Oxygen EDL モードを用いた 物理抽出ガイド

Ver. 1.0



Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved



下記の「免責事項」をご確認いただき、ご理解いただいた上で本マニュアルをご利用ください。



目次

1 イントロダクション
1.1 対象デバイスの前提条件 3
2 事前準備
2.1 EDL ケーブルの準備3
2.2 ドライバのインストール4
3 EDL モードへの切り替え
3-1. ADB を使用する方法6
3-2. fastboot を使用する方法7
3-3. phone keys を使用する方法8
3-4. EDL ケーブルを使用する方法8
3-5. ピンショートを使用する方法8
4 EDL モードでの物理抽出
EDL モード対応 Qualcomm 製チップセット一覧11
日本国内向け EDL モード対応機種一覧12



1 イントロダクション

EDL モードとは、Qualcomm 製チップセットが搭載されているデバイスにおける「復旧モード」のことです。 Oxygen では、この EDL モードを利用して物理抽出を行うことが可能です。 EDL モードへの切り替えには以下 5 種類の手法が用意されています。

ソフトウェアのみ	adb
	fastboot
	phone keys
ハードウェア支援	EDL ケーブル
	ピンショート

▶ adb とピンショートを用いた手法のみ当社にて動作確認済み

▶ 当社で未検証のものについては、以下 Oxygen 公式マニュアルを参考に記載しています

 $https://www.oxygen-forensic.com/uploads/doc_guide/How_to_extract_data_from_devices_based_on_Qualcomm_chipsets_via_EDL_mode.pdf$

1.1 対象デバイスの前提条件

データの抽出と解析を実行する前に、下記の前提条件をご確認ください。

これらの前提条件を満たしていない場合、EDL モードでの抽出を行うことが出来ませんのでご注意ください。

デバイス種別	前提条件
Android	▶ 別紙の「EDL モード対応機種一覧(日本国内向け)」に記載されている機種である
デバイス	▶ 別紙の「EDL モード対応 Qualcomm 製チップセット一覧」に記載されているチ
	ップセットを搭載している

2 事前準備

2.1 EDL ケーブルの準備

「EDL ケーブルを使用する方法」を実施される場合は、EDL ケーブルを別途ご用意ください。 それ以外の方法を実施される場合は不要です。

2.2 ドライバのインストール

1. Customers page にアクセスし、ログインしてください

	OXYGEN FORENSIC® DETECTIVE Helping good people make this world safer		
Customers page Dear customer, You're about to access the Custo SaleID in your registration email re service.	omers Area. To enter the Customers Area, you will need to enter your SaleID into the window below. You will find eceived from us. If you do not know your SaleID or experience a problem logging in, please contact our customer SaleID:	your support	

2. 「Oxygen Forensic Custom Recovery and Bootloaders downloads:」の項目に「Qualcomm EDL pack」 がありますので、[Download]をクリックしてください

Охуд	en Forensic Viewer (64 bit) for OFB\OCB files	201MB	11.6.7.52	22 September	2020	Download
	Oxygen Forensie	c Custom Rec	overy and	Bootloaders down	nloads:	
	Package type	e	Size	Release date	Dowr	nload
	Samsung - Europe and I pack Compatible devi	International	1.41Gb	17 April 2019	Down	load
	Samsung - Asia and P Compatible devi	acific pack ces	1.55Gb	07 June 2017	Down	load
	Samsung - North Ame Compatible devi	erica pack ces	1.86Gb	07 June 2018	Down	load
	Samsung - Latin and South Compatible devi	n America pack ces	171Mb	07 June 2017	Down	load
	Samsung - Legacy Compatible devi	y pack ces	400Mb	17 April 2019	Down	load
	Motorola pac Compatible devi	k ces	57Mb	26 October 2017	Down	load
	Qualcomm EDL Compatible devi	pack ces	21Mb	05 December 2019	Down	load
	Spreadtrum pa Compatible devi	ack ces	8Mb	05 December 2019	Down	load

3. ダウンロードした「QualcommEDL_Image_pack.exe」を実行し、インストールを完了させてください。途中、インストール先を選択する画面が表示されますので、以下と異なる場合は修正してください。

C: ¥Program Files (x86) ¥Oxygen Forensics ¥QualcommEDL_Image_pack



ect Destination Location Where should Oxygen QualcommEDL Image Pack be installed?	
Setup will install Oxygen QualcommEDL Image Pack into the following the following of the following the followin	ng folder.
To continue, click Next. If you would like to select a different folder, click	Browse.
:¥Program Files (x86)¥Oxygen Forensics¥QualcommEDL_Image_pack	Browse
At least 109.1 MB of free disk space is required.	

