**A**: If USB debugging is enabled, you can perform either a physical extraction which extracts all the data on the device, or a File System Extraction which extracts only relevant files.

The advantage of a physical extraction is that it retrieves more data from the device, making it possible to recover deleted files such as photos that were saved on the device. The disadvantage is that it takes more time, and that file system reconstruction is not supported for all devices.

The advantage of a file system extraction is that it takes less time. You are able to view all vital information including deleted records (but excluding deleted files), even if file system reconstruction is not supported.

# Q: When selecting the Generic Profile on Cellebrite UFED, what are Method 1 and Method 2? Which should I choose?

**A**: Methods 1 and 2 are different connection configurations. You cannot tell which Android devices requires which method. Try one method, and if unsuccessful, try the second method.

#### Q: Does the ADB extraction method change any of the data on the device?

A: When extracting using the ADB method, a few client applications are written to the device /data/local/tmp folder.

## 8.1.2. Bootloader extraction

#### Q: What is bootloader extraction?

A: The bootloader extraction method performs a physical extraction when the device is in bootloader mode. In this extraction method, the Android operating system is not running, so the device cannot connect to the mobile network.

#### Q: Does this method bypass the unlock password or pattern? Will I be able to retrieve the code?

A: Using this method, you are able to bypass any type of lock, and can retrieve a numeric PIN lock or unlock pattern.

#### Q: Does this extraction method change any of the data on the device?

A: No, this method is completely forensically sound.

#### Q: Which devices are supported by this method?

A: Currently most Motorola Android devices, and selected Samsung Android, Qualcomm, LG GSM, and LG CDMA are supported.

### 8.1.3. smartStopping an extraction

You can now stop Android File System extractions (not including Android Backup and APK downgrades) before they complete and save the (partial) extraction to that point.

 To stop an extraction in progress, clickthe STOP button in the screen labeled "Extraction in progress".

A confirmation message displays.

Click "Stop Extraction" (the exact wording might change).
 The extraction procedure will finish extracting the current file and stop.

EXTRACTION IN PROGRESS	<b>ф</b> (U)
USING CABLE A WITH BLACK TIP T-100	
Please wait, this can take a few minutes	
4 out of 100 16%	
ABORT STOP BACK	NEXT

EXTRACTION IN PROGRESS		<b>\$</b> ()
Stop extraction 4 3 5 TOP EXTRACTION	extraction?	

The partial extraction can be opened in Physical Analyzer.

16 UPED 7.54.0.504				
	EXTRACTION SUMMARY	0	é	
[	Extraction partially completed - stopped by user			
	Source: XT1754 Moto C Target: Local Drive (FileSystem MTK Live 01)			

A message stating that the extraction is partial and was stopped by the user displays in Physical Analyzer v7.54 and above.

<b>(</b>		View	Tools (	Cloud	Extract	Python	Plug-ins	Report	Help	Tips & Tricks					
វិន	O LG (	GSM_K430	н к10		**	Tips & Tric	ks 👘	Extraction S	Summary (1)	×					
0					1	All Conter	nt	File System							
Timeline	Analy	zed Data				Extracti	ion Sun	nmary					+ Add ext	traction	
~	› <b>::</b>	Application	1 (2667) <mark>(12</mark>				ons: 1								
Data	> 010	Devices &	Networks (4	9				File Syste	т // к430н к10		Image H	lashes			
밚	× ۹	Media (171	2)					File Syste	em [ Android AD oped by user!	8 ] 🖿	Calculating	hash			
File Systems	-	<ul> <li>Audio (152</li> <li>Images (15</li> </ul>	) 59) (1328 k	nown files)				Detraction 08/03/20	start date/time 022 14:17:01(UTC	- 2)	-		-		
.ġ:	•	Videos (1)						08/03/20	and date/time 022 14:26:47(UTC	+2)					
	Data f	files													
		Archives (3	6)			Device Info						Generate prei	liminary device report	ΘÎ	Content
R	۰	Configurat	ions (41)										and a second report	_	Data
		Databases	(2)			Android fing Detected Ph	perprint ione Model	lge/m253_glob LG-K430	bal_com/m253i6/	0/MRA58K/1603	61 build.pr	op:0x517 op:0x24E			88 /
	T	Text (1219)				Detected Ph OS Version	one Vendor	lge 6.0			build.pr	op : 0x268 op : 0x128		- 1	Data Fil
	-	Uncategori	zed (1600)												
						Hash set inf	0							~	

To continue with the extraction and **not** stop the current extraction), click **Continue extraction** (the exact wording might change). The extraction continues uninterrupted.

# 8.2. Technical terms

**Android**: Google's mobile operating system. You can find a list of Android devices here: *http://en.wikipedia.org/wiki/List\_of\_Android\_devices*. Another very helpful resource is *http://pdadb.net*.

**Brick**: A device that cannot function in any capacity (such as a device with damaged firmware). Refer to *http://en.wikipedia.org/wiki/Brick\_%28electronics%29*.

**Client**: A program written by Cellebrite that runs on the Android operating system itself.

**Root / rooting**: A process that allows users of cell phones and other devices running the Android operating system to attain privileged control (*root access*) within Android's Linux subsystem, similar to jailbreaking on Apple devices running the iOS operating system, overcoming limitations that the carriers and manufacturers put on such phones. (*http://en.wikipedia.org/wiki/Rooting\_%28Android\_OS%29*).

# 9. Drone extractions

UFED enables you to extract flight data and multimedia files from supported drones. You can perform physical extractions, as well capture images of drones. For a complete list of supported drones, refer to the UFED Supported Devices file in <u>MyCellebrite</u>.

1. When the extraction completes, the Extraction completed successfully window appears.

# 10. Capture images and screenshots

The Cellebrite UFED camera enables you to collect evidence by taking pictures or videos of a device . You can also use a Screenshot feature to capture internal screenshots directly from a Blackberry, Android or iOS device. Both these options can be useful as complimentary evidence or in instances when data cannot be extracted from a device. You can add notes, categories and bookmarks to the pictures and videos, which will be visible in Physical Analyzer and Logical Analyzer.

The collected evidence can be shown within a standalone custom report or in addition to the extracted information. The report includes information about the device, connection type, Cellebrite UFED version, and serial number. Image information includes file name link, file size, date and time, MD5 and SHA256 hash information. The images are located in a folder called Snapshots and are in PNG format. Video information includes file name, file size, date and time, and a link to the file. The videos are located in a folder called videos and are in AVI format.

## 10.1. The Cellebrite UFED camera

The Cellebrite UFED camera is offered as an add-on that is controlled by the Cellebrite UFED. All necessary drivers are preinstalled with the application. The Cellebrite UFED camera includes a camera stand, which enables you to adjust the height and the angle of the Cellebrite UFED camera, a pad to place the device, and an anti-glare pad to prevent glare when taking pictures. Connect the camera to an available USB port of the computer.

# 10.2. Capturing images

You can take pictures or videos of a device.

To capture images or videos:

1. Click Camera.

The Select Extraction Location screen appears.

SELECT EXTRACTION LOCATION			0	Ċ
Capture Images USB Cam using Cable A with black tip T	nera -100			
	Extraction to Local Drive			
	C:\Users\jonathank\AppData\Local\My   (	3		
ABORT		BACK	NEXT	

- 2. To select an alternate save location, click **Change** target path . A folder for this extraction is created in this location and includes the images (snapshots), videos, UFD file, index file, and report file.
- 3. Click Next.
- 4. Connect the Cellebrite UFED camera to a USB port on the computer. The following window appears.



If you have multiple cameras, you can choose the required camera in Select camera field.

5. Do one of the following:



to start a video recording and click

to stop the video

\* Dick

to take a picture.

- \* Click **Other** to change the default category. Images and videos are displayed in Physical Analyzer and Logical Analyzer under these categories.
- \* Click an image or video, to add notes, bookmarks (🖾), categories 🖾), or delete the file

(🗐). Click 📁 to move back to live view.

To rotate a picture or video, or play a recorded video, click the picture or video, and then click the picture or video in the leftmost screen. Use the rotate

buttons or video buttons **All PIPHOC** . See the following examples.





6. Click **Next** to continue.

When the extraction completes, the Extraction completed successfully window appears.



7. Click Open Preview Report to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click Open with Physical Analyzer to open the extraction in Physical Analyzer, click Show in Folder to open the folder where the UFD extraction file is located, click Additional Extractions to add additional extraction types for the same device, or click Finish to end the process and return to the Home screen.

## 10.3. Capturing screenshots

The Screenshot feature captures internal screenshots directly from a Blackberry, Android or iOS device.

To capture screenshots from the devices:

1. Click Mobile device and identify the device, then click Screenshots.

The Select Extraction Location screen appears.

SELECT EXTRACTION LOCATION	?	Ċ
LG GSM LGL83BL Stylo 3 using Cable A with black tip T-100		
Extraction to Local Drive		
C:\Users\jonathank\AppData\Local\My   🛅		
ABORT BACK	NEXT	

2. If required, select an alternate save location, and click Next.

The Waiting for Device screen appears.

WAITING FOR DEVICE	0 (	ל
LG GSM LGL83BL Stylo 3 using Cable A with black tip T-100		
Connect the source device to the USB port on the computer. If the device is already connected, disconn	ect and then reconnect the device.	
Android 4.2 and Higher Android 4.1.x Android 4.0.x Android 3.2 and Lower		
1. Enable Developer options How to?		
2 . Enable Stay awake and USB debugging modes How to?		
3. Verify screen lock mode How to?		
4. Enable MTP <u>How to?</u> Note: Approve any poque messages that may appear during the process. Approve any coopup messages that may appear during the process. In some devices you may need to disconnect the USB cable from the device in order to enable the USB debugging.		
ABORT BACK		

- 3. Follow the instructions to connect the device.
- 4. Click **Continue**.

