Cellebrite Digital intelligence for a safer world

Access digital evidence faster using Emergency Download (EDL) mode

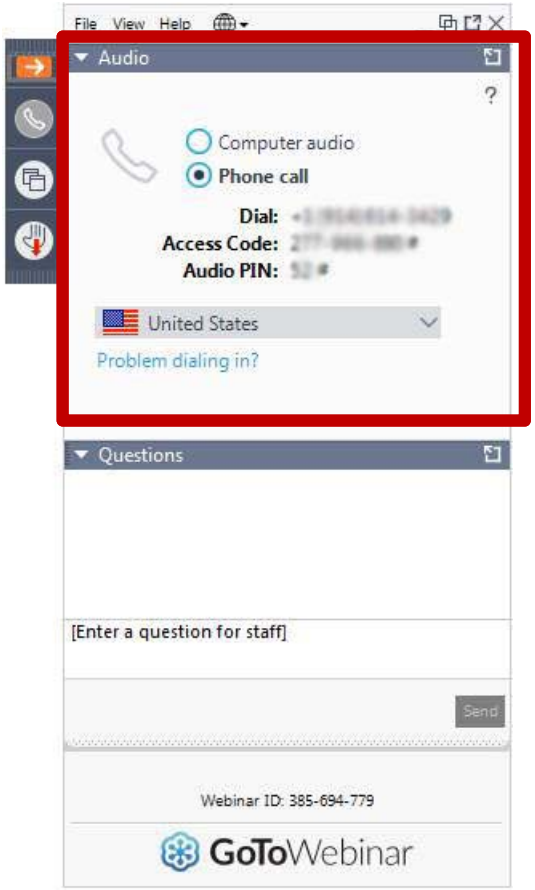
February 21, 2018

Housekeeping - audio

Select “Computer audio” to join via VOIP

OR

Select “Phone call” to dial in

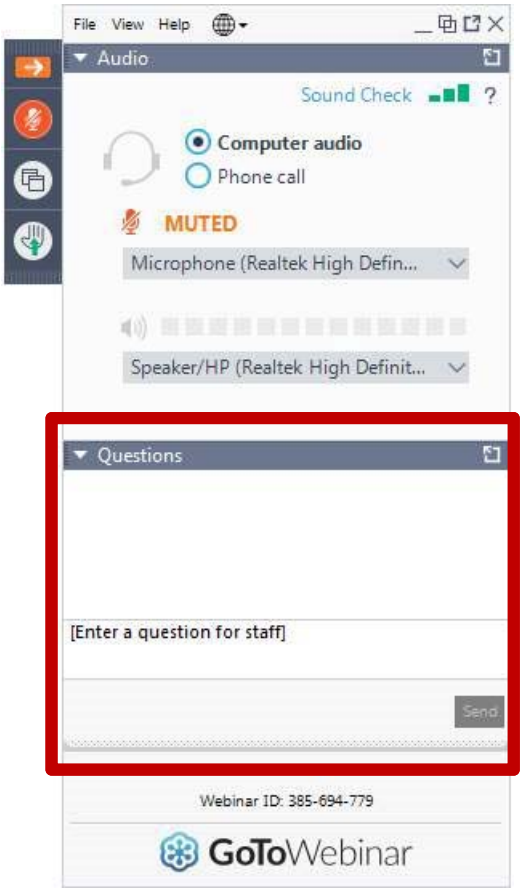


Cellebrite

Housekeeping

Please note the following:

- All attendees are muted
- Webinar is being recorded
- Q&A will be held at the end
- Submit questions via the Question Section located in the operator panel
- Webinar replay and slides will be shared after the event



Cellebrite

Agenda

Welcome and Introductions

Understanding Cellebrite's exclusive automatic EDL capability that bypasses device locks and provides fast physical extraction

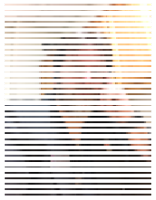
Detecting EDL mode and accessing Qualcomm chipsets for forensically sound mobile device analysis – two cases studies

Best practices and other hardware/software techniques to enter EDL mode and perform physical extractions

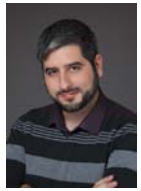
Q&A

Cellebrite

Today’s presenters



Scott Lorenz has been a Texas Police Officer since 1993, a licensed private investigator in Texas since 2003, and currently Chief Forensics Analyst for Centex Technologies. Scott is a member of the faculty and Professor of Criminal Justice at Central Texas College and frequent instructor in the police academy. Scott has been conducting digital forensics investigations since 2009, and conducts examinations for multiple state and local police agencies in state and federal criminal investigations. Scott is a moderator on the Mobile Device Forensics and Analysis group.



Shahar Tal is Vice President of Research at Cellebrite Security Research Labs. Shahar joined Cellebrite in 2015 to lead the mobile forensics extraction research group. Prior to joining Cellebrite, he led a vulnerability research group at Check Point and also served 9-years in the Israeli army holding different technological leadership roles. Shahar is a frequent guest speaker at world-renowned security and forensics conferences, including DEF CON, CCC, MFW and many others.

Emergency Download (EDL) mode

Cellebrite

SRL - Security Research Labs

Traditional forensic extraction methods mainly required **reverse engineering**

- Discover hidden vendor commands and low-level protocols
- Analyze device internals, map access to flash memory

In recent years we have seen dramatic changes to the extraction landscape

- Industry awareness to security and data protection has grown
- Processor performance allows commodity implementations of advanced encryption schemes (Android FDE)

Modern methods require **security research** –

We research and discover vulnerabilities that allow forensic evidence extraction.

Cellebrite

What is EDL?

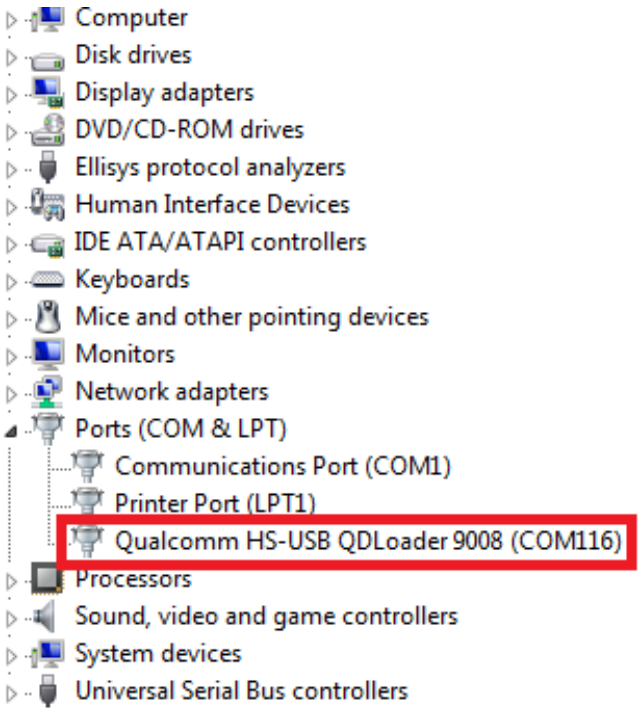
Qualcomm Emergency Download Mode (a.k.a. QDLoader 9008)

A rescue mode targeted for phone diagnostics & repair

- Faults and errors on boot will default into EDL
- Exposes protocol to allow low-level technical recovery
- Requires digitally signed “programmer” files per model

Inherent feature of Qualcomm chipsets

- Not always easily accessible
- Not to be confused with other “Download Modes”



What is EDL?

Support tools available (QPST/QFIL)

Cellebrite

Entering EDL

Device manufacturers can plan and design how a specific phone model enters EDL.

- A common method is a key combination on power up – e.g. holding Vol+ and Vol-
- Another standardized method in cases where ADB is available is ‘adb reboot edl’
- Sometimes a special cable (designated lab cable) will signal the device to enter EDL

Some vendors choose to avoid easy access to EDL altogether, since they have their own flashing modes and protocol implementations (LG LAF, Samsung Odin, etc).

Some hardware methods, however, are built into the chipset, and cannot be disabled or removed by the manufacturer → **they always remain available**

EDL extraction in practice

Cellebrite

EDL extraction in practice

Cellebrite's EDL method of extraction is a viable and sometimes a superior alternative to advanced techniques, such as JTAG, ISP, and Chip-off.

- Many EDL extractions can be accomplished without training in advanced techniques and without invasive measures.
- It is possible to use Cellebrite's EDL method on devices that do not function due to severe damage.
- With the EDL method, it may be possible to extract a complete physical image of a device that may not be available via traditional methods.

Many EDL Extractions can be quickly and easily performed in the field allowing data to be recovered and viewed at the scene of the crime.

The most powerful aspect of Cellebrite's EDL extraction is the ability to decrypt physical images from devices, which is not possible via JTAG, ISP and Chip-off.

Cellebrite's EDL extraction possibilities

- Extract devices with severe damage in minutes.
- Extract a complete physical image of a device that may not be available via traditional methods.
- Extract devices as a viable and sometimes superior alternative to advanced techniques such as JTAG, ISP, and Chip-off.
- Extract devices without training in advanced techniques and without invasive measures.
- Extract devices quickly and easily in the field allowing data to be recovered and viewed at the scene of the crime.
- Extract locked, encrypted devices resulting in a full decrypted physical image.

EDL extraction test – encrypted Alcatel 5044R

- Alcatel 5044R: AKA idealXCITE
- AT&T Prepaid
- 8GB Storage
- Processor – Qualcomm MSM8909
- OS / Platform – Android 7.0
- Not encrypted out of the box
- Test phone encrypted by Lorenz

Cellebrite

EDL extraction test – encrypted Alcatel 5044R

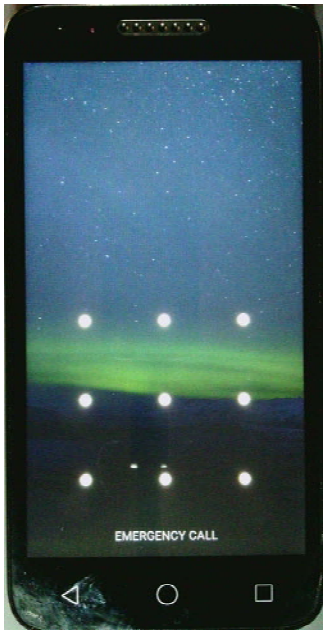
Most phones running Android 6.X and above are encrypted when purchased.

There are exceptions as with this one but they are easily encrypted by the user.

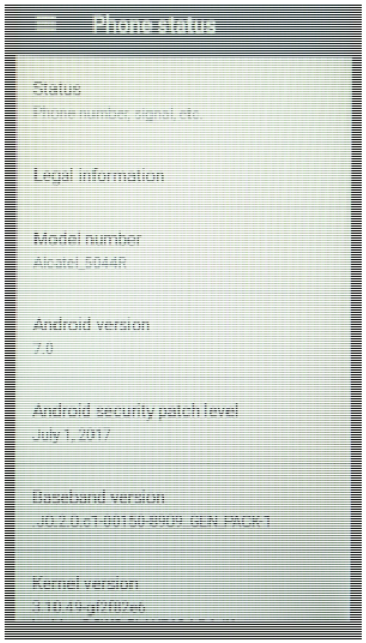
This phone only took a few minutes to encrypt.

Pattern Locked

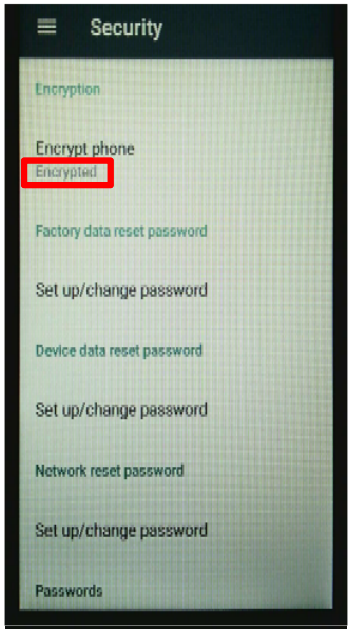
Pattern Locked



Android 7.0



Encrypted



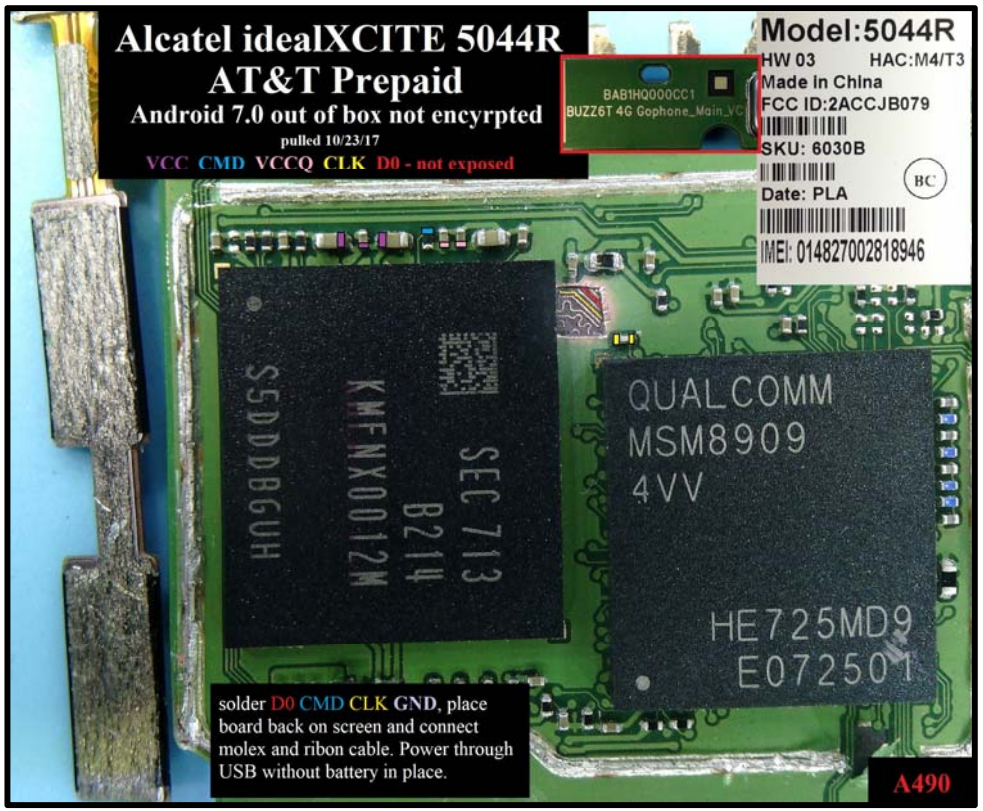
Cellebrite

EDL extraction test – encrypted Alcatel 5044R

Without Cellebrite's EDL capabilities physical extractions are limited with this phone if locked.

ISP is possible but data is not exposed (as with many Alcatels), requiring advanced procedures in the lab.

Chip-off is risky. If the device is encrypted the evidence will be destroyed.



