cellebrite
delivering mobile expertise

UFED series

UFED 4PC

User Manual

January 2015

Legal Notices

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

This manual contains proprietary information belonging to Cellebrite Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the UFED 4PC.

- No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite Ltd.
- The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice.
- Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are Fictitious unless otherwise noted.

WARNING: UFED 4PC should be used only with the dedicated AC/DC adapter supplied with this device.

WARNING: USB, Ethernet and target and source connectors should be connected only to CE approved devices (according to IEC/EN 60065 standard).

WARNING: Make sure that all external connections to other devices (except for the power adapter) are only indoor and SELV (safety extra low voltage, not exceed 42.4 V peak or 60 VDC).

FCC Warning: This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions:

1) This device may not cause harmful interference

2) This device must accept any interference received, including interference that may cause undesired operation

Contents

Chapter 1: Introduction 9

1.1. Overview 9

1.2. System requirements 11

1.3. UFED 4PC extraction types and device tools 12

1.4. UFED 4PC accessories 16

1.4.1. UFED Device Adapter 17

1.4.2. Using cables and tips 18

1.5. Supported devices 21

1.6. Cellebrite YouTube channel 21

Chapter 2: Getting started 23

2.1. Installing UFED 4PC 23

2.2. Activating the license 29

2.2.1. Using a dongle 29

2.2.2. Using a software license 31

2.2.3. Using a network dongle 34

2.2.4. Using an online license 37

2.3. Working with UFED 4PC 40

2.3.1. Opening UFED 4PC 40

2.3.2. Home screen 40

2.3.3. Detect automatically 43

2.3.4. Search function 46

2.3.5. Manual selection 48

2.3.6. Application taskbar 51

Chapter 3: Logical extraction 53

3.1. Performing logical extraction 54

3.1.1. Connect mobile device 55

3.1.2. Select phone memory 56

3.1.3. Select content types 57

3.1.4. Extraction in progress 61

3.1.5. The extracted data folder 67

Chapter 4: Password extraction 69

4.1. Performing password extraction 69

4.2. The extracted passwords folder 75

4.3. Disabling the password 76

Chapter 5: File system extraction 81

5.1. Performing a file system extraction 81

5.2. The file system extraction folder 88

5.3. Android backup 90

Chapter 6: Physical extraction 97

6.1. Performing a physical extraction 97

6.2. The physical extraction folder 107

Chapter 7: Capture images and screenshots 109

7.1. The UFED camera 109

7.1.1. Contents 110

7.2. Capturing images 110

7.3. Capturing screenshots 121

Chapter 8: SIM card functionality 126

8.1. SIM data extraction 126

8.1.1. Performing SIM data extraction 126

8.1.2. The extracted SIM data folder 137

8.2. Clone SIM 137

8.2.1. Cloning an existing SIM card ID 138

8.2.2. Entering SIM data manually 145

8.2.3. Creating a GSM test SIM 154

Chapter 9: Device tools 159

9.1. Bluetooth Scan 161

9.2. Switch to CDMA offline mode 164

9.3. Test peek/poke functionality 166

9.4. Activate TomTom trip log 168

9.5. Uninstall windows mobile client 168

9.6. Uninstall Android client 169

9.7. Exit Odin mode 169

Chapter 10: Settings 171

10.1. General settings 172
10.1.1. Managing the custom list 173
10.1.2. Changing the application interface language 177
10.1.3. Mobile extraction client 181
10.1.4. Changing the extraction location 182
10.2. Report settings 183
10.2.1. Managing report fields 186
10.3. System settings 189
10.4. License settings 191
10.5. Version details 193
10.5.1. Updates and versions 194
10.6. User permissions 195
10.6.1. Permission management 197
Chapter 11: Special cables 205
11.1. Device power-up cable 205
11.2. USB extension cable for UFED Device Adapter 207
11.3. USB Cable for UFED Device Adapter PowerUP 207
Chapter 12: Regulatory compliance 209
Chapter 13: Extracting Android devices 211
13.1. Android extraction methods 211
13.1.1. Android debugging bridge method 212
13.1.2. Bootloader extraction 215
13.2. Performing a file system extraction for an Android device 216
13.2.1. Locked Motorola devices 216
13.2.2. Locked HTC, Huawei, and ZTE devices ...217
13.2.3. Other locked devices 218
13.2.4. Unlocked devices 219
13.3. Technical terms 220
Chapter 14: Appendix 221

Chapter 1: Introduction

UFED 4PC is a new generation application that empowers law enforcement, military, intelligence, corporate security, and e-discovery personnel to capture critical forensic evidence from all mobile devices. This includes mobile phones, handheld tablets, portable GPS devices, and devices manufactured with Chinese chipsets.

1.1. Overview

UFED 4PC enables you to:

- Perform physical, file system, and logical extraction of device data and passwords. Capabilities may vary, based on the UFED 4PC product purchased - UFED 4PC Logical or UFED 4PC Ultimate.
- Extract vital data such as call logs, phonebook entries, text messages (SMS), pictures, videos, audio files, 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.
- Clone 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.

1.2. System requirements

PC	Windows compatible PC with a Pentium® IV or compatible processor running at 1.6 GHz or higher
Operating system	Microsoft Windows XP with SP3 or later Microsoft Windows Vista, Windows 7 or Windows 8 Microsoft Windows 7 Boot Camp on MAC
Memory (RAM)	OS — Recommended — Minimum 32 bit — 4GB — 4GB 64 bit — 8GB — 4GB
Space requirements	500 MB of free disk space for installation
Additional requirements	Microsoft .Net version 4.0
Processor	USB 3.0 Chipset, Renesas,® Intel®
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.

NOTE: This specification is for a PC running both UFED 4PC and the Physical Analyzer application as the decoding operations of the Physical Analyzer require the higher specification. For a standalone PC running UFED 4PC only an ATOM based chipset (or equivalent) is sufficient.

NOTE: To enable extraction to a PC with Windows Vista Operating System, follow the procedure in enabling connectivity with Windows Vista.

1.3. UFED 4PC extraction types and device tools

UFED 4PC includes a range of data extraction types that can be accessed through the Select Extraction Type screen.

NOTE: The available extraction functionalities may vary, based on the type of product purchased; the UFED 4PC Logical or the UFED 4PC Ultimate product.

Table 1-1: Functionalities of the UFED 4PC products

Functionality	UFED 4PC Logical	UFED 4PC Ultimate
Logical Extraction	Yes	Yes
SIM Data Extraction	Yes	Yes
Password Extraction	Yes	Yes
Clone SIM	Yes	Yes
File System Extraction	Not available	Yes
Physical Extraction	Not available	Yes
Capture Images/Screenshots	Optional	Yes

The extraction types are:

- *Logical extraction* (page *53*)

  Logical Extraction enables the extraction of various data types. This includes call logs, phonebook entries, SMS text messages, MMS, emails, calendar events, multimedia files (images, videos, and so on), and more.

- *SIM data extraction* (page *126*)

  SIM Data Extraction enables the extraction of information from a SIM or USIM card.

- *File system extraction* (page *81*)

  File System Extraction enables a full system extraction of a source mobile device's memory.

- *Password extraction* (page *69*)

  Password Extraction enables the extraction and display of passwords from a source mobile device directly in the **Password Obtained** screen.

- *Clone SIM* (page *137*)

  Clone SIM ID copies a SIM ID from one SIM card to a UFED SIM ID Access Card.

- *Physical extraction* (page *90*)

  Physical Extraction uses advanced methods in order to extract a physical bit-for-bit image of the flash memory of a mobile device, including unallocated space. Unlike conventional logical extraction processes, physical extraction bypasses the mobile device's operating system, and extracts data from the phone's internal flash memory directly. Unallocated space may contain deleted items such as SMS, call logs, phonebook entries, pictures, and video and audio files.

- *Capture images and screenshots* (page *109*)

  Capture images and screenshots using the UFED camera to take pictures or videos of a device. You can also capture internal screenshots directly from the connected device.

All extraction types can be saved to your PC, or to a removable storage device, as desired.

The *Device tools* (page *159*) menu tab is also located in the Select Extraction Type screen, and includes:

- Bluetooth scan
- Switch to CDMA offline mode
- Odin mode
- Test Peek/ Poke functionality
- Activate TomTom trip log
- Uninstall Windows Mobile Client
- Uninstall Android Client

1.4. UFED 4PC accessories

The UFED 4PC kit includes connection cables and tips. These are used in order to connect mobile devices to UFED 4PC.

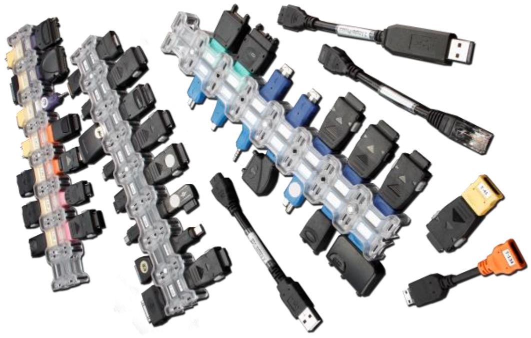


Figure 1: UFED 4PC Cables and tips

The UFED 4PC Ultimate kit contains tips and cables for logical, file system, and physical extractions.

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

1.4.1. UFED Device Adapter

The UFED 4PC kit contains a device adapter that attaches to your PC's USB port.

The device adapter has the following connectors for source devices:

- SIM card reader
- USB port
- RJ45 port

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.

NOTE: Some devices can be extracted only by using the UFED Device Adapter.

1.4.2. Using cables and tips

The cables and tips set includes up to various adapter cables (the number of cables depends on the UFED product and kit purchased). Each cable has a letter and name for example: A Adapter – USB.

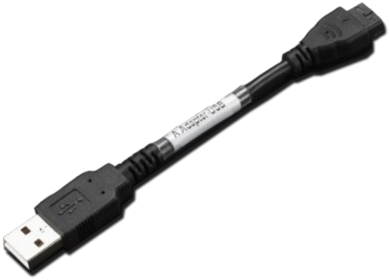


Figure 2: Single cable

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

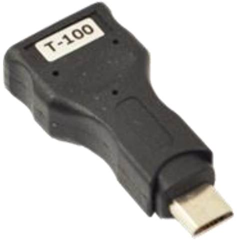
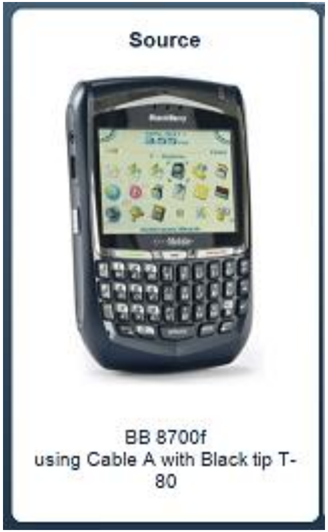


Figure 3: UFED Touch tip (example)

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



Source

BB 8700f
using Cable A with Black tip T-80

Figure 4: Enlargement of notification

1.5. Supported devices

To find out which mobile devices are supported in UFED 4PC and which data extraction capabilities are available for every mobile device use one of the following:

1) The UFED <version no> Supported Phone List file is delivered with every UFED software version update. The Microsoft Excel file contains two worksheets:

   The **UFED Logical** sheet lists the mobile devices supported for logical extraction.

   The **UFED Physical** sheet lists the mobile devices supported for physical, file system, and password extractions.

2) **UFED Phone Detective** (devices supported for logical extraction only).
3) On Cellebrite's website:

   http://www.cellebrite.com/mobile-forensics/support/ufed-supported-devices

1.6. Cellebrite YouTube channel

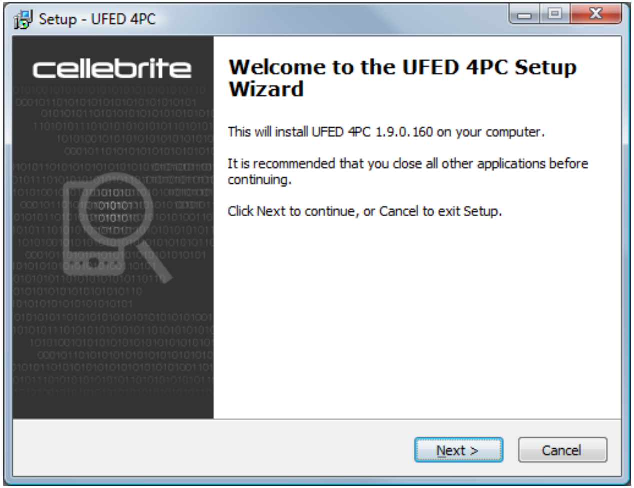
For your convenience, a selection of useful videos demonstrating typical work flows and common procedures are available at youtube.com/cellebriteufed.

Chapter 2: **Getting started**

2.1. Installing UFED 4PC

1) Open the UFED 4PC installation wizard.

   The UFED 4PC Installation wizard screen appears.



Welcome to the UFED 4PC Setup Wizard

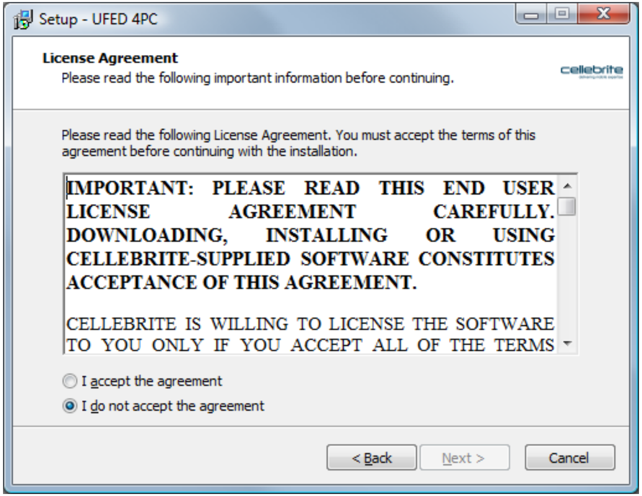
This will install UFED 4PC 1.9.0.160 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

2) Click **Next**.

The License Agreement screen appears.



License Agreement

Please read the following important information before continuing.

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. DOWNLOADING, INSTALLING OR USING CELLEBRITE-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

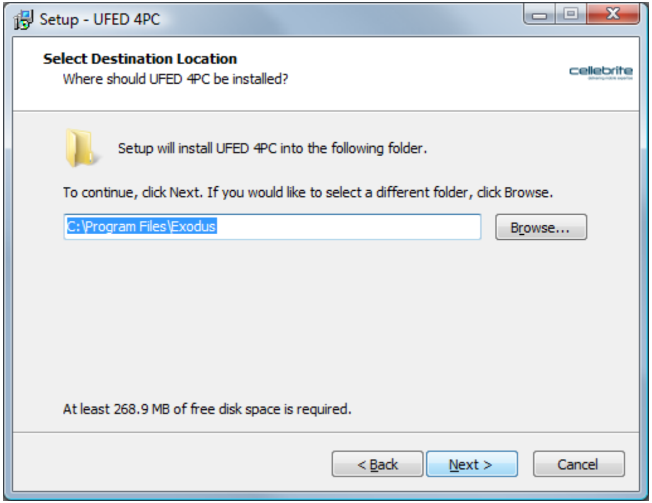
CELLEBRITE IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY IF YOU ACCEPT ALL OF THE TERMS

○ I accept the agreement

● I do not accept the agreement

3) Select **I accept the agreement**, and click **Next**.

The Select Destination Location screen appears.



Select Destination Location

Where should UFED 4PC be installed?

Setup will install UFED 4PC into the following folder.

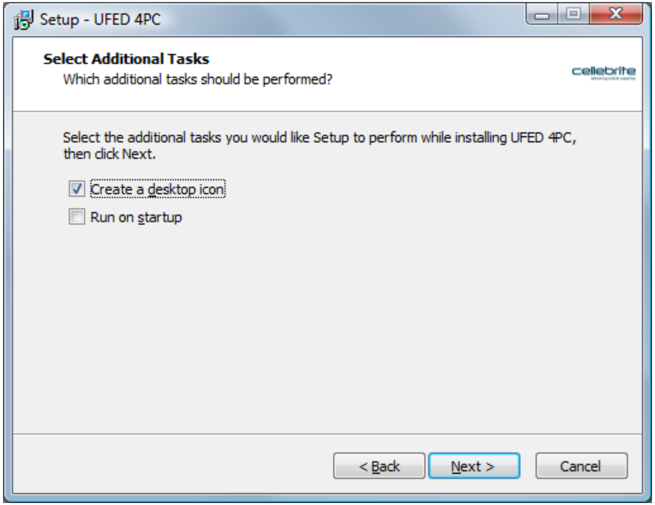
To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Exodus

At least 268.9 MB of free disk space is required.

4) Select the folder where you want the application installed, and click **Next** to continue.

The Select Additional Tasks screen appears.



Setup - UFED 4PC

Select Additional Tasks

Which additional tasks should be performed?

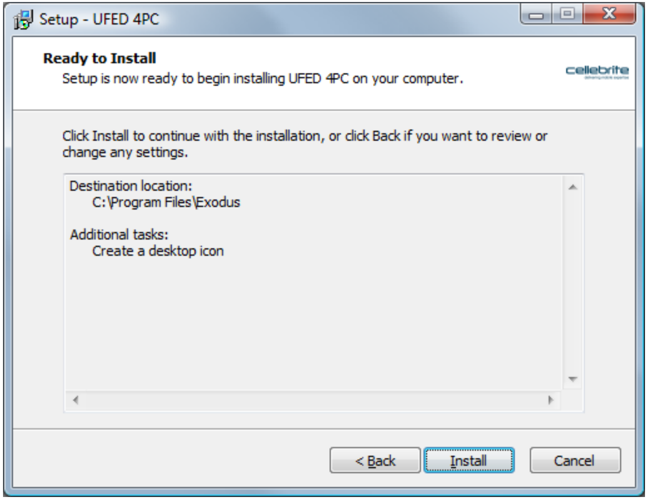
Select the additional tasks you would like Setup to perform while installing UFED 4PC, then click Next.

☑ Create a desktop icon

□ Run on startup

5) Select the additional tasks you want the install wizard to perform, and then click **Next**.

The Ready to Install screen appears.



Ready to Install

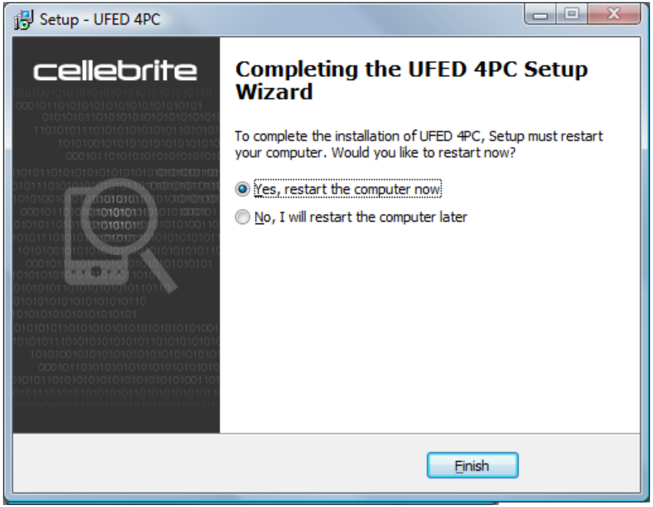
Setup is now ready to begin installing UFED 4PC on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\Exodus

Additional tasks:
Create a desktop icon

6) Click **Install**.



Completing the UFED 4PC Setup Wizard

To complete the installation of UFED 4PC, Setup must restart your computer. Would you like to restart now?

● Yes, restart the computer now

○ No, I will restart the computer later

7) Select **Yes, restart the computer now**, and click **Finish** to restart the computer.

You must now activate the license to use UFED 4PC. Proceed to *Activating the license* (page *29*).

2.2. Activating the license

Activate UFED 4PC in one of the following ways:

- *Using a dongle* (page *29*)
- *Using a software license* (page *31*)
- *Using a network dongle* (page *34*)
- *Using an online license* (page *37*)

NOTE: Check your UFED 4PC kit to make sure which method you should use.

2.2.1. Using a dongle

Use the UFED dongle provided with your UFED 4PC kit. The dongle contains licenses for all the applications purchased.

UFED Dongle

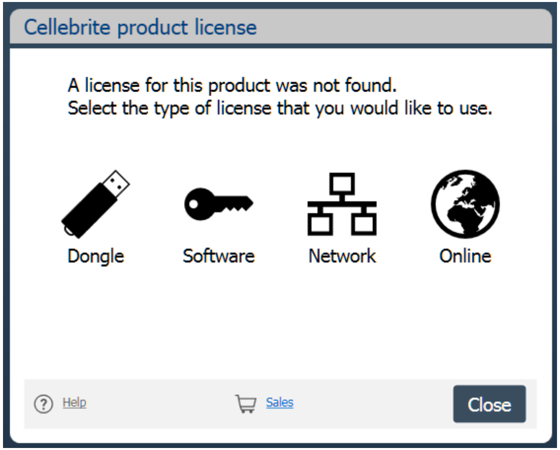
To use UFED 4PC with a dongle:

1) Connect the dongle to a USB port on your computer. The license is automatically located. When the dongle is recognized by the operating system, the application can read the license.
2) Start the application.

Congratulations, your UFED 4 PC 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.



Cellebrite product license

A license for this product was not found.
Select the type of license that you would like to use.

2) Click Dongle. If you connected the dongle to a USB port on your computer, and it still does not work, contact support@cellebrite.com.

NOTE: The HASP dongle drivers must be installed in order to use a hardware license key. If the drivers were not installed during the software installation process, you can run the installation process again and select Install Hasp Dongle Drivers at the end of the process.

2.2.2. Using a software license

Activation Code

Use the PC activation code provided with your UFED 4PC kit to download a software license.

To use UFED 4PC with a software license:

1) Go to https://my.cellebrite.com/ufed4pc and sign in to your MyCellebrite account.

   (If you do not have an account, click **Register now** and create a user. Then go back to https://my.cellebrite.com/ufed4pc.)

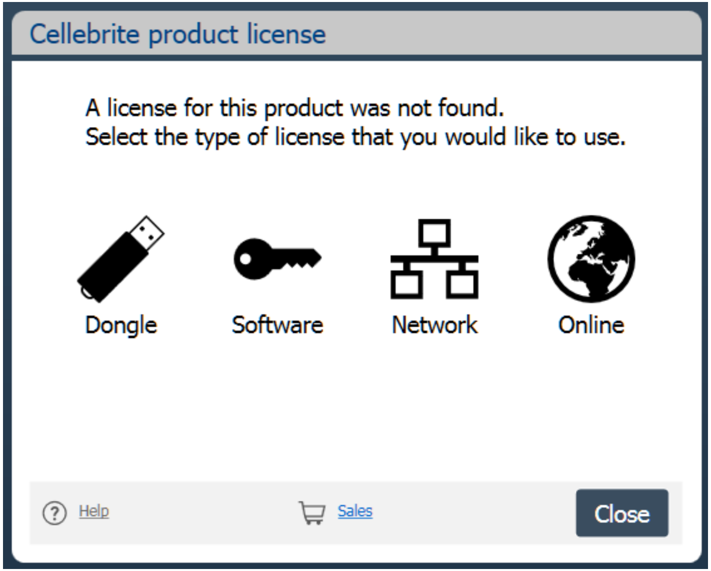
   You are directed to the UFED 4PC activation window.

2) Click **Download UFED 4PC** 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 https://my.cellebrite.com/ufed4pc link.
5) In the Activation Code field, enter the Activation code provided with your UFED 4PC kit.

Activation Code

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

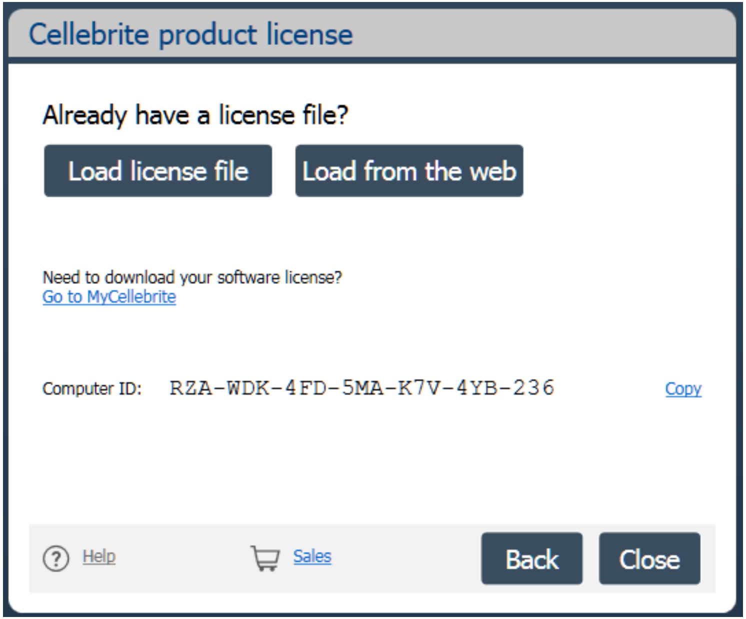
a) Start the application. The Cellebrite product licensing window appears.



Cellebrite product license

A license for this product was not found.
Select the type of license that you would like to use.

b) Click . The following window appears.



Cellebrite product license

Already have a license file?

Need to download your software license?
Go to MyCellebrite

Computer ID: RZA-WDK-4FD-5MA-K7V-4YB-236

c) Click **Copy** to copy the Computer ID displayed in the window.

7) In MyCellebrite paste the copied Computer ID.

Computer ID

8) Click **Generate License** to download the application license key to your PC. The license key will also be sent to your registered MyCellebrite email address.
9) In the UFED 4PC 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 upload the license file from MyCellebrite.

Congratulations, your UFED 4PC application is now ready!

2.2.3. Using a network dongle

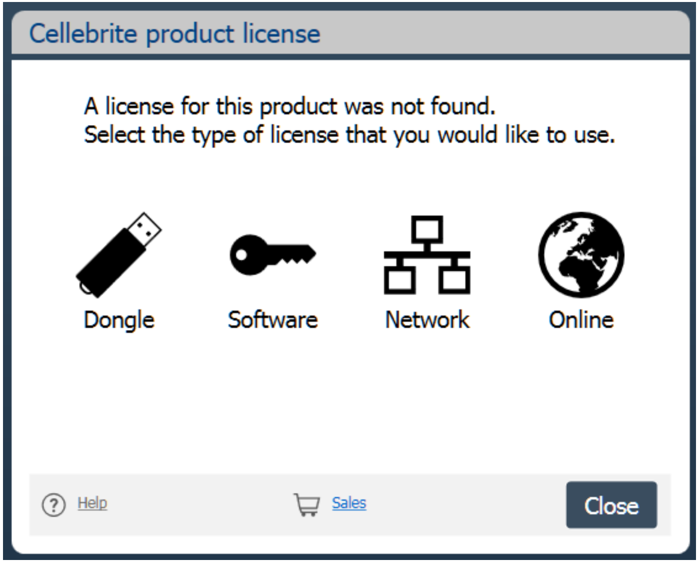
UFED network dongles

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

To use UFED 4PC with a network dongle:

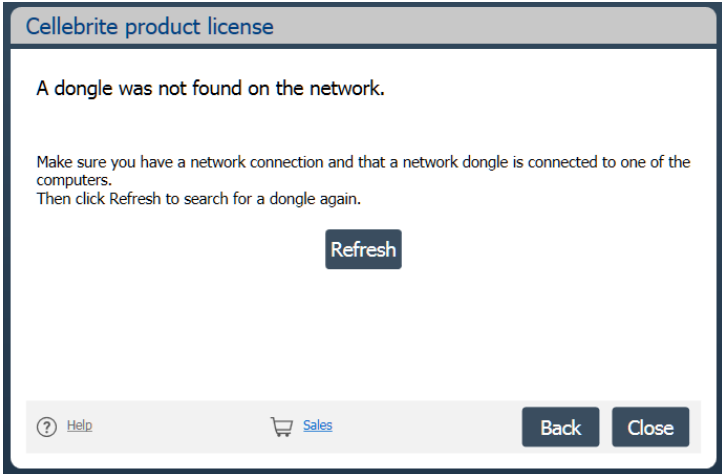
1) Start the application. If the network dongle is connected to the network, the application starts and you can start working immediately.

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


Cellebrite product license

A license for this product was not found.
Select the type of license that you would like to use.

2) Click Network. The following window appears.



Cellebrite product license

A dongle was not found on the network.

Make sure you have a network connection and that a network dongle is connected to one of the computers.
Then click Refresh to search for a dongle again.

NOTE: 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 Refresh to search for a network dongle again.

NOTE: If you click Refresh twice, a new window will appear where you can manually connect to the network dongle. Click Advanced and then enter the IP address (or host name).

NOTE: If there is only one network dongle it will be selected automatically. If there are multiple network dongles, select the required Dongle Serial number.

Congratulations, your UFED 4PC application is now ready!

2.2.4. Using an online license

Use the PC activation code provided with your UFED 4PC kit to download an online license.

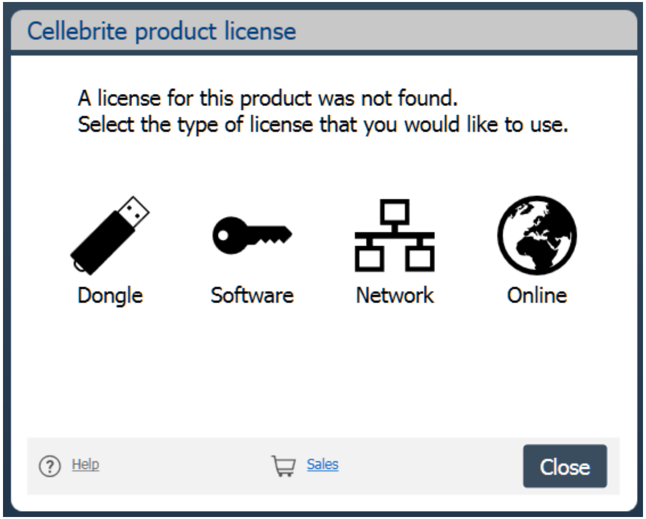
To use UFED 4PC with an online license:

1) Go to https://my.cellebrite.com/ufed4pconline and log on to your MyCellebrite account.

   (If you do not have an account, click Register now and create a user. Then go back to https://my.cellebrite.com/ufed4pconline.)

   You are directed to the UFED 4PC activation window.

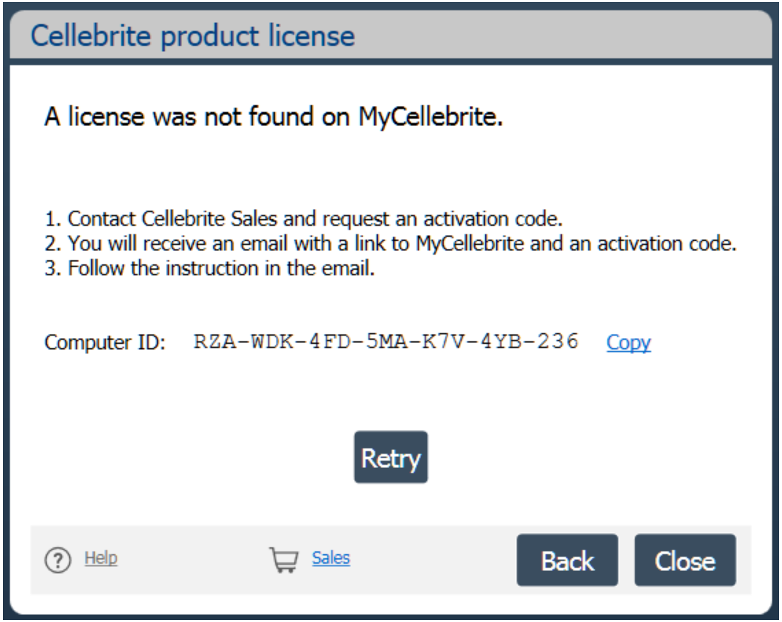
2) Click **Download UFED 4PC** and follow the installation instructions.
3) Start the application. When starting for the first time, or when a license is not found, the Cellebrite product license window appears.



Cellebrite product license

A license for this product was not found.
Select the type of license that you would like to use.

4) Click Online. The following window appears.



Cellebrite product license

A license was not found on MyCellebrite.

1. Contact Cellebrite Sales and request an activation code.
2. You will receive an email with a link to MyCellebrite and an activation code.
3. Follow the instruction in the email.

Computer ID: RZA-WDK-4FD-5MA-K7V-4YB-236

5) Click **Copy** to copy the Computer ID displayed in the window.

6) In the https://my.cellebrite.com/ufed4pconline page, in the Activation Code field, enter the code provided with your UFED 4PC kit.

Activation Code

7) In the Computer ID field, paste the Computer ID that you copied in step 5.

Computer ID

8) Click **Generate License**.
9) Make sure you have an Internet connection on your computer and then click **Retry** in the Cellebrite product license window.

Congratulations, your UFED 4PC application is now ready!

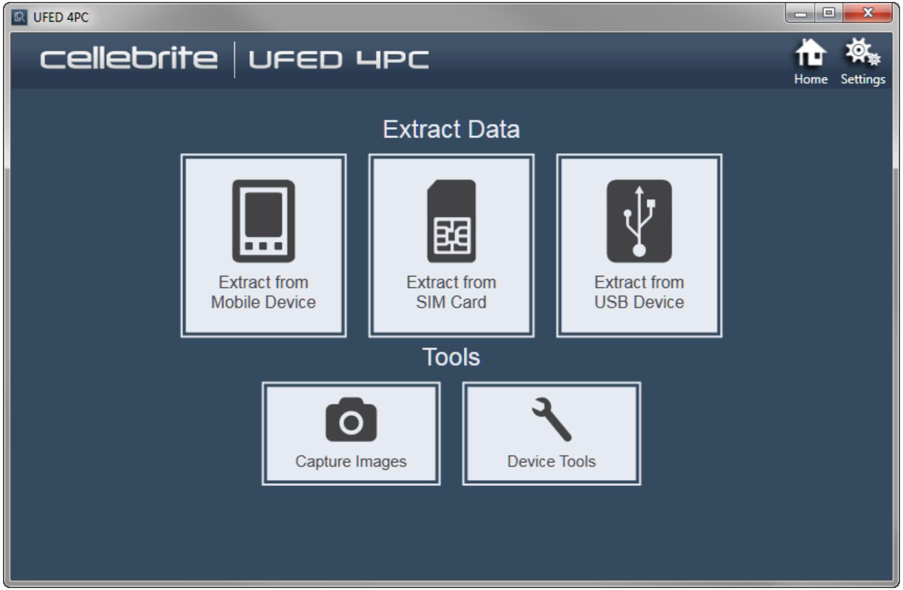
2.3. Working with UFED 4PC

2.3.1. Opening UFED 4PC

- Double-click the UFED 4PC icon to open the application.

2.3.2. Home screen

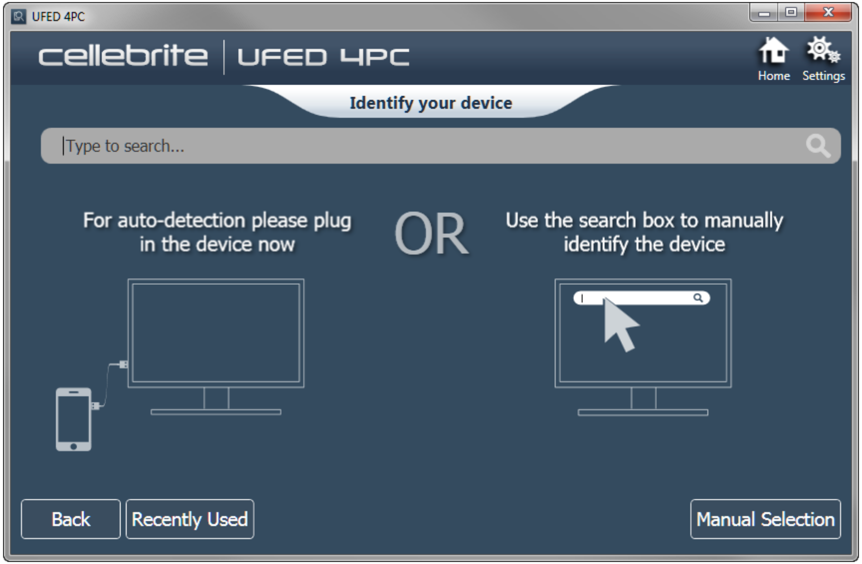
The home screen groups the extraction data into distinct areas: mobile device, SIM card and USB device. In addition, users can directly operate the camera for immediate image capturing or access the device tools. All extraction functionality is driven by **automatic** identification of the device, by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


UFED 4PC
cellebrite | UFED 4PC
Home
Settings
Extract Data
Extract from Mobile Device
Extract from SIM Card
Extract from USB Device
Tools
Capture Images
Device Tools

To extract data from a device:

- Select Extract from Mobile Device.