The Screenshots screen appears.



If you have multiple cameras, you can choose the required camera in Select camera field.

- 5. Capture the desired screenshots and click **Next**. The Capture Screenshots Summary screen appears.
- 6. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with Physical Analyzer** to open the extraction in Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

# 11. SIM card functionality

The SIM Card functions enableS you to perform various SIM card related functions:

- » SIM data extraction
- Clone SIM

## 11.1. SIM data extraction

The SIM Data Extraction function enables you to perform logical extraction from a SIM or USIM card.

## 11.1.1. Performing SIM data extraction

The following example is performed using a SIM Card.

To perform the SIM Data Extraction:

1. Click SIM Card. The following window appears.



2. Click either **SIM** or **Iden SIM**. The Select Extraction Type window appears.



- 3. Click SIM Data Extraction. The Select Extraction Location window appears.
- 4. Select the extraction location and tap **Next**. The following window appears.



5. Connect the UFED Device Adapter or UFED SIM Adapter to a USB port.

The Waiting for Device screen appears.

WAITING FOR DEVICE	0	ப
lden SIM		
Iden SIM: Insert the SIM card into the slot on the MultiSIM adapter (as indicated), with the card contacts facing down and should be inserted up to the stopper point, without applying pressure. Important: Verify that any previously inserted SIM card is removed.	t the clipped corner facing out. The	SIM card
ABORT BACK		NUE

- 6. Insert the SIM card into the SIM card slot.
- 7. Click **Continue**. The extraction begins.

EXTRACTION IN PROGRESS	?	Ċ
Iden SIM		
Please wait, this can take some time		
Connecting		

The following window appears.
Authentica	ating		
Use PIN (3 attempts left)	Use PUK (10 attempts left)	Skip protected data	

8. Click Use PIN, Use PUK, or Skip protected data.

When the extraction completes, the Extraction completed successfully window appears.

EXTRACTION SUMMARY		<u>ن</u> ق	
Extraction completed successful	ly		
	Source: SIM Target: Local Drive (Logical 01)		
Open Preview Report			
Open with UFED Physical Analyzer			
Show in Folder			
OPEN 🔻	ADDITIONAL EXTRACTIONS	FINISH	

9. Click Open Preview Report to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click Open with Physical Analyzer to open the extraction in Physical Analyzer, click Show in Folder to open the folder where the UFD extraction file is located, click Additional Extractions to add additional extraction types for the same device, or click Finish to end the process and return to the Home screen.

### 11.1.1.1. The extracted SIM data folder

At the end of the SIM data extraction process, the extracted SIM data is saved in the location you selected previously.

The extracted SIM data folder is named UFED SIM card with the extraction date and counter: UFED SIM card SIM card <DATE> (001)

If you selected to extract to the local drive, the extracted SIM data folder is located inside the application's Backup folder.

The extracted SIM data folder contains a forensic report of extracted data in both HTML and XML formats and call log file (\*.clog).

# 11.2. Clone SIM

The Clone SIM ID function enables you to copy the SIM ID from one SIM card to a UFED SIM ID Access Card.

Cloning the SIM ID provides a suitable solution to several problems facing forensic examiners, by allowing extraction of the device data:

- While preventing the cellular device from connecting to the network, rendering the device invisible to the network without the ability to send or receive calls or SMS messages, and thereby preserving the device's current information. (No Faraday Bag is required to block RF signals).
- \* When the original SIM is not available, by manually programming the ICCID or IMSI into the Cloned SIM ID Card to mimic the original missing card.
- When the SIM card is PIN locked, by cloning the identification of the original SIM, which allows extraction of the device data without losing critical data including call history and SMS messages.

There are three different ways that a SIM card can be cloned:

- Clone an existing SIM card to create a cloned SIM to use to extract device data without a network connection. See <u>Cloning an existing SIM card ID (on the facing page)</u>.
- Manually enter SIM data to manually program the ICCID and IMSI to the cloned SIM card. See <u>Entering SIM data manually (on page 191)</u>.
- Create GSM Test SIM The GSM test SIM card is used to extract device data when the original SIM is not available a default ICCID and IMSI are programmed into the Cloned SIM ID Card to mimic the original missing card. See <u>Creating a GSM test SIM (on page 195)</u>.

### 11.2.1. Cloning an existing SIM card ID

1. Click **Clone SIM**. The Waiting for Device Adapter screen appears.

WAITING FOR DEVICE ADAPTER	0	Ċ
Source Iden SIM		
Connect the UFED Device Adapter or UFED SIM Adapter to a USB port.		
ABORT	BACK	:

2. Connect the UFED Device Adapter or UFED SIM Adapter to a USB port on the computer.

WAITING FOR DEVICE	(?	Ċ
lden SIM		
Iden SIM: Insert the SIM card into the slot on the MultiSIM adapter (as indicated), with the card contacts facing down and the clipped corner should be inserted up to the stopper point, without applying pressure. Important: Verify that any previously inserted SIM card is removed.	facing out. The !	SIM card
ABORT BACK CONSOLE	CONTIN	IUE

3. Follow the steps below depending on the adapter you are using.

#### If you are using the UFED Device Adapter:



- 1. Insert the MultiSIM adapter into the port marked SIM.
- 2. Insert the SIM card into the slot on the MultiSIM adapter, as indicated on the adapter.



#### IMPORTANT:

Verify that any previously inserted SIM card is removed **before** attempting to insert a SIM.

3. Insert the SIM card up to the stopper point, without applying pressure.



4. Tap **Continue** and follow the instructions (<u>To select the source and clone the SIM card: (on page 189)</u>)

### If you are using the UFED SIM Adapter:



These instructions are for the UFED SIM Adapter. As displayed in the picture below:



#### To select the source and clone the SIM card:

The **Select Source** screen appears.

lect Source			
Clone an existing SIM card	Manually enter SIM data	Create GSM Test SIM	
			CANCEL

1. Click Clone an existing SIM card.

The Clone SIM ID prompt appears.



- 2. Check that the right SIM was inserted into the SIM card reader slot.
- 3. Click **Continue**. The following window appears.

PIN (3) pts left)     Use PUK (10 attempts left)     Skip protected data	thentica	ating			
	se PIN (3 empts left)	Use PUK (10 attempts left)	Skip protected data		
					CANCEL

4. Click Use PIN, Use PUK or tap Skip protected data. The Extraction in Progress Source screen appears.

When the information has been extracted from the SIM, the Insert Target Card prompt appears.



- 5. Remove the original SIM card from the SIM card reader.
- 6. Insert a UFED SIM ID Access Card into the SIM slot.
- 7. Click **Continue**.

At the end of the data process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information of the cloned SIM card.

EXTRACTION SUMMARY	(?)	Ċ
SIM ID Access Card created successfully ICCID: 8938003991816634752 IMSI: 		
ADDITIONAL EXTRACTIONS	FINIS	ł

8. To end the process and return to the home screen, click Finish.

### 11.2.2. Entering SIM data manually

1. In the home screen, click **Clone SIM**.

The Waiting for Device screen appears.

Connect the UFED Device Adapter to a USB port.

- 2. Insert the UFED SIM ID Access card into the UFED Device Adapter.
- 3. Click **Continue**.

The Select Source screen appears.

Clone an existing SIM card SIM data Create GSM Test SIM	Select Source			
	Clone an existing SIM card	Manually enter SIM data	Create GSM Test SIM	

4. Click Manually enter SIM data. The following screen appears.

Source						
ICCID (1-20 digits)						
Enter ICCID						
< Show Characters						
ОК	Cancel					

- 5. Enter the SIM ICCID number (up to 20 digits).
- 6. Click OK. The following screen appears.

Source	
IMSI (1-15 digits) Enter IMSI	
Show Characters	
ОК	Cancel

7. Enter the SIM IMSI number (up to 15 digits), then click OK.

The Select Language screen appears.

None	German	English	Italian	French	Spanish
Dutch	Swedish	Danish	Portuguese	Finnish	Norwegian
Greek	Turkish	Hungarian	Polish		

8. If required, select either a language or click **None**. The Enter advanced settings screen appears.

Enter adva	nced setti	ngs?
No	Yes	

- 9. Click **No** or **Yes** to continue.
  - \* Click **No** to continue. Proceed to step 15.
  - <sup>\*</sup> Click **Yes** to display the advanced settings. Extraction in Progress > Enter SPN screen appears.

Source	
SPN (0-16 chars)	
Please Enter SPN	
🗹 Show Characters	
ОК	Cancel

10. Enter the **SIM SPN** number (up to 16 digits), then click OK. The following screen appears.

Source	
GID 1 (0-8 digits)	
Please Enter GID 1	
< Show Characters	
ОК	Cancel

- 11. Enter the SIM GID 1 number (up to 8 characters) and click OK. The Extraction in Progress > Enter GID 2 screen appears.
- 12. Enter the SIM GID 2 number (up to 8 characters).
- 13. Click OK. The Insert Target Card prompt appears.
- 14. Insert the UFED SIM ID access card into in the UFED Device Adapter SIM card reader.
- 15. Click **Continue**.

The Extraction in Progress screen is displayed throughout the data writing process.

