UFED

Performing extractions

July 2019 | Version 7.20

Cellebrite Digital intelligence for a safer world

Legal notices

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

- This document contains proprietary information belonging to Cellebrite Mobile Synchronization Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the UFED.
- No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite 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.

Contents

1. Overview

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

UFED enables you to:

- Perform physical, file system, and logical extraction of device data and passwords. Capabilities may vary, based on the UFED product purchased - UFED Logical or UFED 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.

1.1. System requirements

PC	Windows compatible PC with Intel i5 or compatible running at 1.9 GHz or higher	
Operating system	Microsoft Windows 10, 64-bit Microsoft Windows 8.x, 64-bit Microsoft Windows 7, 64-bit Microsoft Windows 7 Boot Camp on MAC	
Memory (RAM)	**Recommended** 16 GB	**Minimum** 4 GB
Space requirements	1.5 GB of free disk space for installation	
Additional requirements	Microsoft .Net version 4.5 or later	
Permissions	If you intend to activate the application using a hardware license key (dongle) provided by Cellebrite, you must have administrative rights over the computer.	

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

1.2. Extraction types

UFED includes a range of data extraction types.

> The available extractions may vary, based on the type of product purchased; the UFED Logical or the UFED Ultimate product.

Table 1-1: Functionalities of the UFED products

Functionality	UFED Logical	UFED 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:** Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.
- **SIM card extraction:** Extracts data from a SIM or USIM card.
- **File system extraction:** Extracts files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.
- **Password extractions:** Unlocks and displays passwords from a source mobile device.
- **Clone SIM:** Copies a SIM ID from one SIM card to another SIM card or to a UFED SIM ID Access Card.
- **Physical extraction:** Extracts a physical bit-for-bit image of the flash memory of a device, including the unallocated space using advanced methods. Unallocated space is the area of the flash memory that is no longer tracked by the file system, which may contain images, videos, files, and more.
- **Capture images and screenshots:** Take pictures or videos of a device using the UFED camera. You can also capture internal screenshots directly from the connected device.

1.3. Accessories

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

Figure: UFED Cables and tips

The UFED 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.

1.3.1. UFED Device Adapter with USB 3.0

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

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

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

This device adapter has the following connectors:

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

For information on the specifications, refer to the *Overview Guide*.

To connect the UFED Device Adapter with USB 3.0:

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

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

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

1. Connect the Active Extension cable[1] to the DATA connection cable. Refer to the *Overview Guide*.
2. Connect the other end of this extension cable to a USB port on the PC.
3. Connect a standard USB extension cable to the POWER connection cable.
4. Connect the other end of this extension cable to a USB port on the PC.

1.3.1.0.1. Using the External power supply

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

1.3.2. Multi SIM Adapter

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

> It is recommended to connect the Multi SIM Adapter to an available USB port on your computer, not to the USB port on the UFED Device Adapter.

For information on the specifications, refer to the *Overview Guide*.

[1]This cable is 150 cm in length and allows for the easy and accessible placement of the UFED Device Adapter with USB 3.0.

1.3.3. Using cables and tips

The cables and tips include 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: Single cable

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

Figure: UFED tip (example)

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

1.4. Supported devices

To find out which mobile devices are supported in UFED 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. UFED Supported Devices document in MyCellebrite.

1.5. Cellebrite YouTube channel

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

2. Logical extraction

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

A logical extraction can also be used to extract data from many Android, BlackBerry, iOS, and Windows Phone apps. For an updated list of supported apps and versions for each platform go to **Help** > **Supported Apps** in 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).

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

Logical extraction includes the following:

Advanced logical Android extraction (on the next page)

Advanced logical iOS extraction (on page 24)

Logical (Partial) (on page 28)

Logical extraction via Bluetooth (on page 31)

2.1. Advanced logical Android extraction

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

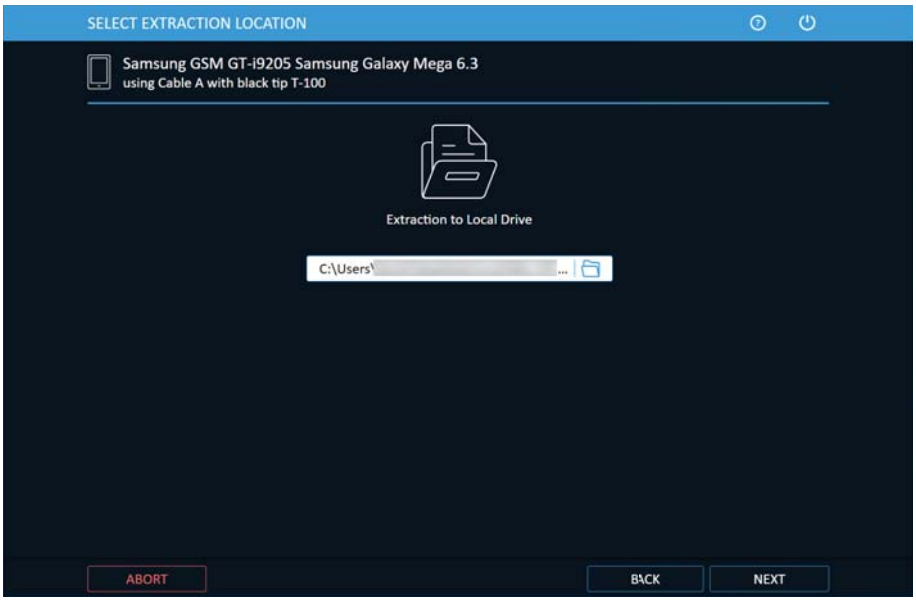
> For more information on the extraction types that are available, see the Performing extractions data sheet.

To perform an Advanced logical extraction from a mobile device:

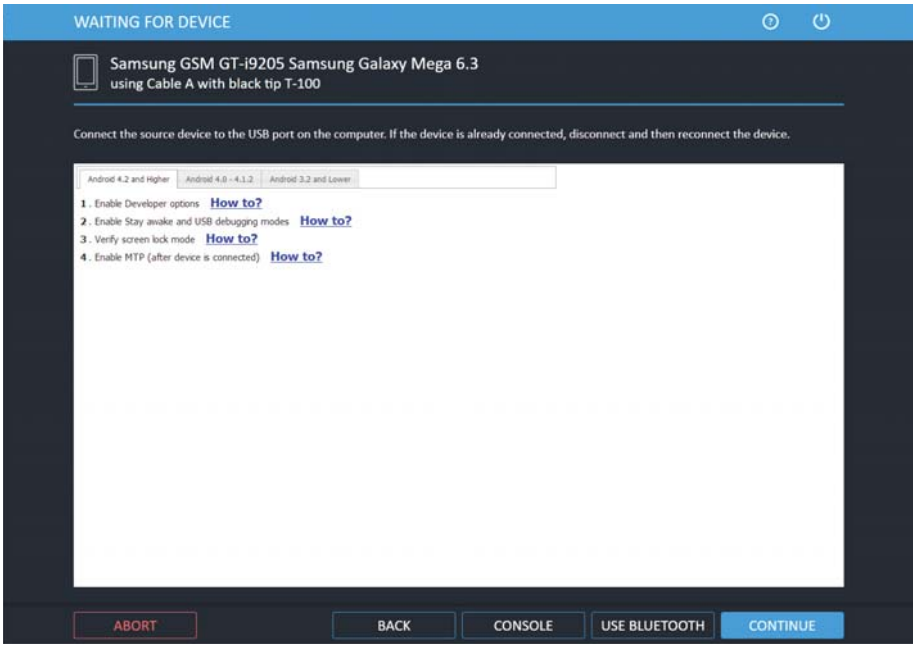
1. Click **Mobile device** and identify the device, then click **Advanced Logical**.

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

   The Select Extraction Location window appears.

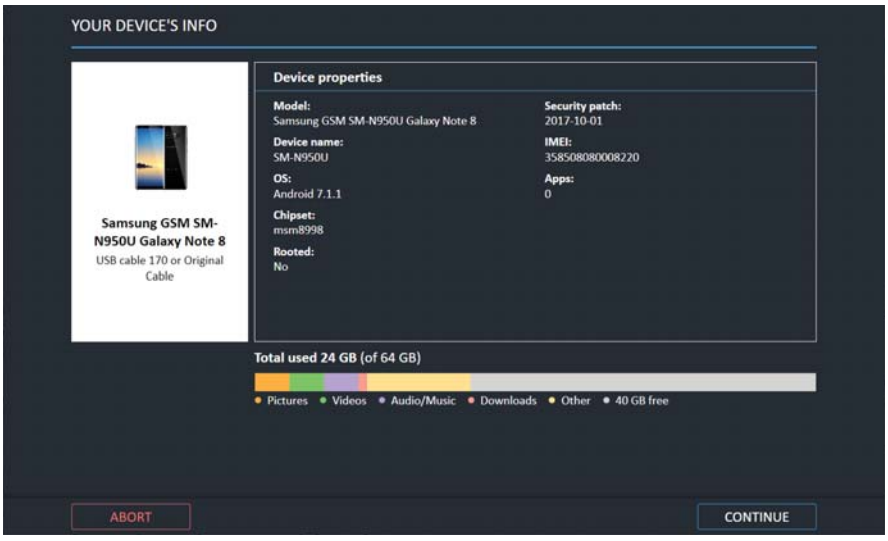


2. Use the current location or click the folder icon to change the target path and select a different location and then click **Next**. The Waiting for Device window appears.



Click the **Console** button to access device information using the Android Debug Console. For more information, see AndroidDebugConsole.htm.

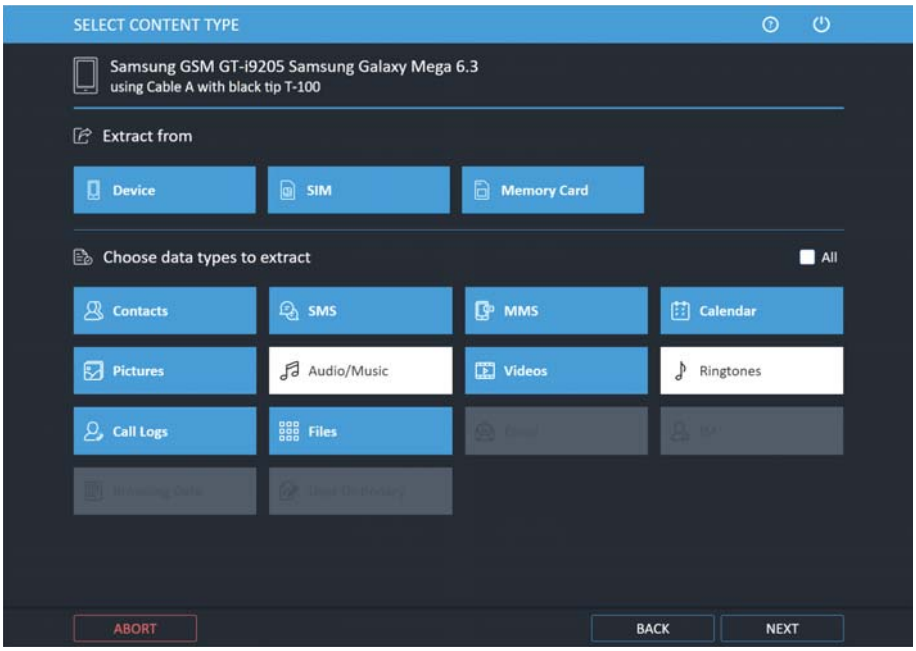
3. Select the correct cable and tip for the mobile device, and change the device settings according to the instructions.
4. Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
5. Click **Continue**. The following window appears if the Enable device preview info screen option is enabled under General settings.



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

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

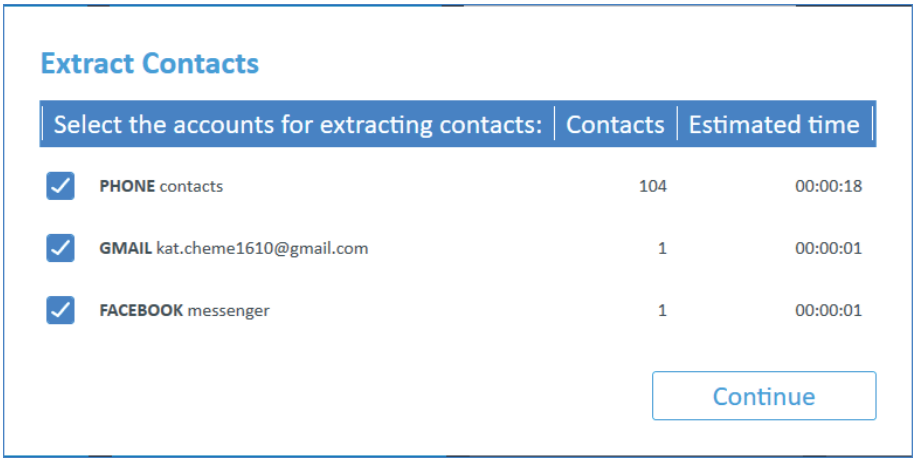
6. Click **Continue**. The following window appears.



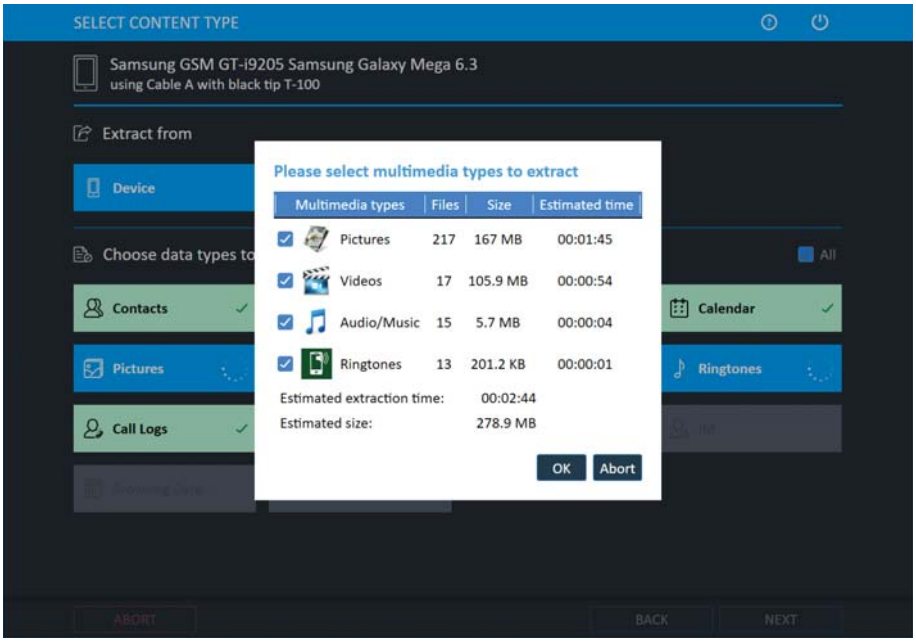
7. Data can be extracted from the Device, SIM and Memory Card of the device. Select from which memory you want to extract.
8. Different data types can be extracted. Select which data types you want to extract. In the example above, music and ringtones are excluded and will not be extracted.

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

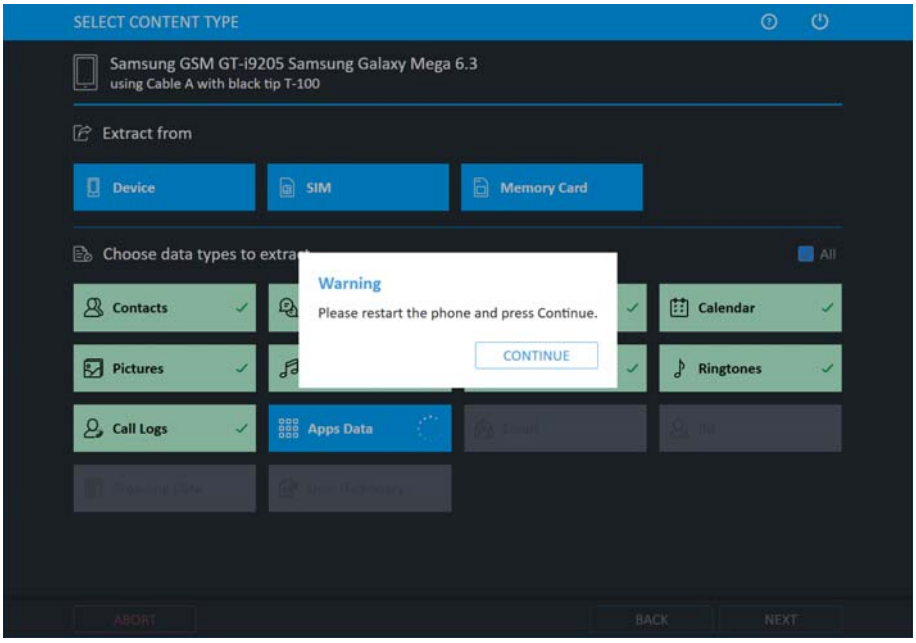
9. Click **Next**. The following window appears.



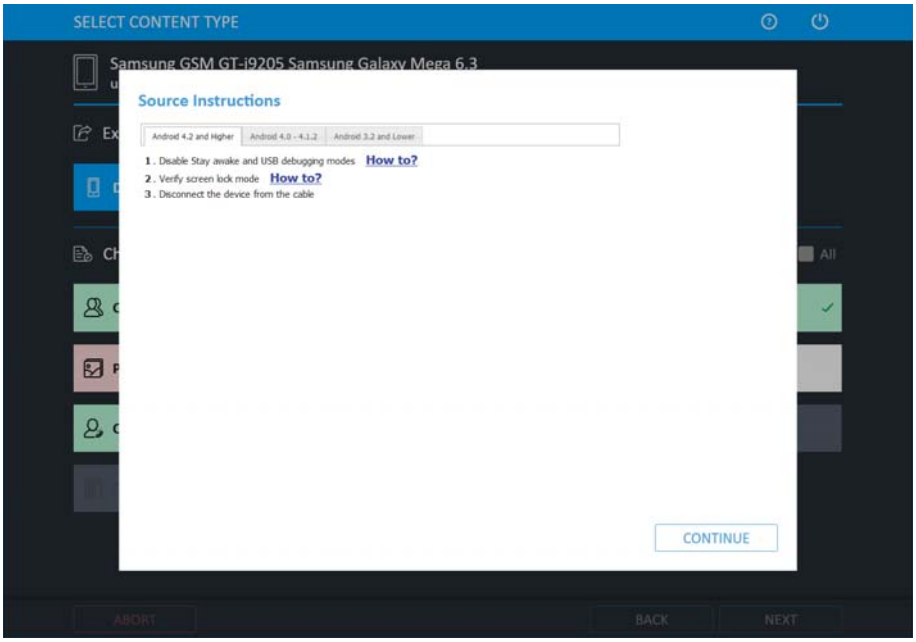
10. Select the required contacts to extract and click **Continue**. The extraction process starts.



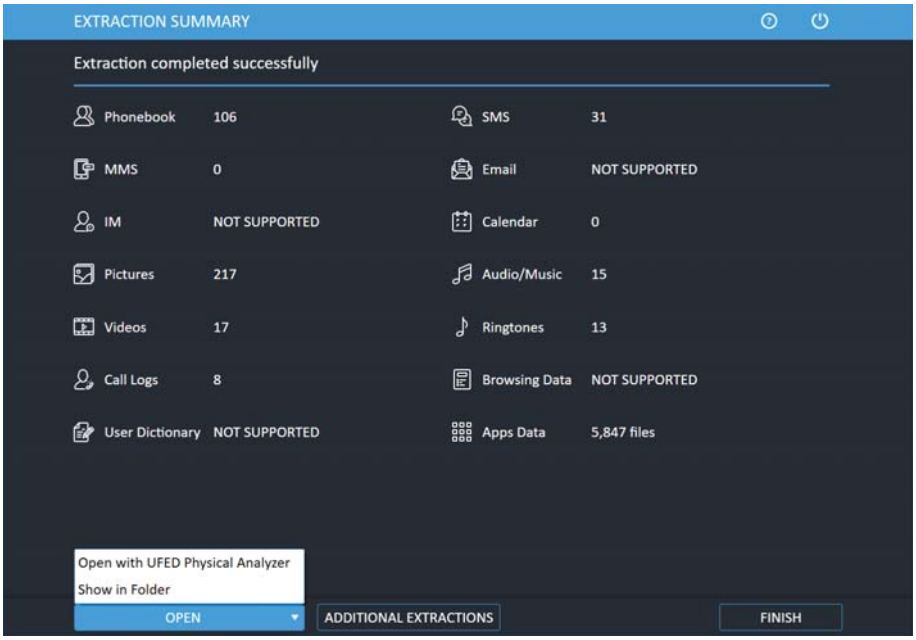
11. Click **OK**. The following window appears.



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

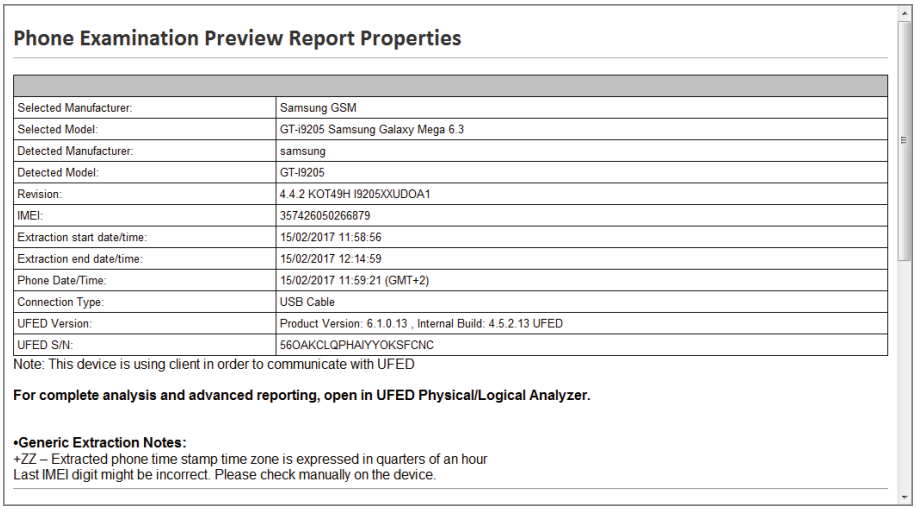


13. Follow the instructions to return the mobile device settings to the original settings, and then click **Continue**.



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

    An example of a preview report is shown next.



Phone Examination Preview Report Properties

Selected Manufacturer:	Samsung GSM
Selected Model:	GT-i9205 Samsung Galaxy Mega 6.3
Detected Manufacturer:	samsung
Detected Model:	GT-I9205
Revision:	4.4.2 KOT49H I9205XXUDOA1
IMEI:	357426050266879
Extraction start date/time:	15/02/2017 11:58:56
Extraction end date/time:	15/02/2017 12:14:59
Phone Date/Time:	15/02/2017 11:59:21 (GMT+2)
Connection Type:	USB Cable
UFED Version:	Product Version: 6.1.0.13 , Internal Build: 4.5.2.13 UFED
UFED S/N:	56OAKCLQPHAIYYOKSFCNC

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

For complete analysis and advanced reporting, open in UFED Physical/Logical Analyzer.

•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.

2.1.1. The extracted data folder

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

> The extracted data folder is named "UFED" with the selected device name, the IMEI/MEID 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.

> 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.

2.2. Advanced logical iOS extraction

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

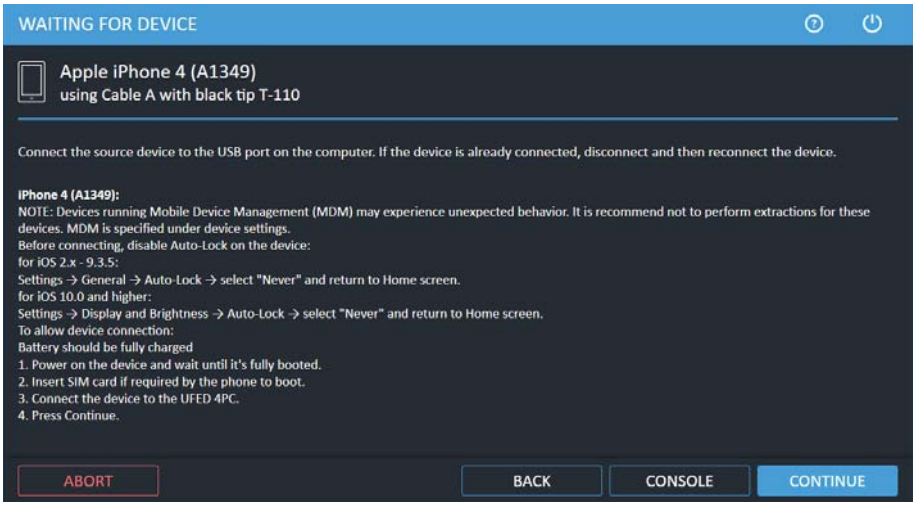
Advanced logical extractions can be used to extract data from Android or iOS operating systems. The following example shows an Advanced logical iOS extraction.

To perform an advanced logical iOS extraction:

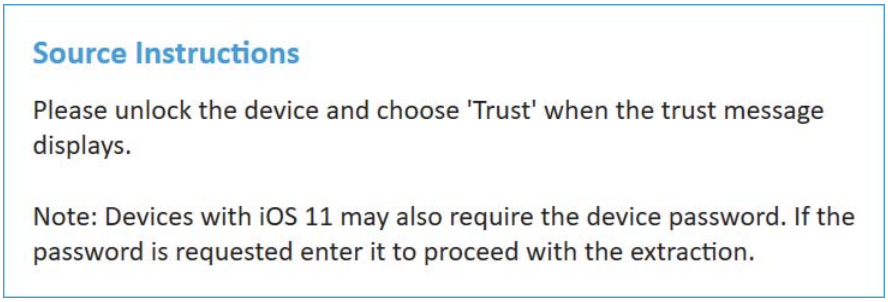
1. Click **Mobile device** and identify the device.
2. Click **Advanced Logical**.

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

   The following window appears.

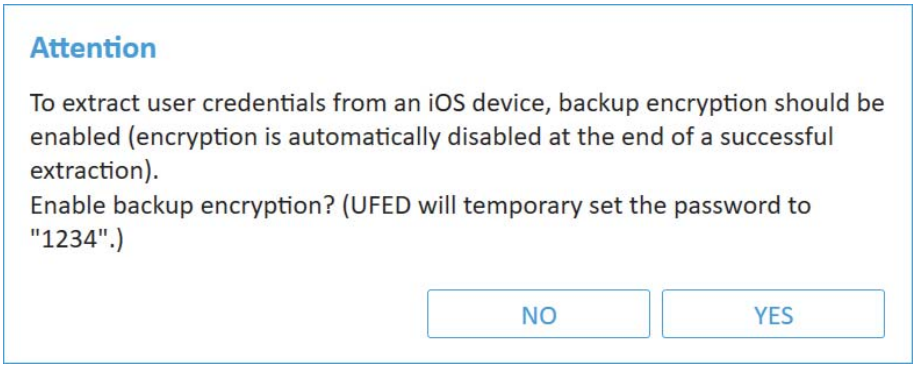


3. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device.
4. Click **Continue**. The following window appears.



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

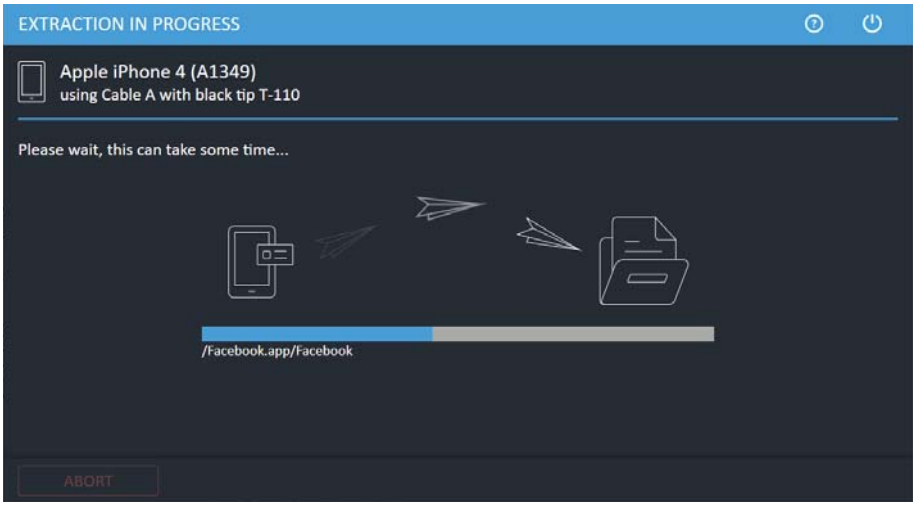
6. This window displays the device name, UDID, iOS version, and whether the backup is encrypted. Click OK. If the iTunes backup is not encrypted, the following message about data encryption appears. If the iTunes backup is encrypted, see Encrypted iTunes backup (on page 27).



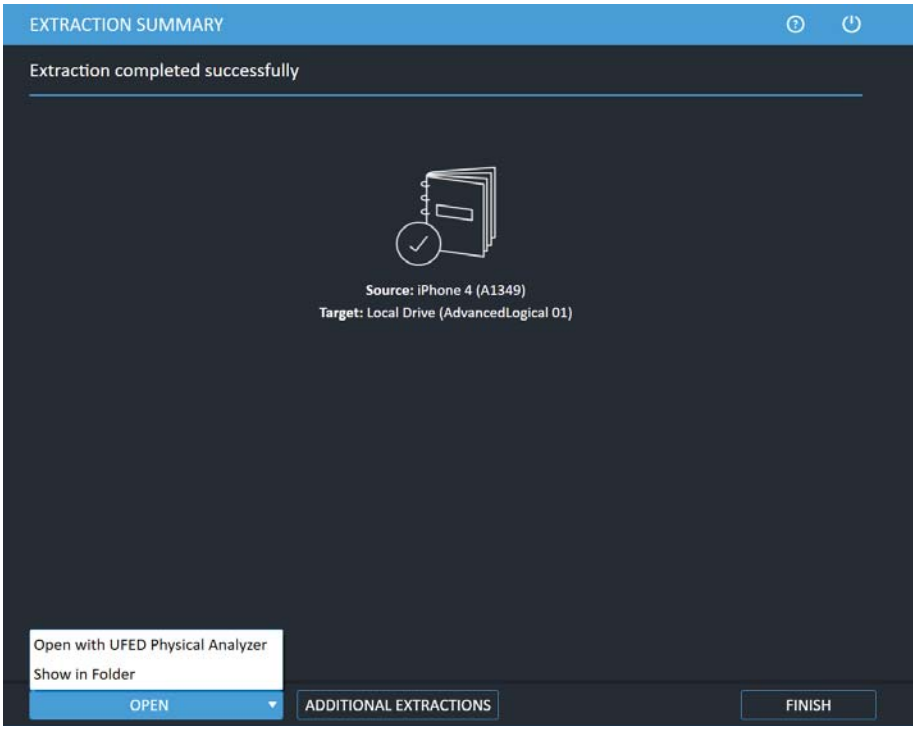
7. In the Attention window click **Yes** to enable backup encryption with the ability to extract additional information from the device, or click **No** if you do not require the additional information. The following window appears.

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

If the extraction was stopped and the device remains encrypted, see Disable iTunes encryption password (on page 136).



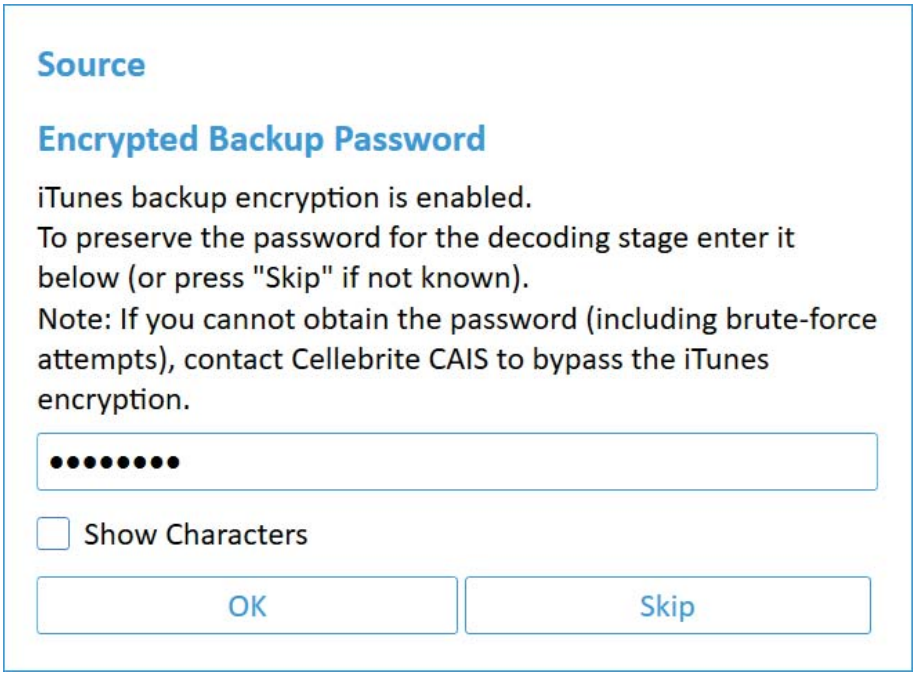
After the extraction completes, the Extraction completed window appears:



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

2.2.1. Encrypted iTunes backup

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



If you know the iTunes backup password:

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

If you do not know the iTunes backup password:

» Click Skip and follow the on-screen instructions to complete the extraction.

The password will be required during the decoding stage (in UFED Physical Analyzer).

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

2.3. Logical (Partial)

This is a quick extraction method that supports the largest number of devices. You can extract Call logs, Phone books, SMSs, Calendar events, Multimedia files, and file data. The available types of data may vary depending on the source device's make and model. In most cases, a logical extraction is not possible for locked devices.

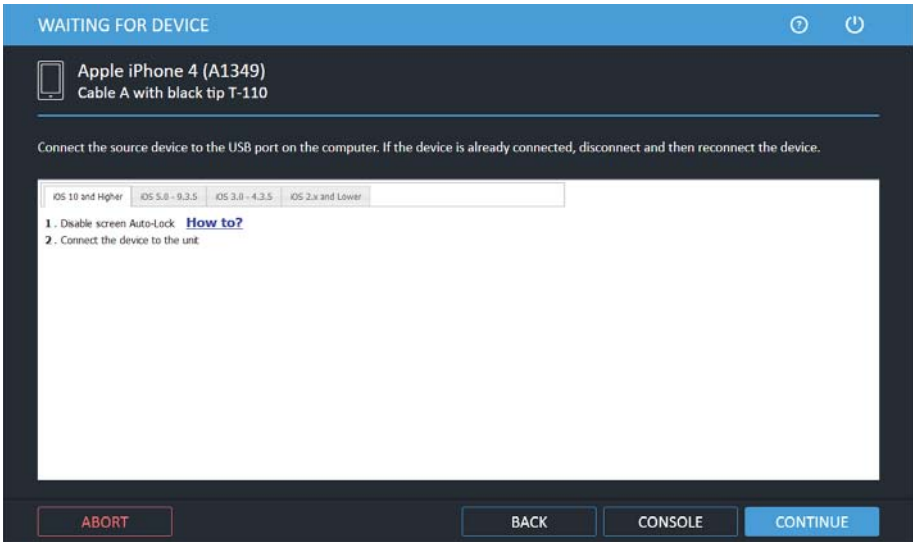
To perform Logical (Partial) extraction:

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

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

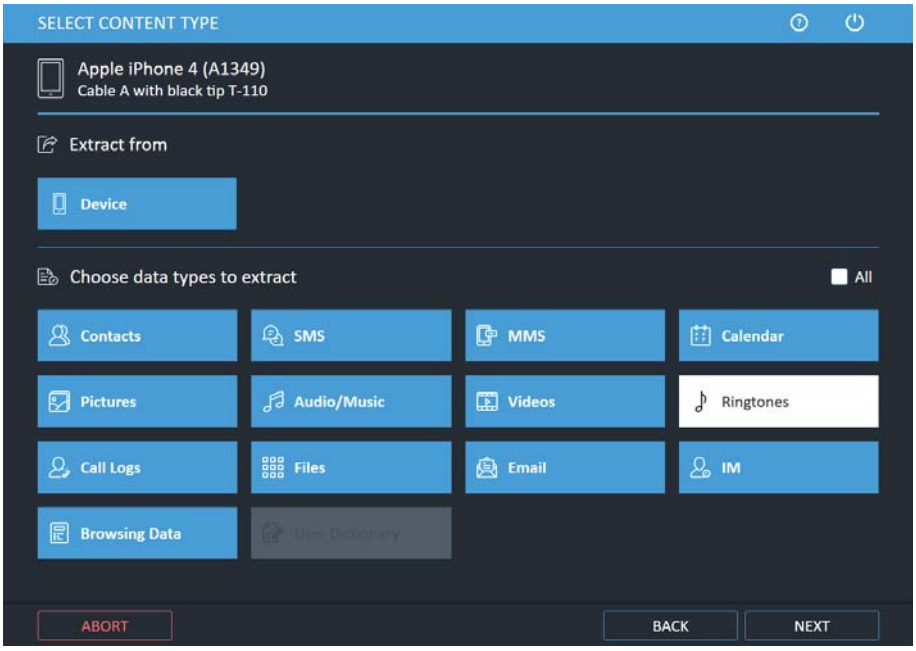
The Select Extraction Location window appears.

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



> The Console button is only supported on Android devices.