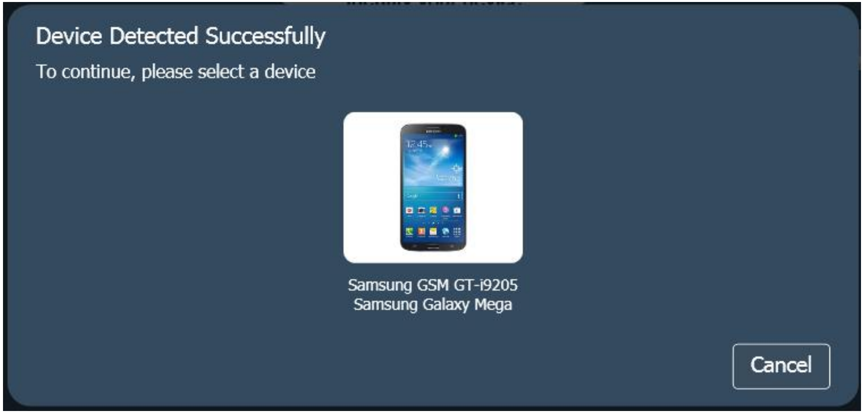
  The following screen appears.



2.3.3. Detect automatically

To use the Autodetect function to locate the mobile device:

1) Connect the mobile device to UFED 4PC.



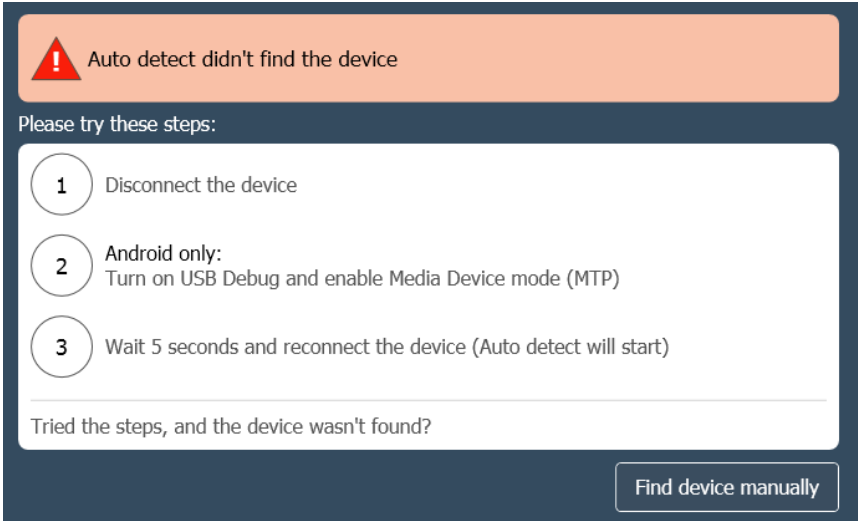
Device Detected Successfully

To continue, please select a device

Samsung GSM GT-i9205
Samsung Galaxy Mega

2) Click the device.
3) In the event that the device has not been connected, a waiting for a device to be connected prompt appears - connect the device.

4) If the connected device cannot be recognized by the system, a message prompts you to try the following steps or click **Find device manually**.



⚠ Auto detect didn't find the device

Please try these steps:

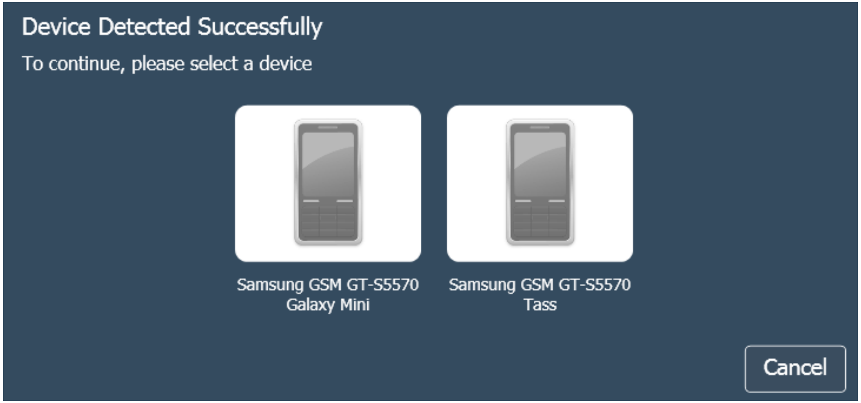
1 Disconnect the device

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?

In the event that multiple matches are found, the Select Autodetected Model screen appears.



Device Detected Successfully

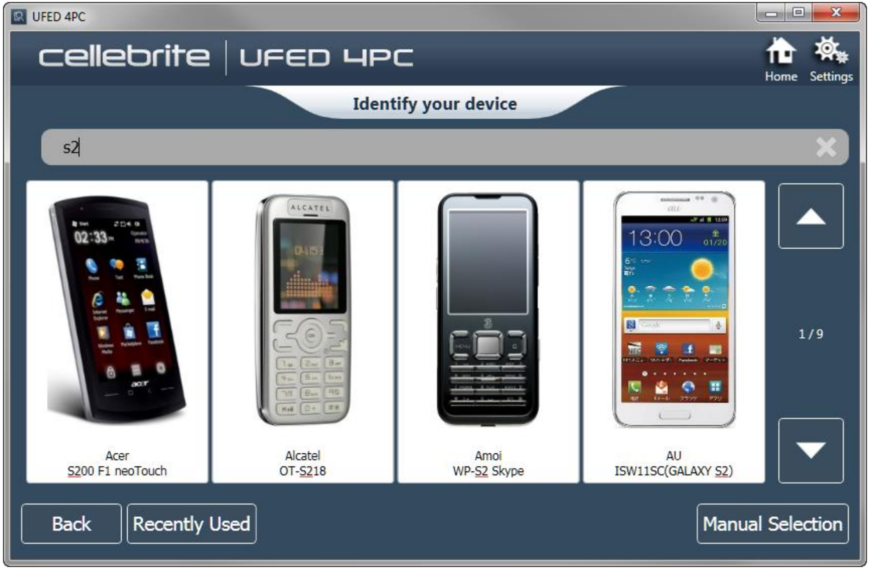
To continue, please select a device

5) Select the relevant device.

2.3.4. Search function

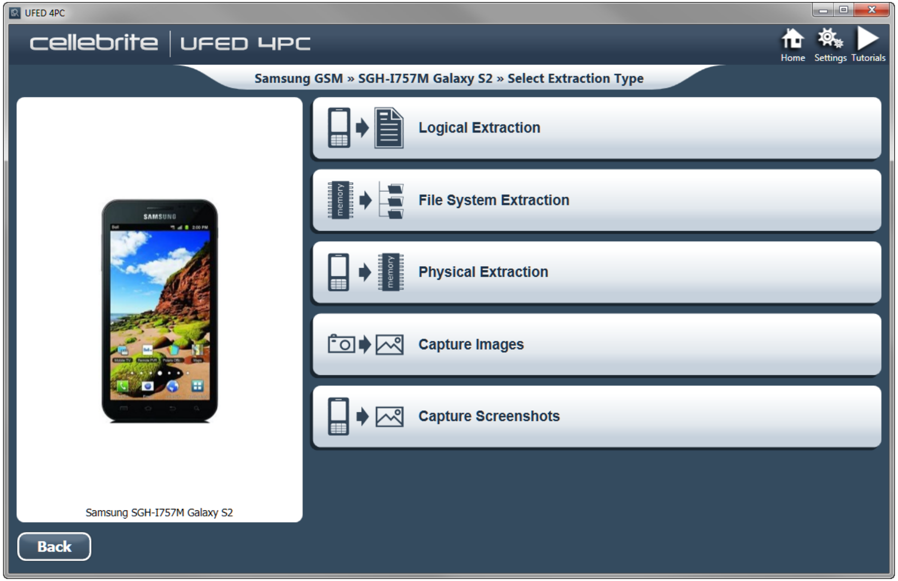
To search for the mobile device:

1) Begin typing the search for device box. As you type each letter, the list of devices is reduced to meet the criteria. In this example "sa" is the search criteria, and the devices that match the criteria are displayed.



2) Select the device model type from the list.

Having selected the **device**, UFED 4PC will determine what extraction functions are available for this combination and present those functions as follows:

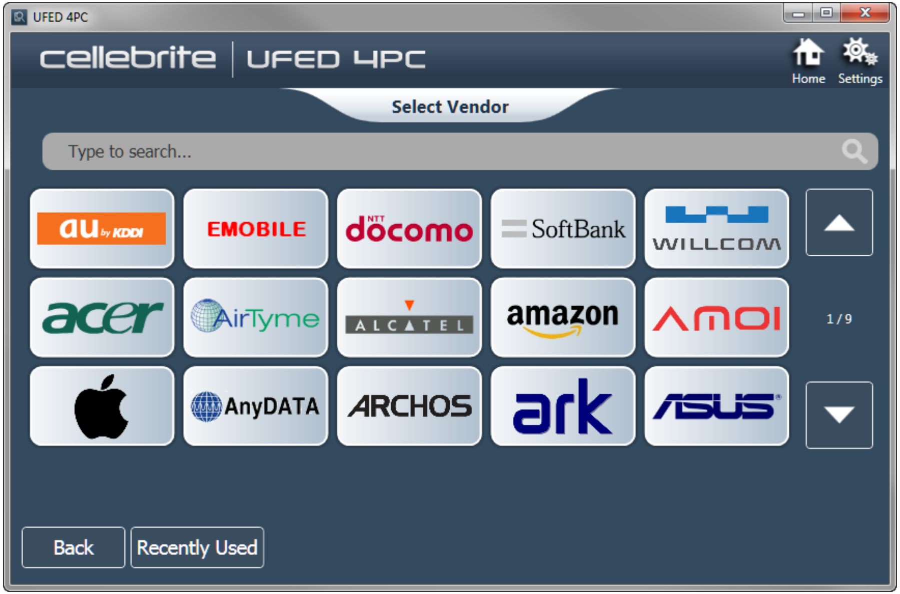


2.3.5. Manual selection

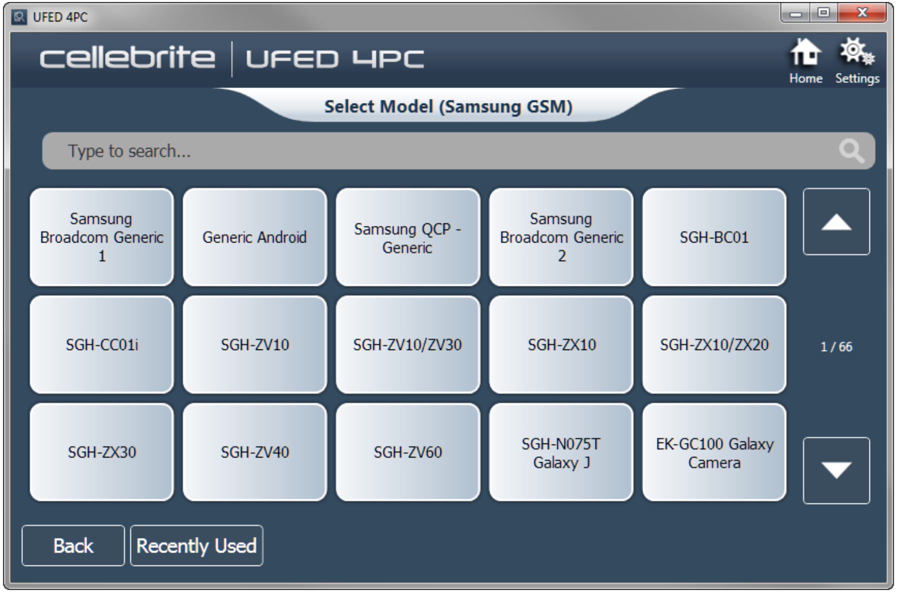
To manually select the vendor and model:

1) Click **Extract from Mobile Device** and then click **Manual Selection**.

   The Select Vendor screen appears where the vendor of the device is chosen.



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**, UFED 4PC will determine what extraction functions are available for this combination and present those functions.

The possible extractions are:

- *Logical extraction* (page *53*)
- *Password extraction* (page *69*)
- *File system extraction* (page *81*)
- *Physical extraction* (page *90*)
- *Capture images and screenshots* (page *109*)

There is also the option to use Device Tools or SIM Card functionality.

- *Device tools* (page *159*)
- *Clone SIM* (page *137*) and *SIM data extraction* (page *126*)

2.3.6. Application taskbar

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

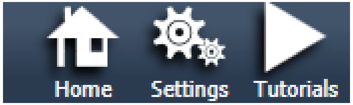


Table 2-1: Application taskbar icons and descriptions

Icon	Description
Home	Return to home screen
Settings	Display the Settings screen from where the device settings can be defined.
Tutorials	Video tutorials. **NOTE:** When UFED 4PC is connected to the Internet, you will receive an automatic notification to install the video tutorials. You can also install the video tutorials manually by downloading the media package from MyCellebrite and then install it via the **Version** tab (**Settings** > **Version** > **File**).

Chapter 3: **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.) from a source device and saved to your PC or to a removable storage device, as desired.

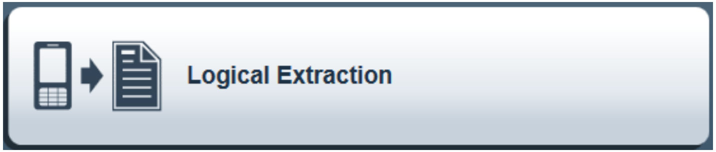
In addition, data can be extracted from many Android and iOS apps. For an updated list of supported apps and versions for each platform, refer to the Decoding Android Apps and Decoding iOS Apps documents in MyCellebrite or from the **Help** > **Supported Apps** menu in UFED Physical/Logical Analyzer. Data extracted from these apps can be analyzed using UFED Physical/Logical Analyzer (although the data is not included in UFED HTML and XML reports).

NOTE: 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 Phone List Microsoft Excel file.

3.1. Performing logical extraction

To perform a logical extraction from a mobile device:

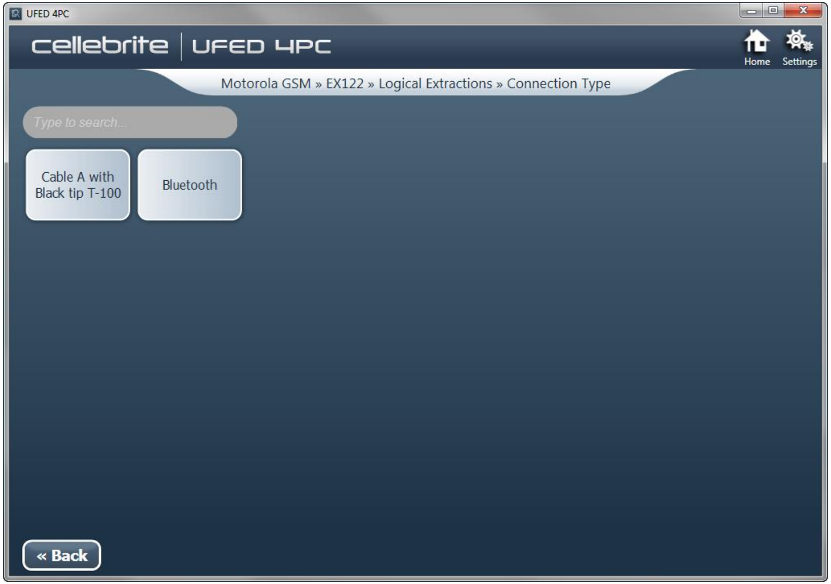
- Click **Extract from Mobile Device** and identify the device, then click **Logical Extraction**.



3.1.1. Connect mobile device

NOTE: The following screen appears only when more than one connection option is available.

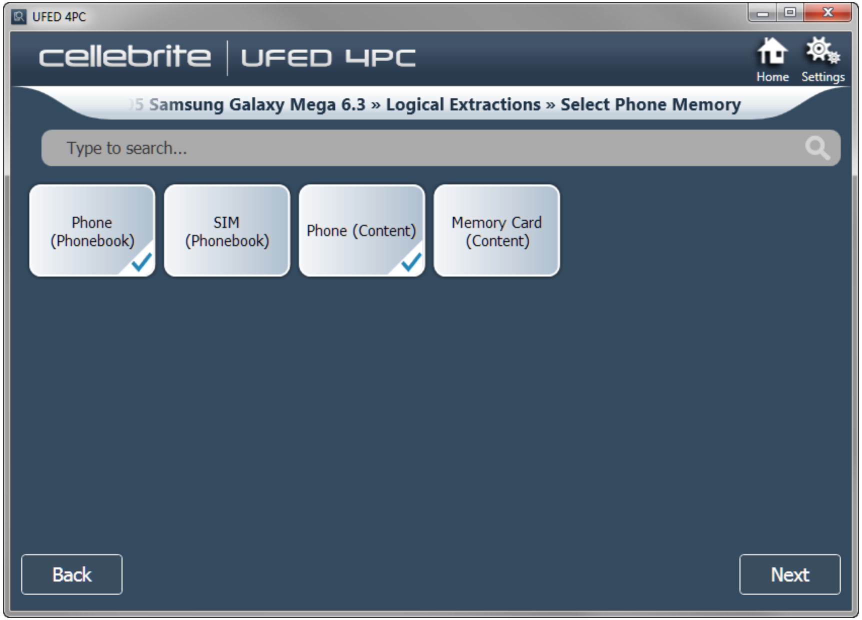
NOTE: For Apple devices use the generic option that is available when selecting a device.


UFED 4PC
cellebrite | UFED 4PC
Home
Settings
Motorola GSM » EX122 » Logical Extractions » Connection Type
Type to search...
Cable A with Black tip T-100
Bluetooth
« Back

- Select the connection type from the options shown.

3.1.2. Select phone memory

Data can be extracted from the device memory, memory cards and SIM memory of the device. All memories can be selected or only one. The types of memories can vary between devices. Where only a single memory is available, this screen is not displayed.



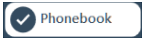
To select the phone memory:

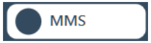
1) The Phone memory selection box is selected by default. It can be deselected if desired.
2) Select any other memories, as desired.
3) Click **Next** to continue.

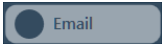
   The Select extraction location screen appears.

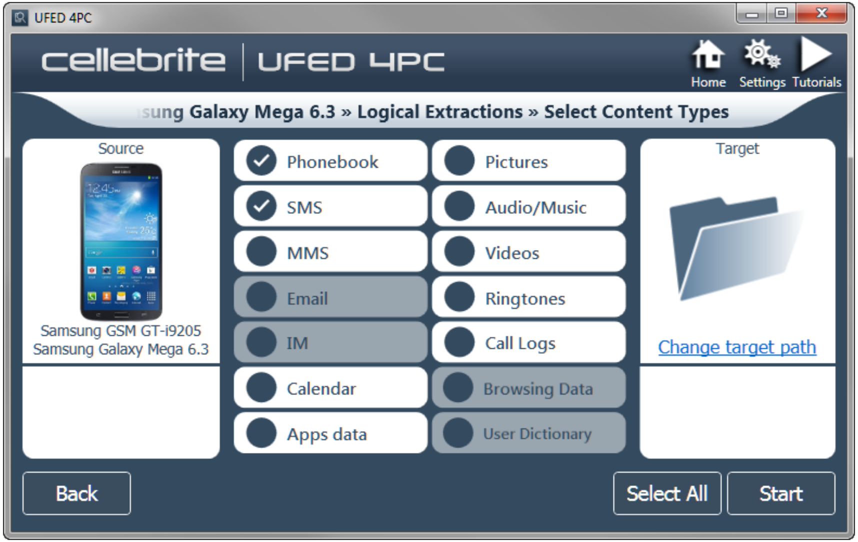
3.1.3. Select content types

Multiple content types are listed. The types are displayed in three different ways:

- Types selected by default – shown with a check mark. 

- Types available for selection – shown without check marks. 

- Types not available – shown as dimmed. 



To select content types:

1) Select the additional content types required to be included in the information extracted from this device.

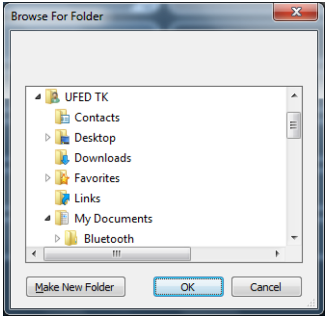
2) Select **Select All** to select all the available types.

NOTE: Only content types that are supported by the selected device are enabled for selection. Unsupported content types appear dimmed.

3) Click **Start** to continue.

4) To change the target path:

   a) Click **Change target path**.



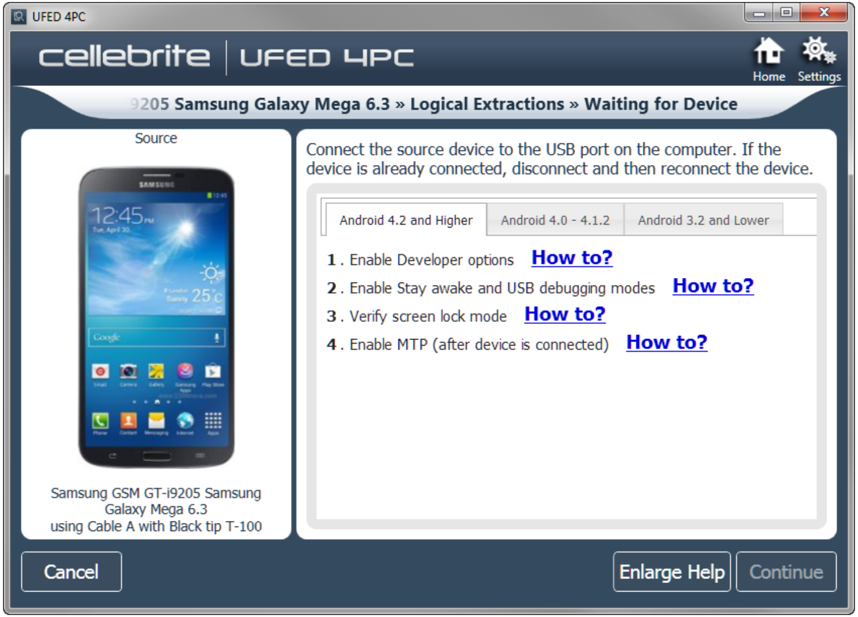
   b) In the Browse for Folder dialog, browse to the location where you want to save the extraction.

   c) Select the desired location, or click **Make New Folder** to create a target directory.

   d) Click **OK**.

   The target path is set.

The Waiting for Device screen appears.



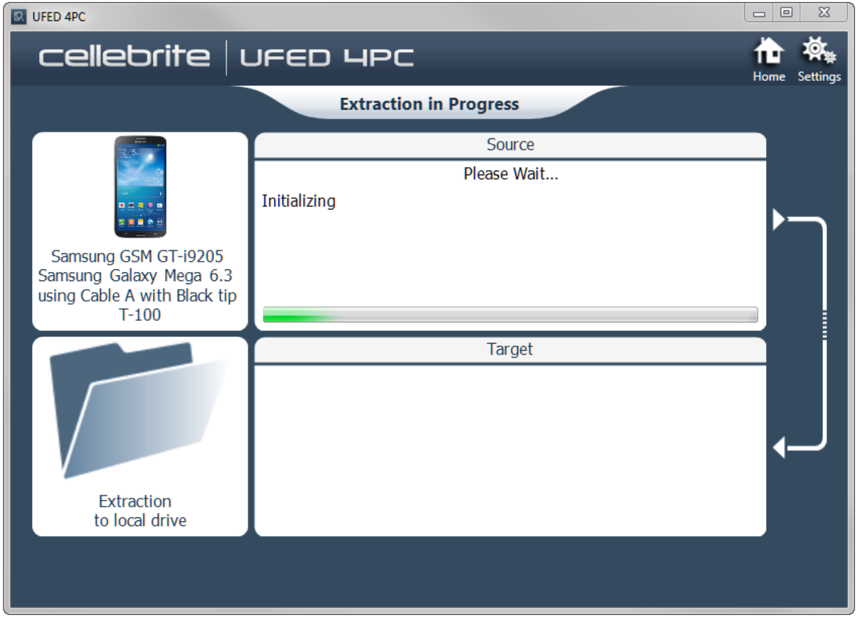
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with Black tip T-100

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

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?

5) Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
6) Click **Continue**.

3.1.4. Extraction in progress



Please Wait...

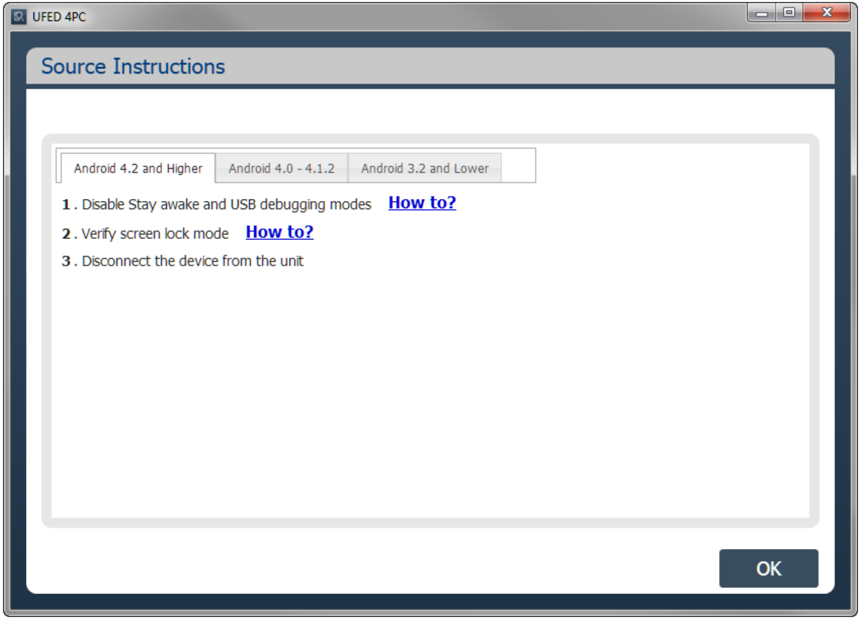
Initializing

Samsung GSM GT-i9205
Samsung Galaxy Mega 6.3
using Cable A with Black tip
T-100

Extraction
to local drive

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

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



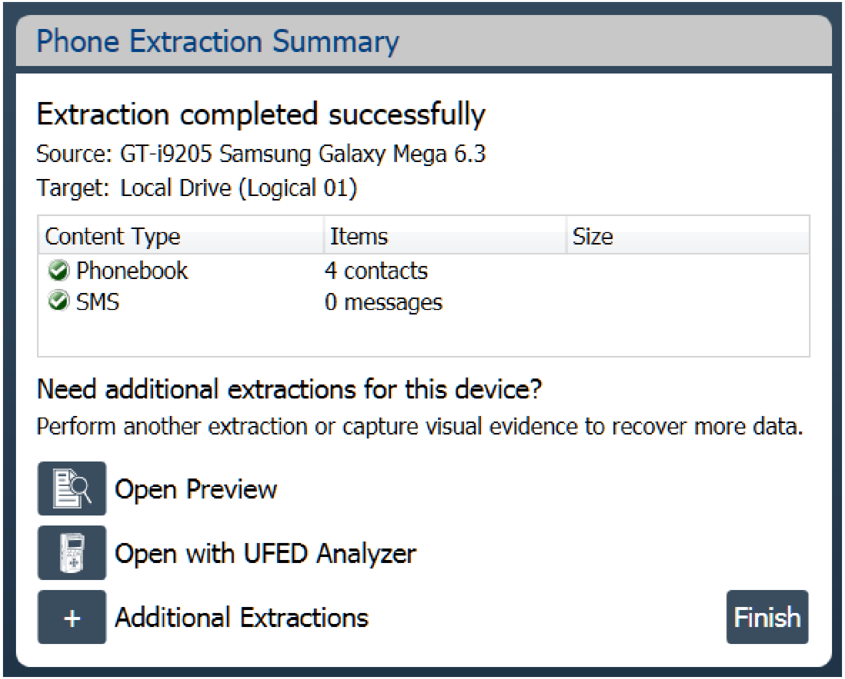
1 . Disable Stay awake and USB debugging modes

2 . Verify screen lock mode

3 . Disconnect the device from the unit

1) Follow the instructions to return the mobile device settings to the correct settings.
2) Click **OK**.

   The Phone Extraction Summary screen appears.



Phone Extraction Summary

Extraction completed successfully

Source: GT-i9205 Samsung Galaxy Mega 6.3

Target: Local Drive (Logical 01)

Content Type	Items	Size
✓ Phonebook	4 contacts	
✓ SMS	0 messages	

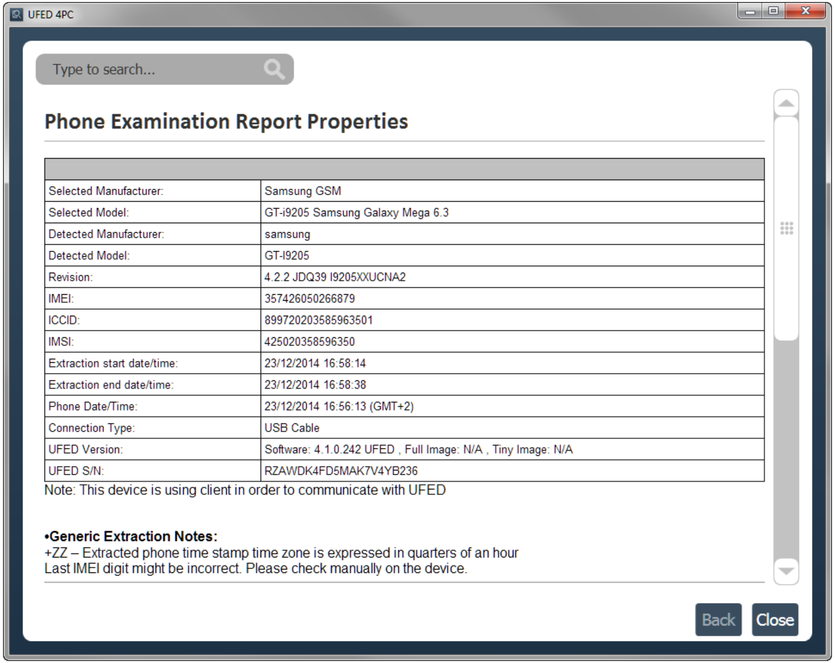
Need additional extractions for this device?

Perform another extraction or capture visual evidence to recover more data.

3) Click the required button.

🔍	To view an HTML preview report that includes information about the device and the extraction.
📱	To open the extraction in UFED Physical/Logical Analyzer.
+	To add additional extraction types for the same device.
Finish	To end the process and return to the home screen.

Examples of a preview report and the additional extraction type screens are show next.

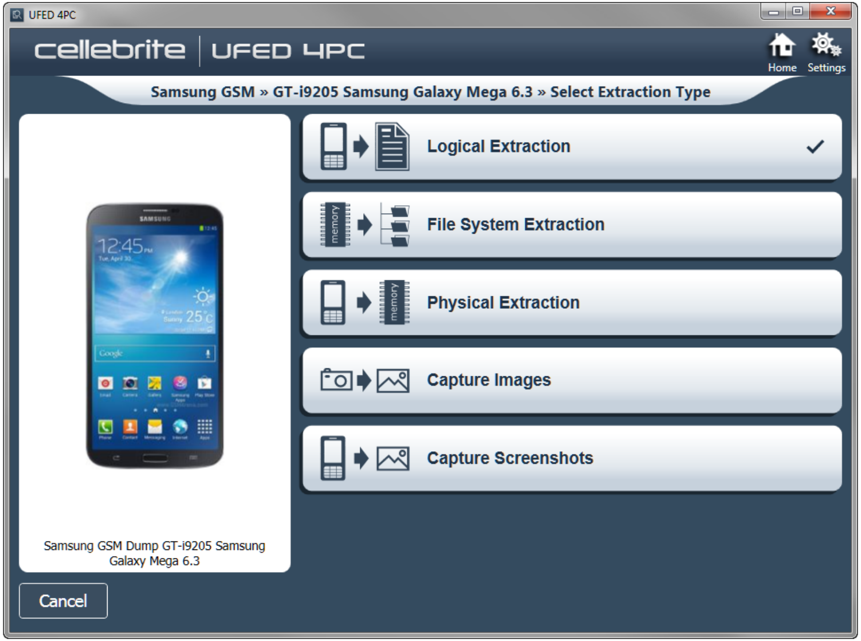


Phone Examination Report Properties

Selected Manufacturer:	Samsung GSM
Selected Model:	GT-i9205 Samsung Galaxy Mega 6.3
Detected Manufacturer:	samsung
Detected Model:	GT-I9205
Revision:	4.2.2 JDQ39 I9205XXUCNA2
IMEI:	357426050266879
ICCID:	899720203585963501
IMSI:	425020358596350
Extraction start date/time:	23/12/2014 16:58:14
Extraction end date/time:	23/12/2014 16:58:38
Phone Date/Time:	23/12/2014 16:56:13 (GMT+2)
Connection Type:	USB Cable
UFED Version:	Software: 4.1.0.242 UFED , Full Image: N/A , Tiny Image: N/A
UFED S/N:	RZAWDK4FD5MAK7V4YB236

Note: This device is using client in order to communicate with UFED

•Generic Extraction Notes:
+ZZ – Extracted phone time stamp time zone is expressed in quarters of an hour
Last IMEI digit might be incorrect. Please check manually on the device.



UFED 4PC

cellebrite | UFED 4PC

Samsung GSM » GT-i9205 Samsung Galaxy Mega 6.3 » Select Extraction Type

Samsung GSM Dump GT-i9205 Samsung Galaxy Mega 6.3

3.1.5. The extracted data folder

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

NOTE: The extracted data folder is named "UFED" with the selected device name, the IMEI/MEID info. 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)
- UFED Manager files of the extracted calls log (*.clog), phonebook (*.pbb), SMS messages (*.sms), and calendar (*.cal) Email (*.Email), MMS (*.MMS) and IM (*.IM) data.
- UFD file.

NOTE: UFED Manager files are generated only for data types that contain items.

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

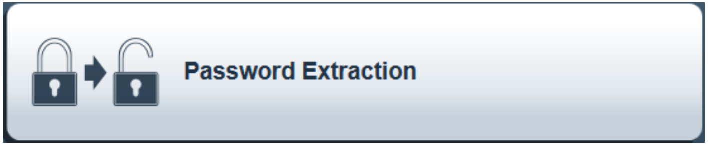
Chapter 4: **Password extraction**

The Extract Password function can extract the password from a device.

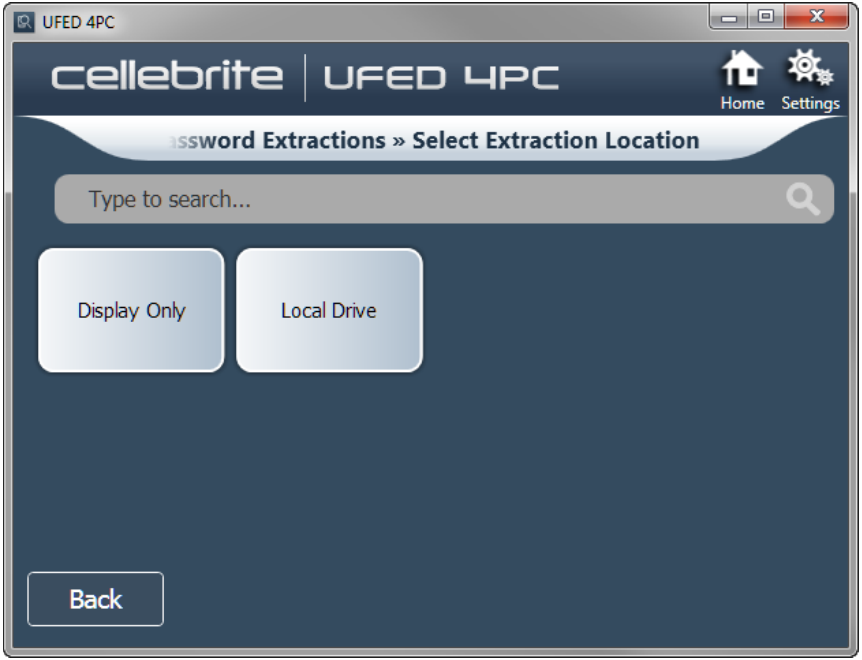
4.1. Performing password extraction

To extract passwords from a mobile device:

1) Click **Extract from Mobile Device** and identify the device, then click **Password Extraction**.