At the end of the data writing process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information programmed to the SIM card.

16. To end the process and return to home screen click **Finish**.

### 11.2.3. Creating a GSM test SIM

#### 1. Click Clone SIM.

The Waiting for Device screen appears.

WAITING FOR DEVICE			(?	Ċ
lden SIM				
Iden SIM: Insert the SIM card into the slot on the MultiSIM adapter (as indicated), with should be inserted up to the stopper point, without applying pressure. Important: Verify that any previously inserted SIM card is removed.	the card contacts facing do	wn and the clipped corner	facing out. The :	SIM card
ABORT	ВАСК	CONSOLE	CONTIN	IUE

The SIM port on the Device Adapter continues to flash even after you insert the SIM card into the SIM reader slot.



- 2. Insert the SIM card into the SIM card reader slot located in the left of the front panel.
- 3. Click Continue. The Select Source screen appears.
- 4. Click **Create GSM Test SIM**. The following screen appears.



- 5. Make sure that the target SIM card is inserted correctly into the SIM card reader slot, then click **Continue**. The Extraction in Progress screen is displayed throughout the data reading process. At the end of the data writing process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information programmed to the SIM card.
- 6. To end the process and return to the home screen, click **Finish**.

# 12. Device tools

#### To access the device tools:

\* From the Home screen, click **Device tools**. The following window appears.



The **Device Tools** screen provides access to the following tools:

12.1. Activate TomTom trip log	
12.2. Android Debug Console	198
12.3. Bluetooth scan	200
12.4. Disable iTunes encryption password	200
12.5. Exit Android recovery mode	201
12.6. Exit iOS recovery mode	
12.7. Exit Motorola Bootloop	203
12.8. Exit Odin mode	203
12.9. Flash Cable 500 Firmware	204
12.10. LG EDL recovery	

12.11. Nokia WP8 recovery tool	204
12.12. Remove Android extraction files	205
12.13. Samsung Exynos Recovery	205
12.14. Switch to CDMA offline mode	. 206
12.15. Uninstall Windows mobile client	. 207

# 12.1. Activate TomTom trip log

This tool enables you to activate or deactivate the trip log logging feature of a connected TomTom device, which is often disabled by the user

#### To activate TomTom trip log:

- 1. Click **Tools** and then click **Activate TomTom trip log**.
- 2. Connect the UFED Device Adapter.

The **Select Mode** prompt appears.

3. Select the desired mode.

A prompt labeled **Attention** appears requesting to connect the device to Cellebrite UFED.

- 4. Connect the device to Cellebrite UFED.
- 5. Click Continue.

### 12.2. Android Debug Console

This tool retrieves device information using Android Debug Bridge (ADB).

#### To use the tool:

- 1. Click **Tools** and then click **Android Debug Console**.
- 2. If required, you are prompted to connect the Cellebrite UFED Device Adapter to a USB port (UFED and non-kiosk platforms only). The following window appears.

Device Tools	
<ul> <li>Android Debug Console:</li> <li>This tool uses Android Debug Bridge (ADB) a Debugging" mode is enabled.</li> <li>To use this tool:</li> <li>1. Go to the device settings &gt; About/Inform number" 7 times. A message is displayed that</li> <li>2. Go back to the Developer options menu, and "Stay awake" (if available).</li> <li>3. Approve the "Allow USB debugging" comby selecting "Always allow".</li> </ul>	and requires that the "USB nation > tap the "Build at you're now a developer. select "USB debugging" nection to the computer
	ОК

3. Follow the on-screen instructions.

4. Tap **OK** to receive the device information. The following window appears.

Device Info	
USB Descriptors	
VID/PID	:0x1004/0x633E
Manufacturer/Model	: LGE/LGL83BL
Interface 0	: MTP
Interface 1	: ADB Interface
ADB	
Manufacturer/Model	: LGE/LGL83BL
Chipset	: Qualcomm Snapdragon 430
MSM8937 32 Bit	
OS Version	: Android 7.0
Security Patch Version	: 2017-01-01
Encryption State	: encrypted
Rooted	: No
Battery Status (%)	: 90
	REFRESH OK

### 12.3. Bluetooth scan

This tool enables you to scan for available Bluetooth devices in your proximity and to pair with them. Make sure that Bluetooth is enabled on the device.

#### To perform a Bluetooth scan:

- 1. Click tools and then click Bluetooth scan.
- 2. Connect the Cellebrite UFED Device Adapter (UFED and non-kiosk platforms only).
- 3. A list of Bluetooth devices in the vicinity appears. Select one or the following options:
  - \* Click one of the devices: The Device summary window appears.
  - \* Click **Continue**: Device summary window appears
  - Click Refresh list: Device tool in progress window appears and Cellebrite UFED tries to find additional devices.

Bluetooth	Devices	
JBL T110BT	LGL83BL	POCOPHONE
		REFRESH LIST CANCEL

### 12.4. Disable iTunes encryption password

If you select to enable backup encryption during an iOS File system extraction (Full or Backup modes), and for any reason the extraction was stopped in the middle, the device may remain encrypted. **Disable iTunes encryption password** resets the encryption on the device.

# 12.5. Exit Android recovery mode

This tool includes two options related to physical extractions using the Forensic Recovery Partition method on Android devices.

- \* **Exit recovery mode**: In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in recovery mode. Takes the device out of recovery mode.
- \* **Exit bootloop**: In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. Takes the device out of this bootloop.

# 12.6. Exit iOS recovery mode

Occasionally, a mobile device may remain in recovery mode following exploitation. This generally happens due to device failure, or when the mobile device was improperly disconnected from Cellebrite UFED. This tool enables the investigator to take the device out of recovery mode manually.

#### To use the tool:

1. Select Tools > iOS Exit Recovery Mode.



2. Connect the device to Cellebrite UFED.



3. The process is initialized. The following window appears.



The device is released from recovery mode and restarts automatically.



### 12.7. Exit Motorola Bootloop

In some cases, due to device failure, or if the Motorola mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. **Exit Motorola Bootloop** takes the device out of this bootloop.

### 12.8. Exit Odin mode

To perform physical extractions on some Samsung devices, the device is placed in Odin mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in Odin mode. **Exit Odin mode** takes the device out of Odin mode.

# 12.9. Flash Cable 500 Firmware

When using the Smart ADB method, the firmware on Cable No. 500 is changed and no longer supports the Cellebrite UFED User Lock Code Recovery Tool. The Flash Cable 500 Firmware tool flashes the required firmware to the cable to support either the Smart ADB method or the Cellebrite UFED User Lock Code Recovery Tool.

In the Smart ADB method, Cellebrite UFED verifies the cable firmware and flashes it if required. Cellebrite UFED User Lock Code Recovery Tool does not include cable verification.

#### To flash the firmware for the Smart ADB extraction method:

- 1. Click Tools and then click Flash Cable 500 Firmware.
- 2. Connect the Cellebrite UFED Device Adapter to a USB port (UFED and non-kiosk platforms only).
- 3. Connect Cable No. 500 (side A) to the USB port.
- 4. Tap **Smart ADB Firmware** and wait for the process to finish.

### 12.10. LG EDL recovery

In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the LG device remains in emergency download (EDL) mode and appears off. **LG EDL recovery** takes the device out of EDL mode.

#### To use the tool:

- 1. Click **Tools** and then click **LG EDL recovery**.
- 2. If required, you are prompted to connect the Cellebrite UFED Device Adapter to a USB port (UFED and non-kiosk platforms only).
- 3. Follow the on-screen instructions.
- 4. Tap **Continue** and wait for the tool to finish running.

### 12.11. Nokia WP8 recovery tool

To perform physical extraction on some Nokia Windows Phone 8 devices, the device is placed in recovery mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in recovery mode. **Nokia WP8 recovery tool** takes the device out of recovery mode.

# 12.12. Remove Android extraction files

When performing extractions of devices with Android operating systems, a client is installed and some files are written to the mobile device. In some cases (e.g., due to a failure, or if the mobile device was improperly disconnected from Cellebrite UFED) the client and the files remain on the mobile device. This tool uninstalls the client and removes the files from the device.

### 12.13. Samsung Exynos Recovery

In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the device remains off and the Android OS does not start. **Samsung Exynos Recovery** attempts to resolve this issue.

### 12.14. Switch to CDMA offline mode

This tool enables you to switch radio on CDMA devices to offline mode.

To switch to CDMA offline mode:

- 1. Click tools and then click Switch to CDMA offline mode.
- 2. Connect the Cellebrite UFED Device Adapter (UFED and non-kiosk platforms only). The Select Link prompt appears.

Select Link USB Cable Serial Cable	Switch to CDMA offline mode	
USB Cable Serial Cable	Select Link	
	USB Cable Serial Cable	
CANCEL		CANCEL

3. Select the link type (USB Cable or Serial Cable). The Device Tool in Progress window appears.



4. Tap OK.

Upon completion, the Device Tool Summary appears.

# 12.15. Uninstall Windows mobile client

To perform logical extractions on devices with Windows Phone operating systems, a client is installed on the device. In some cases, due to a device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the client remains installed on the mobile device. **Uninstall Windows mobile client** enables the client to be manually uninstalled.

# 13. Settings

The settings screen provides access to a set of functional and behavioral setup options used to control the functionality and usability of Cellebrite UFED.

To access the settings screen, click the menu icon in the application taskbar and select Settings.

The settings are grouped in the settings screen in the following tabs:

- \* General settings (on the next page)
- \* Report settings (on page 217)
- \* System settings (on page 223)
- \* License settings (on page 224)
- \* Version details (on page 233)
- \* Activity Log (on page 242)

The settings screen opens on the General tab.

