Cellebrite Digital intelligence for a safer world

Safely Extract Digital Evidence with Emergency Download (EDL)

September 12, 2018

Revisiting EDL Theory

What is EDL?

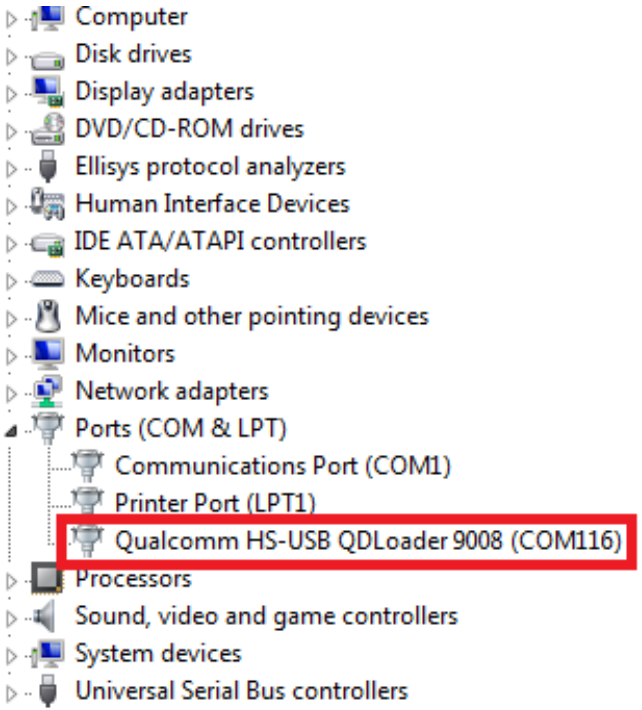
Qualcomm Emergency Download Mode **(a.k.a. QDLoader 9008)**

A rescue mode targeted for phone diagnostics & repair

- 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 Mode”s



What devices can be supported for EDL extractions?

- All mobile devices with Qualcomm processors can be placed in EDL mode
- Not all devices placed in EDL mode can be extracted with the EDL methods
- Placing a device in EDL mode will not harm a device
- Attempting to extract data from a device not supported for an EDL extraction with the UFED will not harm the device

Programmers (aka “Firehose”)

- Programmers are pieces of software containing raw flash read/write functionality
- Programmers can be digitally signed with a vendor signature that is verified by the device
- EDL accepts and verifies a programmer
  - ***The programmer must match both the hardware and signature requirement***

- e.g. to rescue LG G5 (MSM8996) with EDL, you must obtain programmer specifically created for the G5, supporting MSM8996, signed by LG Electronics.
  - You cannot use other MSM8996 programmers, you cannot use other LG programmers
- Some devices don’t require signatures at all (not common)
  - Require a hardware-matching programmer

EDL Extractions in UFED

- **UFED includes a wide set of programmers (>200)**
  - Will automatically attempt to match a valid specific programmer for the connected device
  - Should also match most devices that don’t require a signature
- **UFED has a proprietary exploit to bypass signature checks for several chipsets**
  - MSM8909, MSM8916, MSM8936, MSM8939, MSM8952
  - We call these chipsets “widely supported” because practically any phone with those chipsets can be considered supported
- **UFED has a unique method to decrypt user data partitions**
  - Don’t forget - programmers are designed to only allow raw flash access…

Decrypting EDL

- **Supported for decryption:**
  - MSM8909, MSM8916, MSM8936, MSM8939, MSM8952
  - MSM8996, MSM8917, MSM8937, MSM8940, MSM8953

- **To obtain decrypted user data, UFED will attempt to fully boot the device before the extraction stage begins**
  - Boot must complete normally or the decrypting extraction will fail

- **Some devices will not boot when peripheral disconnection is detected**
  - Missing battery / lcd / other may halt boot and prevent extraction

- **Secure Startup not supported**

UFED EDL Timeline

Capability	Available since
EDL Gen1 – Programmer-based	UFED 6.0 February 2017
EDL Gen2 - Signature bypass	UFED 6.4 October 2017
EDL Gen3 - Decrypting EDL	UFED 7.0 February 2018
EDL Gen4 - Extended Decryption	UFED 7.8 July 2018
EDL Gen5	In research