4. 「デバイスドライバのインストールウィザードの開始」が起動した場合は、インストーラの指示に従って インストールを完了させてください



- 5. デバイスを起動させてください
- 6. PC とデバイスを電源ケーブルで接続してください
- 7. デバイス側で「USB でバッグの許可」を求めるアラートが出ますので、[許可]を選択してください
- 8. デバイスマネージャを開き、「ほかのデバイス」にデバイスが表示されていることを確認してください





- 9. 8 で確認したデバイスを右クリックし、プロパティを表示します
- 10. ドライバータブを開き、[ドライバーの更新]をクリックします
- 11. [コンピュータを参照してドライバー ソフトウェアを検索]をクリックします

12. Oxygen のフォルダ内にある Android フォルダを指定します

Oxygen v12	C:¥Program Files¥Oxygen Forensics¥Oxygen Forensic		
	Detective¥OFD12¥Extractor¥Drivers¥Android		
Oxygen v13	C:¥Program Files¥Oxygen Forensics¥Oxygen Forensic		
	Detective¥Extractor¥Drivers¥Android		

3 EDL モードへの切り替え

EDL モードへの切り替え方法には5つの方法があります。この章では各種の切り替え手順を説明します。



3-1. ADB を使用する方法

- 1. デバイスを起動させてください
- 2. PC とデバイスを接続してください。ケーブルは通常使用しているもので構いません
- 3. デバイス側で「USB でバッグの許可」を求めるアラートが出ますので、[許可]を選択してください
- 4. PC 側でコマンドプロンプトなどのターミナルを開き、下記のコマンドを実行してください。成功するとデ バイスの画面が暗転します。

adb reboot edl

5. ポート一覧にデバイスが追加されていることを確認してください





3-2. fastboot を使用する方法

- 1. デバイスの電源を切ります
- 2. 音量ボタン(+)and 電源ボタンで起動してください
- 3. 「fastboot Mode !!! long press power key to restart system」と表示される事を確認してください



4. PC 側でコマンドプロンプトなどのターミナルを開き、下記のコマンドを実行してください



5. 以下のように表示されているかを確認してください。

これにより、デバイスが認識されているかを確認出来ます。

6. PC 側でコマンドプロンプトなどのターミナルを開き、下記のコマンドを実行してください。

これにより、EDL モードに入ることが出来ます。

fastboot oem edl

3-3. phone keys を使用する方法

- 1. デバイスの電源を切ります
- 2. PC に USB ケーブルを接続してください。USB ケーブルには、デバイスをまだ接続しないでください
- 3. デバイスの音量ボタンの(+)と(-)を同時に押しながら、USB ケーブルに接続してください
- 4. 3~5 秒ほど音量ボタンを押し続けてください
- 5. EDL モードに入れていれば、画面が暗転します

3-4. EDL ケーブルを使用する方法



- 1. デバイスの電源を切ります
- 2. PC に EDL ケーブルを接続してください。EDL ケーブルには、デバイスをまだ接続しないでください
- 3. EDL ケーブルのボタンを押しながら、デバイスに接続してください

3-5. ピンショートを使用する方法

- この方法は電子機器の専門的知識を有している方向けのものです
- 1. デバイスの電源を切ります
- 2. デバイスを分解し、テストポイントを露出させてください。テストポイントはデバイス毎に異なります



テストポイント

Copyright © 2021 Cyber Defense Institute, Inc. All Rights Reserved

- 3. PC に USB ケーブルを接続してください。USB ケーブルには、デバイスをまだ接続しないでください
- 4. テストポイントをジャンパーワイヤなどで抑え、短絡(ショート)させてください
- 5. 4 の状態のまま、USB ケーブルをデバイスに接続してください
- 6. PC 側でデバイスマネージャを開き、ポートに一覧に「Qualcomm…」が追加されていることを確認して ください。無事に追加されていれば、EDL モードへの切り替えは成功です。4.で短絡させていたジャン パーワイヤは外して問題ありません

