

# checkm8 を用いたデータ抽出ガイド

Ver. 1.4



**OXYGEN  
FORENSICS**

## 目次

1	イントロダクション.....	1
1.1	このガイドについて.....	1
1.2	Oxygen の checkm8 は JB しない.....	1
1.3	対象デバイスの前提条件.....	1
2	checkm8 を用いたエクスプロイト.....	2
2.1	checkm8 のメニュー起動.....	2
2.2	抽出準備.....	4
2.3	抽出実施.....	12
2.4	日本語訳.....	15
3	抽出データの違い.....	16

## 1 イン트로ダクション

### 1.1 このガイドについて

本ガイドでは、「Oxygen Forensic® Detective（以降 OFD と記載）」を用いることによって、Windows から checkm8 による iOS の論理抽出を行う手順および補足事項を記載します。

画像は、現在の最新（2022年5月13日時点）：OFDv14.4.1.1（2022年4月27日リリース）のスクリーンショットを掲載しています。

### 1.2 Oxygen の checkm8 は JB しない

Oxygen では「checkm8」と呼ばれる脆弱性を利用して、iOS デバイスからデータ抽出を行うことができます。また、Oxygen では JailBreak(以降 JB と記載)は行いませんので安心してご利用頂けます。

#### JB を行いたい場合：

「checkra1n」という checkm8 の脆弱性を使って JB するフリーツールがインターネット上に公開されています。macOS 及び Linux のみサポートされています。（2022年1月19日時点）

また、checkm8 の脆弱性は、tethered Jailbreak（紐付き JB と呼ばれ、一時的に JB 状態にするもの）を利用しているため、再起動すると一時的な JB の状態は解除されます。

### 1.3 対象デバイスの前提条件

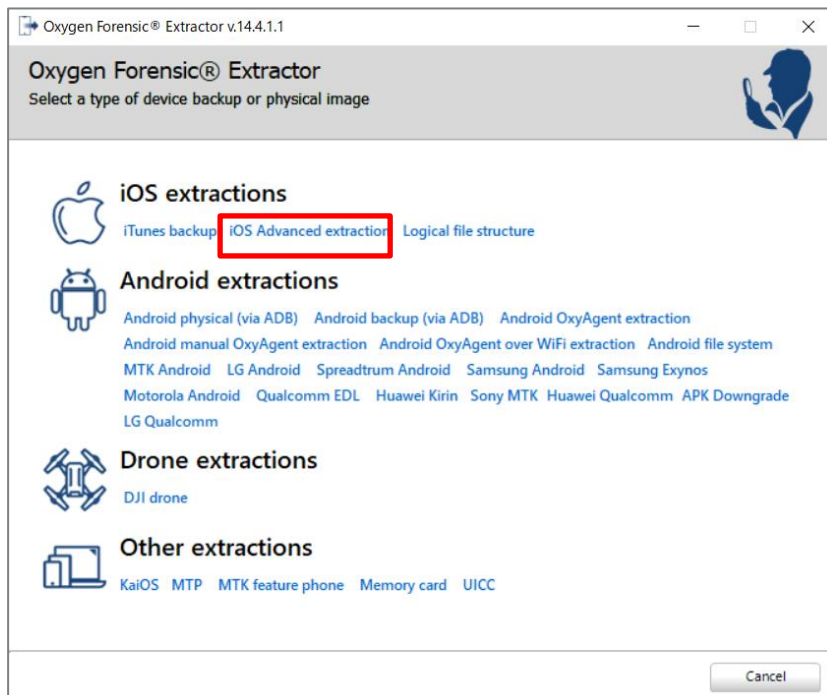
対象デバイスは、手順③をご確認ください。

## 2 checkm8 を用いたエクспロイト

iOS Advanced extraction の、iOS Checkm8 又は iOS full logical via checkm8 は、checkm8 を利用した脆弱性を使用し、iOS デバイスからの論理抽出を実施します。論理抽出ではありますが、現在の iOS デバイスで可能な限り最大限の抽出を行います。

### 2.1 checkm8 のメニュー起動

- ① 「Oxygen Forensic® Extractor」を起動します。「iOS extractions」項目の中から、「iOS Advanced extraction」をクリックします