EDL Extractions in Practice

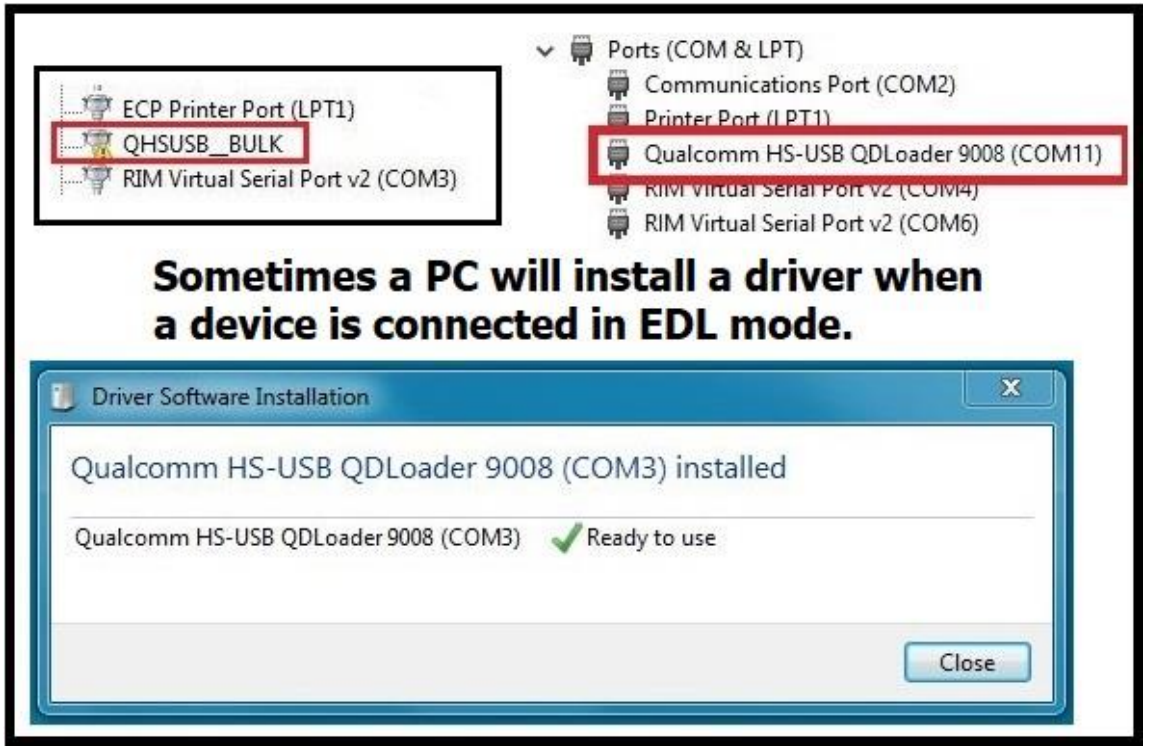
Methods Used to Create EDL Mode

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 (shorting)

Methods used to create EDL mode can be disabled on devices. Some hardware methods, however, are built into the chipset, and cannot be disabled or removed by the manufacturer → **they always remain available.**

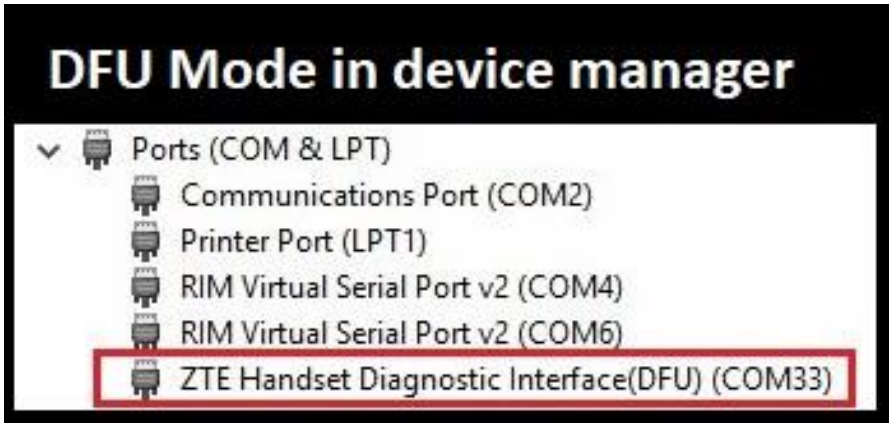
Checking a Device for EDL Mode in Device Manager

- Close UFED 4PC to test for EDL Mode
- A device in EDL Mode will appear in device manager
- An audible connection will occur when a device is connected in EDL mode
- The device screen will typically be black and appear to be off



Checking for DFU mode (Handset Diagnostic Interface)

- Close UFED 4PC to test for DFU Mode
- A device in DFU mode will appear in device manager
- An audible connection will occur when a device is connected in DFU mode
- The device screen will typically be black and appear to be off
- Some devices my have a blinking indicator light