Cellebrite

EDL extraction test – encrypted Alcatel 5044R

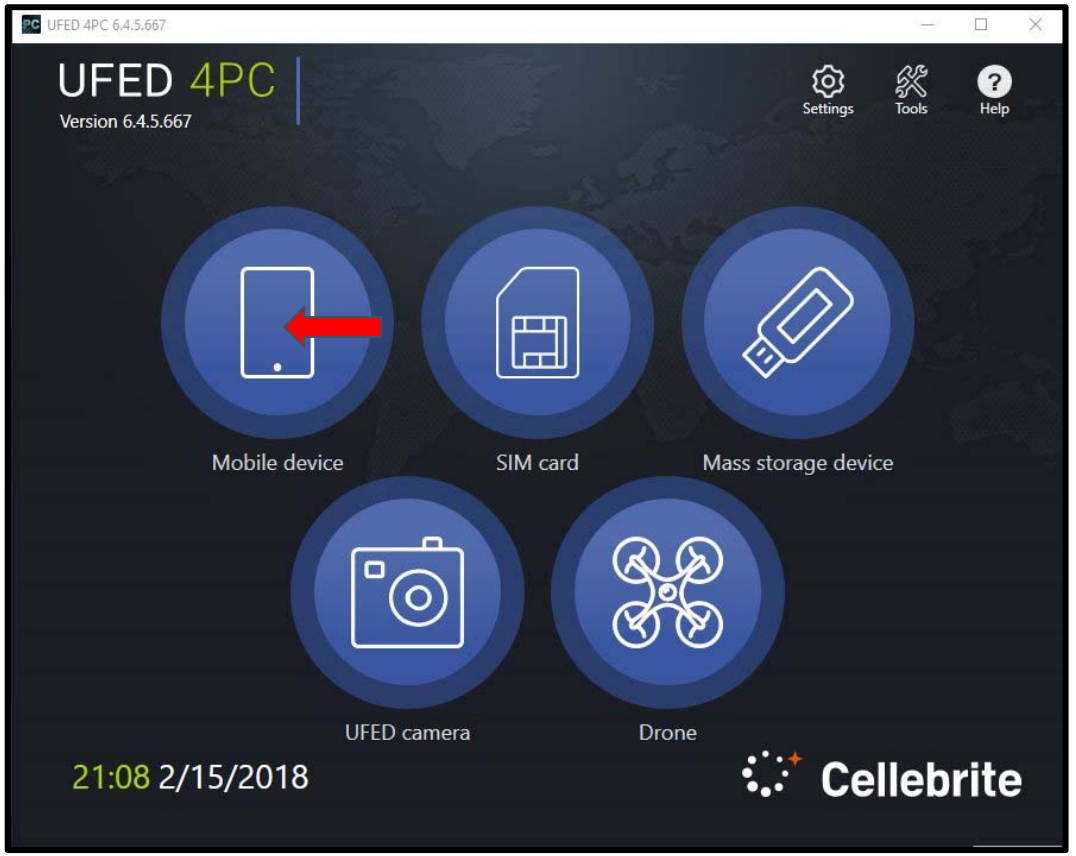
With the EDL method all that is required is:

- stock USB cable
- UFED Ultimate 4PC or Touch / Touch 2

Cellebrite

EDL extraction test – encrypted Alcatel 5044R

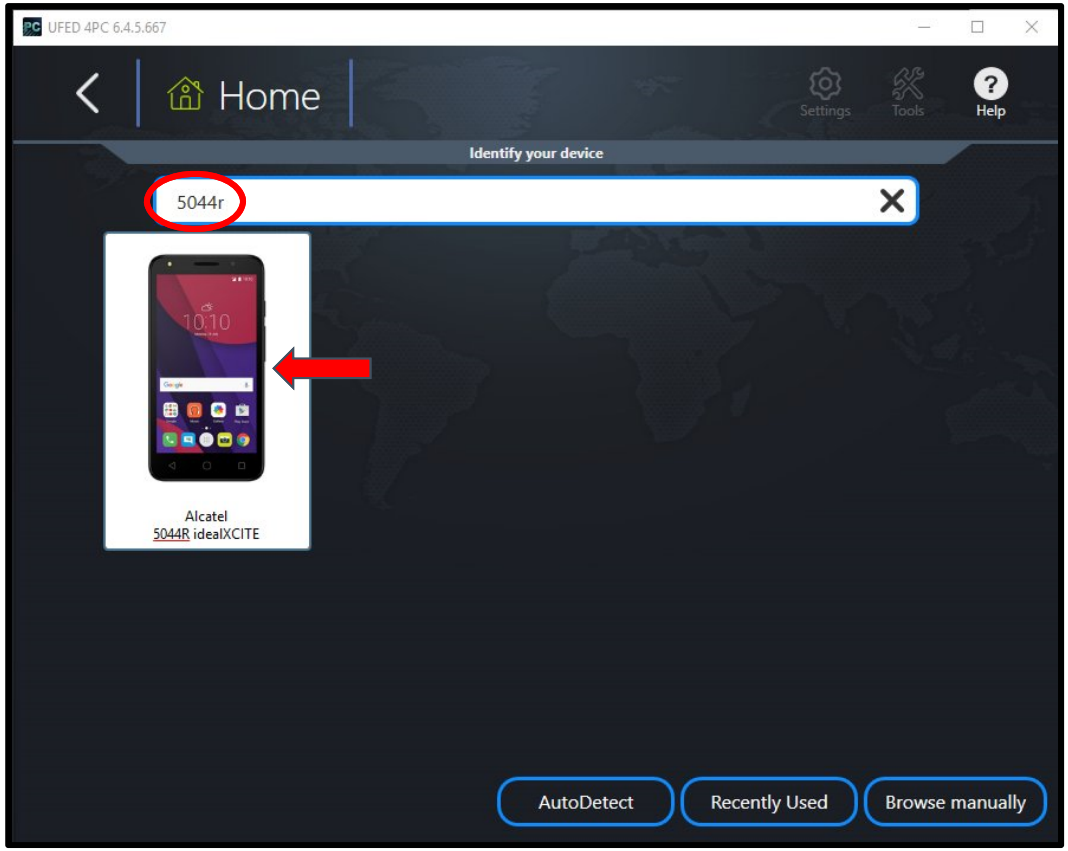
Begin by clicking
“Mobile Device”



Cellebrite

EDL extraction test – encrypted Alcatel 5044R

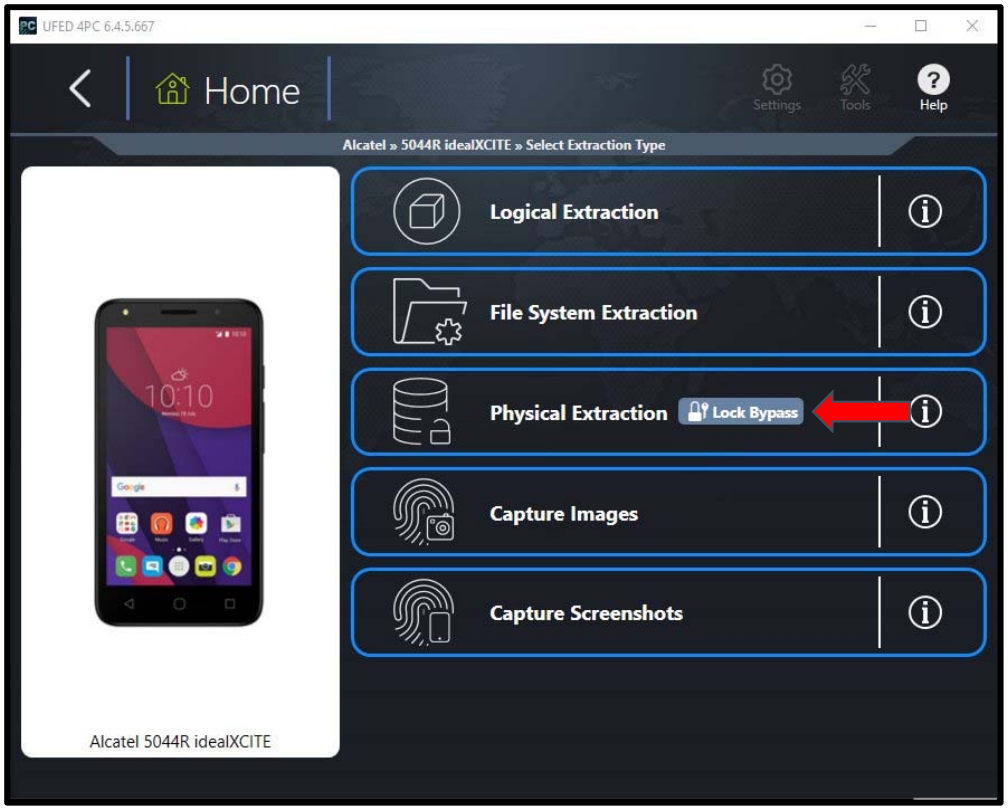
Type “5044r” in the manual search bar and then click on the device photo



Cellebrite

EDL extraction test – encrypted Alcatel 5044R

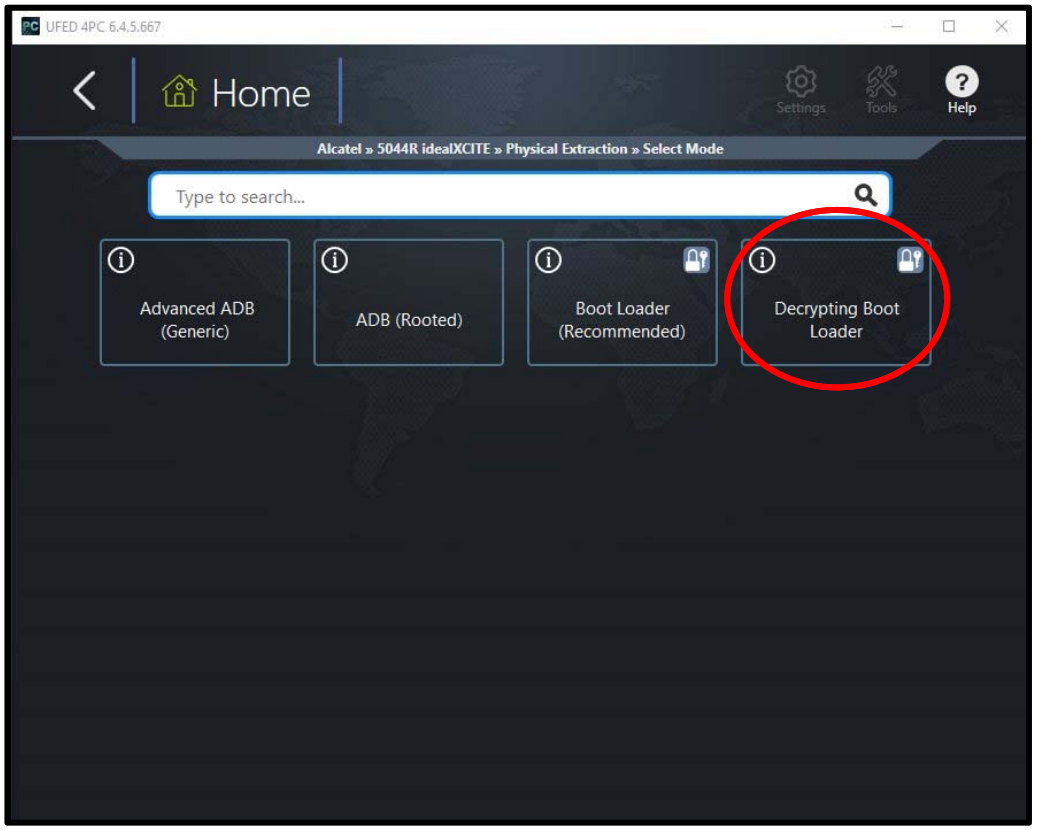
Select “Physical Extraction – Lock Bypass”



Cellebrite

EDL extraction test – encrypted Alcatel 5044R

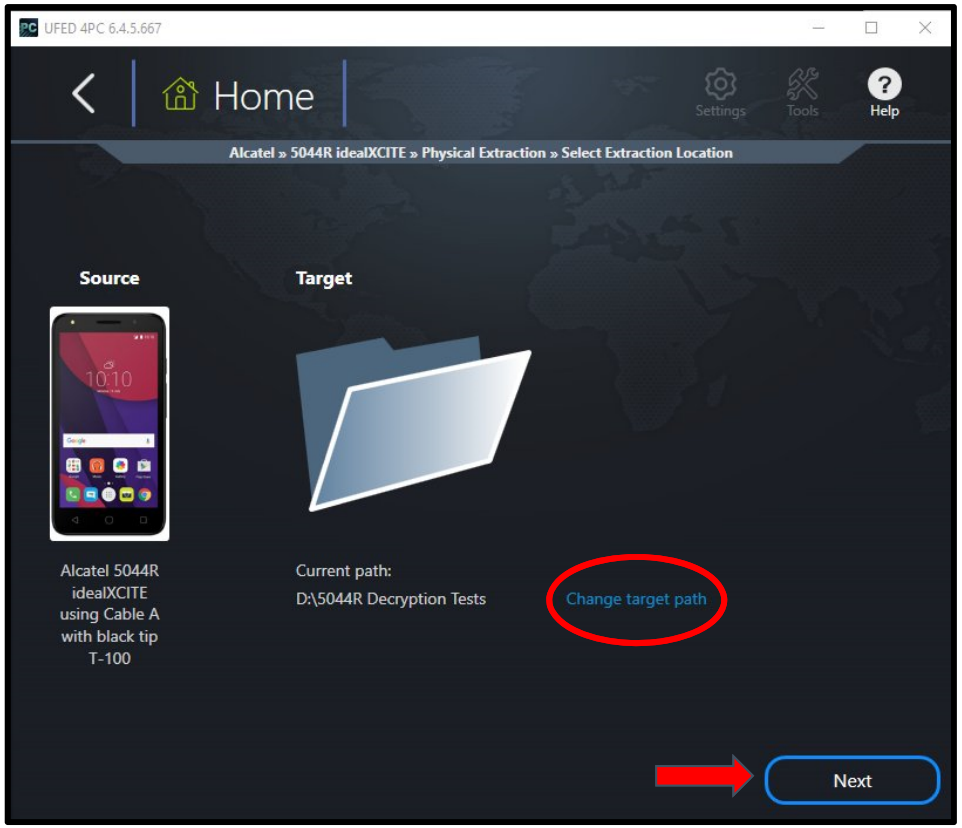
Select “Decrypting Boot Loader”



Cellebrite

EDL extraction test – encrypted Alcatel 5044R

Select your target location for the extraction and then click “Next”

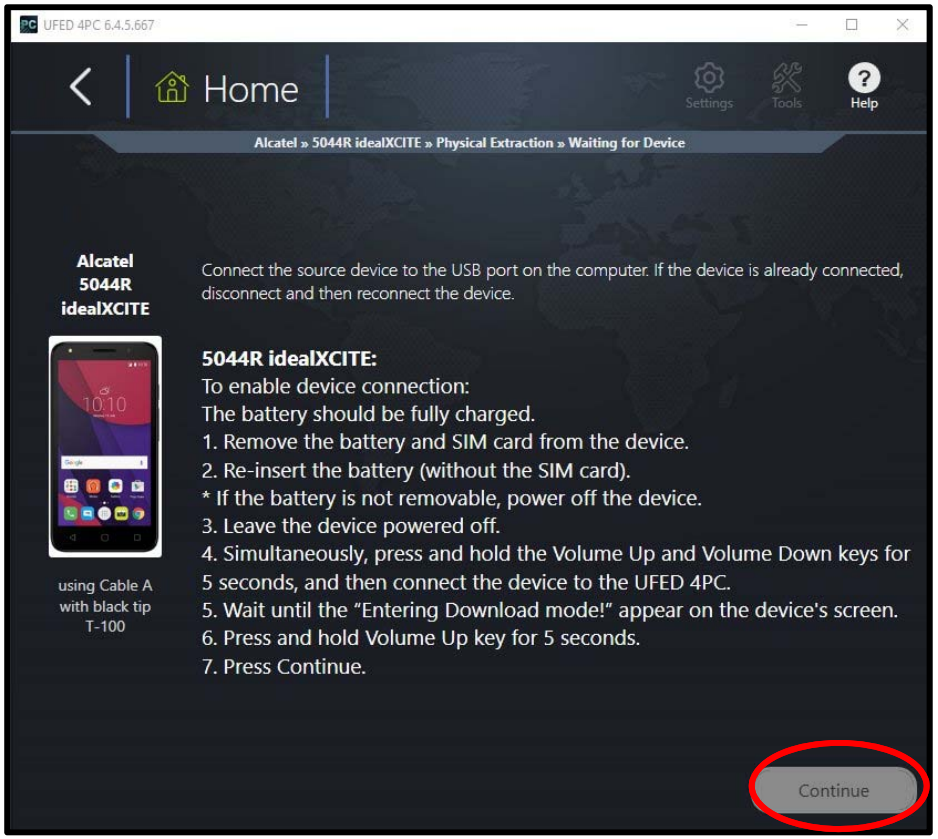


Cellebrite

EDL extraction test – encrypted Alcatel 5044R

When arriving at this screen, the “Continue” button should be grey – not active.