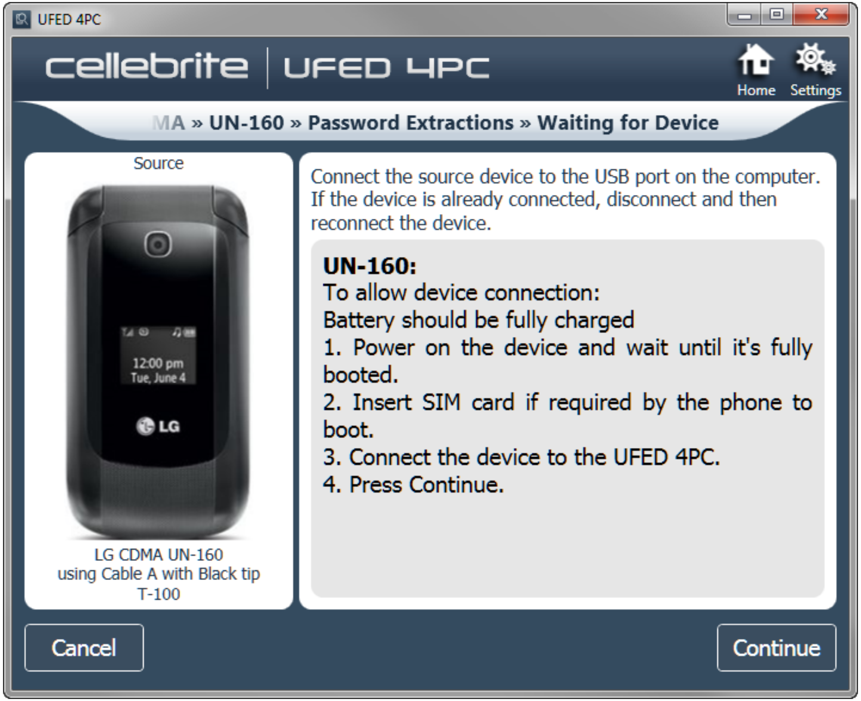


2) The Select Extraction Location screen appears.



3) Select **Display Only** or **Local Drive**.

The Waiting for Device screens appears.



LG CDMA UN-160
using Cable A with Black tip
T-100

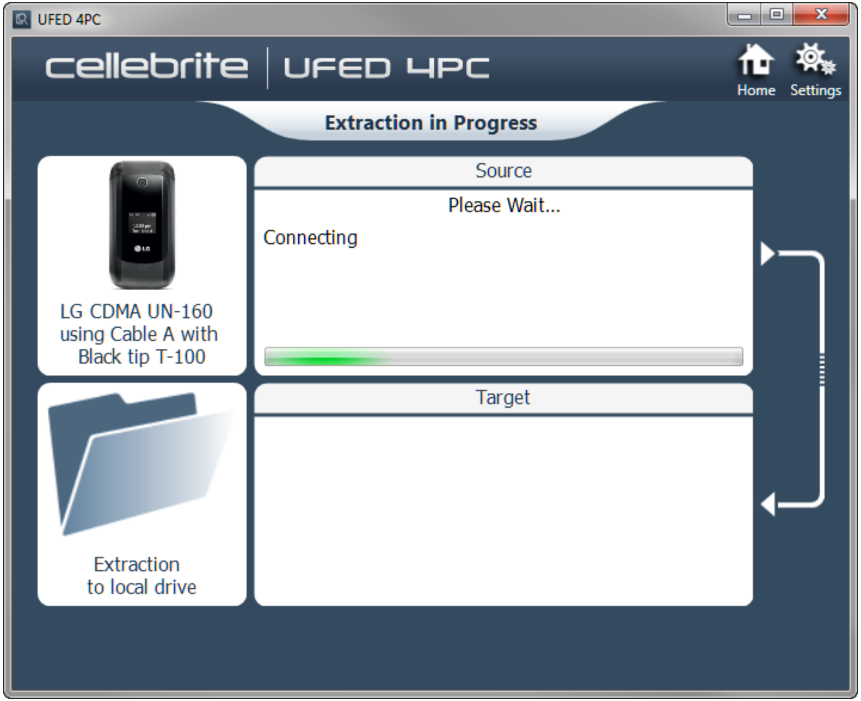
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

UN-160:
To allow device connection:
Battery should be fully charged
1. Power on the device and wait until it's fully booted.
2. Insert SIM card if required by the phone to boot.
3. Connect the device to the UFED 4PC.
4. Press Continue.

4) Connect the source device, either directly to the PC, or via the UFED Device Adapter.

5) Click **Continue**.

The Extraction in Progress screen appears.



Extraction in Progress

LG CDMA UN-160 using Cable A with Black tip T-100

Source

Please Wait...

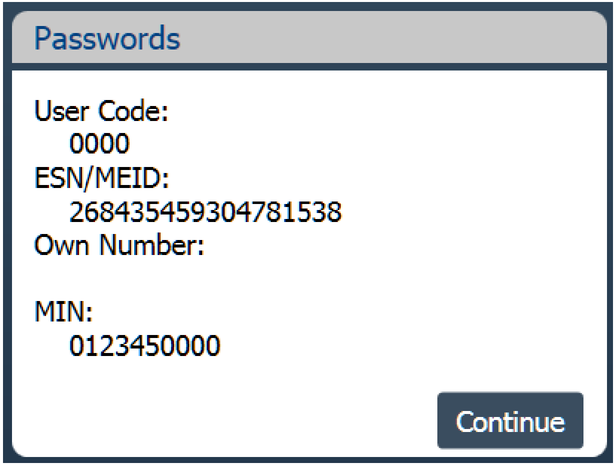
Connecting

Extraction to local drive

Target

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

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



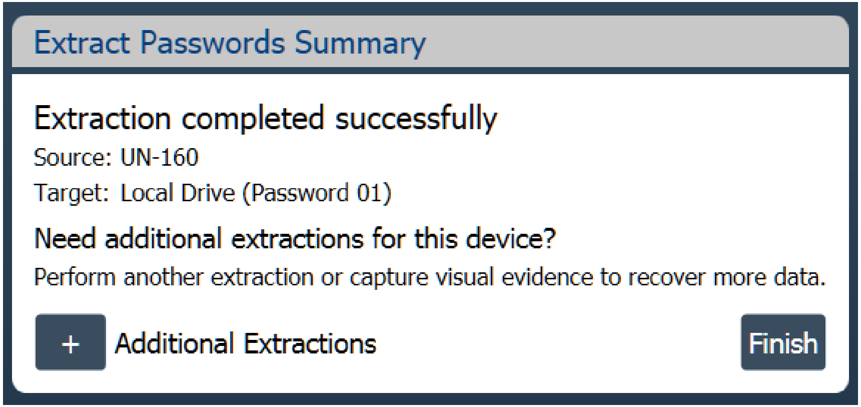
Passwords

User Code:
0000
ESN/MEID:
268435459304781538
Own Number:

MIN:
0123450000

7) Click **Continue**.

The following screen appears.



Extract Passwords Summary

Extraction completed successfully

Source: UN-160

Target: Local Drive (Password 01)

Need additional extractions for this device?

Perform another extraction or capture visual evidence to recover more data.

8) Click the required button.

+	To add additional extraction types for the same device.
Finish	To end the process and return to the home screen.

4.2. The extracted passwords folder

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.

NOTE: 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)"

4.3. Disabling the password

You can disable the password for particular devices. For example:

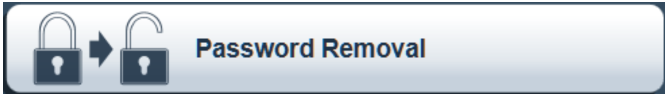
Apple	iPhone 2G
Apple	iPhone 3G
SamsungCDMA	SPH-M820 Galaxy Prevail (Android)
SamsungGSM	SGH-T499 Dart (Android)
SamsungGSM	SGH-T589 Gravity Smart (Android)
SamsungGSM	SGH-i857 Doubletime (Android)
SamsungGSM	GT-i5500 Europa Galaxy 5 (Android)
SamsungGSM	GT-i5510 Galaxy (Android)
SamsungGSM	GT-S5570 Galaxy Mini (Android)
SamsungGSM	GT-S5660 Galaxy Gio (Android)
SamsungGSM	GT-S5670L (Android)
SamsungGSM	GT-S5830 Ace (Android)

For a complete list of supported devices, refer to
http://www.cellebrite.com/mobile-forensics/support/ufed-supported-devices

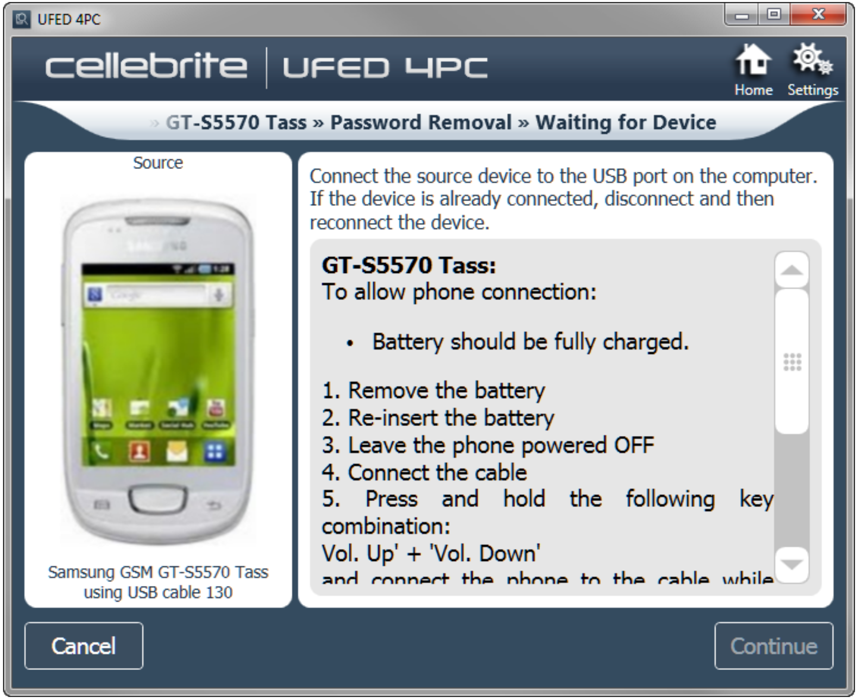
When you disable the password, UFED 4PC disables the code that enables the password.

Each device model has a slightly different process, depending on the phone lock combination and how the model connects to UFED 4PC.

1) Click **Extract from Mobile Device** and identify the device, then click **Password Removal**.



The Waiting for Device screen appears.



» GT-S5570 Tass » Password Removal » Waiting for Device

Samsung GSM GT-S5570 Tass using USB cable 130

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

GT-S5570 Tass:
To allow phone connection:

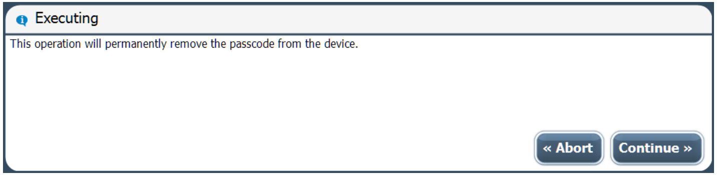
- Battery should be fully charged.

1. Remove the battery
2. Re-insert the battery
3. Leave the phone powered OFF
4. Connect the cable
5. Press and hold the following key combination:
Vol. Up' + 'Vol. Down'
and connect the phone to the cable while

2) Follow the instructions for the device and then click **Continue**.

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

   The following screen appears.

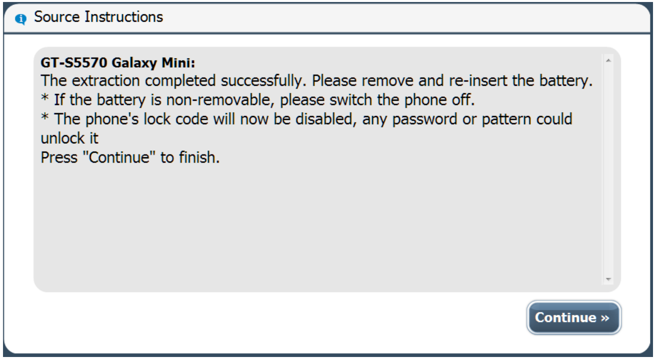


Executing

This operation will permanently remove the passcode from the device.

3) Click **Continue** and follow any on-screen instructions.

   The following the screens appears.

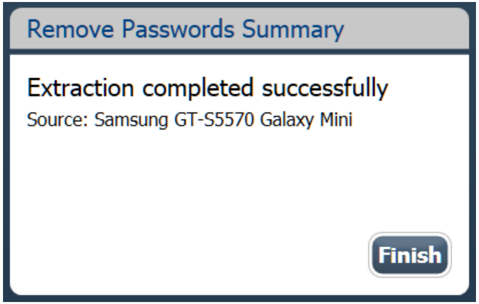


Source Instructions

GT-S5570 Galaxy Mini:
The extraction completed successfully. Please remove and re-insert the battery.
* If the battery is non-removable, please switch the phone off.
* The phone's lock code will now be disabled, any password or pattern could unlock it
Press "Continue" to finish.

4) Click **Continue.**

The following screen appears.



Remove Passwords Summary

Extraction completed successfully

Source: Samsung GT-S5570 Galaxy Mini

5) Click **Finish.**

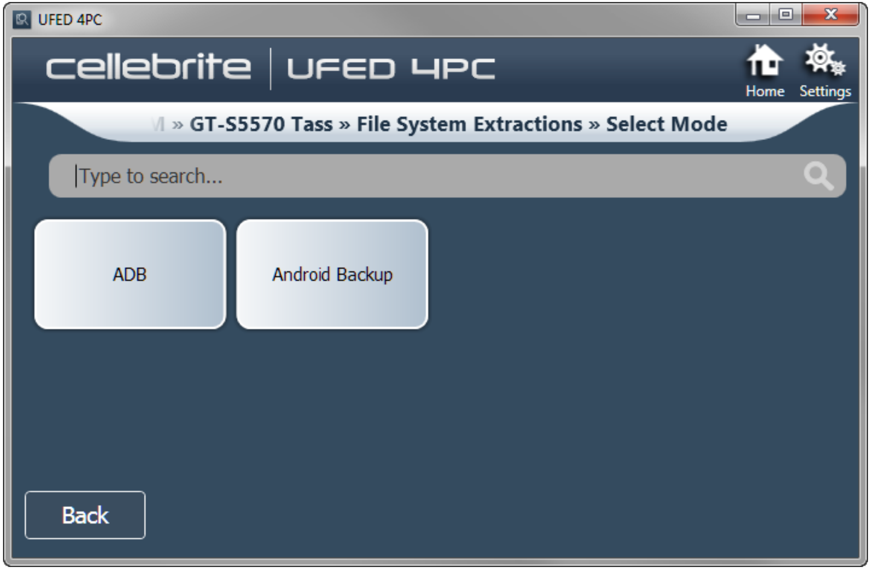
Chapter 5: **File system extraction**

The File System Extraction function enables you to perform a full system extraction from a device.

5.1. Performing a file system extraction

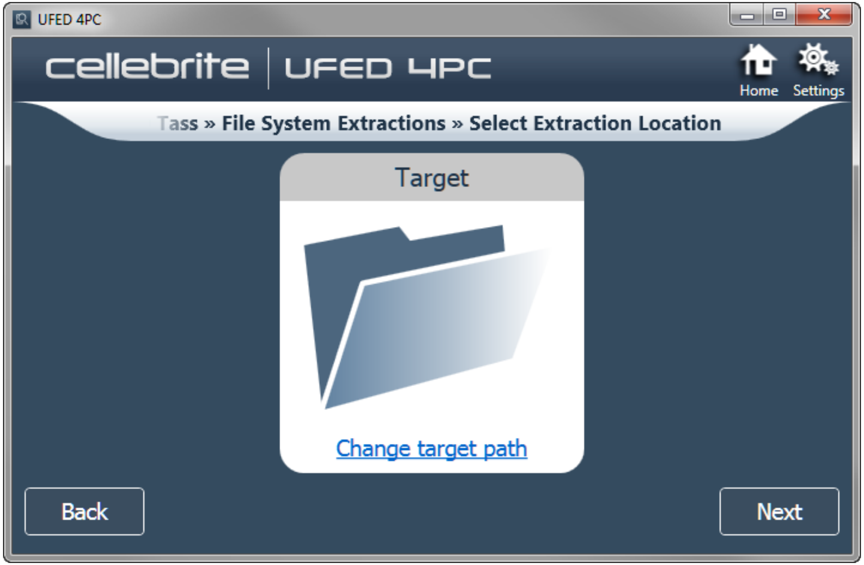
1) Click **Extract from Mobile Device** and identify the device, then click **File System Extraction**.

2) The Select Mode screen appears.



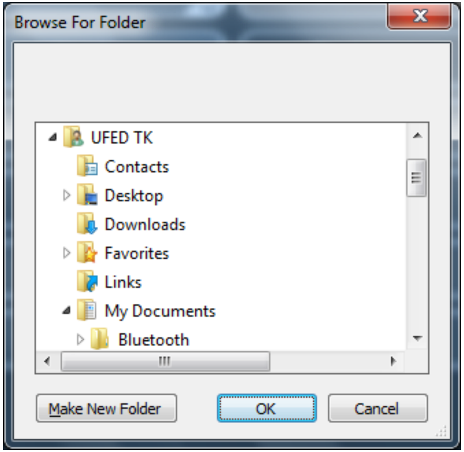
3) Select **ADB** (for Android Backup, see *Android backup* (page *90*.)

The Select Extraction Location screen appears.


UFED 4PC
cellebrite UFED 4PC
Home
Settings
Tass » File System Extractions » Select Extraction Location
Target
Change target path
Back
Next

4) To change the target path:

   a) Click **Change target path**.



Browse For Folder

   b) In the Browse For Folder dialog, browse to the location where you want to save the extraction.

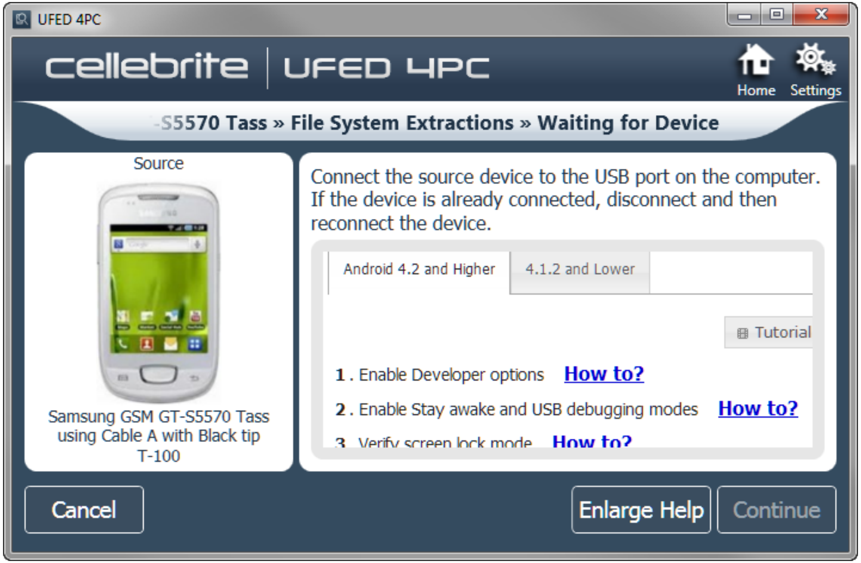
   c) Select the desired location, or click **Make New Folder** to create a target directory.

   d) Click **OK**.

   The target path is set.

5) Click **Next**.

The Waiting for Device screen appears.



Samsung GSM GT-S5570 Tass 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.

1 . Enable Developer options How to?

2 . Enable Stay awake and USB debugging modes How to?

3 . Verify screen lock mode How to?

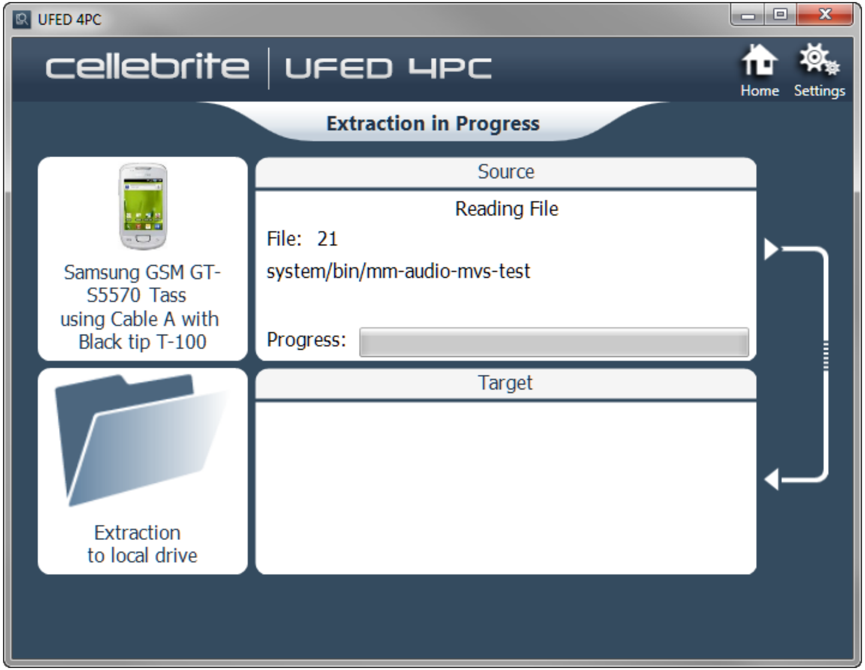
6) Select the correct cable and tip for the mobile device based on the information written in the screen.

7) Change the device settings according to the instructions

8) Connect the device.

9) Click **Continue**.

The Extraction in Progress screen appears.



Extraction in Progress

Samsung GSM GT-S5570 Tass using Cable A with Black tip T-100

Source

Reading File

File: 21

system/bin/mm-audio-mvs-test

Progress:

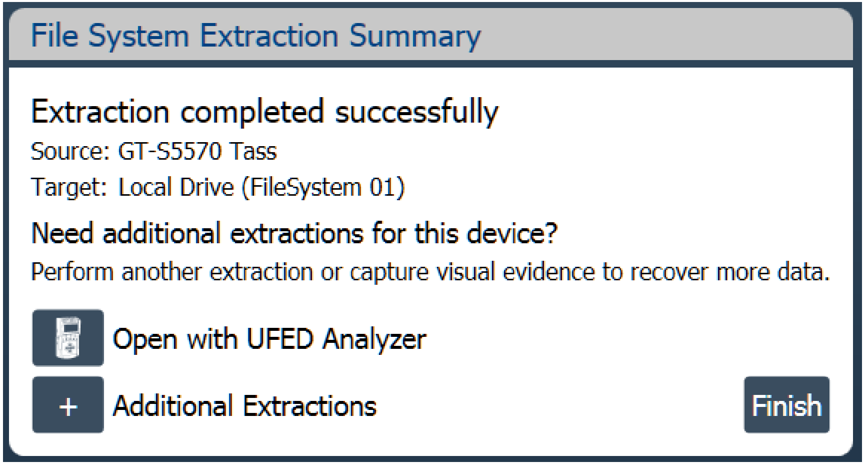
Extraction to local drive

Target

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

NOTE: 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.



File System Extraction Summary

Extraction completed successfully

Source: GT-S5570 Tass

Target: Local Drive (FileSystem 01)

Need additional extractions for this device?

Perform another extraction or capture visual evidence to recover more data.

10) Click the required button.

📱	To open the extraction in UFED Physical/Logical Analyzer.
+	To add additional extraction types for the same device.
Finish	To end the process and return to the home screen.

5.2. 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 File System Extraction)

NOTE: 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 UFED Physical Analyzer application.
- PM file.

The File System extraction can be viewed using the UFED Physical Analyzer.

5.3. 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 later.

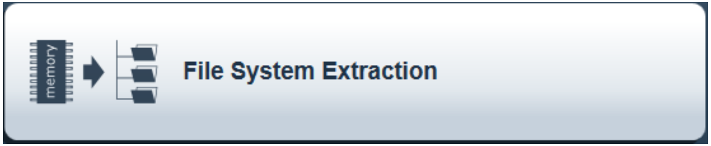
Android Backup may provide less data then other methods, therefore, you should use this feature when other file system methods such as ADB are not successful, or when other file system methods are not available for the device (for example, if the android version is not supported).

There are two extraction methods:

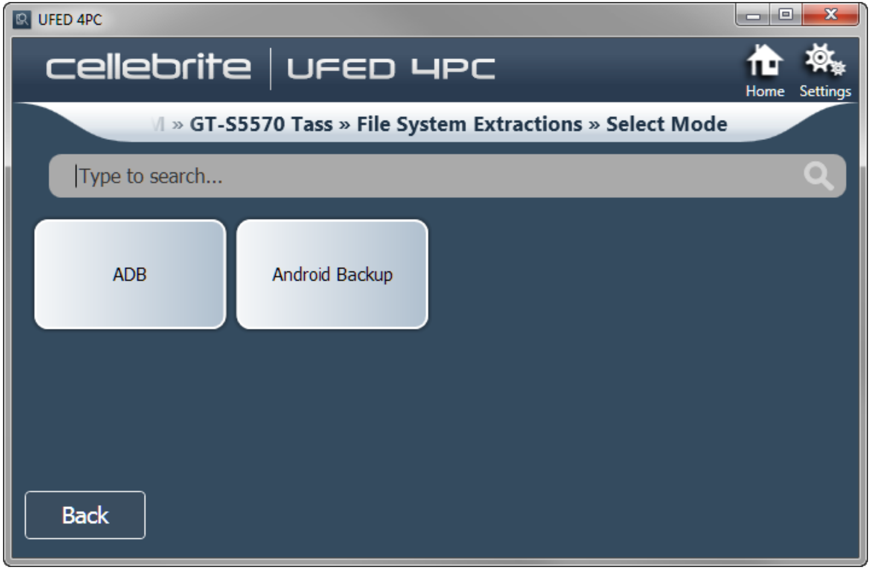
- **No Shared**: Extracts all the applications (native and non-native) that reside on the device.
- **With Shared**: Extracts all the applications (native and non-native) that reside on the device plus data from the device's internal storage and memory card (included images, videos, etc.). This method takes additional time for the extraction. If this method is not successful you should try the No Shared method.

To extract data using Android backup:

1) Click **Extract from Mobile Device** and identify the device, then click **File System Extraction**.



The following screen appears.



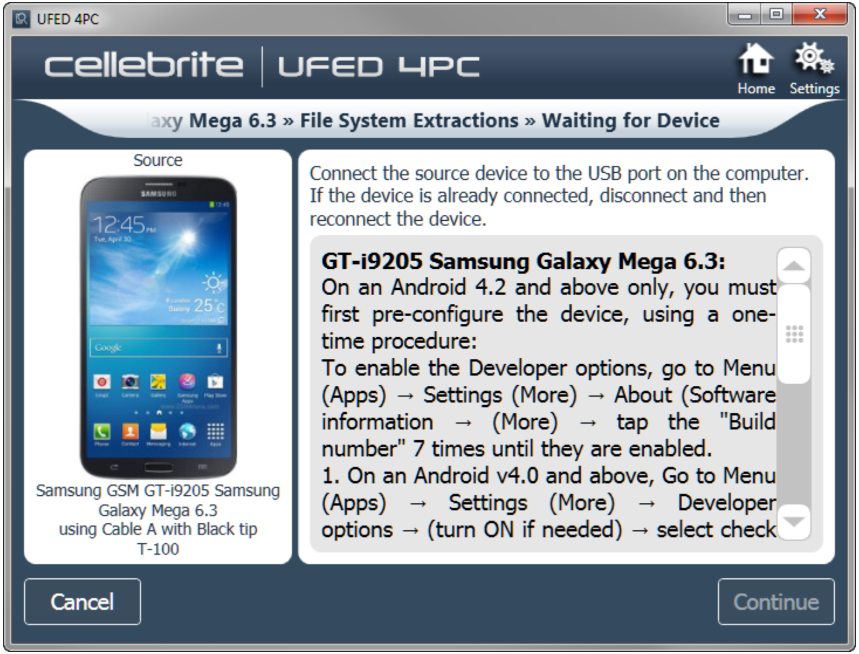
2) Click **Android Backup**.

A message appears to indicate that Android backup mode extracts the data according to the device's specific characteristics.

3) Click **Continue**.

4) Select the target path and click **Next**.

   The waiting for Device screen appears.


UFED 4PC
cellebrite | UFED 4PC
Home
Settings
axy Mega 6.3 » File System Extractions » Waiting for Device
Source
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with Black tip T-100
Cancel
Continue

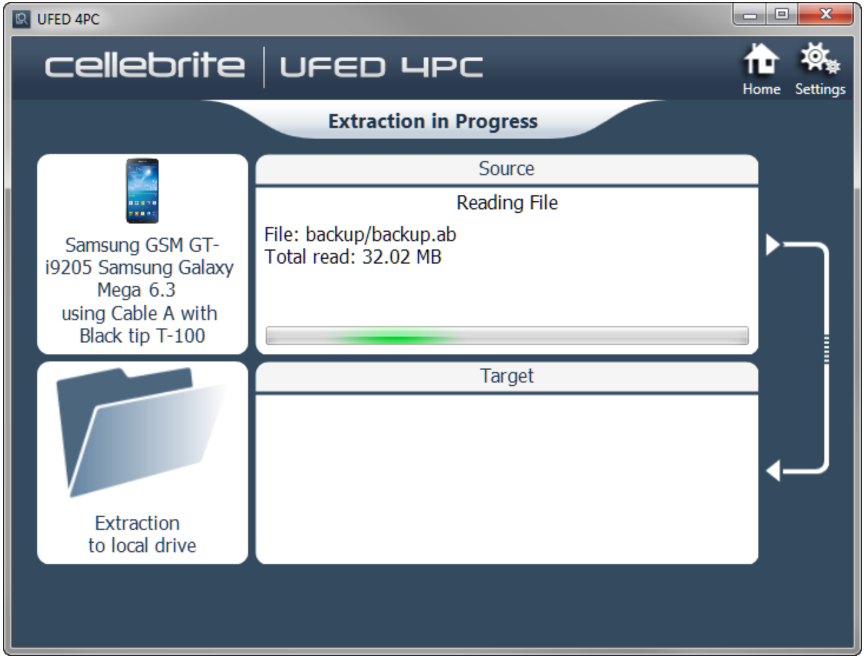
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

GT-i9205 Samsung Galaxy Mega 6.3:
On an Android 4.2 and above only, you must first pre-configure the device, using a one-time procedure:
To enable the Developer options, go to Menu (Apps) → Settings (More) → About (Software information → (More) → tap the "Build number" 7 times until they are enabled.
1. On an Android v4.0 and above, Go to Menu (Apps) → Settings (More) → Developer options → (turn ON if needed) → select check

The Extraction in Progress screen appears.

5) Click **Continue**, and then select **Backup my data** on the device.

   The following screen appears.

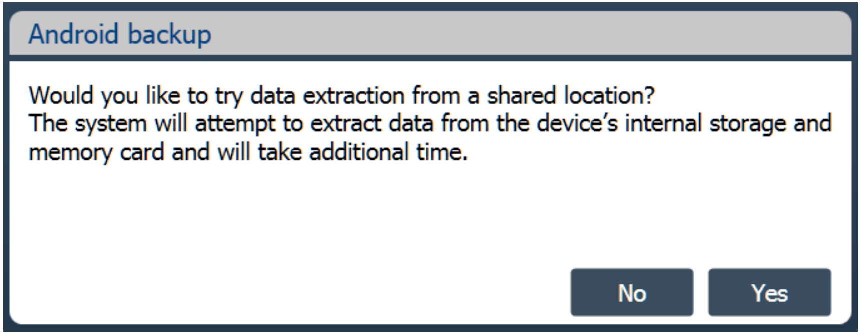


UFED 4PC
cellebrite | UFED 4PC
Home
Settings
Extraction in Progress
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with Black tip T-100
Source
Extraction to local drive
Target

Reading File

File: backup/backup.ab
Total read: 32.02 MB

   The following screen appears.

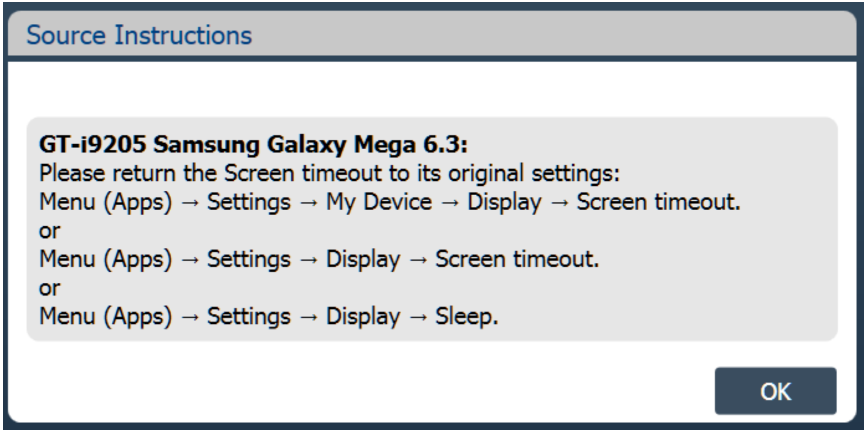


Android backup

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.

6) Click **No** if you do not want to try extract data from a shared location. Click **Yes** if you want to try extract information from a shared location.

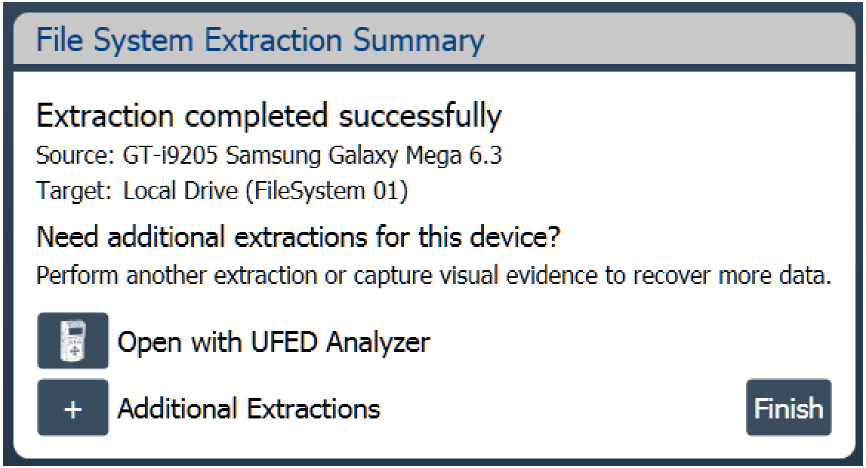
   The following screen appears.



GT-i9205 Samsung Galaxy Mega 6.3:
Please return the Screen timeout to its original settings:
Menu (Apps) → Settings → My Device → Display → Screen timeout.
or
Menu (Apps) → Settings → Display → Screen timeout.
or
Menu (Apps) → Settings → Display → Sleep.

7) Follow the instructions and click OK.

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



File System Extraction Summary

Extraction completed successfully

Source: GT-i9205 Samsung Galaxy Mega 6.3

Target: Local Drive (FileSystem 01)

Need additional extractions for this device?

Perform another extraction or capture visual evidence to recover more data.

8) Click the required button.

📱 To open the extraction in UFED Physical/Logical Analyzer.

+ To add additional extraction types for the same device.