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



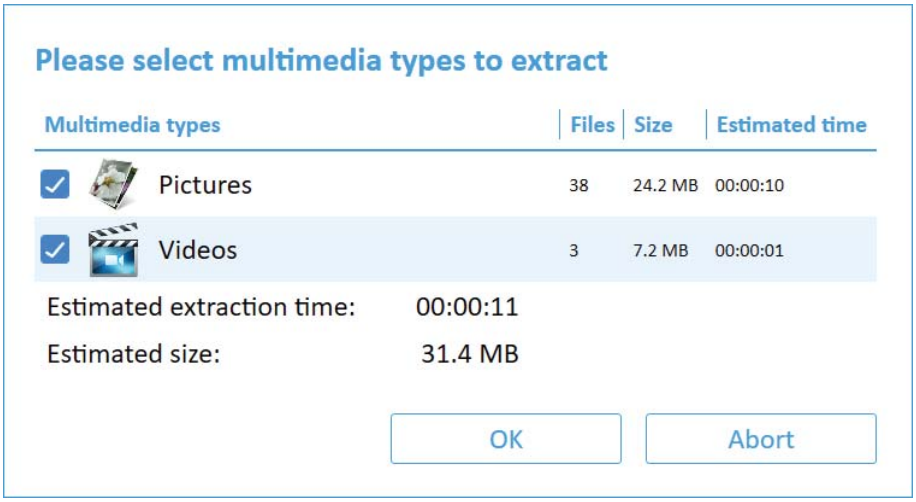
7. Different data types can be extracted. Select which data types you want to extract. In the example above Ringtones are excluded and will not be extracted.

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

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

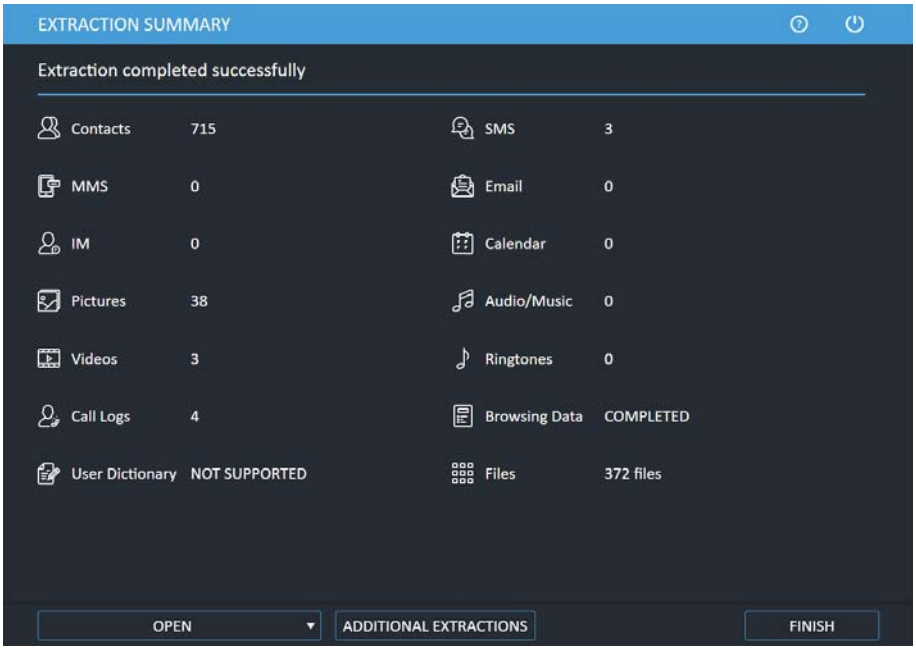
> **Source Instructions**
>
> Please unlock the device and choose 'Trust' when the trust message displays.
>
> Note: Devices with iOS 11 may also require the device password. If the password is requested enter it to proceed with the extraction.

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



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

    After the extraction completes, the Extraction completed window appears:



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

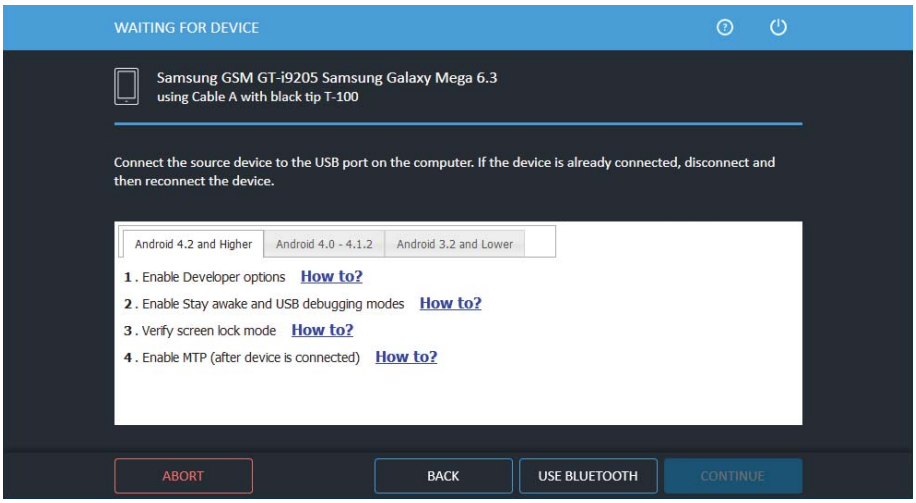
2.4. Logical extraction via Bluetooth

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

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

To perform a logical extraction via Bluetooth:

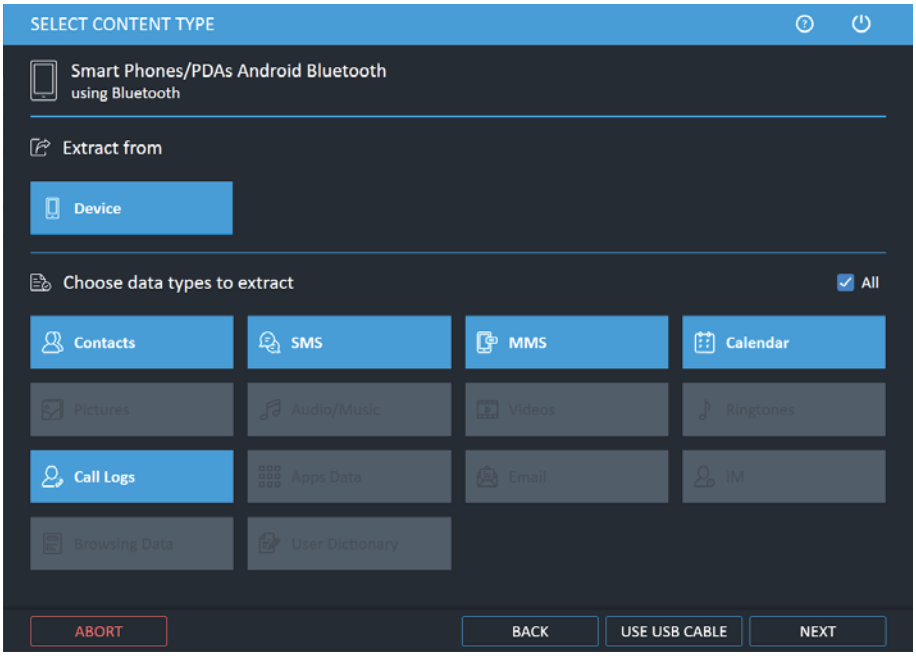
1. Click **Mobile device**, identify the device, select the extraction location, and then click **Logical**.
2. Select the extraction location. The following window appears.



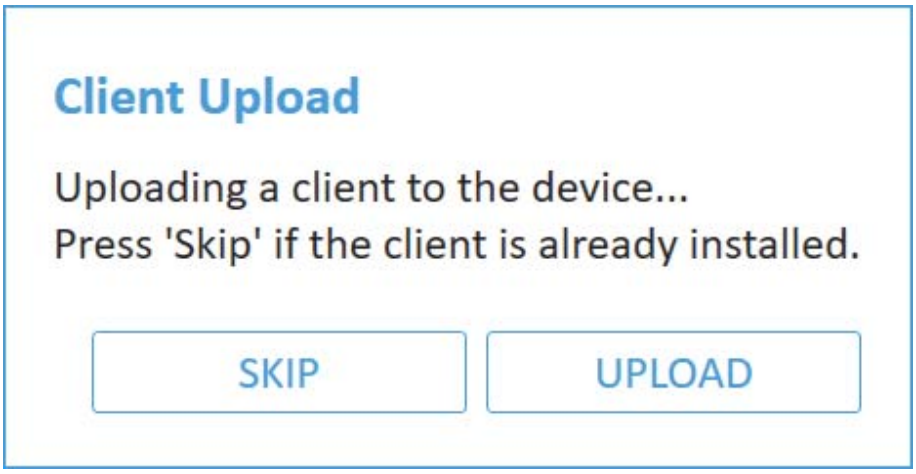
3. Click **Use Bluetooth**. The following window appears.

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

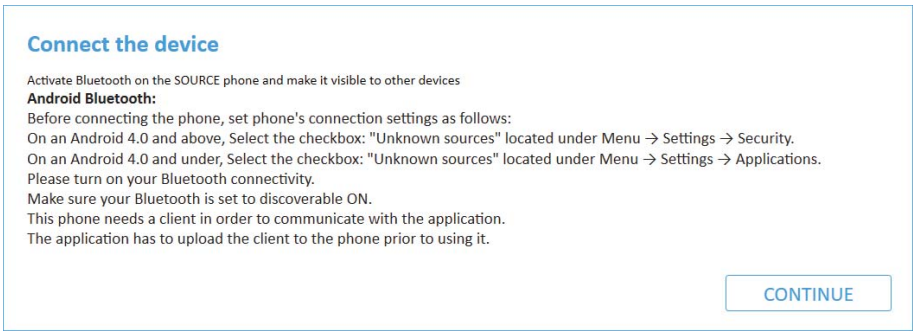
   The following window appears.



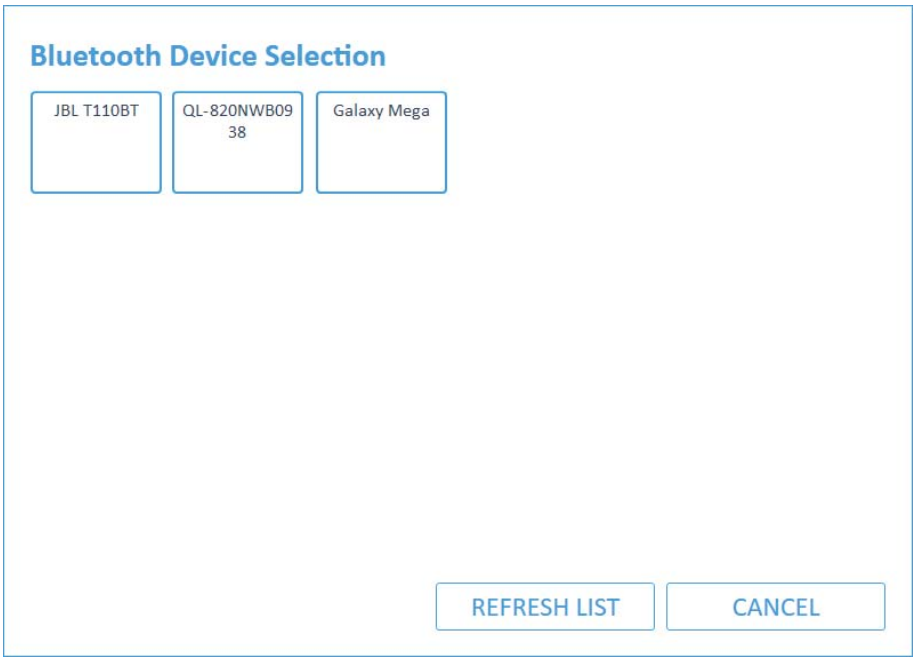
6. Select the required content types and then click **Next**.



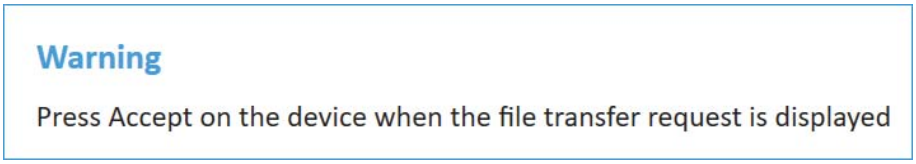
7. Click **Upload** to upload the client to the device or click **Skip** if you have already uploaded the client to the device. The following window appears.



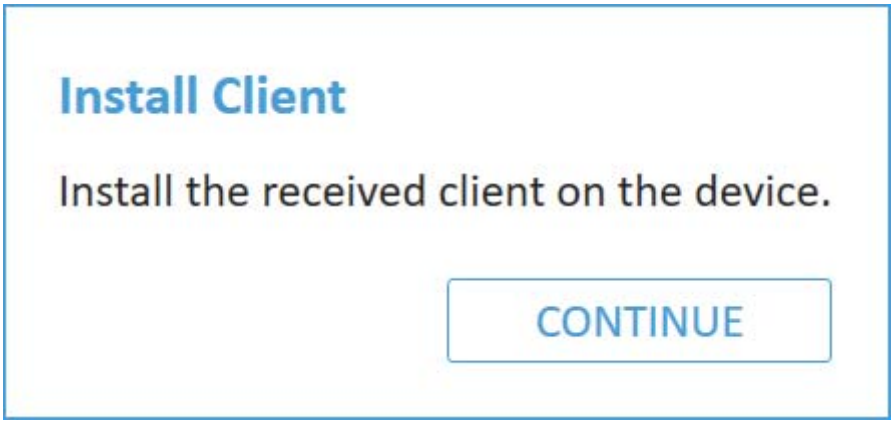
8. Activate Bluetooth on the source device and make it visible to other devices. Follow the on-screen instructions to set the devices connections, then click **Continue**. The following window appears.



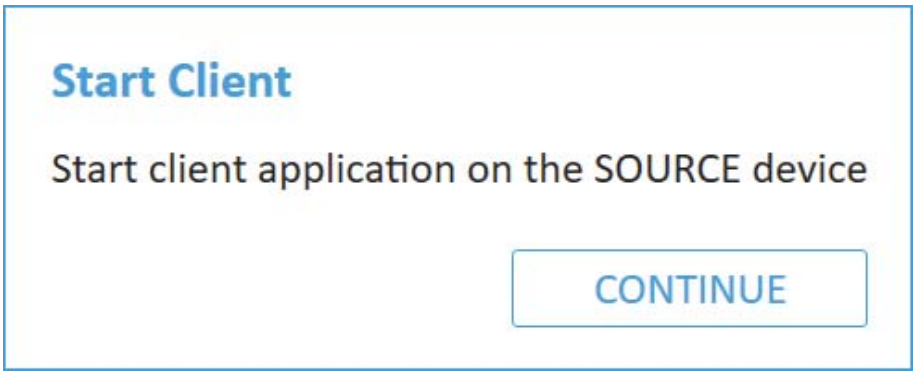
9. Click the required device. The following window appears.



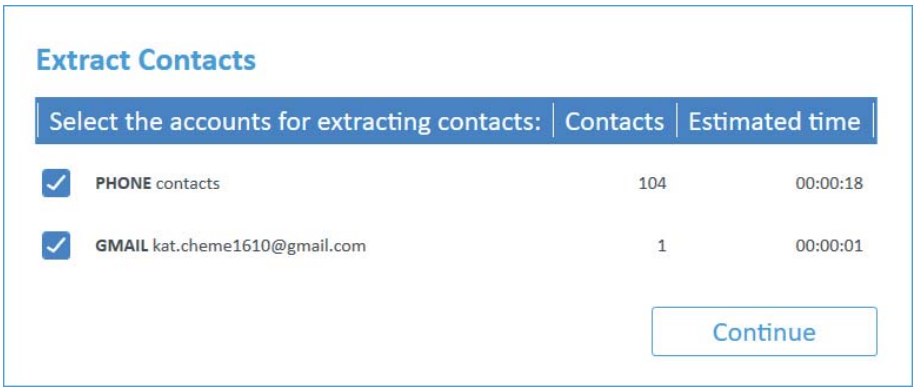
10. Press **Accept** on the device when the file transfer request is displayed (this is skipped if the client is already installed). The following window appears.



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



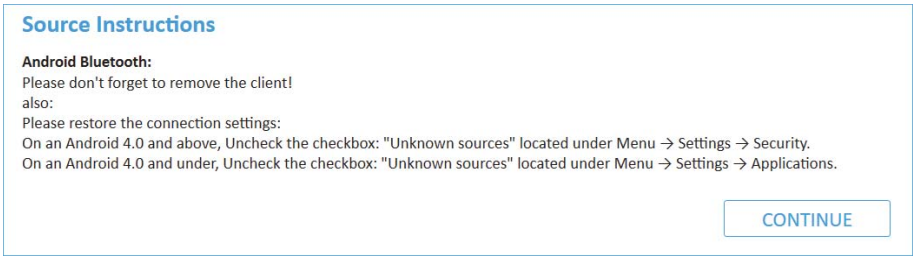
12. Open (or start) the client on the source device and confirm the Bluetooth permission request on the device.
13. Click **Continue**. The following window appears.



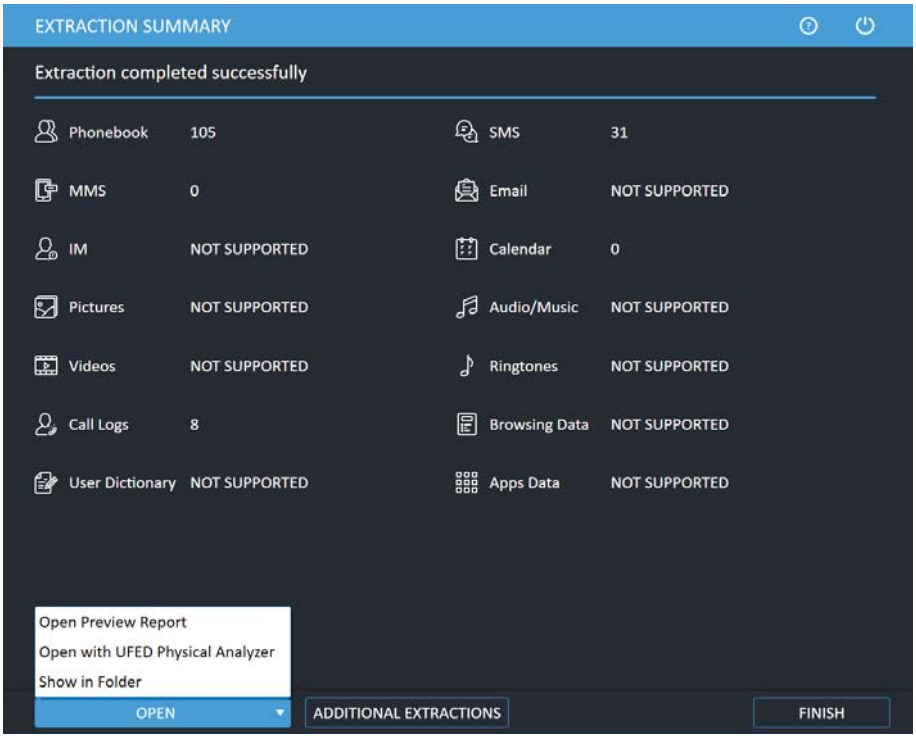
14. Click **Continue**.

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

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



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



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

3. Password extraction

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

Password extraction includes the following:

Extracting the user lock (below)

Disabling or re-enabling the user lock (on page 40)

Removing the screen lock (on page 42)

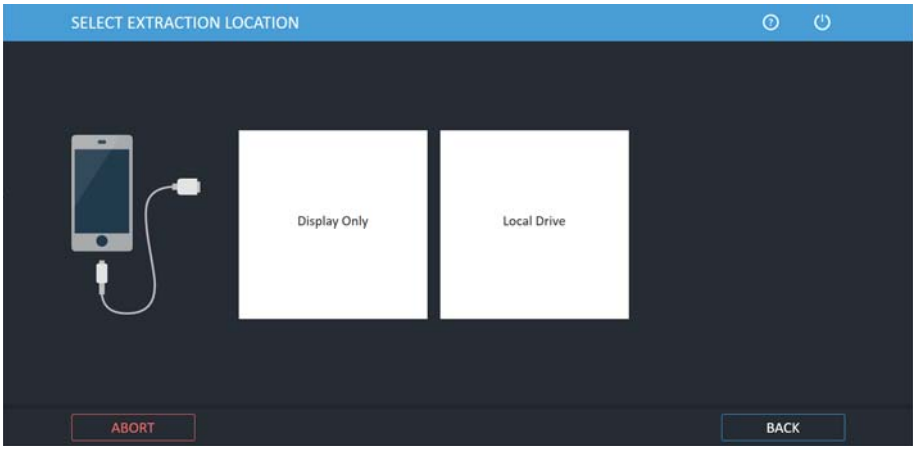
3.1. Extracting the user lock

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

To extract a user lock on a mobile device:

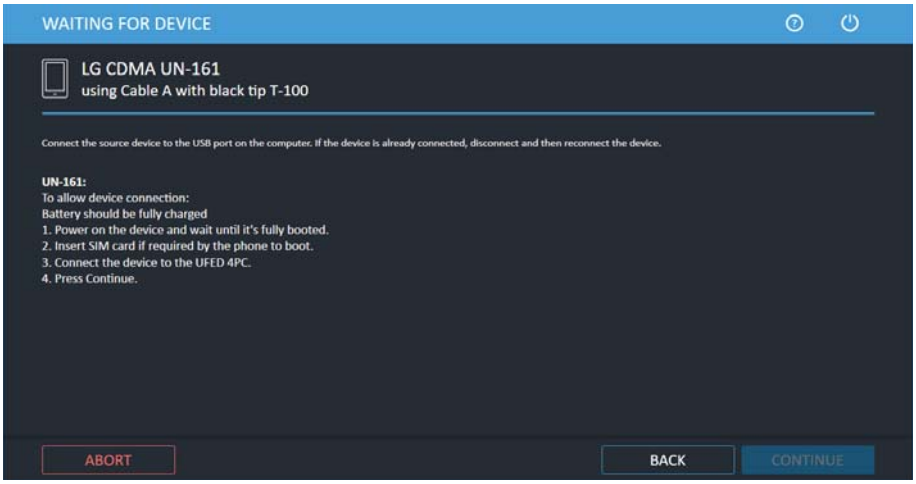
1. Click **Mobile device** and identify the device, then click **Extract User Lock**.

   The Select Extraction Location screen appears.



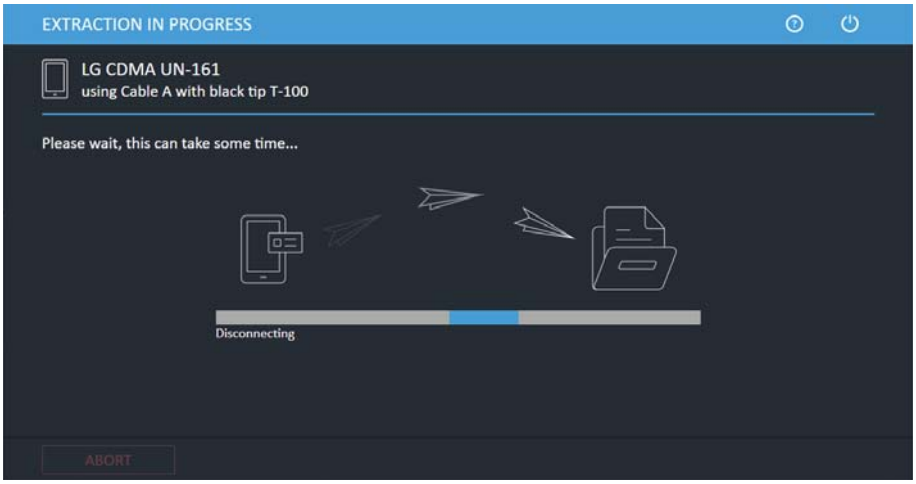
2. Select **Display Only** or **Local Drive**.

The Waiting for Device screen appears.



3. Connect the source device to the USB port, or via the UFED Device Adapter.
4. Click **Continue**.

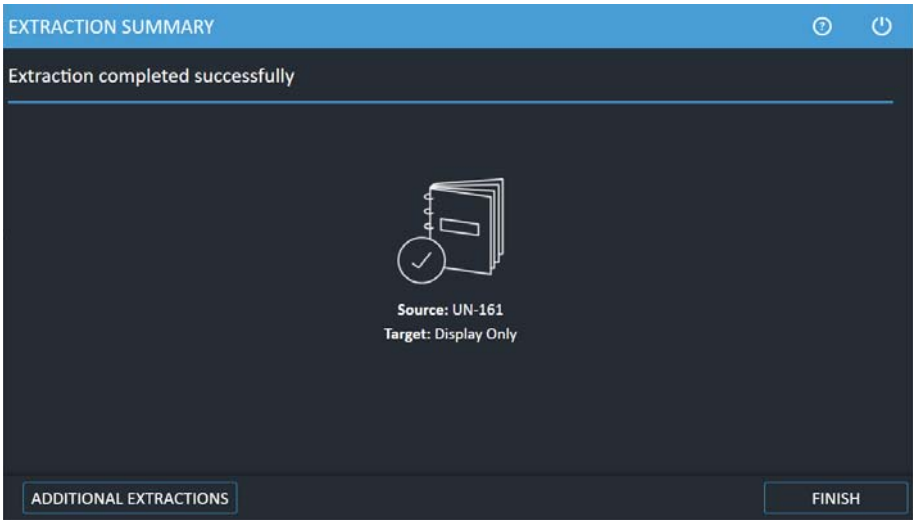
   The Extraction in Progress screen appears.



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

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

The following screen appears.



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

3.1.1. 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.

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)"

3.2. Disabling or re-enabling the user lock

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

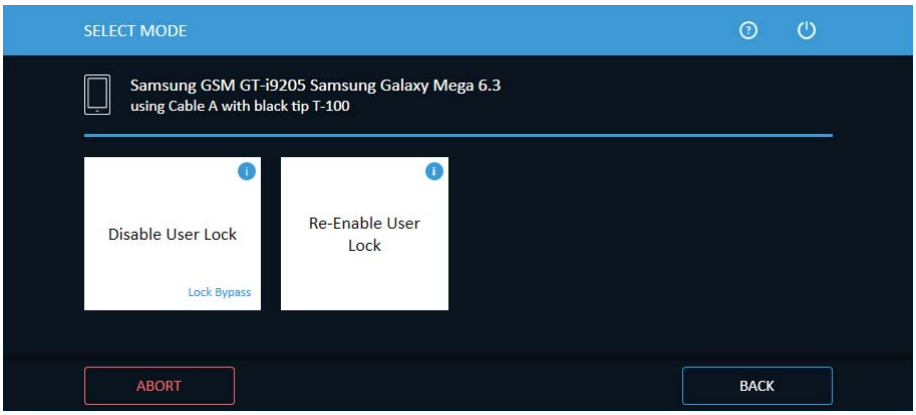
- **Disable the user lock:** Disable the user lock (or password), which means that the device will no longer be locked. Each device model has a slightly different process, depending on the device lock combination and how the model connects to UFED. When more than one method is available for the device,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

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

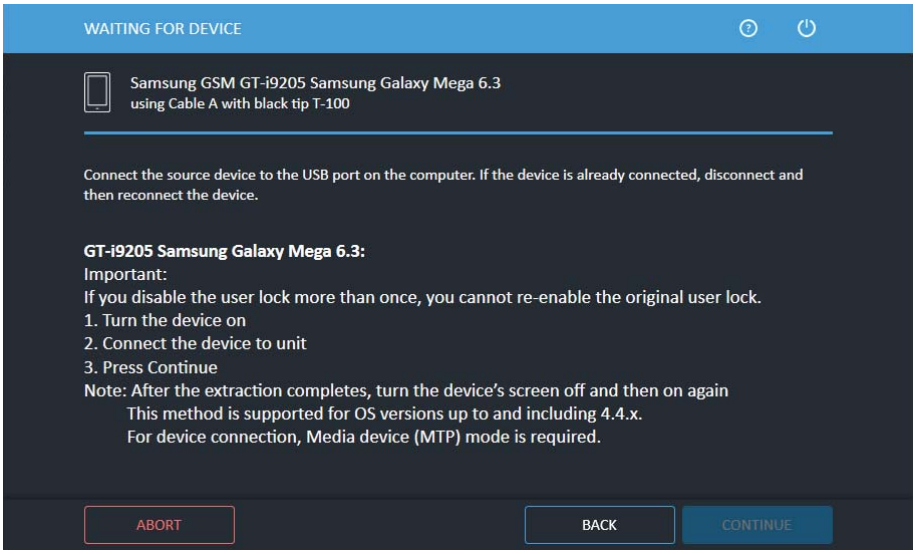
> UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: https://www.cellebrite.com/en/services/advanced-unlocking-services/

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

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



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



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

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

The Extraction completed successfully screen appears.

4. Click **Finish**.

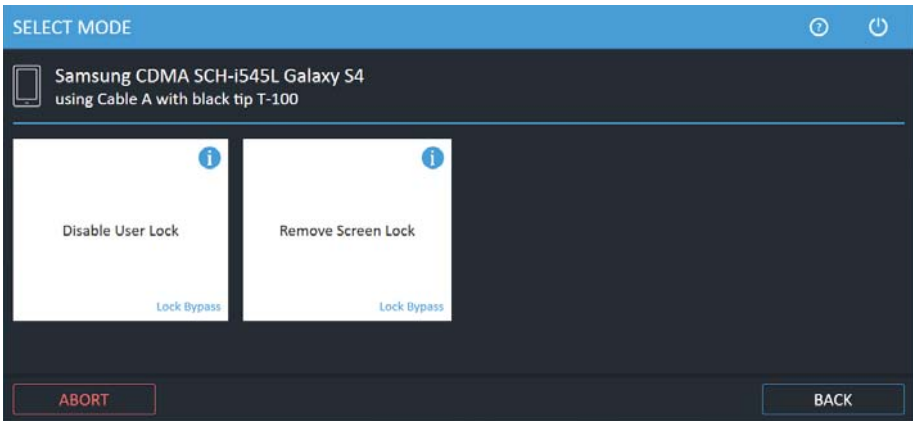
3.3. Removing the screen lock

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

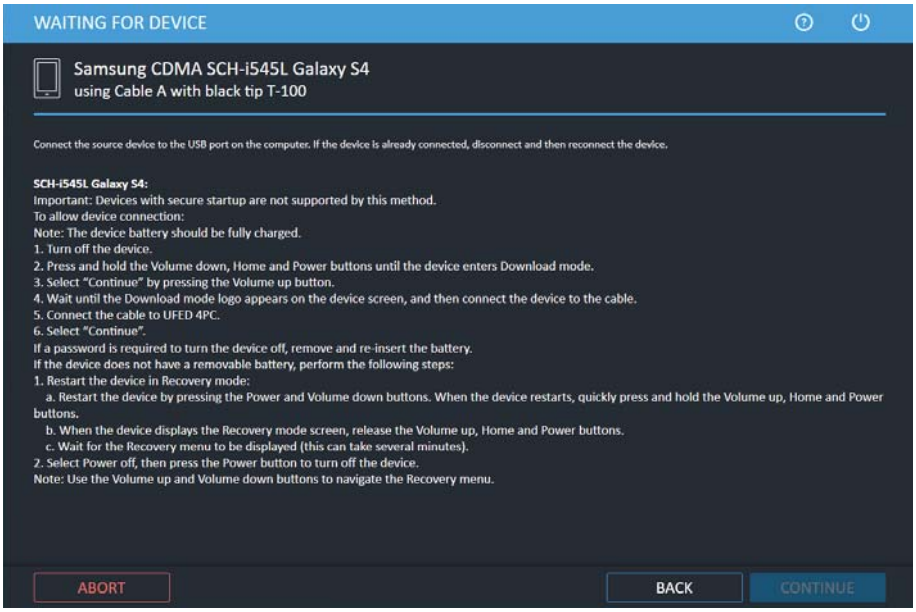
UFED cannot re-enable the screen lock after running the process.

To remove the screen lock from a device:

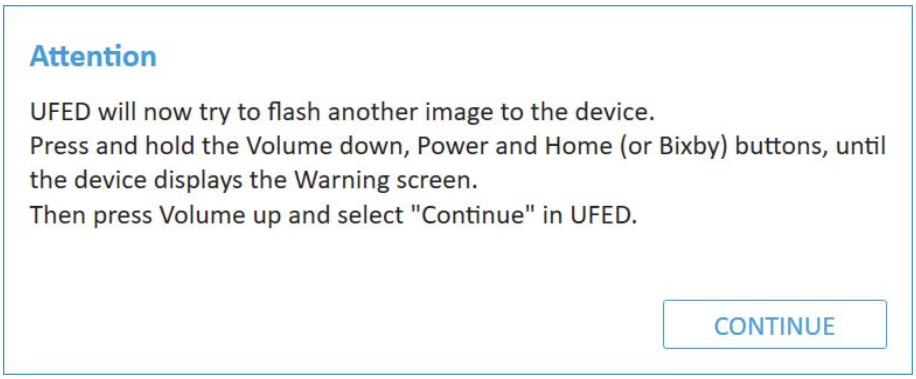
1. Click **Mobile device** and identify the device, then click **Disable/Re-enable User Lock**. The following window appears.



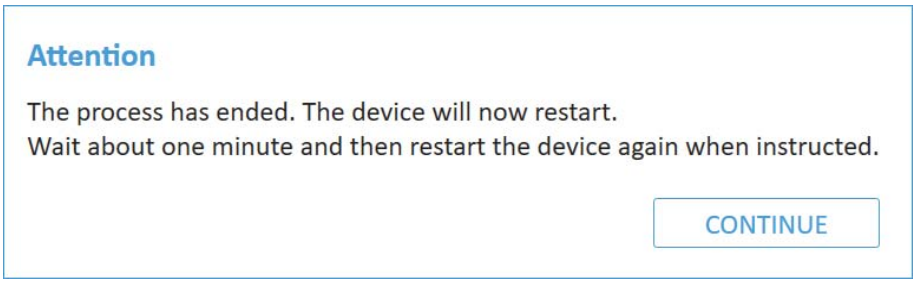
2. Click **Remove Screen Lock** to remove the screen lock from the device. The Waiting for Device window appears.



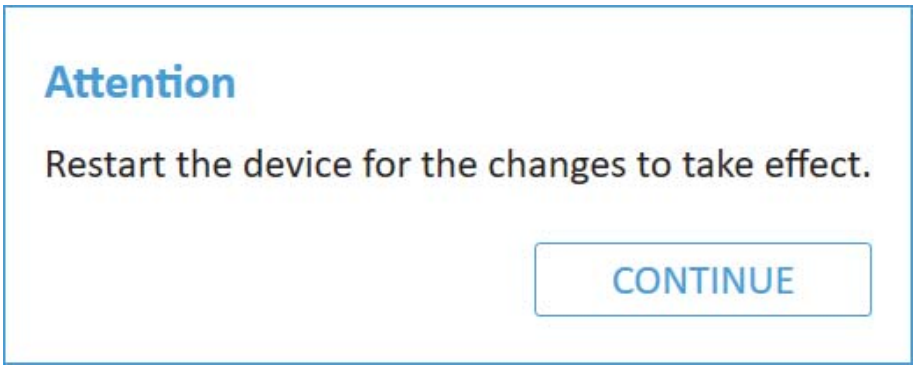
3. Follow the instructions to place the device in Download mode, then click **Continue**. The following window appears.



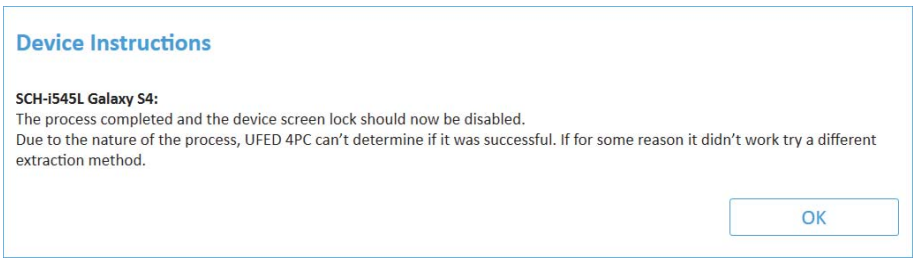
4. UFED will now try to flash another image to the device. Follow the on-screen instructions until the device the device displays the Warning screen and Download mode again. Then click **Continue** in UFED. The following window appears.