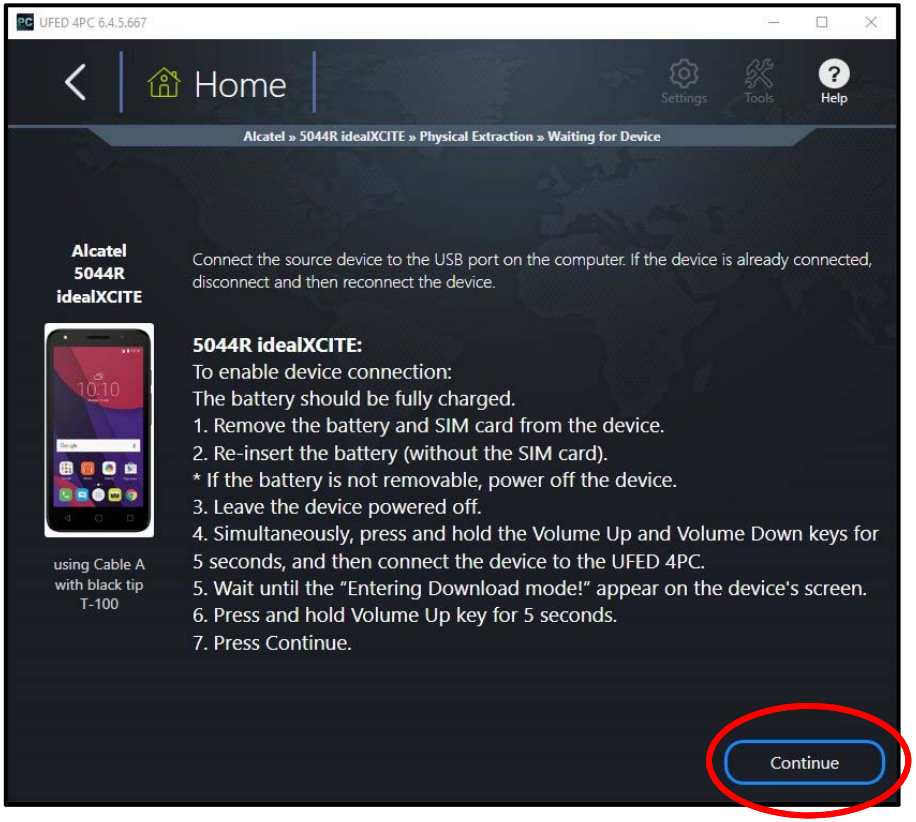
Follow the UFED instructions on the screen.



Cellebrite

EDL extraction test – encrypted Alcatel 5044R

After removing the SIM and reinserting the battery, follow the button procedure as instructed. When done correctly, the download screen will appear and then turn black after the final step. Press “Continue” when the button becomes active.



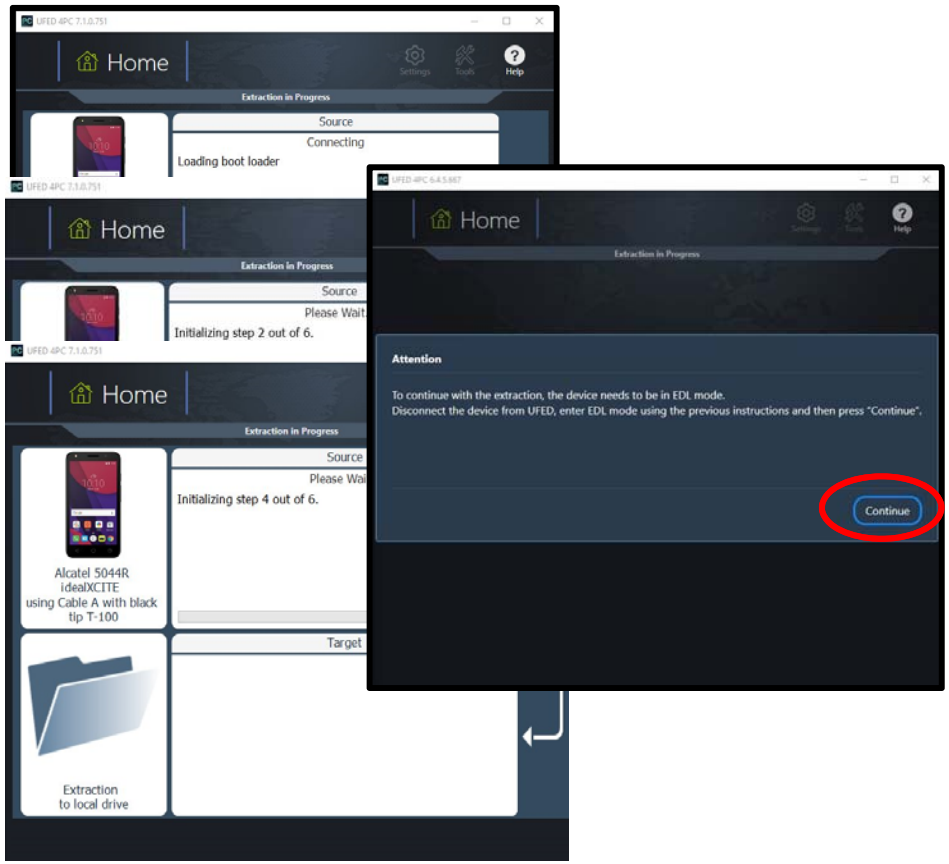
Cellebrite

EDL extraction test – encrypted Alcatel 5044R

The UFED will go through several screens before you will be prompted to disconnect the device, remove the battery and use the button combinations to place the device in EDL mode exactly as you did the first time.

The procedure is easy for this device and only takes a few seconds. The “Continue” button will remain active during this procedure.

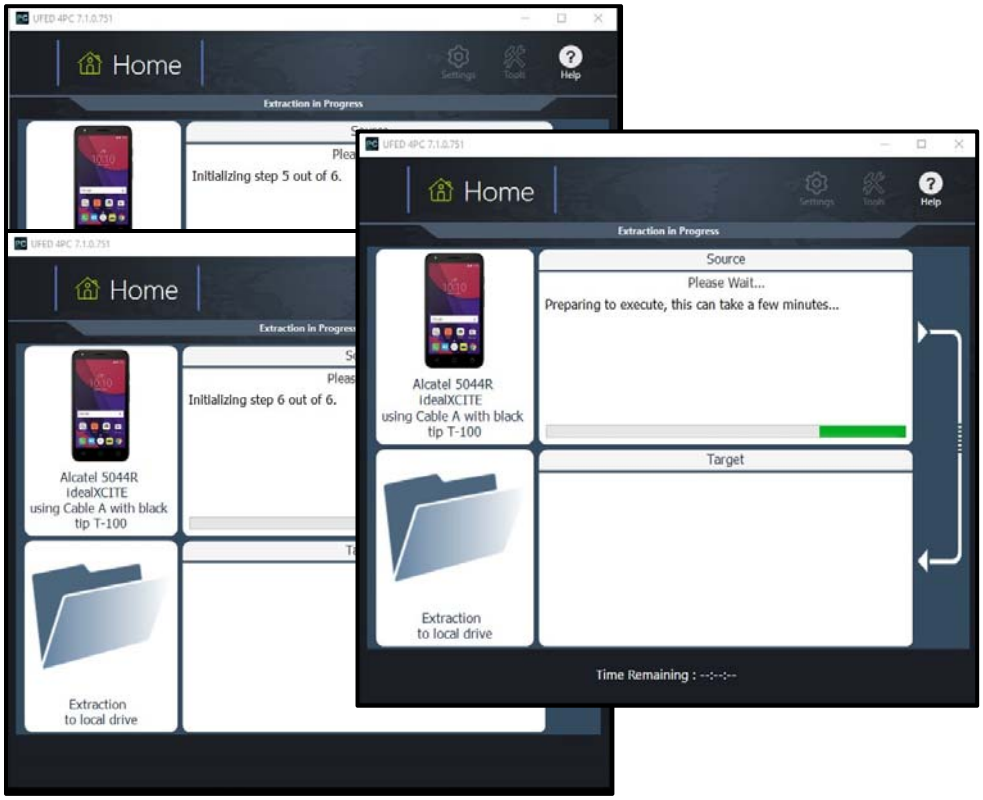
After repeating the steps as before, click “Continue”.



Cellebrite

EDL extraction test – encrypted Alcatel 5044R

The UFED will go through step 5 and 6 then to the executing screen. This can take a couple of minutes.

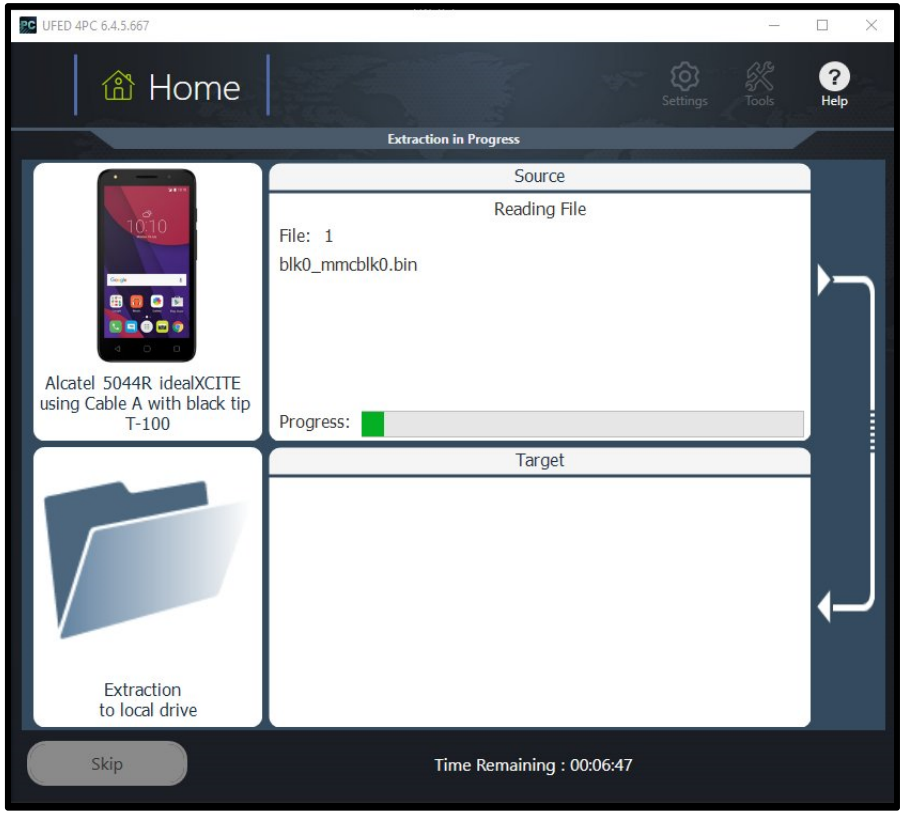


Cellebrite

EDL extraction test – encrypted Alcatel 5044R

After executing, the UFED will begin extracting a decrypted physical image from the phone.

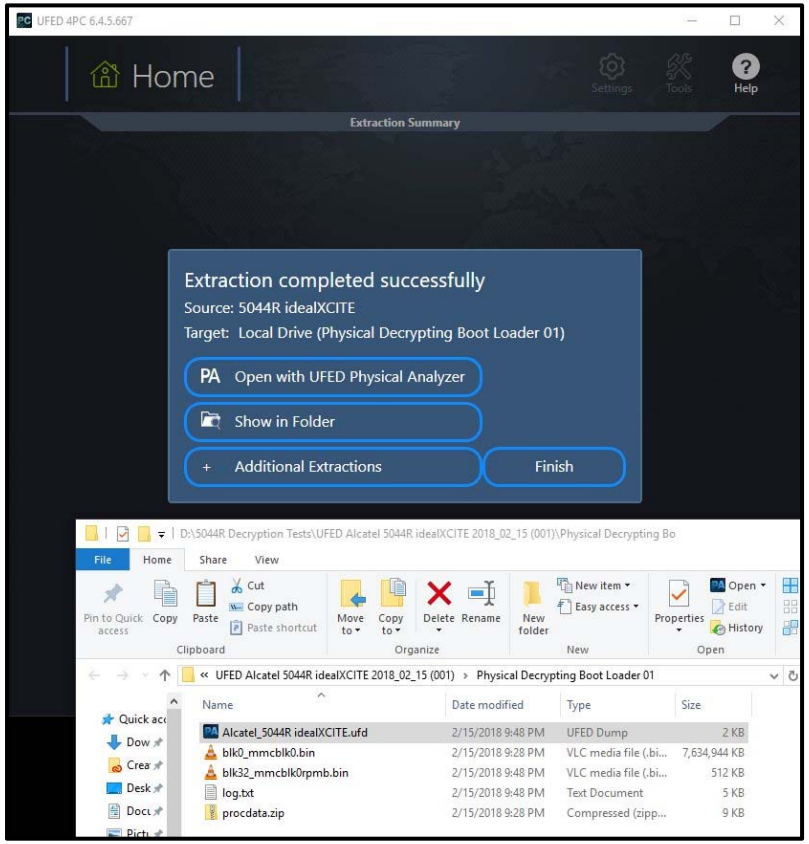
This process takes about 24 minutes on this device.



Cellebrite

EDL extraction test – encrypted Alcatel 5044R

When finished you can open the device or navigate to the .ufd file and open the device.



Cellebrite

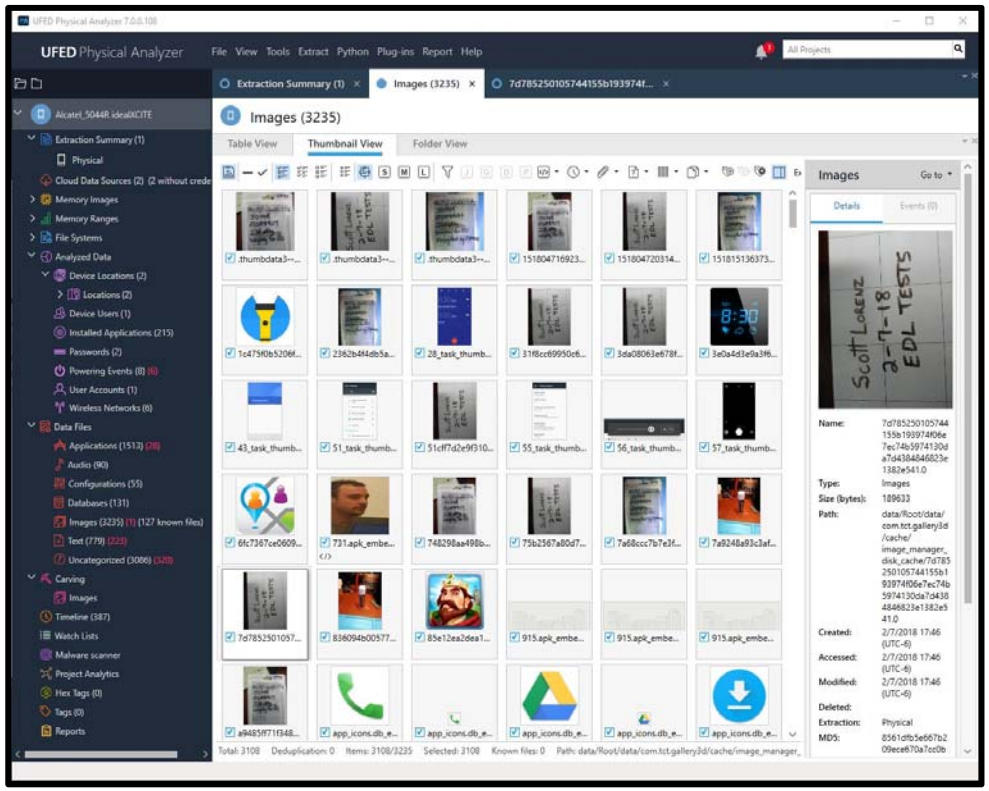
EDL extraction test – encrypted Alcatel 5044R

The test resulted in completely decrypted user data partition.

28 minutes total time elapsed from beginning the procedure with the UFED Ultimate 4PC, placing the device in EDL mode to extracting, opening and parsing the data.

The only tools needed are a laptop with UFED Ultimate 4PC and UFED Physical Analyzer installed, and a stock cable or Cellebrite's Cable 100.

Because this procedure is simple and fast, evidence can be seized, decrypted, extracted, parsed and viewed at a crime scene or the scene of a search warrant.