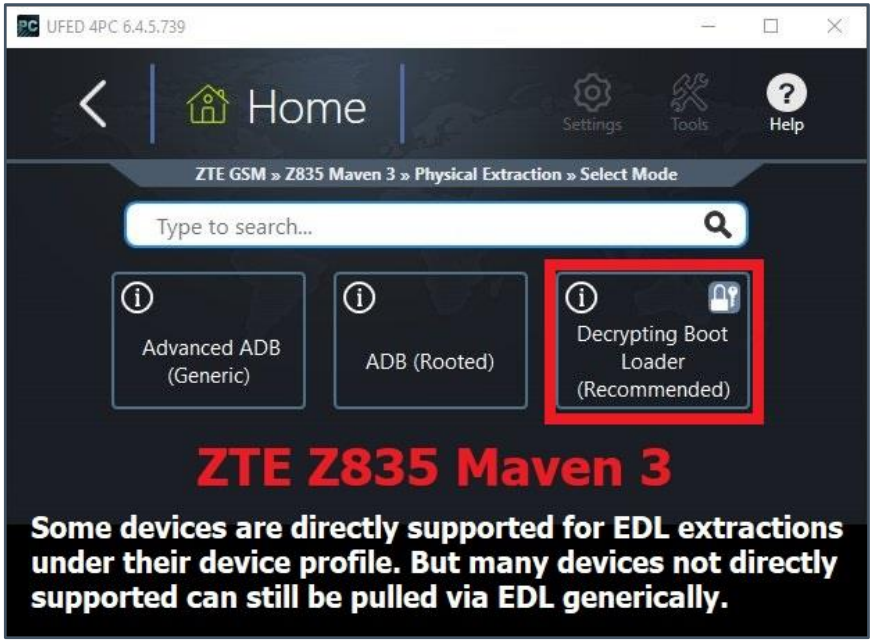
Checking for FTM mode (Factory Test Mode)

- Close the UFED 4PC to test for EDL Mode
- A device in FTM mode will appear in device manager
- A device will appear to be booting before entering FTM mode
- An audible connection will occur when a device is connected in DFU mode
- FTM mode will usually be visible on the device screen

ZTE Blade Spark placed in FTM by holding Volumn down and connecting to USB.

Devices Directly Supported for EDL Extractions with UFED

- Many devices are directly supported for EDL extractions
- Specific instructions are provided for placing the specific device in EDL mode
- These instructions will include key combinations or the use of cable # 523
- Devices supported for the “Decrypting Boot Loader” means that UFED will boot the device during the extraction
- Devices directly supported in UFED can also be extracted using the Generic Qualcomm profile



Generic Qualcomm EDL Extractions with the UFED

- Manually type in the word “Qualcomm”
- Choose decrypting or non-decrypting Qualcomm
- Either choice will attempt to extract any Qualcomm device using UFED’s EDL methods
- Used to attempt the extraction of any device whether or not it is listed as directly supported under the device profile in UFED
- Allows the user the option of a decrypting or non-decrypting extraction
- Requires the user to select the method used to create EDL, DFU, or FTM

Decrypting or Non-decrypting EDL Extractions?

Decrypting EDL Extraction

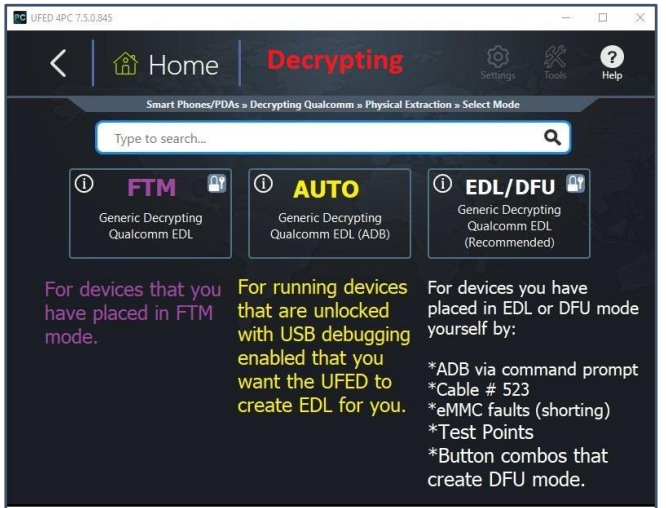
- Works on pattern or passcode locked devices
- For devices suspected to be encrypted
- Will require the device to boot
- Will usually require a battery
- Can be used on encrypted or non-encrypted devices
- Extracting a device that is not encrypted will produce forensically sound evidence

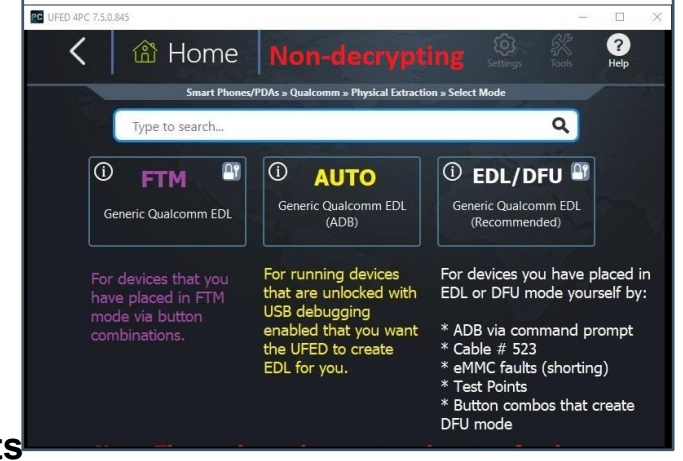
Non-decrypting EDL Extraction

- Works on pattern or passcode locked devices
- For devices suspected not to be encrypted by default.
- Low level extraction that will not require the device to boot
- Normally works without a battery and on damaged devices
- Will not harm encrypted devices or affect data on the device extracted