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

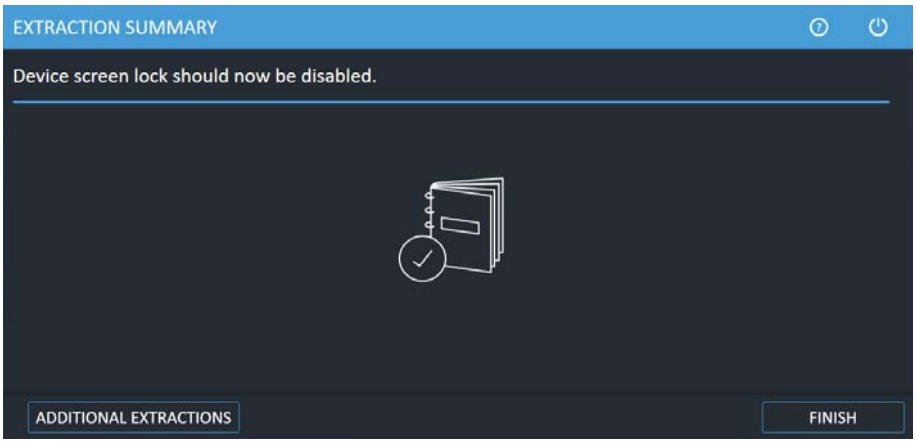


6. Restart the device for the changes to take effect and then click **Continue**. The following window appears.



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

7. Click OK. The following window appears.



8. Click **Finish**.

4. File system extraction

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

File system extractions include the following:

Performing a file system extraction (below)

Android backup (on page 49)

Android backup APK downgrade (on page 54)

Selective file system extraction (on page 64)

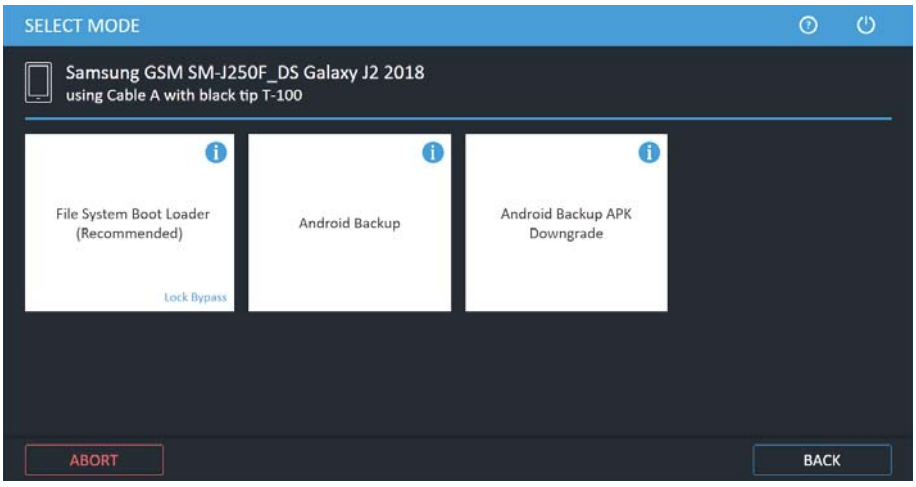
UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: https://www.cellebrite.com/en/services/advanced-unlocking-services/

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

4.1. Performing a file system extraction

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

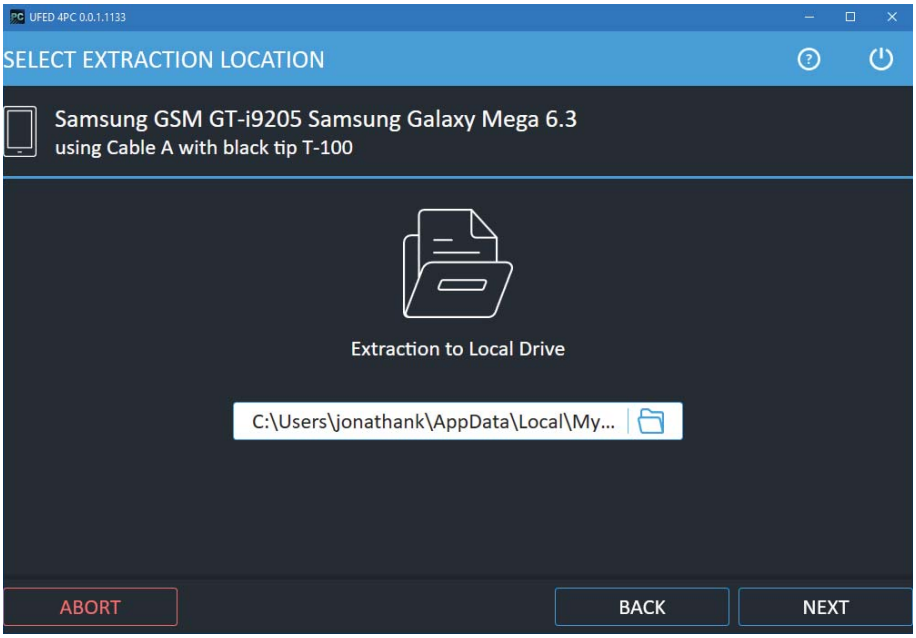
   The Select Mode screen appears.



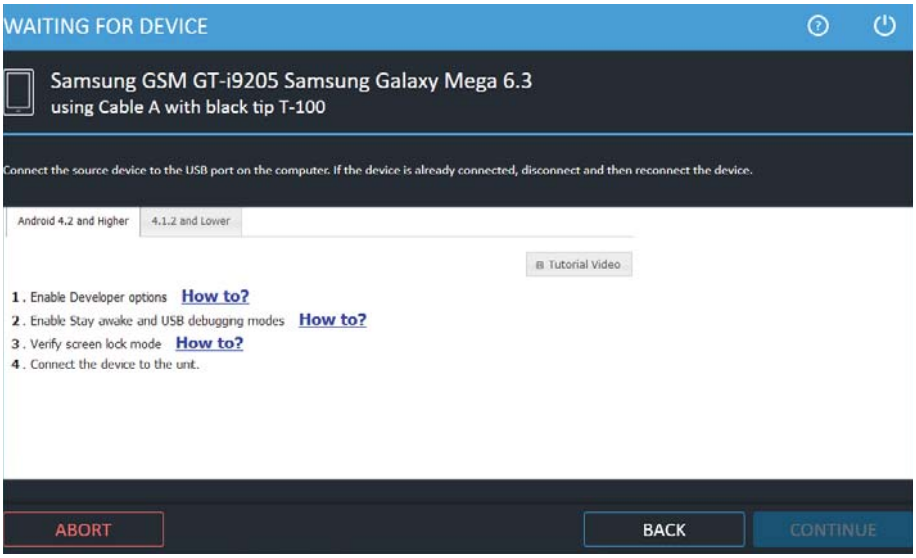
2. Select **ADB** (for Android Backup, see Android backup (on page 49)).

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

The Select Extraction Location screen appears.

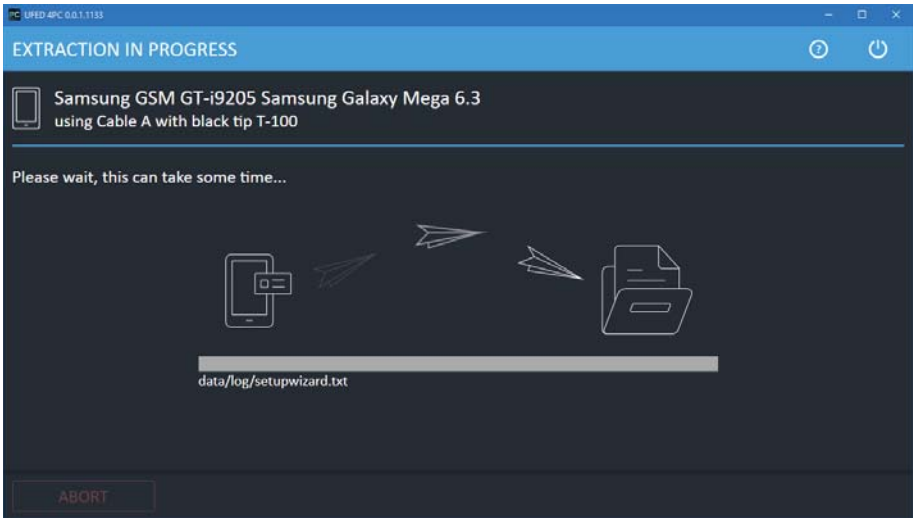


3. Select a location. The following window appears.



4. Select the correct cable and tip for the mobile device based on the information written in the screen.
5. Change the device settings according to the instructions
6. Connect the device.

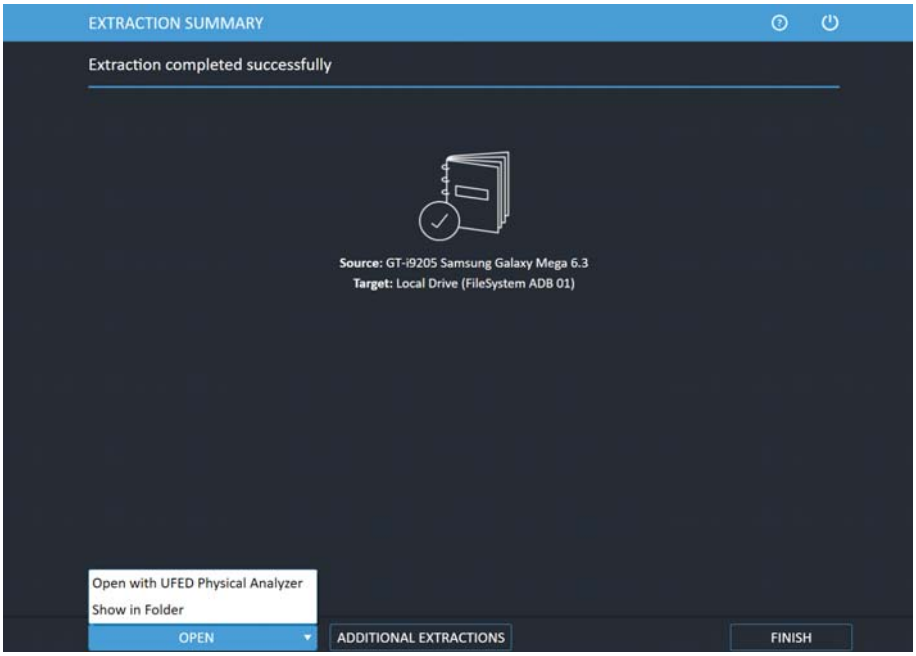
7. Click **Continue**. The Extraction in Progress screen appears.



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

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

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



8. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with UFED Physical Analyzer** to open the extraction in UFED Physical Analyzer, click **Show in Folder** to open the folder where the UFD extraction file is located, click **Additional Extractions** to add

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

4.1.1. 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 (on page 45)).

> 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.

4.2. Android backup

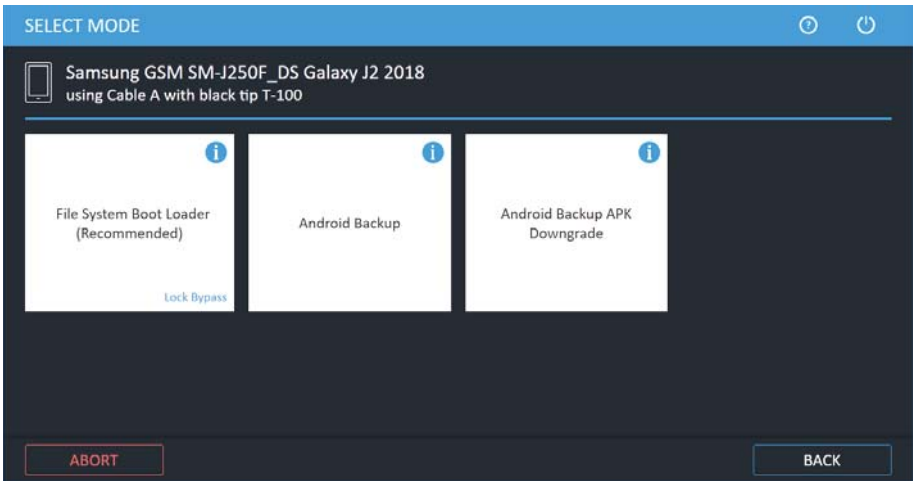
The Android Backup feature communicates with a connected Android device and enables you to extract data from the device. The data that is extracted is dependent on the device's specific characteristics. Android backup supports Android devices with version 4.1 and later.

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).

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

To extract data using Android backup:

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

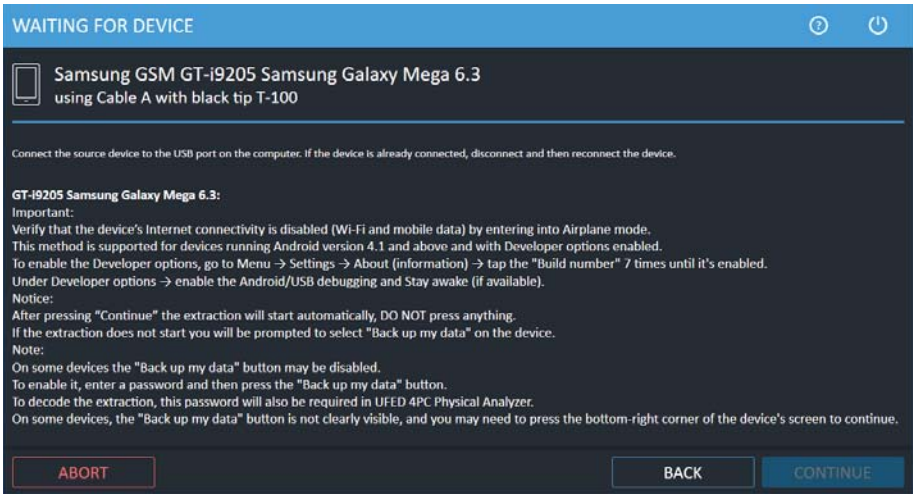


2. Click **Android Backup**.
3. Select the extraction location.

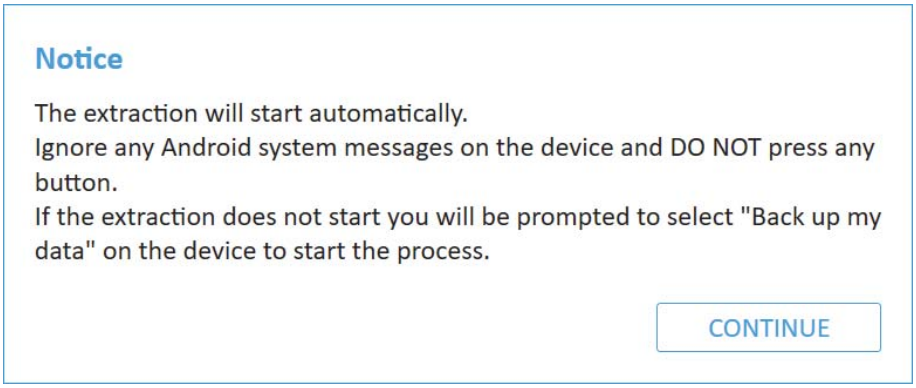
> For information on using optional timeframe and party filters, refer to the *Overview Guide*.

4. Click **Continue**.

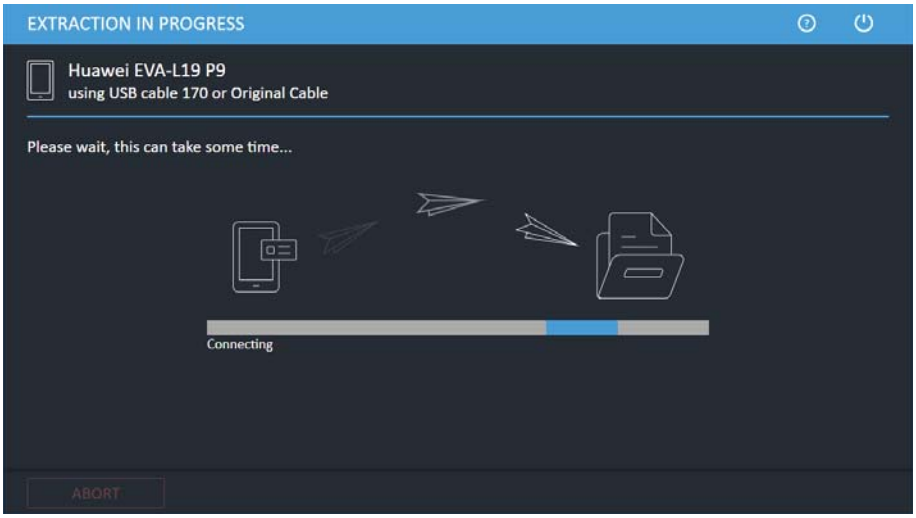
The Waiting for Device screen appears.



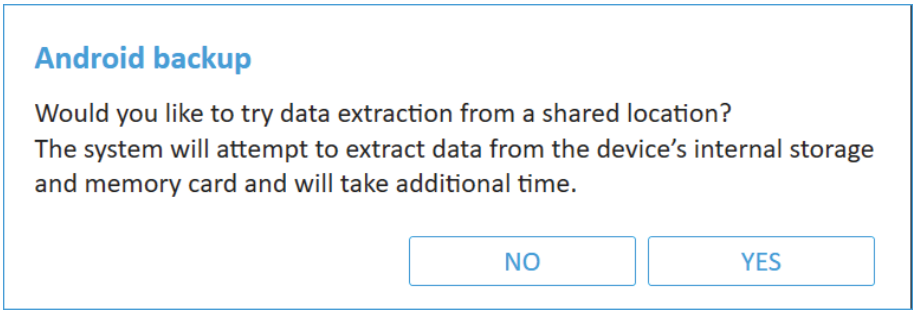
5. Connect the source device to the USB port. If the device is already connected, disconnect and then reconnect the device.
6. Click **Continue**. The following window appears.



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

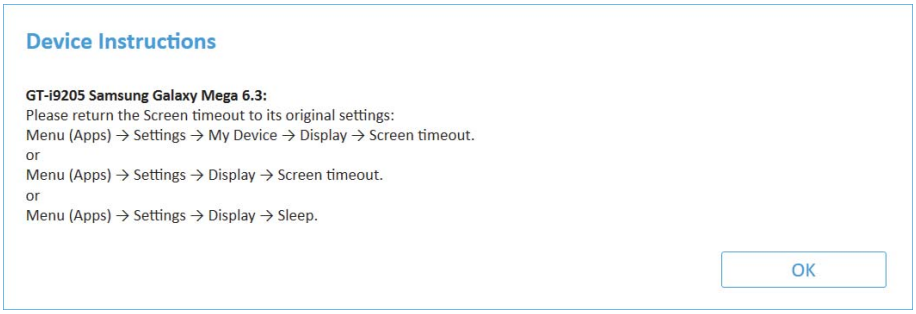


The following screen appears.



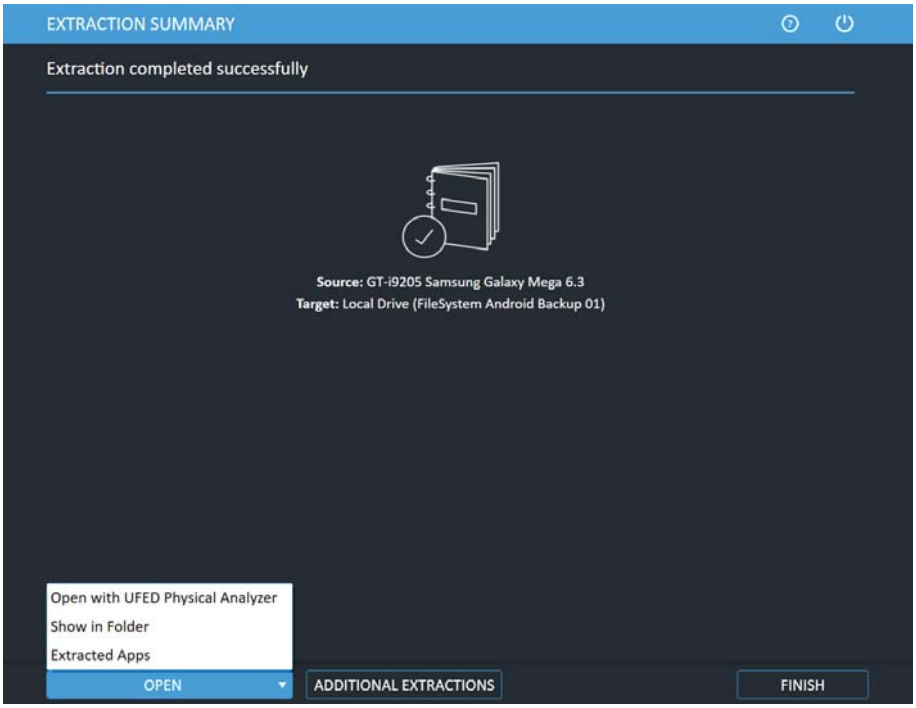
8. Click **No** if you do not want to extract data from a shared location. Click **Yes** if you want to try extract data from a shared location. With a shared location, UFED extracts all the applications (native and non-native) that reside on the device, as well as data from the device's internal storage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

   The following screen appears.



9. Follow the instructions and click OK.

   When the extraction completes the Extraction summary window appears.

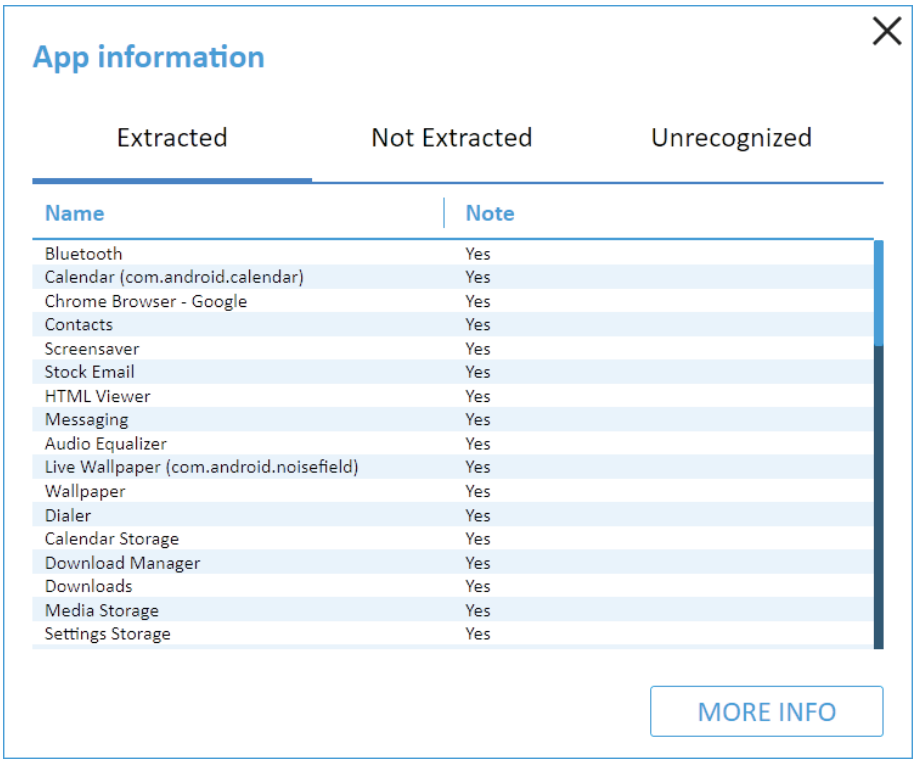


10. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with UFED Physical Analyzer** to open the extraction in UFED Physical Analyzer, click **Show in Folder** to open the folder where the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

4.2.1. Extracted apps

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

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



4.3. Android backup APK downgrade

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

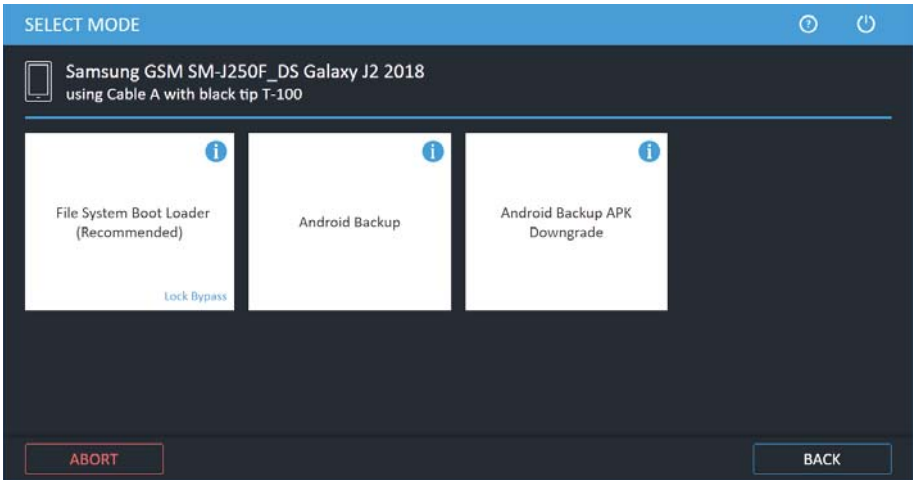
> The Android Backup APK Downgrade method should be used only as a last resort after other extraction methods have been exhausted (including JTAG and chip-off).

> To use Android backup APK downgrade you need to download the APK Downgrade Pack. For more information, see Installing the latest APK version (on page 58).

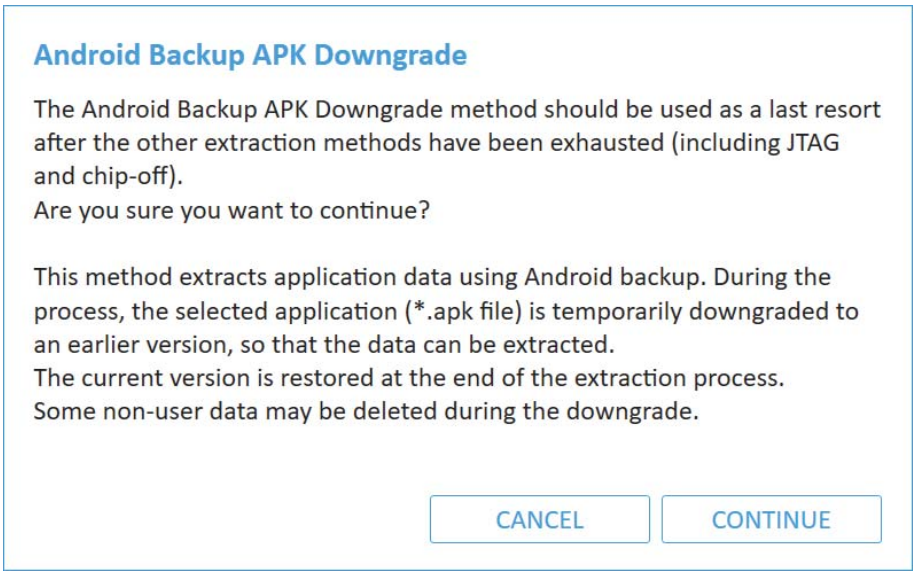
> It is recommended to document the process during the extraction.

To extract data using Android backup APK downgrade:

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



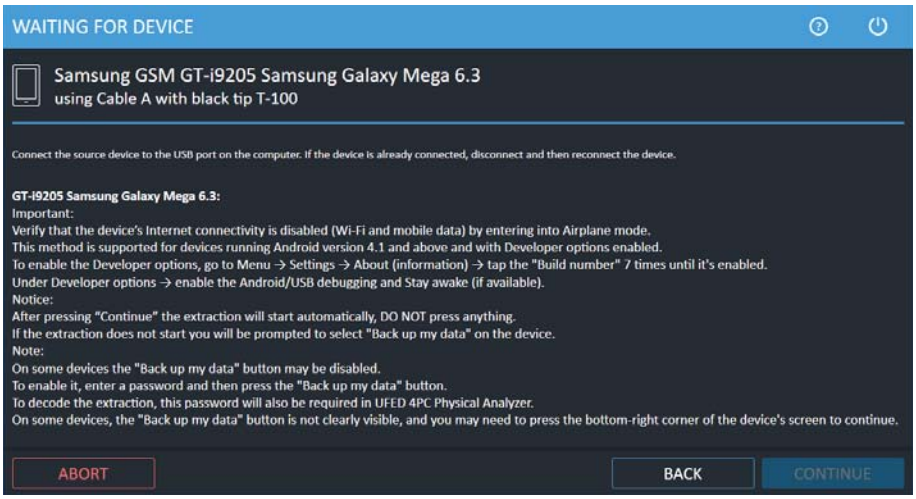
2. Click **Android Backup APK Downgrade**. The following window appears.



3. Click **Continue**.

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

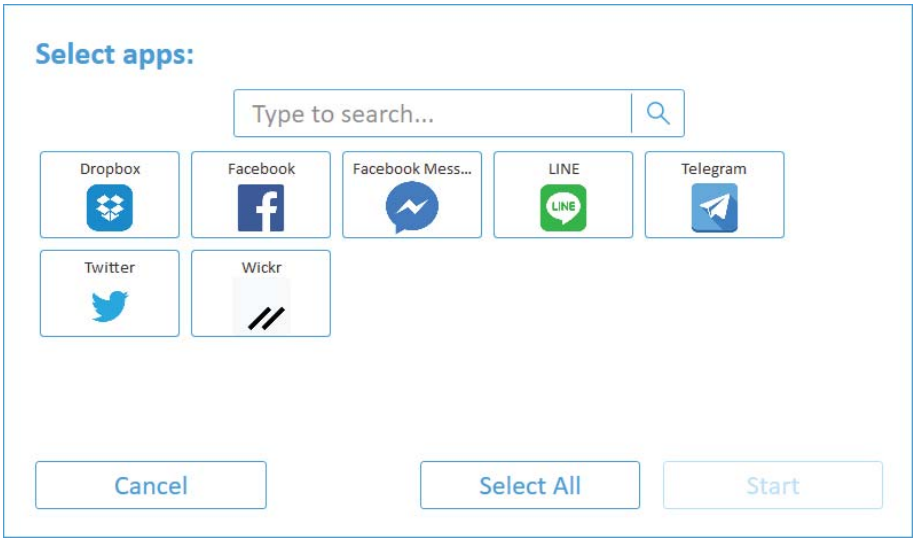
4. Select the target path and click **Next**. The Waiting for Device screen appears.



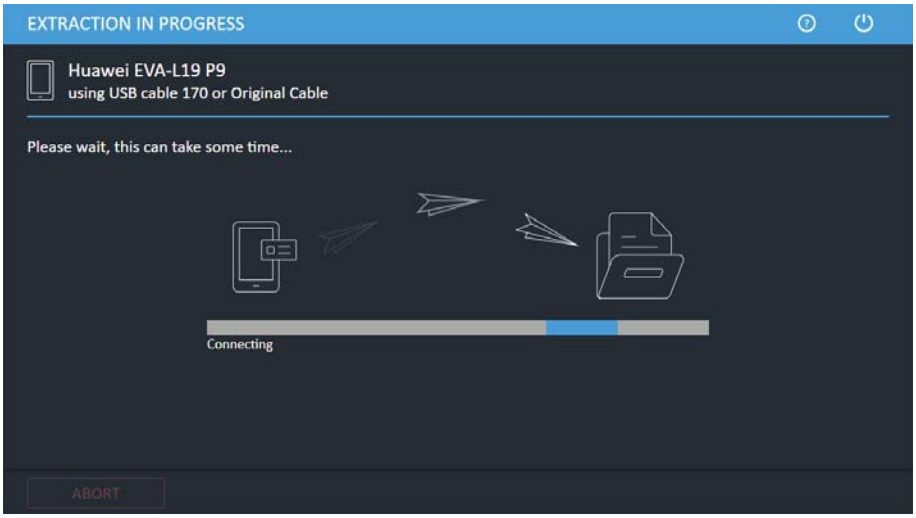
5. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device.
6. Follow the on-screen instructions for the device and then click **Continue**. The following screen appears.

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

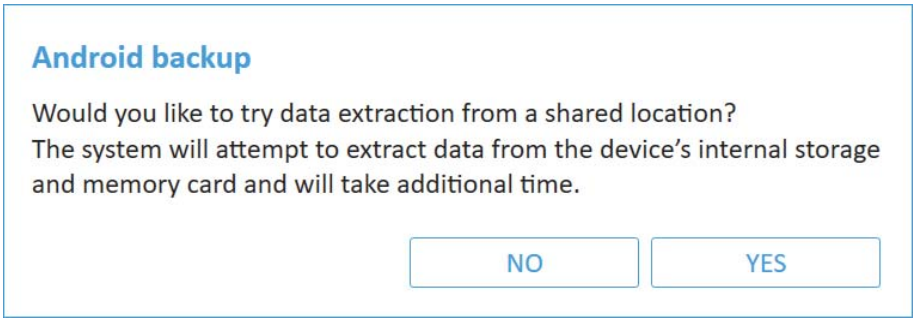
The following window appears.



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



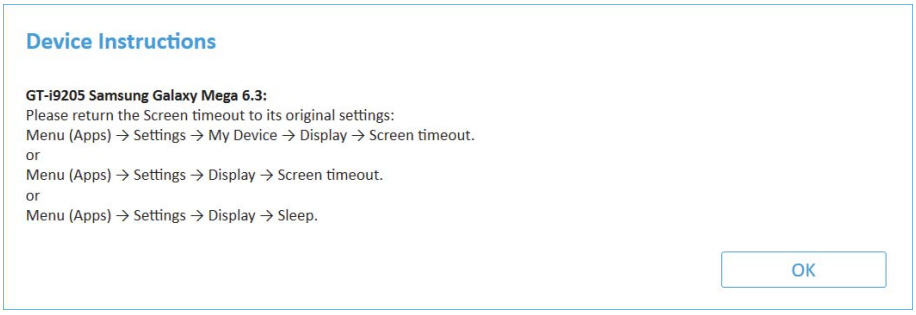
8. Select **Backup my data** on the device. The following window appears.



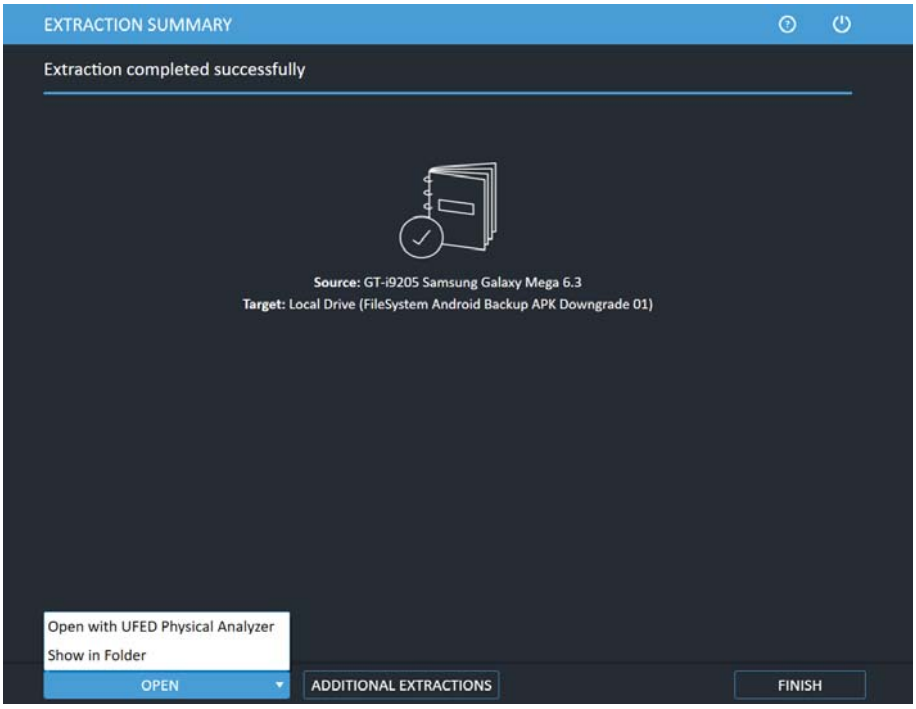
9. Click **No** if you do not want to extract data from a shared location. Click **Yes** if you want to try extract data from a shared location. With a shared location, UFED extracts all the applications (native and non-native) that reside on the device, as well as data from the device's internal storage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

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

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



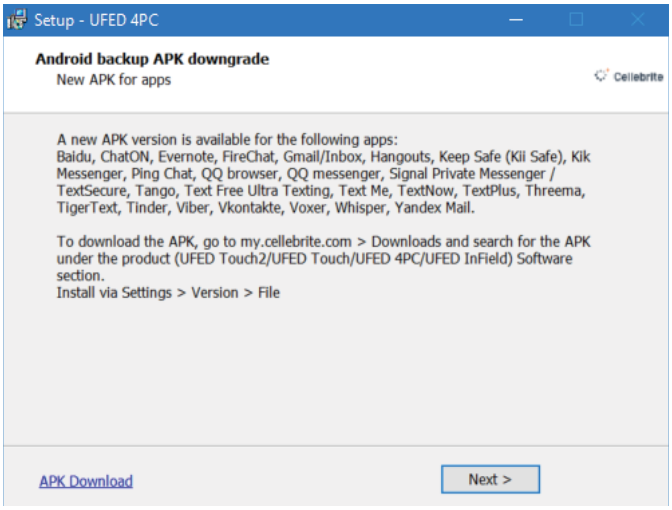
11. Follow the instructions and click OK. The Extraction summary window appears.