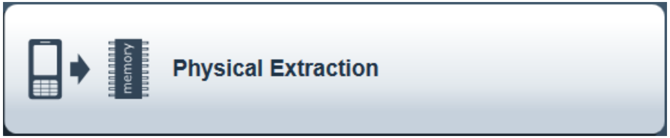
Finish To end the process and return to the home screen.

Chapter 6: **Physical extraction**

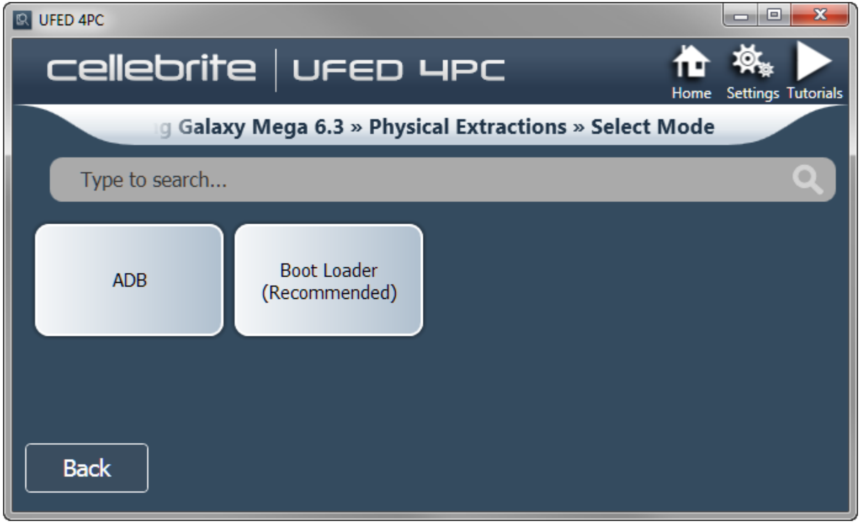
The **Physical Extraction** function enables you to perform a physical bit-for-bit image of the source device memory to a removable storage device or PC.

6.1. Performing a physical extraction

1) Click **Extract from Mobile Device** and identify the device, then click **Physical Extraction**.



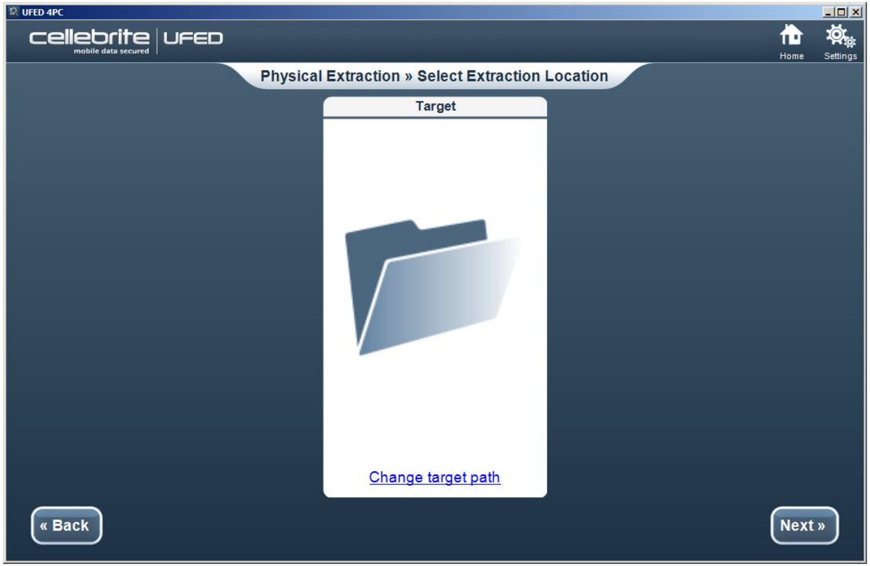
The Select Mode screen appears.



UFED 4PC
cellebrite | UFED 4PC
Home
Settings
Tutorials
g Galaxy Mega 6.3 » Physical Extractions » Select Mode
Type to search...
ADB
Boot Loader (Recommended)
Back

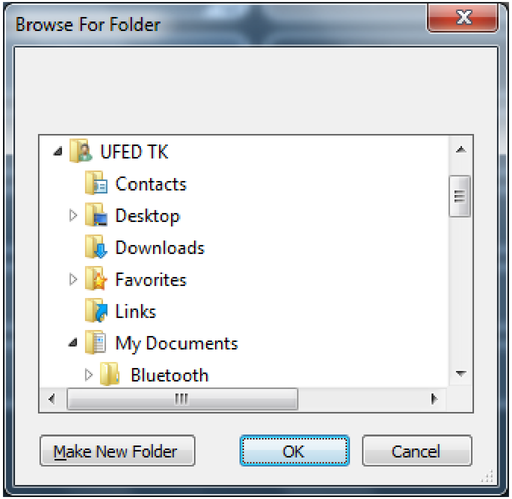
2) Click **ADB** or **Boot Loader** (recommended)..

The Select Extraction Location screen appears.


UFED 4PC
cellebrite mobile data secured | UFED
Home
Settings
Physical Extraction » Select Extraction Location
Target
Change target path
« Back
Next »

3) To change the target path:

a) Click **Change target path**.



b) In the Browse For Folder dialog, browse to the location where you want to save the extraction.

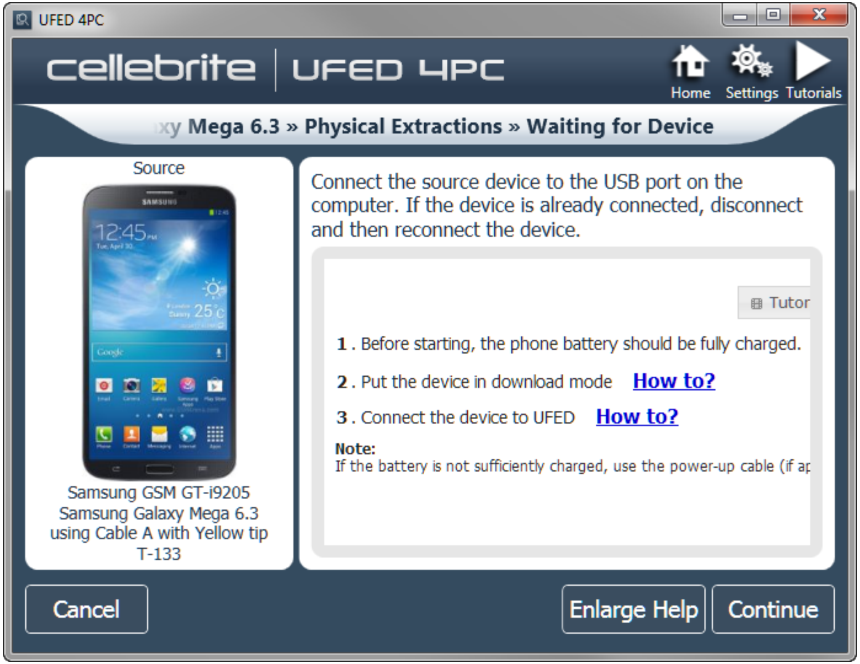
c) Select the desired location, or click **Make New Folder** to create a target directory.

d) Click **OK**.

The target path is set.

4) 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.



Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

1 . Before starting, the phone battery should be fully charged.

2 . Put the device in download mode How to?

3 . Connect the device to UFED How to?

Note:
If the battery is not sufficiently charged, use the power-up cable (if ap

5) Do one of the following:

   If you can connect the device directly to the PC:

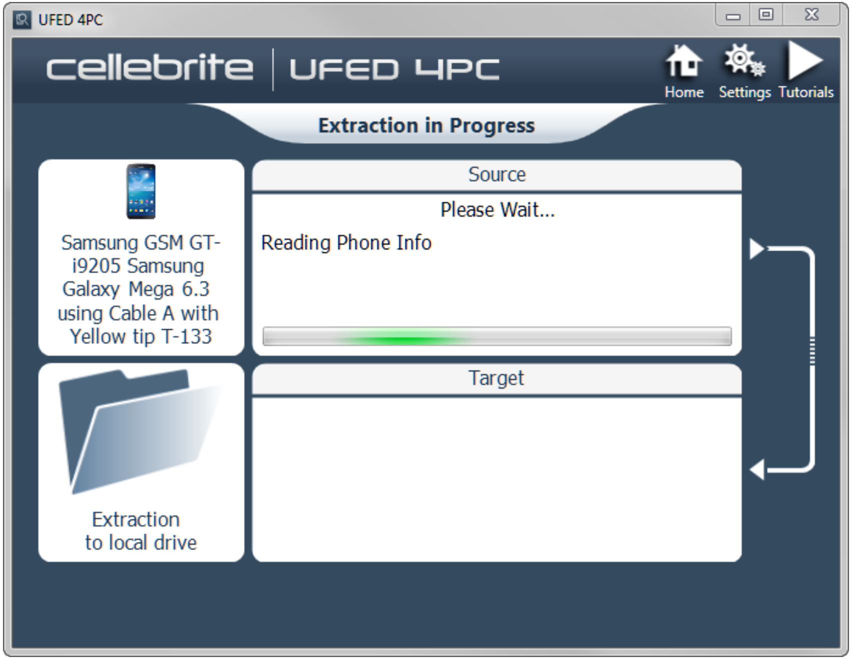
   - Select the correct cable and tip for the mobile device based on the instruction on the screen.
   - Change the device settings according to the instructions.
   - Connect the device to the PC.

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

   - Connect the UFED Device Adapter to the PC USB port.
     The source port on the UFED Device Adapter flashes.
   - Connect the device to the UFED Device Adapter.

6) Click **Continue**.

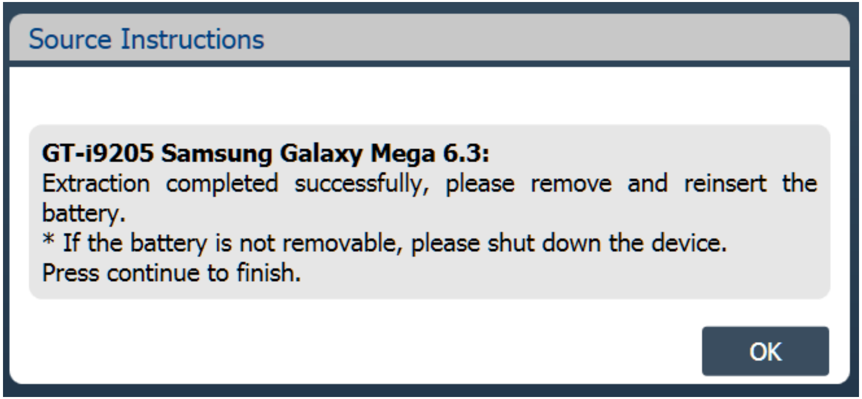
The Extraction in Progress screen appears.



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

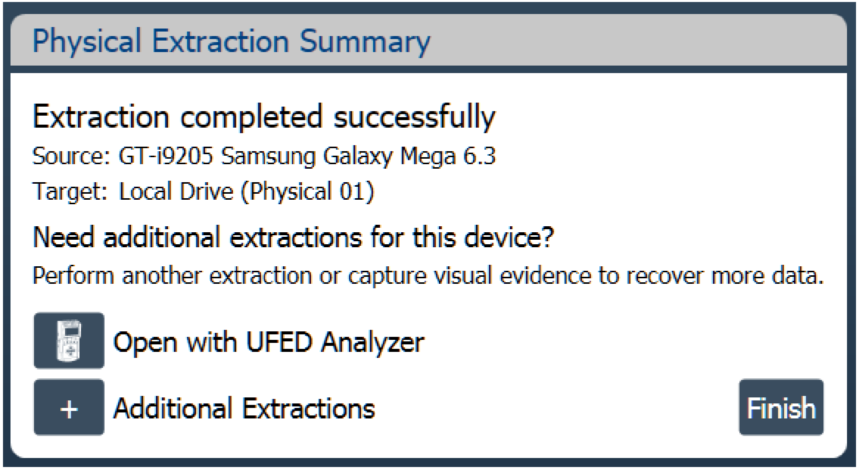
7) Follow any on-screen instructions. The following screen appears.

NOTE: 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.



GT-i9205 Samsung Galaxy Mega 6.3:
Extraction completed successfully, please remove and reinsert the battery.
* If the battery is not removable, please shut down the device.
Press continue to finish.

8) Click OK. When extraction is complete the Physical Extraction Summary screen appears.



Physical Extraction Summary

Extraction completed successfully

Source: GT-i9205 Samsung Galaxy Mega 6.3

Target: Local Drive (Physical 01)

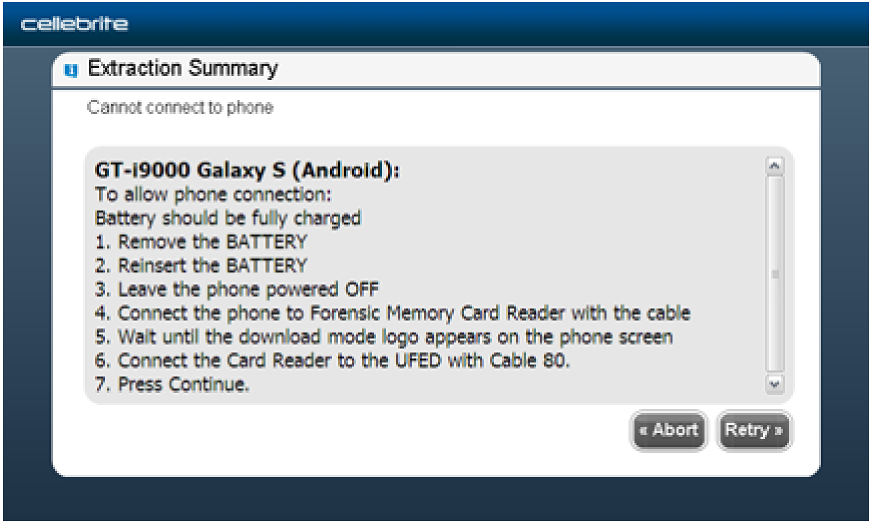
Need additional extractions for this device?

Perform another extraction or capture visual evidence to recover more data.

9) Click the required button.

▯	To open the extraction in UFED Physical/Logical Analyzer.
+	To add additional extraction types for the same device.
Finish	To end the process and return to the home screen.

In the event that the system cannot connect to the device the Extraction Summary screen appears with an error message.



Cannot connect to phone

GT-i9000 Galaxy S (Android):
To allow phone connection:
Battery should be fully charged
1. Remove the BATTERY
2. Reinsert the BATTERY
3. Leave the phone powered OFF
4. Connect the phone to Forensic Memory Card Reader with the cable
5. Wait until the download mode logo appears on the phone screen
6. Connect the Card Reader to the UFED with Cable 80.
7. Press Continue.

10) Follow the instructions on the screen and click **Retry**.

6.2. 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. See step 5 of Performing a Physical Extraction.

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

Chapter 7: **Capture images and screenshots**

The UFED camera enables you to collect evidence by taking pictures or videos of a device (see *Capturing images* on page *110*). You can also use a Screenshot feature to capture internal screenshots directly from a Blackberry, Android or iOS device (see *Capturing screenshots* on page *121*). 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 images and videos, which will be visible in the UFED Physical/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, 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.

7.1. The UFED camera

The UFED camera is offered as an add-on and it is controlled by the UFED 4PC. All necessary drivers are preinstalled with the application. The UFED camera includes a camera stand, which enables you to adjust the height and the angle of the 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.

7.1.1. Contents

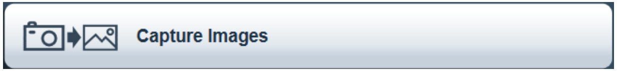
Part	Quantity
Anti-glare pad	1
camera	1
Camera case	1
Camera pad	1
Camera stand	1

7.2. Capturing images

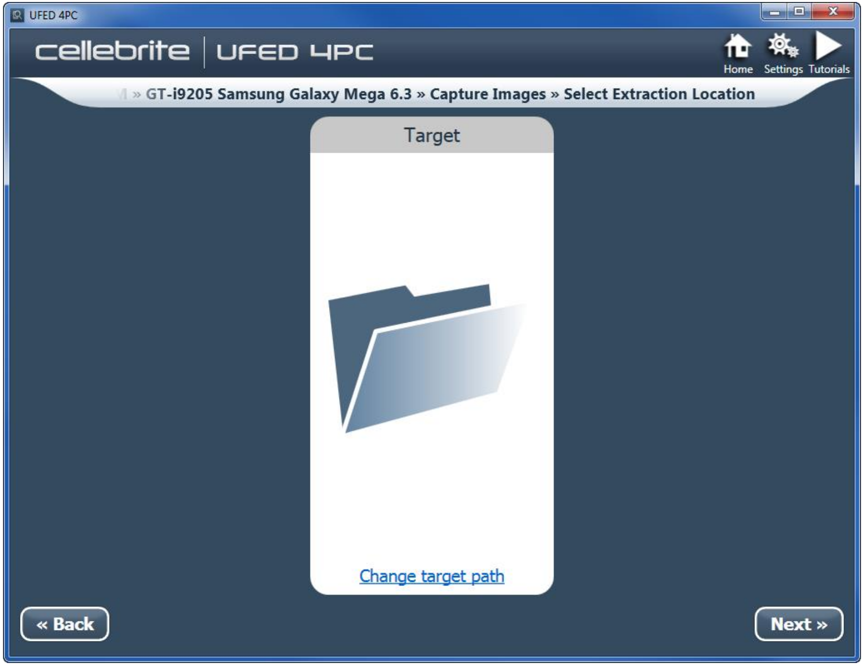
When taking pictures or videos of a device, you have two options. Capture images as an additional extraction type for a selected device, or without specifying a device.

To capture images or videos for a specific device:

1) Click **Extract from Mobile Device** and identify the device, then click **Capture Images**.



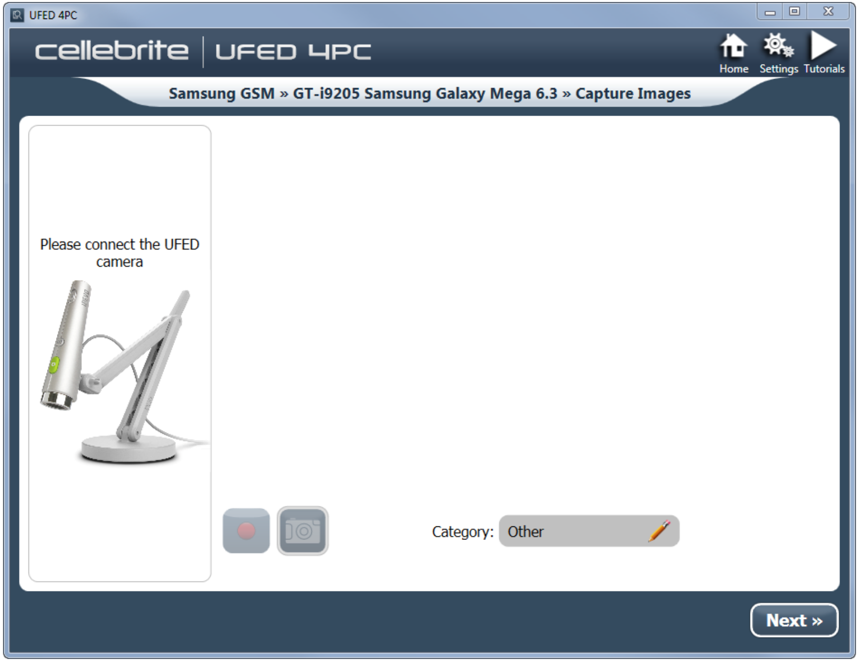
The Select Extraction Location screen appears.



2) If required, click **Change target path** to select an alternate save location. A folder for this extraction will be created in this location and will include the images (snapshots), videos, UFD file, index file, and report file.

3) Click **Next**.

The following screen appears if no camera is detected.



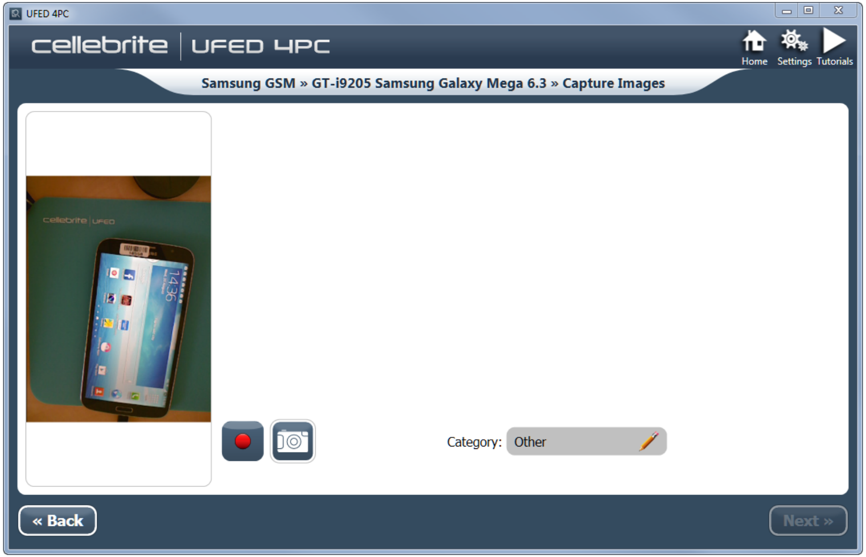
Samsung GSM » GT-i9205 Samsung Galaxy Mega 6.3 » Capture Images

Please connect the UFED camera

Category: Other

4) Connect the UFED camera to a USB port on the computer.

The Capture Images screen appears.



Samsung GSM » GT-i9205 Samsung Galaxy Mega 6.3 » Capture Images

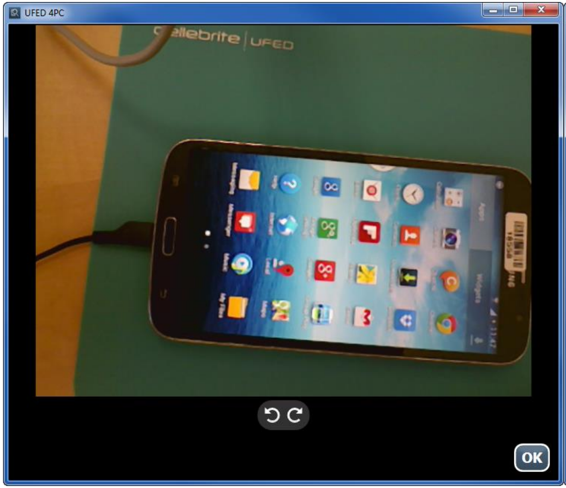
Category: Other

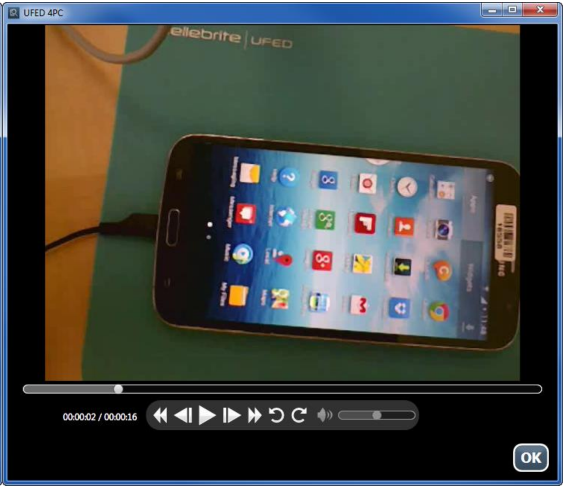
5) Do one of the following:

- Click ● to start a video recording and click ■ to stop the video recording.
- Click 📷 to take a picture.
- Click Other ✎ to change the default category. Images and videos will be displayed in UFED Physical/Logical under these categories.
- Click an image or video, to add notes, bookmarks (★), categories (🗀), or delete the file (🗑).

Click ↶ to move back to live view.

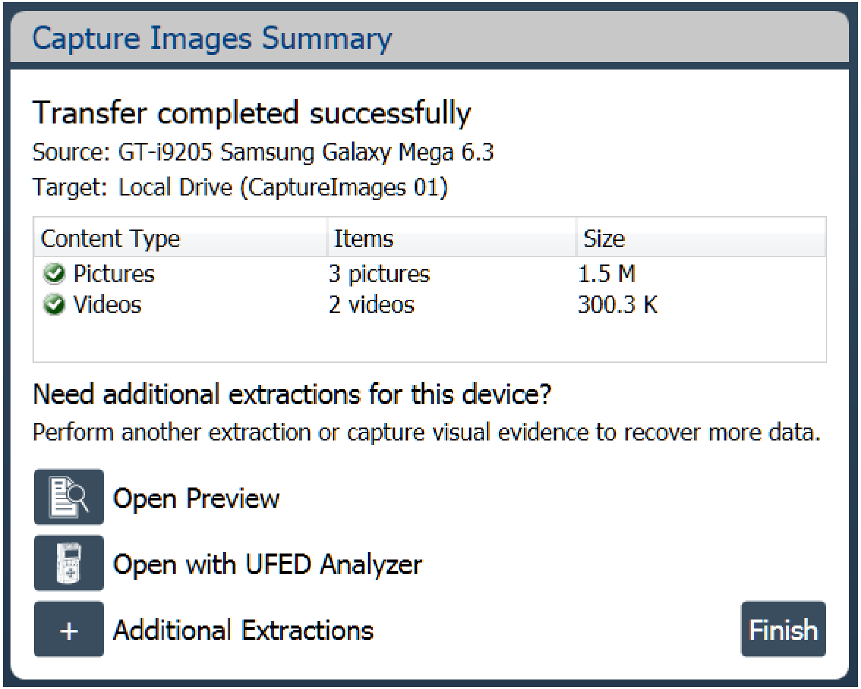
NOTE: To rotate a picture or video, or play a recorded video, click the picture or video, and then click the picture or video in the leftmost screen. Use the rotate buttons ↺ ↻ or video buttons ⏪ ⏴ ▶ ⏵ ⏩ ↺ ↻ 🔊. See the following examples.





6) Click OK and then click **Next** to continue.

The Capture Images Summary screen appears.



Capture Images Summary

Transfer completed successfully

Source: GT-i9205 Samsung Galaxy Mega 6.3

Target: Local Drive (CaptureImages 01)

Content Type	Items	Size
✓ Pictures	3 pictures	1.5 M
✓ Videos	2 videos	300.3 K

Need additional extractions for this device?

Perform another extraction or capture visual evidence to recover more data.

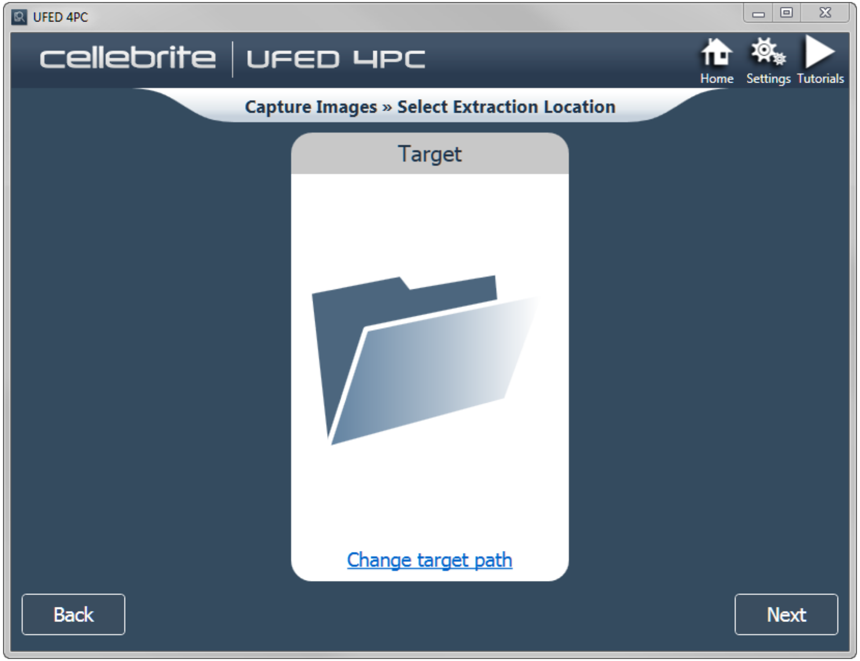
7) Click the required button.

🔍	To view an HTML preview report that includes information about the device and the extraction.
📱	To open the extraction in UFED Physical/Logical Analyzer.
+	To add additional extraction types for the same device.
Finish	To end the process and return to the home screen.

To capture images without a device:

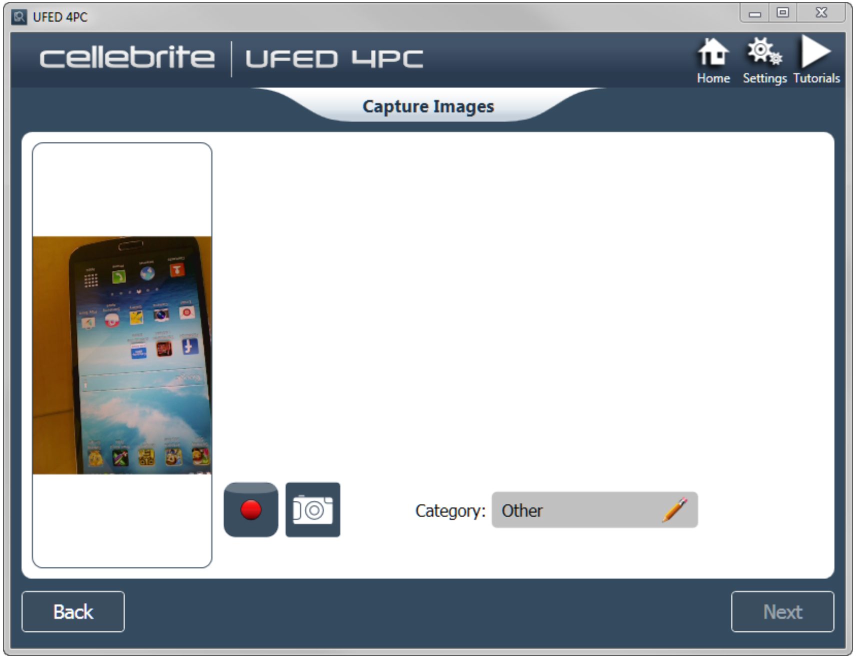
1) Click **Capture Images**.

   The Select Extraction Location screen appears.



2) If required, click **Change target path** to select an alternate save location.
3) Click **Next**.

   The Capture Images screen appears.

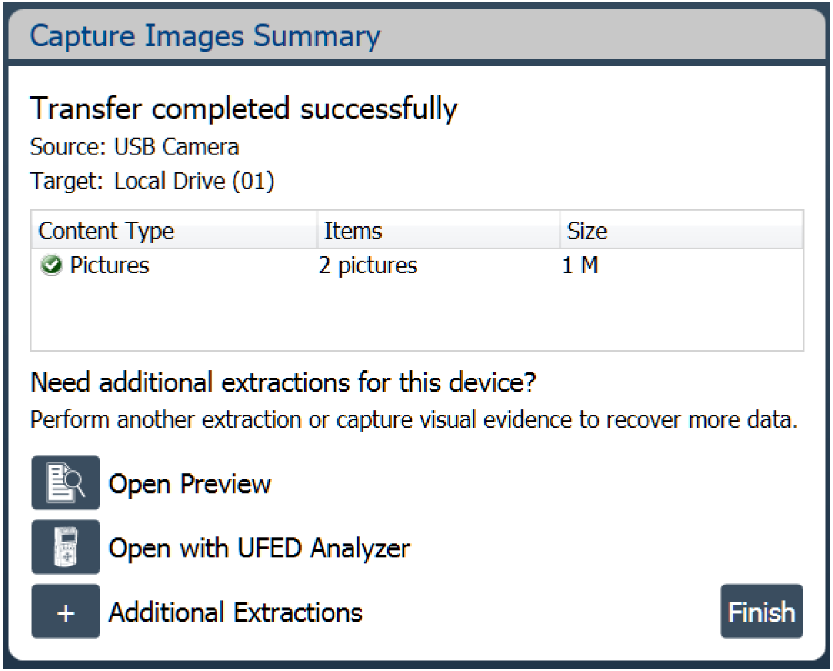


Category: Other

See page *114* for information on available options in this screen.

4) Click **Next** to continue.

The Capture Images Summary appears.



Capture Images Summary

Transfer completed successfully

Source: USB Camera

Target: Local Drive (01)

Content Type	Items	Size
✓ Pictures	2 pictures	1 M

Need additional extractions for this device?

Perform another extraction or capture visual evidence to recover more data.

5) Click the required button.

To view an HTML preview report that includes information about the device and the extraction.

To open the extraction in UFED Physical/Logical Analyzer.

+ To add additional extraction types for the same device.

Finish To end the process and return to the home screen.

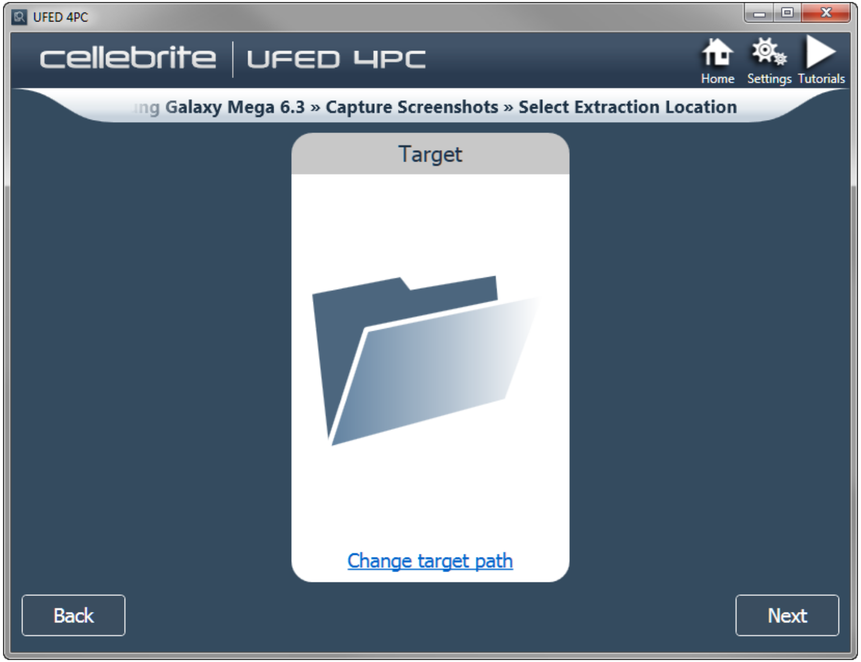
7.3. Capturing screenshots

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

To capture screenshots from the devices:

1) Click **Extract from Mobile Device** and identify the device, then click **Capture Screenshots**.

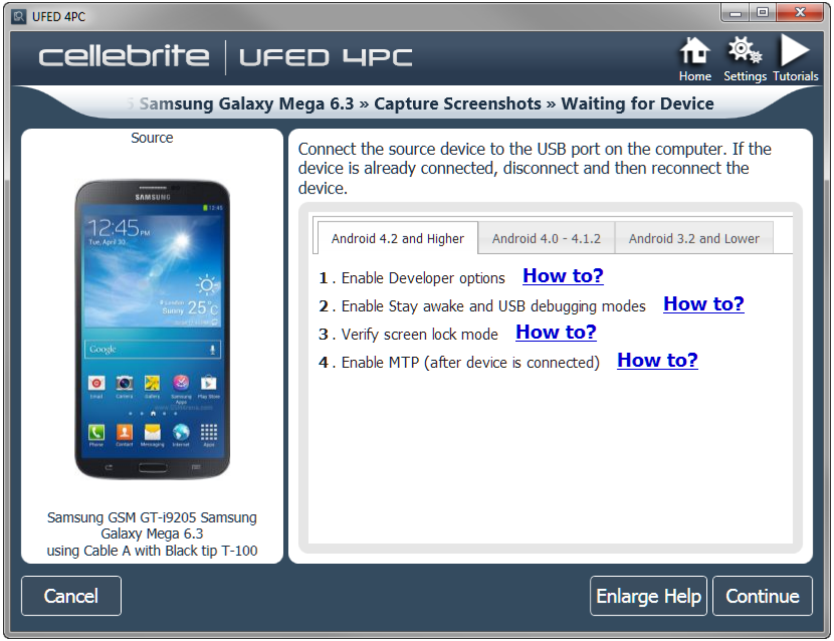
The Select Extraction Location screen appears.