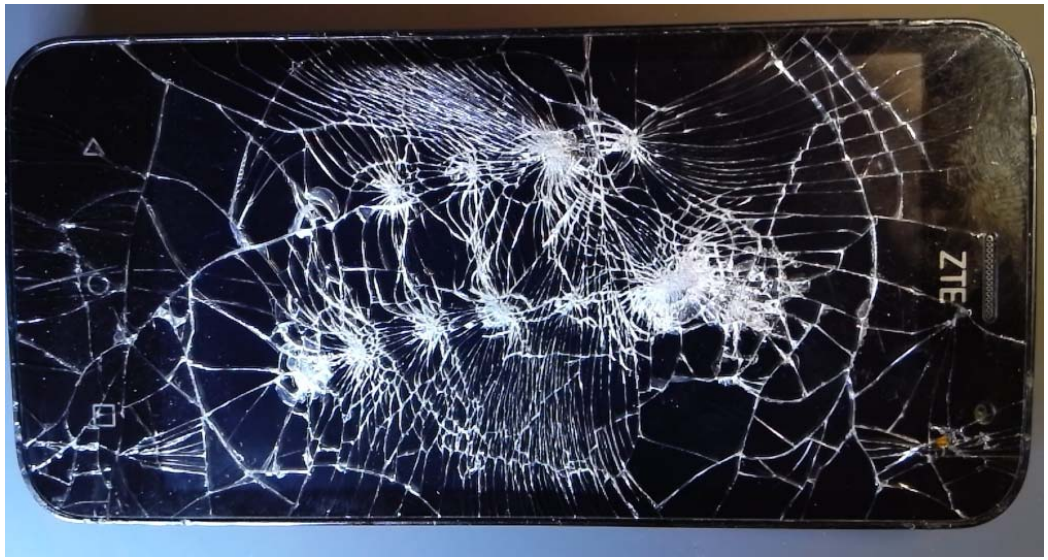


Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

Intake:

- Device was seized in an off-state
- Badly damaged
- Appeared completely inoperable



Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

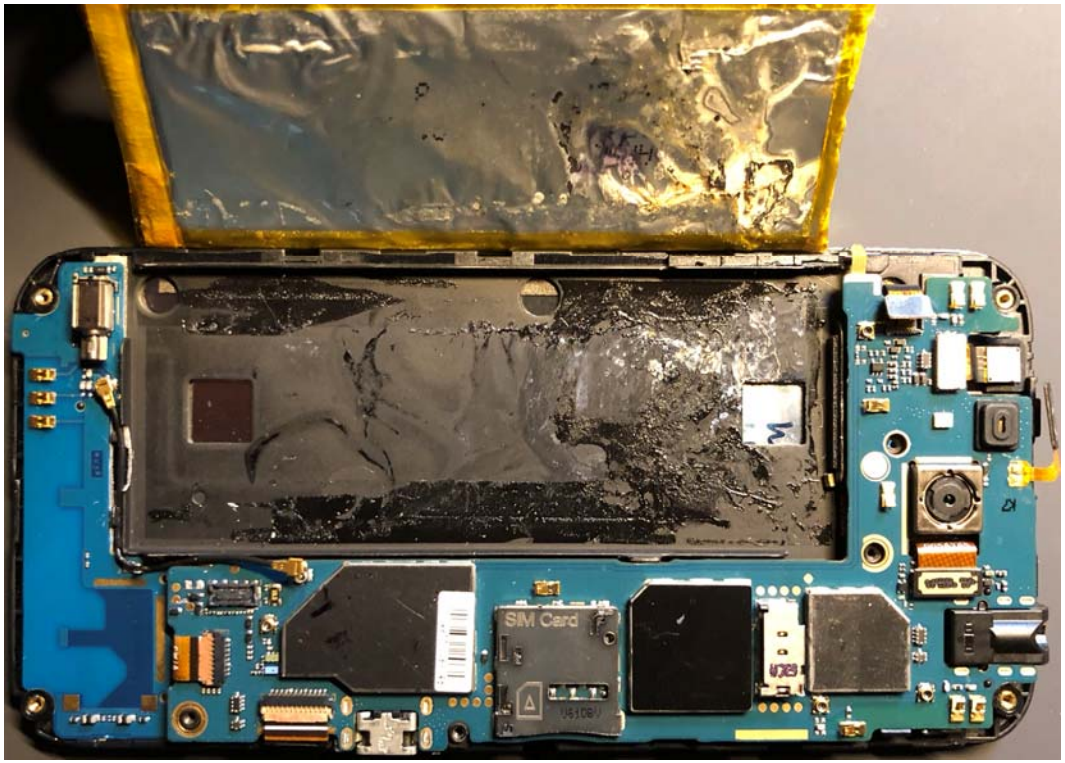
Intake: Signs of possible water damage, swollen batteries, or unknown conditions mean that attempts to charge or power-on the device could cause further damage.

Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

Intake:

- Identified phone as ZTE Z812, aka: ZTE Overture 2 / Maven
- Battery ruptured



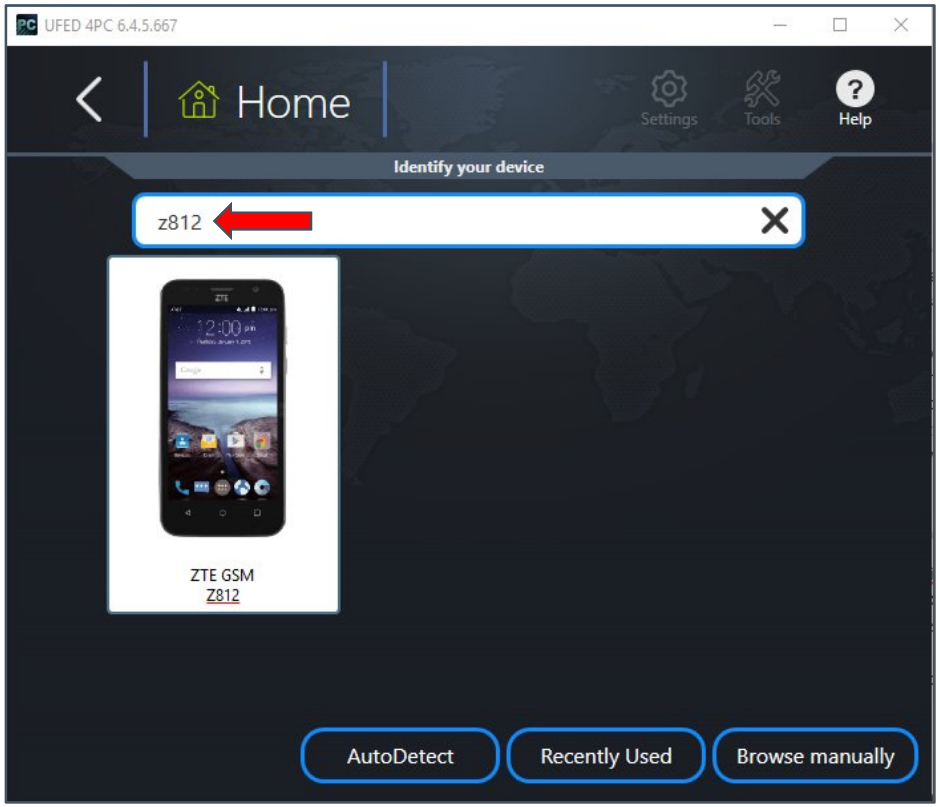
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

Is the ZTE Z812 a candidate for possible EDL extraction? How do you make this determination?

STEP 1: Check with Cellebrite UFED Ultimate 4PC or Touch2

- In this case the phone was badly damaged so AutoDetect through USB is not advised.
- Type in “Z812” then filter down to the device.
- Click on the device photo.



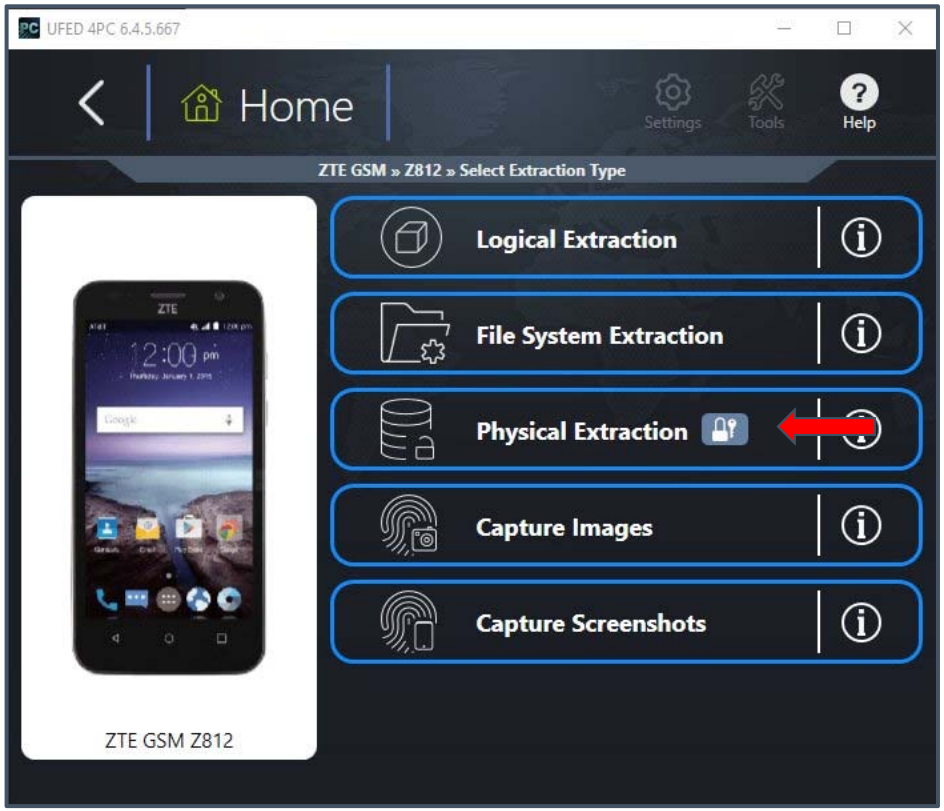
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

Checking for EDL support

STEP 1: Check with Cellebrite UFED Ultimate 4PC or Touch2

- The UFED reveals there is support for a physical extraction of a locked device for the Z812.
- Click on “Physical Extraction” for details on the next screen.



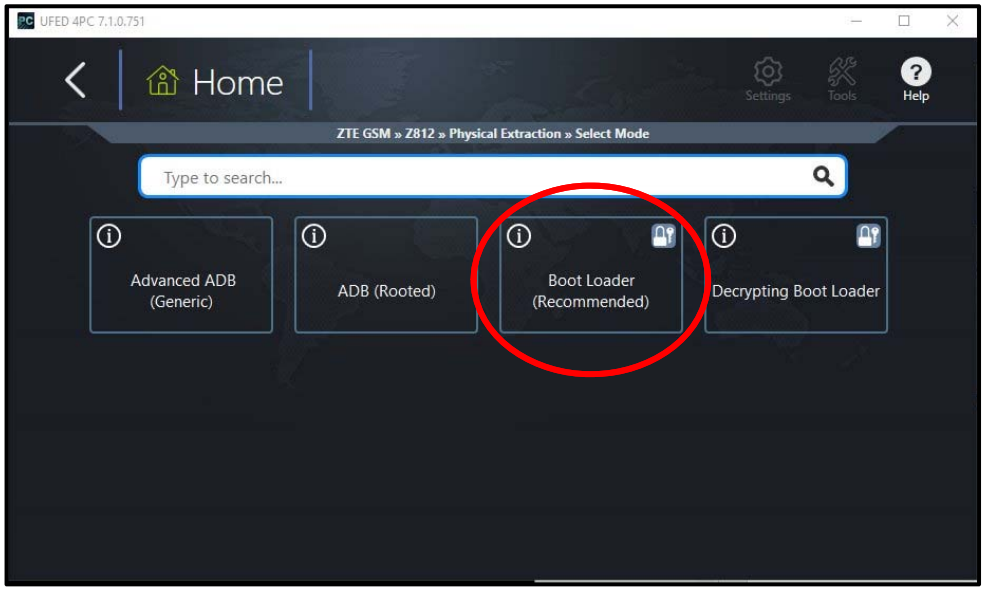
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

Checking for EDL support

STEP 1: Check Cellebrite UFED Ultimate 4PC or Touch2

- Click on “Boot Loader (Recommended)”



Cellebrite

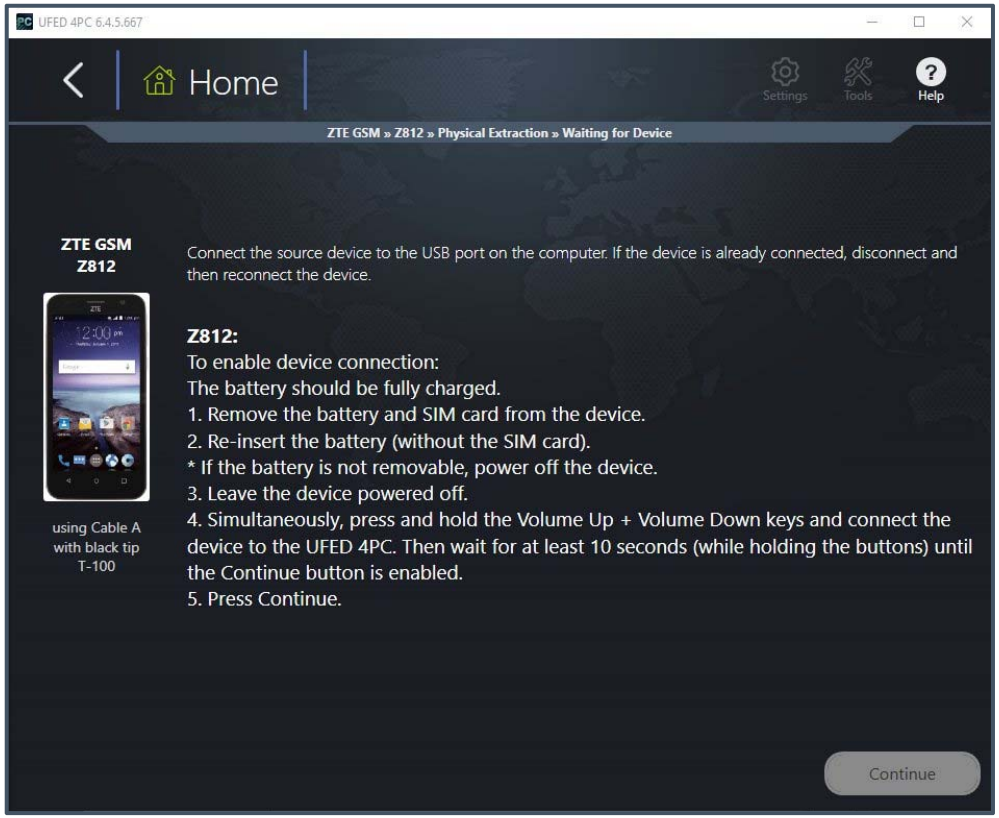
EDL extraction case study:
Narcotics investigation – badly damaged device

Checking for EDL Support

STEP 1: Check Cellebrite UFED Ultimate 4PC or Touch2

The extraction instructions listed here indicate that this is an EDL extraction. However, the condition of this device means that you will have to seek an alternate method to place the device in EDL.

*Note: Using alternate methods of achieving EDL for an extraction can be accomplished under the device profile or using the generic Qualcomm physical extraction.



Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

Checking for EDL Support

STEP 2: Determine what processor the ZTE Z812 is running.

A device may not be supported under the device profile in the UFED. It is still possible to extract a device via the EDL method under the generic method depending on the processor used by the phone.

There are various resources for determining what processor a phone is running. Here are a few:

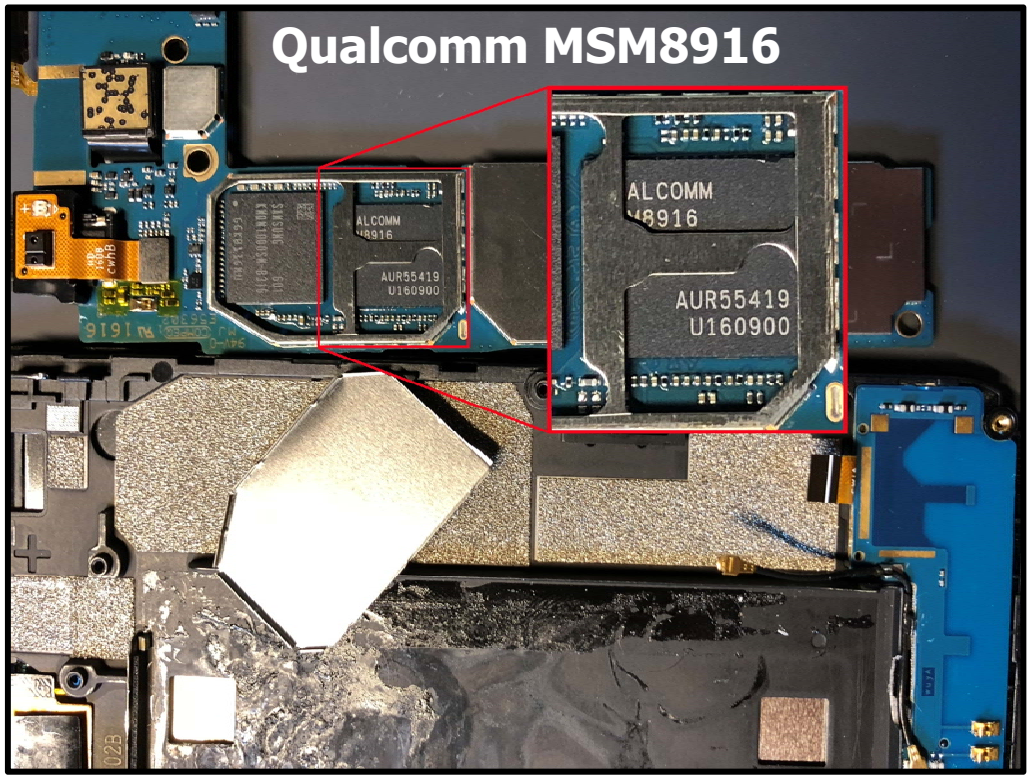
- www.phonescoop.com
- www.gsmarena.com
- https://www.fcc.gov/oet/ea/fccid
- http://phonedb.net/index.php?m=device

EDL extraction case study:
Narcotics investigation – badly damaged device

Checking for EDL Support

STEP 2: Determine what processor the ZTE Z812 is running.