Menu Options for Decrypting and Non-Decrypting Extractions

- When using the generic Qualcomm EDL options, selecting the decrypting or non-decrypting method will present the user with the same three menu selections in UFED
- The method used to create EDL on the device to be extracted will determine which menu option to select
- Devices placed in DFU or FTM modes are still extracted via the EDL methods by UFED
- Many devices can be placed in EDL mode by more than one option
- Some devices can be placed in EDL, DFU, or FTM modes





Precautions Required for EDL Extractions

EDL mode itself is not harmful to devices. Devices can be placed in EDL mode many times without harming the device or affecting its normal operation. Methods used to create EDL mode can harm devices if done improperly or without training, research or preparation. Creating EDL mode on devices can require device disassembly, soldering to devices using a microscope, and intentionally shorting points on devices to ground. Any extraction requiring device disassembly can void warranties on devices or otherwise render devices inoperable even after a successful extraction of data. Some damage can prevent a successful extraction of devices by any means in not repaired.

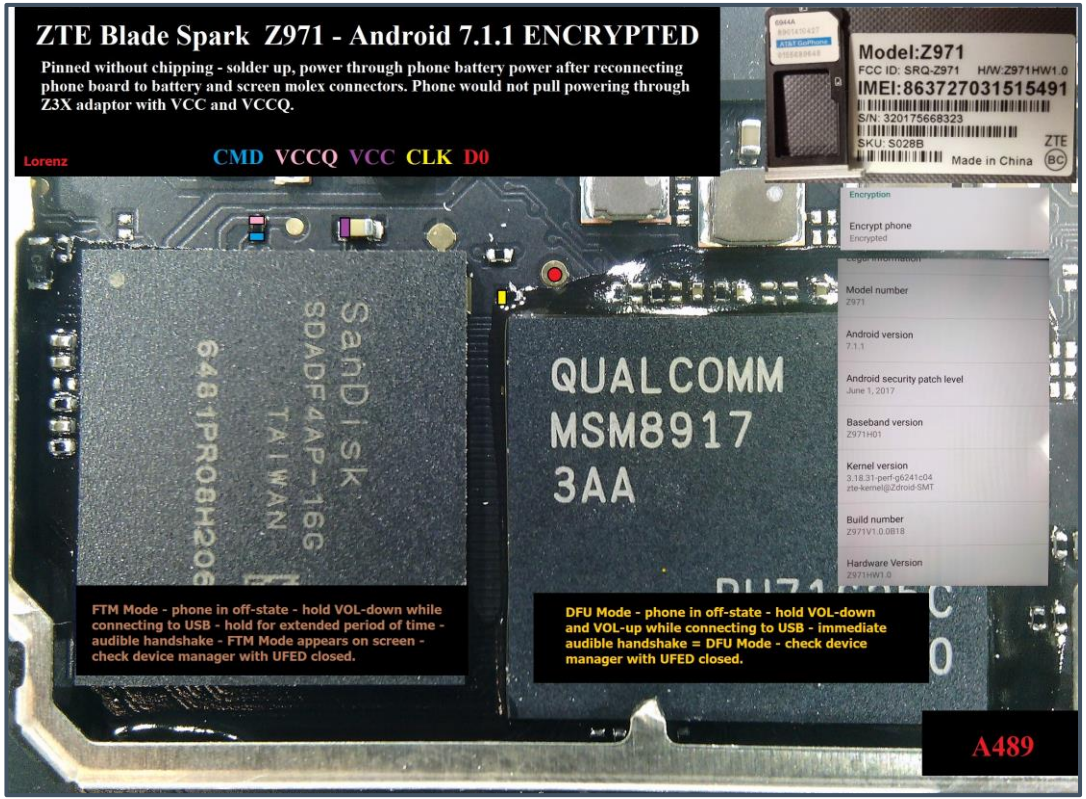
Common user-created damage occurs when users:

- Disassemble a device without research or proper tools
- Remove heat shields on the logic board, causing gouges in the board or damage to resistors or capacitors
- Solder to devices without a microscope or proper equipment
- Shorting the wrong location on a device

ZTE Blade Spark – Android 7.1.1 Encrypted – Cable 523

- Cable 523 can be used on devices that are user locked and encrypted
- The ZTE Z971 can be extracted by using several methods to create EDL, DFU, or FTM mode
- Cable 523 is an EDL cable and creates EDL mode by shorting the D+ line inside the USB cable
- EDL is created by pressing and holding the EDL button while connecting the device to the UFED