2) If required, click **Change target path** to select an alternate save location.

3) Click **Next**.

The Waiting for Device screen appears.



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.

1 . Enable Developer options **How to?**

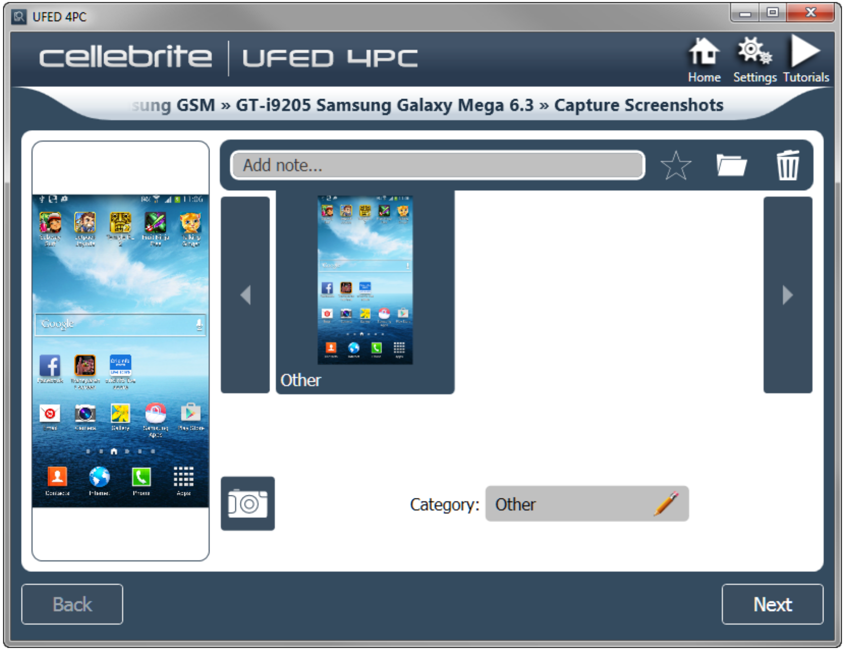
2 . Enable Stay awake and USB debugging modes **How to?**

3 . Verify screen lock mode **How to?**

4 . Enable MTP (after device is connected) **How to?**

4) Follow the instructions to connect the device.
5) Click **Continue**.

   The Capture Screenshots screen appears.



See page *114* for the screenshot options available this screen.

6) Click **Next**.

The Capture Screenshots Summary screen appears.

7) Click the required button.

🔍	To view an HTML preview report that includes information about the device and the extraction.
📱	To open the extraction in UFED Physical/Logical Analyzer.
+	To add additional extraction types for the same device.
Finish	To end the process and return to the home screen.

Chapter 8: **SIM card functionality**

The **SIM Card** functions enable you to perform various SIM card related functions:

- Sim Data Extraction

- Clone SIM

- File System Extraction

8.1. SIM data extraction

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

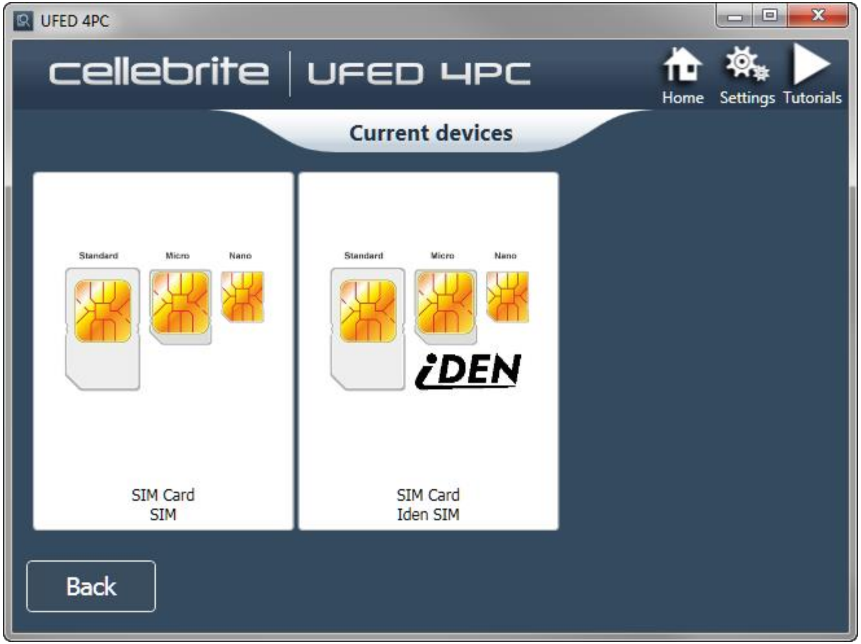
8.1.1. Performing SIM data extraction

The following example is performed using a SIM Card.

To perform the SIM Data Extraction:

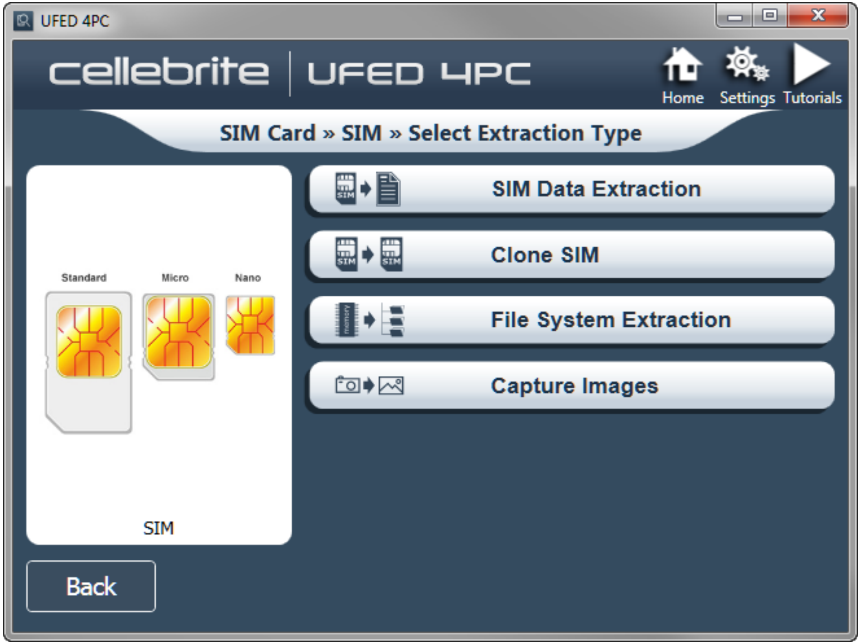
1) Select **Extract from SIM Card.**

   The following screen appears.

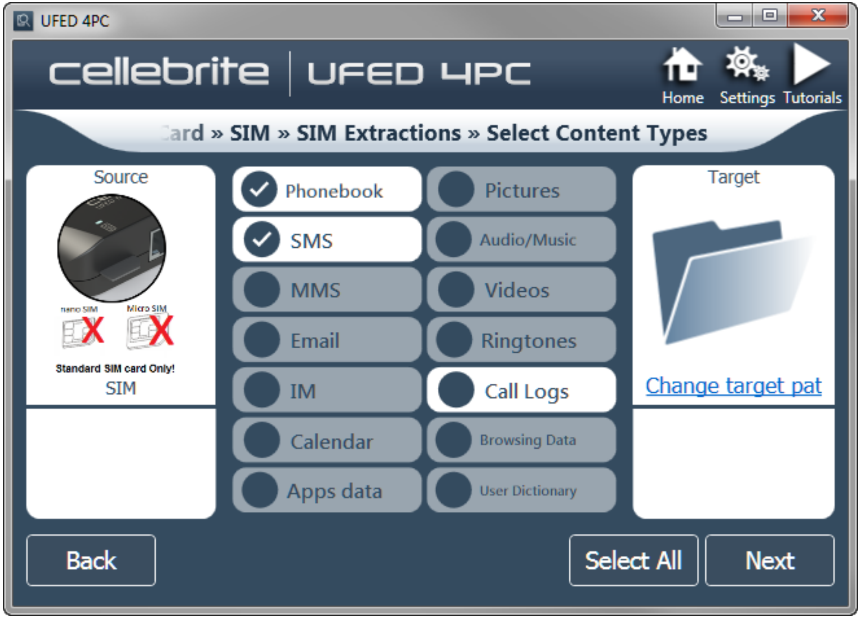


2) Click either **SIM** or **Iden SIM**.

3) The Select Extraction Type screen appears.



4) Select an option. The Select Content Types screen appears.

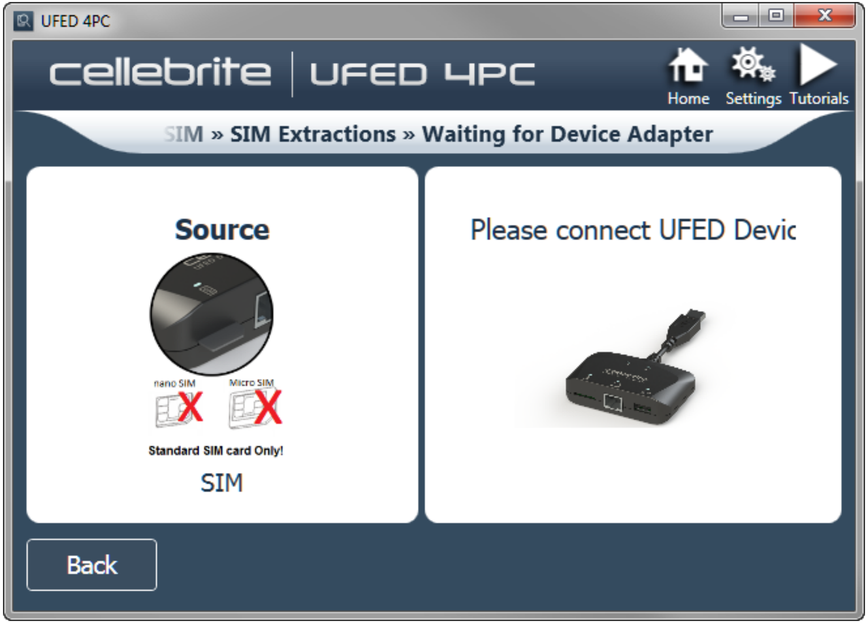


5) In the Select Content Types screen, select the content types that you want to extract from the list of options on the center of the screen.

   To select all the available data types, click **Select All** under the data types list (**Select All** appears after you click one or more of the options on the screen).

6) Click **Next**.

The Waiting for Device Adapter screen appears.



SIM » SIM Extractions » Waiting for Device Adapter

Source

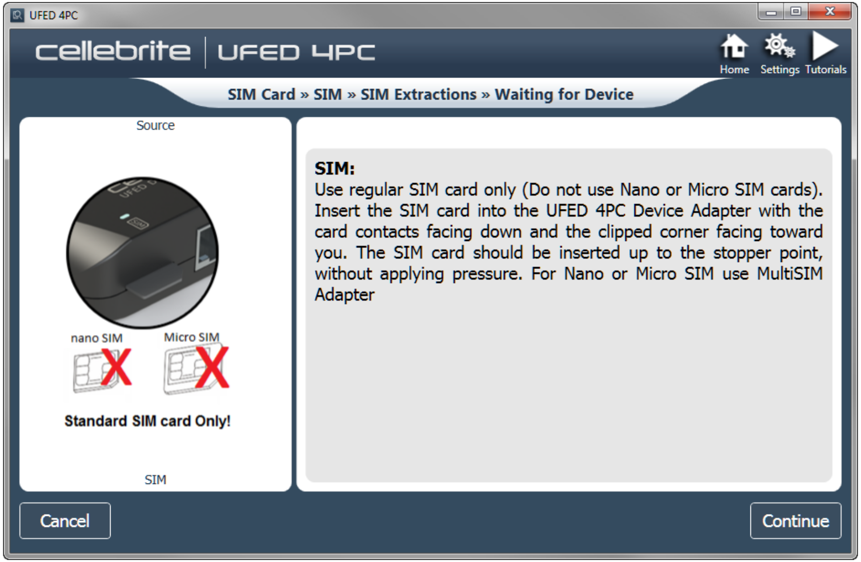
Standard SIM card Only!

SIM

Please connect UFED Devic

7) Connect the UFED Device Adapter.

On the UFED Device Adapter, the SIM port flashes red. The Waiting for Device screen appears.



SIM:
Use regular SIM card only (Do not use Nano or Micro SIM cards). Insert the SIM card into the UFED 4PC Device Adapter with the card contacts facing down and the clipped corner facing toward you. The SIM card should be inserted up to the stopper point, without applying pressure. For Nano or Micro SIM use MultiSIM Adapter

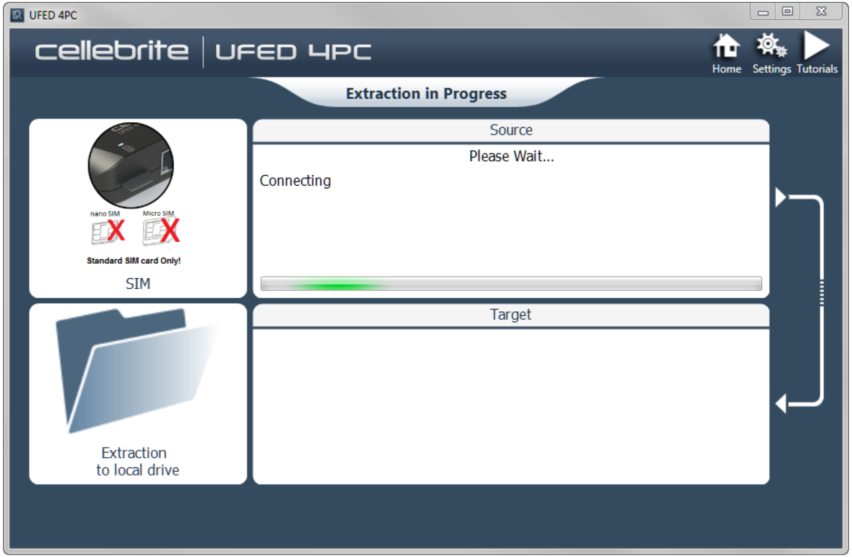
8) Insert SIM card into the SIM card reader slot.

NOTE: The SIM port continues to flash even after the SIM card has been inserted into the SIM reader slot.

9) Click **Continue**.

The Extraction in Progress screen appears.

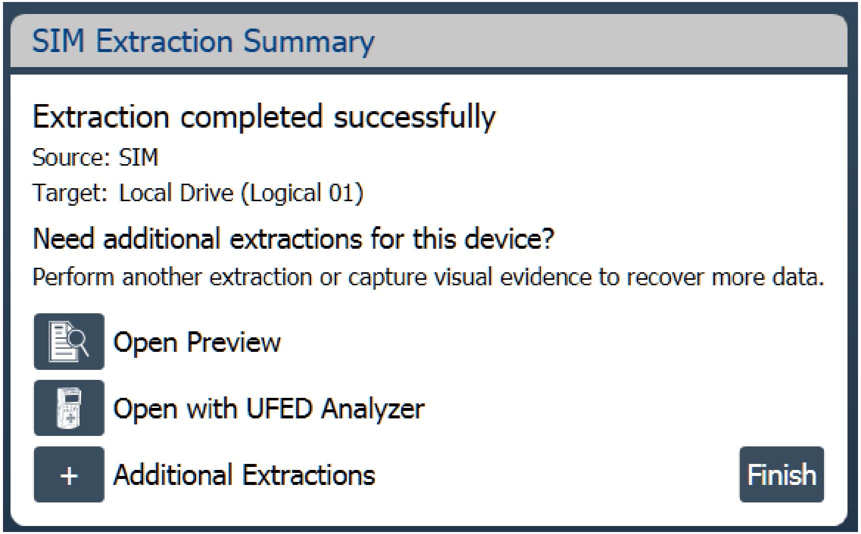
10) If prompted, select which of the SIM card partitions to read.



Please Wait...

Connecting

When the extraction process is complete, the SIM Extraction Summary screen appears, displaying a summary of the extraction process.



SIM Extraction Summary

Extraction completed successfully

Source: SIM

Target: Local Drive (Logical 01)

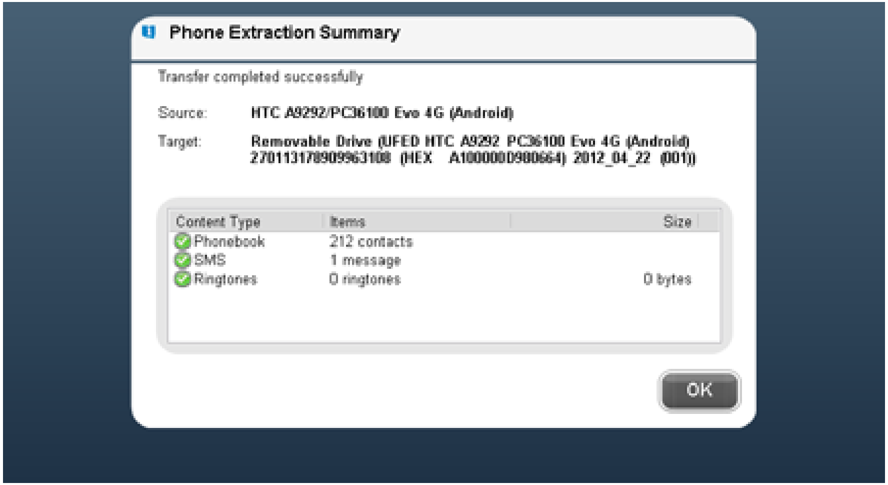
Need additional extractions for this device?

Perform another extraction or capture visual evidence to recover more data.

11) Click the required button.

🔍	To view an HTML preview report that includes information about the device and the extraction.
📱	To open the extraction in UFED Physical/Logical Analyzer.
+	To add additional extraction types for the same device.
Finish	To end the process and return to the home screen.

In the event that the Phone Extraction option was selected, the Phone Extraction Summary screen appears.



Phone Extraction Summary

Transfer completed successfully

Source: HTC A9292/PC36100 Evo 4G (Android)

Target: Removable Drive (UFED HTC A9292 PC36100 Evo 4G (Android) 270113178909963108 (HEX A1000000980664) 2012_04_22 (001))

Content Type	Items	Size
✓ Phonebook	212 contacts	
✓ SMS	1 message	
✓ Ringtones	0 ringtones	0 bytes

12) To end the process and return to the home screen, click **OK**.

8.1.2. 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.

NOTE: 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 detailed report of extracted data in both HTML and XML formats and call log file (*.clog).

8.2. 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).

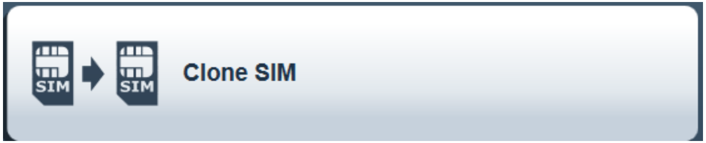
- When the original SIM is not available, by manually programming the ICCID or IMSI into the Cloned SIM ID Card to mimic the original missing card.
- When the SIM card is PIN locked, by cloning the identification of the original SIM, which allows extraction of the device data without losing critical data including call history and SMS messages.

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

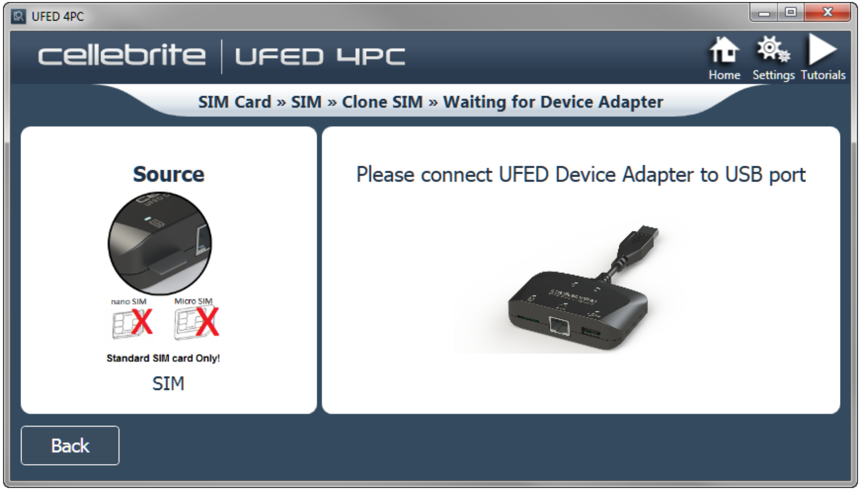
- Clone an existing SIM card - to create a cloned SIM to use to extract device data without a network connection. See Cloning an existing SIM card ID.
- Manually enter SIM data - to manually program the ICCID and IMSI to the cloned SIM card. See Entering SIM data manually.
- Create GSM Test SIM - The 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 Creating GSM test SIM.

8.2.1. Cloning an existing SIM card ID

1) Click **Clone SIM**.



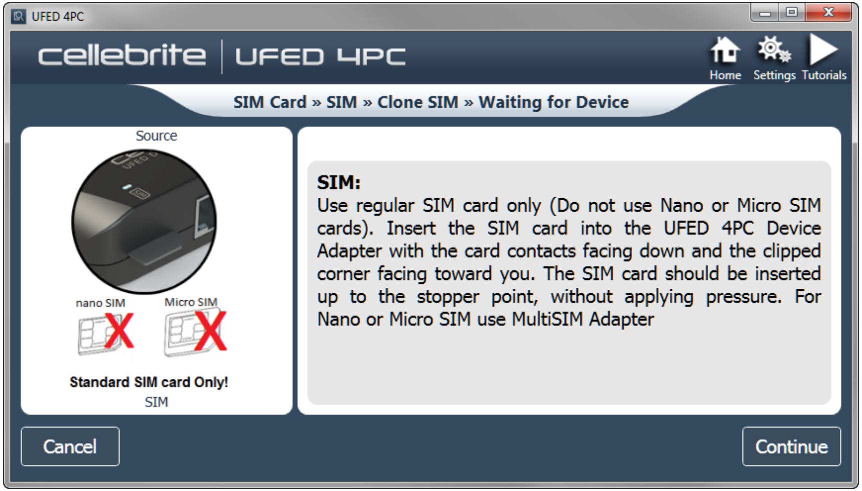
If the UFED Device Adapter is not connected, The Waiting for Device Adapter screen appears.



SIM Card » SIM » Clone SIM » Waiting for Device Adapter

Please connect UFED Device Adapter to USB port

2) Connect the UFED Device Adapter to the PC USB port.



SIM:
Use regular SIM card only (Do not use Nano or Micro SIM cards). Insert the SIM card into the UFED 4PC Device Adapter with the card contacts facing down and the clipped corner facing toward you. The SIM card should be inserted up to the stopper point, without applying pressure. For Nano or Micro SIM use MultiSIM Adapter

The source port on the UFED Device Adapter flashes.

3) Insert the SIM card into the UFED Device Adapter.

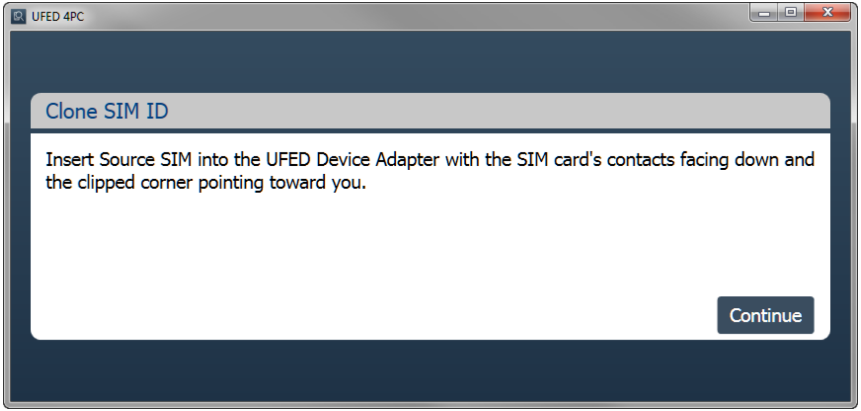
NOTE: The SIM port on the Cellebrite Phone Adapter flashes even after you insert the SIM card into the SIM reader slot.

4) Click **Continue**.

The Select Source screen appears.

5) Click **Clone an existing SIM card**

   The Clone SIM ID prompt appears.

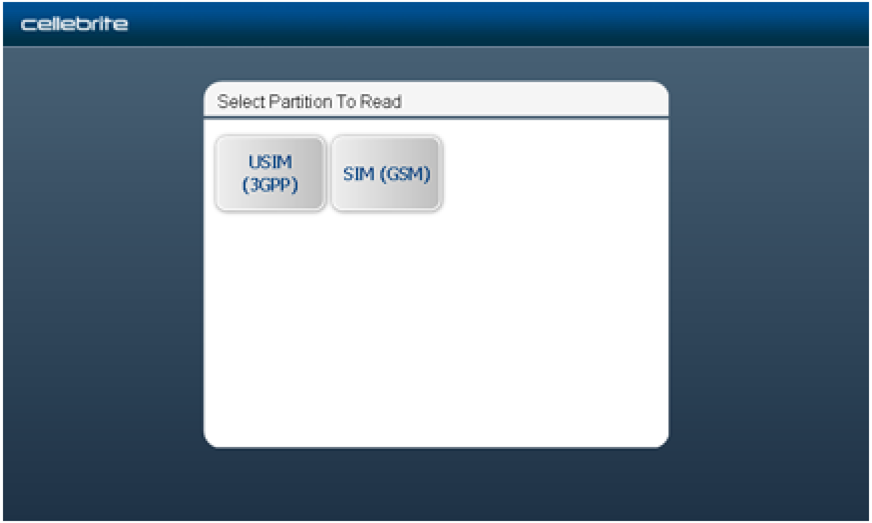


Clone SIM ID

Insert Source SIM into the UFED Device Adapter with the SIM card's contacts facing down and the clipped corner pointing toward you.

6) Check that the right SIM was inserted into the SIM card reader slot.
7) Click **Continue**.

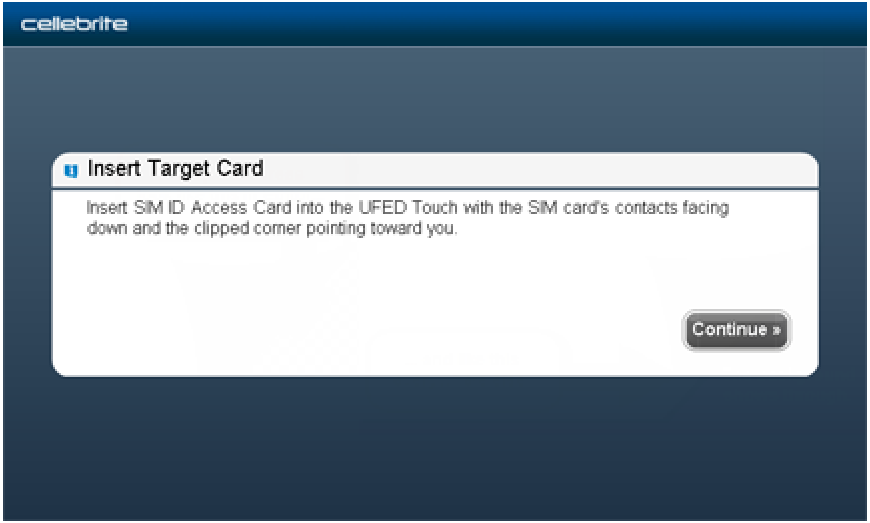
If the SIM card is partitioned, a prompt appears.



8) **Select** which of the SIM card partitions to read.

The Extraction in Progress Source screen appears.

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

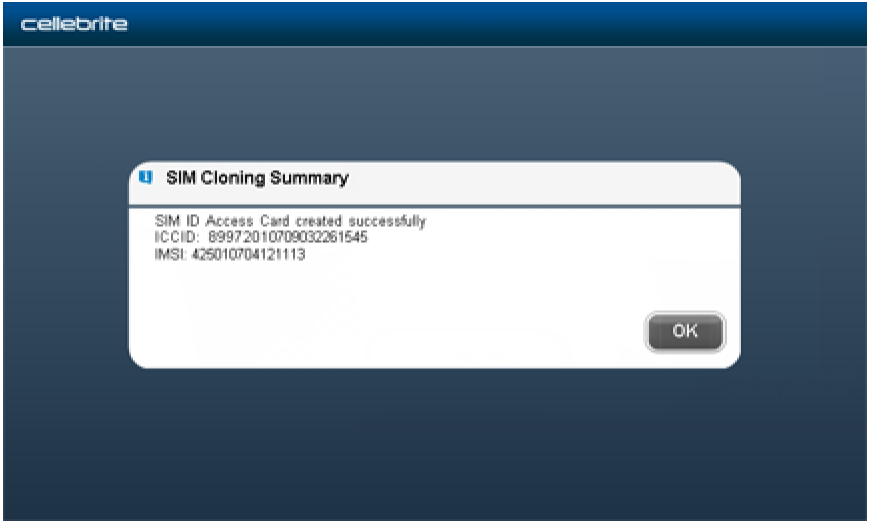


Insert Target Card

Insert SIM ID Access Card into the UFED Touch with the SIM card's contacts facing down and the clipped corner pointing toward you.

9) Remove the original SIM card from the UFED Device Adapter SIM card reader.
10) Insert a UFED SIM ID Access Card into the UFED Device Adapter SIM card reader.
11) 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.

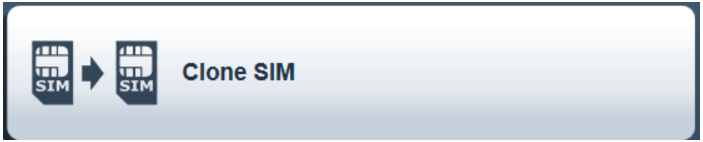


SIM ID Access Card created successfully
ICCID: 89972010709032261545
IMSI: 425010704121113

12) To end the process and return to the home screen, click **OK**.

8.2.2. Entering SIM data manually

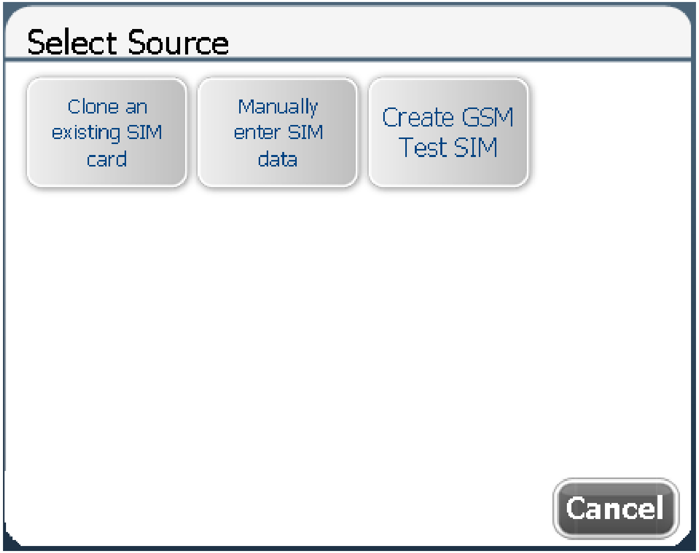
1) Click **Clone SIM**.



The Waiting for Device screen appears.

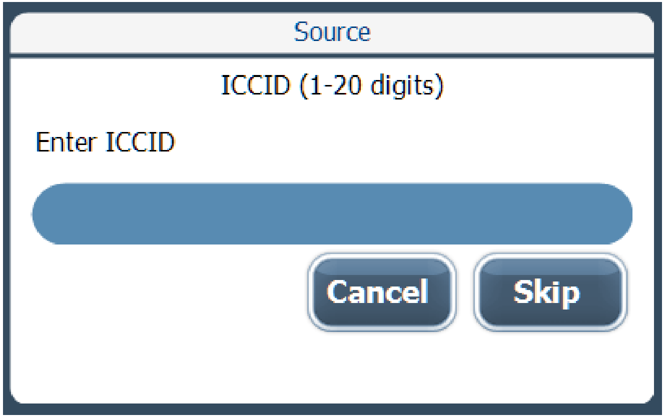
2) Connect the UFED Device Adapter to the PC USB port
3) Insert the UFED SIM ID Access card into the UFED Device Adapter.
4) Click **Continue**.

The Select Source screen appears.



Select Source

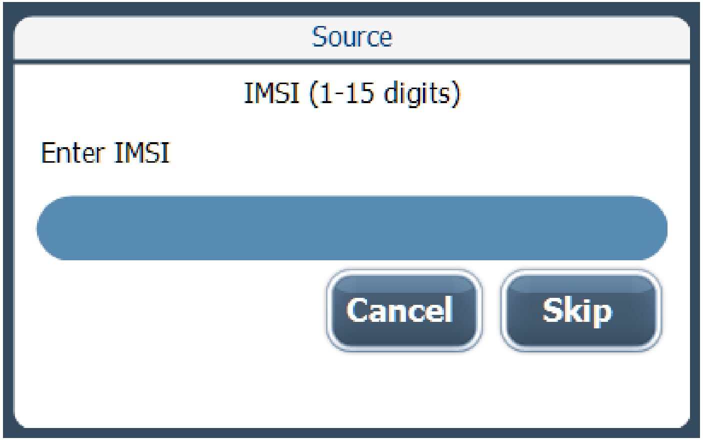
5) In the Select Source screen, click **Manually enter SIM data**.



6) Enter the SIM ICCID number (up to 20 digits).

7) Click **OK**.

The following screen appears:



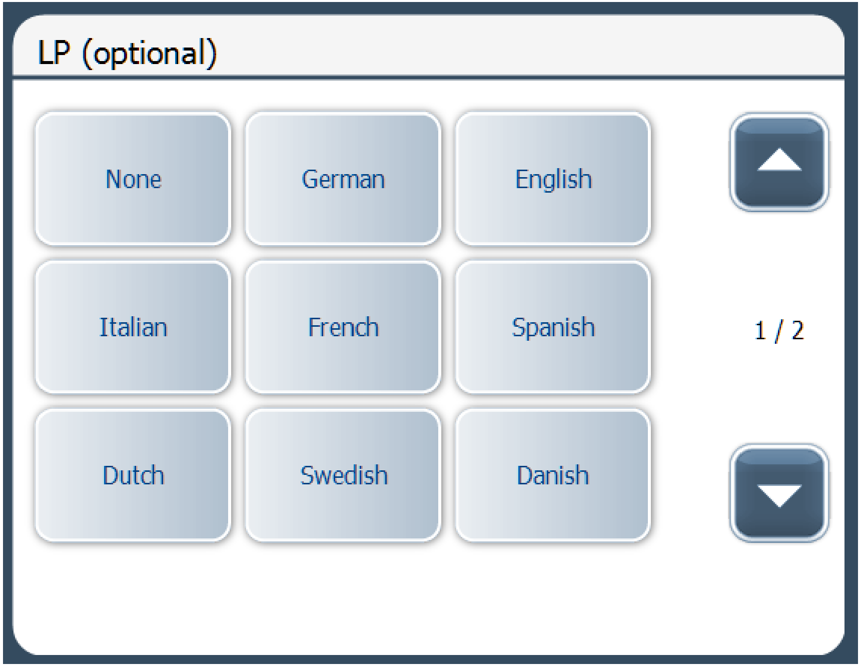
Source

IMSI (1-15 digits)

Enter IMSI

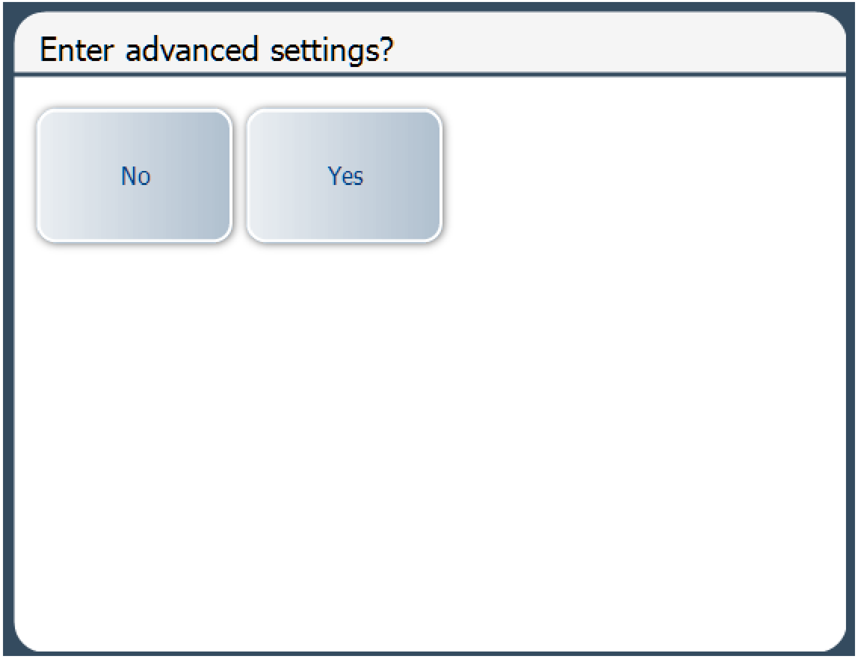
8) Enter the SIM IMSI number (up to 15 digits), then click **OK**.