When using the Cellebrite Commander, these settings may be managed by Cellebrite Commander.



Ē

Changes that are made to the settings via Cellebrite Commander or manually by a user, affect all users on the same machine.

# 13.1. General settings

The settings screen opens on the General tab.

«	General	Reports	System	License	Version ≫
🗾 Swa	p first and last name	e in phonebook			
Interfac	e language:				
Englis	h 🧪				
Mobile	extraction client:				
	Operate in covert mo	ode			
<b>u</b>	Jninstall reminder				
Save ext	tractions to:				
C:\User B	s\jonathank\AppDa rowse	ta\Local\My UFED Extra	actions		
🗾 Allo	w user predefined f	lter			
🔽 Enal	ble extraction of del	eted messages from SII	м		
🗾 Reqi	uire a password on	wakeup			
🔽 Enal	ble Android Backup	APK Downgrade			
📃 Enal	ble online device ins	tructions			
				SAVE	CANCEL

The **General** tab provides access to the functions and settings listed in the following table.

Setting	Description	Default
Swap first and last name in phonebook	Swaps the first and last name in phone book entries.	Selected
Interface language	Changes the interface language. For more information, see <u>Changing the</u> <u>application interface language (on</u> <u>page 213)</u>	English
Operate in covert mode	Renames the application client name from Cellebrite.sis/exe to AAA.sis/exe.	Selected
Uninstall reminder	When enabled, the Cellebrite UFED prompts you to uninstall the client from the examined device.	Selected

Setting	Description	Default
Save extractions to	Sets the location where extractions are saved. For more information, see <u>Changing</u> <u>the extraction location (on page 216)</u>	
Allow user predefined filter	Displays the timeframe and select parties windows during an extraction. For more information about the User predefined filter, see <u>User predefined</u> <u>filter (on page 59)</u> .	Cleared
Enable extraction of deleted messages from SIM	Extracts deleted messages from a SIM.	Selected
Require a password on wakeup	Requires the user to enter a password when Cellebrite UFED is in sleep mode.	Selected
Enable Android Backup APK Downgrade	Enables the Android Backup APK Downgrade method.	Selected
	Displays the online device instructions instead of the offline device instructions.	
Enable online device instructions	This setting is for the Waiting for Device instructions, which explains how to connect a source device to Cellebrite UFED. If you have network performance issues when using the online device instructions, clear Enable online device instructions.	Cleared
Show device restart alerts	Displays device restart alerts during the extraction process.	Cleared

Setting	Description	Default
Cable and Tip mode	Indicates the cable or tip to be used during the extraction.	Tip
Include Case details screen	Displays the Case details window during the extraction process. For more information, see <u>Case details (on</u> <u>page 51)</u> . If selected, you can also display the extraction folder name according to the case details. The default is according to the device model name.	Cleared
Show investigation notes	Displays the Investigation notes widget, which enables you to add pictures, screen shots and text to document the investigation. See <u>Investigation notes</u> (on page 51).	Cleared
Include camera screen	<b>e camera screen</b> Displays the camera window during the extraction process.	
Automatically open extractions with Physical Analyzer	If installed, the extraction is opened automatically in Physical Analyzer.	Cleared
Choose additional logo	Select an additional logo that is displayed in the title bar of the home screen.	

Setting	Description	Default
Video quality	Set the video quality of the Cellebrite UFED camera to Best (1920 x 1280), Normal (1024 x 1280 default) or Low (640 x 480).	Normal
Enable device info (Advanced logical)	Displays the Device Info window during the Advanced Logical extraction. This window provides information about the device data, before performing an Android extraction.	Selected

### 13.1.1. Changing the application interface language

1. Click the language field.



The Select Language screen appears with the current language selected. (In this case, **English**).



ð

Use the arrows to scroll through the list of available interface languages.

2. Click the required language.



The following message appears (in the selected language).

Notice		
You must restart the application for the language change to take effect.		
	ОК	

3. Click OK.

The General tab appears with the language of choice in the Interface language field.

- 4. Click **Save** to close the Settings panel.
- 5. To restart the application:



- a. To close the application, click \_\_\_\_\_ in the application taskbar.
- b. To restart the application, do one of the following:
  - \* Click the application shortcut icon located in the UFED shortcuts panel at the right of the screen.
  - <sup>»</sup> Double- click the Cellebrite UFED icon located on the Desktop.
  - Click Start > Cellebrite UFED
  - \* Click Start > All Programs > Cellebrite Mobile Synchronization > Cellebrite UFED.

Cellebrite UFED starts in the selected language.

If Simplified Chinese is added to the Cellebrite UFED license, you must restart the application before the change takes effect.

### 13.1.2. Changing the extraction location

1. In the Save extractions to area, click Browse. The Browse for folder dialog box appears.

📃 Desktop	
Dibraries	
Flare_lang_v5.2_TN	
Description of the second s	
Network	
Description Panel	
👿 Recycle Bin	
Make New Folder	OK Cancel

2. Select the folder where you want to save the extraction files, and click OK.

# 13.2. Report settings

«	General	Reports	System	License	Version	Activity Log	≫
Gen	erate reports language:						
Eng	glish (English) 🧪						
Note	es display mode:						
Em	bedded Notes 🔻						
Repo	ort format:						
No	rmal 🔻						
Керс	del Seriel XXXX MM DI						
Hash	n using: (Using multiple	hash mechanisms incr	eases the extraction time				
🗹 S	HA-256						
	ND5						
	Create MD5 list file (L						
<b>V</b> F	Partial extraction						
	Report custom fields						
					ŠAVE	CÂNCEL	

#### To set the report settings:

- 1. Access the **Settings** > **Reports** tab.
- 2. To set the generated reports language, click 🖉 next to Generate Reports Language, and select the desired language.
- 3. To set how the known issues notes about the extracted device are logged in the generated report, click and next to **Note display modes**, and select one of the following:
  - \* **Disable** Do not include device specific notes in the report.
  - \* Separated Notes Add all the device specific notes at the end of the report.
  - Embedded Notes Device-specific notes follow the content type they refer to in the report.
- 4. To set the generated reports visual formats, click report format, and select one of the following:
  - » Normal The standard report structure, suitable to standard display screens.
  - \* **Compact** A compact report structure, suitable for devices with a small display area.
5. To set the generated reports folder name formats, select next to **Report folder format**, and select one of the following:

\* Model Serial YYYY\_MM\_DD - The folder name is constructed from <the model name> <the model serial> <the year in 4 digits>\_<the month in 2 digits>\_<the day in 2 digits>

- YYYYMMDD Model Serial The folder name is constructed from <the year in 4 digits><the month in 2 digits><the day in 2 digits> <the model name> <the model serial>
- 6. Select or clear **Hash using MD5** to toggle the display of the MD5 values which are generated for each file in the extracted data. This increases the time required to complete the extraction.
- 7. Select **Create MD5 list file** to generate a Checksums.md5 file that contains all the generated MD5 values of the extracted data.
- 8. Select or clear **Hash using SHA-256** to toggle the display of the SHA-256 values which are generated for each file in the extracted data.
- 9. Select or clear **Partial Extraction**, in the event of an extraction error, whether or not to include the partially extracted data up to the error point in the generated report.
- 10. Click **Report custom fields** to add, remove and edit report fields. For more information, see <u>Managing report fields (on the facing page)</u>.
- 11. To set a field as required, click the field in the **Required** column.
- 12. Click Save.

# 13.2.1. Managing report fields

1. Click **Report custom fields** to customize the report by defining additional fields that are filled at the end of the extraction.

Field Name Required	Add
Case number	Delete
Examiner name	
Department	Edit
Address	
Notes	

- 2. To add a new field:
  - a. Click Add.

anage report	custom fields	
Field Name	Required	
	Save	Cancel

b. Enter the field name in the **Field Name** field.



- c. To set the field as mandatory, select **Required** next to the field name.
- d. Click **Update**, or to exit without saving, click **Cancel**.
- 3. To add additional fields, repeat step 2.
- 4. To edit an existing field:

- a. Click the field in the list, and click **Edit**.
- b. Repeat steps 2b-2d.



You cannot edit the field name of a default custom field.

- 5. To delete a field:
  - a. Click the field in the list, and click **Delete**.



- b. In the confirmation message, click **Yes**.
- 6. Click **Save** in the **Reports** tab.

# 13.3. System settings



#### Define the following additional settings in the System tab:

\* To set Cellebrite UFED to alert you when your attention is required, such as when it is waiting for your input or when an extraction fails, select **Play notification sounds**.

# 13.4. License settings

Change the license type in the **License** tab.

The current license type is displayed.

«	General	Reports	System	License	Version	Activity Log	≫
Softv	vare license						
Your	license will exp	ire on 1/5/2020					
This	license includes						
Extra	ict phone, Extra	ct SIM, Clone SIM, Ph	ysical extraction, File system e	extraction, Password extra	ction		
Com	puter ID:						
Cha	inge license	Deactivate					
Re	ebuild cache	Copyright					
(?) Н	elp 🛱 Sales	sales@cellebrite.c	om				
					SAVE	CANCEL	

To change the license type, follow the instructions in <u>Activating the license (on page 25)</u>.

## 13.4.1. License not found

If a license cannot be found the following window appears.