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

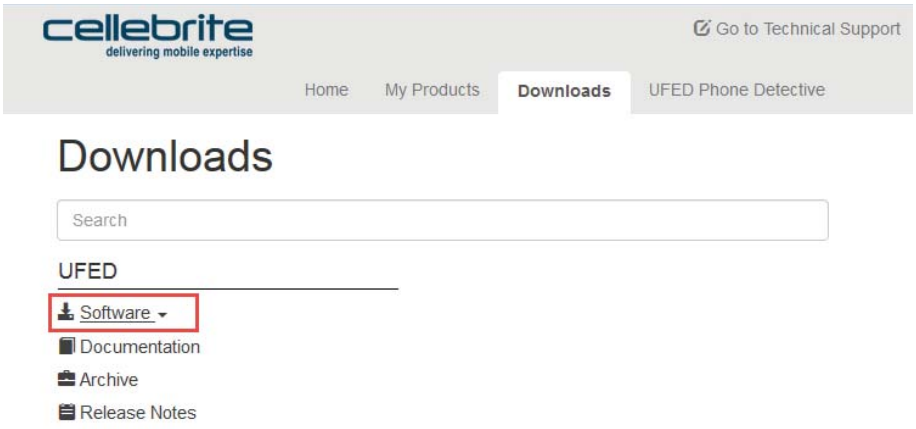
4.3.1. Installing the latest APK version

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



To download and install the latest APK version:

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



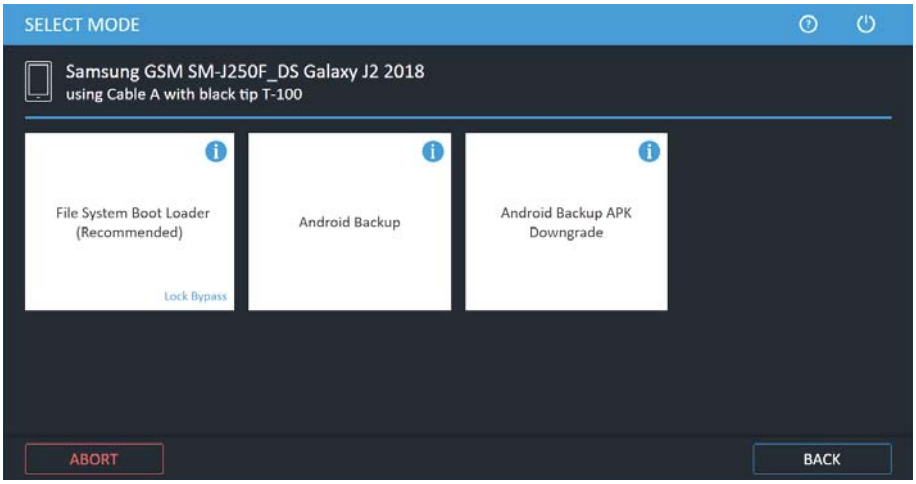
4. Download the APK Downgrade Pack and save it on the computer or to a USB drive.
5. In UFED, install the APK via **Settings** > **Version** > **File**.

4.3.2. Android backup APK downgrade - Manual installation

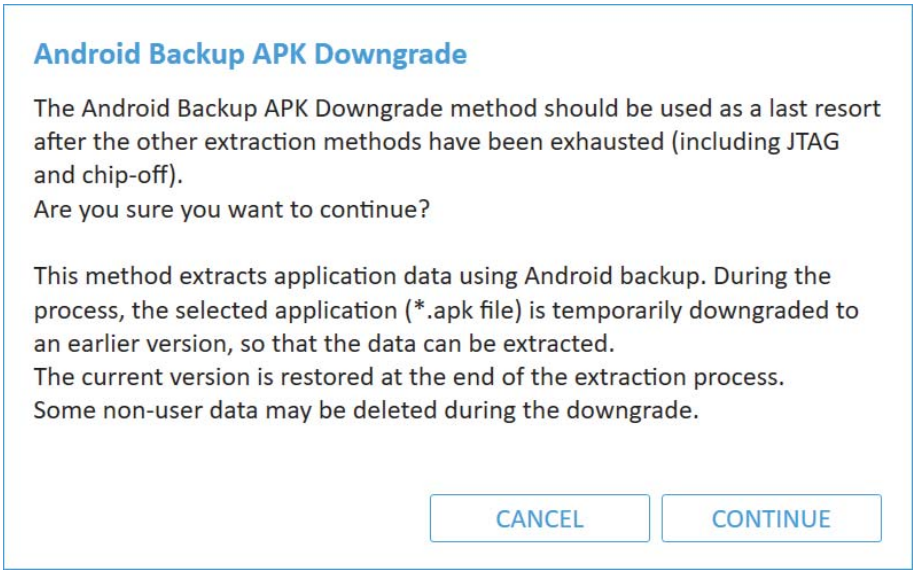
Manually intervene during the APK downgrade process to overcome installation issues where the device is not compatible.

To extract data using Android backup APK downgrade by manually installing the apps:

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



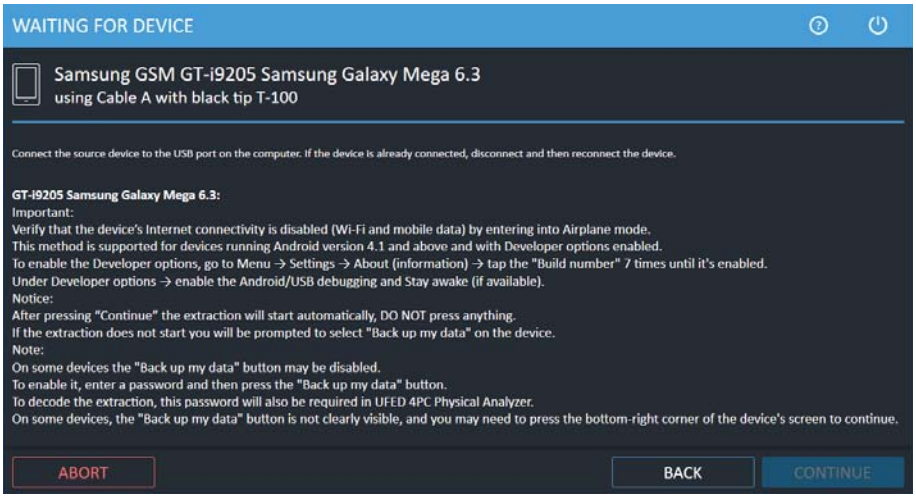
2. Click **Android Backup APK Downgrade**. The following window appears.



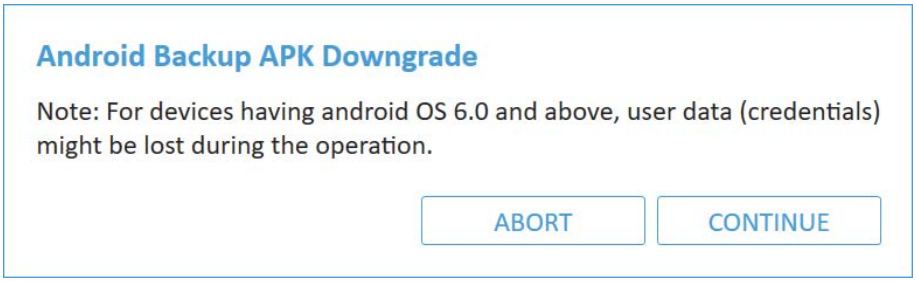
3. Click **Continue**.

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

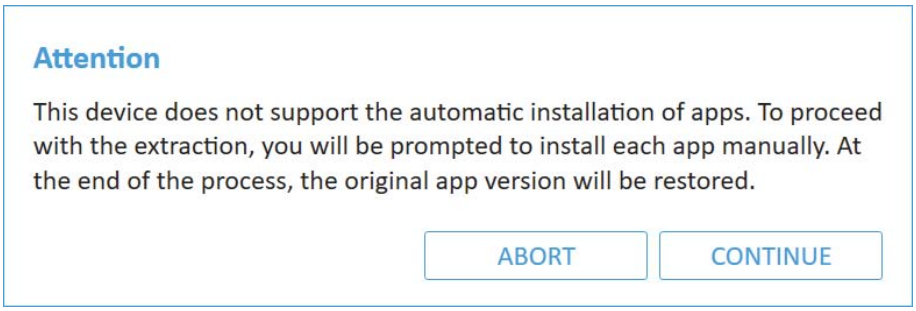
4. Select the target path and click **Next**. The Waiting for Device screen appears.



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

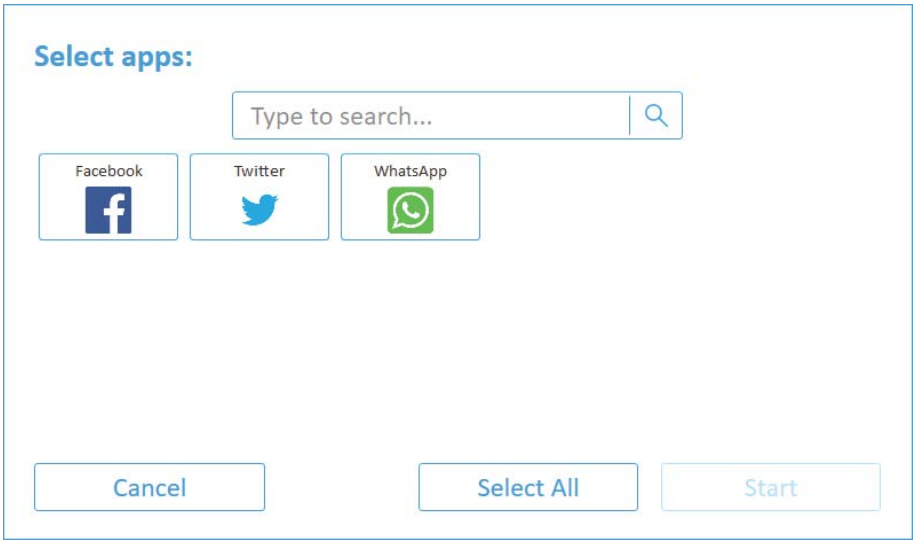


7. Click **Continue**.

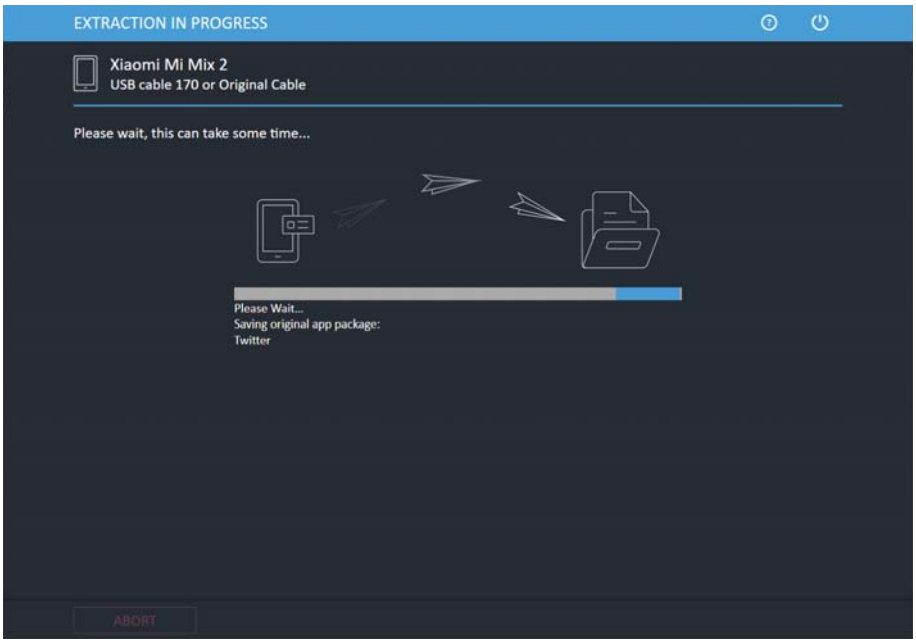


8. This notification appears on devices that do not support automatic installation of apps. You will be prompted to install the apps manually. Click **Continue**.

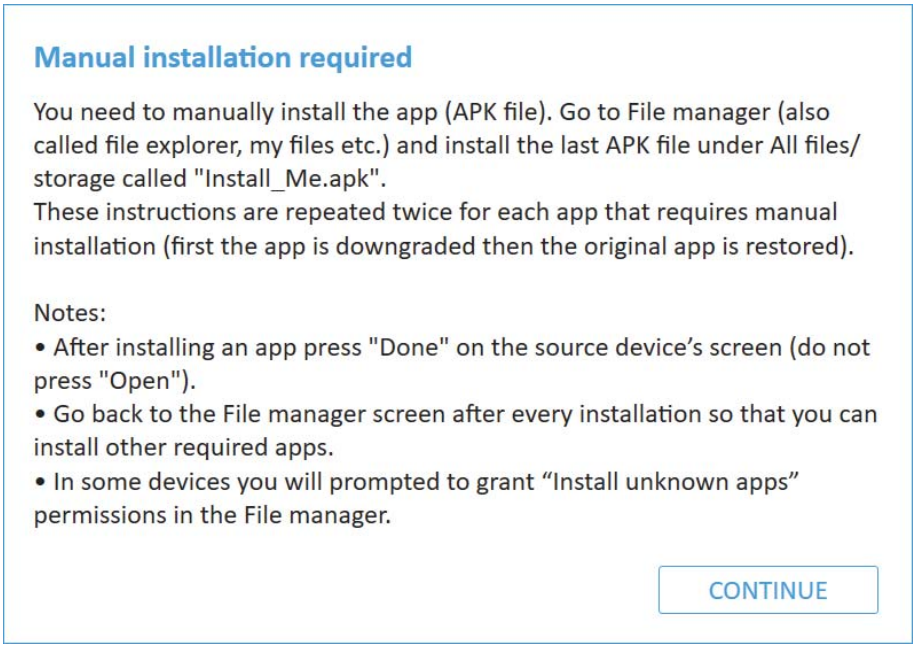
   The following window appears.



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



The following window appears.



10. Manually install the APK file. Go to the File Manager (also called File Explorer, My Files, Mi File Manager etc.) on the source device and install the "Install_Me.apk" under All files or Storage. The icon of the app appears next to the "Install_Me.apk".
11. After installing the app, press **Done** on the source device's screen (do not press **Open**).
12. Go back to the File Manager screen after every installation so that you can install all the required apps.
13. Click **Continue**.

You will be notified when to select **Backup my data** on the device to continue with the Android Backup process. For more information, see Android backup APK downgrade (on page 54).

4.4. Selective file system extraction

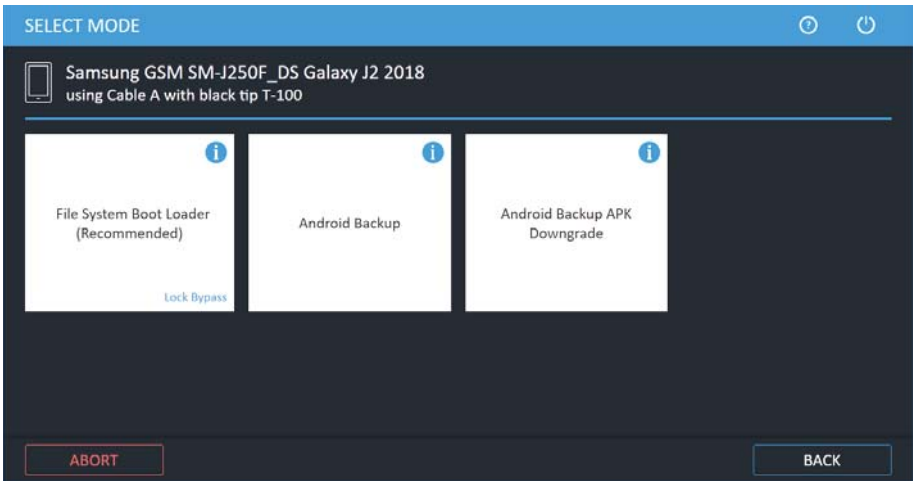
Selective extraction is part of the full file system extraction. It extracts all relevant app data located under the root directory. The app data includes folders and files associated with the app such as databases, APKs, images, and keys. Selective extraction takes less time to complete compared to a full file system extraction and enables you to only select the apps that are required.

Selective extraction is currently supported for EDL Decrypting Bootloader, Samsung Qualcomm Decrypting Bootloader and Huawei Decrypting Bootloader methods.

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

To extract data using Selective file system extraction:

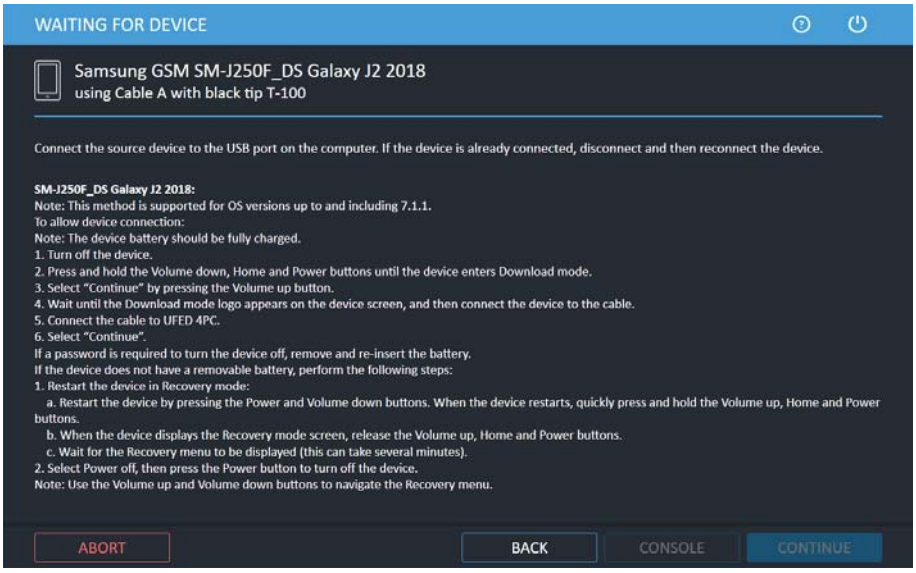
1. Click **Mobile device** and identify the device, then click **File System**.



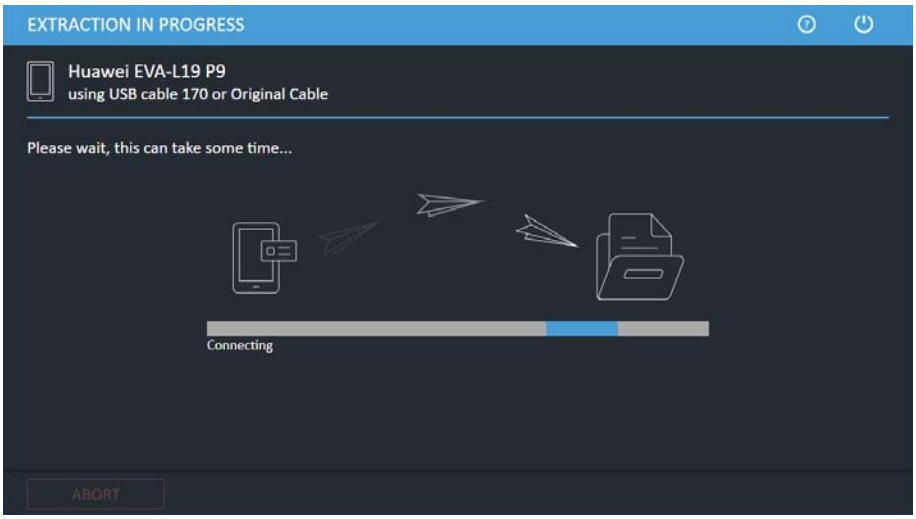
2. Click **File System Boot Loader**.

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

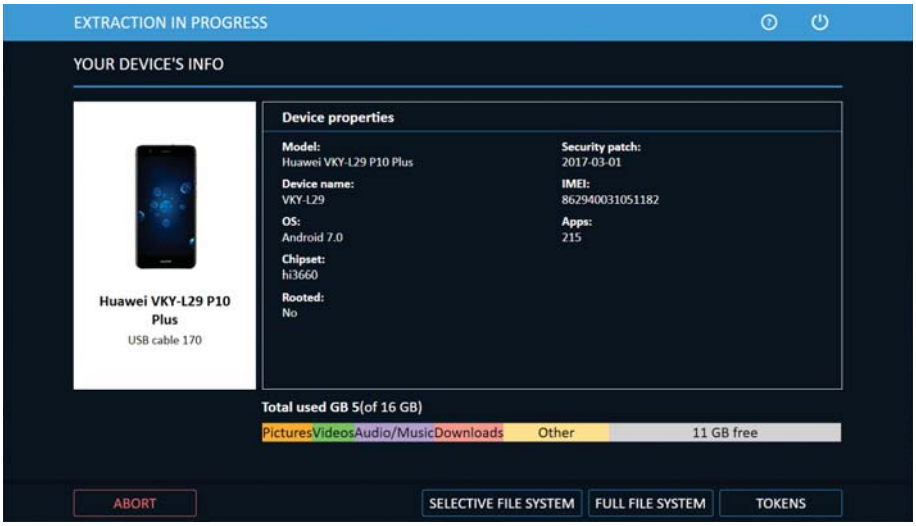
3. Select the extraction location.
4. Click **Continue**. The Waiting for Device screen appears.



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



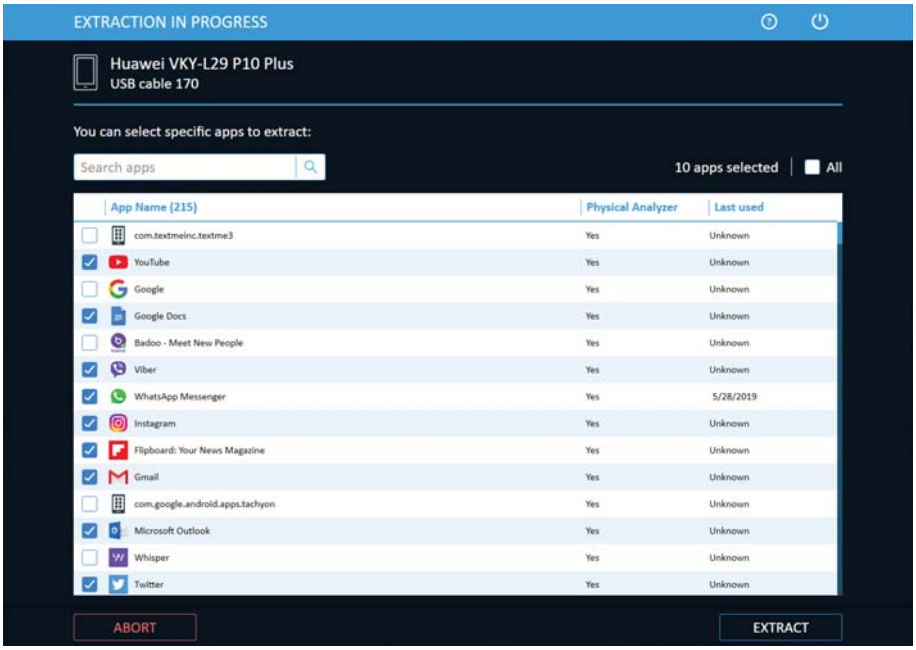
The following window appears.



This window displays the device properties such as such as model, device name, OS, chipset, whether the device is rooted, date security patch installed, IMEA, and the number of installed apps, and what data is on a device including storage volume, data types, volume of storage per data type, and free data. Click one of the following options:

- **Selective File System:** The Selective extraction takes less time to complete and enables you to only select the required apps to extract.
- **Full File System:** Full file system extraction including all apps and tokens.
- **Tokens:** Retrieve data from cloud sources. Upon extraction and decoding, create the account package in UFED Physical Analyzer and upload it into UFED Cloud Analyzer.

A Selective file system extraction example is displayed next.



7. Select the required apps and the click **Extract**. The Extraction Summary window appears.

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

5. 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.

Physical extractions include the following:

Performing a physical extraction (on the next page)

ADB rooted (on page 73)

Advanced ADB (on page 76)

Boot loader (FW flashing) (on page 93)

Decrypting boot loader (on page 97)

Forensic recovery partition (on page 99)

Smart ADB (on page 104)

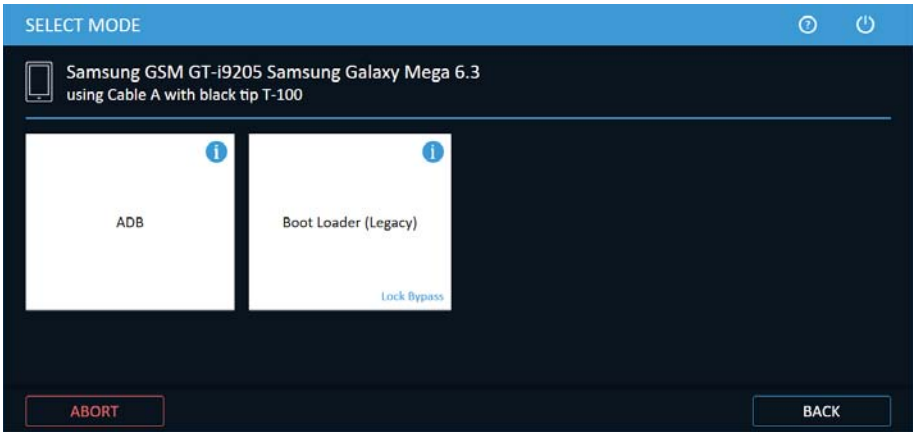
UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: https://www.cellebrite.com/en/services/advanced-unlocking-services/

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

5.1. Performing a physical extraction

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

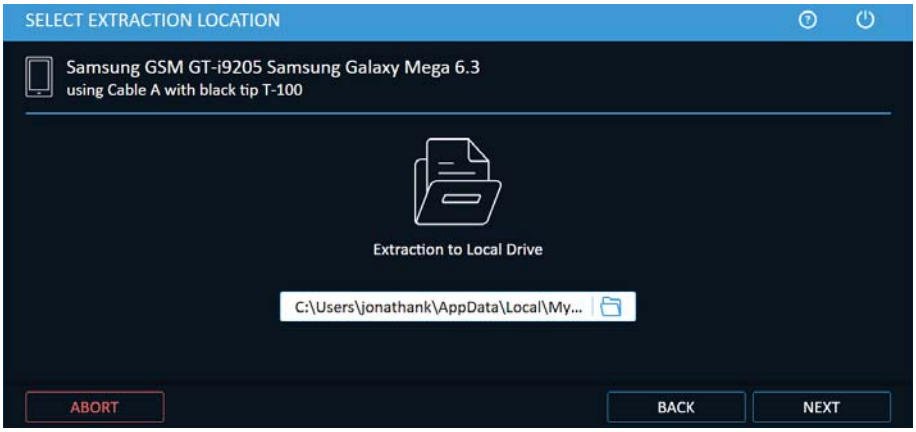
   The Select Mode screen appears.



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

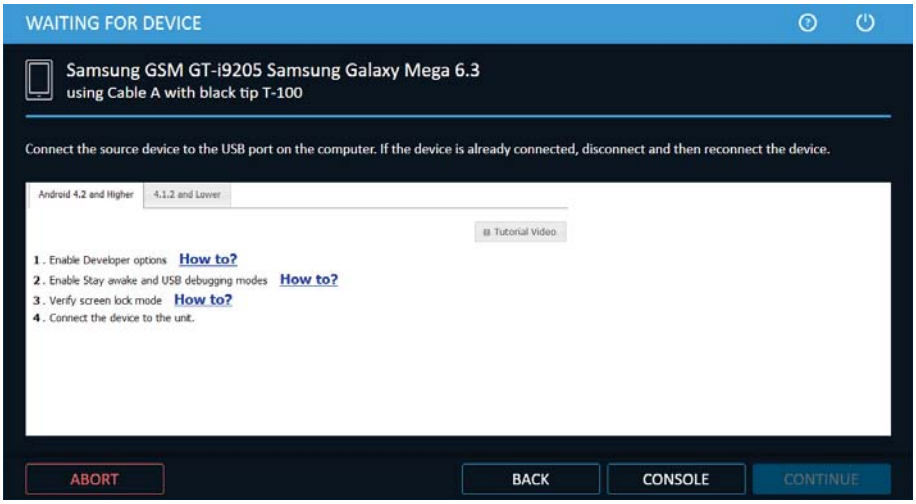
   For information on using optional timeframe and party filters, refer to the *Overview Guide*.

   The Select Extraction Location screen appears.



3. Click **Next**.

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



4. Do the following:
   - 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.

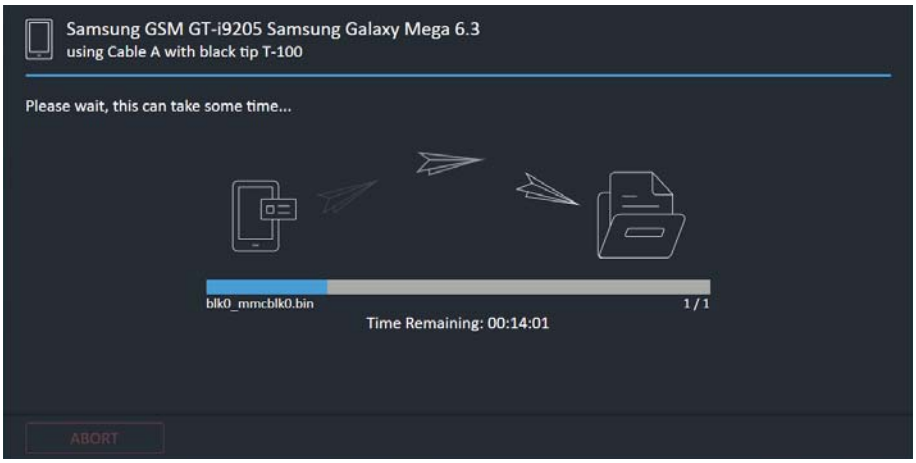
   If the device requires the UFED Device Adapter to perform the extraction:

   - Connect the UFED Device Adapter to a USB port on the computer.

     The source port on the UFED Device Adapter flashes.

   - Connect the device to the UFED Device Adapter.

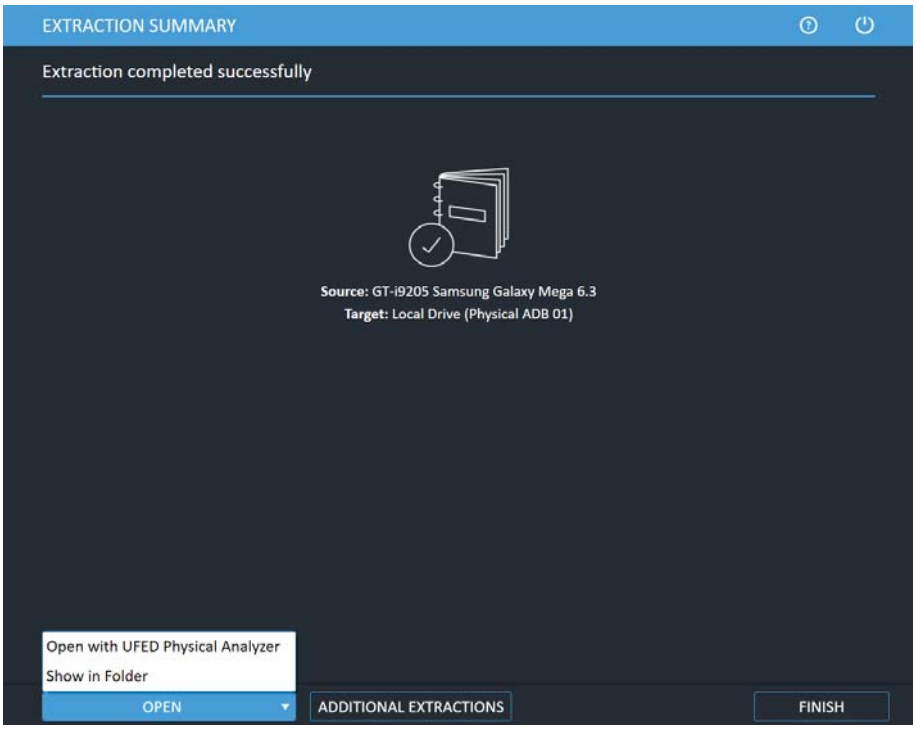
5. Click **Continue**. The Extraction in Progress screen appears.



6. Follow any on-screen instructions.

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

When the extraction completes, the Extraction summary window appears.

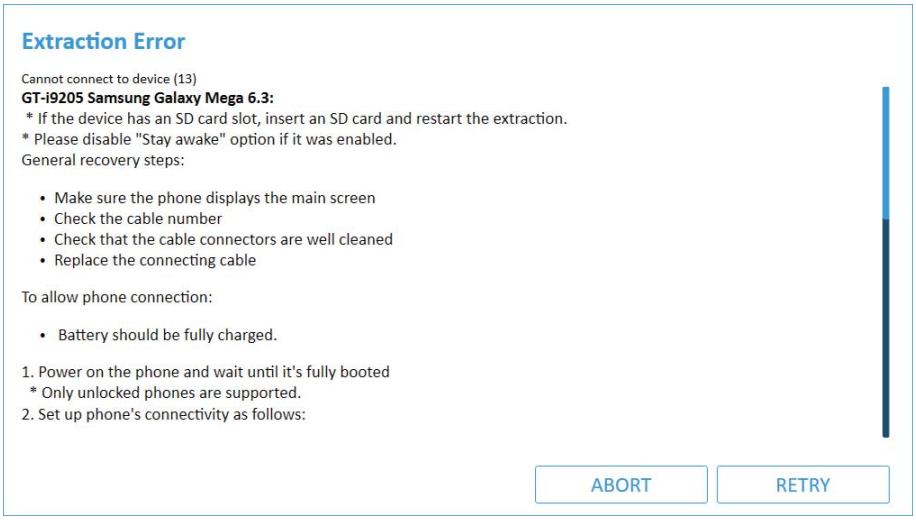


7. Click **Open Preview Report** to view an HTML preview report (Logical extractions only) that includes information about the device and the extraction, click **Open with UFED Physical Analyzer** to open the extraction in UFED Physical Analyzer, click **Show in Folder** to open

the folder where the UFD extraction file is located, click **Additional Extractions** to add additional extraction types for the same device, or click **Finish** to end the process and return to the Home screen.

If the system cannot connect to the device:

The following window appears with an error message.



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

5.1.1. The Physical extraction folder

At the end of the physical extraction process, the extracted data is saved in the location you selected during the physical extraction process. See step 5 of Performing a Physical Extraction.

> 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.

5.2. ADB rooted

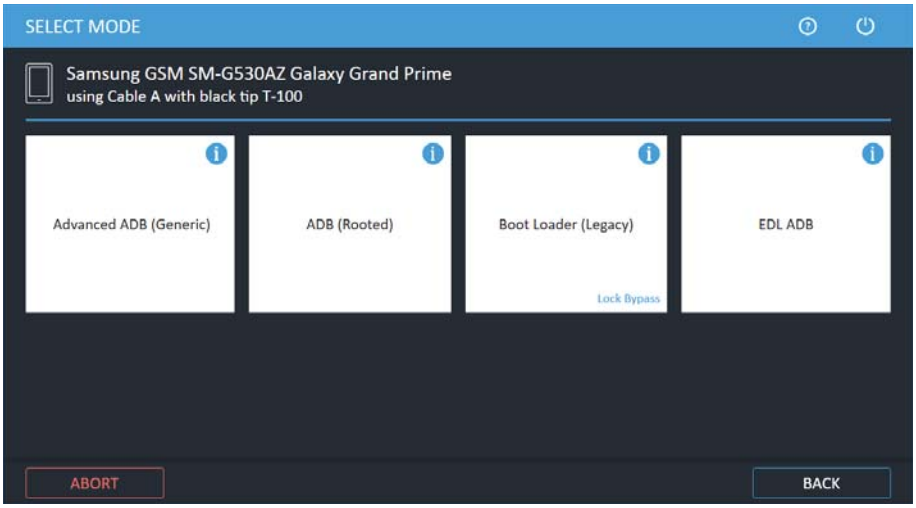
The ADB method for Android rooted devices can be used when the physical extraction method is not supported. Using the ADB method, you can perform a physical extraction from rooted Android devices. This extraction method is for pre-rooted devices only, and does not root the device. To "root" a device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

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

To perform a physical extraction for a rooted Android device:

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

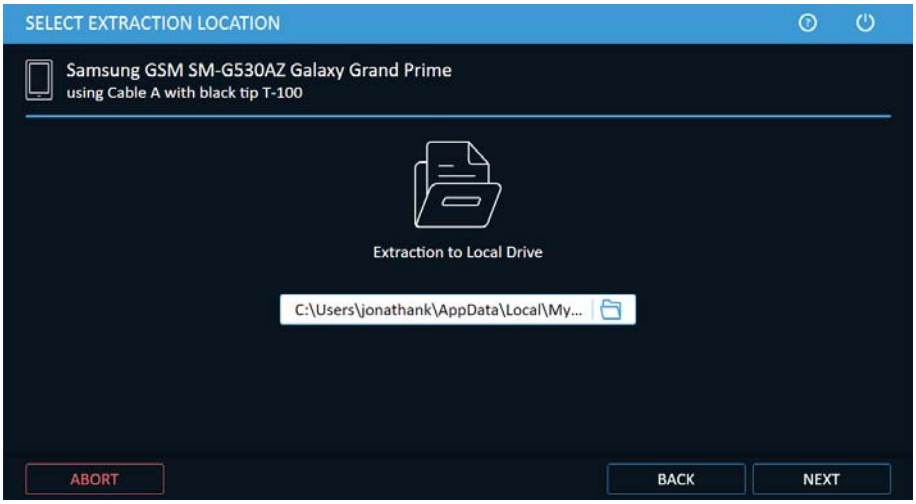
   The Select Mode screen appears:



2. Click **ADB (Rooted)**.

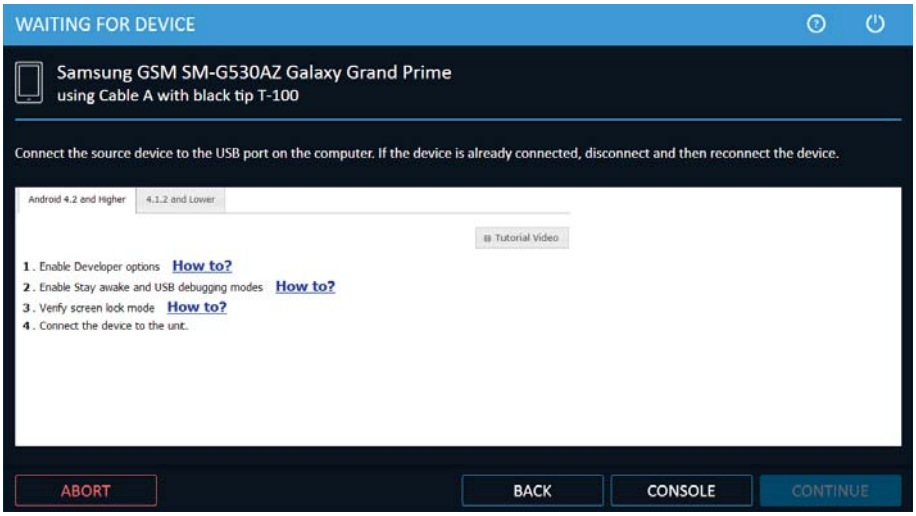
   For information on using optional timeframe and party filters, refer to the *Overview Guide*.