The Select Language screen appears.



9) If required, select either a language or click **None**.

The Enter advanced settings screen appears.

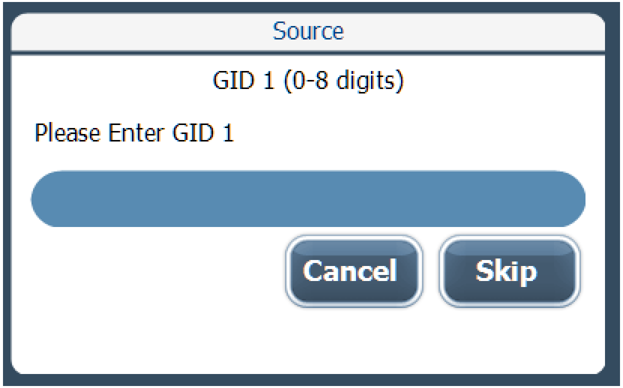


Enter advanced settings?

10) Click **Yes** or **No** to continue.

- Click **Yes** to display the advanced settings. The Extraction in Progress > Enter SPN screen appears. Proceed to step 11.
- Click **No** to continue. Proceed to step 15.

11) Enter the SIM **SPN** number (up to 16 digits), then click **OK**.

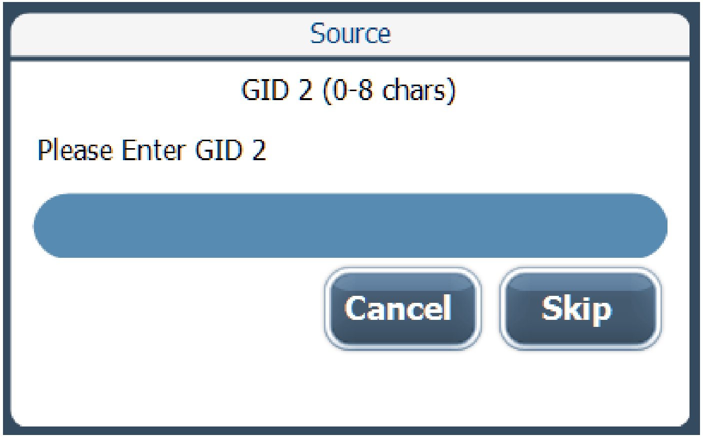


Source

GID 1 (0-8 digits)

Please Enter GID 1

The following screen appears:



Source

GID 2 (0-8 chars)

Please Enter GID 2

12) Enter the **SIM GID 1** number (up to 8 characters).

13) Click **OK**.

The Extraction in Progress > Enter GID 2 screen appears.

14) Enter the **SIM GID 2** number (up to 8 characters).

15) Click **OK**.

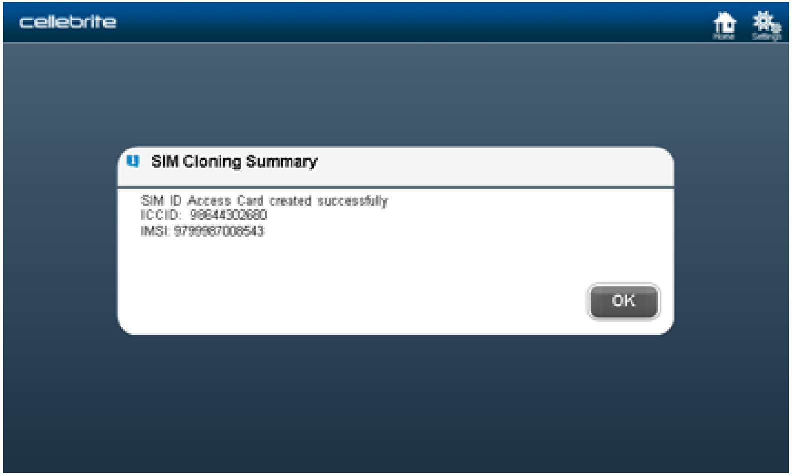
The Insert Target Card prompt appears.

16) Insert the UFED SIM ID access card into the UFED Device Adapter SIM card reader.

17) Click **Continue**.

NOTE: 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.

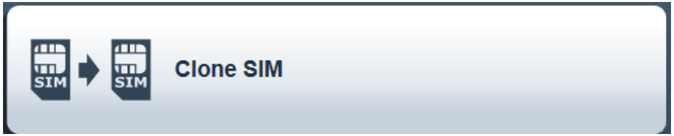


SIM ID Access Card created successfully
ICCID: 98644302680
IMSI: 9799987008543

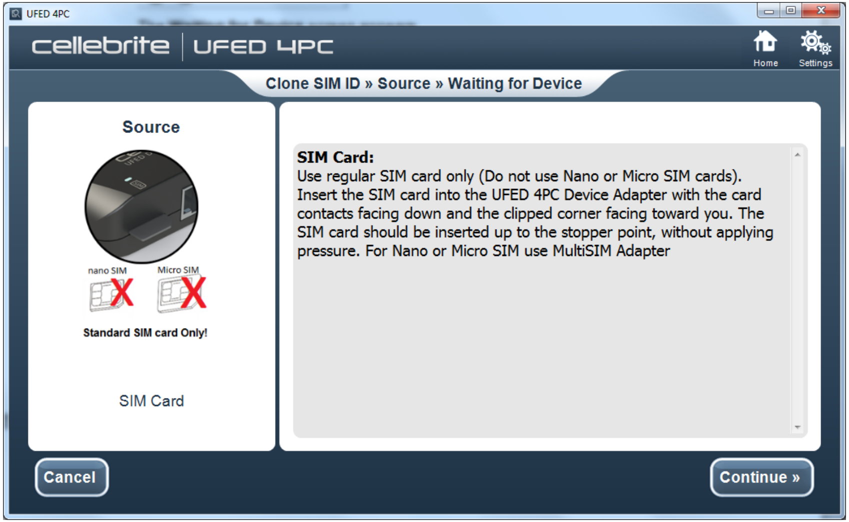
18) To end the process and return to home screen click **OK**.

8.2.3. Creating a GSM test SIM

1) Click **Clone SIM**.

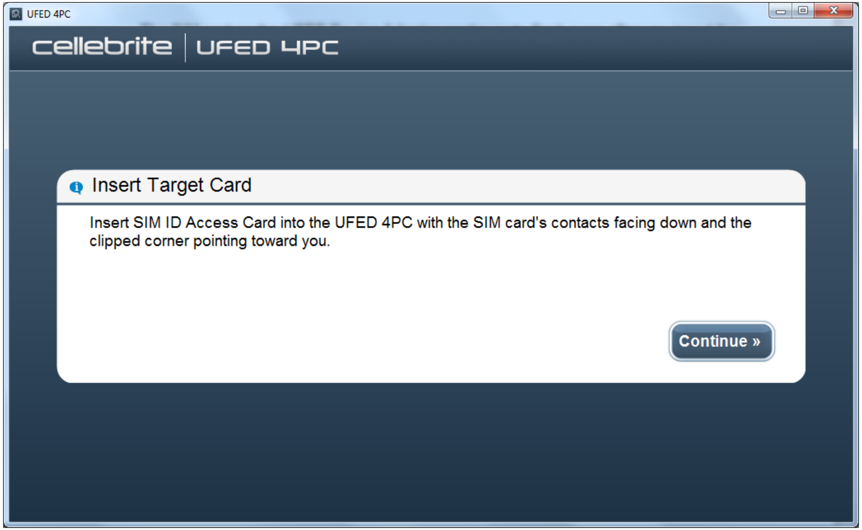


The Waiting for Device screen appears.



SIM Card:
Use regular SIM card only (Do not use Nano or Micro SIM cards). Insert the SIM card into the UFED 4PC Device Adapter with the card contacts facing down and the clipped corner facing toward you. The SIM card should be inserted up to the stopper point, without applying pressure. For Nano or Micro SIM use MultiSIM Adapter

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



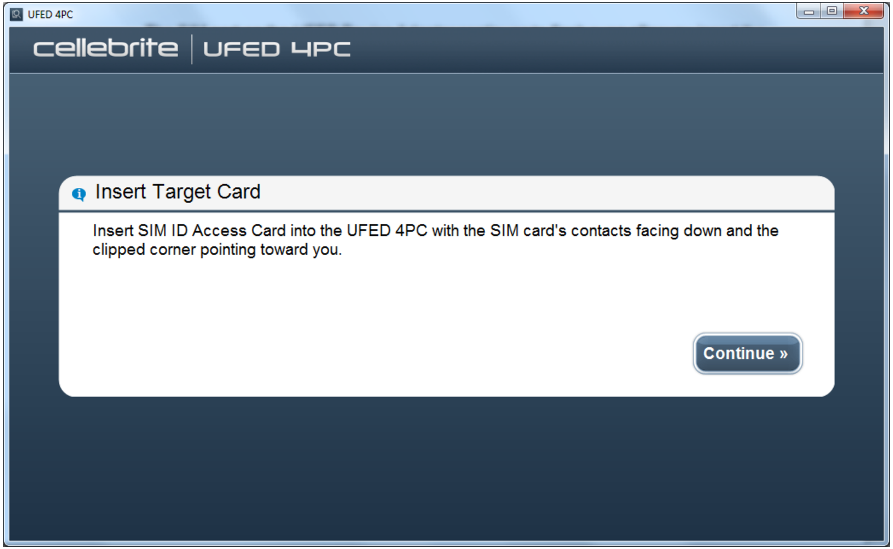
Insert Target Card

Insert SIM ID Access Card into the UFED 4PC with the SIM card's contacts facing down and the clipped corner pointing toward you.

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.



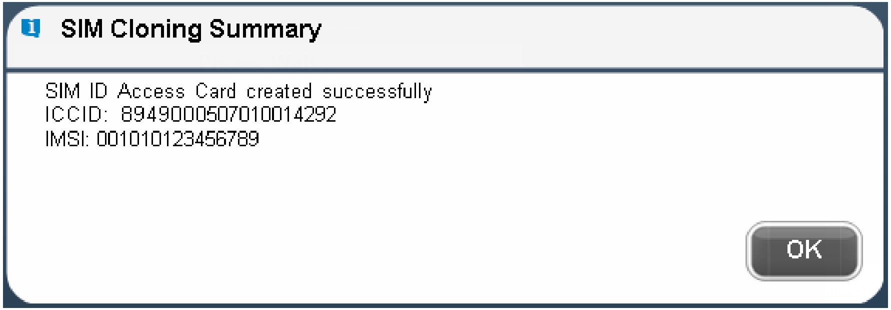
Insert Target Card

Insert SIM ID Access Card into the UFED 4PC with the SIM card's contacts facing down and the clipped corner pointing toward you.

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.



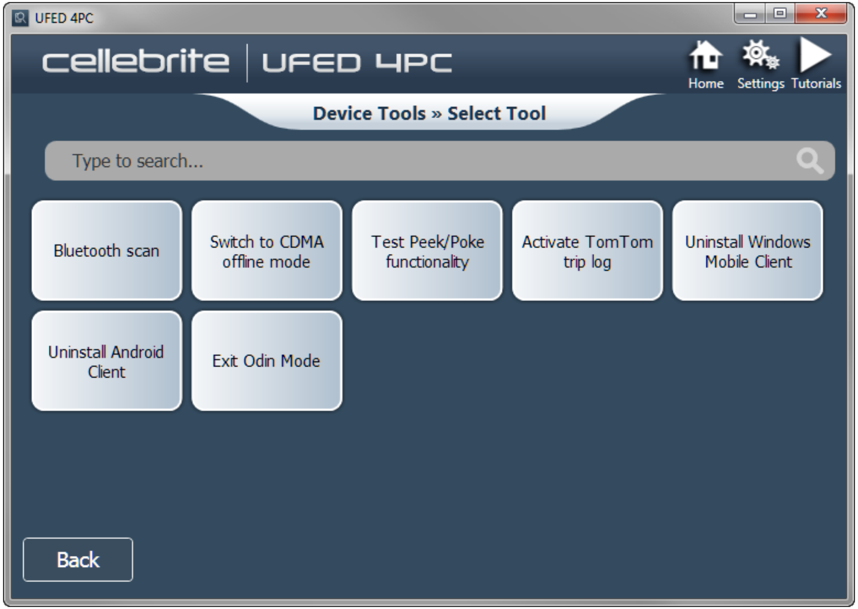
SIM ID Access Card created successfully
ICCID: 8949000507010014292
IMSI: 001010123456789

6) To end the process and return to the home screen, click **OK**.

Chapter 9: **Device tools**

The **Device Tools** are located on the home screen and include the following:

- *Bluetooth Scan* (page *161*)
- *Switch to CDMA Offline Mode* (page *164*)
- *Test Peek/Poke functionality* (page *166*)
- *Activate TomTom Trip log* (page *168*)
- *Uninstall Windows Mobile Client* (page *168*)
- *Uninstall Android Client* (page *169*)
- *Exit Odin Mode* (page *169*)


UFED 4PC
cellebrite | UFED 4PC
Home
Settings
Tutorials
Device Tools » Select Tool
Type to search...
Bluetooth scan
Switch to CDMA offline mode
Test Peek/Poke functionality
Activate TomTom trip log
Uninstall Windows Mobile Client
Uninstall Android Client
Exit Odin Mode
Back

9.1. Bluetooth Scan

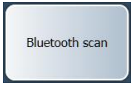
NOTE: This feature is available for Bluetooth-enabled PCs only.

This tool scans for available Bluetooth devices in your proximity and enables you to pair with them.

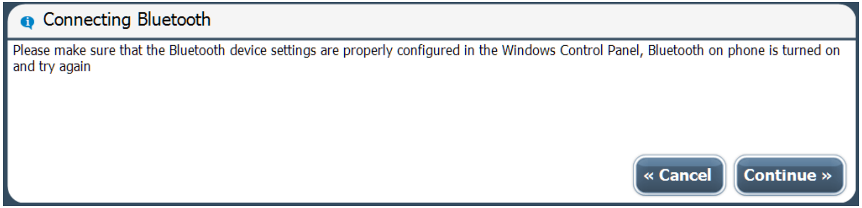
Make sure that the Bluetooth feature of the device is enabled.

Make sure that the Bluetooth switch is on.

To perform a Bluetooth scan:

1) Click **Device Tools** and then click **Bluetooth scan** .

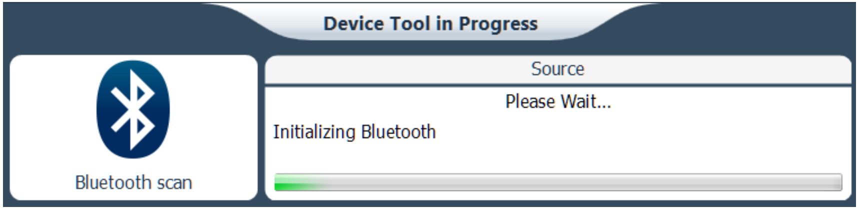
The Connecting Bluetooth prompt appears.



Connecting Bluetooth

Please make sure that the Bluetooth device settings are properly configured in the Windows Control Panel, Bluetooth on phone is turned on and try again

2) Click **Continue**.



Device Tool in Progress

Source

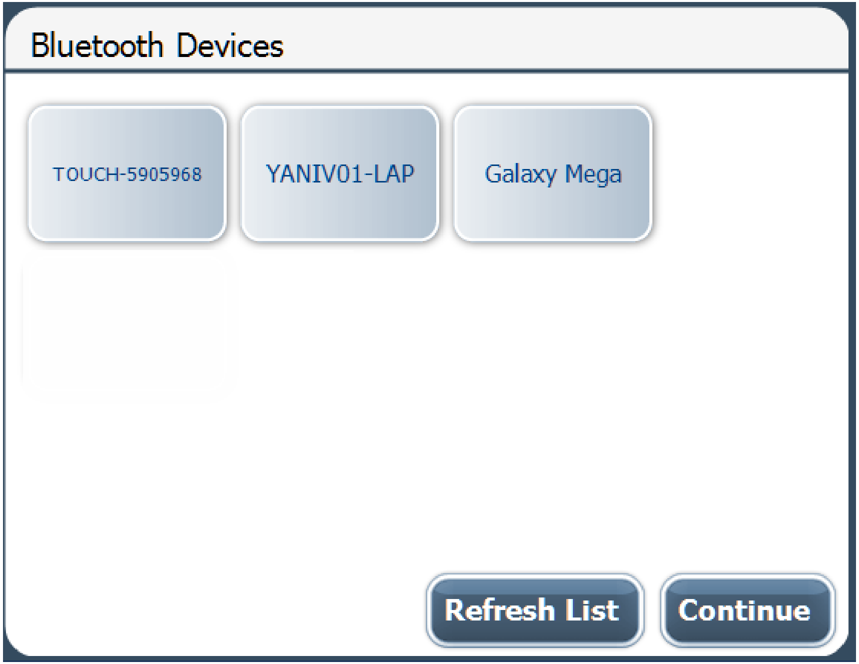
Please Wait...

Initializing Bluetooth

3) A list of Bluetooth devices in the vicinity appears. Select one or the following options:

- Click one of the devices – Device summary screen appears
- Click **Continue** – Device summary screen appears

- Click **Refresh list** - Device tool in progress screen appears and UFED 4PC tries to find additional devices.



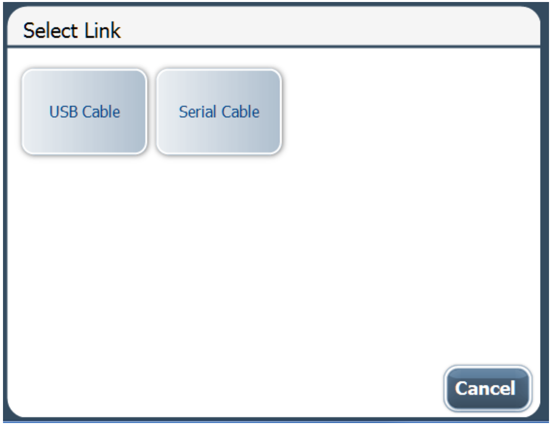
9.2. Switch to CDMA offline mode

This tool enables you to switch radio on CDMA devices to offline mode.

To switch to CDMA offline mode:

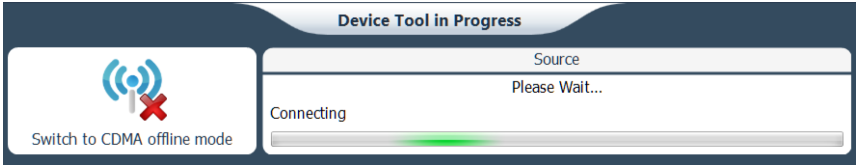
1) Click **Device Tools** and then click **Switch to CDMA offline mode**.

   The Select Link prompt appears.



2) Select the link type (**USB Cable** or **Serial Cable**).

The Device Tool in Progress screen appears.



Device Tool in Progress

Switch to CDMA offline mode

Source

Please Wait...

Connecting

The Device Tool Summary appears.

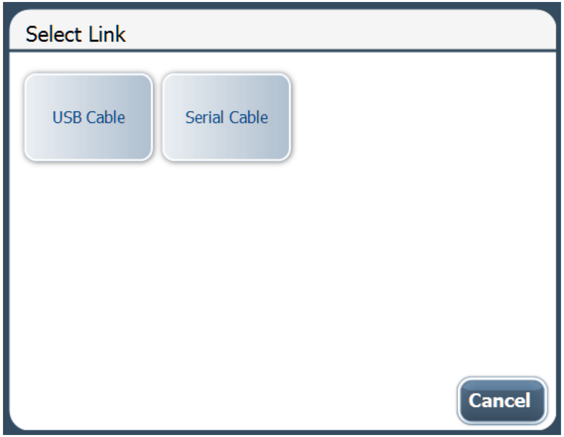
9.3. Test peek/poke functionality

This tool enables you to perform a Peek/Poke test in order to check if the device is supported by the UFED 4PC.

To Test Peek/Poke functionality:

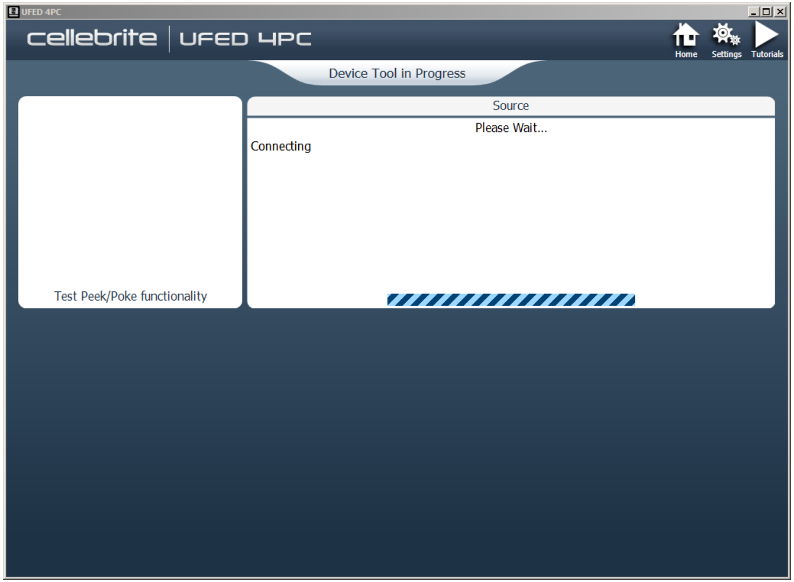
1) Click **Device Tools** and then click **Test Peek/Poke functionality**.

   The Select Link prompt appears.



2) Select the link type (**USB Cable** or **Serial Cable**).

The Device Tool in Progress screen appears.



Please Wait...

Connecting

Test Peek/Poke functionality

The Peek check reply prompt appears.

3) Click **Continue**.

The Device Tool in Progress screen appears.

The Reporting prompt appears.

9.4. Activate TomTom trip log

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

To Activate TomTom trip log:

1) Click **Device Tools** and then click **Activate TomTom trip log**.

   The **Select Mode** prompt appears.

2) Select the desired mode.

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

3) Connect the device to the PC.
4) Click **Continue**.

9.5. Uninstall windows mobile client

In order to perform Logical Extraction, the client is installed on the device. In some cases, due to device failure, or if the mobile device was improperly disconnected from the UFED 4PC, the client remains installed on the mobile device.

This option enables the client to be manually uninstalled.

9.6. Uninstall Android client

In order to perform Logical Extraction, the client is installed on the device. In some cases, due to device failure, or if the mobile device was improperly disconnected from the UFED 4PC, the client remains installed on the mobile device.

This option enables the client to be manually uninstalled.

9.7. Exit Odin mode

In order to perform Logical Extraction, the device is placed in Odin mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from the UFED 4PC, the mobile device remains in Odin mode.

This option enables the device to be taken out of Odin mode.

Chapter 10: **Settings**

The settings screen provides access to a set of functional and behavioral setup options used to control the functionality and usability of UFED 4PC.

To access the settings screen, click Settings in the application taskbar.

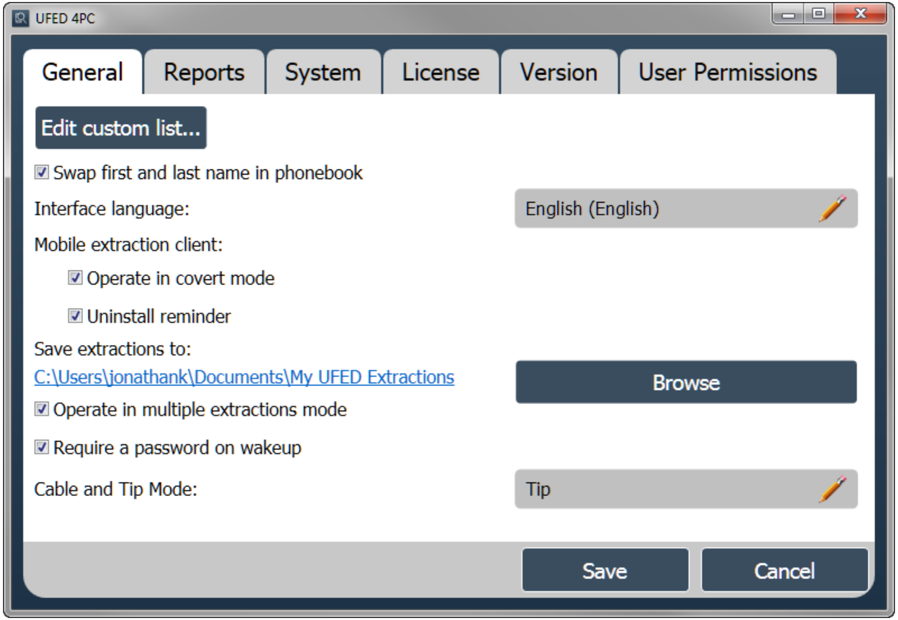
The settings are grouped in the settings screen in the following tabs:

- *General* (page *172*)
- *Report settings* (page *183*)
- *System settings* (page *189*)
- *License settings* (page *191*)
- *Version details* (page *193*)
- *User permissions* (page *195*)

The settings screen opens on the **General** tab.

10.1. General settings

The settings screen opens on the **General** tab.



☑ Swap first and last name in phonebook

Interface language: English (English)

Mobile extraction client:

☑ Operate in covert mode

☑ Uninstall reminder

Save extractions to:
C:\Users\jonathank\Documents\My UFED Extractions

☑ Operate in multiple extractions mode

☑ Require a password on wakeup

Cable and Tip Mode: Tip

The **General** tab provides access to the following functions and settings:

- *Managing the Custom List* (page *173*)
- *Changing the application interface language* (page *177*)
- *Mobile Extraction Client* (page *181*)
- *Changing the extraction location* (page *182*)

To swap the first and last name in the phone book:

- Select **Swap first and last name in phonebook**.

10.1.1. Managing the custom list

The Custom List is the list of devices available for use during the Logical Extraction process.

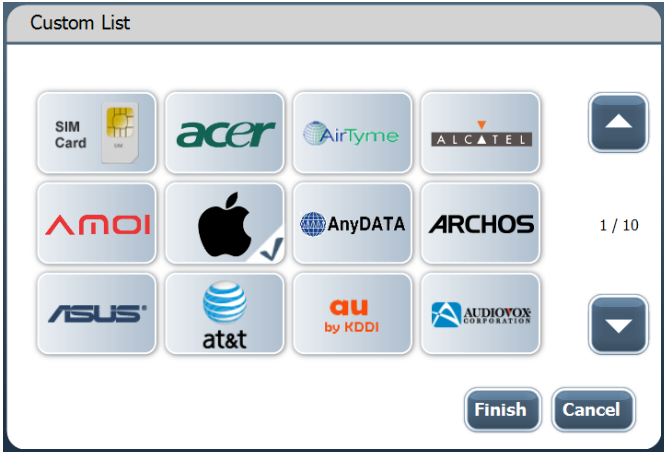
Device models can be added to or deleted from the list. Multiple device models can be defined.

After a Custom List has been defined, a **Custom List** button is added to the Logical Extraction screen.

To add devices to the Custom List:

- Click **Edit Custom List**.

The Custom List opens. In the event that devices have been previously defined in the custom list, the vendor names are selected.

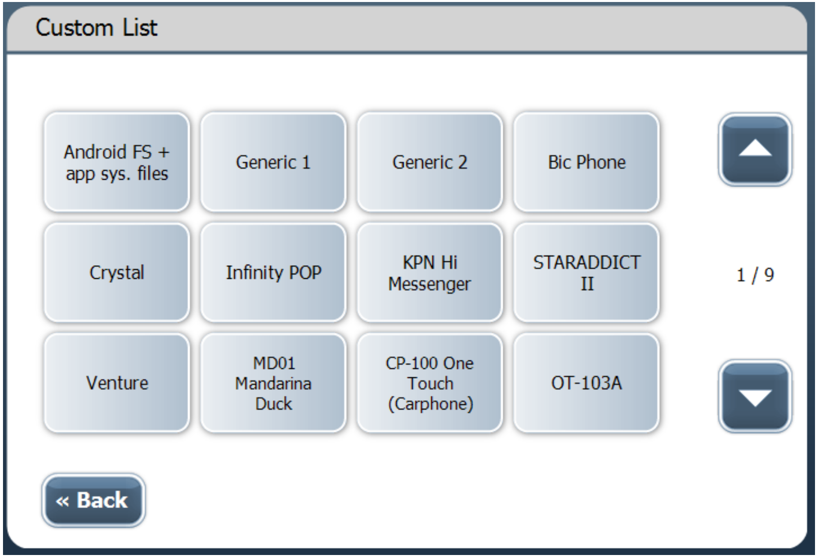


In this example the Apple device was previously defined for the custom list and is indicated with a blue✓.

NOTE: Use ▼ and ▲ to scroll through the lists of manufacturers and devices.

1) In the Custom List, select the required device vendor. For example, **Alcatel**.

   The list of device models appears.

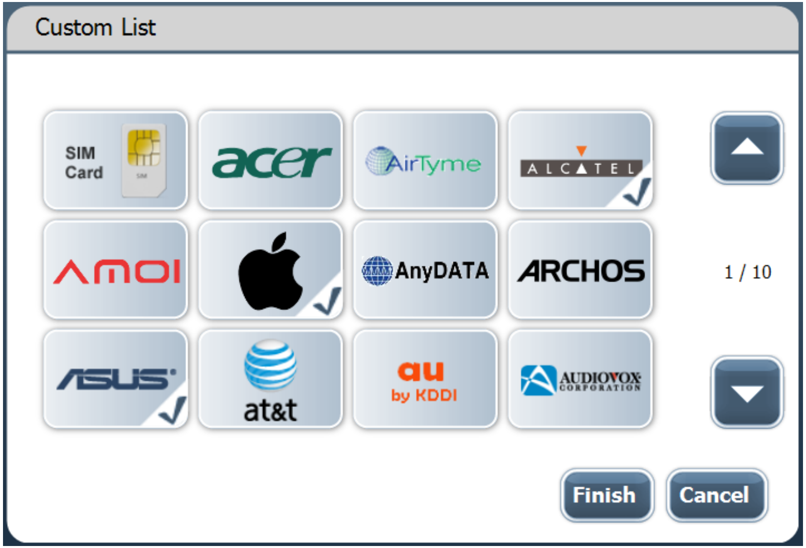


2) Select one or more device models that you would like to associate with this Device Manufacturer.

A blue ✓ appears in each selected device model box.

3) Click **Back**.

The selected manufacturer is marked with a blue ✓.



4) Repeat steps 2-4 for each device manufacturer and model/s to be added to the Custom List.

5) Click **Finish**.

To remove a device from the Custom List:

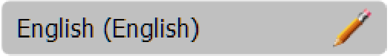
1) Click **Edit Custom List**.
2) In the displayed Custom List dialog, select a device manufacturer marked with a blue✓ that you would like to remove (all the associated models or only one).
3) Select one or more device models marked with a blue✓ that you would like to remove from the Custom List.

   The ✓ mark is removed.
4) Click **Back**.
5) Repeat steps 2-4 for each device that needs to be removes from the Custom List.

   NOTE: Removing all the marked devices of a manufacturer also removes its blue✓ mark.
6) Click **Finish**.

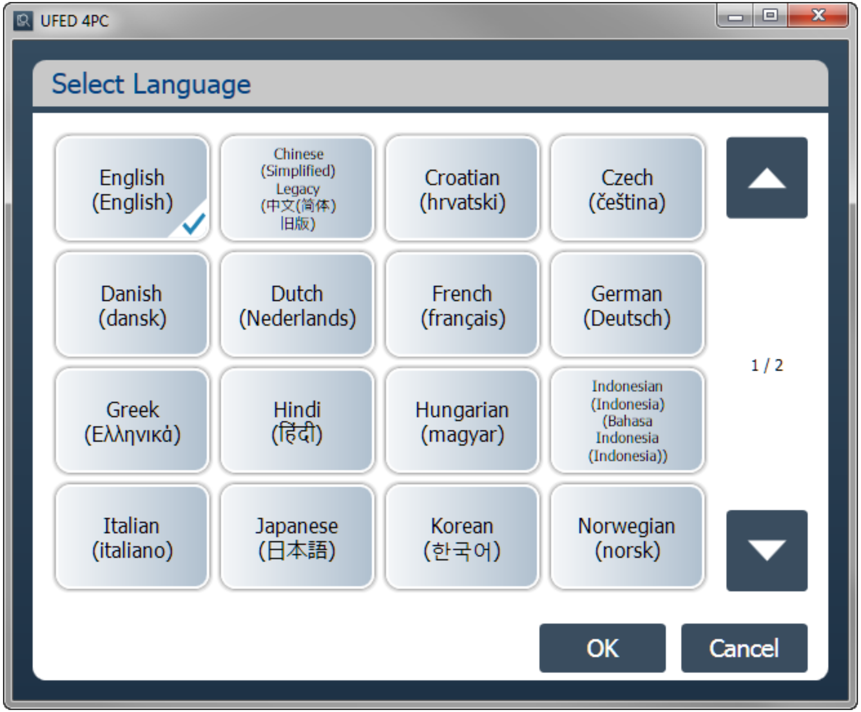
10.1.2. Changing the application interface language

1) Click the language field.



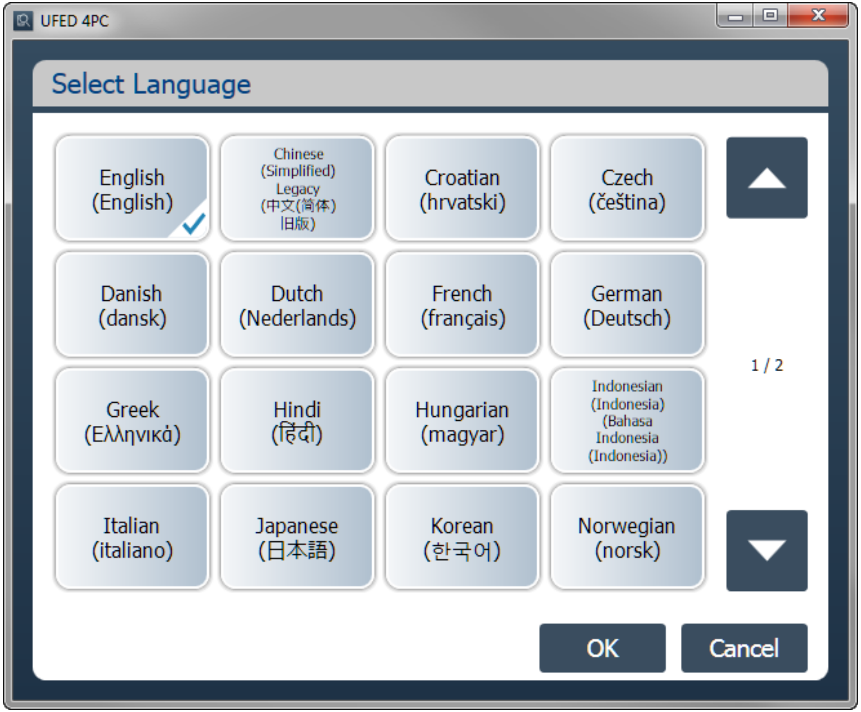
English (English)

The Select Language screen appears with the current language selected. (In this case, **English**).

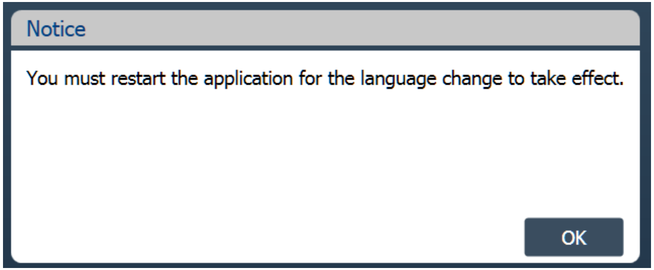


NOTE: Use the arrows to scroll through the list of available interface languages.