### If you are using Cellebrite Commander:

1. Click I'm using Cellebrite Commander. The following window appears.

Cellebrite product license Connect to your Centralized Management Sys CMS Server:	tem (CMS) server
http:/ubuntu.local	Validate
If you have a license dongle, connect it before	validating
<b>Status:</b> Connection not initiated	
⑦ Help  \ □ Sales Back Back Back	Close

- 2. Connect the license dongle before validating.
- 3. Enter the Cellebrite Commander Server information. For more information about entering the information in this window, see <u>Connect a Cellebrite UFED device to Cellebrite</u> <u>Commander (on page 234)</u>.
- 4. Click Validate.

# If you are not using Cellebrite Commander:

1. Click I'm not using Cellebrite Commander. The following window appears.

Select your license type:		
Dongle	Software	
	Pack	Class

2. Select your license type.

# 13.4.2. Updating a dongle license online

When an Internet connection is available, you can update the dongle license directly from Cellebrite UFED.

#### To update a dongle license online:

2. From the Home screen, click

1. Contact your Cellebrite sales representative to renew or update the dongle license. After the license is approved, you can proceed with the following steps.



and then click the License tab. The following window appears.

«	General	Reports	System	License	Version	Activity Log 📎
Soft	ware license					
You	r license will expi	re on 1/5/2020				
This Extr	license includes act phone, Extra	: ct SIM, Clone SIM, Physical e	xtraction, File system ext	raction, Password extrac	tion	
Com	nputer ID:					
Ch	ange license	Deactivate				
R	Rebuild cache	Copyright				
. ⊘ ⊦	Help 🛱 Sales	sales@cellebrite.com				
					SAVE	CANCEL

3. Click **Change license**. The following window appears.

<b>Cellebrite product</b> Select your license type:	license	
Dongle	Software	
⑦ Help  ☐ Sales		Close

4. Click **Dongle**. The following window appears.

Cellebrite product license		
Connect the dongle to a USB port on It will be detected automatically.	your computer.	
If you connected a dongle and it still Load license file Update license (onli	doesn't work, <u>contac</u> <u>ne)</u>	t Cellebrite support.
⑦ Help ☐ Sales	Back	Close

- 5. Click Update license (online).
- 6. Click OK to complete the process.

## 13.4.3. Updating a software license online

When an Internet connection is available, you can update a software license directly from Cellebrite UFED.

To update a software license online:

2. From the Home screen, click

1. Contact your Cellebrite sales representative to renew or update the dongle license. After the license is approved, you can proceed with the following steps.



and click the **License** tab. The following window appears.

«	General	Reports	System	License	Version	Activity Log	<b>»</b>
So	ftware license						
Vo	ur license will evni	ire on 1/5/2020					
ть	is license includes						
Ex	tract phone, Extra	ct SIM, Clone SIM, Physica	al extraction, File system ex	traction, Password extrac	ction		
-							
Co	omputer ID:						
	hange license	Deactivate					
	Debuild seeks	Convictor					
	Rebuild cache	Copyright					
	Help ₩ Sales	sales@cellebrite.com					
					SAVE	CANCEL	

3. Click **Change license**. The following window appears on Cellebrite UFED.

For Cellebrite UFED Touch, accept the Cellebrite UFED License Agreement and skip to step 6.



<b>Cellebrite product l</b> Select your license type:	icense	
Dongle	Software	
⑦ Help \ \ Sales		Close

4. Click **Software**. The following window appears.

Cellebrite product license			
Software license			
Your license will expire on 1/5/2020			
This license includes:			
Extract phone, Extract SIM, Clone SIM, Physical extrac	tion, File system e	extraction,	, Password extract
Extract phone, Extract SIM, Clone SIM, Physical extract Computer ID: N3Y-2EW-PID-WNB-ZWJ-X2W-YG4 Update software license	tion, File system e	extraction,	, Password extract

5. Click **Update software license**. The following window appears.

ready have a license file?	
Load license file	
oad from the web	
leed to download yo	ur software license?
leed to download yo to MyCellebrite	ur software license? W-PID-WNB-ZWJ-X2W-YG4 Copy

- 6. Click Load from the web.
- 7. Click OK in the Cellebrite product license window to complete the process.

# 13.5. Version details

The version tab displays information about the Cellebrite UFED version and build.

Under Software updates, select Automatically check for software updates.

«	General	Reports	System		Version	Commander	Activity Log	User Permissio ≫
Vers	sion 7.44.0.245							
© 2	009-2021 Celle	brite delivering	mobile expertis	se.				
Inte	rnal build: 7.44	.0.245 built on	5/2/2021 11:25	5:46 AM				
Soft	ware updates Automatically c	heck for softwa	re updates					
You	have the latest	version						Refresh
Upd	late version fro	m:						File
1								
:								

# 13.5.1. Connect a Cellebrite UFED device to Cellebrite Commander

Cellebrite UFED devices automatically detect when a new Cellebrite Commander server is added to their subnet and prompt the user to connect automatically. If necessary, you can also connect a Cellebrite UFED device to Cellebrite Commander manually.

### To connect a Cellebrite UFED device to Cellebrite Commander automatically:

1. Right-click on the application shortcut and select **Run as Administrator** 



Enable Admin permissions to enable the Cellebrite UFED device to automatically download the SSL certificate. This ensures secure SSL communication between a managed Cellebrite UFED unit and Cellebrite Commander server.
To enable downloading of certificates, make sure the setting is enabled in Cellebrite UFED Settings.

2. Restart the Cellebrite UFED unit.

Ē

- 3. The unit automatically detects the Cellebrite Commander server and prompts the user to connect.
- 4. After the unit connects to the Cellebrite Commander server, it automatically switches to managed mode and downloads the secure SSL certificate.

If more than one Cellebrite Commander is detected, the user can choose from the list of servers.

### To connect a Cellebrite UFED device to Cellebrite Commander manually:

	al	System	License N	Version C	ommander	Activity Log	User Pe
Cellebrite Co Managed	ommand	ler server conno Inmanaged	ection				
🔵 Manual	<b>()</b> N	etwork					
Enter FQDN							
Your display na Responder 7	nme in Cell 7.40.0.33	lebrite Commande test	r: (optional)				
Status:							
Connecte	d to Celleb	orite Commander					
Connecte	d to Cellet on files	orite Commander					
Configuratio	d to Celleb on files Version	vrite Commander	Last version check	Last status		_	
Configuratio	d to Celleb n files Version 1.0.0.8	Imported date	Last version check 11/19/2020 17:31	Last status No upgrade informatio	an Import	_]	
Connecte Configuratio Type Guidance Agency forms	d to Celleb n files Version 1.0.0.8 1.0.0.9	rite Commander	Last version check 11/19/2020 17:31 11/19/2020 17:31	Lest status No upgrade informati No upgrade informati	on Import		
Connecte Configuratio Type Guidance Agency forms Camera checklist	d to Celleb n files Version 1.0.0.8 1.0.0.9 1.0.0.4	Imported date 11/17/2020 14:31 11/06/2020 08:56 11/06/2020 08:56	Last version check 11/19/2020 17:31 11/19/2020 17:31 11/17/2020 16:16	Lest status No upgrade informatio No upgrade informatio Latest version	on Import on Import Import		
Connecte Configuration Type Guidance Agency forms Camera checklist Case details	d to Celleb n files Version 1.0.0.9 1.0.0.4 1.0.0.5	Imported date 11/17/2020 14:31 11/06/2020 08:56 11/06/2020 07:25	Last version check 11/19/2020 17:31 11/19/2020 17:31 11/17/2020 16:16 11/19/2020 17:31	Lest status No upgrade informatio No upgrade informatio Latest version Update downloaded	on Import on Import Import Import		
Connecte Configuratio Type Guidance Agency forms Camera checklist Case details User	d to Celleb n files Version 1.0.0.8 1.0.0.9 1.0.0.4 1.0.0.5 1.0.0.22	Imported date 11/17/2020 14:31 11/06/2020 08:56 11/06/2020 08:56 11/06/2020 08:56 11/06/2020 08:56	Last version check 11/19/2020 17:31 11/19/2020 17:31 11/17/2020 16:16 11/19/2020 17:31 11/19/2020 17:31	Lest status No upgrade informatik No upgrade informatik Latest version Update downloaded Latest version	on Import on Import Import Import Import		

1. Go to **Settings > Commander**. The following window appears.

- 2. Select Managed mode.
- 3. Enter the Commander's FQDN (fully qualified domain name). **Example**: qas99.cellebrite.wxyz
- 4. Click **Connect**. If the validation is successful, the status changes to **Connected to Cellebrite Commander**.
- 5. Click Save.

## 13.5.2. Updates and versions

When Cellebrite UFED is connected to the Internet, automatic notifications appear in the event of updates and new versions of the application.

Click Refresh in the Settings > Version tab to update the information available on the screen.

#### To install a newer version of the Cellebrite UFED application via the web:

- 1. Ensure that the unit is connected to the network.
- 2. In the **Settings** > **Version** tab, in the **Version** area, click **Web**.

The application is upgraded to the latest version available on the Cellebrite Commander (if relevant) or Cellebrite download server.

## To install a newer version of the Cellebrite UFED application using the file option:

- 1. Download the latest application version from your account in MyCellebrite, and save it to the specified directory on the PC or external device.
- 2. In the **Settings** > **Version** tab, in the **Version** area, click **File**.
- 3. Select the directory where you saved the file and then click **Open**.

# 13.5.3. Importing settings and configuration files

You can use Cellebrite Commander to download initial export files, which can then be edited if necessary and manually imported into Cellebrite UFED. These files can also be set using Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.