   The Select Extraction Location screen appears.



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

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



4. Do the following:
   - 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.

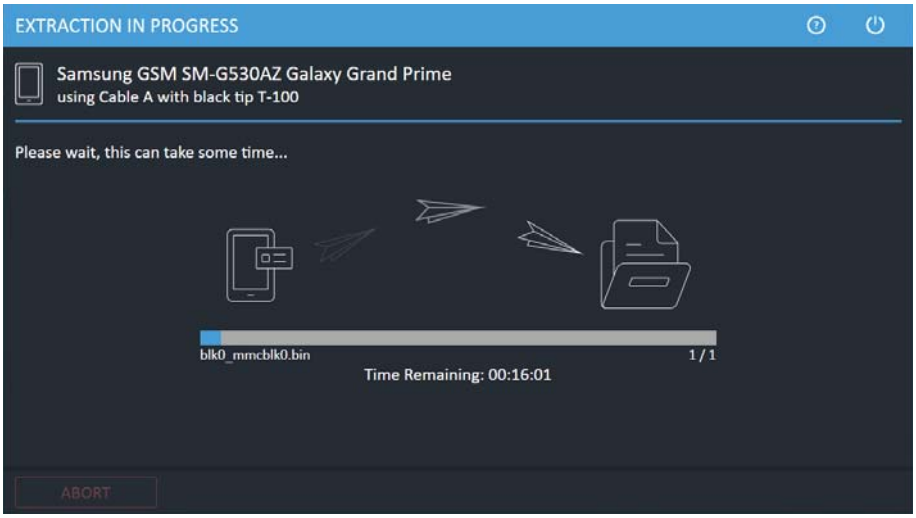
   If the device requires the UFED Device Adapter to perform the extraction:

   - Connect the UFED Device Adapter to a USB port on the computer.

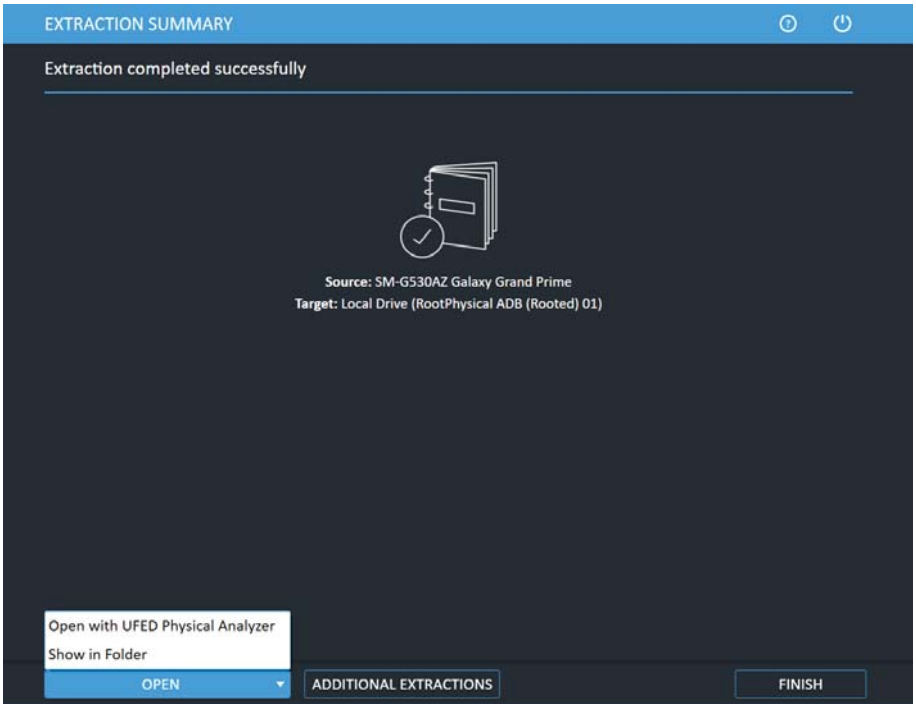
     The source port on the UFED Device Adapter flashes.

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

   The Extraction in Progress screen appears.



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



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

5.3. Advanced ADB

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

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

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

Before performing an Advanced ADB extraction:

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

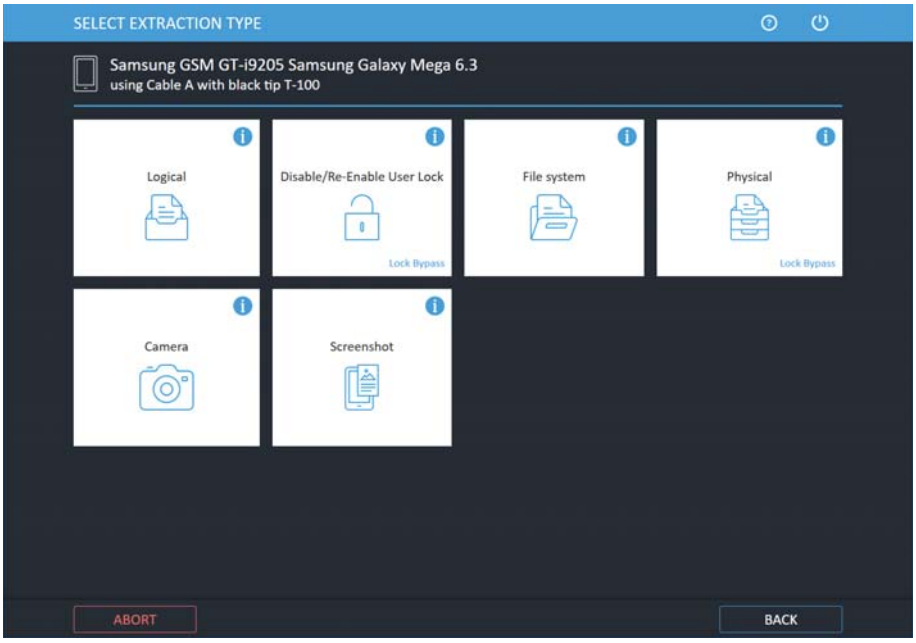
   - If an SD card is selected for the target storage, place it in the Android device now.

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

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

To perform an Advanced ADB extraction:

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



> If the relevant model is not listed, browse manually for a generic Android model. See Generic model (on page 84).

2. Click **Physical**.

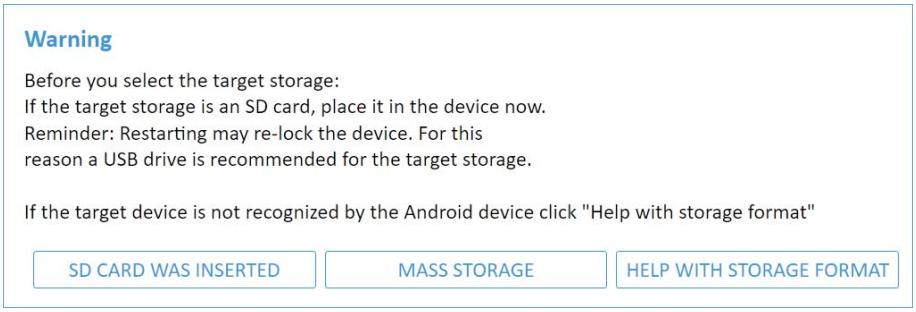
   The Select Mode screen appears.

3. Click **Advanced ADB**.

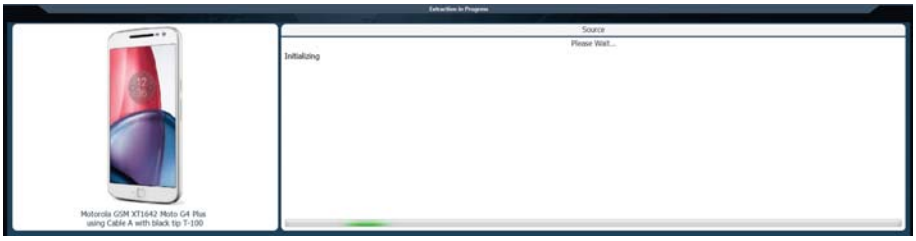
> For information on using optional timeframe and party filters, refer to the *Overview Guide*.

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

6. On the UFED screen, click **Continue**. The following window appears.

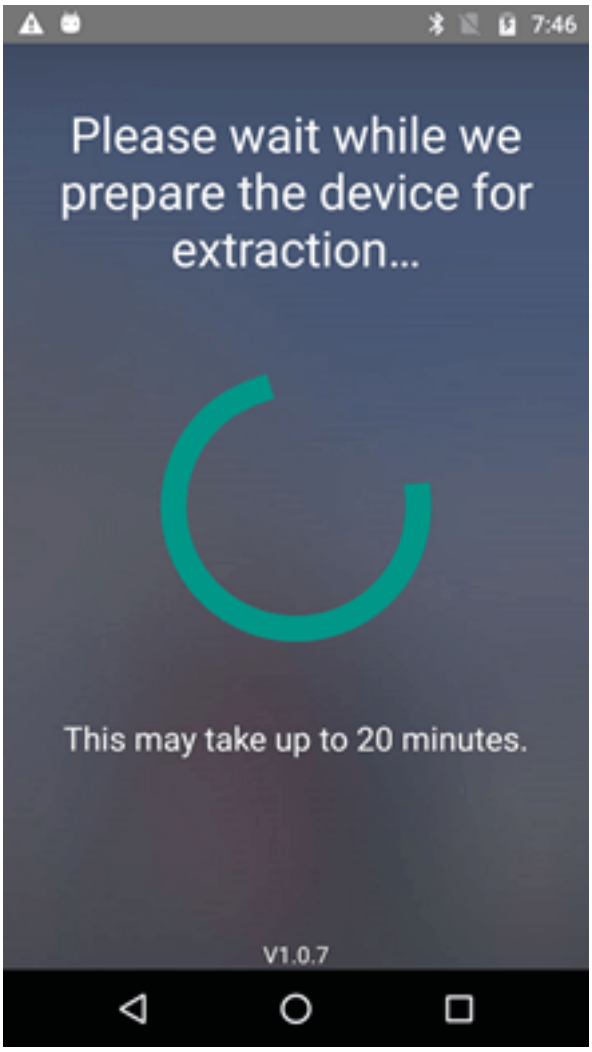


7. Click the relevant target storage. The following window appears.



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

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



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

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

10. If a **USB drive target** was selected, the following screen appears.

a. Follow the on-screen instructions:

i. Disconnect the device from UFED.

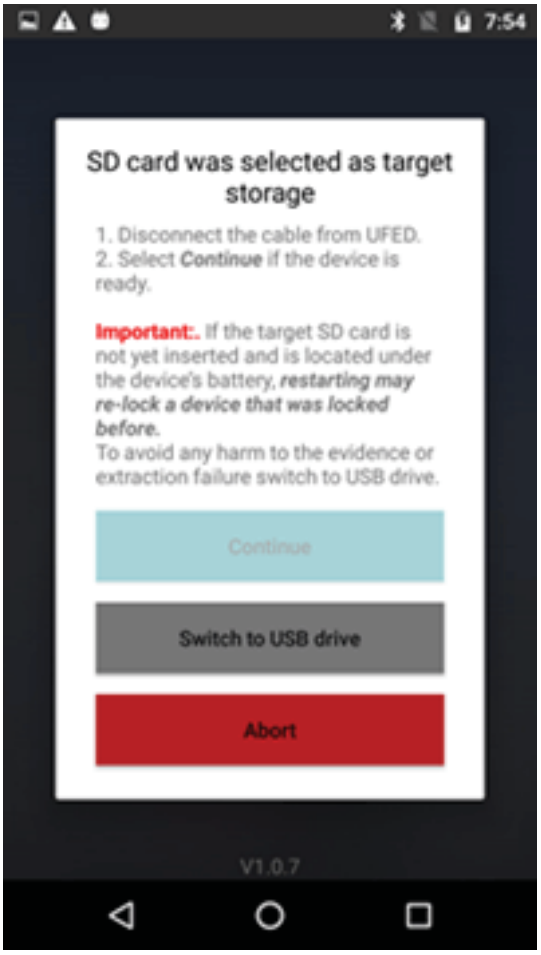
ii. Use the OTG cable to connect the source device to the USB drive.

> Selecting **Switch to SD card** will change the target type configuration.

> Selecting **Abort** will end the extraction process and will require a device restart.

b. Skip the SD card step.

c. If an **SD card target** was selected, the following screen appears.



a. Follow the on-screen instructions:

i. Disconnect the device from UFED.

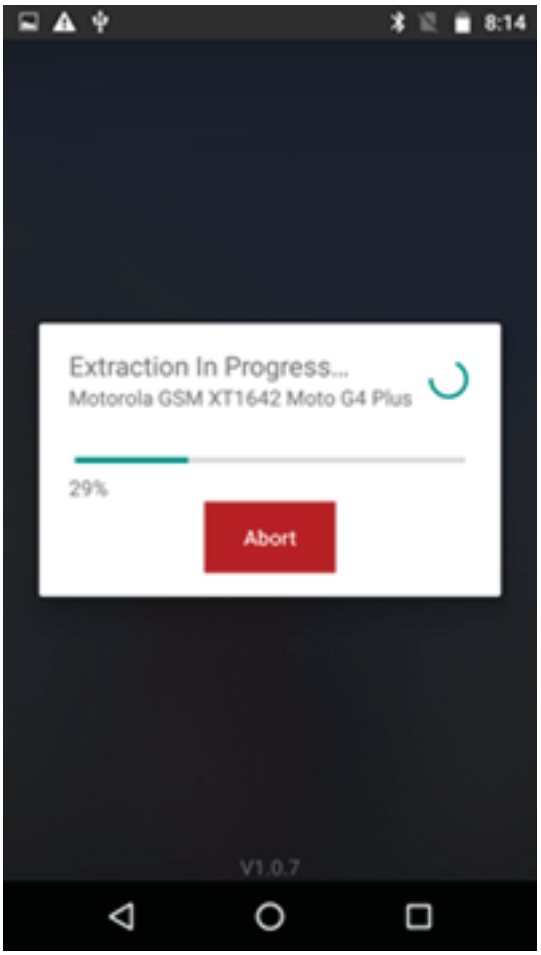
ii. If the target SD card is not yet inserted and is located under the device's battery, restarting may re-lock a device that was locked before. To avoid an extraction failure (for devices with OTG support), select Switch to USB drive.

Reminder: This target device requires A FAT32*/vFAT/exFAT format SD card with sufficient space for the extraction.

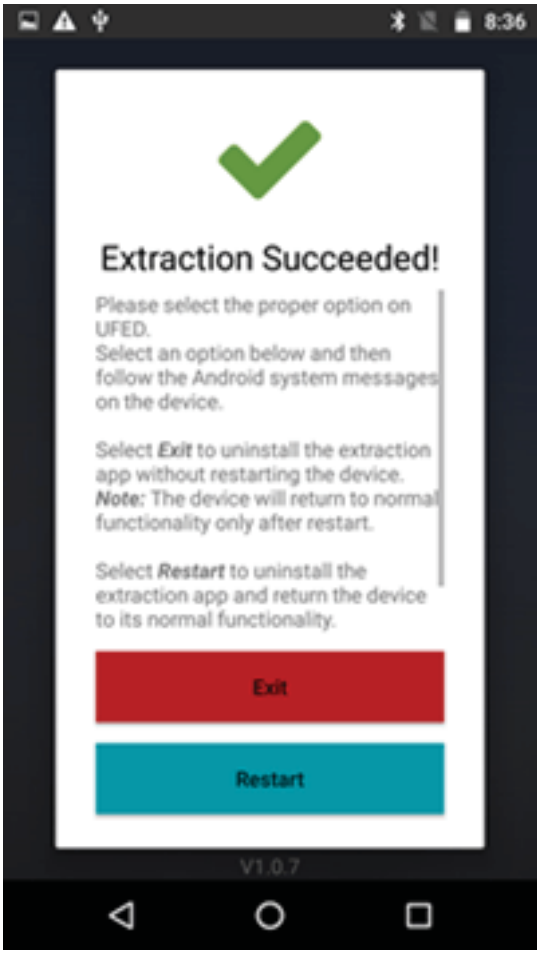
Selecting Switch to USB drive will change the target type configuration.

Selecting Abort will end the extraction process and will require a device restart.

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



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



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

> Restarting may re-lock a device that was locked before.

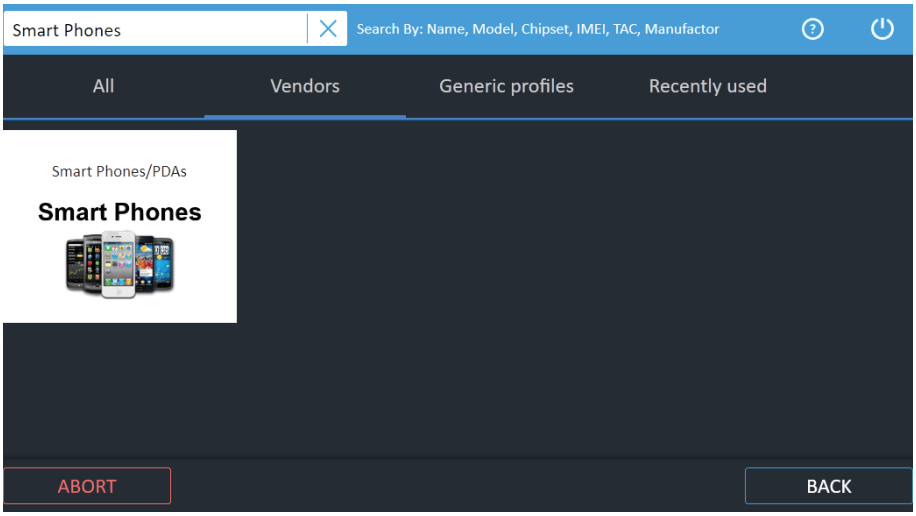
> The device will only return to normal functionality after restart.

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

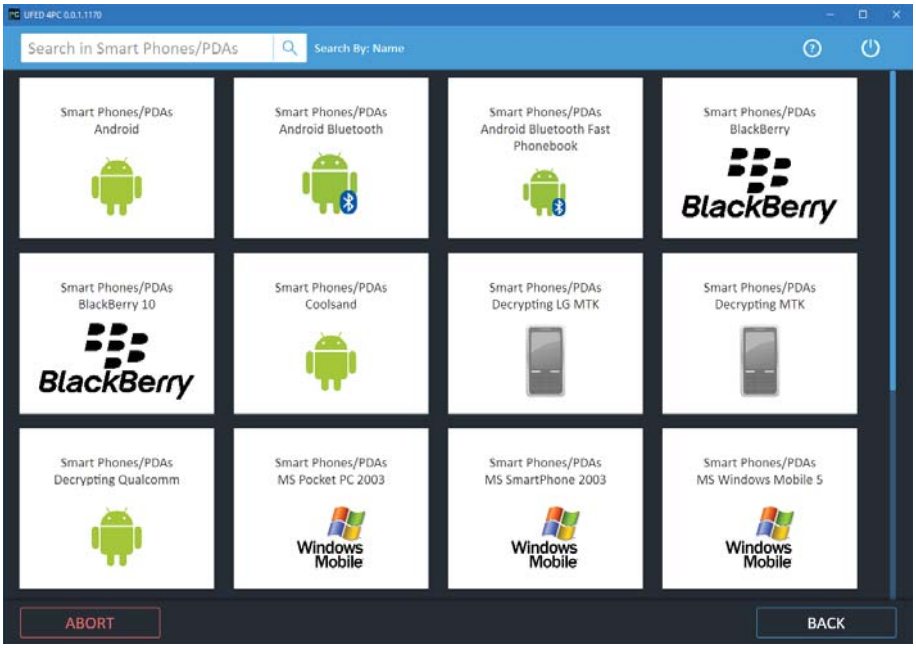
5.3.1. Generic model

To perform an Advanced ADB extraction:

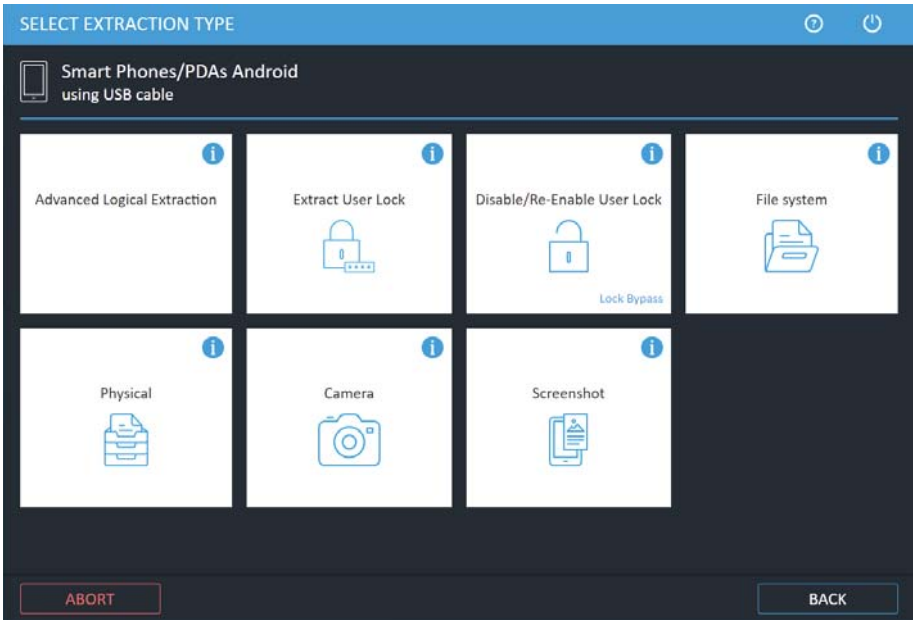
1. From the Home screen, click **Skip** > **Vendors** (tab) and search for "Smart Phones". The following window appears.



2. Click **Smart Phones**. The following window appears.



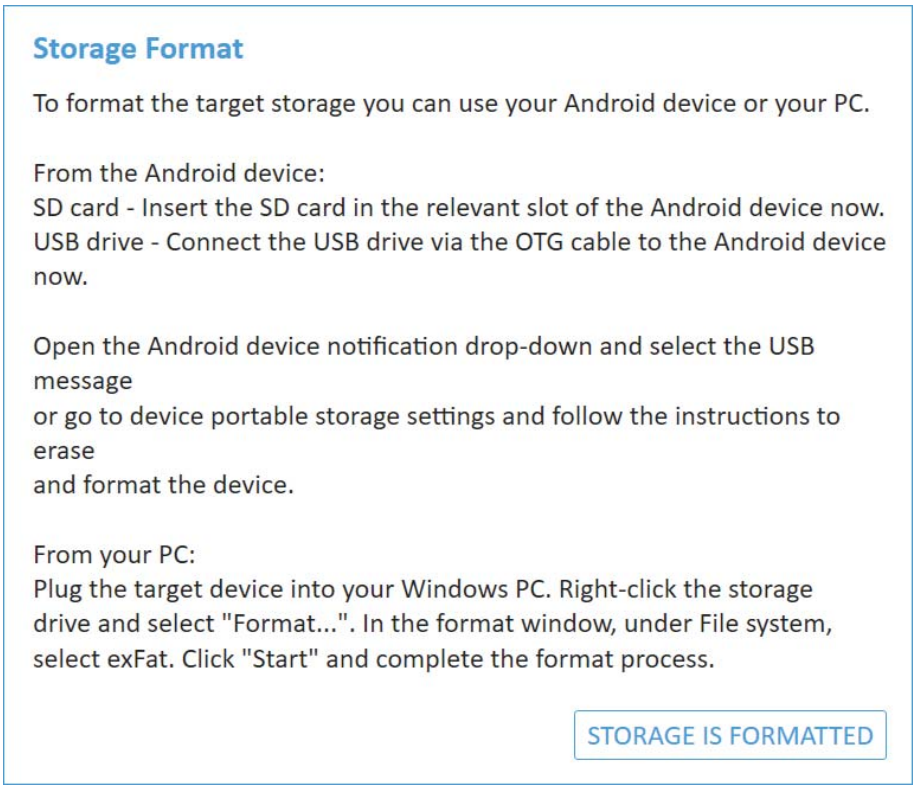
3. Click the relevant model. The following window appears.



4. Click **Physical**.
5. To continue, refer to Advanced ADB (on page 76).

5.3.2. Errors and notifications

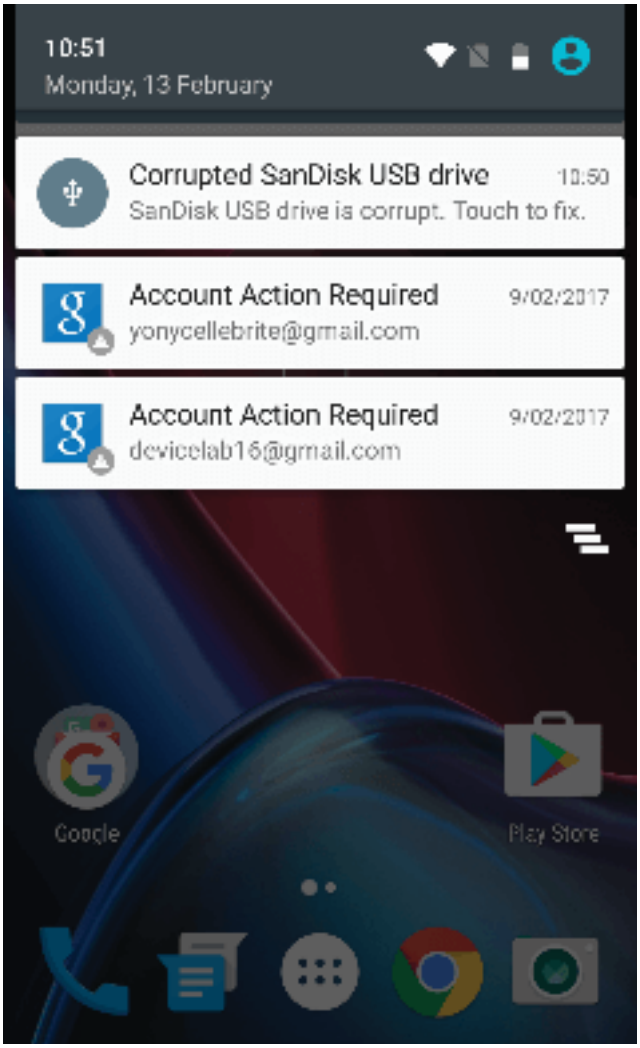
5.3.2.1. Disk format error



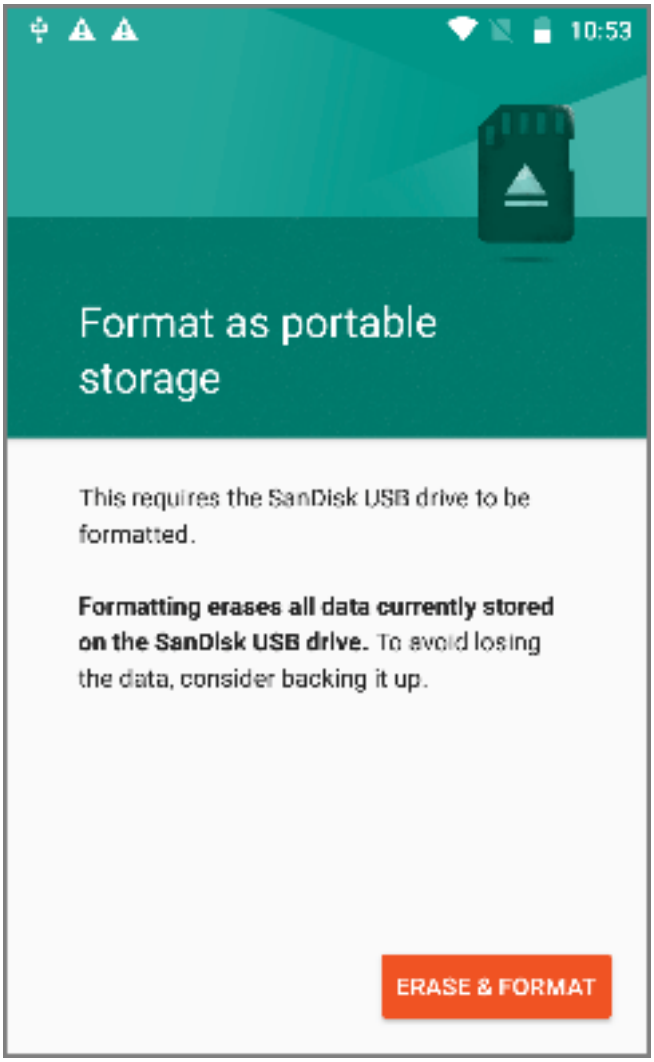
If you receive this error message, follow the instructions listed in the error message.

To format the storage device from the Android device:

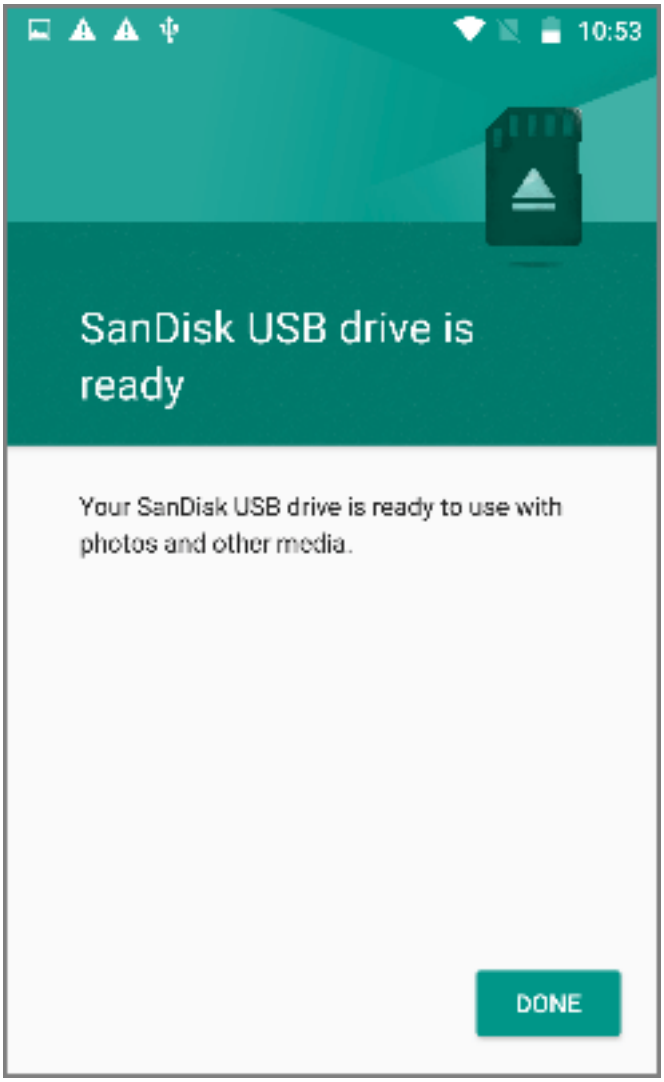
1. Open notification.



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

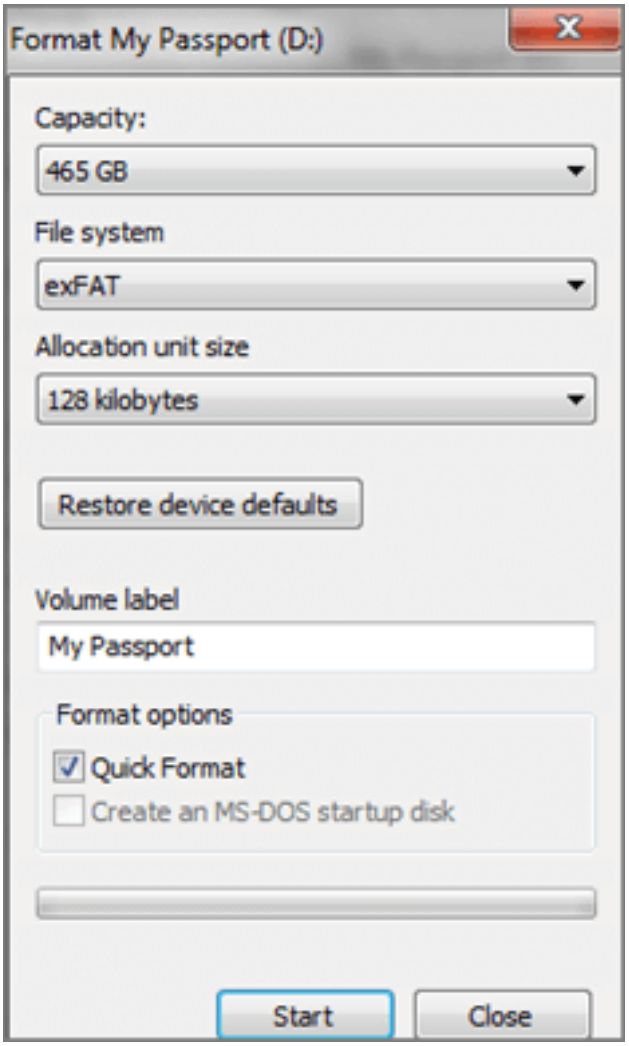


3. Follow the instructions to erase and format the device. Upon completion, the following screen appears.



To format the storage device from the PC:

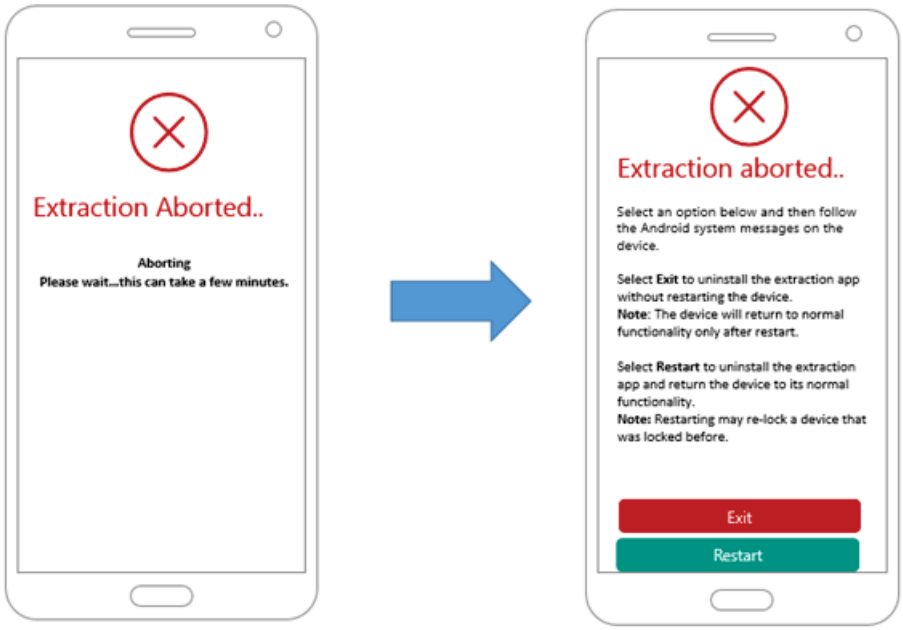
1. Plug the hard drive into your Windows PC. Right-click on the D drive and select "Format" The following window appears.



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

5.3.2.1.1. Extraction aborted

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



» Select **Exit** to uninstall the extraction app without restarting the device.

> The device will only return to normal functionality after restart.

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

> Restarting may re-lock a device that was locked before.

5.3.2.1.2. Extraction failed

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

» Select **Exit** to uninstall the extraction app without restarting the device.

> The device will only return to normal functionality after restart.

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

> Restarting may re-lock a device that was locked before.