2) Click the required language.



The following message appears:



Notice

You must restart the application for the language change to take effect.

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) Close the application.

   b) To re-launch the application, do one of the following:

   - Click the application shortcut icon located in the UFED shortcuts panel at the right of the screen.
   - Double-click the **UFED 4PC** icon located on the Desktop.
   - Click **Start** > **UFED 4PC**

UFED 4PC starts in the selected language.

10.1.3. Mobile extraction client

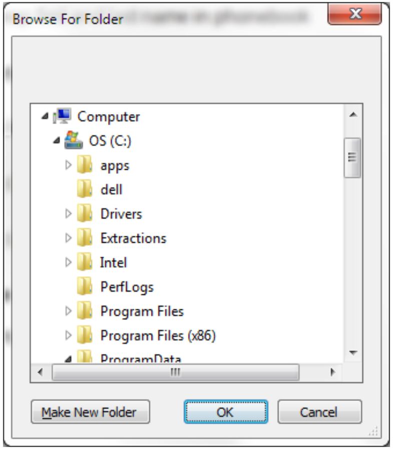
To operate in covert mode:

- In the Settings > **General** tab, select the following:
  - **Operate in covert mode** - Renames the application client name from "Cellebrite.sis/exe" to "AAA.sis/exe".
  - **Uninstall reminder** - When enabled, the UFED 4PC prompts you to uninstall the client from the examined smartphone.

10.1.4. Changing the extraction location

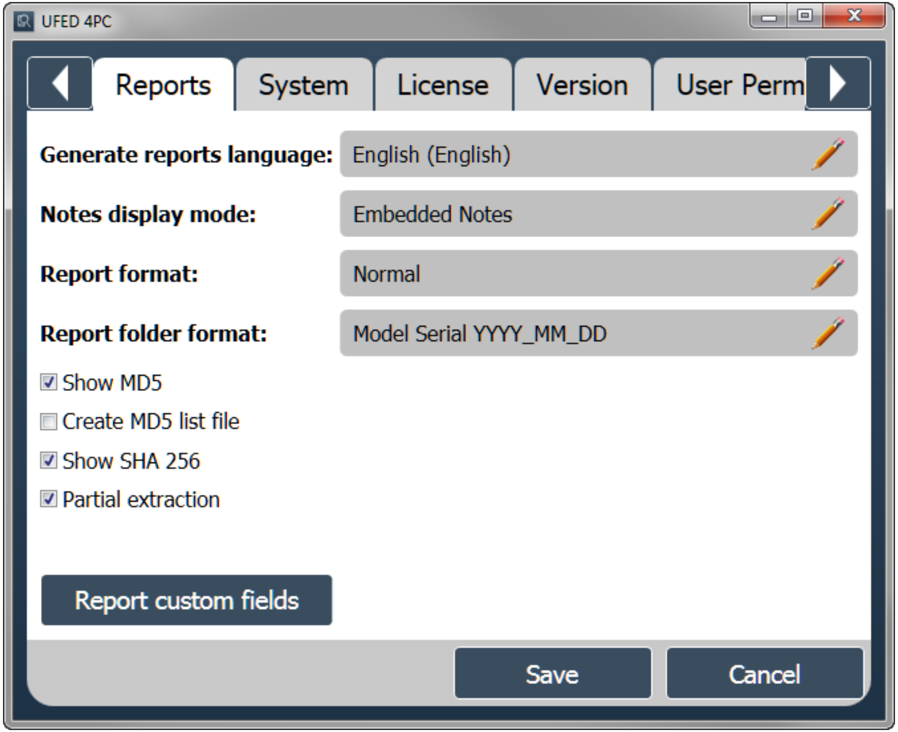
1) In the **Save extractions to** area, click **Browse**.

   The Browse For Folder dialog appears.



2) Select the folder where you want to save the extraction files, and click **OK**.

10.2. Report settings



Generate reports language: English (English)

Notes display mode: Embedded Notes

Report format: Normal

Report folder format: Model Serial YYYY_MM_DD

☑ Show MD5

□ Create MD5 list file

☑ Show SHA 256

☑ Partial extraction

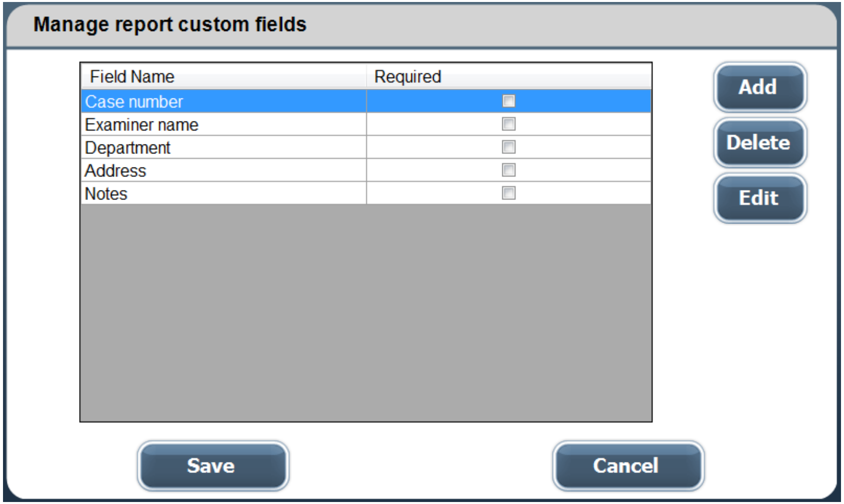
To set the report settings:

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 ✏ 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 ✏ next to **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 **Show MD5** to toggle the display of the MD5 values which are generated for each file in the extracted data.
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 **Show SHA256** 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** to set, 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 *Managing report fields* (page *186*).
11) To set a field as required, click the field in the **Required** column.
12) Click **Save**.

10.2.1. Managing report fields

1) Click **Report custom fields** to customize the report by defining additional fields which will be filled at the end of the extraction.

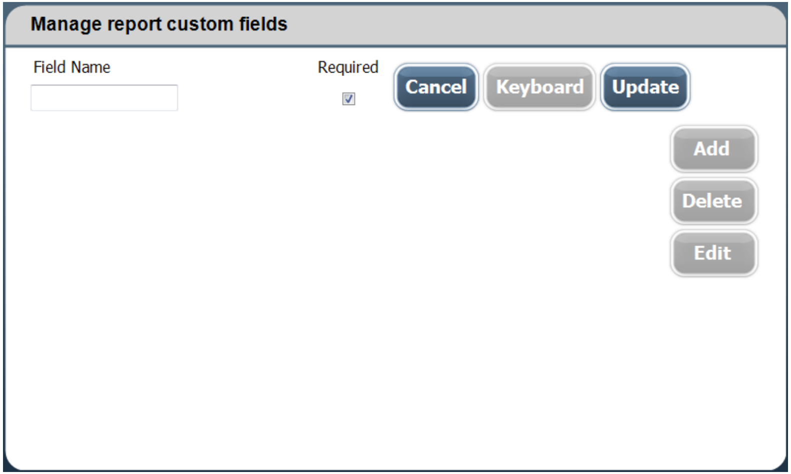


Manage report custom fields

Field Name	Required
Case number	□
Examiner name	□
Department	□
Address	□
Notes	□

2) To add a new field:

   a) Click **Add**.



   b) Enter the field name in the **Field Name** box.

NOTE: To display the keyboard, click **Keyboard**.

   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 3.

4) To edit an existing field:

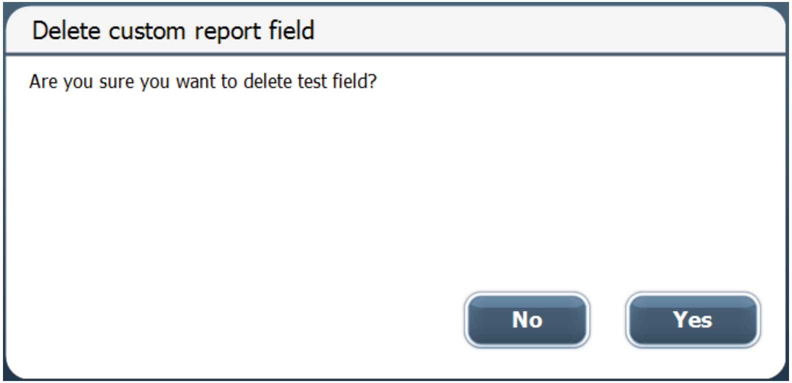
   a) Click the field in the list, and click **Edit**.

   b) Repeat steps 3b-3d.

   NOTE: 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**.



Delete custom report field

Are you sure you want to delete test field?

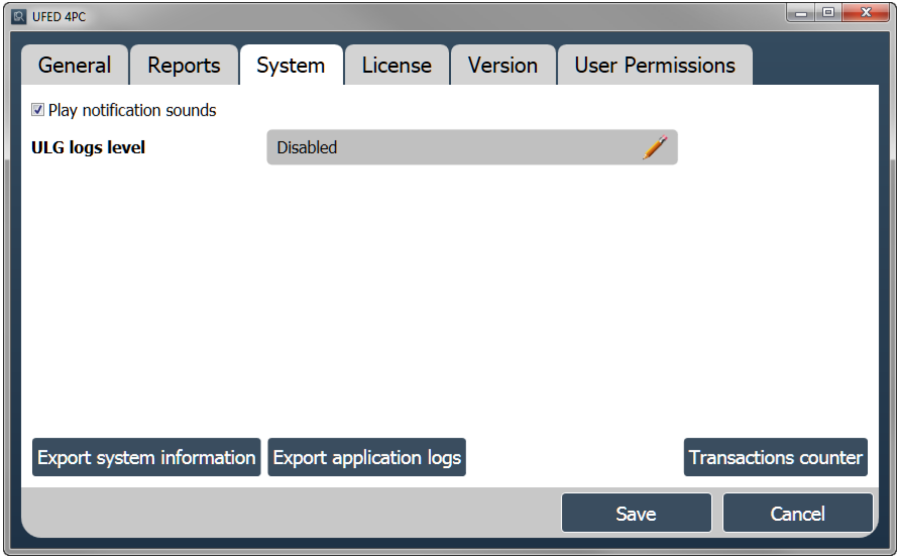
   b) In the confirmation message, click **Yes**.

6) Click **Save** in the **Reports** tab.

10.3. System settings

Set the following in the **System** tab:

- Additional settings
- Extraction target



☑ Play notification sounds

ULG logs level Disabled

Define the following additional settings in the System tab:

1) To set the unit to make a sound for UFED 4PC operations such as failure, select **Play notification sounds**.

2) To change the ULG log level, click ✏ next to **ULG logs level**, and select one of the following:

    - **Disable** – set to not generate log files.
    - **Normal** – set to generate log files. If the transaction is very fast, not all the information is written to the log.
    - **Detailed** – set to generate detailed log files. The transaction will be slower in order to write to the log. Recommended in case of debugging/error situation.

3) To export system information, click **Export system information**.

4) To save the application logs, click **Export application logs**.

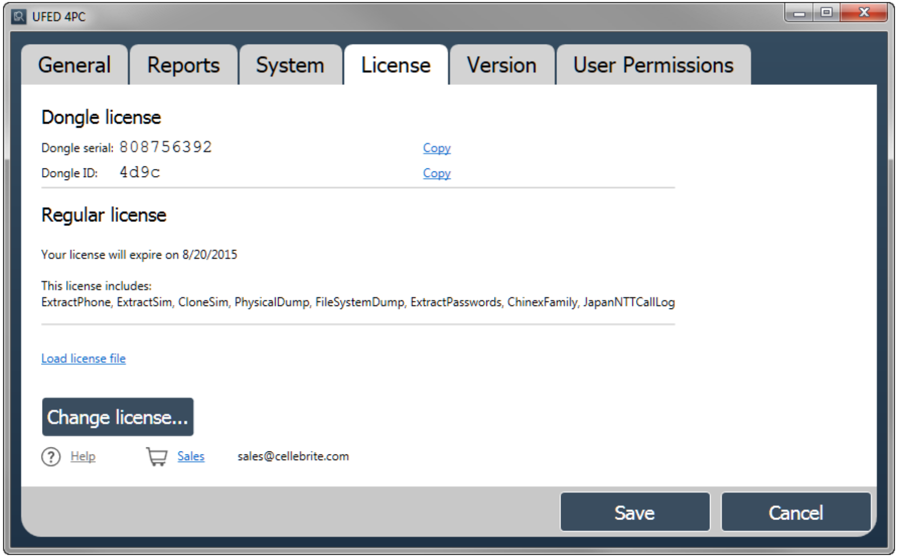
5) To monitor device usage, click the **Transactions counter**. This counts the number of transactions performed on the UFED 4PC. Transactions include all extractions per type and device tool actions. The counters are managed locally and can be reset.

NOTE: The password to rest the Transactions counter is the computer ID (displayed in the Version tab).

10.4. License settings

Change the license type in the **License** tab.

The current license type is displayed.



Dongle license

Dongle serial: 808756392 Copy

Dongle ID: 4d9c Copy

Regular license

Your license will expire on 8/20/2015

This license includes:
ExtractPhone, ExtractSim, CloneSim, PhysicalDump, FileSystemDump, ExtractPasswords, ChinexFamily, JapanNTTCallLog

Load license file

sales@cellebrite.com

To change the license type, follow the instructions in *Activating the license* (page *29*).

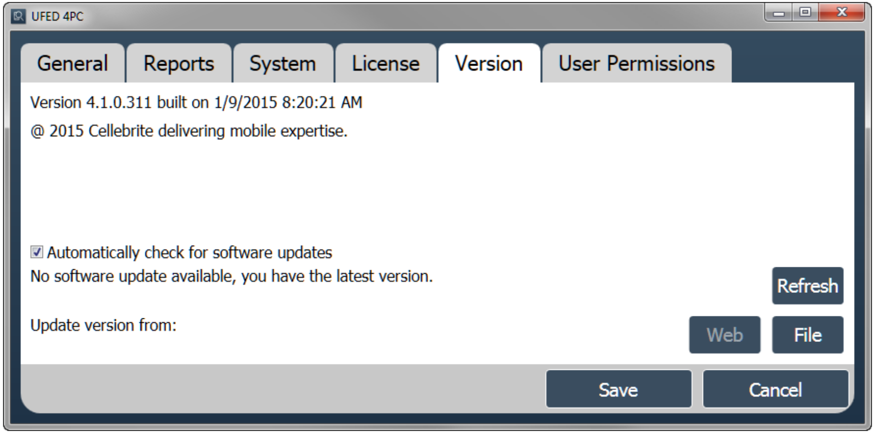
For software licenses, you can do the following:

- To deactivate the current license, click **Deactivate**.
- To update the license, click **Update from file**.

10.5. Version details

The version details display information about the UFED 4PC version and build.

The **Version** tab displays current information regarding the license and the available version for upgrade.



Version 4.1.0.311 built on 1/9/2015 8:20:21 AM

@ 2015 Cellebrite delivering mobile expertise.

☑ Automatically check for software updates

No software update available, you have the latest version.

Update version from:

The following information is displayed:

- **Version** – The application version

For more information on downloading a software update or new version, see *Updates and versions*.

10.5.1. Updates and versions

When UFED 4PC 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 UFED 4PC application via the web:

NOTE: Before using this option, ensure that the unit is connected to the network.

- In the Settings > **Version** tab, in the **Version** area, click **Web**.

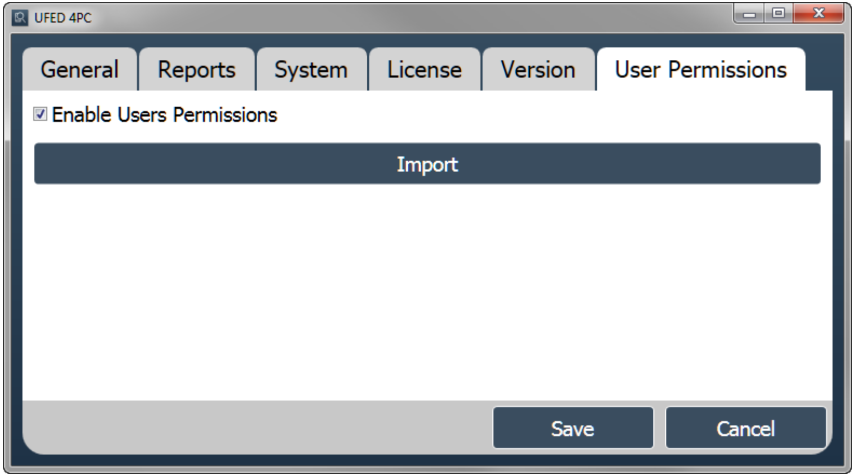
  The unit upgrades the application to the latest version available on the Cellebrite download server.

To install a newer version of the UFED 4PC 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**.

10.6. User permissions

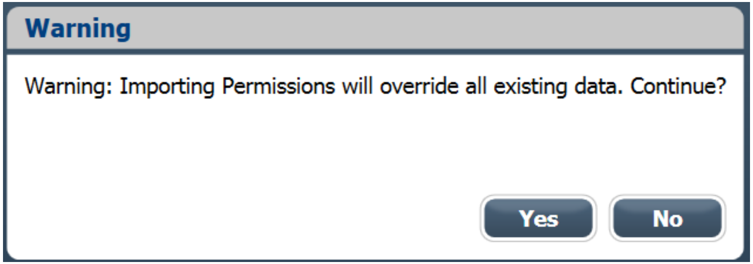
UFED 4PC enables user authentication ensuring that only users with the right credentials can access the application. Access rights are further enforced by defining permission levels per profile. For more information, see *Permission management* ***page*** *197*).



To import user permissions:

1) Run the UFED 4PC as an administrator.
2) Select **Enable Users Permissions** and click **Import**.

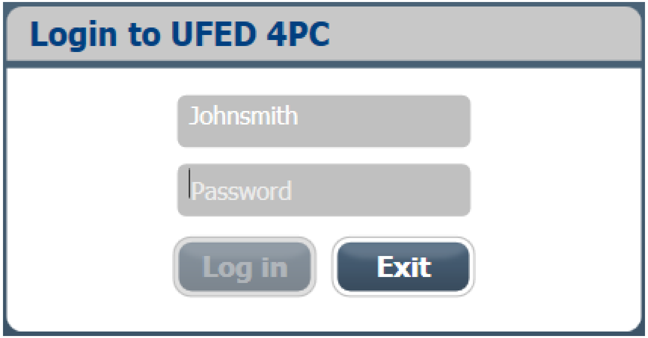
The following warning appears.



Warning

Warning: Importing Permissions will override all existing data. Continue?

3) Click **Yes** and navigate to the directory where the permission management file (*.cp) is located. For information on creating a permission management file, see *Using the UFED Permission Manager page 198*).
4) Click **Open** and then click **Save**.
5) Restart the UFED 4PC application, which will now prompt for login credentials.



6) Use one of the login credentials configured in the permission management file. For more information, see *Permission management*.

10.6.1. Permission management

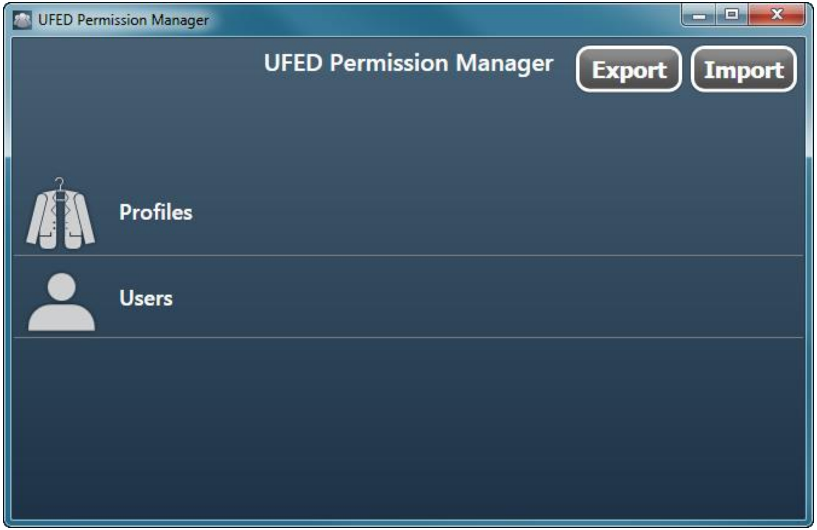
The administrator can create multiple profiles using the UFED Permission Manager standalone application. Each profile contains access permissions, including operation rights per extraction type, content types etc. A single profile can be assigned to multiple users. The users and profiles can be exported into an encrypted permission management file, which can be imported into multiple UFED 4PC applications.

10.6.1.1. Using the UFED Permission Manager

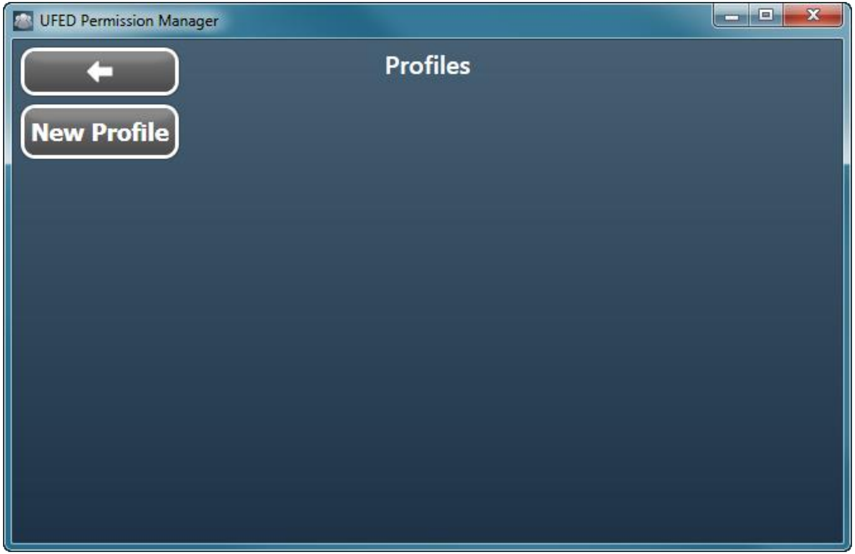
To create a new profile:

1) Download the latest UFED Permission Manager application from your account in MyCellebrite, and save it to a directory on a PC or external device.
2) Run the UFED Permission Manager and follow the setup instructions.

   The UFED Permission Manager screen appears.

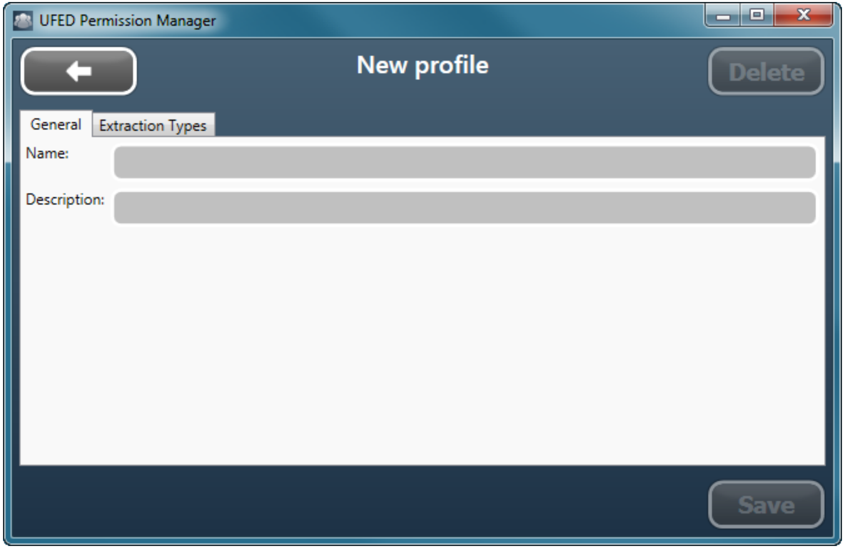


3) Click **Profiles**.

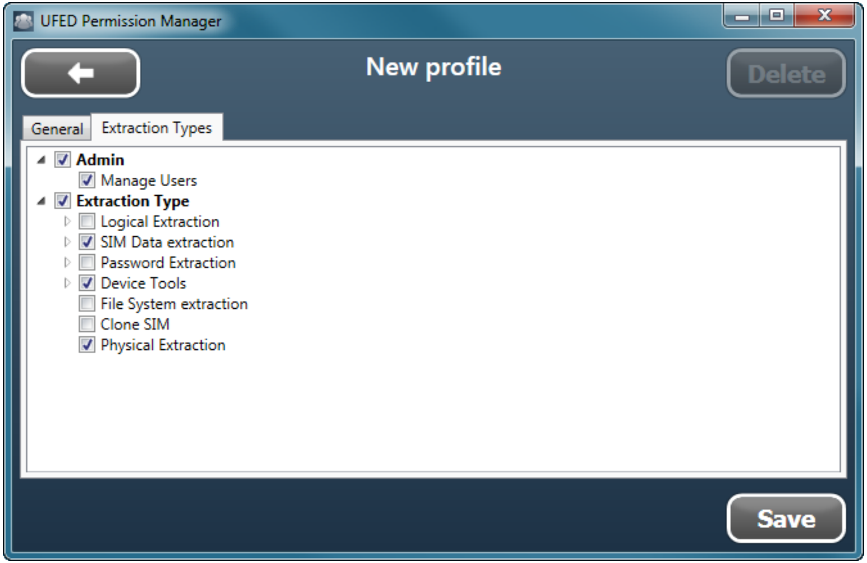


4) Click **New Profile**.

The following screen appears.



5) Enter a name and description for this profile, and then click the **Extraction Types** tab.



- ☑ **Admin**
  - ☑ Manage Users
- ☑ **Extraction Type**
  - □ Logical Extraction
  - ☑ SIM Data extraction
  - □ Password Extraction
  - ☑ Device Tools
  - □ File System extraction
  - □ Clone SIM
  - ☑ Physical Extraction

6) Select the options for this profile, such as Admin who can manage users, and the Extraction Type: Logical Extraction, SIM Data extraction, Password extraction etc.

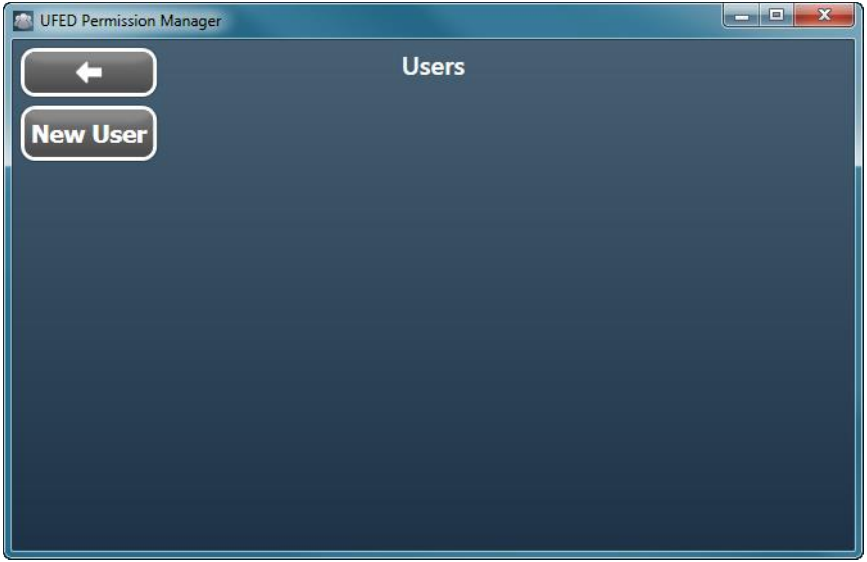
NOTE: At least of the enabled users must be an Administrator (Admin).

7) Click **Save** and proceed to create a new user.

To create a new user:

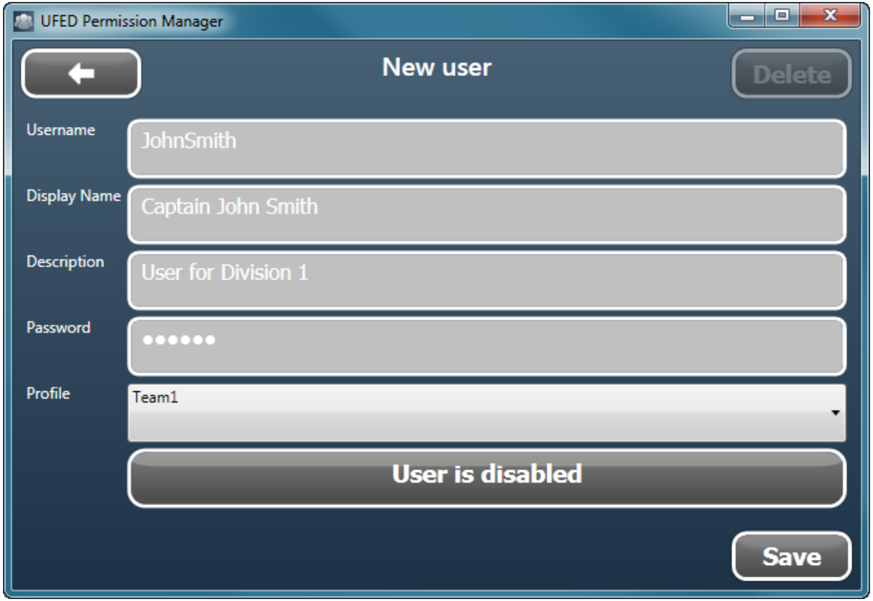
1) In the UFED Permission Manager screen, click **Users**.

   The following screen appears.



2) Click **New User**.

The following screen appears.



New user

Username: JohnSmith

Display Name: Captain John Smith

Description: User for Division 1

Password: ••••••

Profile: Team1

User is disabled

3) Enter the details for the new user including Username, Display Name, Description, and Password.

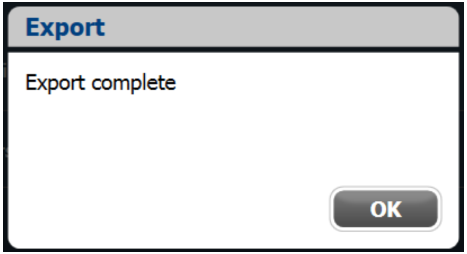
4) Select a profile for the user.

5) Click **User is disabled** to enable the user.
6) Click **Save**.

To export an encrypted permission management file:

1) In the UFED Permission Manager screen, click **Export**, specify a directory for the file and click **Save**.

   The following screen appears.



Export

Export complete

2) Click OK.

   NOTE: The next time you run the UFED Permission Manager you will be prompted for your user credentials to access the application.

   NOTE: Click **Import** to configure an existing permission management file.

Chapter 11: **Special cables**

UFED 4PC requires a special cable for certain functions known as the device power-up cable.

11.1. Device power-up cable

In case of a drained or absent battery, 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, "-", "+".

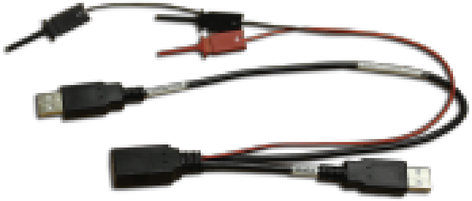


Figure 5: Phone power-up cable

To connect the device power-up cable:

1) Connect the Extra Power connector to the UFED 4PC USB Port extension.
2) Connect the Data connector to the UFED 4PC USB Port extension.
3) Identify the device's battery contacts:
   - Open the device battery cover.
   - Locate the positive ('+') and negative ('–') pole markings of the battery, usually found next to the contacts area.
   - Make sure that the battery contacts are marked clearly on the device's body.
   - Remove the battery in order 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, simply 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.

   NOTE: Use a multi-meter 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 to middle pole in case of three poles or to the one next to the (-) in case of 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 UFED 4PC menu.

11.2. USB extension cable for UFED Device Adapter

In the Desktop environment where the computer is mounted in a difficult to access or distant location the **USB Extension cable for UFED Device Adapter** should be used. This USB extension cable is 150cm in length and will allow for the easy and accessible placement of the UFED Device Adapter.

The **USB Extension cable for UFED Device Adapter** 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 an extension cable is needed it is **essential** that the provided **USB Extension cable for UFED Device Adapter** is used. Use of third-party cables will affect performance of your UFED 4PC and may prevent some functions from starting or completing.

11.3. USB Cable for UFED Device Adapter PowerUP

Two USB PowerUP cables have been provided with your UFED 4PC.

- The **USB Cable for UFED Device Adapter PowerUP S** has been provide with your UFED 4PC for use in the laptop environment. It is 75cm in length.
- The **USB Cable for UFED Device Adapter PowerUP L** has been provide with your UFED 4PC for use in the Desktop environment. 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 will plug into the UFED Device Adapter and a USB-A connector which can be plugged into any available powered USB port - including A/C powered USB chargers and car chargers.

The PowerUP cable will double the power capacity of the **UFED Device Adapter.** This will ensure that all devices with excess power requirements will function correctly and will allow UFED 4PC to provide all functions. In addition devices that are fully discharged may need the additional power that the PowerUp cable will provide.

In the desktop environment it is recommended that the PowerUp cable is used at all times.

In the laptop environment it is recommended that the PowerUp cable is used when UFED 4PC indicates that the extra power is needed.

NOTE: The PowerUp cable is NOT required for smooth operation of the UFED 4PC for most devices, but is provided for those cases where power consumption is above the capacity of the unpowered **UFED Device Adapter**.

Chapter 12: **Regulatory compliance**

Part	UFED Standard and Ruggedized
CE This device complies with the essential requirements the R&TTE 1999/5/EC Directive and the following standards:	
EMC	EN 301 489-1 EN 301 489-7
Safety	IEC/EN 60950-1, CB Scheme
Radio frequency spectrum usage	EN 300 328 V1.7.1
FCC	
EMC	FCC part 15, subpart B
Radio	FCC part15.247

Chapter 13: **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.

13.1. 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, it is possible to perform a physical or file system extraction on almost any Android device, provided that the device USB debugging option is enabled. All currently available Android OS versions are supported. For more information, see *Android Debugging Bridge method* (page *212*).
- 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 *Bootloader extraction* (page *215*).

13.1.1. 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:

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

Q: How do I turn on the USB debugging option?

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: The device USB debugging option must be turned on before it’s 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/password). Following a successful physical extraction, you can view the numeric password or pattern lock protecting the device in UFED 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, UFED 4PC automatically detects the Android OS version, and whether or not access is at administrator level. If it is not, UFED 4PC automatically gains root permissions.

NOTE: It is possible to 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: Once 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 UFED 4PC, what are "Method 1" and "Method 2"? Which should I choose?

A: Methods 1 and 2 are different connection configurations. It is not possible to 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.

13.1.2. 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.

13.2. Performing a file system extraction for an Android device

13.2.1. Locked Motorola devices

If you have a locked Motorola device, perform the following procedure to bypass the lock and perform a file system extraction:

1) click **File System Extraction**.

The Select Vendor screen appears.

NOTE: If you do not see the device model in the list, select **<Vendor> Generic** option.

The Select Mode screen opens.

2) If lock bypass is supported for the device, select **File System Bypassing Lock (Recommended)**.
3) Follow the on-screen instructions.

File system extraction is successful for locked Motorola devices in the following circumstances:

- If lock bypass is supported for the device.
- If lock bypass is not supported for the device, but the device **USB debugging** option is enabled.

4) If lock bypass is NOT supported for the device, and the device **USB debugging** option is NOT enabled, perform a physical extraction in order to retrieve the device lock code, and unlock the device. Then follow the directions in *Unlocked devices* (page *219*).

13.2.2. Locked HTC, Huawei, and ZTE devices

If you have a locked HTC, Huawei, or ZTE device, perform the following procedure to bypass the lock and perform a file system extraction:

1) Click **File System Extraction**.

NOTE: If you do not see the device model in the list, select **<Vendor> Generic** option.

2) Follow the on-screen instructions.

File system extraction is successful for locked HTC devices in the following circumstances:

- If lock bypass is supported for the device.
- If lock bypass is not supported for the device, but the device **USB debugging** option is enabled.