Cellebrite UFED can import the following type of settings and configuration files:

- \* Importing a camera checklist (on the next page)
- \* Importing case details (on page 239)
- \* Importing user management (on page 241)
- \* Importing configuration files (on page 242)

### 13.5.3.1. Importing a camera checklist

The camera checklist enables you to upload an XML file that the user can use as a reference as to what pictures are required of the device. As the user completes each step, they can place a check mark next to the completed items.



#### To manually import a Camera checklist file:

- In the Version tab, click the Import button next to the setting file you would like to import. The following window appears.
- 2. Browse to the relevant file and click **Open**.
- 3. Click **OK** to update the application.

The following example shows the structure of the XML file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CheckListData>
<Version>1.0.0.48</Version>
<CheckListItems>
<CheckListItem>Main screen</CheckListItem>
<CheckListItem>Date and time</CheckListItem>
<CheckListItem>IMEI number</CheckListItem>
</CheckListItems>
</CheckListItems>
```

### 13.5.3.2. Importing case details

You can import an XML file to change the options that appear in the Case Details window (see <u>Case</u> <u>details (on page 51)</u>).

# To manually import a case details file:

- 1. In the Version tab, click the **Import** button next to the setting file you would like to import.
- 2. Browse to the relevant file and click **Open**.
- 3. Click OK to update the application.

The following example shows the structure of the XML file.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<CaseDetails>
    <Version>1.0.0.38</Version>
    <Fields>
         <Field>
              <Type>String</Type>
              <Caption>Case ID</Caption>
              <Mandatory>true</Mandatory>
              <AutoFill>true</AutoFill>
              <lsDefaultFolderName>true</lsDefaultFolderName>
         </Field>
         <Field>
              <Type>String</Type>
              <Caption>Seized by</Caption>
              <Mandatory>false</Mandatory>
              <AutoFill>false</AutoFill>
              </Field>
         <Field>
              <Type>String</Type>
              <Caption>Crime type</Caption>
              <Mandatory>false</Mandatory>
              <AutoFill>false</AutoFill>
              <lsDefaultFolderName>false</lsDefaultFolderName>
              <Values>
                  <Value>Armed Robbery</Value>
                  <Value>Attempted Murder</Value>
                  <Value>Child Exploitation</Value>
              </Values>
         </Field>
         <Field>
              <Type>String</Type>
              <Caption>Device owner</Caption>
              <Mandatory>false</Mandatory>
              <AutoFill>false</AutoFill>
              <lsDefaultFolderName>false</lsDefaultFolderName>
              <Values>
                  <Value>Victim</Value>
                  <Value>Suspect</Value>
                  <Value>Witness</Value>
             </Values>
         </Field>
    </Fields>
</CaseDetails>
```

# 13.5.3.3. Importing user management

Cellebrite Commander enables user authentication ensuring that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile.

### To manually import a user management file:

- 1. In the **Version** tab, select the **Import** button next to the setting file you would like to import.
- 2. Browse to the relevant file and click **Open**.
- 3. Click **OK** to update the application.

### 13.5.3.4. Importing configuration files

Configuration files enables you to import various settings into the system.

To manually import a configuration file:

- 1. In the **Version** tab, select the **Import** button next to the setting file you would like to import.
- 2. Browse to the relevant file and click **Open**.
- 3. Click **OK** to update the application.

# 13.6. Activity Log

The Activity Log lists all transactions performed by Cellebrite UFED. It includes information such as when the extraction started and ended, transaction type, duration, status, device vendor, device model, name, serial number of Cellebrite UFED, case ID, crime type, device owner, and who seized the device. You can also clear the activity log, export the activity data to a CSV file and show or hide the activity data.

Cellebrite	Responder 7.36.0.152							-	
«	System	License	Versi	on	Activity	Log	User Permissions	Storage	»
🔲 Hid	e device identification	number			N				
Activit	y log:								
Z Ena	ble detailed activity lo	g							
Short D	wextraction log	Transation Trans	Duration	Chantara -	Mandar	Madal	News	Linit Social Number	I Case I
Start D		Transaction Type	Duration	Status	vendor	Woder	Name	Onic Senar Number	Case
	NUMBER OF STREET			1000		March 1			
Expo <u>rt</u>	to USB						Clear	Export to Export	kcel 🔻
							SAVE	CANCE	L

## 13.6.1. Exporting metadata to Cellebrite Commander

If a Cellebrite UFED unit is used in an offline environment, you can export the usage metadata file. This file contains the following: Cellebrite UFED device information (e.g., MAC address, serial number, software version number), transaction start times and end times, source phone information (e.g., vendor, model name, IMEI, and operating system), and type of information extracted (e.g., Phone memory, SMS memory, MMS, pictures, videos, audio). The exported Zip file can then be manually imported into Cellebrite Commander. For more information, refer to the Cellebrite Commander manual.

### To export the metadata:

- 1. Connect or reconnect a USB flash drive to the Cellebrite UFED unit. The button is only available when a USB drive is connected.
- 2. Click the **Export to mgmt (acc)** button. The metadata can now be imported into Cellebrite Commander.

This button is only displayed if you are using the Managed mode (see <u>Version</u> details (on page 233)).



Ē)

Exported data is removed from the Cellebrite UFED device and is not available for export again.

# 13.7. Users permissions

Define and configure user authentication settings to ensure that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile.

User permissions can be set using Cellebrite Commander (refer to the Cellebrite Commander *manual*) or the UFED Permission Manager (see <u>Permission</u> <u>management (on page 254)</u>).



#### To disable USB device extraction:

\* Select **Disable USB device extraction**. This option is not available on the home screen.

### To import user permissions:

- 1. Run the Cellebrite UFED as an administrator.
- 2. Click Import. The following warning appears.



- Click Yes and navigate to the directory where the permission management file (\*.cp) is located. For information about creating a permission management file, see <u>Using the</u> <u>Cellebrite UFED Permission Manager (on page 254)</u>.
- 4. Click **Open** and then click **Save**.
- 5. Restart the Cellebrite UFED application, which now prompts for login credentials.
- 6. Use one of the login credentials configured in the permission management file. For more information, see Permission management (on page 254).

Select the checkbox to require password on wakeup.

# 13.7.1. Active Directory integration

Active Directory is a Microsoft product providing a range of directory-based identity-related services. It authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers and installing or updating software.

When a user logs in to the system, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user before allowing the user to log in. Active Directory also enables the management and storage of information at the admin level and provides authentication and authorization mechanisms.

Use the Windows Active Directory account to enable *quicker and easier* log in to your Cellebrite UFED applications. Cellebrite UFED can manage the permissions with two permissions levels:

- \* Active Directory Groups
- » Active Directory Users with Commander roles

### 13.7.1.1. Determining the Active Directory groups

When using the **Groups level**, the permissions are applied according to the Active Directory groups of which the users are members (directly and indirectly). When



using the **Users level**, you must map the users to Cellebrite Commander and then to the permissions applied according to the selected profile in Cellebrite Commander. For more information, see <u>To enable Active Directory (on page 248)</u>.

You can use the following procedure to determine all the Active Directory groups for a specific user.

1. To get a list of groups for a specific user, replace <user name> with the actual user name

Open a command prompt (cmd.exe) and run:

gpresult /V /user <user name>

2. The output looks like this (truncated with only the group information):

The user is a part of the following security groups

\_\_\_\_\_

Domain Users Everyone BUILTIN\Users NT AUTHORITY\INTERACTIVE CONSOLE LOGON NT AUTHORITY\Authenticated Users This Organization

LOCAL

Marketing

Platforms Dev Team

In the above example, you can see that this user is a member of several Active Directory (security) groups. In the following example we use the **Platforms Dev Team** security group.

ð

If a group is contained within another group, other commands (such as whoami /groups) only display the groups of which the user is a direct member. Therefore, we recommend that you avoid whoami as an indicator.

## 13.7.1.2. Using Cellebrite Commander

When using Cellebrite Commander, the system administrator must decide the permission management level. The possible levels are presented below:



### 13.7.1.3. Initial setup

When Cellebrite Commander is used in conjunction with Active Directory, the following procedures are required for initial setup.

#### 13.7.1.3.1. Permission Level - Groups

The Cellebrite Commander administrator must:

- 1. Create *profiles* with the exact same name of the relevant Active Directory groups.
- 2. Publish the users and permissions to all the relevant Cellebrite UFED units.

After Active Directory is set up, each login request via a Windows user is sent to Active Directory before approval. Active Directory checks the user permissions and notifies the Cellebrite UFED unit whether to approve or deny the login request based on the user profile permissions.

If the Cellebrite UFED units are offline, you cannot log in to the Cellebrite UFED unit. However, an ongoing session is not disconnected if a disconnection occurred.



Should you choose not to work with Active Directory, the Cellebrite Commander administrator can regulate the users and permissions via Cellebrite Commander or the Cellebrite UFED Permission Manager.

### 13.7.1.3.2. Permission Level – Users

The Cellebrite Commander administrator must:

- 1. Create *profiles* and set the permissions for each profile.
- 2. Import a CSV list of relevant *users* that matches the Users and Profiles settings in Cellebrite Commander.
- 3. Publish the users and permissions to all the relevant Cellebrite UFED units.