5.4. Boot loader (FW flashing)

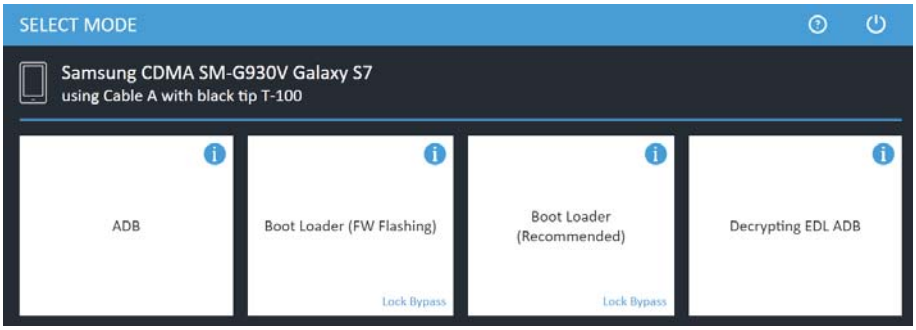
The Boot loader (FW flashing) extraction method uses boot loader reflashing, which enables a physical extraction while bypassing user lock (non-secure startup). This method is for Qualcomm-based Samsung Galaxy S7 devices running firmware version of Android 7.x. For a complete list of supported devices,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

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

To perform Boot loader (FW flashing):

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

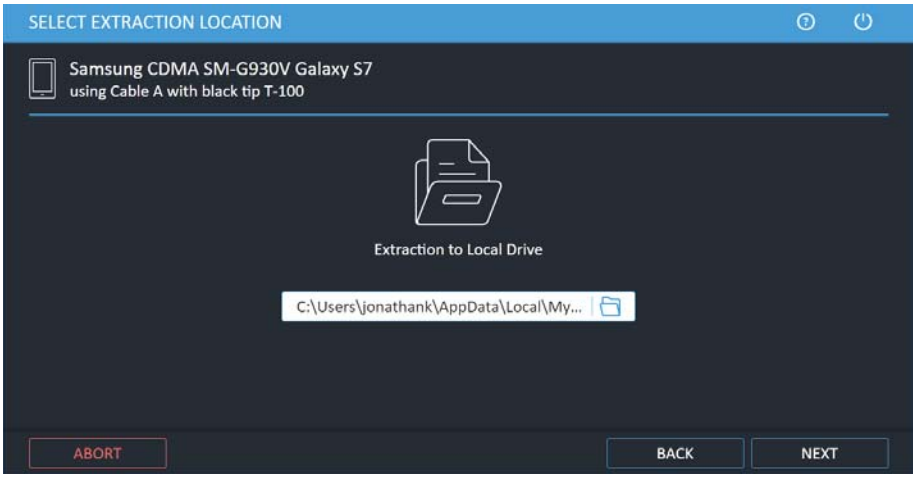
   The Select Mode screen appears:



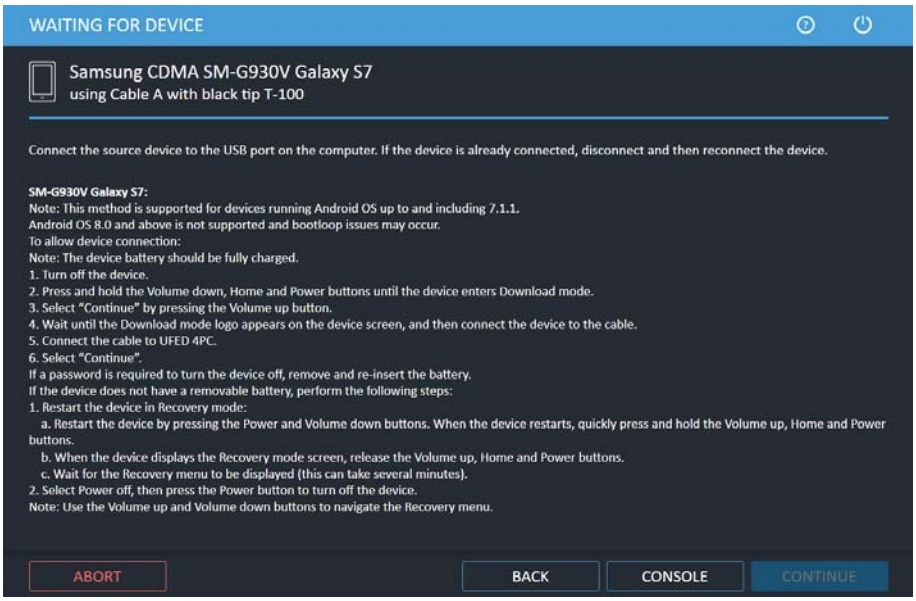
2. Select **Boot loader (FW Flashing)**.

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

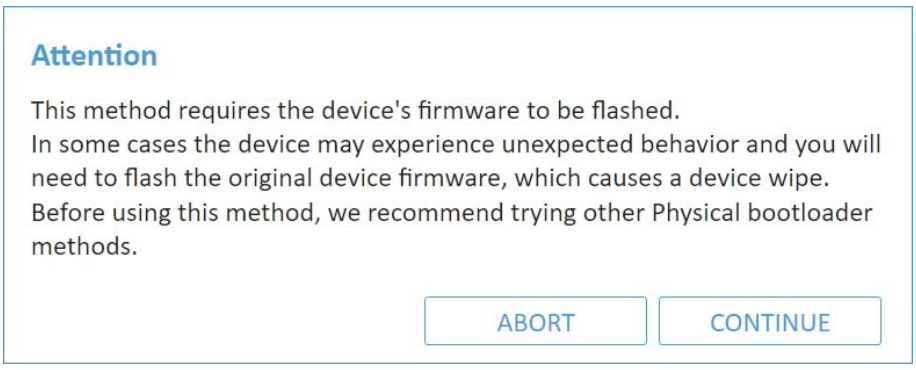
   The following Select extraction location window appears.



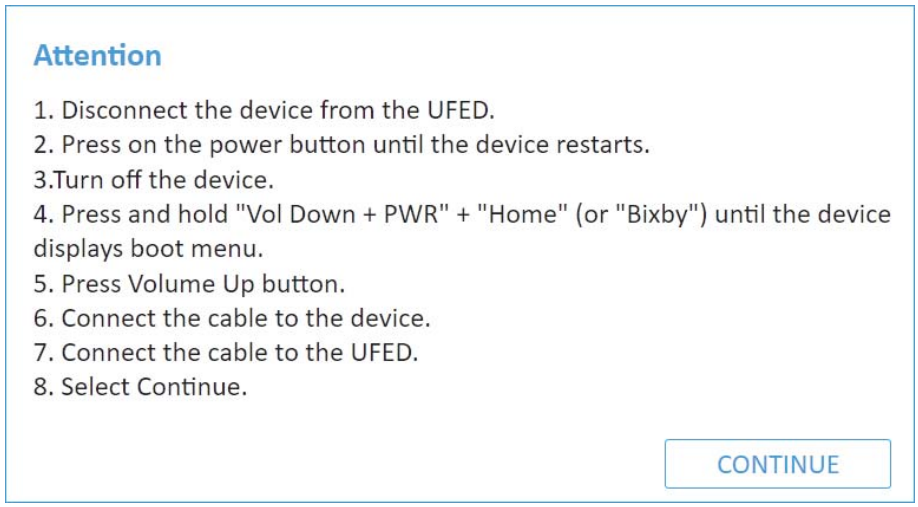
3. Select the extraction location. Click **Next**. The Waiting for Device screen appears.



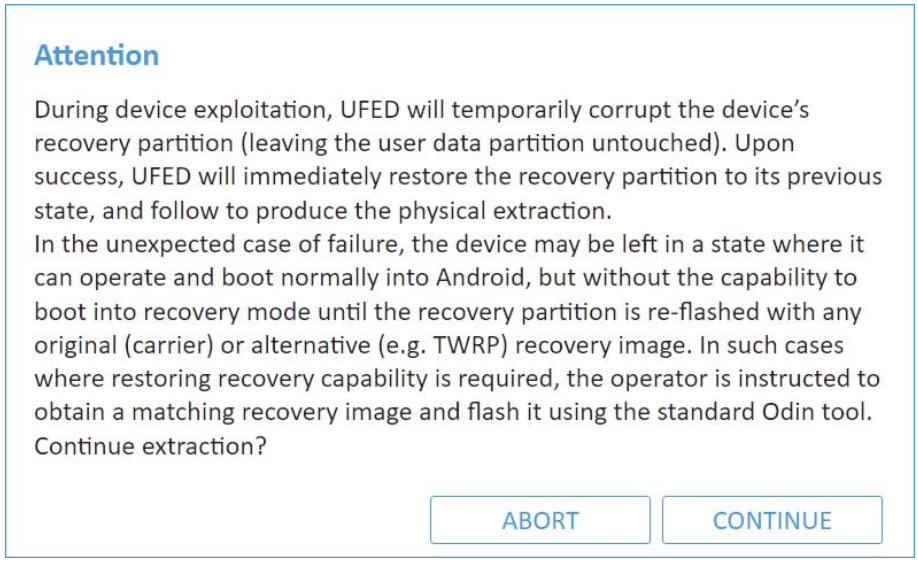
4. Follow the on-screen instructions to place the device in Download mode, then connect the required cable to the device and UFED.
5. Click **Continue**. The following window appears.



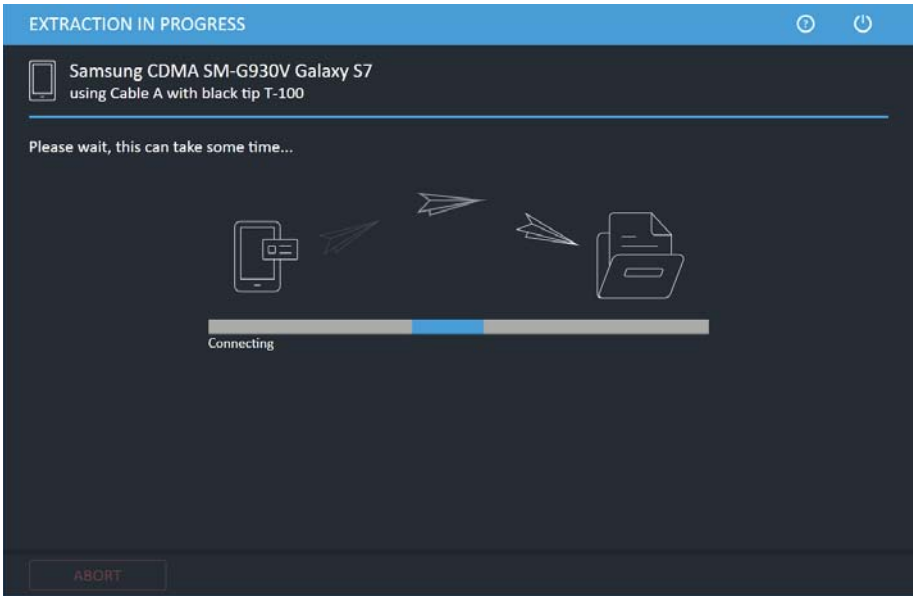
6. Click **Continue** to flash the device's firmware. The following window appears.



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



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



10. Follow any on-screen instructions.

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

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

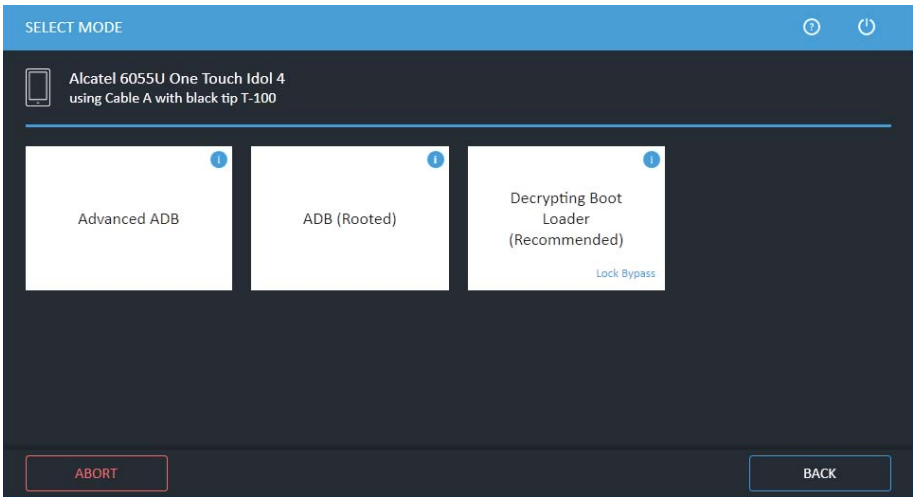
5.5. Decrypting boot loader

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

To perform a Decrypting boot loader extraction:

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

   The Select Mode window appears:

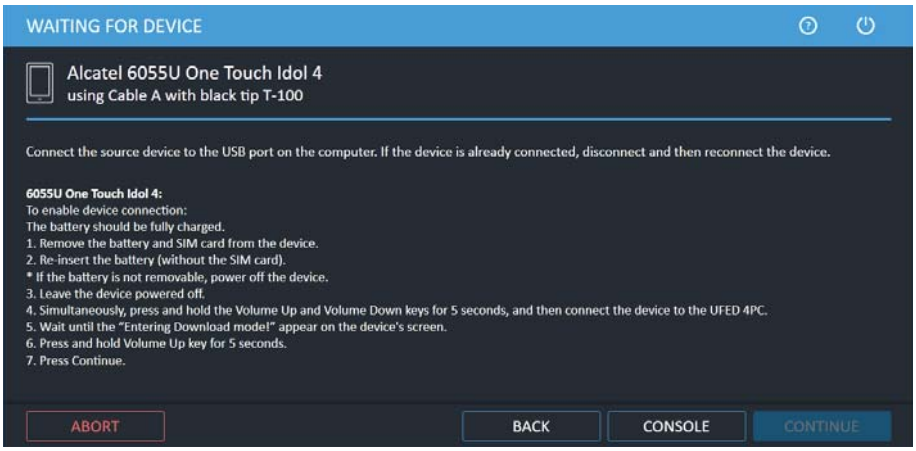


2. Click **Decrypting Boot Loader**.

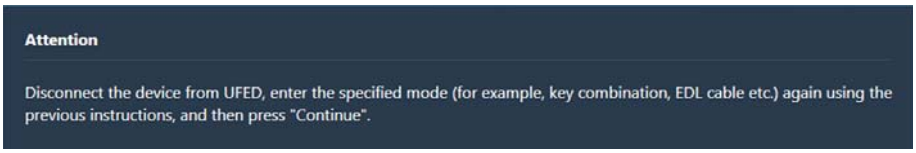
   > For information on using optional timeframe and party filters, refer to the *Overview Guide*.

   The Select Extraction Location window appears.

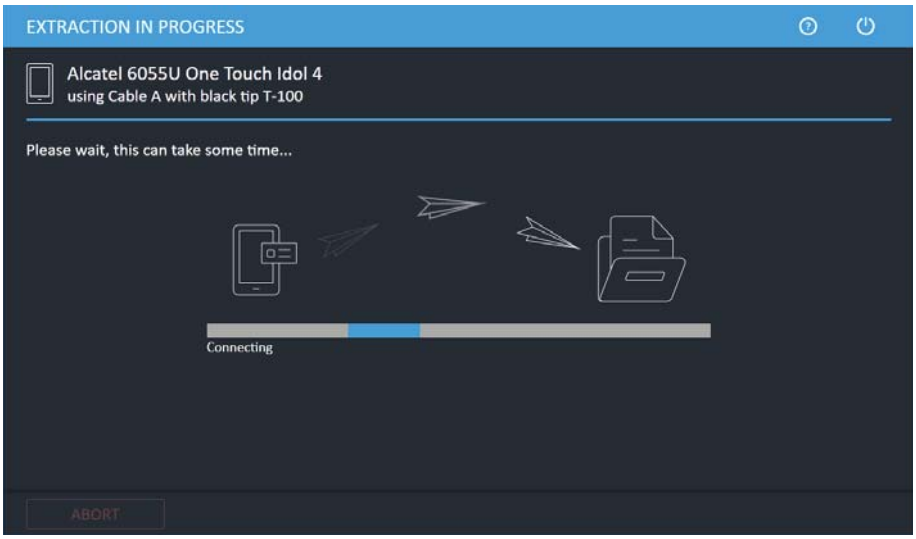
3. Select the extraction location. Click **Next**. The Waiting for Device window appears.



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



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



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

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

5.6. Forensic recovery partition

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

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

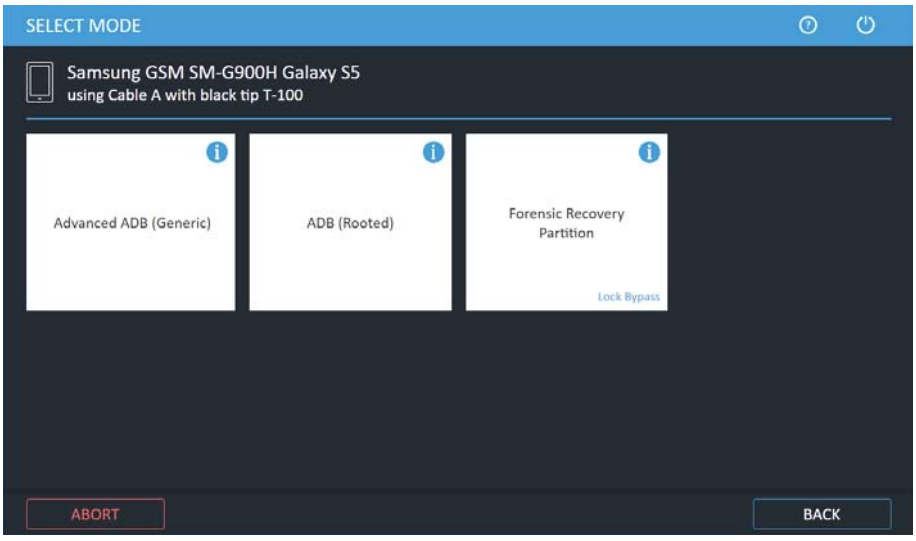
It is recommended to use the Forensic recovery partition method when other physical extraction msm-ethods (e.g., Bootloader) are not successful, or not available (e.g., if the Android firmware version is not supported).

If the device does not start correctly after using this extraction method, use the Exit Android Recovery Mode device tool. See Exit Android recovery mode (on page 137).

To perform a forensic recovery partition extraction:

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

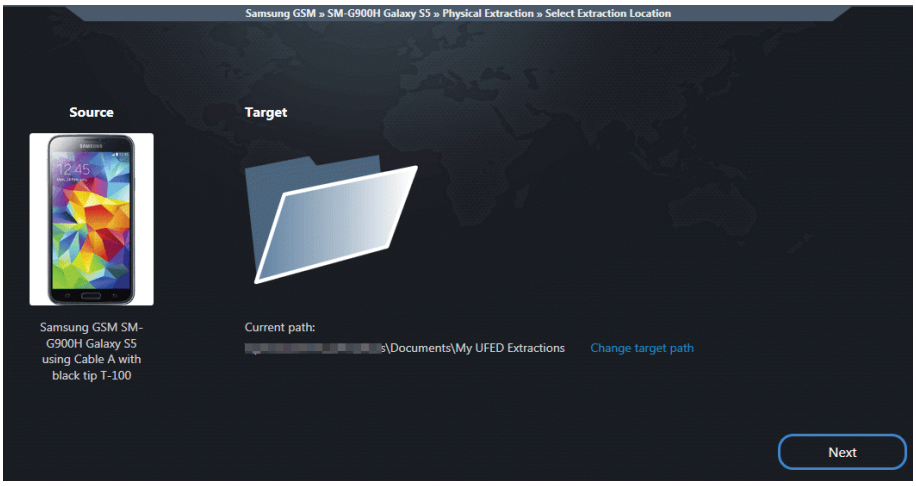
   The Select Mode screen appears:



2. Select **Forensic Recovery Partition**.

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

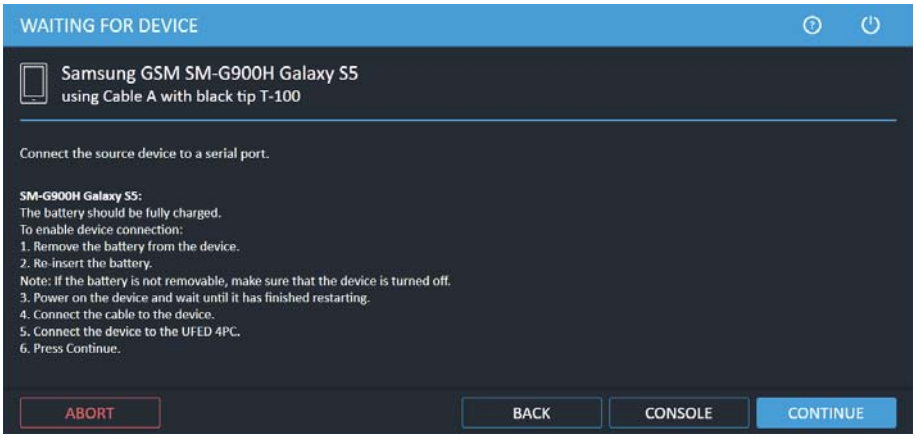
The following screen appears.



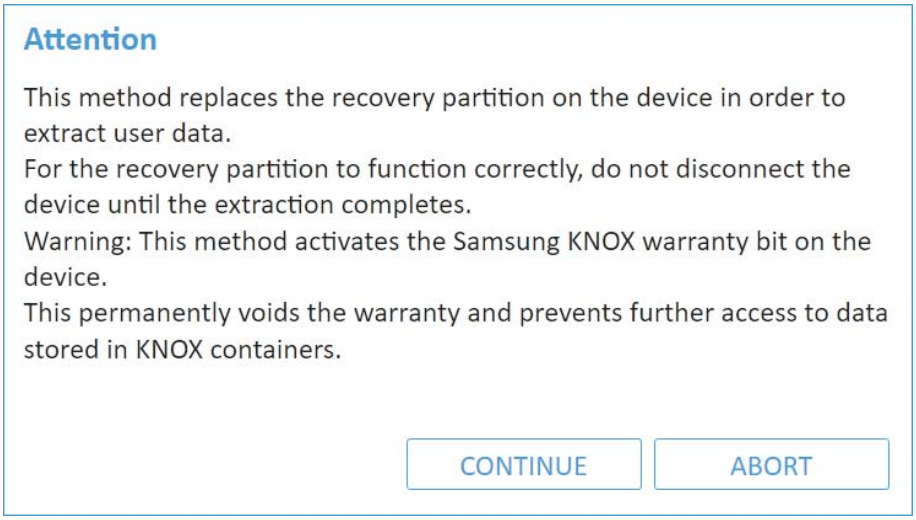
3. Click **Next**.

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

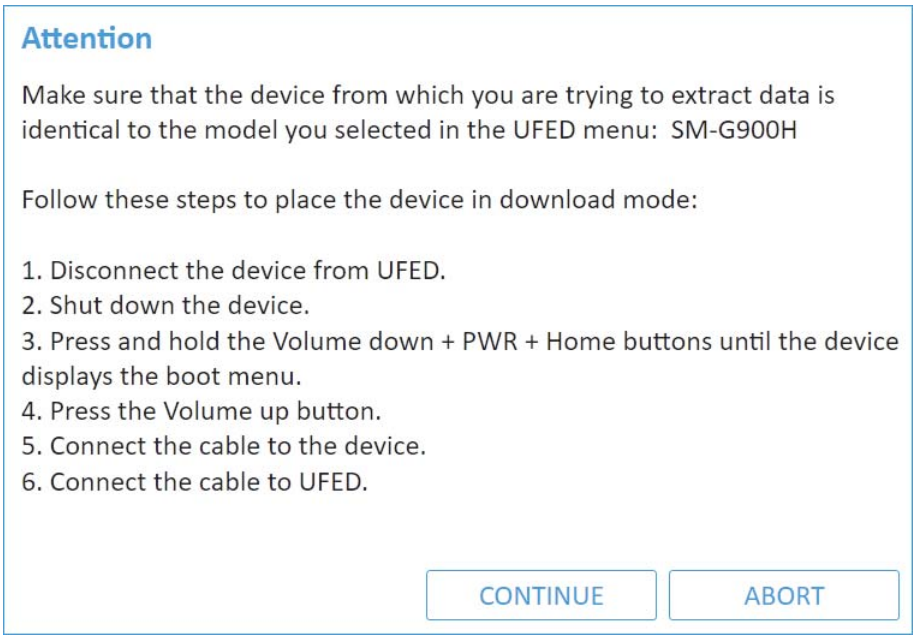
The Waiting for Device screen appears.



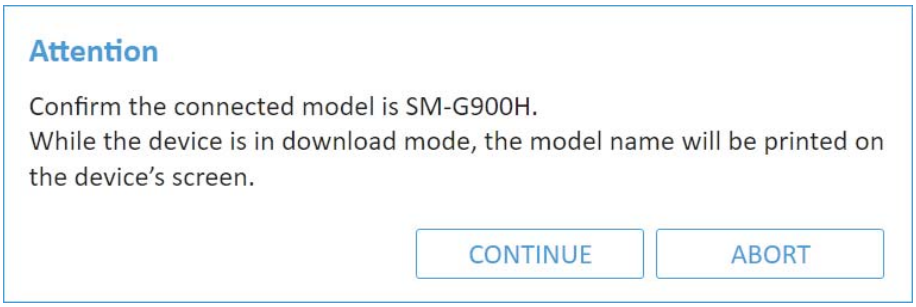
4. Click **Continue**. The following warning is displayed.



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

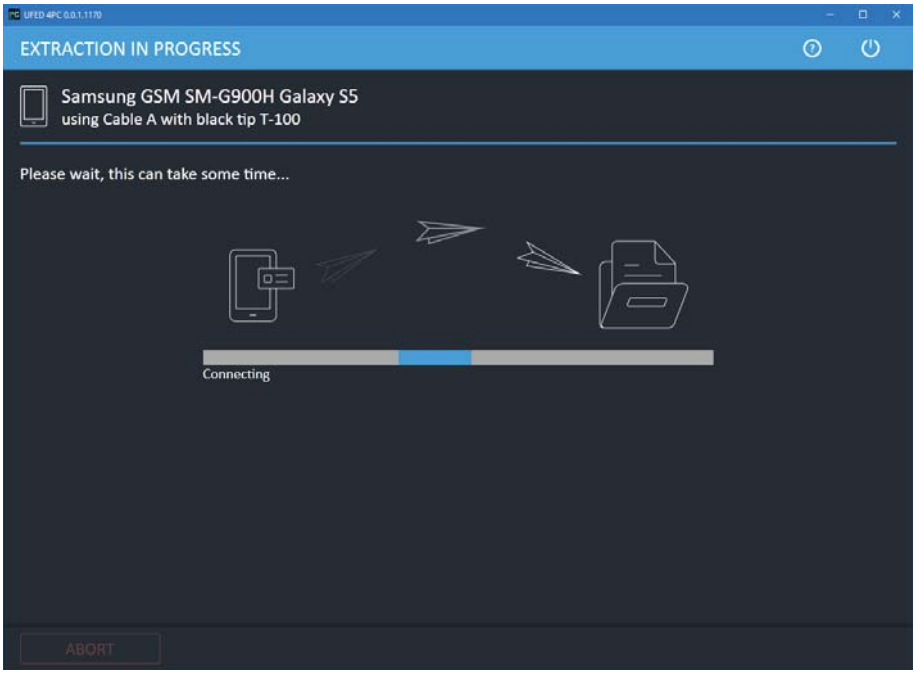


6. Click **Continue**. The following screen appears.



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

The Extraction in Progress screen appears.



9. Follow any on-screen instructions.

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

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

5.7. Smart ADB

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

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

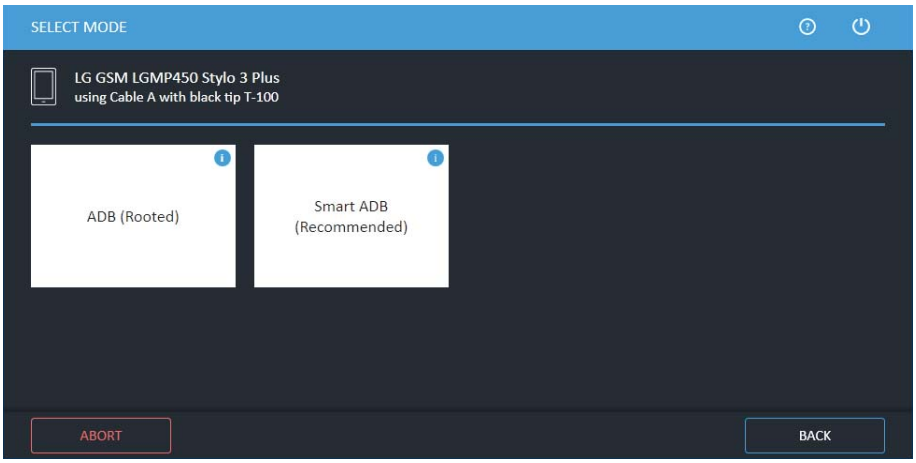
> It is recommended to place the device in Flight mode.

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

To perform a Smart ADB extraction:

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

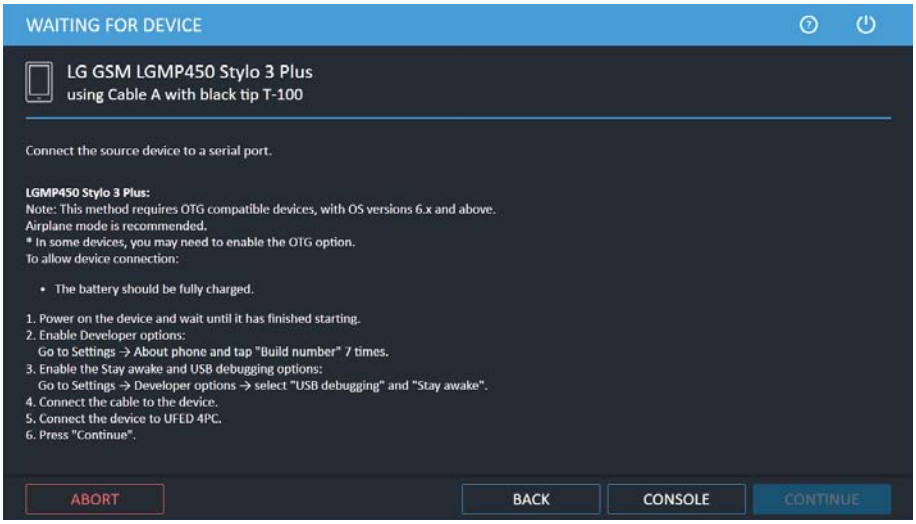
   The Select Mode screen appears:



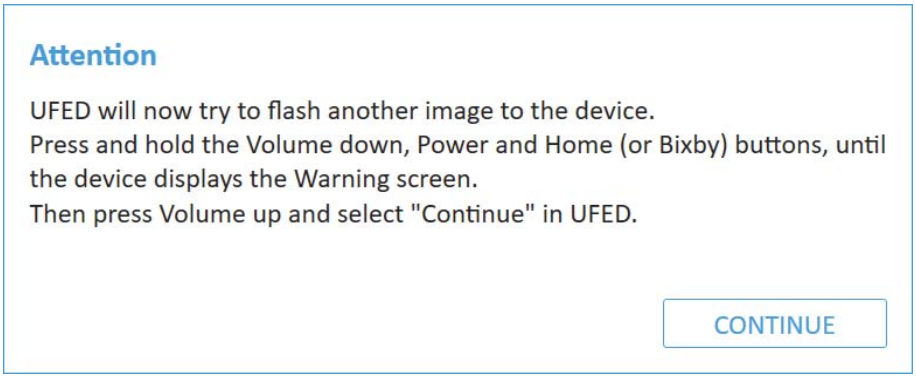
2. Click **Smart ADB**.

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

   The Waiting for Device screen appears.



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



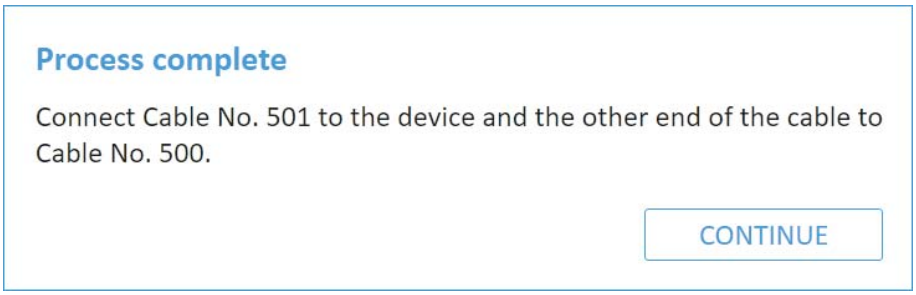
4. Click **Continue**. The following window appears.

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

The initializing stage can take up to 30 minutes.

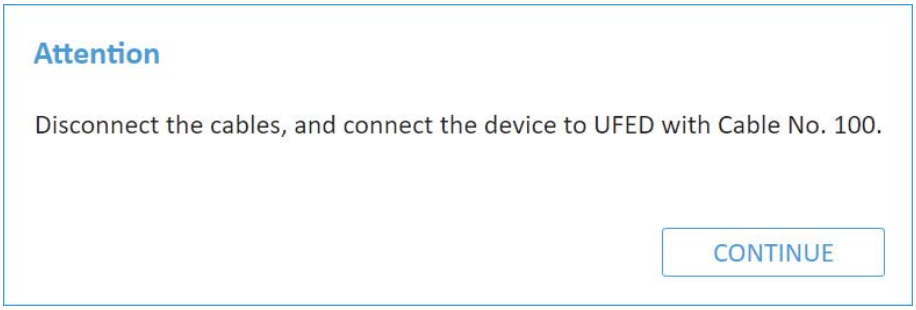
If required, this process flashes new firmware to the cable. You can also use the Flash Cable 500 Firmware (on page 137) tool.

The following window appears.

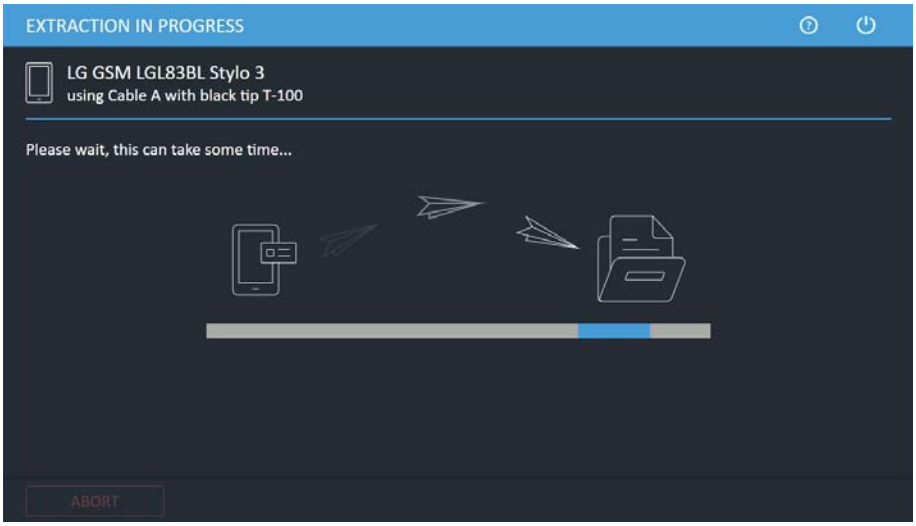


6. Connect Cable No. 501 (or other specified cable) to the device and the other end of the cable to Cable No. 500, then click **Continue**. The initialization process starts.

   The following window appears.

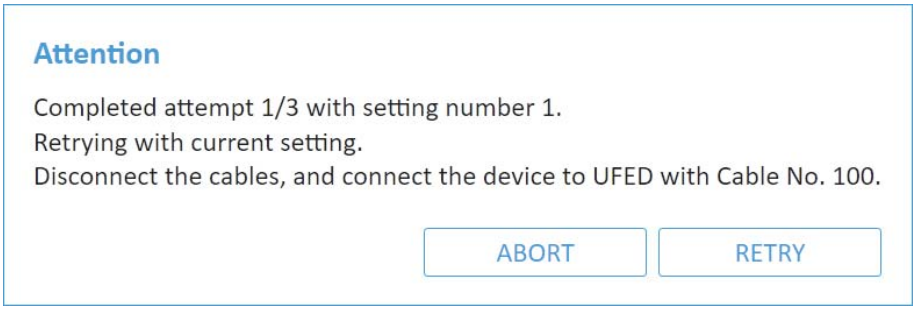


7. Disconnect Cable No. 500 and reconnect the device using Cable No. 100 (or other specified cable). Click **Continue** to start the extraction. The following window appears.



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

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



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

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

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

6. Capture images and screenshots

The UFED camera enables you to collect evidence by taking pictures or videos of a device (see Capturing images (on the next page)). You can also use a Screenshot feature to capture internal screenshots directly from a Blackberry, Android or iOS device (see Capturing screenshots (on page 113)). Both these options can be useful as complimentary evidence or in instances when data cannot be extracted from a device. You can add notes, categories and bookmarks to the pictures and videos, which will be visible in 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.

6.1. The UFED camera

The UFED camera is offered as an add-on and it is controlled by the UFED. 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.

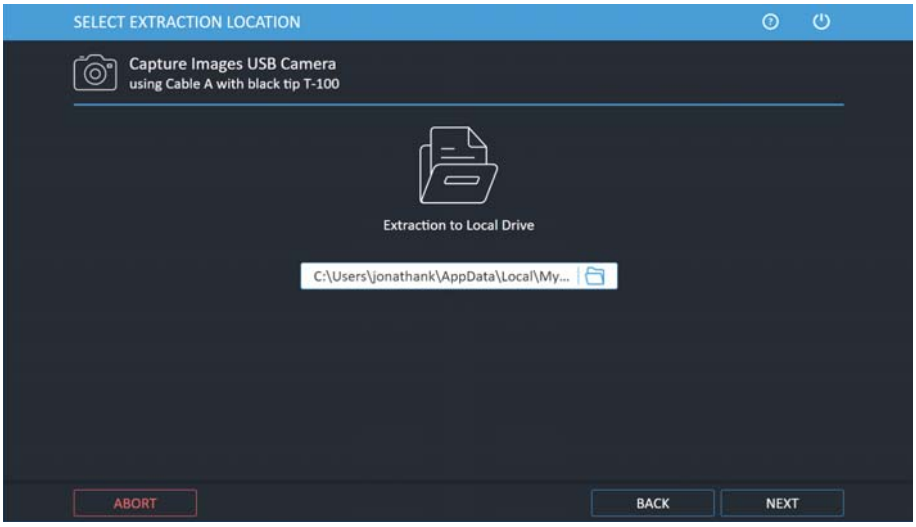
6.2. Capturing images

You can take pictures or videos of a device.