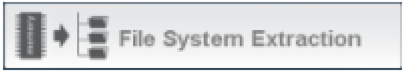
File system extraction is NOT successful for locked HTC devices in the following circumstances:

- If lock bypass is NOT supported for the device, and the device **USB debugging** option is NOT enabled.

13.2.3. Other locked devices

If you have a locked device that is not an HTC or Motorola device, perform the following procedure to bypass the lock and perform a file system extraction:

1) Click **File System Extraction**.



NOTE: If you do not see the device model in the list, select **<Vendor> Generic** option.

2) Follow the on-screen instructions.

File system extraction is successful for locked devices if the device **USB debugging** option is enabled.

3) If the device **USB debugging** option is NOT enabled, perform a physical extraction in order to retrieve the device lock code, and unlock the device. Then follow the directions in *Unlocked devices* (page *219*).

13.2.4. Unlocked devices

If you have an unlocked device, perform the following procedure to perform a file system extraction:

1) Click **File System Extraction**.

2) Do one of the following:

   - For an advanced File System extraction including application system files, select **Android FS + app sys. files**.
   - For a standard File System extraction, select the device model.

   NOTE: If you do not see the device model in the list, select **<Vendor> Generic** option.

3) Follow the on-screen instructions. File system extraction is successful for unlocked devices.

13.3. 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 (known as "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*).

Chapter 14: **Appendix**

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. DOWNLOADING, INSTALLING OR USING CELLEBRITE-SUPPLIED SOFTWARE CONSTITUTES ACCEPTANCE OF THIS AGREEMENT.

CELLEBRITE IS WILLING TO LICENSE THE SOFTWARE TO YOU ONLY IF YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS AGREEMENT (THE "EULA"), ANY ADDITIONAL TERMS IN AN AGREEMENT SIGNED BY BUYER (AS DEFINED BELOW) AND CELLEBRITE AND ANY "CLICK-ACCEPT" AGREEMENT, AS APPLICABLE. TO THE EXTENT OF ANY CONFLICT AMONG THIS AGREEMENT, ANY ADDITIONAL TERMS IN AN AGREEMENT SIGNED BY BUYER AND CELLEBRITE, ANY "CLICK-ACCEPT" AGREEMENT, ANY TERMS ON A PURCHASE ORDER AND CELLEBRITE’S TERMS AND CONDITIONS OF SALE, THE ORDER OF PRECEDENCE SHALL BE (A) AN AGREEMENT SIGNED BY BUYER AND CELLEBRITE; (B) THIS AGREEMENT; (C) THE "CLICK-ACCEPT" AGREEMENT; (D) CELLEBRITE’S TERMS AND CONDITIONS OF SALE; AND (E) BUYER’S PURCHASE ORDER, TO THE EXTENT SUCH TERMS ARE PERMISSIBLE UNDER CELLEBRITE’S TERMS AND CONDITIONS OF SALE OR AN AGREEMENT SIGNED BY BUYER AND CELLEBRITE (COLLECTIVELY, (A)-(E), AFTER APPLYING THE ORDER OF PRECEDENCE, THE "AGREEMENT").

BY DOWNLOADING, INSTALLING OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED IN THE AGREEMENT, YOU INDIVIDUALLY AND ON BEHALF OF THE BUSINESS OR OTHER ORGANIZATION THAT YOU REPRESENT (THE "BUYER") CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED IN THE

AGREEMENT, THEN (A) DO NOT DOWNLOAD, INSTALL OR USE THE SOFTWARE (OR, AS APPLICABLE, THE CELLEBRITE PRODUCT IN WHICH THE SOFTWARE IS EMBEDDED), AND (B) WITHIN THIRTY (30) DAYS AFTER RECEIPT OF THE SOFTWARE (OR, IF AN AGREEMENT BETWEEN YOU AND CELLEBRITE PROVIDES A SHORTER TIME PERIOD FOR ACCEPTANCE, SUCH SHORTER TIME PERIOD FOR ACCEPTANCE), EITHER RETURN THE SOFTWARE TO CELLEBRITE OR THE APPLICABLE AUTHORIZED RESELLER FOR FULL REFUND OF THE SOFTWARE LICENSE FEE, OR, IF THE SOFTWARE IS EMBEDDED IN A CELLEBRITE PRODUCT FOR WHICH NO SEPARATE SOFTWARE LICENSE FEE WAS CHARGED, RETURN THE EQUIPMENT AND EMBEDDED SOFTWARE, UNUSED, TO CELLEBRITE OR THE APPLICABLE RESELLER FOR A FULL REFUND OF THE PURCHASE PRICE. YOUR RIGHT TO RETURN AND REFUND ONLY APPLIES IF YOU ARE THE ORIGINAL END USER PURCHASER.

This EULA governs Buyer's access to and use of the Software (as defined below) first placed in use by Buyer on or after the release date of this EULA (the "Release Date").

4) **DEFINITIONS** – In this Agreement, the following capitalized terms shall have the meaning set forth below:

"**Affiliate**" of a party means such party's parent corporation, an entity under the control of such party's parent corporation at any tier or an entity controlled by such party at any tier. For these purposes, "control" shall mean the power to direct or cause the direction of the management and policies of the entity, whether through the ownership of more than 50% of the outstanding voting interests in such entity or otherwise.

"**Authorization Product**" means a product sold by Cellebrite or an authorized reseller of Cellebrite with embedded License Authorization Software, including but not limited to a USB stick with embedded License Authorization Software.

"**Authorized Users**" means the number of Concurrent Users that Buyer is licensed to have access to the Software.

"**Cellebrite**" means (i) Cellebrite Mobile Synchronization Ltd., an Israeli corporation with offices at 94 Em Hamoshavot Road, Petach Tikva, Israel 49130 or (ii) any subsidiary of Cellebrite Mobile Synchronization Ltd. (Including without limitation Cellebrite USA Inc. and Cellebrite GMBH) which is engaged by Buyer and issue invoices to Buyer with respect to the Software and/or the Product; as applicable.

"**Concurrent Users**" means the number of Users of Buyer concurrently accessing the Software. If a single User connects to Software using multiple concurrent log-ins or connections, each such active logical connection or log-in is counted toward the number of Concurrent Users.

"**Documentation**" means any documentation related to any Software.

"**Embedded Software**" means a copy of Software delivered embedded in or loaded onto Cellebrite hardware equipment when such equipment is sold by Cellebrite. Updates or Upgrades to Embedded Software are also deemed "Embedded Software" to the extent such an Update or Upgrade would be deemed Embedded Software without regard to this sentence had it been delivered installed on the Cellebrite equipment.

"**Forensic Product**" means a Product used for the purposes of conducting forensic analysis, including without limitation Products sold under the trade name "UFED".

"**License Authorization Software**" means Software that is provided together with hardware on which it is embedded that is used to validate the authorized use of Standalone Software.

"**License Term**" means the term of a paid subscription to the Standalone Software.

"**Product**" means a product sold by Cellebrite or an authorized reseller of Cellebrite with Embedded Software.

"**Software**" means an instance of a program, module, feature, function, service, application, operation or capability of the Cellebrite-supplied software. Software includes Embedded Software and Standalone Software.

"**Standalone Software**" means Software that is not Embedded Software or License Authorization Software.

"**Third Party**" means an individual or entity other than Buyer, Buyer's Affiliates, Cellebrite and Cellebrite's Affiliates.

"**Update**" means an update to the Software or the Standalone Software that is provided by Cellebrite and that may incorporate (i) corrections of any substantial defects; (ii) fixes of any minor bugs; (iii) at the sole discretion of Cellebrite, allowing additional compatibility of the Software with cellular phones provided by third parties; and/or (iv) at the sole discretion of Cellebrite, minor enhancements to the Software or Standalone Software, as the case may be; provided, however, that Updates shall not include Upgrades. Updates are generally identified by Cellebrite by a change to the version number to the right of the first decimal point (e.g., version 4.1 to 4.2).

"**Upgrade**" means a new release of the Software or Standalone Software that incorporates substantial changes or additions that (i) provide additional value and utility; (ii) may be priced and offered separately as optional additions to the Software or the Standalone Software, as the case may be; and/or (iii) are not generally made available to Cellebrite's customers without a separate charge. Upgrades are generally identified by Cellebrite by a change to the version number to the left of the first decimal point (e.g., version 4.2 to 5.0).

"**User**" means an individual able to gain access to any Software functionality (whether Embedded Software or Standalone Software).

"**You**" means any individual seeking the benefit of or evaluating this EULA.

5) LICENSE GRANT

A. **Embedded Software**. Subject to the terms and conditions of this Agreement, Cellebrite hereby grants to Buyer, and Buyer accepts, upon delivery of the Embedded Software, a nonexclusive, perpetual and nontransferable license to use (only if such use does not violate the prohibitions in Sections 2.F or 2.G) each copy of the Embedded Software, in executable form only, provided by Cellebrite, and the accompanying documentation, only for Buyer's internal use in connection with the Products, in the country in which the Product with the Embedded Software was purchased from Cellebrite or an authorized reseller of Cellebrite and only as authorized in the Agreement.

i. **General Limitations**. Buyer shall use Embedded Software solely for execution on the unit of Product originally delivered to Buyer with such Embedded Software installed, or any replacement unit provided under a warranty from Cellebrite. Any Update or Upgrade of such Embedded Software that Cellebrite has licensed to Buyer may be loaded and executed only on the Product on which the originally licensed Embedded Software is authorized to execute.

ii. **License Exclusion**. Notwithstanding any other provision of this EULA, except as may otherwise be required by applicable law, no license is granted for installation or use of any Embedded Software or associated Update or Upgrade on any Product resold by anyone who is not an authorized reseller of Cellebrite for such Product.

iii. **Single Product**. Buyer's license to the Embedded Software is limited to a license to use the Embedded Software on one (1) Product for each Product purchased from Cellebrite or Cellebrite's authorized reseller.

B. **Standalone Software**. Subject to the terms and conditions of this EULA, Cellebrite hereby grants to Buyer, and Buyer accepts, upon delivery of the Standalone Software, during the License Term, a nonexclusive and nontransferable license to (i) use (only if such use does not violate the prohibitions in Sections 2.F or 2.G) each copy of the Standalone Software, in executable form only, provided by Cellebrite, and the accompanying documentation, only for Buyer's internal use, only as authorized in the Agreement; (ii) only use a number of Concurrent Users that is equal to or less than the number of Authorized Users specified in a written agreement signed by both the Buyer and Cellebrite or purchase order accepted by Cellebrite, even if available on a higher number of computer systems; (iii) make a reasonable number of copies of the Standalone Software for use only as licensed in this Section 2.B, though in no case more than the number of Authorized Users; and (iv) make one (1) copy of the Standalone Software for backup, archival or disaster recovery purposes.

C. **License Authorization Software**. Subject to the terms and conditions of this EULA, Cellebrite hereby grants to Buyer, and Buyer accepts, upon delivery of the Standalone Software, during the License Term, a nonexclusive and nontransferable license to use (only if such use does not violate the prohibitions in Sections 2.F or 2.G) each copy of the License Authorization Software, in executable form only, provided by Cellebrite, and the accompanying documentation, only for Buyer's internal use and only in the country in which the Standalone Software was licensed from Cellebrite or an authorized reseller of Cellebrite and only as authorized in the Agreement. Buyer's license to the License Authorization Software is limited to a license to use the License Authorization Software on one (1) Authorization Product for each license to the Standalone Software the authorized use of which is validated by such License Authorization Software and where such license is purchased from Cellebrite or Cellebrite's authorized reseller.

D. **Updates and Upgrades**.

i. **Updates**. Updates or Upgrades to the Software may be made available to Buyer pursuant to a separate agreement between Cellebrite and Buyer. Any particular Update or Upgrade shall be licensed under the terms of the Software that is being updated by such Update or Upgrade, as the case may be.

ii. **Limitation**. Except as expressly provided in the Agreement, Buyer shall have no rights in any Update or Upgrade to Software, nor any rights to support services associated with such Software.

iii. **No Obligation**. Nothing in this EULA requires Cellebrite to provide Updates or Upgrades to Buyer or Buyer to accept such Updates or Upgrades. The provision of any Updates or Upgrades shall be governed by a separate agreement between Cellebrite and Buyer, or by a purchase order issued by Buyer and accepted by Cellebrite, in Cellebrite's sole discretion.

E. **Specific License Terms for Particular Products**.

i. **Forensic Products**. Subject to the terms and conditions of this Agreement, Cellebrite hereby grants to Buyer, and Buyer accepts, a nonexclusive, time-limited and nontransferable license, effective upon delivery, to use (only if such use does not violate the prohibitions in Sections 2.F or 2.G) a copy of an Update or Upgrade to the Embedded Software, in executable form only, provided by Cellebrite, and the accompanying documentation, only for Buyer's internal use in connection with the Forensic Products or for a trial of such Update or Upgrade, as the case may be, in the country in which the Forensic Product with the Embedded Software was purchased from Cellebrite or an authorized reseller of Cellebrite and only as authorized in the Agreement, for a period as specified by Cellebrite, but, in any case, no longer than seven (7) days. Any time-limited license for the Embedded Software on a Forensic Product shall be subject to the foregoing license grant and such license may be issued at Cellebrite's sole discretion. Buyer agrees to provide to Cellebrite one or more email addresses at which Cellebrite can contact Buyer for communications from Cellebrite, including regarding Updates or Upgrades. Buyer shall provide Cellebrite with updated email address(es) each time such email address(es) change.

ii. **Forensic Products Exclusions**. Any use or operation of the Cellebrite UFED family of products (including without limitation, UFED Logical, UFED Ultimate, UFED Physical Analyzer) in connection with any product and/or cellular device developed, manufactured, produced, programmed, assembled or otherwise maintained by any corporation, shall be permitted only after the User of the Cellebrite UFED family of products has obtained any consents or approvals required (to the extent required) pursuant to applicable law in the jurisdiction in which such use is made. UNDER NO CIRCUMSTANCES SHALL CELLEBRITE, ITS OFFICERS, EMPLOYEES OR REPRESENTATIVES BE LIABLE TO USER OR ANY OTHER THIRD PARTY UNDER ANY CAUSE OF ACTION (WHETHER IN CONTRACT, TORT OR OTHERWISE) FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES UNDER ANY LEGAL THEORY WHATSOEVER ARISING OUT OF OR RELATING TO THE USE OF THE CELLEBRITE UFED FAMILY OF PRODUCTS IN CONNECTION WITH ANY PRODUCT AND/OR CELLULAR DEVICE DEVELOPED, MANUFACTURED, PRODUCED, PROGRAMMED, ASSEMBLED OR OTHERWISE MAINTAINED BY ANY CORPORATION, WITHOUT OBTAINING THE APPLICABLE CONSENTS AND APPROVALS. User agrees to indemnify and hold harmless Cellebrite its directors, shareholders and employees, from and against any damages, claims, liabilities and expenses (including legal fees) arising as a result of the use of the Cellebrite UFED family of products in connection with any product and/or cellular device developed, manufactured, produced, programmed, assembled or otherwise maintained by any corporation, without obtaining the applicable consents and approvals.

iii. **Reserved**.

F. **No Right to Sublicense or Assign**. Except to the extent otherwise required by applicable law or expressly provided for assignment generally in the Agreement, no license provided in this Section 2 is sublicensable, transferable or assignable by Buyer, including by operation of law, change of control, merger, purchase or otherwise, without the prior written consent of Cellebrite in each instance. Other than as expressly permitted by the foregoing, any attempted sublicense, transfer or assignment by Buyer shall be null and void.

G. **License Prohibitions**. Notwithstanding anything to the contrary in this EULA, Buyer shall not, alone, through a User, an Affiliate or a Third Party (or allow a User, an Affiliate or a Third Party to): (a) modify any Software; (b) reverse compile, reverse assemble, reverse engineer or otherwise translate all or any portion of any Software; (c) pledge, rent, lease, share, distribute, sell or create derivative works of any Software; (d) use any Software on a time sharing, service bureau, application service provider (ASP), rental or other similar basis; (e) make copies of any Software, except as provided for in the license grant above; (e) remove, alter or deface (or attempt any of the foregoing) proprietary notices, labels or marks in any Software; (f) distribute any copy of any Software to any Third Party, including without limitation selling any Product with Embedded Software in a secondhand market; (g) use any Embedded Software other than with Products provided by Cellebrite or an authorized reseller of Cellebrite or for more than the number of Products purchased from Cellebrite or an authorized reseller of Cellebrite; (h) disclose the results of testing or benchmarking of any Software to any Third Party without the prior written consent of Cellebrite; (i) use any Update or Upgrade beyond those to which Buyer is entitled or with any Software to which Buyer does not have a valid, current license; (j) deactivate, modify or impair the functioning of any disabling code in any Software; (k) circumvent or disable Cellebrite's copyright protection mechanisms or license management mechanisms (l) use the Software in violation of any applicable law or to support any illegal activity; (m) use the Software to violate the rights of any Third Party; or (n) attempt any of the foregoing. Cellebrite expressly reserves the right to seek all available legal and equitable remedies to prevent any of the foregoing and to recover any lost profits, damages or costs resulting from any of the foregoing.

H. **Legal Exception**. Buyer agrees that, to the extent that any applicable laws (including without limitation national laws implementing EC Directive 91/250 on the Legal Protection of Computer Programs) give Buyer the right to reverse engineer any Software to make it interoperable without Cellebrite's consent, before Buyer exercises any such rights, Buyer shall notify Cellebrite of such desire and, no later than sixty (60) days following receipt of such request, Cellebrite may decide either: (a) to perform the work to achieve such interoperability and charge its then-standard rates for such work to Buyer; or (b) to permit Buyer to reverse engineer parts of the Software only to the extent necessary to achieve such interoperability. Only if and after Cellebrite, at its sole discretion, partly or completely denies Buyer's request, shall Buyer exercise its statutory rights.

I. **Network Usage**. Buyer understands and agrees that Cellebrite may use Buyer's internal network and Internet connection for the limited purpose of transmitting license-related data at the time of installation, registration, use or update of Software to a Cellebrite-operated license server. At such time, Cellebrite may validate the license-related data in order to protect Cellebrite against unlicensed or illegal use of the Software. Cellebrite may, at its option, only permit activation of the Software upon exchange of license related data between Buyer's computer and the Cellebrite license server.

6) **OWNERSHIP** – Cellebrite (or its licensors) retains ownership of all right, title and interest in and to the Software and Documentation and any derivative works thereof, and all copies of the Software. Nothing in this EULA constitutes a sale, transfer or conveyance of any right, title or interest in the Software or Documentation and any derivative works thereof. Notwithstanding anything to the

contrary, all Software is licensed and not sold and any reference to a sale of Software shall be understood as a license to Software under the terms and conditions of the Agreement.

7) **CONFIDENTIALITY** – Buyer agrees the Software and Documentation are the confidential information of Cellebrite. Buyer shall maintain the Software and Documentation in confidence, using the same degree of care it uses for its own confidential information, but at least reasonable care.

8) **EXCLUSIVE REMEDIES AND LIMITATION OF LIABILITY.**

A. **Definitions**. For purposes of the exclusive remedies and limitations of liability set forth in this Section 5, Cellebrite shall be deemed to include its subsidiaries and affiliates and the directors, officers, employees, agents, representatives, shareholders, subcontractors and suppliers of each of them; and "damages" shall be deemed to refer collectively to all injury, damage, loss or expense incurred.

B. **Exclusive Remedies**. Cellebrite's entire liability and Buyer's exclusive remedies against Cellebrite for any damages caused by any Software defect or failure, or arising from the performance or non-performance of any obligation hereunder, regardless of the form of action, whether in contract, tort including negligence, strict liability or otherwise shall be:

i. For bodily injury or death to any person proximately caused by Cellebrite, Buyer's direct damages; and

ii. For claims other than as set forth above, Cellebrite's liability shall be limited to direct damages that are proven, in an amount not to exceed the total amount paid by Buyer to Cellebrite during the twelve (12) month period that immediately preceded the event that gave rise to the applicable claim.

C. **Limitation of Liability**. Notwithstanding any other provision of this EULA, CELLEBRITE shall NOT be liable for incidental, indirect, special, exemplary or consequential damages, including but not limited to lost profits, savings or revenues of any kind, whether or not CELLEBRITE has been advised of the possibility of such damages. This provision shall APPLY EVEN IN THE EVENT OF THE failure of an exclusive remedy.

D. **No Liability to any Third Party**. TO THE MAXIMUM PERMITTED EXTENT, CELLEBRITE DISCLAIMS ANY AND ALL LIABILITIES OR OBLIGATIONS WHATSOEVER RELATED TO THE SOFTWARE OR ITS LICENSING TO OR USE BY ANYONE OTHER THAN BUYER.

9) **BUYER INDEMNITY** – Buyer will, at its expense: (i) indemnify and hold Cellebrite and its affiliates, officers and directors harmless from any claim (whether brought by a Third Party or an employee, consultant or agent of Buyer's) alleging that any Product or Software furnished under this Agreement was used in a manner other than as authorized under this EULA, including but not limited to using the Product or Software in a manner that violates a person's fourth amendment rights under the United States Constitution (or its equivalent in the Territory) or misappropriating a person's list of contacts or other personal information; (ii) reimburse Cellebrite for any expenses, costs and liabilities (including reasonable attorney fees) incurred relating to such claim; and (iii) pay all settlements, damages and costs assessed against Cellebrite and attributable to such claim.

10) **DISABLING CODE**

A. **Disabling Code**. Software may be provided to Buyer with disabling code that allows Cellebrite to disable such Software or the Products such Software is embedded in. Any Updates or Upgrades to the Software may include disabling code. Cellebrite agrees not to invoke such disabling code except as provided for in Section 7.B, without Buyer's prior consent, which may be given by telephone or email.

B. **Invocation of Disabling Code**. In addition to the invocation of disabling code when Cellebrite has received Buyer's consent described in Section 7.A, Cellebrite may, at its option, invoke disabling code in Cellebrite's Software without receiving Buyer's consent (i) if in Cellebrite's sole, reasonable discretion, Cellebrite believes that such Software has been, is being or will be used in violation of laws; (ii) if Cellebrite is required to do so, because of a court or regulatory order; (iii) if Buyer has not paid an outstanding invoice more than sixty (60) days after such invoice is due; or (iv) if Buyer has used the Software other than as authorized by Buyer's license. Cellebrite shall have no liability to Buyer for any good faith invocation of any such disabling code.

11)TERM AND TERMINATION

A. **Term**. The term of this EULA is while any Software is under Buyer's control or possession. Notwithstanding the foregoing, (i) the license to any Embedded Software may be terminated if Buyer has not paid an invoice sixty (60) days after such invoice is due; and (ii) the license to any Standalone Software is only during the License Term. The License Term shall be determined in a separate agreement between Cellebrite and the Buyer.

B. **Termination**. Cellebrite shall have the right to terminate this EULA upon thirty (30) days prior written notice to the other party if such other party has not cured any material breach of this EULA by the end of such thirty (30) day notice period. Upon termination of this EULA for any reason, (i) Buyer shall be responsible for payment for all purchase orders delivered to Buyer by Cellebrite before the effective date of termination; and (ii) Buyer shall destroy all copies of the Standalone Software under Buyer's control or possession.

C. **Survival.** The provisions of Sections 1, 2.C, 2.E, 2.F, 2.G, 3, 4, 5, 6, 7, 8.C, and 9-13 of this EULA shall survive any termination in accordance with their terms. In addition, any purchase order accepted by Cellebrite prior to the effective date of termination shall survive in accordance with its terms.

12)**CHOICE OF LAW; JURISDICTION** – The construction, interpretation, and performance of the Agreement and all transactions under it shall be governed by the laws of the State in which the Cellebrite entity engaged by Buyer is incorporated (the "Governing State"), excluding its choice of law rules and excluding the Convention for the International Sale of Goods. Buyer acknowledges that the courts of the Governing State shall have exclusive jurisdiction with respect to any dispute arising under this Agreement, which is initiated against Cellebrite by Buyer or any Third Party on its behalf. Notwithstanding the above: (i) to the extent Cellebrite Mobile Synchronization Ltd. has engaged Buyer, the courts of Tel-Aviv shall have exclusive jurisdiction with respect to any dispute arising under this Agreement, which is initiated against Cellebrite by Buyer or any Third Party on its behalf; and (ii) to the extent Cellebrite USA Inc. has engaged Buyer, the courts of the State of New York shall have exclusive jurisdiction with respect to any dispute arising under this Agreement, which is initiated against Cellebrite by Buyer or any Third Party on its behalf. For the avoidance of any doubt, Buyer further acknowledges and agrees that Cellebrite shall be allowed, at its sole and absolute discretion, to initiate any dispute against Buyer in any jurisdiction worldwide (whether in or outside the Governing State), including with respect to any application for injunctive remedies (or an equivalent type of urgent legal relief).

13) **ASSIGNMENT** – Neither party may assign its rights and obligations hereunder without the prior written consent of the other party. Notwithstanding the foregoing, either party may assign this EULA to any Affiliate of the other or to an acquirer (by purchase, merger or otherwise) of all or substantially all of such party’s business or assets relating to this EULA, provided that (i) the

assignee agrees in writing to be bound by the terms and conditions of this EULA, (ii) neither the assignor nor assignee are in default hereunder. Any attempted assignment other than as permitted shall be null and void.

14) **NON-WAIVER** – No course of dealing or failure of either party to strictly enforce any term, right or condition of this Agreement shall be construed as a waiver of such term, right or condition.

15) **ENTIRE AGREEMENT** – The terms and conditions contained in this Agreement supersede all prior oral or written understandings between the parties and shall constitute the entire agreement between the parties with respect to the subject matter of this Agreement, except as provided for in the preamble to this Agreement regarding the order of precedence. This Agreement shall not be modified or amended except by a writing signed by Buyer and Cellebrite.

16) **CONSTRUCTION; SEVERABILITY** – The headings used in this Agreement are for reference purposes only and will not be deemed to limit, expand or in any way affect the interpretation of any term or provision hereof. If any provision or part hereof shall be held to be invalid or unenforceable for any reason, then the meaning of such provision or part hereof shall be construed so as to render it enforceable to the extent feasible. If no feasible interpretation would save such provision or part hereof, it shall be severed herefrom, but without in any way affecting the remainder of such provision or any other provision contained herein, all of which shall continue in full force and effect unless such severance effects such a material change as to render the Agreement unreasonable. In case of any inconsistency between this Agreement and any other agreement, document and/or instrument entered into by Buyer and Cellebrite, the terms of this Agreement shall prevail.

17) **WARRANTY**

A. **Hardware Warranty**. Cellebrite warrants that each Product, including all firmware and excluding Software (for which the warranty is only as provided under Section D below), but not related services or prototypes of any such Product, shall be materially in conformance with the written specification furnished or agreed to by Cellebrite for twelve (12) months after acceptance (the "**Warranty Period**"). If any failure to materially conform to such specification ("**Defect**") is suspected in any Product during the Warranty Period, Buyer, after obtaining return authorization information from Cellebrite, shall ship suspected defective samples of the Product to Cellebrite in accordance with Cellebrite's instructions. No Product will be accepted for repair, replacement, credit or refund without the written authorization of Cellebrite. Cellebrite shall analyze the failures, making use, when appropriate, of technical information provided by Buyer relating to the circumstances surrounding the failures. Cellebrite will verify whether any Defect appears in the Product. If a returned Product does not have a Defect, Buyer shall pay Cellebrite all costs of handling, inspection, repairs and transportation at Cellebrite's then-prevailing rates. If a returned Product has a Defect, Cellebrite shall, at Buyer's option, either repair or replace the defective Product with the same or equivalent Product without charge or, if such repair or replacement has not occurred by the thirtieth (30th) day following Cellebrite's receipt of the returned Product, credit or refund (at Buyer's option) the purchase price within ten (10) days after such thirtieth (30th) day; provided: (i) Buyer notifies Cellebrite in writing of the claimed Defect within thirty (30) days after Buyer knows or reasonably should know of the claimed Defect, (ii) the claimed Defect actually exists, and (iii) the Defect appears within the Warranty Period. Cellebrite shall ship any replacement Product FCA Cellebrite's premises (Incoterms 2010), freight prepaid to Buyer's destination. Any replaced Product or replaced parts of any Product shall become Cellebrite's property. In no event shall Cellebrite be responsible for de-installation or reinstallation of any Product or for the expenses thereof. Repairs and replacements covered by the above warranty are warranted to be free from Defects as set forth above with respect to any Defect that appears (i) within six (6) months from the date of repair or replacement or (ii) prior to the expiration of the original Warranty Period, whichever is later.

B. **Touch Screen Exclusion**. Notwithstanding Section A, the Warranty Period for the touch screen of any Product with a touch screen is the period from the date of Buyer's initial receipt of the Product until thirty (30) days after such date, and Cellebrite warrants such touch screen only to the extent any damage to it was not caused by Buyer's negligence or willful misconduct.

C. **Warranty of Title**. Cellebrite warrants that any title conveyed hereunder (excluding Software) shall be good and its transfer rightful, and that the Products delivered under this EULA shall be free from all liens, encumbrances and restrictions. Cellebrite further warrants that it has all rights and powers necessary to perform its obligations under this EULA and that to its knowledge, it has the right to grant the licenses and other rights provided to Buyer by this EULA.

D. **Software Warranty**. Cellebrite warrants to Buyer that for a period of sixty (60) days after the date of shipment, the Software will perform substantially in conformity with its Documentation. As Buyer's sole and exclusive remedy, Cellebrite will, at its sole expense, in its sole discretion and as its sole obligation, promptly repair or replace any Software that fails to meet this limited warranty.

E. **Exclusions**. Notwithstanding anything to the contrary in this warranty, the warranties herein do not apply to, and Cellebrite makes no warranties with respect to defects in Products or Software in the following cases: (a) Buyer's misuse, damage, or unauthorized modification of the Products or Software; (b) Buyer's combination of the Products or Software with other products or software, other than as authorized in writing by Cellebrite; (c) placement of the Products or Software in an operating environment contrary to specific written instructions and training materials provided by Cellebrite to Buyer; (d) Buyer's intentional or negligent actions or omissions, including physical damage, fire, loss or theft of a Product; (e) cosmetic damage to the outside of a Product, including ordinary wear and tear, cracks or scratches; (f) for any Product with a touch screen, any defect in such a touch screen after thirty (30) days from the date of receipt of such Product, or any defect caused in a touch screen by Buyer's negligence or willful misconduct; (g) maintenance of the Products or Software in a manner that is contrary to specific written instructions provided by Cellebrite to Buyer; (h) a product or service not provided, authorized or approved by Cellebrite for use with the Products or Software; (i) any repair services not authorized or approved by Cellebrite; (j) any design, documentation, materials, test data or diagnostics supplied by Buyer that have not been authorized or approved by Cellebrite; (k) usage of any test units, experimental products, prototypes or units from risk lots (each of which is provided "AS IS"); (l) any third party original equipment manufacturer's restrictions on individual phones or models of phones that prevent the phones or models of phones from working with the Products or Software; (m) any damage to a third party device alleged to or actually caused by or as a result of use of a Product or Software with a device; (n) any Products that have had their serial numbers or month and year of manufacture or shipment removed, defected or altered; (o) any interactions or other effects relating to or arising out of the installation of copies of the Software beyond the number of copies authorized by an agreement between Cellebrite and Buyer; (p) use of Products or Software incorporated into a system, other than as authorized by Cellebrite; or (q) any Products or Software that has been resold or otherwise transferred to a third party by Buyer (any Product or Software affected by the cases in (a)-(q) is referred to hereinafter as an "**Excluded Item**").

F. It is expressly clarified that (i) the operation of the Software and/or Product will not be error-free; (ii) not all defects in the Software and/or Product will be corrected; (iii) the Software may not operate on hardware or operating systems or in conjunction with other software other than as expressly specified in the Documentation or approved by Cellebrite in writing.

G. **Warranty Limitations**. EXCEPT AS STATED IN THIS WARRANTY, CELLEBRITE, ITS SUBSIDIARIES AND AFFILIATES, SUBCONTRACTORS AND SUPPLIERS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AND SPECIFICALLY DISCLAIM ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. BUYER'S SOLE AND EXCLUSIVE REMEDY FOR FAILURE OF AN ITEM TO CONFORM WITH ITS SPECIFICATIONS SHALL BE SELLER'S OBLIGATION (i) TO REPAIR OR (ii) TO REPLACE OR, (iii) IF NEITHER (i) NOR (ii) IS COMMERCIALLY FEASIBLE, TO CREDIT OR REFUND (AT BUYER'S OPTION) SUCH ITEM AS SET FORTH ABOVE. THIS DISCLAIMER AND EXCLUSION SHALL APPLY EVEN IF THE EXPRESS WARRANTY FAILS OF ITS ESSENTIAL PURPOSE. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE AND PRODUCT REMAINS WITH BUYER.

H. **Repaired or Replaced Products**. Before returning a Product for service, Cellebrite recommends that Buyer back up any data contained in such a Product. IN NO EVENT WILL CELLEBRITE, ITS AFFILIATES OR SUPPLIERS BE LIABLE TO BUYER OR ANY THIRD PARTY FOR ANY DAMAGES OF ANY KIND WHATSOEVER RELATING TO OR ARISING OUT OF DAMAGE TO, OR LOSS OR CORRUPTION OF, ANY RECORDS, PROGRAMS OR OTHER DATA RESULTING FROM CELLEBRITE'S REPAIR OR REPLACEMENT SERVICES UNDER THIS WARRANTY, OR AS A RESULT OF A FAILURE OR MALFUNCTION OF A PRODUCT.

A

Activate TomTom Trip log • 159, 168

Activating the license • 28, 29, 191

Android backup • 90

Android Debugging Bridge method • 211, 212

Android extraction methods • 211

Appendix • 221

Application taskbar • 51

B

Bluetooth Scan • 159, 161

Bootloader extraction • 211, 215

C

Capture • 14

Capture images • 50

Capture images and screenshots • 109

Capture s • 50

Cellebrite YouTube channel • 21

Changing the application interface language • 173, 177

Changing the extraction location • 173, 182

Clone SIM • 14, 50, 137

Cloning an existing SIM card ID • 138

Connect mobile device • 55

Cover Page • 1

Creating GSM test SIM • 154

D

Detect automatically • 43

Device power-up cable • 205

Device tools • 15, 50, 159

Disabling the password • 76

E

Entering SIM data manually • 145

Exit Odin Mode • 159, 169

Extracting Android devices • 211

Extraction in Progress • 61

F

File system extraction • 14, 50, 81

G

General settings • 172

Getting started • 23

H

Home screen • 40

I

Image capture • 14, 109

Installing UFED 4PC • 23

Introduction • 9

L

Legal notices • 3

License settings • 191

Locked HTC, Huawei, and ZTE devices • 217

Locked Motorola devices • 216

Logical extraction • 13, 50, 53

M

Managing report fields • 185, 186

Managing the Custom List • 173

Mobile Extraction Client • 173, 181

O

Opening UFED 4PC • 40

Other locked devices • 218

Overview • 9

P

Password extraction • 14, 29, 50, 69

Performing a file system extraction • 81

Performing a physical extraction • 97

Performing File System extraction for an Android device • 216

Performing logical extraction • 54

Performing password extraction • 69

Performing SIM data extraction • 126

Permission management • 197

Physical extraction • 14, 50, 97

R

Regulatory compliance • 209

Report settings • 183

S

screenshots • 14, 109

Search function • 46, 48

Select Content Types • 57

Select phone memory • 56

Settings • 171

SIM Card Functionality • 126

SIM data extraction • 14, 50, 126

Special cables • 205

Supported devices • 21

Switch to CDMA Offline Mode • 159, 164

System Requirements • 11

System settings • 189

T

Technical terms • 220

Test Peek/Poke functionality • 159, 166

The Extracted Data Folder • 67

The extracted passwords folder • 75

The extracted SIM data folder • 137

The file system extraction folder • 88

The Physical Extraction folder • 107

U

UFED 4PC accessories • 16

UFED 4PC extraction types and device tools • 12

UFED Device Adapter • 17

Uninstall Android Client • 159, 169

Uninstall Windows Mobile Client • 159, 168

Unlocked devices • 217, 218, 219

Updates and versions • 194

USB Cable for UFED Device Adapter PowerUP • 207

USB Extension cable for UFED Device Adapter • 207

User permissions • 195

Using cables and tips • 18

V

Version details • 193

W

Working with UFED 4PC • 40