### 13.7.1.4. To enable Active Directory

1. In Cellebrite Commander select **Configurations > By product**. The following window appears.

COMMANDER			Help	A.	0	Q UFED A	Q UFED Admin	Q UFED Admin -	Q UFED Admin -	Q UFED Admin -
A Dashboard		Product configuration								
# Product monitoring		UFED Products	-							
3 Software management		UFED master template - Anna's 👻 🔂 Duplicate template 🔮 Deline template EDT 🛛 🗛 Deline template	1							
2 Configurations		General								
Global		Application language English								
By product		Set the internace language for manages units.								
Publishing history		Additional languages Enable additional interface languages in managed units. Enable additional interface languages in managed units.								
E SOPs										
2. User management		Additional languages for reports in managed units. English, Arabic, Chinese, Croatian, Czech, Dani								
<i>∂</i> Device management		Prompt for confirmation on exit Require a second confirmation to quit the system. Protects against user errors and data Off loss.								
II Usage analyses		Story virtual indexed								
X Offline management	ETA	Enable the on-screen virtual keyboard.								
		Enable access to connectivity settings								
		Enable the Connectivity tab under Settings.								
		Include Case Details 0 0 00								
		Enable users to add case details to extractions.								
		Include Camera somen Tra Bec On								
Ö Commander settions		Require users to use UFED Camera during extractions.								
a contraction seconds		Min. number of pictures/videos								

- 2. Click **Edit**, to enable the following under the Access Control section:
  - a. Require login.
  - b. Enable Active Directory integration.
- 3. Under **Permissions level**, select one of the following options:
  - \* Active Directory groups: Manage permissions at the Active Directory groups level. The match is performed by Active Directory group names.
  - Active Directory users with Commander roles: Manage permissions per user independently from Active Directory groups.
- 4. Click Save to save the configuration template.
- 5. Publish the configuration template to the relevant product.

Next you must add the Active Directory profile and select the required permissions.

### 13.7.1.4.1. To add a role and select permissions

Adding roles and selecting permissions are managed in the User Management System. For more information, see the Managing Roles section in the User Management System manual.

## 13.7.1.4.2. Adding Users

Adding users is managed in the User Management System. For more information, see the Managing Users section in the User Management System manual.

## 13.7.1.5. Logging in to Cellebrite UFED

After Active Directory is enabled, the following occurs depending on the Cellebrite UFED device you are using.

- \* In PC applications such as Cellebrite UFED and Cellebrite Responder, the login occurs automatically when you start the Cellebrite UFED application.
- <sup>\*</sup> In closed systems such as Cellebrite UFED Touch and Kiosk, Cellebrite UFED tries to locate the domain and display the following login screen.

Cellebrite Re Version: 0.0 — Welcon	esponder <sup>0.0.0</sup>
User	8
Password	۵
LOGIN	

- » Enter the Active Directory credentials.
- » Verify the Domain field.

If the text in the Domain field (that is, domain controller host) is missing or incorrect, contact your IT department.

### 13.7.1.6. Cellebrite UFED Permission Manager

If you are not using Cellebrite Commander, use the following procedures in the Cellebrite UFED Permission Manager and Cellebrite UFED application to enable Active Directory.

### To configure Active Directory in the Cellebrite UFED Permission Manager:

In the Cellebrite UFED Permission Manager, create a profile that corresponds to the required Active Directory group.

1. Run the Cellebrite UFED Permission Manager. The following window appears.

👛 UFED Permission Manager (0.0.3.819)			- 0	
	UFED Permission Manager Export profile reports	xport	Import	
Profiles				
Lisers				

2. Click **Profiles > New Profile**. The following window appears.

+	) New j	profile	Delete
General Ext			
Name: *	Platforms Dev Team		
Description:	Platforms Dev Team		
User Notif			

- 3. In the Name field enter the name of the Active Directory group (for example, Platforms Dev Team).
- 4. (Optional) Enter a description.

5. Click **Extraction Types** and enter all the required permissions for the profile. The following window appears.

-	New profile	Delete
General Extraction Ty	pes	
• 🔵 Admin		
Manage Users		
🗸 Extraction Type		
Cogical Extraction		
🗸 Logical Extract	tion Content Type : Phonebook	
🗸 Logical Extract	tion Content Type : SMS	
🗸 Logical Extract	tion Content Type : MMS	
🗸 Logical Extract	tion Content Type : Email	
🗸 Logical Extract	tion Content Type : Instant Messaging	
🗸 Logical Extract	tion Content Type : Calendar	
🗸 Logical Extract	tion Content Type : Application Data	
🗸 Logical Extract	tion Content Type : Pictures	
🝼 Logical Extract	tion Content Type : Audio/Music	
🗸 Logical Extract	tion Content Type : Videos	
		Save

6. Click Save.

Ē

## To enable Active Directory in the Cellebrite UFED application:

This step is not required if you are using Cellebrite Commander.

1. In Cellebrite UFED go to **Settings** > **User Permissions**.

«	Reports	System	License	Version	Activity Log	User Permissions	≫
C	Disable USB device extr	action					
<b></b>	Enable Users Permissio	ns					
	Use Active Directory	/					
	Import						
					SAVE	CANCEL	

2. Select Use Active Directory.

You can only log in to the application using Active Directory users, there are no longer Cellebrite UFED users such as Manager and Investigator. After activating Active Directory either in Cellebrite Commander or Cellebrite UFED application.

3. Click **Save**. The following window appears.



4. Click OK and restart the Cellebrite UFED application.

For information about logging in to the Cellebrite UFED devices, see Logging in to Cellebrite UFED (on page 250).

### 13.7.1.7. Turning off default SSO when using Active Directory

This feature enables you to turn off the default permissions for SSO when using Active Directory authentication.

General	Reports	System	License	Version	Commander	Activity Log	User Permissions				
Disable USB device extraction											
Z Require login											
🗾 Use Activ	ve Directory										
🔽 Enabl	e SSO										

## 13.7.2. Enabling Active Directory in Cellebrite UFED application

Active Directory is a Microsoft product providing a range of directory-based identity-related services. It authenticates and authorizes all users and computers in a Windows domain type network, assigning and enforcing security policies for all computers and installing or updating software.

When a user logs in to the system, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user before allowing the user to log in. Active Directory also enables the management and storage of information at the admin level and provides authentication and authorization mechanisms.

Use the Windows Active Directory account to enable quicker and easier login to your Cellebrite UFED applications. Cellebrite UFED can manage the permissions with two permissions levels:

- \* Active Directory Groups
- <sup>\*</sup> Active Directory Users with Commander roles
### 13.7.2.1. Turning off default SSO when using Active Directory

This feature enables you to turn off the default permissions for SSO when using Active Directory authentication.



# 13.7.3. Permission management

Permission management can be performed via Cellebrite Commander or the Cellebrite UFED Permission Manager standalone application.

The Cellebrite UFED Permission Manager standalone application is available from <u>MyCellebrite</u>. Each profile contains access permissions, including operation rights per extraction type and content types. A single profile can be assigned to multiple users. The users and profiles can be exported into an encrypted permission management file, which can be imported into multiple Cellebrite UFED applications.

### 13.7.3.1. Using the Cellebrite UFED Permission Manager

#### To create a new profile:

- 1. Download the latest Cellebrite UFED Permission Manager application from your account in <u>MyCellebrite</u>, and save it to a directory on a computer or external device.
- 2. Run the Cellebrite UFED Permission Manager and follow the setup instructions. The Cellebrite UFED Permission Manager screen appears.

UFED Permiss	on Manager (4.2.5.111)		
	UFED Permission Manager	Export Import	
Â	Profiles		
	Users		
· <u>Ľ</u> -	Crime Types		
		DB v1	.6

3. Click **Profiles**.

UFED Permission Manager (4.2.3.5)		
New Profile	Profiles	
Admin Profile		
General Profile Extractions Only Generaland Settings General user as well as settings Investigator All extraction types and settings		
		 DB v1.5

4. Click New Profile. The following screen appears.

UFED Permission Manager (4.2.3.5)		
-	New profile	Delete
General Extraction	ypes	
Name:  Description: User Notification Load Text		
		Save

- 5. Enter a name and description for this profile.
- 6. If required, select **User Notification**, which enables you to load a RTF file with text and graphics for the profile.
- 7. Click the Extraction Types tab.



8. Select the options for this profile, such as Admin who can manage users, the Extraction Type (Logical Extraction, SIM Data extraction, Password extraction etc.) and UFED Settings (Activity Log).



At least one of the enabled users must be an Administrator (Admin).

9. Click Save and proceed to create a new user.

### To create a new user:

1. In the Cellebrite UFED Permission Manager screen, click **Users**. The following screen appears.

UFED Permission Man	ager (4.2.3.5)	
← New User	Users	
Admin UFED InField Investigate	<u>d</u> Admin User or prs that are not administrators	
		DB v1.5

2. Click **New User**. The following screen appears.

UFED Permission Manager		- <b>-</b> X
-	New user	Delete
Username	*	
Display Name	*	
Description		
Password	Password must contains at least 8 characters.	
Confirm Password	Password must contains at least 8 characters.	
Profile	*	~
Enabled?		
		Save

- 3. Enter the details for the new user including Username, Display Name, Description, and Password.
- 4. Select a profile for the user.
- 5. Select **Enabled** to enable the user.
- 6. Click Save.

### To manage crime types:

1. Click **Crime Types**. The following screen appears.

🔊 UFED Permissi	on Manager (4.2.5.111)		
New Cr	Crime Types	/pes	
Armed R Armed Ro Attemped Child Exp Child Exp Child Mo Child Mo Child Porr Counterfe Counterfe Crime Co	obbery bbery d Murder Murder oloitation oitation oitation lest st mography ography eiting ting nfinement	De v1.6	
ß	The crime types are only relevant for Cellebrite Responder	r.	
	You can delete all crime types; however you must add at least one crime to be able to export a permission management file.		
ð	To edit a crime type, click the crime type and edit the Nam	ne.	