Manual Inspection of the Device may be a fairly easy option for some phones. In this case, removing the logic board and the heat shield covering the processor was relatively easy.



Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

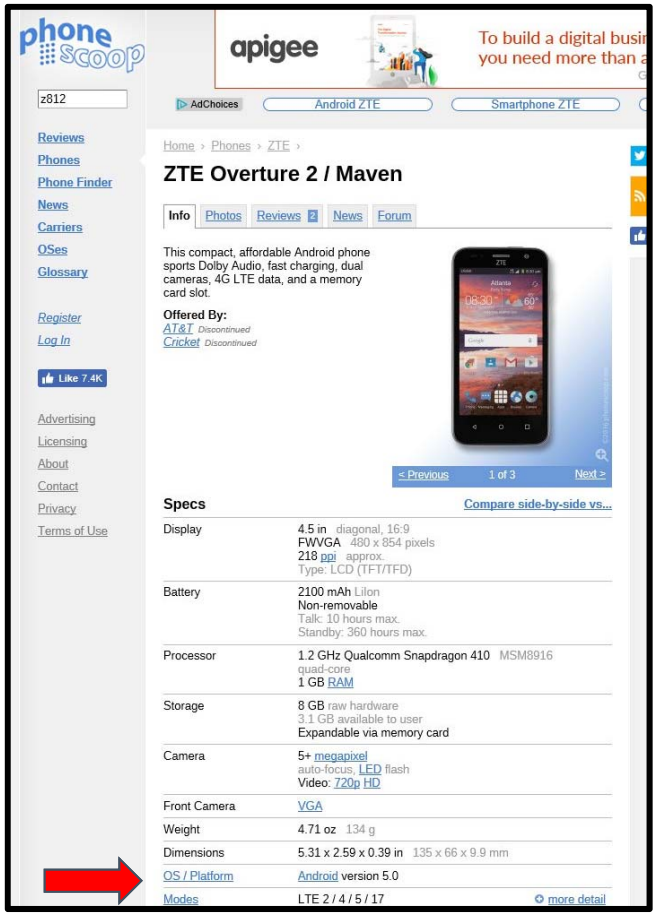
Checking for EDL Support

STEP 3: Is the device encrypted?

Many of the same databases used to research the processor can be used to determine whether the phone will likely be encrypted or not.

Phones shipped with Android 6 or higher are likely to be encrypted “out of the box”.

The Z812 was released running Android 5.0 so it is not likely to be encrypted.

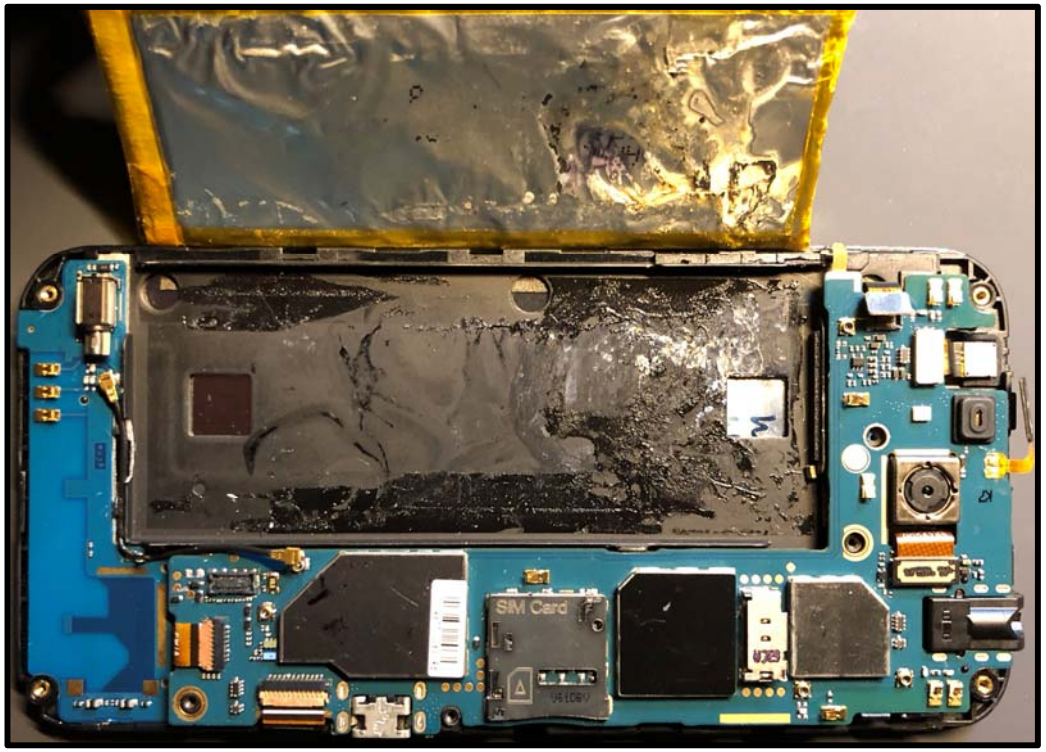


Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

Overview of Assessment:

- Identified phone as ZTE Z812, aka: ZTE Overture 2 / Maven
- Battery ruptured
- Unknown other damage
- Processor – MSM8916 is supported for EDL extraction
- Phone is likely not encrypted
- Phone will not pull with conventional methods due to damage



Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

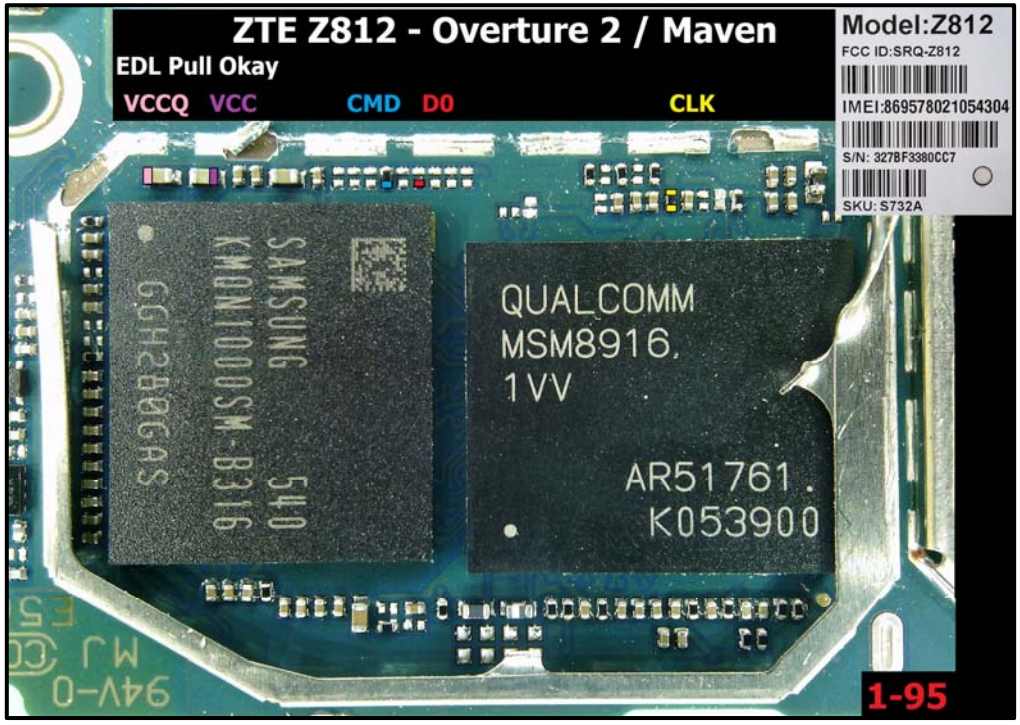
Overview of Assessment: Why EDL?

Before Cellebrite's EDL method of extracting devices, this phone and other damaged phones like it, would have to be extracted using advanced techniques like JTAG, ISP, or Chip-off.

While those techniques are reliable and produce forensically sound physical extractions, they require training, additional equipment or hardware, and practice.

Another limitation of JTAG, ISP and Chip-off is that these methods will not work on encrypted devices as there is currently no means to decrypt physical images after extraction.

Cellebrite's EDL method can decrypt data as it is being extracted from the device.



Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 4: Putting a device into EDL mode.

With this ZTE Z812, ADB and other automated functions offered by the UFED will not work because the phone is not functioning.

Button combinations will likely not work without power and a functioning phone.

Using an EDL cable or shorting the eMMC are possible methods to get the phone in EDL mode.

Using an EDL cable should be attempted before attempting to short the eMMC.

Cellebrite

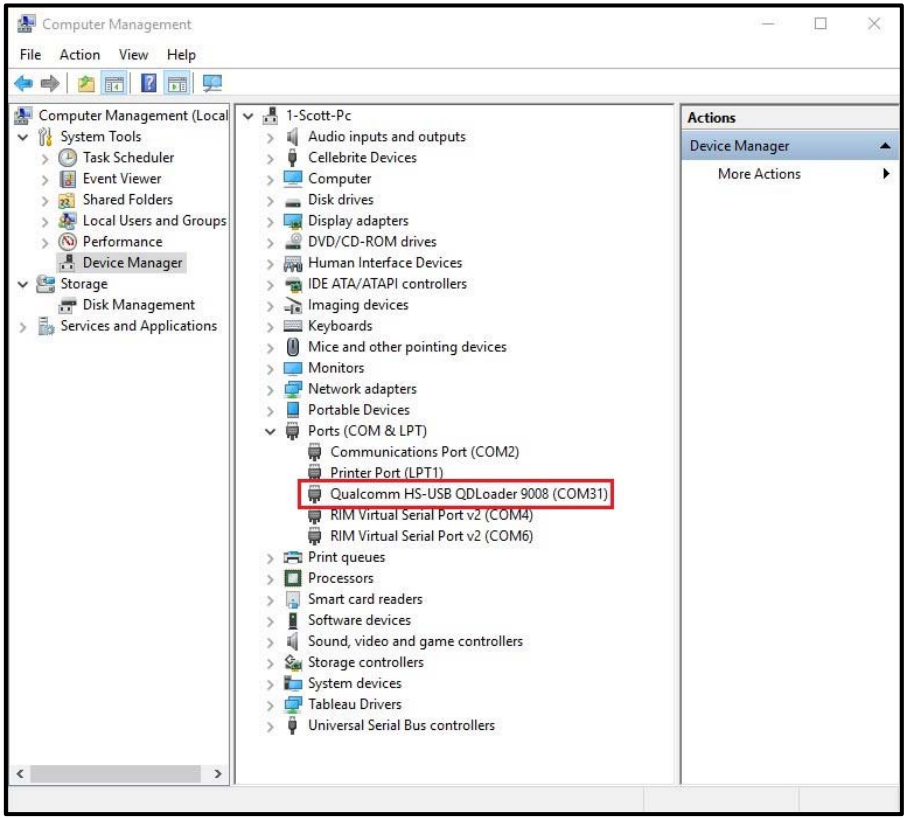
Cellebrite's EDL Cable # 523

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 4: Putting Device in EDL mode.

Before attempting an EDL extraction with the UFED Ultimate 4PC with a damaged device, it is best to test the method(s) you intend to use to initiate EDL.

On Windows systems it is possible to detect EDL mode when the device is connected via USB and the right conditions are met. Sometimes this may happen immediately and sometimes a driver may install.



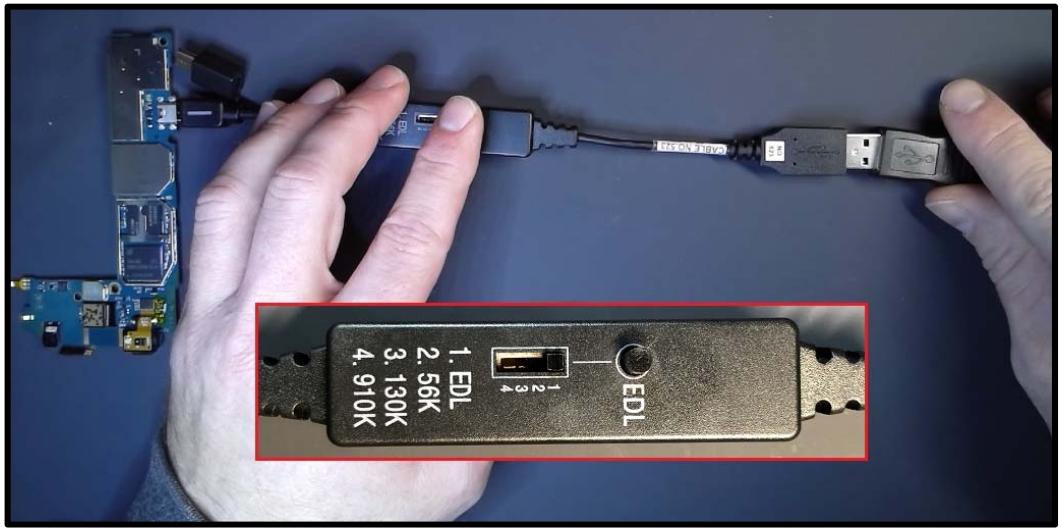
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 4: Putting Device in EDL mode.

Because this ZTE Z812 is so badly damaged with no working battery. I attempted to place it in EDL mode using only the Cellebrite EDL Cable # 523 and USB power from a windows PC.

- Connect the cable to the device.
- Make sure the selector switch is set to EDL.
- Press and hold the EDL button while connecting it to the PC.
- Release the EDL button when connected.

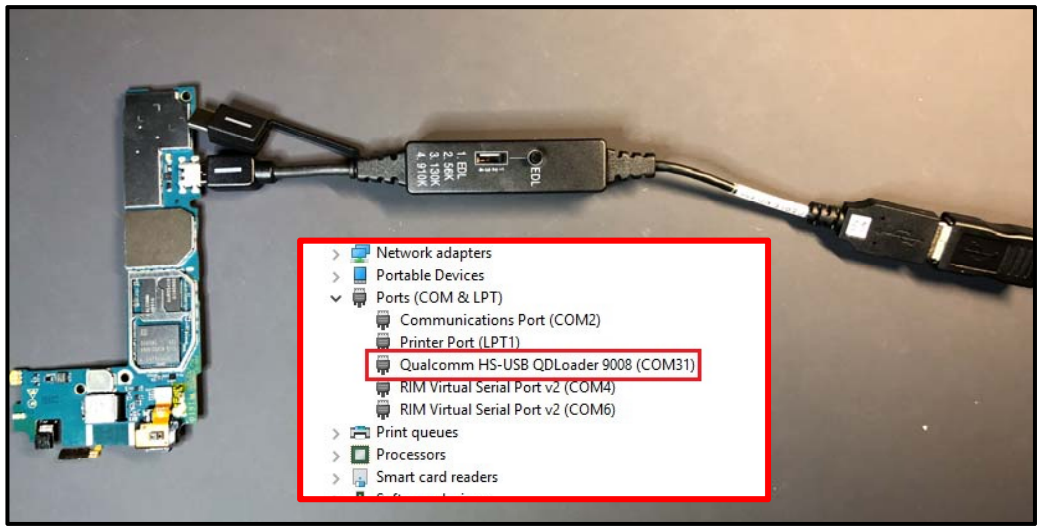


Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 4: Putting Device in EDL mode.

Once releasing the EDL button after connecting to the PC, an audible handshake will occur, device manager will refresh, and the device is now in EDL mode as show in device manager.



After confirming EDL mode can be achieved on the Z812, without a battery using cable # 523, the process will have to be repeated in conjunction with the UFED.

Disconnect the cable from USB and open the 4PC. Cable 523 can remain connected to the Z812.

Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

After confirming that the Z812 can be placed in EDL mode with cable # 523, it has been disconnected from the PC and is no longer in EDL mode. (Devices with no battery are no longer in EDL mode when disconnected from USB)

Leave the device disconnected from the PC.