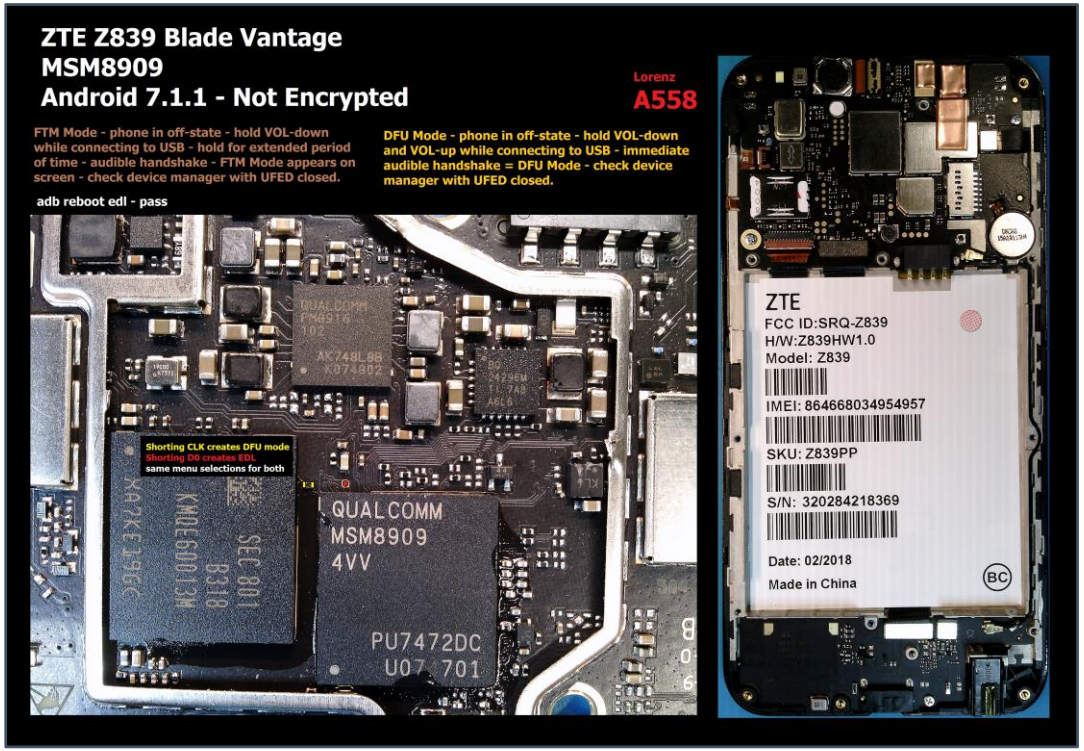
EXTRACTION VIDEO 01



ZTE Z839 – DFU Mode Extraction

- DFU Mode is usually created by holding volume down and volume up while connecting the device to USB
- DFU is created and visible in device manager
- An audible handshake is created almost immediately upon connection to USB
- DFU is handled by the UFED using the same menu selections as devices in EDL mode

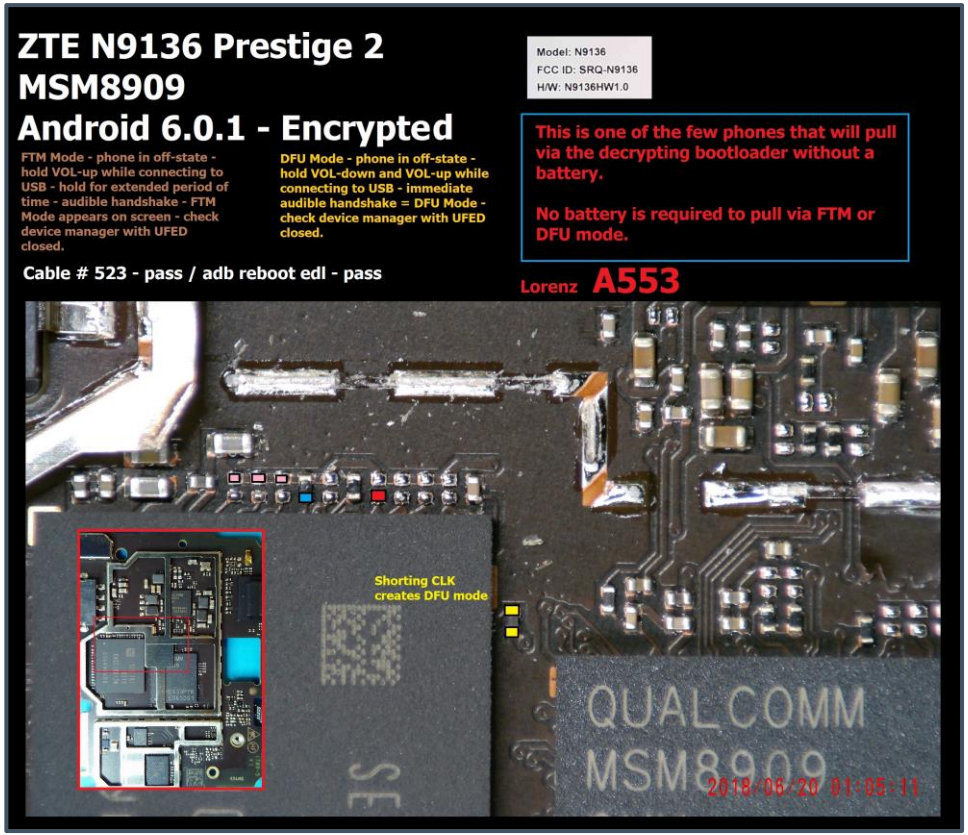
EXTRACTION VIDEO 02



ZTE N9136 – FTM (Field Test Mode) Extraction

- FTM Mode is usually created by holding either volume down or volume up and then connecting the device to USB
- May require holding the volume button for several seconds after connection
- FTM usually requires a battery
- The device appears to begin to boot before going into FTM
- Devices in FTM require an alternate menu selection under the generic Qualcomm options
- Locked and encrypted devices can be extracted