4 EDL モードでの物理抽出

- 1. Oxygen Forensic Extractor を起動してください
- 2. 「Android extractions」の中の[Qualcomm EDL dump]をクリックしてください

Oxygen デバイスの/	Forensic® Extractor パックアップタイプまたは物理イメージを選択してください
Ĉ	iOS extractions iTunes backup iOS Advanced extraction Logical file structure
Û	Android extractions Android physical (via ADB) Android backup (via ADB) Android OxyAgent extraction Android manual OxyAgent extraction Android OxyAgent over WiFi extraction Android logical file system MTK Android dump LG Android dump Spreadtrum Android dump Samsung Android dump Samsung Exynos dump Motorola Android dump Cualcomm EDL dump Huawei Android dump Sony MTK Android dump
<u>ع</u>	Drone extractions DJI drone dump
٦٦	Other extractions JioPhone MTP Memory card dump UICC

3. 「上記手順を確認しました」にチェックを入れ、[Next >]をクリックしてください



 Select EDL bootloader」画面で、左上の検索ボックスにモデル名またはチップセットの番号を入力し、 当てはまるチップセットとデバイスを選択し、[Connect]をクリックしてください

Oxygen Forensic® Ext Qualcomm EDL connection	tractor	
	Select EDL bootloader Choose device MSM 8916 業	ップセ Clear
	Lenovo Phab WDefaultVprog_emmc_firehose_8916_lenovo_pb1-750p.mbn LYF Wind 1 WDefaultVprog_emmc_firehose_8916_lyf, wind-1.mbn	MSM 8916 A
	Asus ZenFone 2 Lazer Yother¥prog_emmc_firehose_8916_asus.mbn	MSM 8916
	VotherVprog_emmc_firehose_8916_asus.mbn Coolpad F1 plus VotherVprog_emmc_firehose_8916_cool.mbn	MSM 8916
	Coolpad Fance ¥other¥prog_emmc_firehose_8916_cool.mbn	MSM 8916
	Coolpad Fancy Pro ¥other¥prog_emmc_firehose_8916_cool.mbn	MSM 8916
	If your device is not found in this list try automatic connector or use your firehose file.	tion
	< Back Connect	Cancel

5. 正常に認識出来た場合は下図のような結果が表示されます。そのまま[Extract]をクリックし、抽出を開始してください

Oxygen Forensic® 接続されたデバイス	Extractor	
	テバイスが正常に接続	されました!
Connected!	Device information Model: S/N: Hardware Revisio Software Revisio	Qualcomm HS-USB QDLoader 9008 AD_SCD4AA342C01 on: N/A n: N/A
¥	Extraction options 抽出するデータの保存先を選択 C:¥Users¥minAd¥Documents¥	してください。 Dxygen Forensics¥Backups¥2020-10-29 06-43-53 AD¥ 📄
		Extract Cancel

- 抽出に失敗した場合は、正しく EDL モードに切り替えられているかを再確認してください
- EDL モードの切り替えが上手くいかない場合は、別の切り替え方法をお試しください



EDL モード対応 Qualcomm 製チップセット一覧

MSM 8909
MSM 8916
MSM 8917
MSM 8939
MSM 8952
MSM 8929
MSM 8936
MSM 8937
MSM 8940
MSM 8953
MSM 8974
MSM 8976
MSM 8992
MSM 8994
MSM 8996
MSM 8x10
MSM 8x26

日本国内向け EDL モード対応機種一覧

メーカー名	機種名
Acer	LIQUID Z330
Alcatel	Idol 4
	ZenPad
	ZenFone Go
	ZenFone 2 Laser
	ZenFone 4 Max Pro
	ZenFone 4 Max
	ZenFone 4 Selfie
Acus	ZenPad 8.0
ASUS	ZenFone 3 Laser
	ZenFone 3 Max
	ZenFone Max
	ZenFone 3 Deluxe
	ZenFone 3
	ZenFone 4 Selfie Pro
	ZenFone AR
	Y6
Huawei	Nexus 6P
	Yoga Tab 3
	Tab 4 10 Plus
Lenovo	Tab 4 8 Plus
	Phab 2 Pro
	Yoga Tab 3 Plus
Орро	R11s
Wiko	Tommy
	Axon 7 mini
ZTE	Axon Pro
	Axon 7

改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2021年03月09日	初版発行