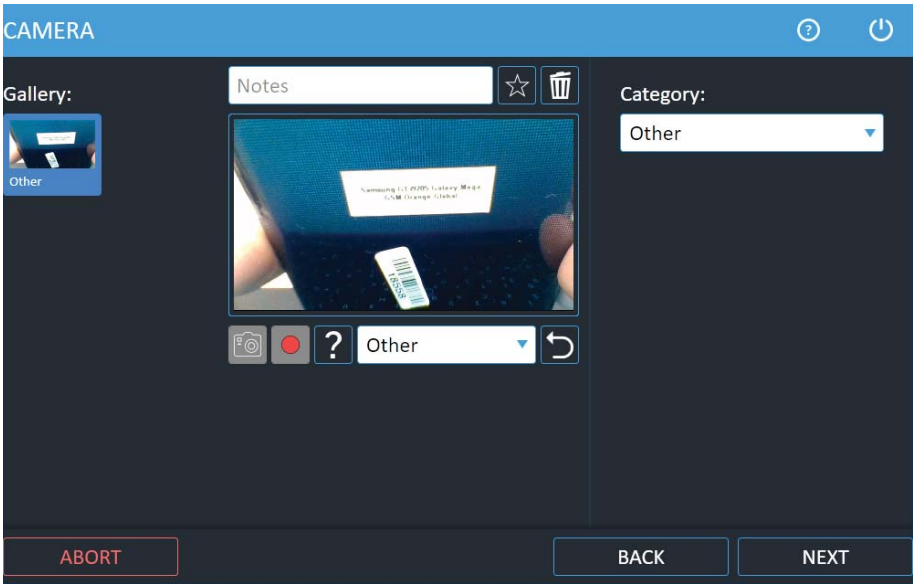
To capture images or videos:

1. Click **Camera**.

   The Select Extraction Location screen appears.



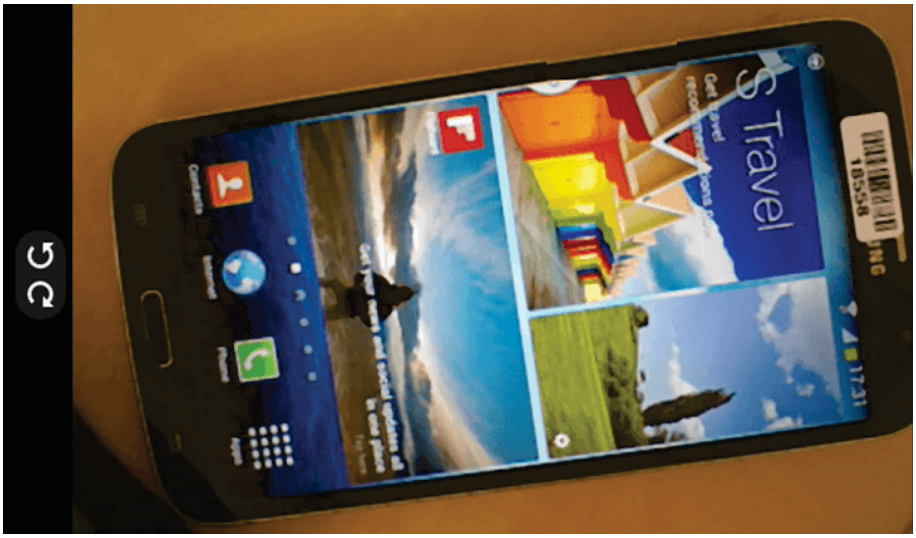
2. If required, click **Change** target path to select an alternate save location. A folder for this extraction will be created in this location and will include the images (snapshots), videos, UFD file, index file, and report file.
3. Click **Next**.
4. Connect the UFED camera to a USB port on the computer.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



5. Do one of the following:

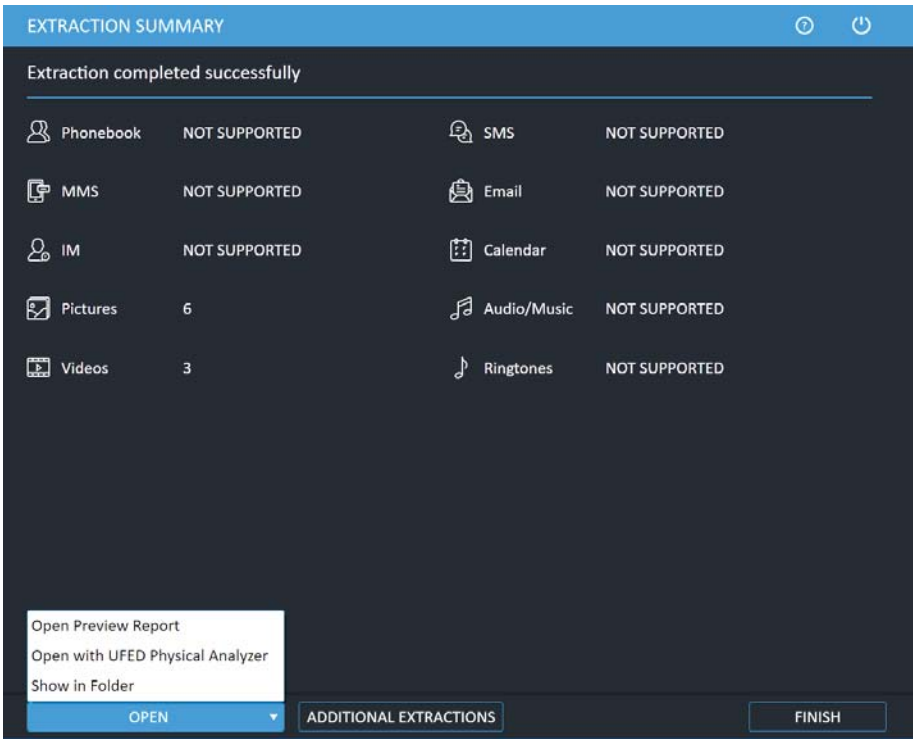
   - Click  to start a video recording and click  to stop the video recording.
   - Click  to take a picture.
   - Click **Other** to change the default category. Images and videos will be displayed in UFED Physical/Logical under these categories.
   - Click an image or video, to add notes, bookmarks (), categories (), or delete the file (). Click  to move back to live view.

> 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 **Next** to continue.

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



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

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

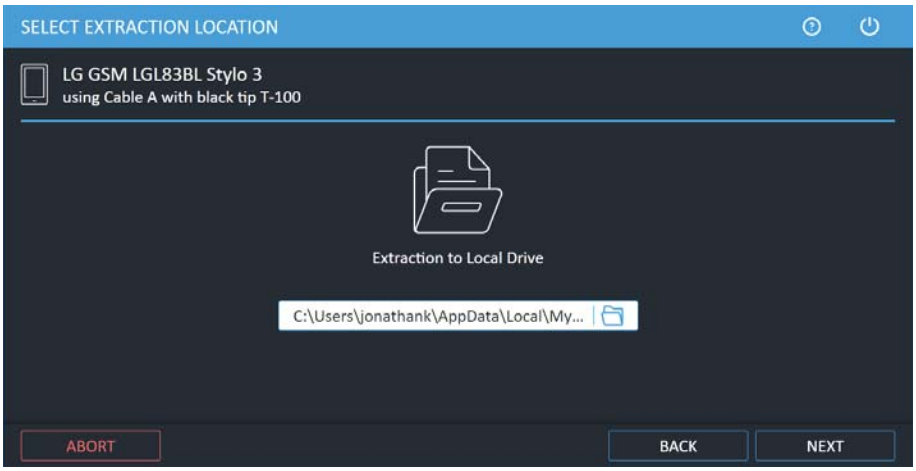
6.3. Capturing screenshots

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

To capture screenshots from the devices:

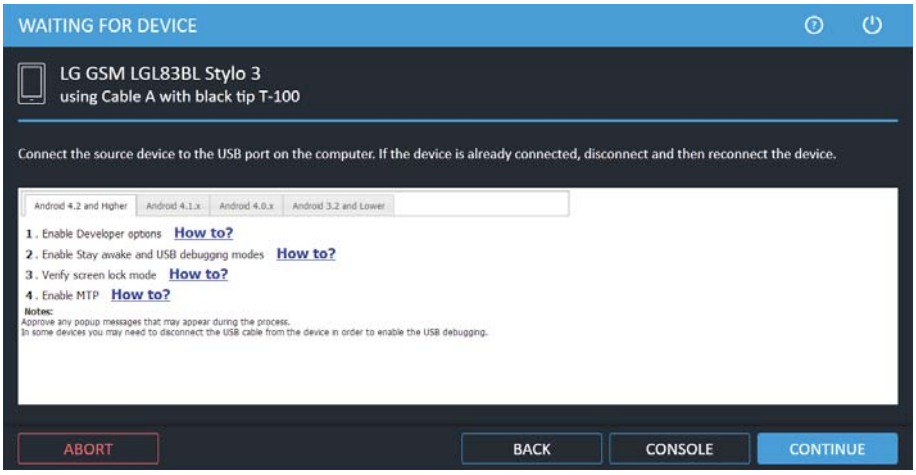
1. Click **Mobile device** and identify the device, then click **Screenshots**.

   The Select Extraction Location screen appears.



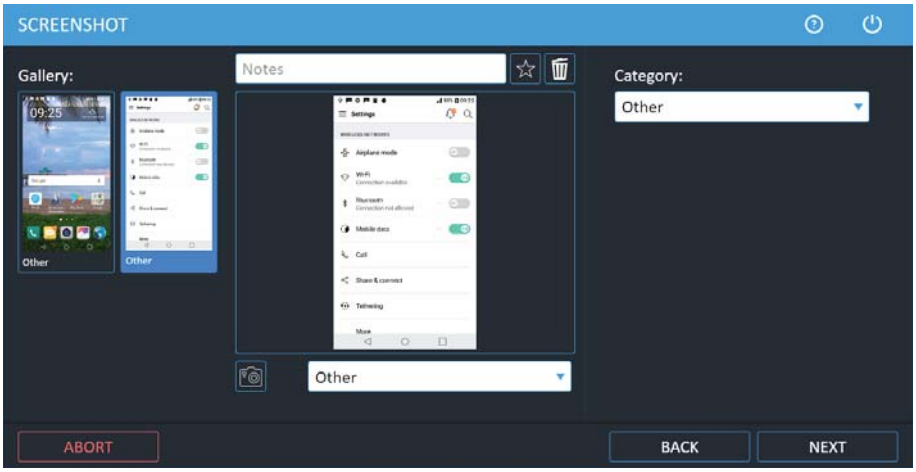
2. If required select an alternate save location, and click **Next**.

   The Waiting for Device screen appears.



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

   The Screenshots screen appears.



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

7. SIM card functionality

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

- Sim data extraction
- Clone SIM
- File system extraction

7.1. SIM data extraction

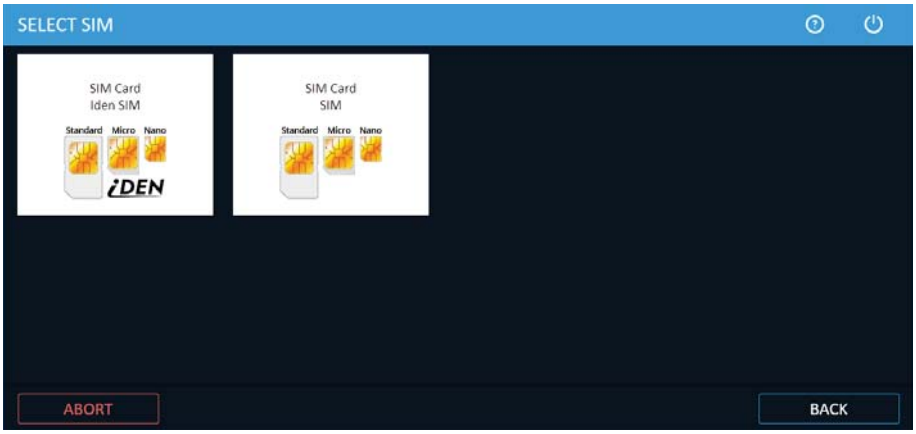
The SIM Data Extraction function enables you to perform logical extraction from a SIM or USIM card.

7.1.1. Performing SIM data extraction

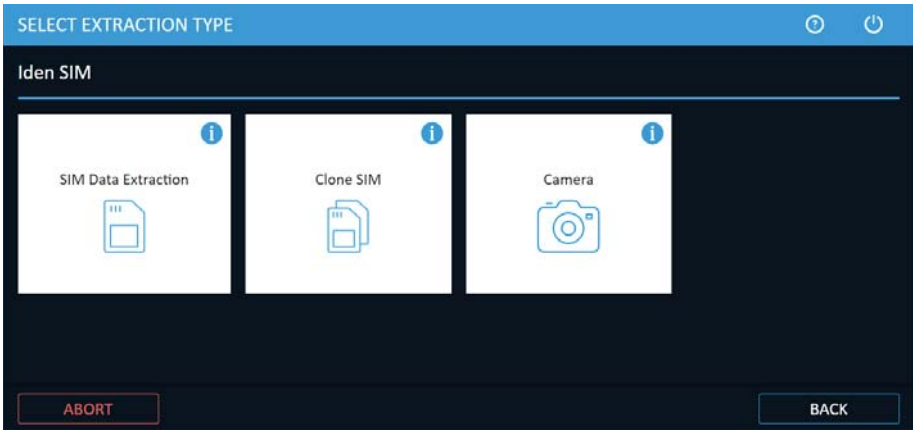
The following example is performed using a SIM Card.

To perform the SIM Data Extraction:

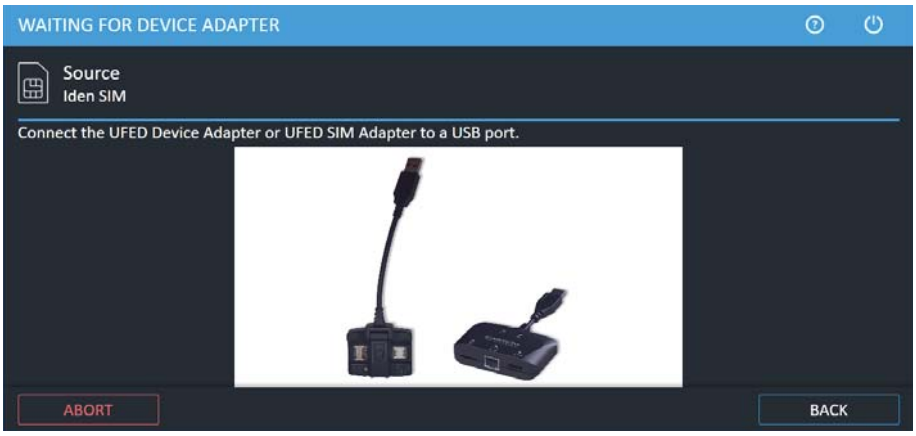
1. Click **SIM Card**. The following window appears.



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

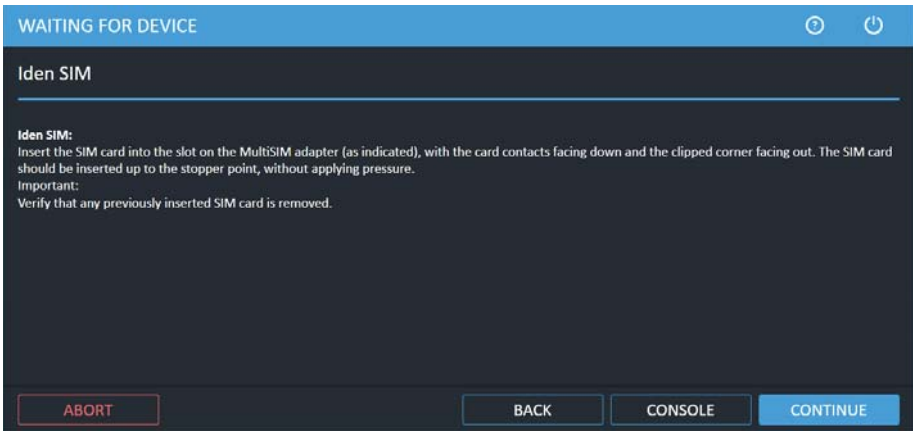


3. Click **SIM Data Extraction**. The Select Extraction Location window appears.
4. Select the extraction location and tap **Next**. The following window appears.

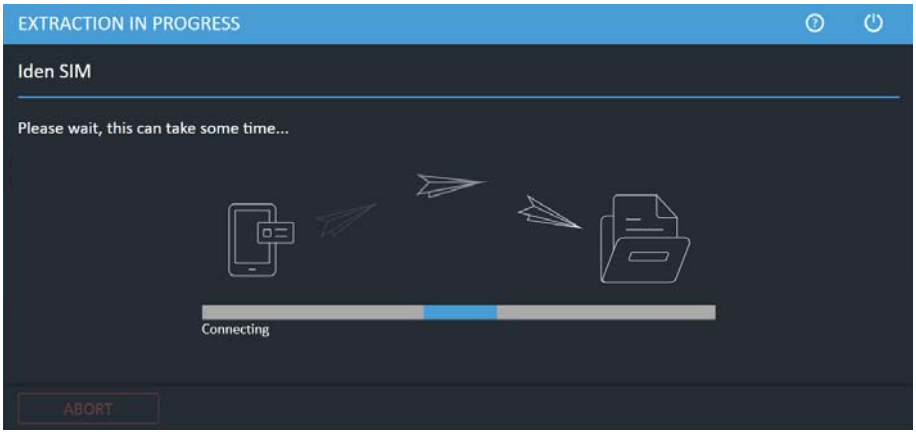


5. Connect the UFED Device Adapter or UFED SIM Adapter to a USB port.

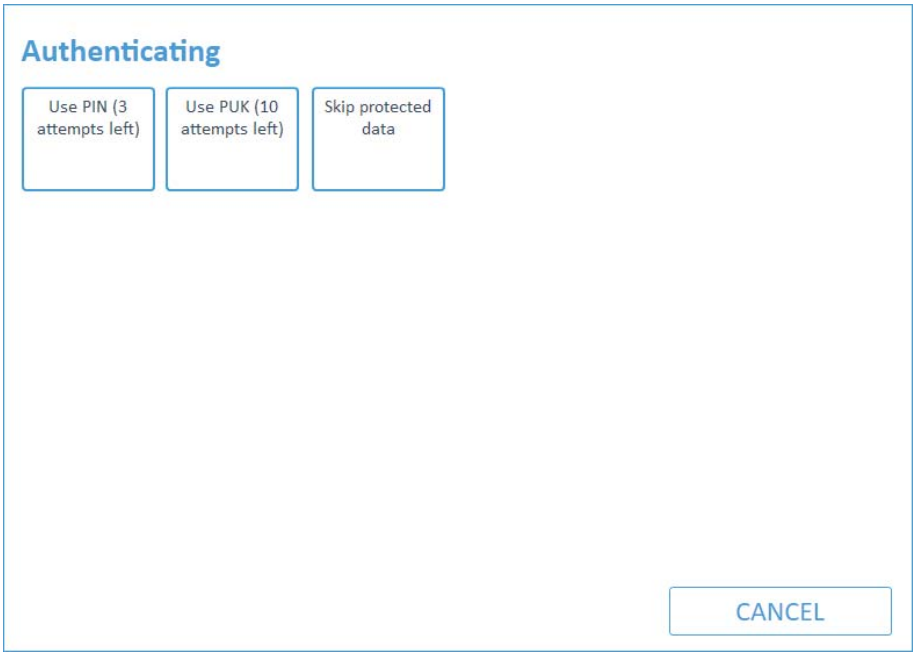
   The Waiting for Device screen appears.



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

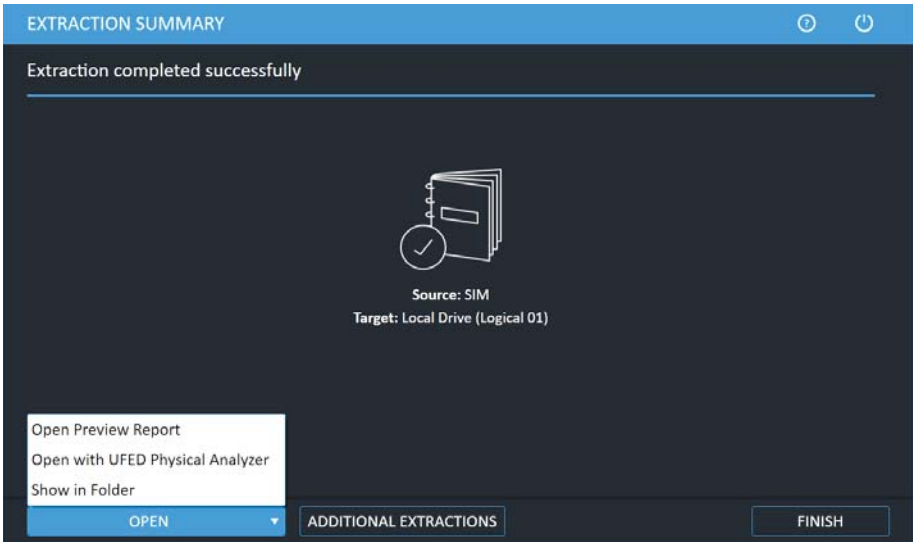


   The following window appears.



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

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



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

7.1.1.1. The extracted SIM data folder

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

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

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

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

7.2. 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:

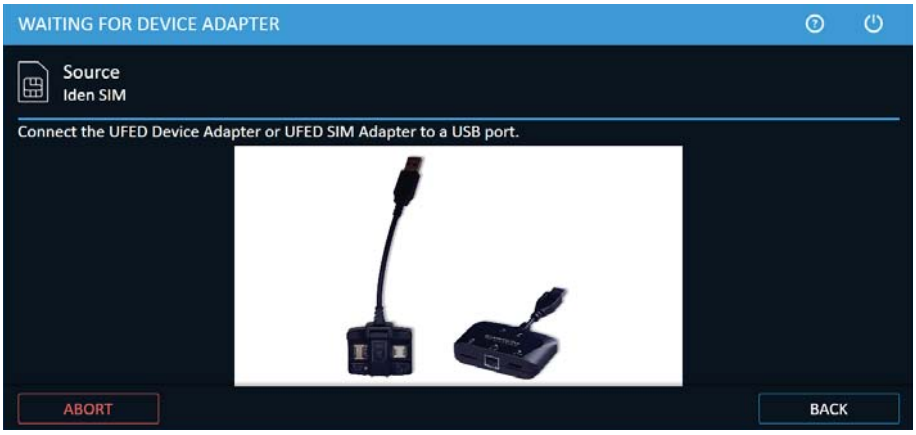
- While preventing the cellular device from connecting to the network, rendering the device invisible to the network without the ability to send or receive calls or SMS messages, and thereby preserving the device's current information. (No Faraday Bag is required to block RF signals).
- When the original 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:

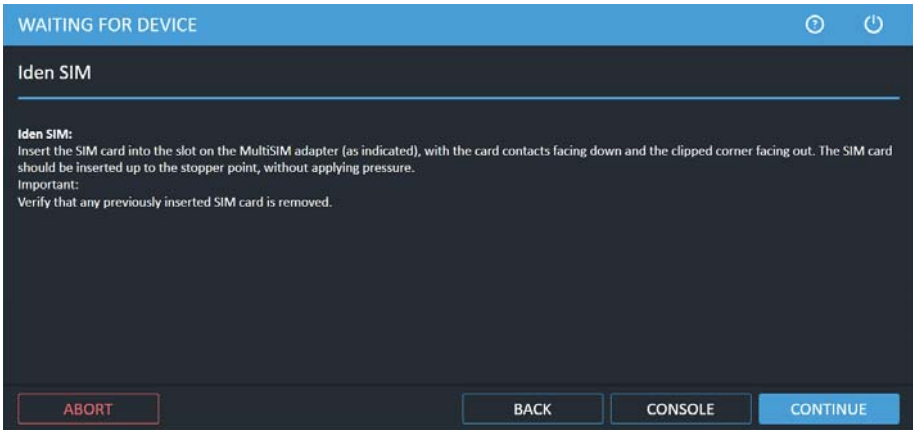
- Clone an existing SIM card - to create a cloned SIM to use to extract device data without a network connection. See Cloning an existing SIM card ID (below).
- Manually enter SIM data - to manually program the ICCID and IMSI to the cloned SIM card. See Entering SIM data manually (on page 125).
- Create 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 a GSM test SIM (on page 129).

7.2.1. Cloning an existing SIM card ID

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



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



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

If you are using the UFED Device Adapter:

These instructions are for the previous version of the UFED Device Adapter. As displayed in the picture below:

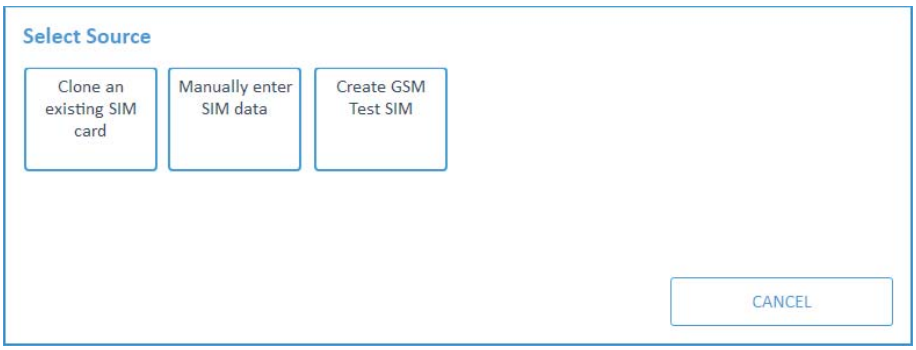
1. Insert the MultiSIM adapter into the port marked SIM.
2. Insert the SIM card into the slot on the MultiSIM adapter, with the card contacts facing down and the clipped corner facing out. The SIM card should be inserted up to the topper point, without applying pressure.
3. Tap **Continue** and follow the instructions (To select the source and clone the SIM card: (on page 123))

If you are using the UFED SIM Adapter:

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

To select the source and clone the SIM card:

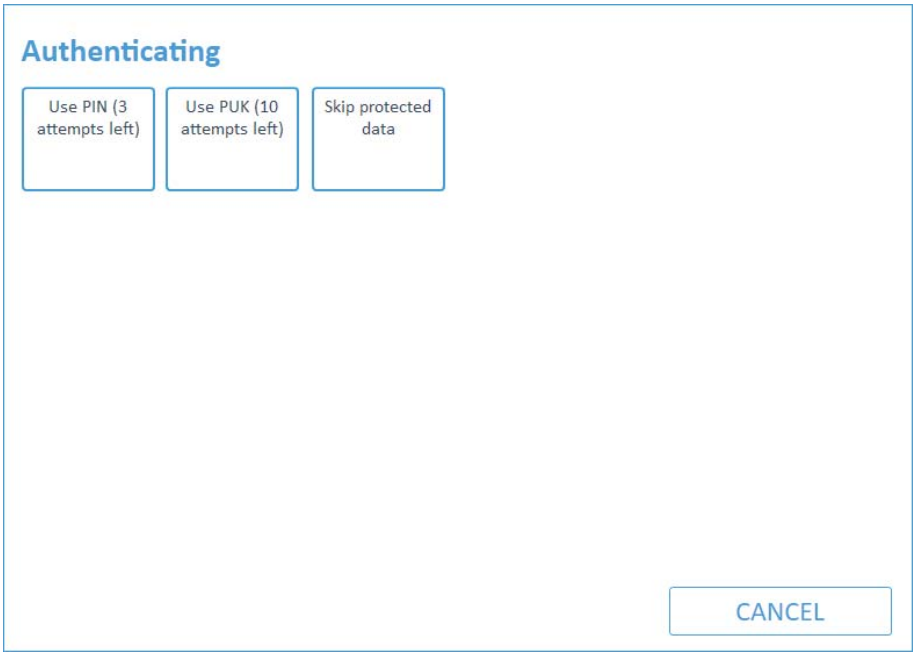
The **Select Source** screen appears.



4. Click **Clone an existing SIM card**.

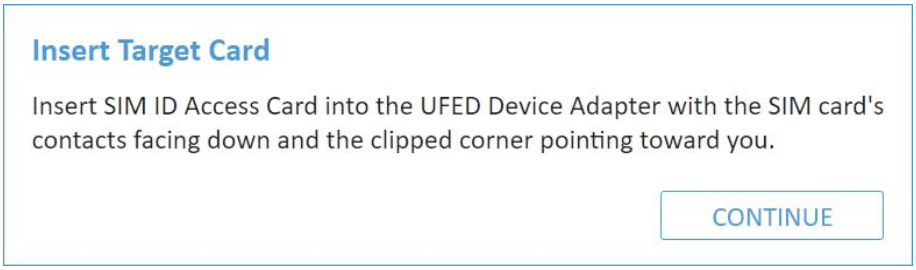
   The Clone SIM ID prompt appears.

5. Check that the right SIM was inserted into the SIM card reader slot.
6. Click **Continue.** The following window appears.



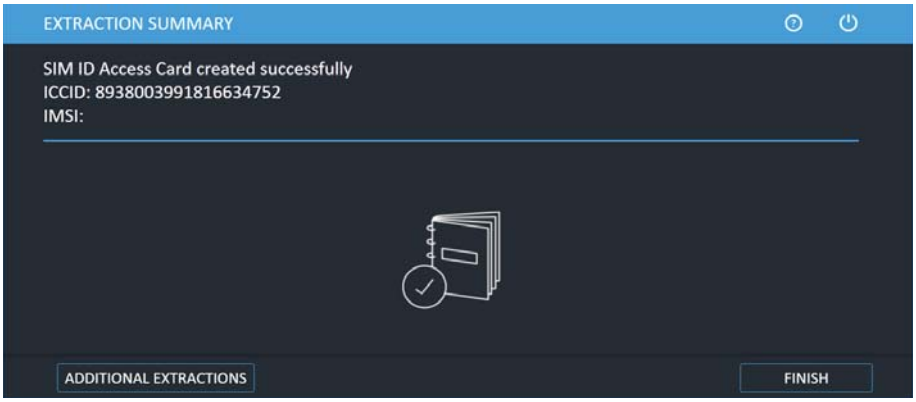
7. Click **Use PIN**, **Use PUK** or tap **Skip protected data**. The Extraction in Progress Source screen appears.

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



8. Remove the original SIM card from the SIM card reader.
9. Insert a UFED SIM ID Access Card into the SIM slot.
10. 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.



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

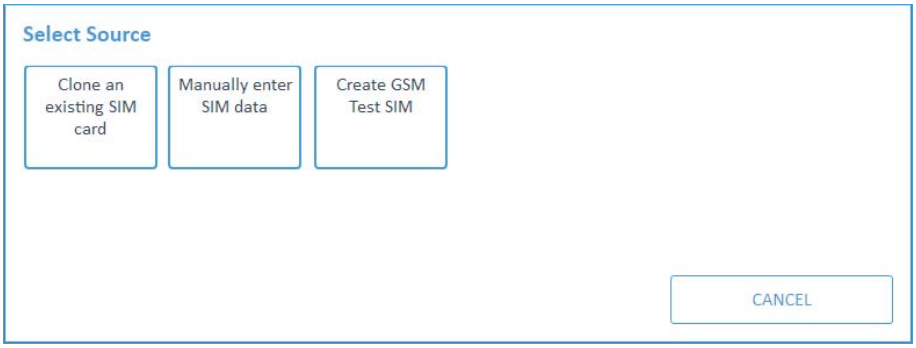
7.2.2. Entering SIM data manually

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

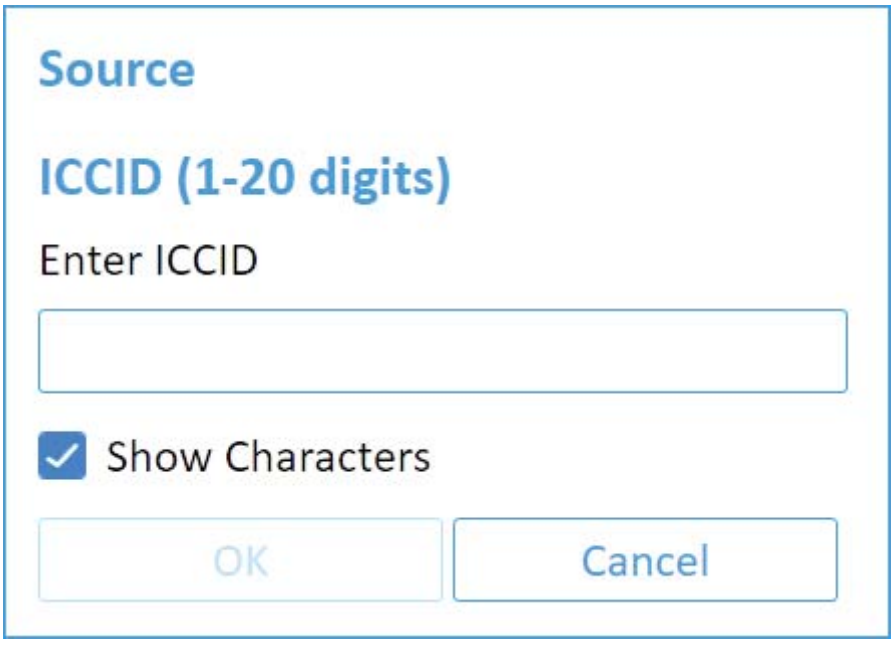
   The Waiting for Device screen appears.

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

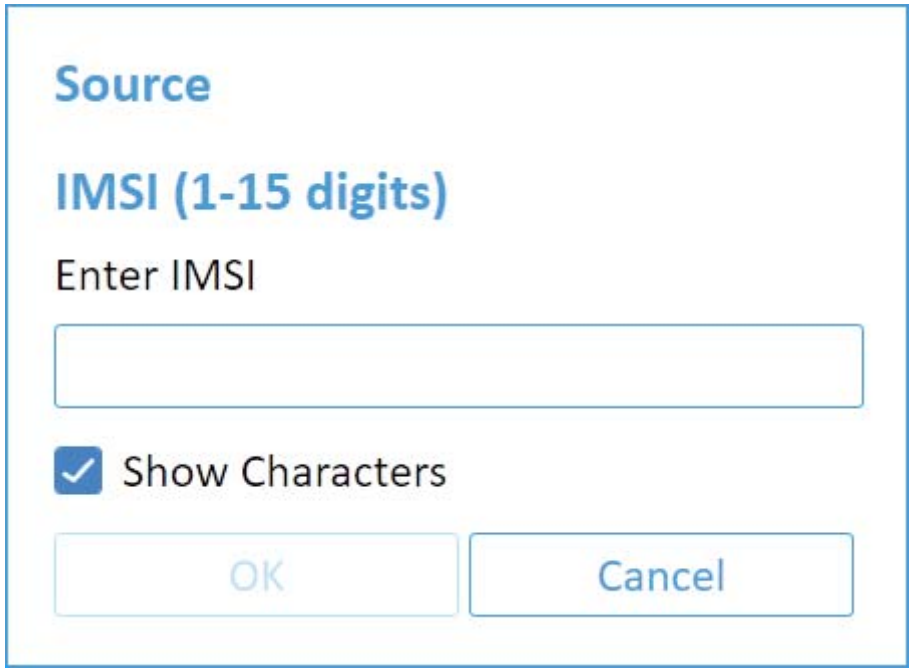
   The Select Source screen appears.



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



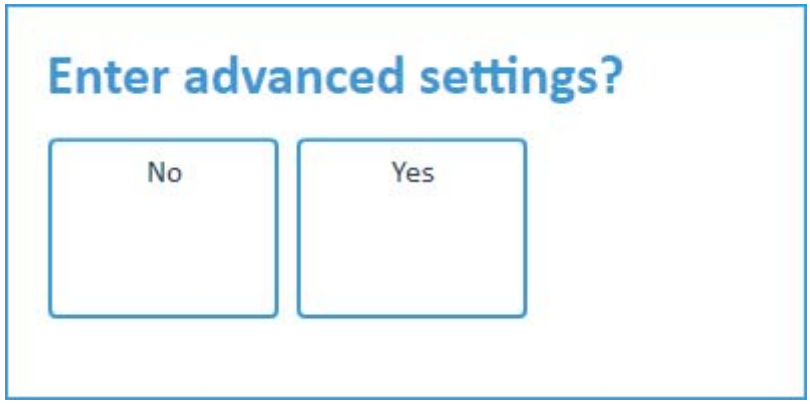
5. Enter the SIM ICCID number (up to 20 digits).
6. Click OK. The following screen appears.



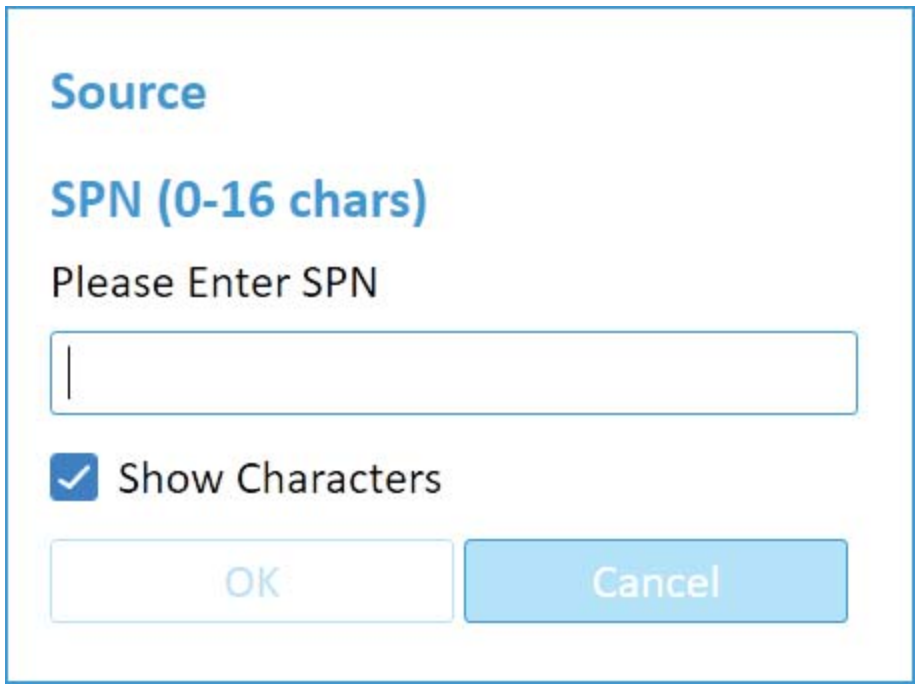
7. Enter the SIM IMSI number (up to 15 digits), then click OK.