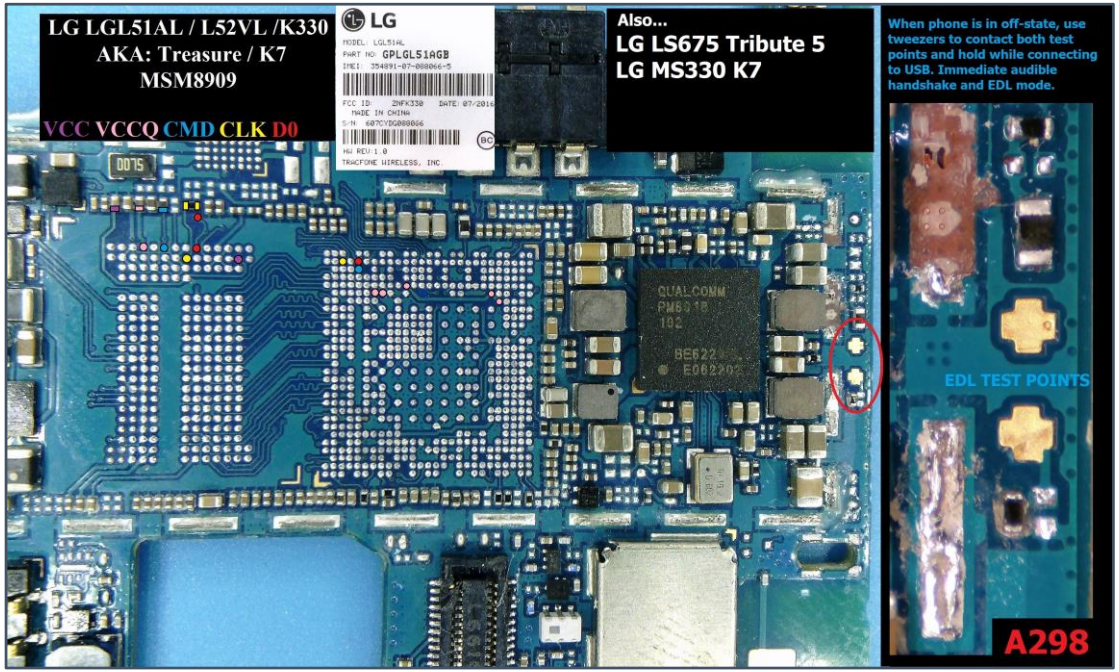
EXTRACTION VIDEO 03



LG MS330 – Test Point Extraction

- Disconnect or remove the battery or make sure the device is in the off-state
- Close the UFED 4PC
- Open Device Manager
- Connect the two Test Points with metal tweezers
- Connect the device to the PC via USB
- EDL mode is created almost immediately after connection

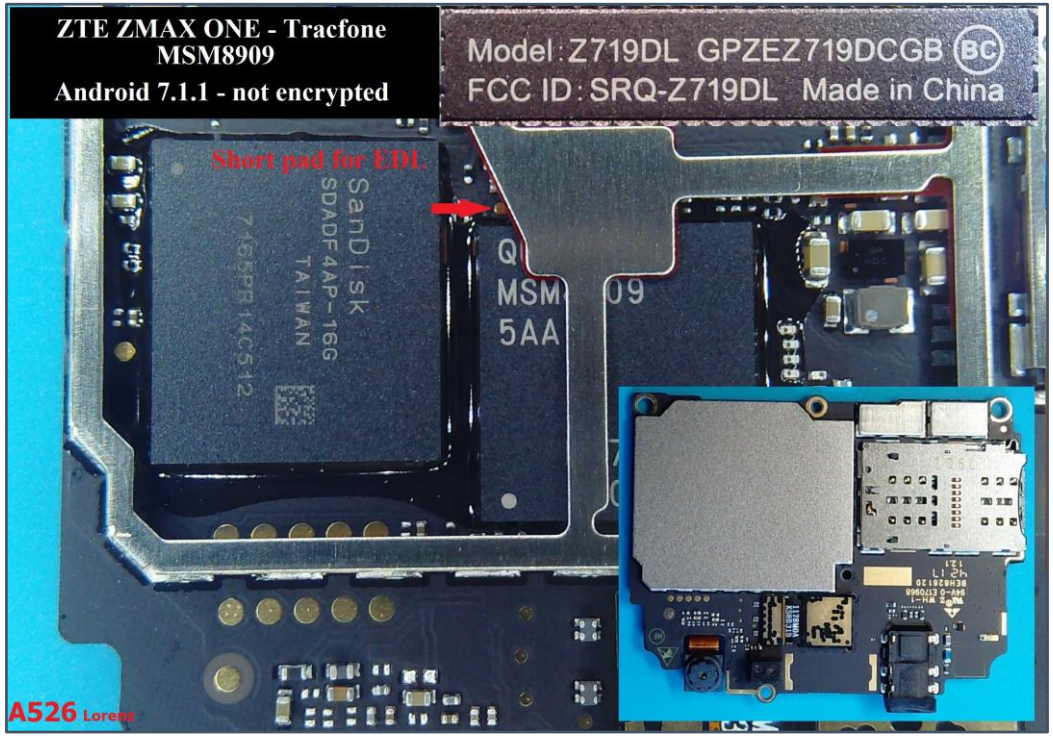
[EXTRACTION VIDEO 04]