Begin navigating through the menus of the UFED to extract the device by selecting “Mobile Device”

Cellebrite

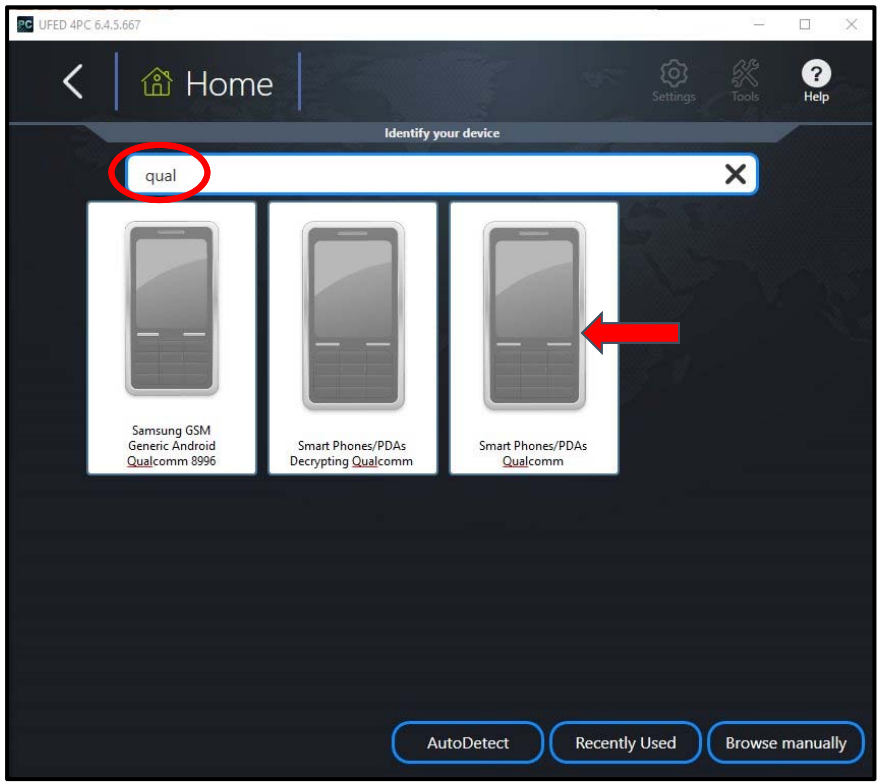
EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

Even though the Z812 is supported for EDL under the Z812 profile, this EDL extraction cam be performed under the generic Qualcomm options.

Start typing the word Qualcomm in the manual search bar. Three options will appear.

Because this Z812 is presumed to be unencrypted, select “Smart Phones/PDAs Qualcomm”

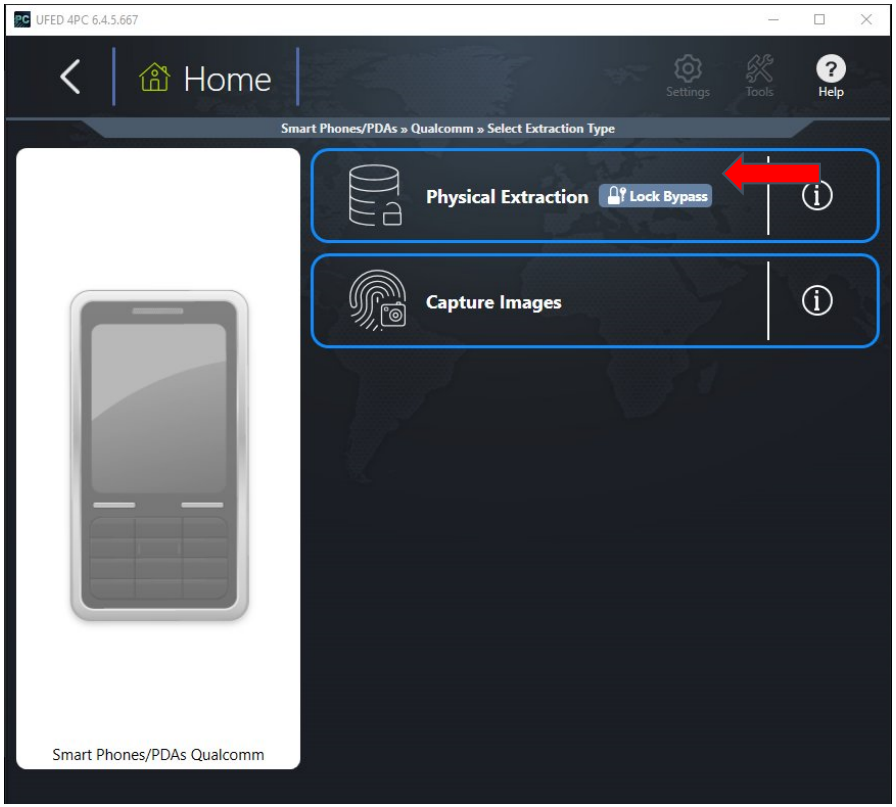


Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

Select “Physical Extraction Lock Bypass”



Cellebrite

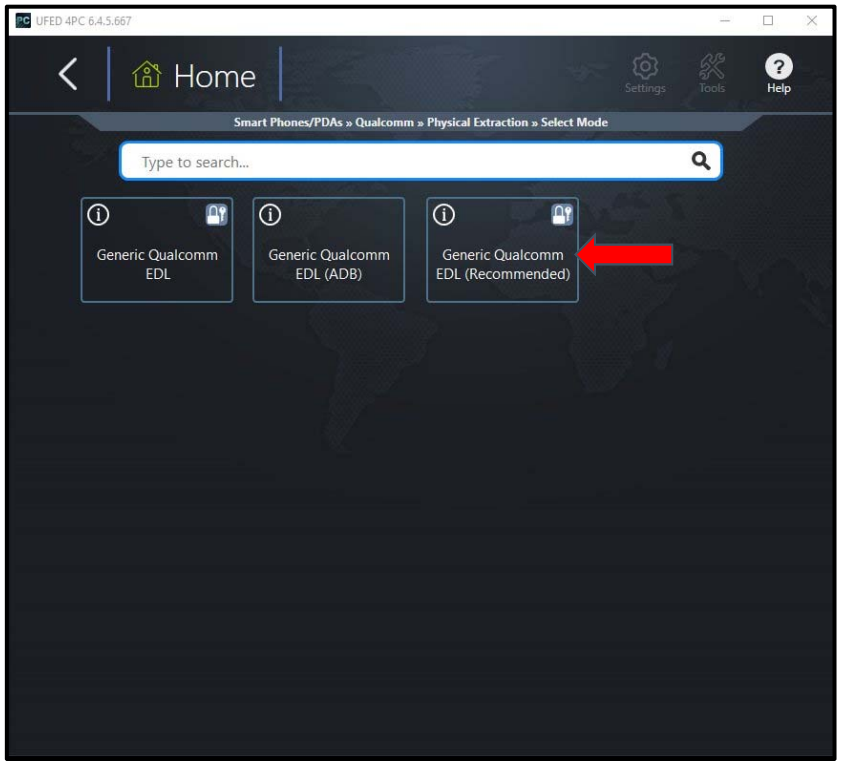
EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

Select “Generic Qualcomm EDL (Recommended)”

This method is used as an option when the examiner is placing the device to be extracted in EDL mode via external methods.

- eMMC shorts
- Test points
- EDL Cables
- Button Combinations
- ADB using command line



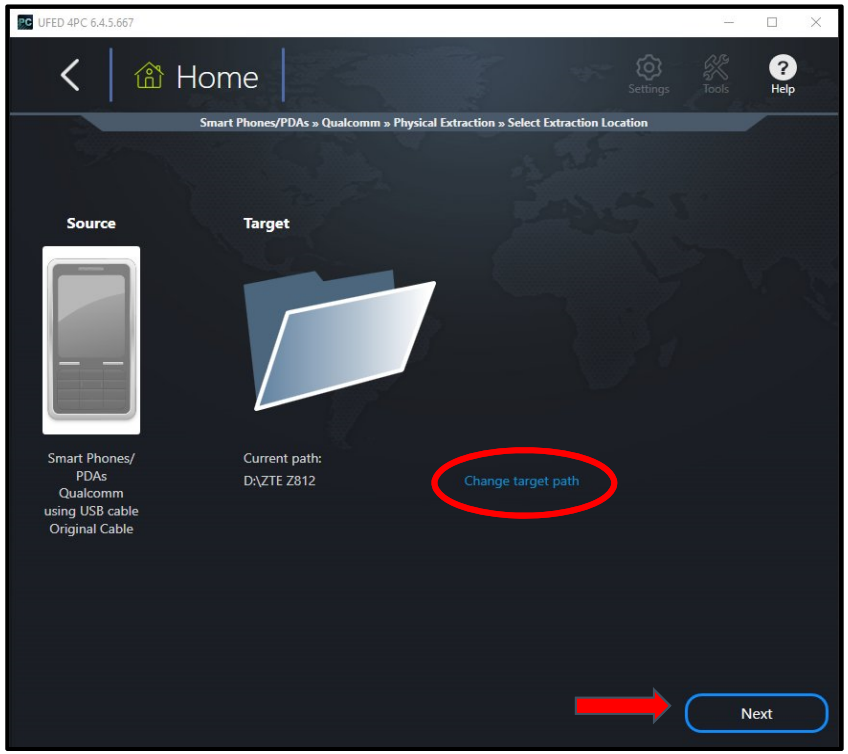
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

Choose a target location for the extraction.

Click Next.



Cellebrite

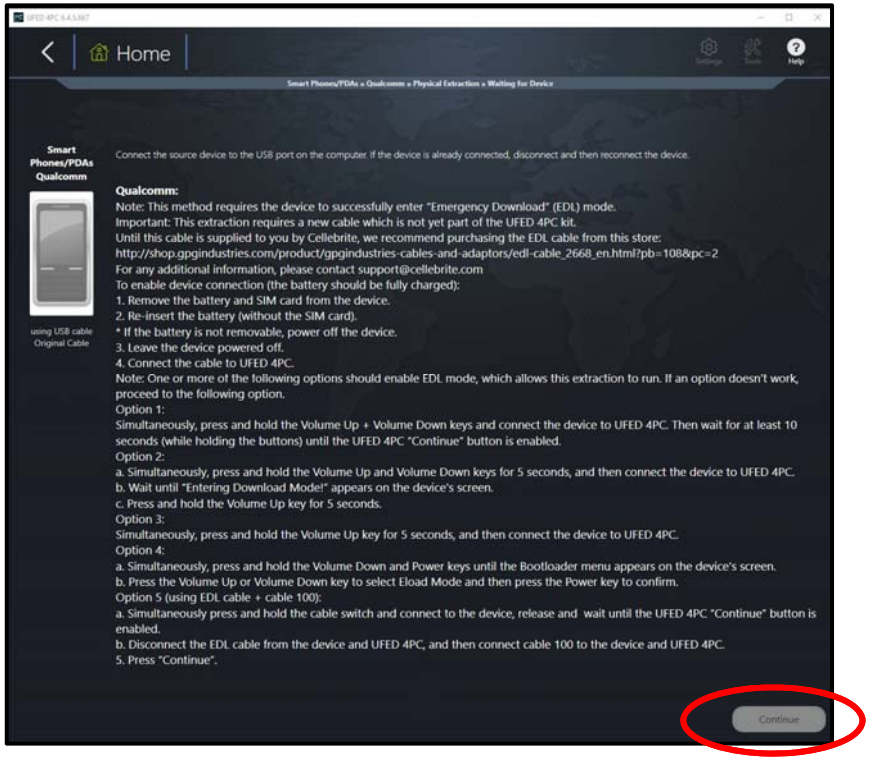
EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

When reaching this screen the “continue” button should be grey. This is because the device to be extracted is not connected to the PC yet and is not in EDL mode.

The UFED describes a variety of different methods for placing devices in EDL mode. The test conducted on the Z812 before starting the UFED demonstrated that using Cellebrite’s EDL Cable # 523 will place the device in EDL mode.

The steps taken to achieve EDL during the initial test should be duplicated here.



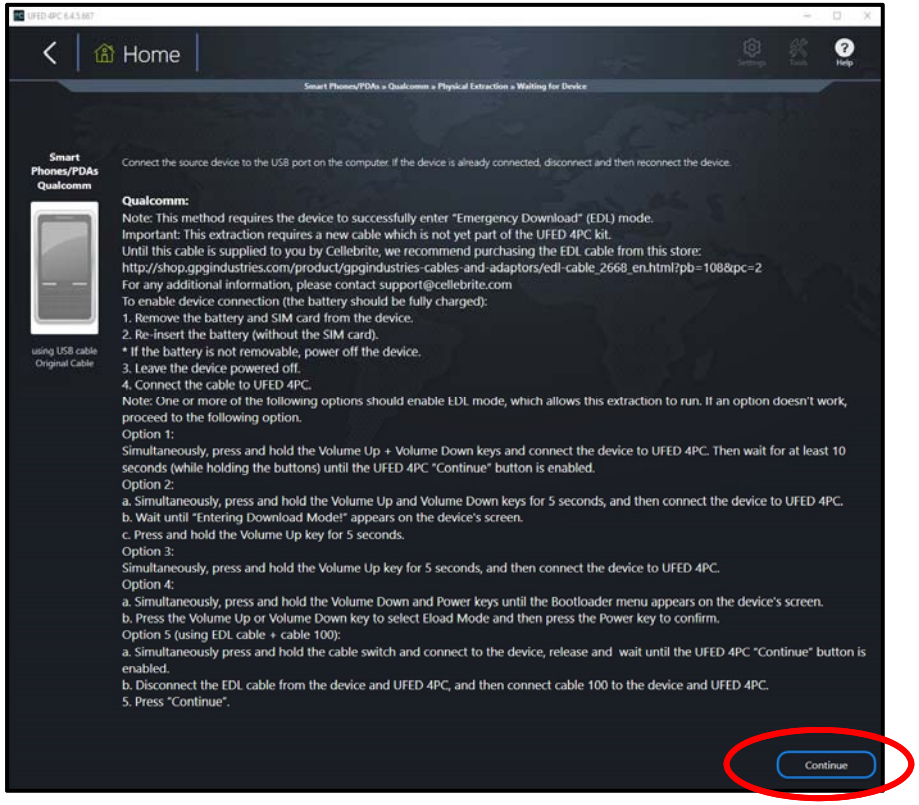
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

Repeating the steps described earlier at this point in the UFED menus will place the Z812 back in EDL mode and the “Continue” button will become active. An audible handshake will occur and device manager will refresh.

Click “Continue”.

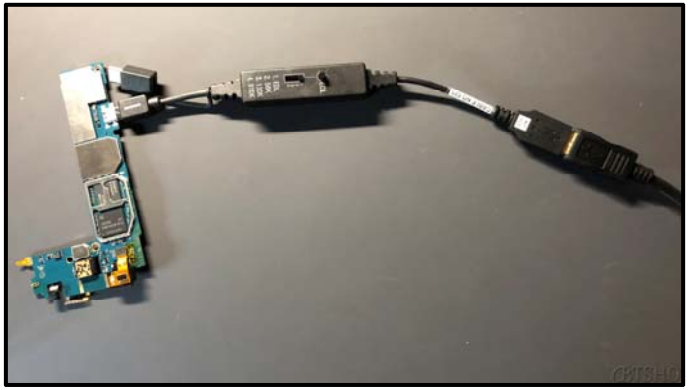


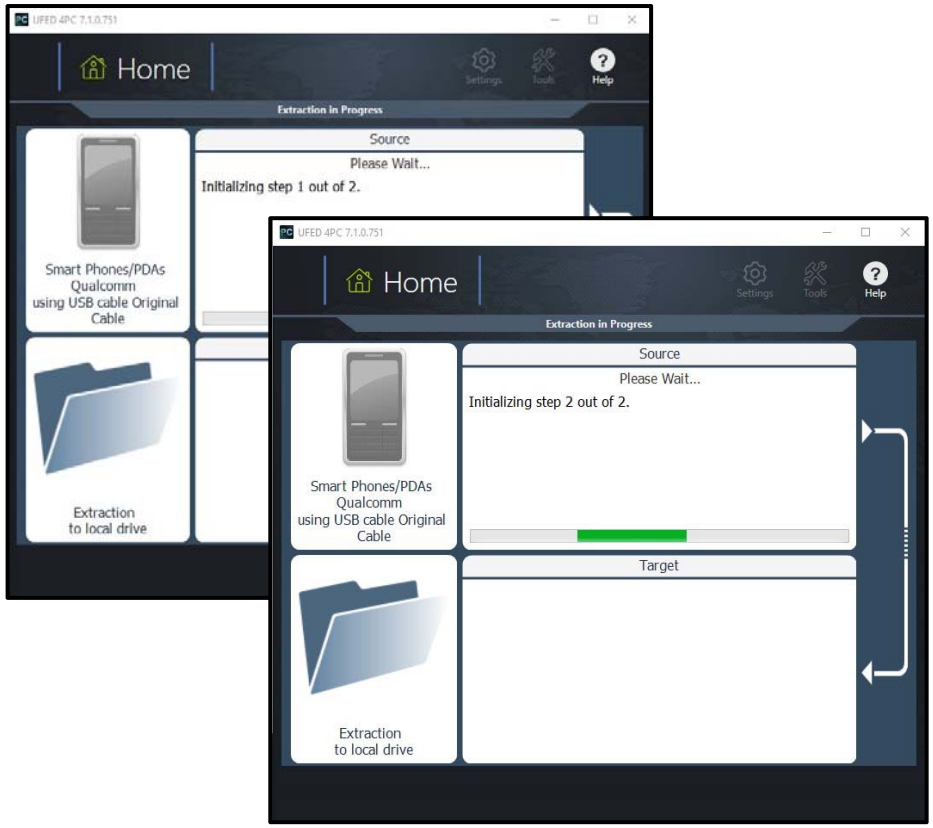
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

After hitting the “continue” there will be two initializing screens.