   The Select Language screen appears.

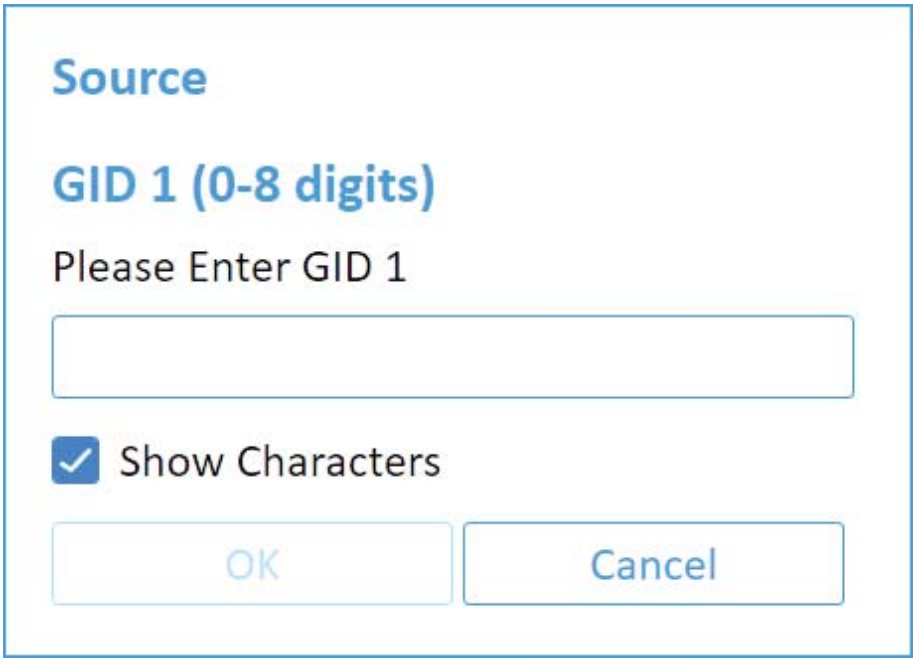
8. If required, select either a language or click **None**. The Enter advanced settings screen appears.



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



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



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

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

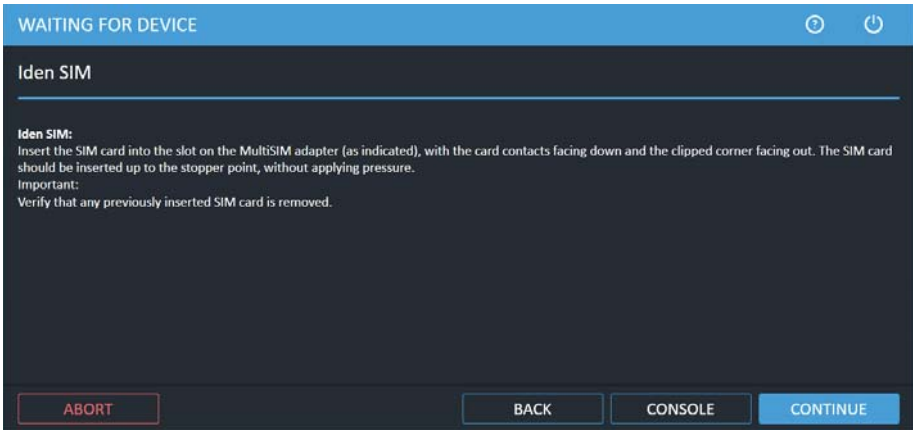
At the end of the data writing process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information programmed to the SIM card.

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

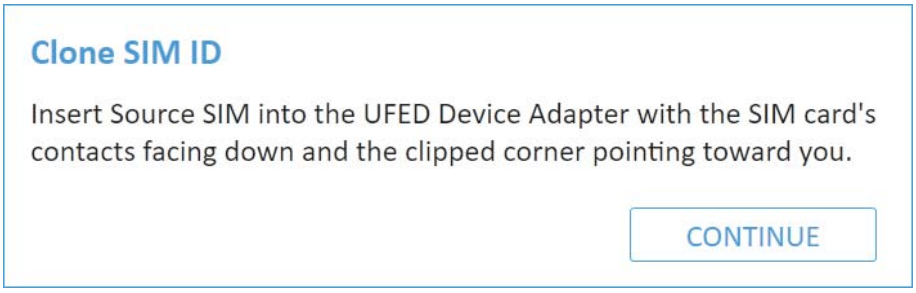
7.2.3. Creating a GSM test SIM

1. Click **Clone SIM**.

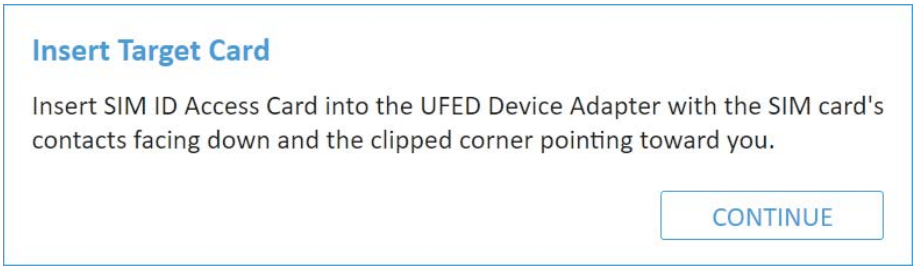
   The Waiting for Device screen appears.



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



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



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

8. Drone extractions

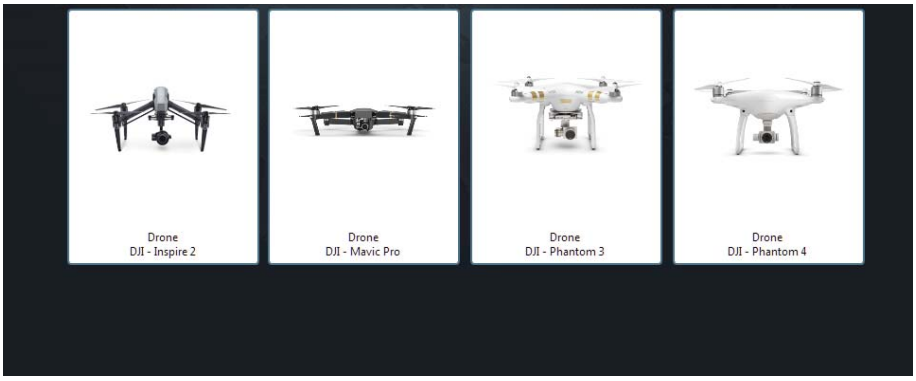
UFED enables you to extract flight data and multimedia files from supported drones. You can perform physical extractions, as well capture images of drones. For a complete list of supported drones, refer to the UFED Supported Devices file in MyCellebrite.

The following example shows how to perform a physical extraction of a drone.

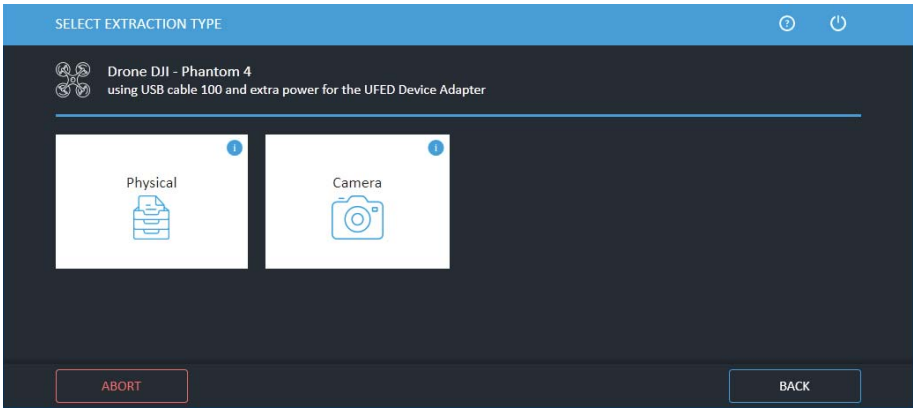
To perform a drone extraction:

1. Click **Drone**. The following window appears.

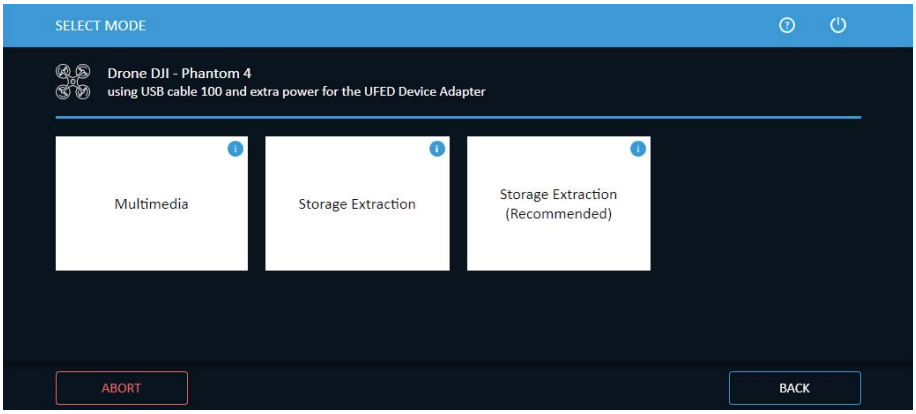
> You can also access drones via **Mobile device**, **Mass storage device** or global search.



2. Select the required drone and then click **Next**. The following window appears.



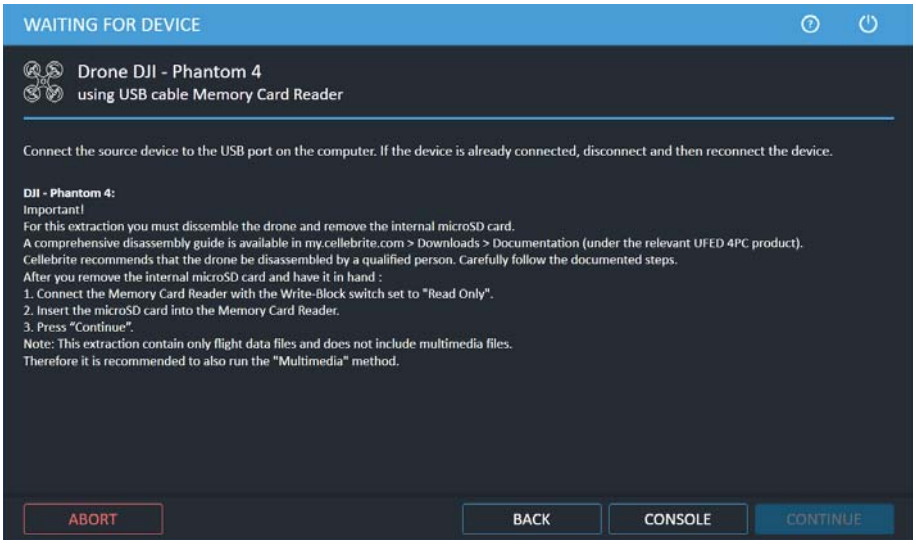
3. Click **Physical**. The following window appears.



4. Select an option as follows:
   - **Multimedia:** The *external* microSD card stores the multimedia files of the drone i.e., (images and videos) only. To obtain a full data extraction including flight data, it is also recommended to run the "Storage Extraction Recommended" method.
   - **Storage Extraction:** The *internal* microSD card stores the .dat file, which contains the flight data of the drone. The data stored on this card is updated to the time of the extraction. This extraction method is easier than the Storage Extraction (Recommended) mode, but it requires the drone to be turned on which triggers additional log data that is written to the card. This extraction method already includes multimedia files, therefore the Multimedia mode is not required.
   - **Storage Extraction (Recommended):** The *internal* microSD card stores the .dat file, which contains the flight data of the drone. The data stored on this card is updated to the time when the drone was last turned off. This is the recommended extraction method, because the drone stays off and no additional log data is written to the card. However this extraction method is more complicated due to the fact that the microSD card can only be accessed after disassembling the drone. This extraction method does not include multimedia files, therefore it is recommended to also run the Multimedia method. For information on disassembling the drone, refer to MyCellebrite.com > **Downloads** > **Documentation** (under the relevant UFED product). Cellebrite recommends that the drone be disassembled by a qualified person. Carefully follow the documented steps.

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

The following window appears.



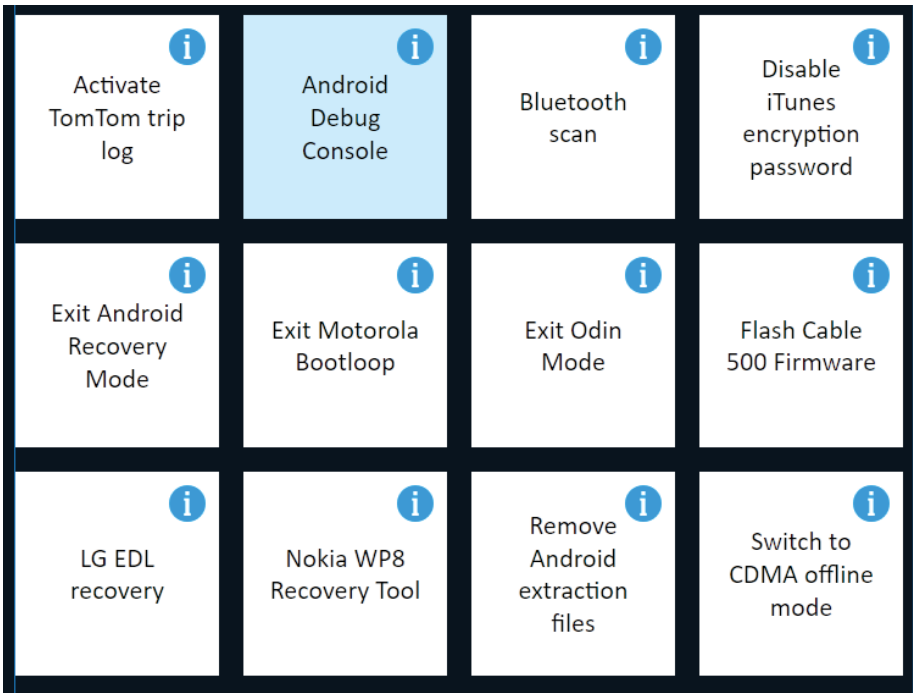
5. Use the specified cable and follow the on-screen instructions.
6. Tap **Continue**.

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

9. Device tools

To access the device tools:

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



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

9.1. Activate TomTom trip log

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

To Activate TomTom trip log:

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

   The **Select Mode** prompt appears.
3. Select the desired mode.

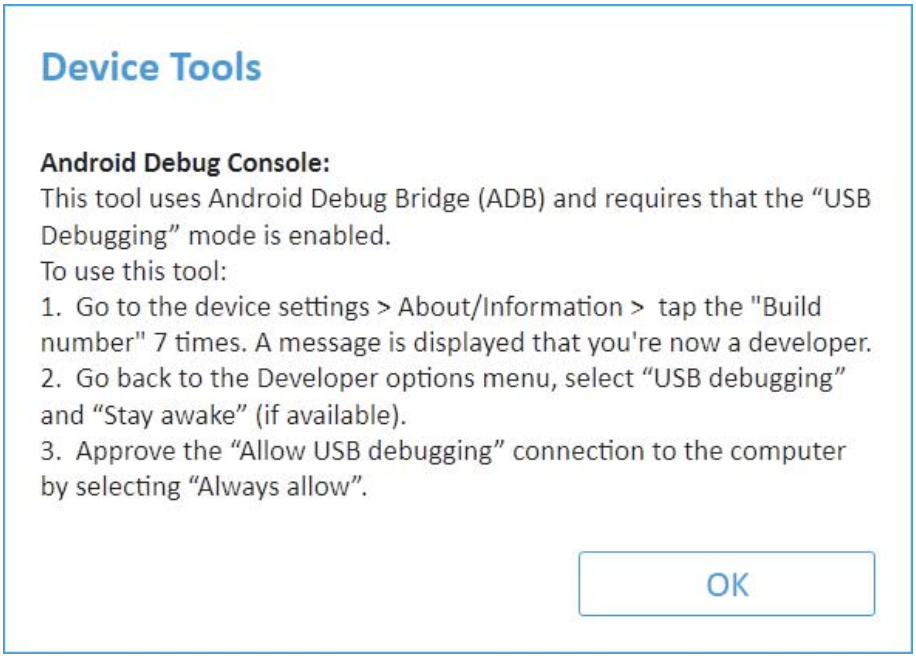
   A prompt labeled **Attention** appears requesting to connect the device to UFED.
4. Connect the device to UFED.
5. Click **Continue**.

9.2. Android Debug Console

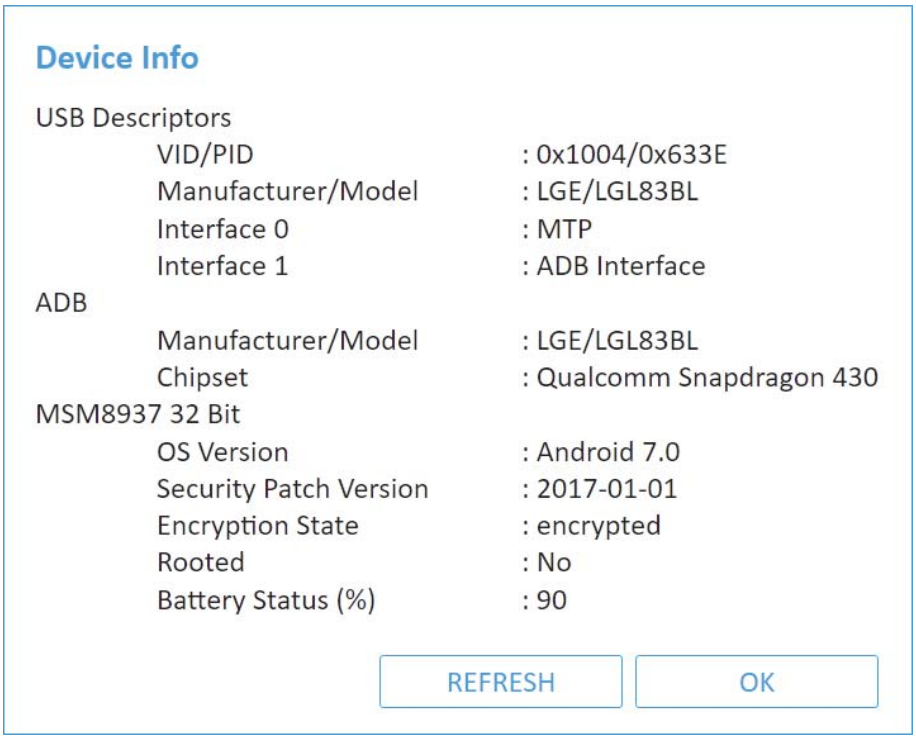
This tool retrieves device information using Android Debug Bridge (ADB).

To use the tool:

1. Click **Tools** and then click **Android Debug Console**.
2. If required, you will be prompted to connect the UFED Device Adapter to a USB port (4PC and non-kiosk platforms only). The following window appears.



3. Follow the on-screen instructions.
4. Tap OK to receive the device information. The following window appears.

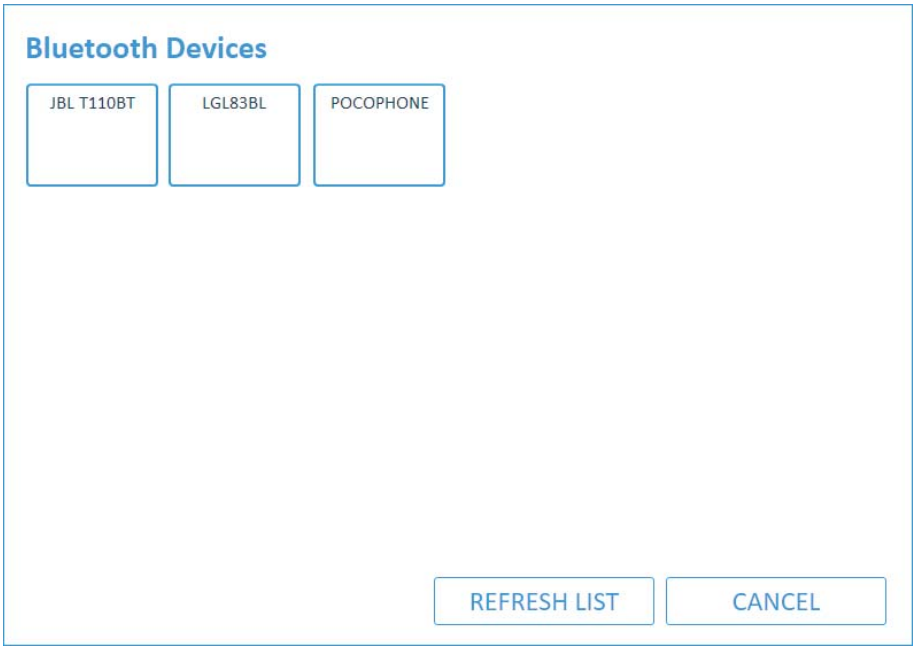


9.3. Bluetooth scan

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

To perform a Bluetooth scan:

1. Click **tools** and then click **Bluetooth scan**.
2. Connect the UFED Device Adapter (4PC and non-kiosk platforms only).
3. A list of Bluetooth devices in the vicinity appears. Select one or the following options:
   - Click one of the devices: The Device summary window appears.
   - Click **Continue:** Device summary window appears
   - Click **Refresh list:** Device tool in progress window appears and UFED tries to find additional devices.



9.4. Disable iTunes encryption password

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

9.5. Exit Android recovery mode

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

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

9.6. Exit Motorola Bootloop

In some cases, due to device failure, or if the Motorola mobile device was improperly disconnected from UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop.

9.7. Exit Odin mode

To perform physical extractions on some Samsung devices, the device is placed in Odin mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from UFED, the mobile device remains in Odin mode. This option enables the device to be taken out of Odin mode.

9.8. Flash Cable 500 Firmware

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

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

To flash the firmware for the Smart ADB extraction method:

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

9.9. LG EDL recovery

In some cases, due to device failure, or if the mobile device was improperly disconnected from UFED, the LG device remains in emergency download (EDL) mode and appears off. This option enables the device to be taken out of EDL mode.

To use the tool:

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

9.10. Nokia WP8 recovery tool

To perform physical extraction on some Nokia Windows Phone 8 devices, the device is placed in recovery mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from UFED, the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode.

9.11. Remove Android extraction files

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

9.12. Samsung Exynos Recovery

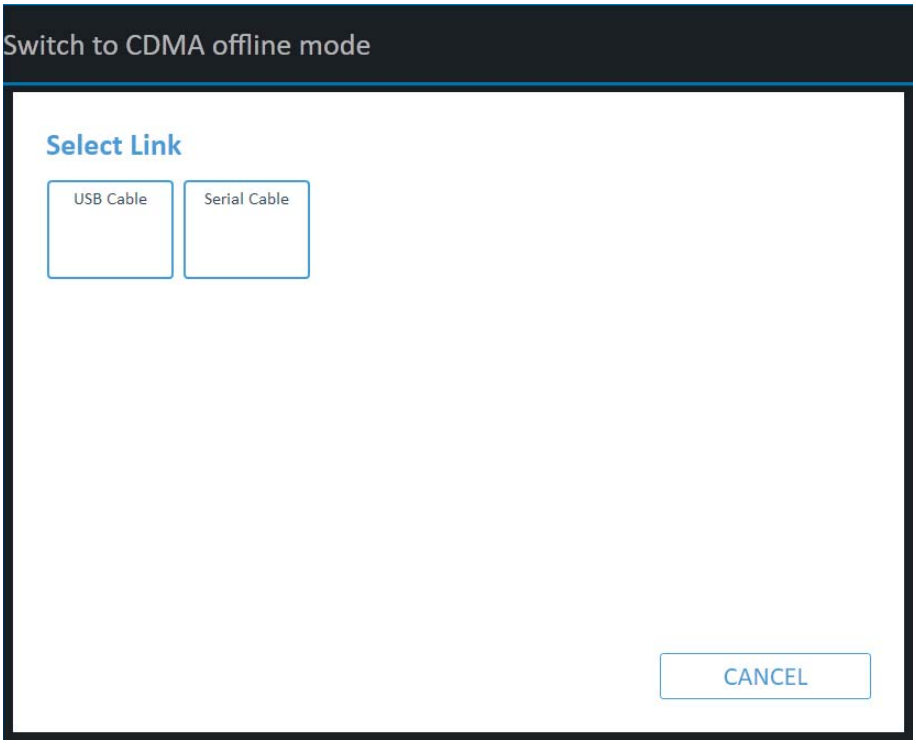
In some cases, due to device failure, or if the mobile device was improperly disconnected from UFED, the device remains off and the Android OS does not start. This option attempts to resolve this issue.

9.13. Switch to CDMA offline mode

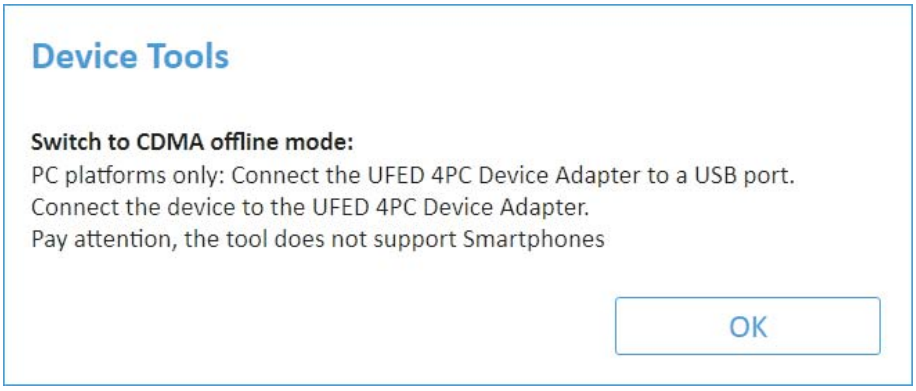
This tool enables you to switch radio on CDMA devices to offline mode.

To switch to CDMA offline mode:

1. Click **tools** and then click **Switch to CDMA offline mode**.
2. Connect the UFED Device Adapter (4PC and non-kiosk platforms only). The Select Link prompt appears.



3. Select the link type (**USB Cable** or **Serial Cable**). The Device Tool in Progress window appears.



4. Tap OK.

   Upon completion, the Device Tool Summary appears.

9.14. Uninstall Windows mobile client

To perform logical extractions on devices with Windows Phone operating systems, a client is installed on the device. In some cases, due to a device failure, or if the mobile device was improperly disconnected from UFED, the client remains installed on the mobile device. This option enables the client to be manually uninstalled.

10. Glossary

A

Active extension cable

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

ADB

Refers to an extraction method most commonly used for file system extractions. ADB, AKA Android Debug Bridge, is a built-in communication mechanism originally designed for device debugging. To enable the device extraction, ADB must be turned on.

ADB (Rooted)

When extracting a rooted device, the operating system version is not a limitation and the extraction can be completed on any Android version.

Advanced ADB

Refers to a physical extraction method, where ADB is used to facilitate the extraction. This method is available for Android OS versions created before December 2016. Depending on the device, this extraction may perform faster than other extraction methods, but takes considerably longer than other extraction methods. With this extraction type, the source device will continue the extraction, once the appropriate commands are sent to the device, with the output directed towards a USB mass storage device (via OTG cable) or SD memory card.

Advanced ADB (Generic)

This process is similar to the ADVANCED ADB mentioned however it is not verified for use on a specific device. It has however been shown to be successful on many

similar devices. In some rare cases, it may not perform as expected, therefore, we recommend trying other extraction types first.

Advanced logical extraction

An extraction method that combines both the logical and file system extractions into a single extraction method for iOS and Android devices. This method helps users overcome the pain of long and convoluted extractions, saving time and effort while maintaining forensically sound data.

Airplane mode

Flight mode, Offline mode, or Standalone mode is a setting that when activated it disables all voice, text, telephone, and other signal-transmitting technologies such as Wi-Fi and Bluetooth. Wi-Fi and Bluetooth can be enabled separately even while the device is in airplane mode.

Allocated space

The area on a device's memory that stores data in an organized manner, and contains its operating system and user data. Logical extractions obtain data from allocated space only.

Android Backup

Supports Android devices running OS version 4.1 and later. It typically provides less data than a regular "ADB" backup, however, depending on the make, model and OS version of the device, it may be the only option available or can be used when the ADB option exists, but is not successful.

Android Backup APK Downgrade extraction

This method focuses on specifically supported apps for decoding. It should be used as a last resort method as data alteration will occur during this process. This method temporarily downgrades the updated version of the app on the device and installs the latest supported version of the app that it can decode.

apk

Android application package file. Each Android application is compiled and packaged in a single file that includes all of the application's code (.dex files), resources, assets, and manifest file.

Apple File Conduit

AFC2. A service that is used by computer applications such as iTunes and iPhoto to read files from a device over USB.

B

Boot loader

A small piece of code that is inserted into the RAM during start-up. In the commercial wireless world, this allows flashing of firmware. In the forensic world, it allows a non-intrusive means of accessing and copying user data into a forensic image.

Brick

A device that cannot function in any capacity (such as a device with damaged firmware).

Brute force

Refers to an unlocking technique that relies on trial and error. Combinations are attempted until the correct password or PIN is found.

C

CAS

Cellebrite Advanced Services (CAS) offers customers the ability to recover valuable evidence from heavily damaged, locked or encrypted devices.

CDMA

Code Division Multiple Access. These networks connect using different methods to allow multiple callers access to single voice radio waves, hence Code and Time Division. True CDMA networks do not require handsets to have a SIM card, as the network connects to the device and the subscriber details are contained in the handset rather than a SIM card.

Chip-off

Otain data straight from the mobile device's memory chip.The chip is detached from the device and a chip reader or a second device is used to extract data stored on the device under investigation.

CMS

Simplify how you manage and control all deployed devices and systems with the Cellebrite Central Management System (CMS). Reduce ongoing administration costs by remotely accessing devices and systems across your operation.

D

Decrypting Bootloader

This process is designed for Android devices that have Qualcomm chipsets. This extraction can be performed when the device is in Bootloader mode. Bootloader extractions do not support extractions from a memory card or SIM card.

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, "-", "+".

Dongle license

Is a software copy protection device that plugs into the USB port of the computer. Upon startup, the application looks for the key and will run only if the key contains

the appropriate code.

E

EDL (Emergency Download)

Included in the cable or tip set received with your UFED, is an EDL cable. The EDL method is sometimes a superior alternative to advanced techniques, such as JTAG, ISP and Chip-off as they typically can be accomplished without advanced or invasive techniques. It's also possible to use this method on devices that do not function due to damage.

Extraction

The process of obtaining mobile device data and storing it in an approved location for processing.

Extraction files

Files used to capture forensic evidence from mobile devices. This includes mobile phones, handheld tablets, portable GPS devices, and devices manufactured with Chinese chipsets. Extraction types include Logical, SIM Password, File system, physical, capture images, and capture screen shots. Extraction files: MSAB Extended XML, XLS, XLSX, XMK, CSV, TXT, UFD, UFDR, CDR

F

Facelock

Uses an image of the user captured by the front camera to unlock the device. There must be some movement in the face when unlocking the device, to prevent someone from using a still photo to gain access.

File system extraction

Obtains files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction.

Fingerprint

Newer devices have a fingerprint sensor built into the home button. The user places their finger upon the sensor to gain access to the device.

Forensic Recovery Partition

This extraction method will perform a physical extraction while the device is in Recovery mode. With this extraction method, the original recovery partition is replaced with Cellebrite's custom forensic recovery partition. Using Cellebrite's custom forensic recovery partition does not affect any of the user data, is forensically sound, and will bypass the user lock from a number of Samsung Android devices.

Forensically sound

Extracted data is said to be forensically sound if it was collected, analyzed, handled, and stored in a manner that is acceptable by the law, and there is reasonable evidence to prove so. Forensic soundness provides reasonable assurance that extracted data was not corrupted or destroyed during investigative processes, whether on purpose or by accident.

I

ICCID

Integrated Circuit Card Identifier. GSM identifier

IMEI

International Mobile Equipment Identifier. GSM identifier

IMSI

International Mobile Subscriber Identity. GSM identifier

Iris scan

Different from retina scans, an iris scan is a form of biometric identification using iris pattern-recognition techniques. The owner of the device establishes the security

feature by video scanning the complex, unique but stable patterns of the eye portion surrounding the pupil.

J

Jailbreaking

A jailbroken iOS device or a rooted Android device is one whose owner has taken steps to bypass its factory settings, including built-in security and other restrictions. Jailbreaking an iOS device allows the user to install third-party apps from sources other than the App Store, while rooting an Android device provides administrative "root" access to its operating system. UFED solutions do not rely on jailbreaking or permanent rooting to perform forensic extractions, as other mobile forensic tools do.

K

Knock pattern

The user taps certain locations on the screen in a certain order to gain access to the device.

L

Logical extraction

Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data.

M

MEID

Mobile Equipment Identity (MEID) is the CDMA equivalent of the International Mobile Equipment Identifier (IMEI) for Global System for Mobile communications (GSM) handsets and is often referred to as the serial number of the handset.

MIN

Mobile ID Number (MIN) is often compared to the International Mobile Subscriber Identity (IMSI) found associated to GSM handsets. The MIN is the number which identifies the subscriber to the CDMA network provider.

MSISDN

Mobile Station International Subscriber Dialing Number. GSM identifier.

MultiSIM Adapter

Is a small-size adaptor which enables reading, data extraction and cloning Nano SIM, Micro SIM and SIM cards.

P

Password Lock/Bypass

Users of devices are routinely secure their data with the user of password locks and security measures. The bypassing or discovery of these security measures largely depends on the make and model of the device as well as the operating system that is in use. Using Cellebrite's extraction technology, some devices are able to have bypasses, where a series of specialized cables and instructions are supplied to either bypass or defeat a security mechanism used. In other cases, instructions will be provided which will allow the user to have the PIN/PASSCODE displayed on the screen.

Physical extraction

The most comprehensive extraction and forensically sound. It uses advanced methods to extract a physical bit-for-bit image of the flash memory of a device, including the unallocated space. Unallocated space is the area of the flash memory that is no longer tracked by the file system. Unallocated space may contain images, videos, files, and more.

PIN/Password and Pattern Lock

All of the above locks require a secondary lock such as a PIN, password, or pattern lock. Also, a user may select one of these as the primary screen lock for their device.

R

Root

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 devices.

S

Selective extraction

Performs fast and focused extractions. Pick and choose the applications in which you suspect contains relevant data or leads, and perform a Selective extraction rather waiting several hours for a full file system extraction.

Smart ADB

This method is designed for Android devices that include the “November 2016” security patch. It is supported by OTG compatible devices with OS versions 6.0 and above. Only security unlocked devices are supported.

Smart location

Trusted locations leave the device unlocked for up to four hours when it is turned on, and the device is connected to a secured Wi-Fi access point, trusted Bluetooth device, trusted NFC tag, or if the device detects body movement.

T

TAC

The Type Allocation Code (TAC) is the initial eight-digit portion of the 15-digit IMEI and 16-digit IMEISV codes used to uniquely identify wireless devices. The Type Allocation Code identifies a particular model (and often revision) of wireless telephone for use on a GSM, UMTS or other IMEI-employing wireless network.

U

UFD

Once logical, file system, and physical extractions are complete, UFED generates an extraction file, along with a .UFD (text) file. The .UFD file contains information about the extraction, such as which UFED was used (including its serial number); start time, finish time, and date; and hash information. With iOS physical extractions, the .UFD file also contains decryption keys. For binary images, it may contain some information to aid the decoding process.

UFDR

Universal Forensic Extraction Device Report

UFDX

UFED generates a UFDX file when there are multiple extractions for a device. It contains information about each extraction

UFED

Universal Forensic Extraction Device

UFED 4PC

Enables users to deploy extraction capabilities on Windows based tablets, laptops, and desktop computer systems. It performs physical, logical, file system and password extractions on a wide range of devices.

UFED CHINEX

The UFED Chinex kit, is the solution to complete a physical extraction, decoding of evidentiary data and passwords from mobile devices manufactured with Chinese chipsets; including MTK and Spectrum.

UFED Device Adpater

The UFED kit contains a device adapter that attaches to your PC's USB ports. Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition, there are LEDs for power and Bluetooth. Depending on when you received your UFED kit, there are two types of device adapters: UFED Device Adapter with USB 3.0 (latest version) and UFED Device Adapter with USB 2.0 (previous version).

UFED kit

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

UFED Memory Card Reader

A multi-format card reader that provides either read-only or read-write access to a variety of flash media cards.

UFED Physical/Logical Analyzer

An analysis and reporting tool for logical, file system and physical extractions. This software solution provides users with the capability to extract data, perform advanced analysis, decoding and reporting and presenting the results in a clear and concise manner.

UFED Touch

Enables the simplified extraction of mobile device data. Depending on the license purchased, it performs physical, logical, file system and password extractions on a wide range of devices.

V

Voice lock

The user speaks while unlocking the device, and their voice gains access.

11. Index

W