2. Click **New Crime Type**. The following window appears.

UFED Permission N	fanager (4.2.5.111)	
+	New Crime Type	Delete
Name:		
Description:		
		Save
		DB v1.6

- 3. Enter a name for the crime type and (optional) description.
- 4. Click Save.

### To export an encrypted permission management file:

1. In the Cellebrite UFED Permission Manager screen, click **Export**, specify a directory for the file and click **Save**. The following screen appears.



Ē)

2. Click OK. The permission file must be imported into Cellebrite UFED via the User Permissions tab in the Settings window.

The next time you run the Cellebrite UFED Permission Manager, you are prompted for your user credentials to access the application.

# 14. Special cables

Cellebrite UFED requires a special cable for certain functions:

Device power-up cable (below)

Active extension cable (on the next page)

USB extension cable (on the next page)

USB cable for Cellebrite UFED Device Adapter V2 PowerUP (on page 262)

### 14.1. Device power-up cable

If the battery is drained or absent, the device power-up cable powers the device instead of the battery while performing an extraction.

The device power-up cable contains four parts marked as: Data, Extra power, -, +.



Phone power-up cable

#### To connect the device power-up cable:

- 1. Connect the Extra Power connector to the Cellebrite UFED USB Port extension.
- 2. Connect the Data connector to the Cellebrite UFED USB Port extension.
- 3. Identify the device's battery contacts:
  - a. Open the device battery cover.
  - b. Locate the positive (+) and negative (–) pole markings of the battery, usually found next to the contacts area.
  - c. Make sure that the battery contacts are marked clearly on the device's body.
  - d. Remove the battery to gain access to the device's battery contacts.

**TIP**: For battery contacts which are not clearly marked on the device's body, use the pole markings on the battery body to identify them. To do that, flip the battery along its contacts edge, and place it along the edge of the battery housing, then mark the device's contacts according to those on the battery.



Use a multimeter to identify the positive and negative poles of an unmarked battery.

- 4. Connect the **RED** alligator clip to the device's positive pole (+), the Primary **Black** alligator clip to the negative pole (-) and the secondary **Black** alligator clip to the middle pole if there are three poles or to the one next to the (-) if there are four poles. Make sure the alligator clips are not closing a circuit by touching each other.
- 5. Connect the source device to the **phone power-up cable** using the references cable from the cable organizer kit as listed in the Cellebrite UFED menu.

# 14.2. Active extension cable

This cable is 150 cm in length and allows for the easy and accessible placement of the Cellebrite UFED Device Adapter with USB 3.0. For more information about the adapter, see <u>Cellebrite UFED Device</u> Adapter with USB 3.0 (on page 14).

The USB Device Adapter Active extension cable is a custom made, high grade cable with an active USB 3.0 extension. It is a bus-powered extension cable that can be used to increase the length of the Cellebrite UFED Device Adapter without any signal loss or performance issues. It contains active electronics, which boost the USB signal for maximum reliability and performance over extended distances.

Only use the previous USB extension cable (USB Extension cable for Cellebrite UFED Device Adapter) with the Cellebrite UFED Device Adapter with USB 2.0.

### 14.3. USB extension cable

This USB extension cable is 150 cm in length and allows for the easy and accessible placement of the Cellebrite UFED Device Adapter V2. In a desktop environment where the computer is mounted in a difficult to access or distant location use the USB Extension cable.

The USB Extension cable is a custom made high grade cable. This high grade cable prevents voltage fluctuation and is shielded from EMI interference which would cause signal degradation or loss.

If you need an extension cable, you **must** use the provided USB Extension cable. Use of third-party cables affects performance of your Cellebrite UFED and may prevent some functions from starting or completing.

# 14.4. USB cable for Cellebrite UFED Device Adapter V2 PowerUP

- The following USB PowerUP cables are applicable to the Cellebrite UFED Device Adapter V2. These cables are **no longer required** with the Cellebrite UFED Device Adapter V3.
- \* The USB Cable for Cellebrite UFED Device Adapter PowerUP S for use with your Cellebrite UFED. It is 75cm in length.
- \* The USB Cable for Cellebrite UFED Device Adapter PowerUP L for use with your Cellebrite UFED. It is 150cm in length.

Both cables provide the same functionality and differ only in length.

The PowerUP cable has a miniUSB male end which plugs into the Cellebrite UFED Device Adapter V2 and a USB-A connector that can be plugged into any available powered USB port - including A/C powered USB chargers and car chargers.

The PowerUP cable doubles the power capacity of the Cellebrite UFED Device Adapter V2. This ensures that all devices with excess power requirements function correctly and allows Cellebrite UFED to provide all functions. In addition devices that are fully discharged may need the additional power that the PowerUp cable provides.

In the laptop environment, we recommend that you use the PowerUp cable when Cellebrite UFED indicates that the extra power is required.

The PowerUp cable is NOT required for smooth operation of the Cellebrite UFED for most devices, but is provided for those cases where power consumption is above the capacity of the unpowered Cellebrite UFED Device Adapter V2.

# 15. Index

### А

Accessories 13 Activating the license 25 Active Directory 245 Activity log 242 Activity Log 256 ADB, definition 129 Android backup 22, 117, 121-122, 126 Android backup APK downgrade 123 Android extraction methods 168 APK downgrade 123 APK for Android backup APK downgrade 22 Application taskbar 62 Autodetecting 44 **B** 

Bluetooth scan 200 Bluetooth, logical extraction 96 Boot Loader, definition 129 Bootloader extraction 168, 170 C Camera checklist, importing 238 Camera screen, enabling 211 Capture 12, 174, 179 Capture images 12, 173-175 Capture images and screenshots 12, 174 Case details 51 Case details, importing 239 Cellebrite YouTube channel 18 Changing the application interface language 213 Changing the extraction location 216 Clone SIM 180, 184-185, 191, 195 Cloning an existing SIM card ID 185 Console, Android Debug 45, 83 D

Device power-up cable 260 Device tools 63, 196 Dongle 26, 33, 40, 229 Dongle license 32 Drone, extractions 173 **E** Entering SIM data manually 191 Exit Motorola bootloop 203 Exit recovery mode 202 Export options 27, 62, 237, 242, 258 Extracted passwords folder 76 Extracted SIM data folder 183 Extracting Android devices 168 Extraction in progress 74, 103, 130, 134, 156, 163, 189, 193, 195 Extractions, (Refer to Performing extractions in MyCellebrite) 12, 67, 72, 76, 82, 91, 95, 100, 104, 111, 120, 126, 132, 135, 157, 159, 163, 167, 169, 177, 179, 182, 252, 255 Extractions, refer to Performing extraction in MyCellebrite 13 F File system extraction 12, 200 File system extraction folder 106 file system extractions, timeframe options 59 Files, logical extraction type 85, 94 Flashing 154 Forensic recovery partition 160 FW flashing 154 G General settings 84, 209 Getting started 19 GSM test SIM 195 Н Help 82 Home screen 43, 51, 76, 87, 91, 95, 100, 104, 111, 120, 126, 132, 135, 137, 144, 157, 159, 163, 167, 177, 179,

182, 196, 228, 230

I IMEI, search 46 Importing settings and configuration files 237 Interface language 209, 213 Introduction 10 Investigation notes 51 iOS extraction 89 iTunes backup encryption 92 J JTAG 122 Legal notices 9 license not found 225 License settings 224

icense settings 2.

Licensing 26

Logging in 250

Logical extraction 10, 12-13, 17, 82, 89, 92, 96, 100, 180, 212, 256

#### Μ

Managing report fields 221

### Ν

Network 39 Network dongle 39 Nokia WP8 recovery tool 204

#### 0

Odin mode 203 Online license 25 Overview 10, 82, 89, 93, 102, 117, 123, 129, 133, 137, 154, 158, 161, 164 Ρ Password extraction 74, 256 Performing a physical extraction 129 Performing extractions 13, 45, 83 Performing SIM data extraction 180 Permission management 254 Permission Manager 244, 248, 254 Permissions Users 244 Physical extraction 12, 110, 128-129, 132-133, 136, 154, 158, 160, 169-170, 204 Q Qualcomm chipsets 158 R Re-enable User Lock option 77 Report settings 217 Rooted Android devices, physical extraction 133 S

Screenshots 12, 53, 174, 178

Searching for a device 46

Select content types 17 Select extraction location 154 Selective extraction 59-60 Settings 22, 51-52, 59, 100, 112, 117, 127, 137, 168, 208, 214, 217, 234-235, 252, 256 SIM data extraction 180, 183 Simplified Chinese 215 Smart ADB method, tool 204 Software license 35-36, 38 Sounds, play notifications 223 Special cables 260 Specifications 9 Specify a network location 63 Starting the application 42 Supported devices 17 Switch to CDMA offline mode 206 System requirements 11 System settings 84, 223 Т TAC number search 49 Technical terms 172

#### U

UFED Device Adapter 14, 16, 74, 130, 134, 161, 181, 185, 191, 198, 200, 204, 206, 261-262 UFED User Lock Code Recovery Tool 204

Unallocated space 12

Update via the web 235

Updates and versions 235

User permissions 244

User predefined filter 59

Using cables and tips 17

### ۷

Version details 233

### W

Working with TomTom 198