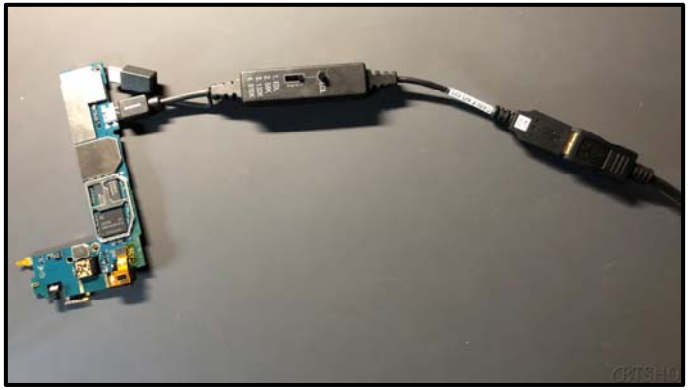


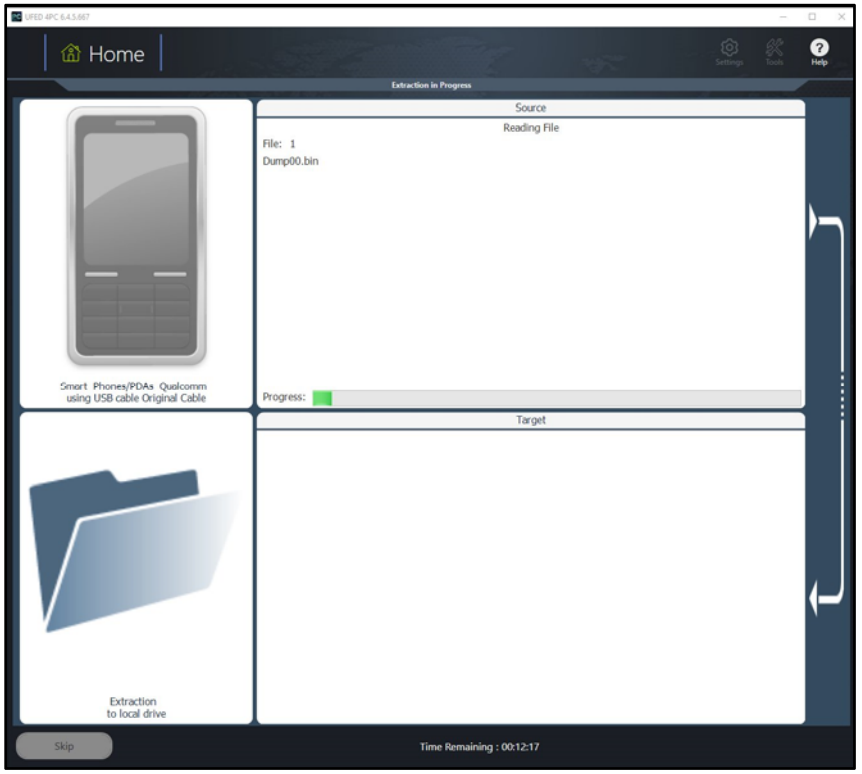
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

The final screen will be the physical dump. Dump00.bin…



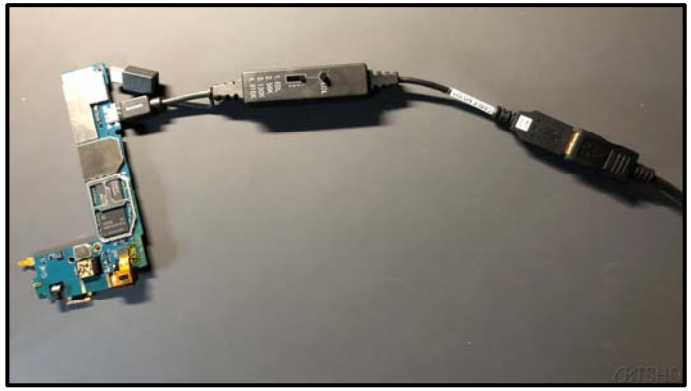


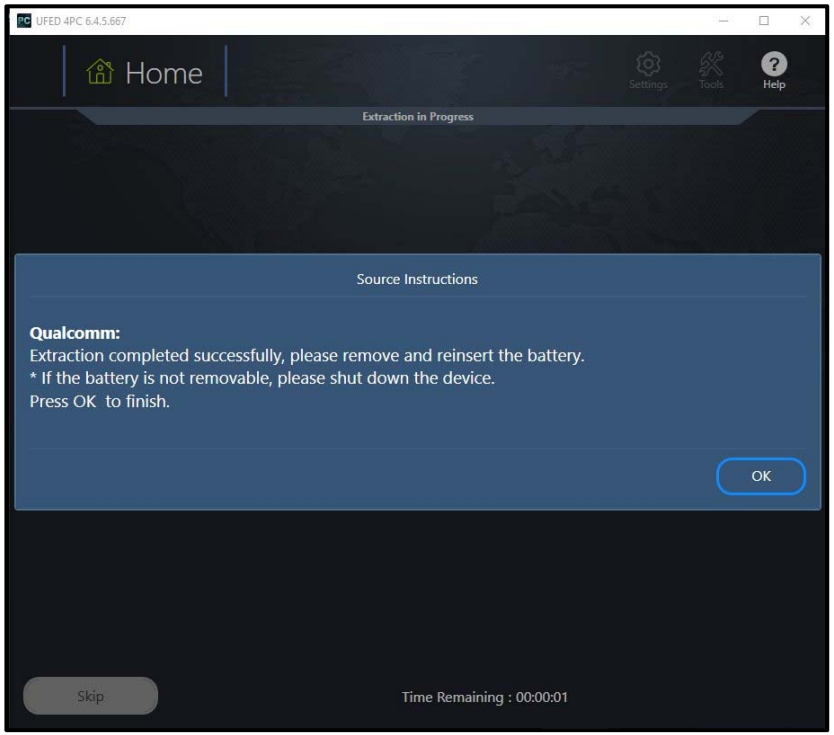
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 5: Extracting the Z812 with the UFED via EDL method.

After the extraction is completed you may disconnect the device from the UFED.
Press “OK”



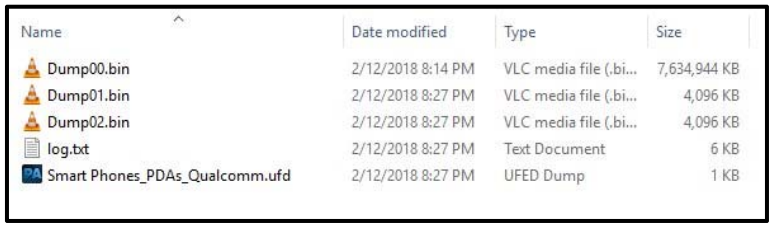


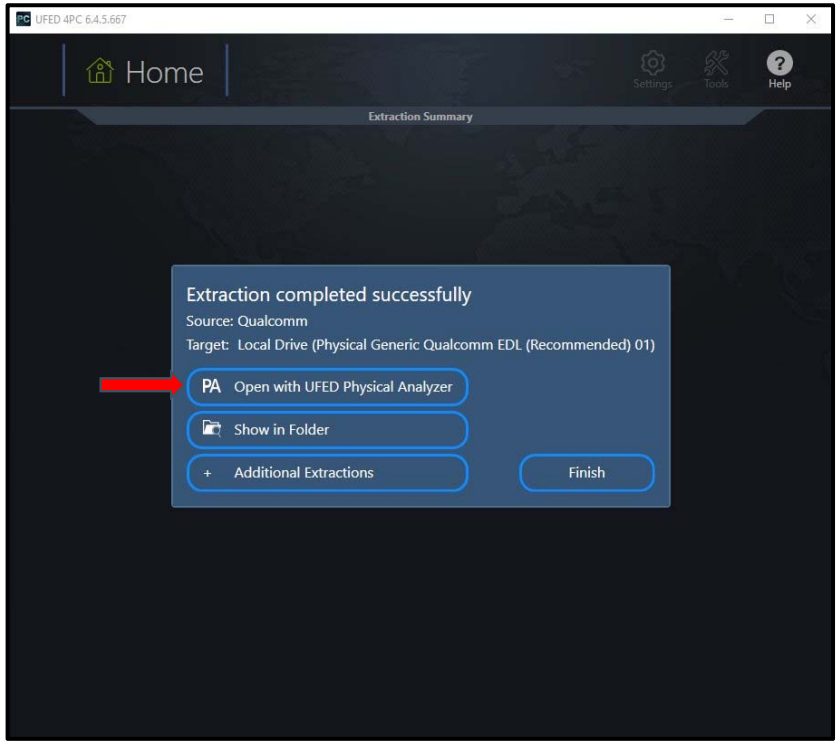
Cellebrite

EDL extraction case study:
Narcotics investigation – badly damaged device

STEP 6: Open Extraction

The extraction is completed and you can open the extraction in Physical Analyzer from this screen or navigate to the extraction location and open the .ufdx or the .ufd file.





Cellebrite

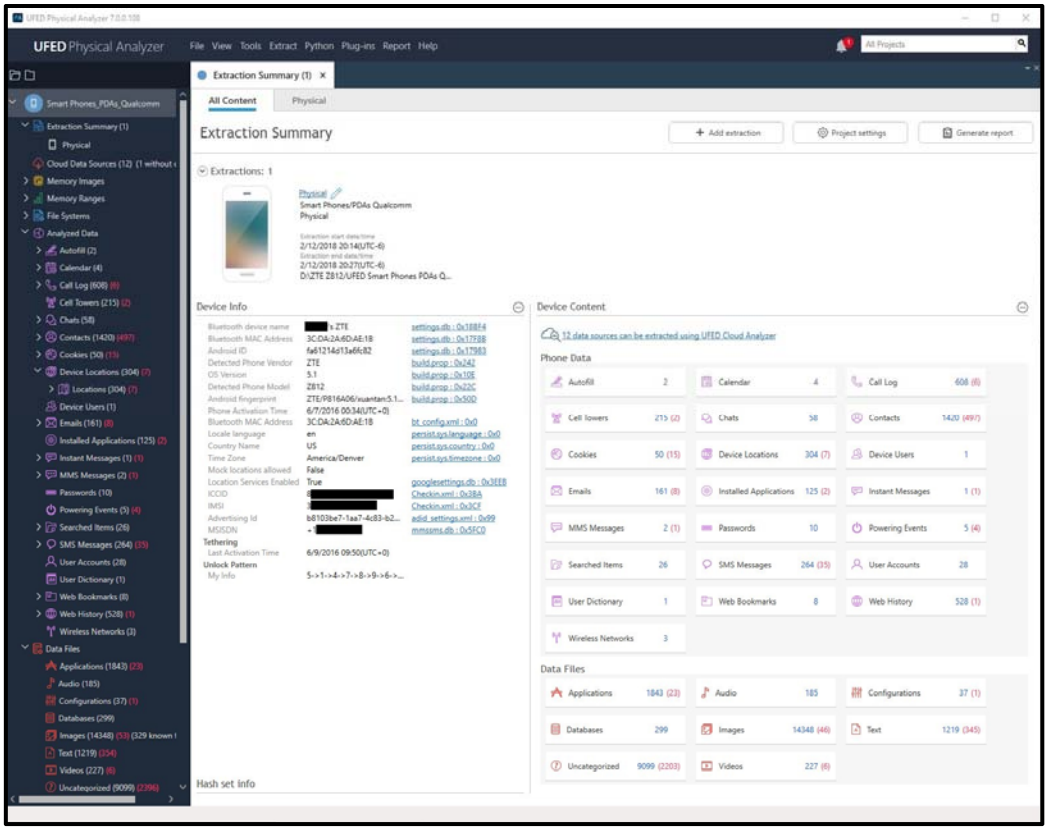
EDL extraction case study:
Narcotics investigation – badly damaged device

Results

Other than any research that may have to be done. This phone can be extracted and parsed on a laptop at the execution of a search warrant or scene of a crime in about 30 minutes.

For narcotics investigators, this is an invaluable tool and can yield almost immediate actionable intelligence.

Before the EDL extraction method this phone would have to be sent to a lab with advanced capabilities.

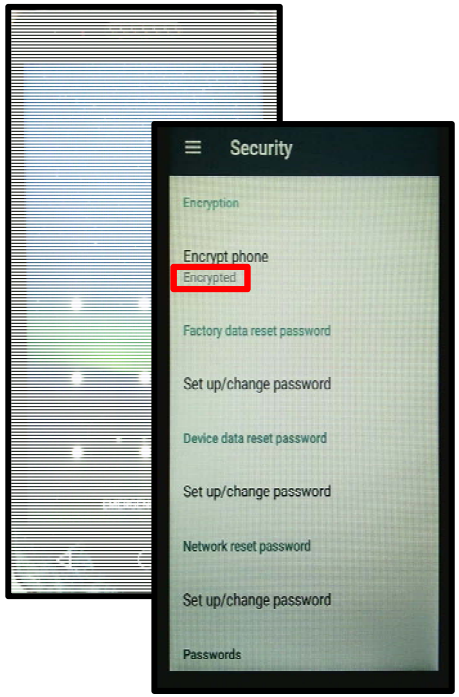


Cellebrite

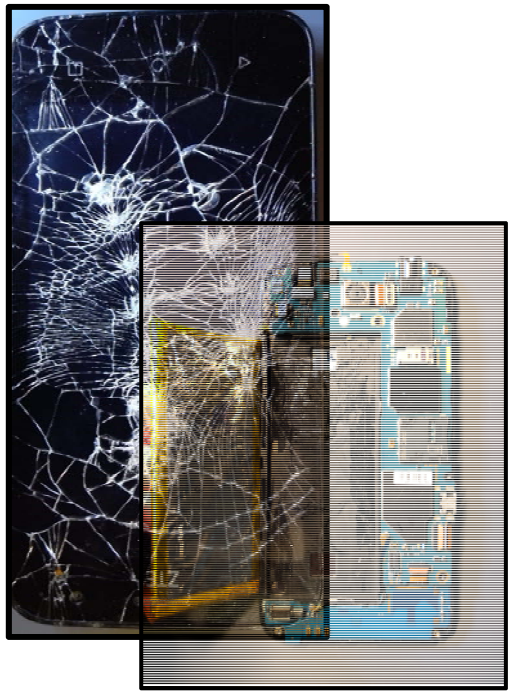
Cellebrite's EDL (Emergency Download) extractions

- Extract locked, encrypted devices
- Extract badly damaged devices
- Extractions done in minutes instead of hours
- Evidence on the scene instead of in the lab
- Forensically sound extractions of full physical **decrypted** images
- No advanced training required
- No disassembly required for many devices

Locked & Encrypted



Destroyed Devices



Cellebrite

Tips and resources

Cellebrite

Enter EDL cheat sheet

1. Key combinations – e.g. holding Vol+ and Vol-
2. Cable 523
3. ‘adb reboot edl’ (from FTM, too)
4. ‘fastboot oem edl’
5. Test points
6. eMMC fault injection

Some hardware methods, however, are built into the chipset, and cannot be disabled or removed by the manufacturer → **they always remain available.**