ZTE Z719DL – eMMC Faults - Needlepoint Shorting

- eMMC Faults (shorting) can sometimes be created without soldering
- Various methods can be used to connect CMD, CLK, or Data locations to ground while connecting to USB
- Using a needle and a wire that can be connected to a ground point on a device is an effective way to create EDL or DFU mode on some devices

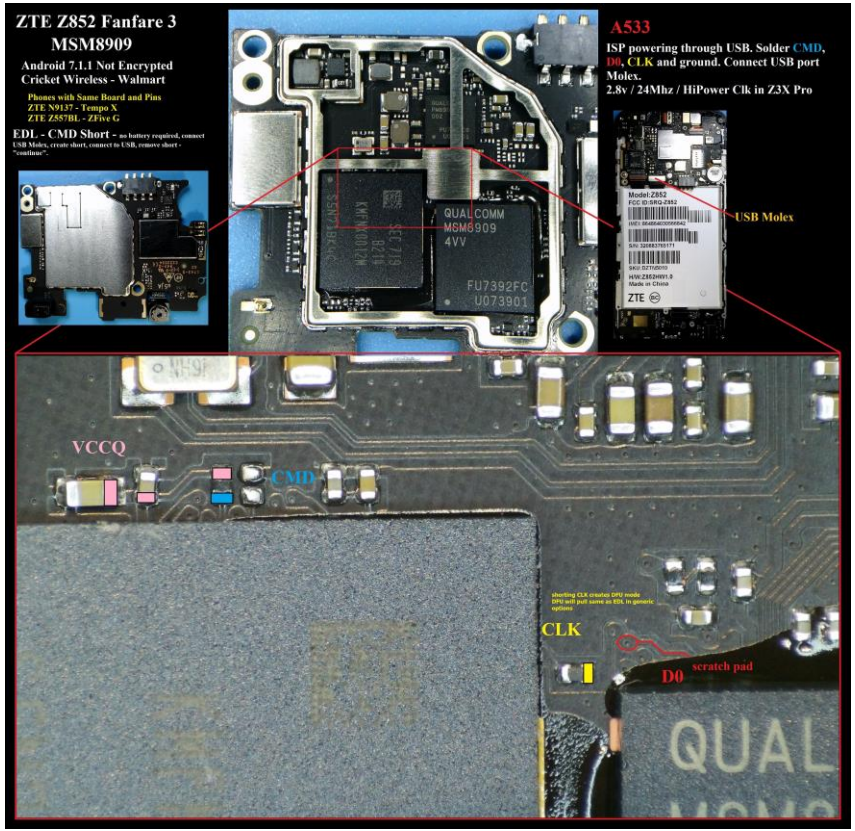
EXTRACTION VIDEO 05



ZTE Z852 eMMC Faults (Shorting) – Breadboard Method

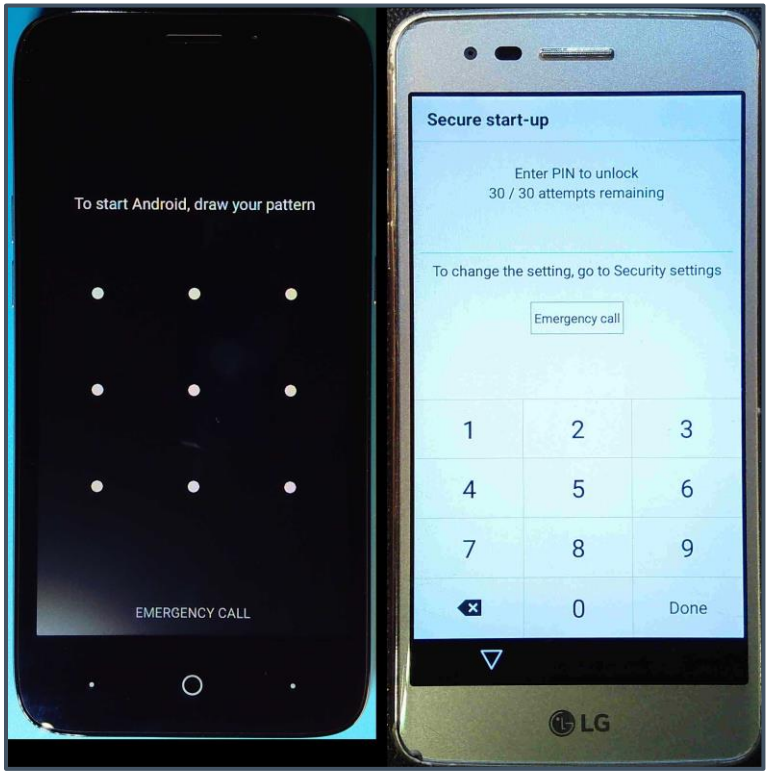
- eMMC Faults can be created by shorting CMD, CLK, or Data locations to ground points on a device
- Soldering is required for some devices that may require the device to be reassembled in order to boot for decrypting EDL extractions
- Some devices must be reassembled to connect the USB Molex for extraction
- Various soldering methods allow creating and removing the short after the device is reassembled

EXTRACTION VIDEO 06



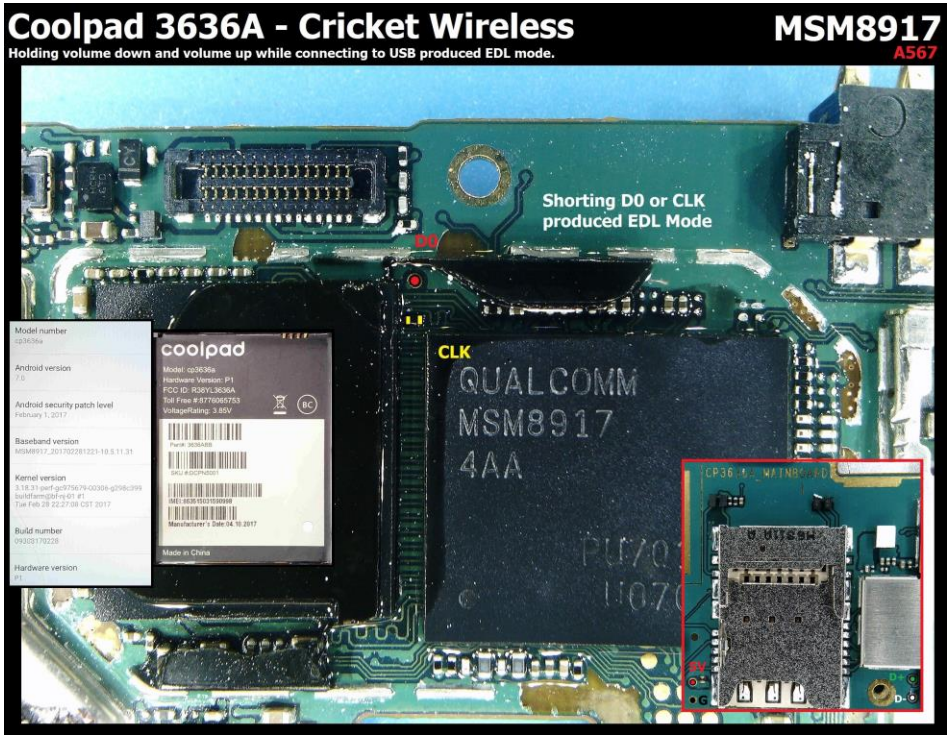
Secure Startup, and Other Booting Issues Related to EDL Extractions

- Decrypting EDL extractions require devices to fully boot to allow the UFED to apply the decrypting bootloader. Devices with Secure Startup cannot be extracted because the device is not allowed to boot into Android unless the Secure Startup passcode or pattern is entered.
- Some device boot to charge-only mode which can interfere with the application of the decrypting bootloader
- Alternate procedural steps can be used to create EDL mode in a way that coordinates or alters the booting of some devices so the decrypting bootloader can be applied.



Coolpad 3636A – Decrypting EDL – Button Combos After Connection

- Some phones, including some Coolpad models, boot to charge-only mode and prevent a decrypting EDL extraction
- This issue can be resolved by changing the usual order in which EDL is created after the device is connected to the UFED
- With the Coolpad 3636A, the device booting to charge-only mode can prevent a decrypting EDL extraction with the traditional order of button combos
- Connect the device to the UFED
- Wait for charging indicator
- Apply the button Combo



EXTRACTION VIDEO 07

Oppo R9S – Cable 523 – Alternate Method

- The Oppo R9S can be placed in EDL mode with Cable 523
- A decrypting EDL extraction fails with this device using Cable 523
- A decrypting EDL extraction fails with this device when using eMMC faults to create EDL mode
- An alternate use of Cable 523 allows a successful decrypting EDL extraction

[EXTRACTION VIDEO 08]