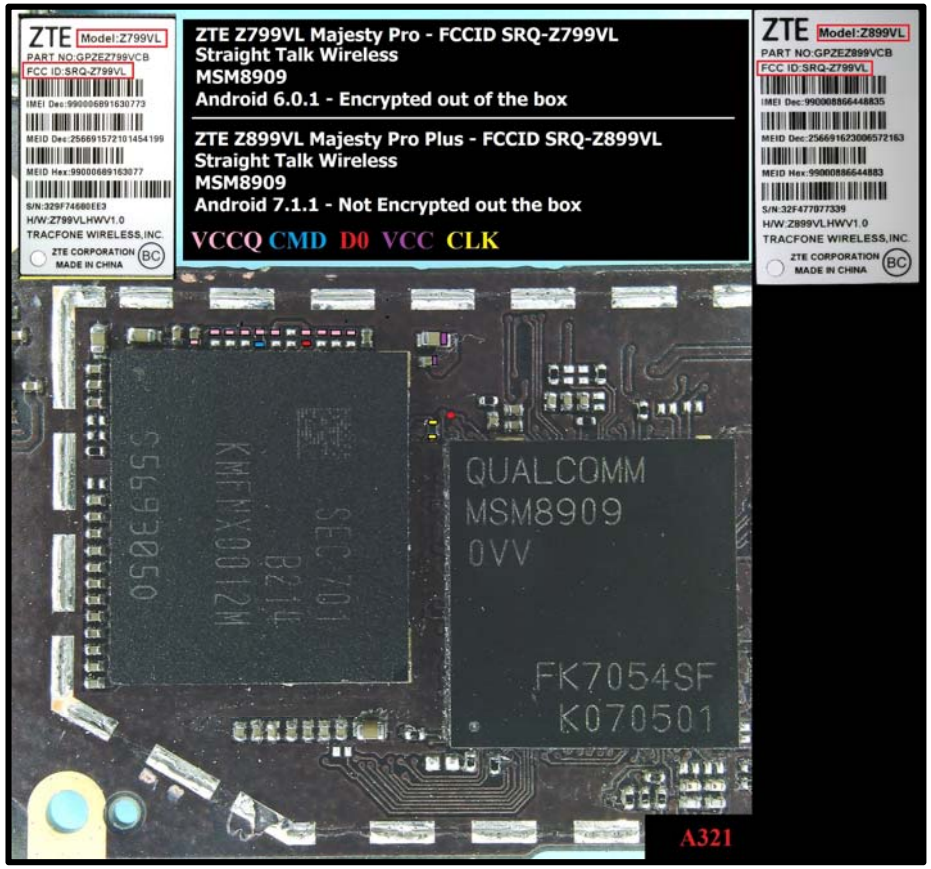
Entering EDL – eMMC faults (Shorting)

- Shorting the eMMC is one of the most reliable methods of placing a device in EDL. (Also the most invasive)
- Experience with ISP and Chip-off will be beneficial with this method of introducing EDL.
- Knowing the location of CMD, D0, and CLK pins on a device will be useful if it is necessary to short the eMMC to introduce EDL
- Shorting the power lines is not recommended.

Cellebrite

Entering EDL – eMMC faults (Shorting)

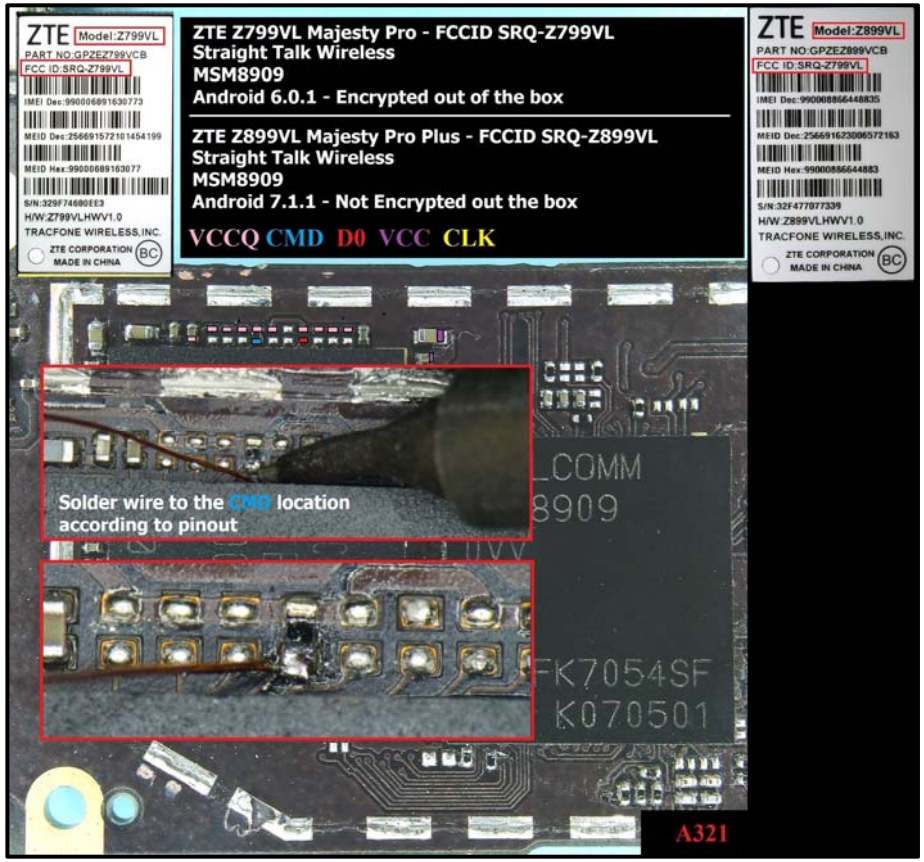
- ZTE Z799VL aka: Majesty Pro
- ZTE Z899VL aka: Majesty Pro Plus
- Both devices have the same FCCID – SRQ-Z799VL
- The ISP pinout for both devices is the same so we can use the pinout to create EDL on either device.
- In this example we will short the CMD on the Z899VL (not encrypted)
- The short is created by grounding the CMD while introducing power to the device.



Cellebrite

Entering EDL – eMMC faults (Shorting)

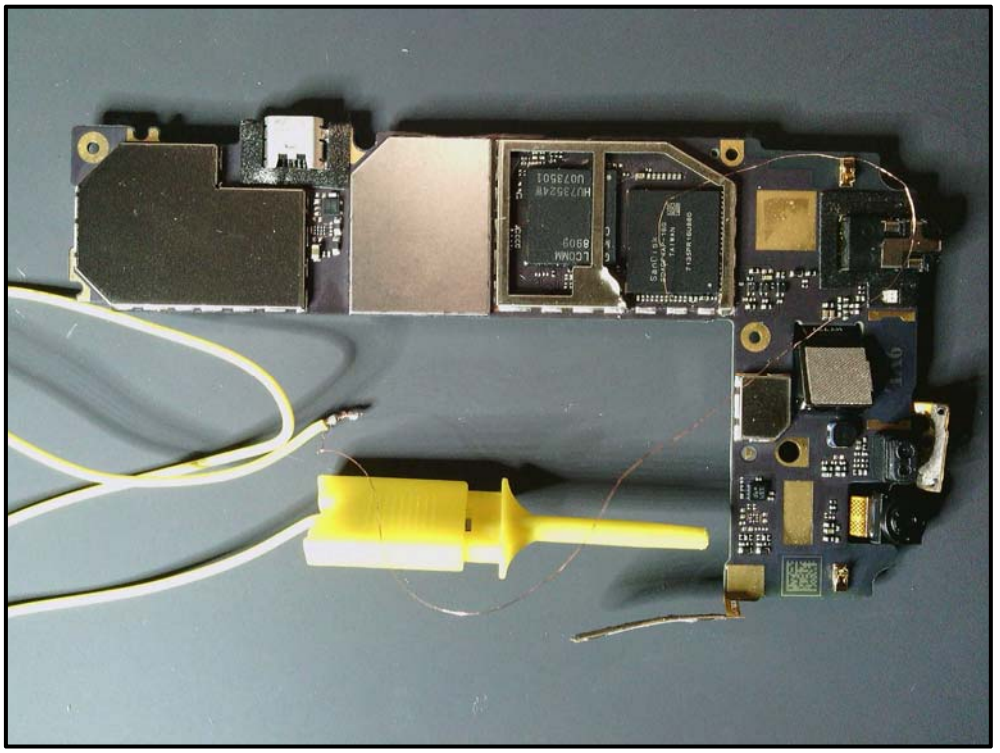
- Shorting ISP points usually requires soldering because the points are very small and the short may have to be applied while inserting a USB cable. (Also while holding power button with battery method)
- The short may have to removed or applied more than once during an extraction.
- A microscope is preferable.
- A wire with a clip on one end is preferable to apply and remove the short.
- All power removed and battery removed when soldering.



Cellebrite

Entering EDL – eMMC faults (Shorting)

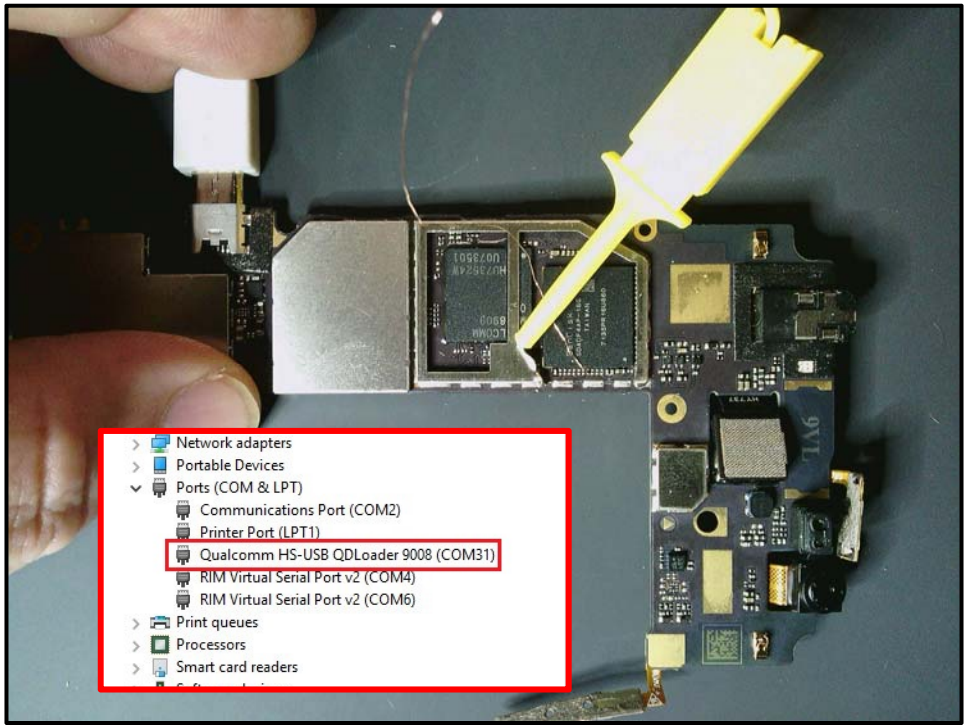
- The wire with the clip too large to solder to most ISP locations so it is preferable to use a smaller wire used for ISP and JTAG for the portion soldered to the device.
- The larger wire with the clip can now be used to apply and remove the ground by clipping to larger locations on the device.
- Clipping to any metal portion of the device will create the ground needed to create EDL.



Cellebrite

Entering EDL – eMMC faults (Shorting)

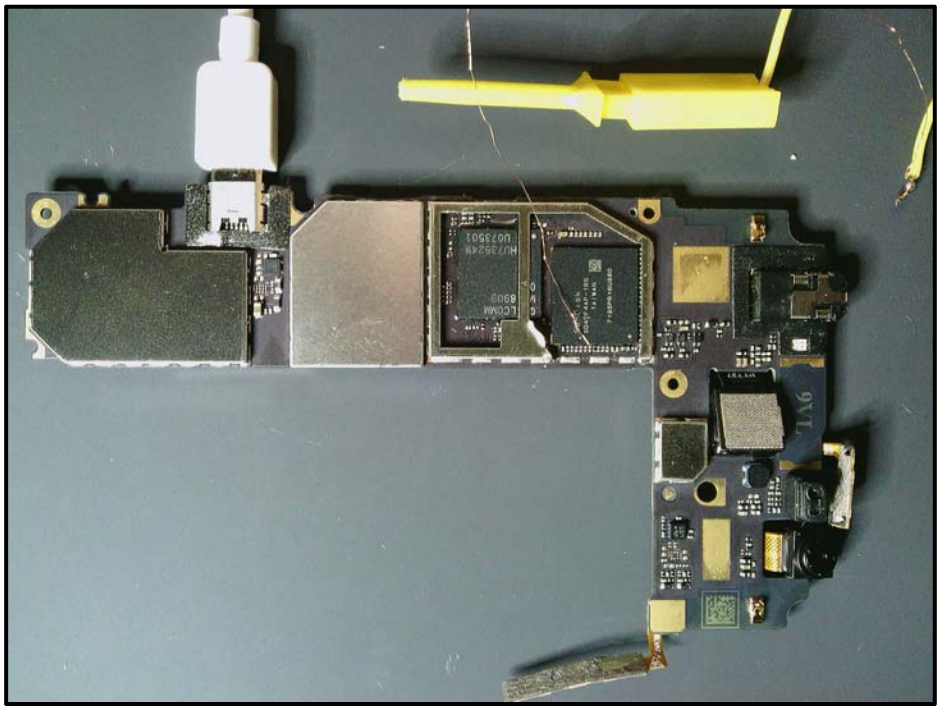
- With the clip attached to the heat shield frame and the other end soldered to the CMD location, all that is needed is to plug in the USB cable.
- No battery is required for this method for extracting a device that is not encrypted.
- As with the Z812, EDL is created as soon as the device is connected to USB while shorted.
- Test the method using device manager.



Cellebrite

Entering EDL – eMMC faults (Shorting)

- With the phone in EDL mode remove the cable before beginning the extraction.
- The short used to place the device in EDL will prevent the UFED from extracting if the short is not removed.
- Practice using this method to put the device in EDL before opening the UFED 4PC.
- The same coordination with the UFED as demonstrated with the ZTE Z812 must be followed with this method.



Cellebrite

Device support

Widely supported list: MSM8909, MSM8916, MSM8936, MSM8939, MSM8952

- Other chipsets are sometimes supported, but support is limited

If you can put the device in EDL, it is safe to try the Generic Qualcomm methods.

We are always working on supporting more devices, and hope to extend the widely supported list in the future.

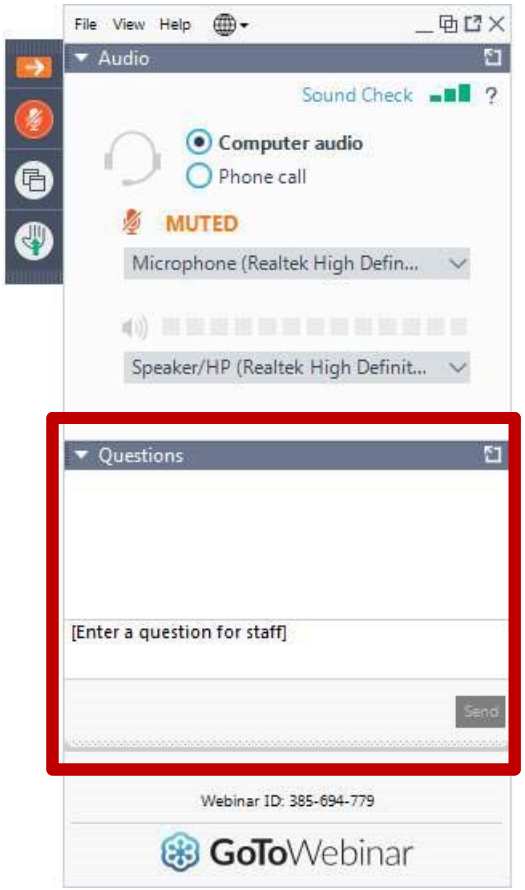
EDL and Decrypting EDL are available in **UFED 7.1** released yesterday

- We have more very interesting methods in the pipeline for this year…

Cellebrite

Q&A

Please submit questions via the Question Section located in the operator panel.



Cellebrite

Wrap up and resources

Practical guide for Qualcomm EDL extractions

Available in UFED 6.5 release notes published in January 2018

Cellebrite

Cellebrite Digital intelligence for a safer world

Thank you

Scott Lorenz
Professor of Criminal Justice at Central Texas College, Chief Forensic Analyst – Centex Technologies

Shahar Tal
Vice President of Research at Cellebrite Security Research Labs