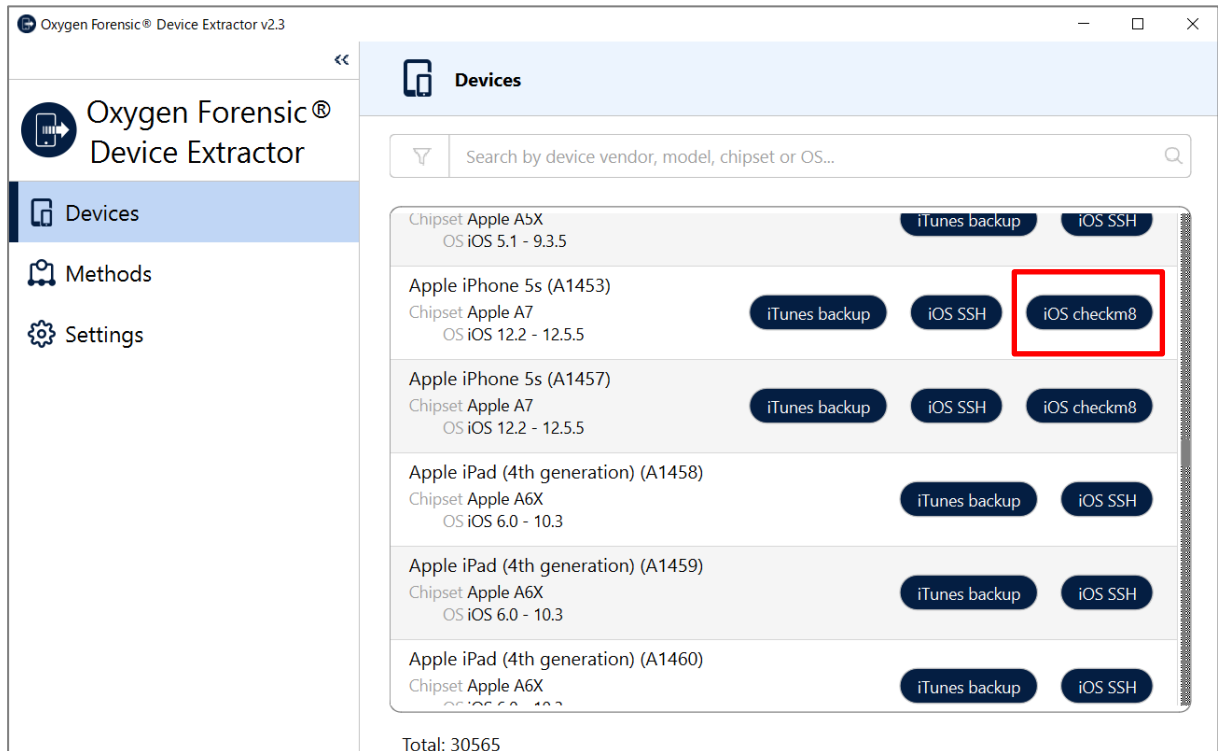


② 対象の中から「iOS checkm8」ボタンをクリックします。

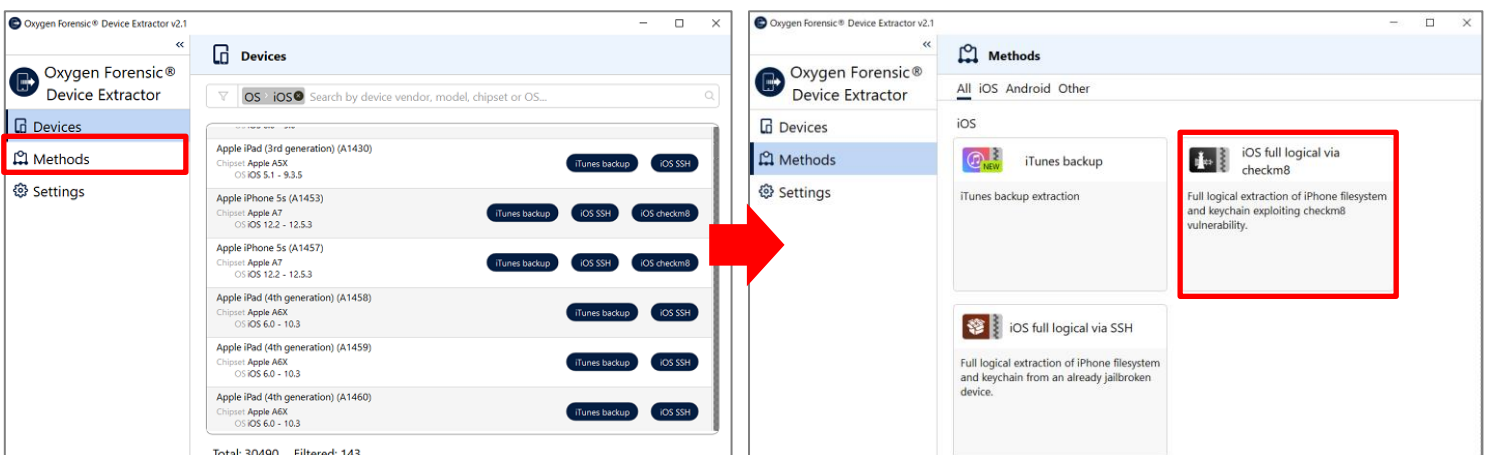
※デバイスが checkm8 に対応していない場合、ボタンは表示されません

※「iOS checkm8」ボタンならどちらをクリックしても問題ありません

例えば、抽出対象デバイスが iPhone5s だとして、iPad Pro の横にある「iOS checkm8」ボタンをクリックしても問題はありませ



または、左端の「Methods」をクリックし、「iOS full logical via checkm8」をクリックして起動する方法もあります。



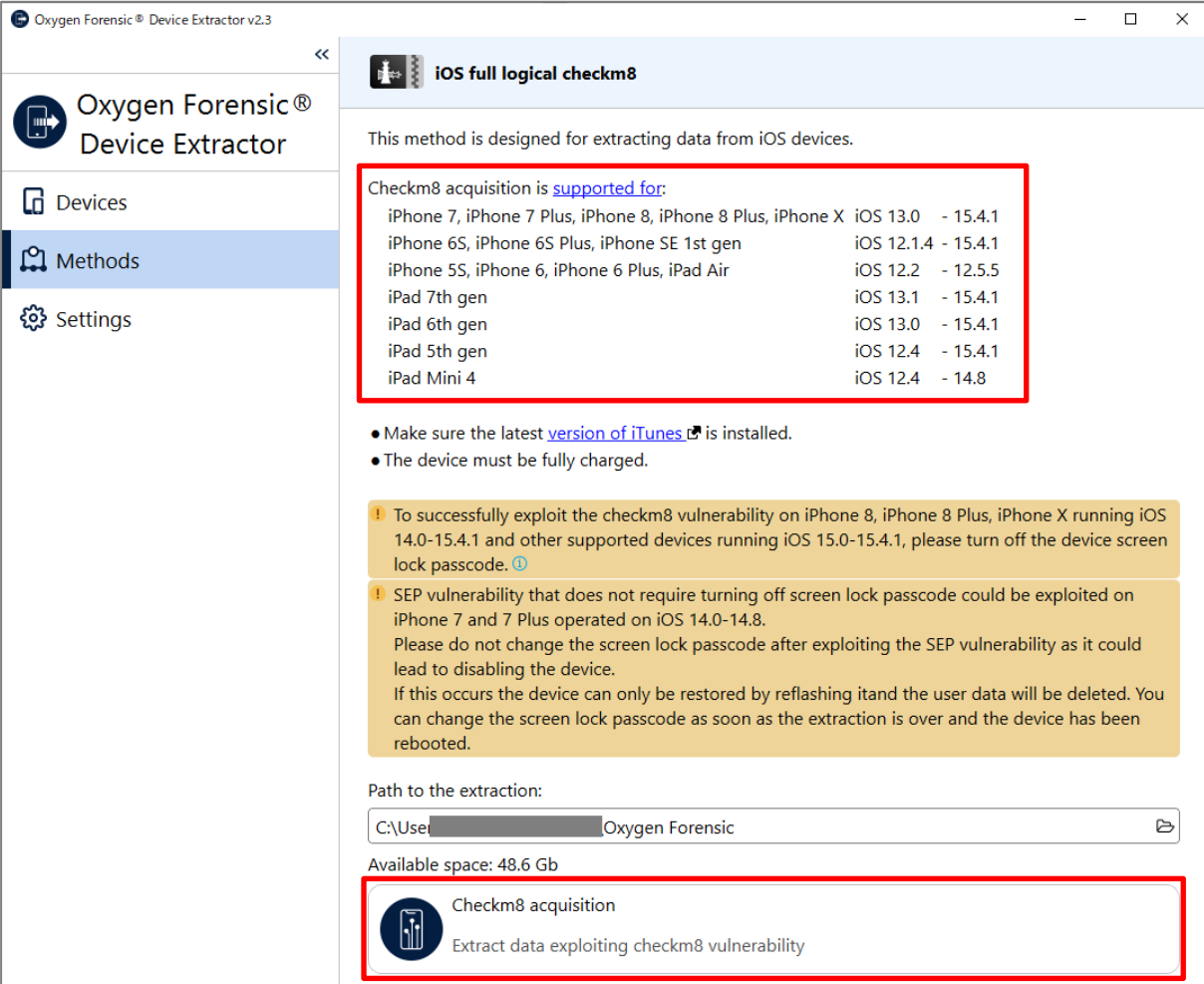
## 2.2 抽出準備

③ 下図の一番上の赤枠部分を参照し、対象デバイスがあることを確認し一番下の赤枠内の「Checkm8 acquisition」をクリックします。

**iOS14.0-14.8 搭載の iPhone7、iPhone7 Plus または iOS14.0-15.4.1 搭載の iPhone8、iPhone8 Plus、iPhone X および iOS15.0-15.4.1 搭載の他のデバイスが対象の場合：**

画像のオレンジで色付けされた注意事項を確認の上、実行をご確認ください。

日本語が必要な方は、後述の **2.4 日本語訳** をご参照ください



Oxygen Forensic® Device Extractor v2.3

**iOS full logical checkm8**

This method is designed for extracting data from iOS devices.

Checkm8 acquisition is [supported for](#):

iPhone 7, iPhone 7 Plus, iPhone 8, iPhone 8 Plus, iPhone X	iOS 13.0 - 15.4.1
iPhone 6S, iPhone 6S Plus, iPhone SE 1st gen	iOS 12.1.4 - 15.4.1
iPhone 5S, iPhone 6, iPhone 6 Plus, iPad Air	iOS 12.2 - 12.5.5
iPad 7th gen	iOS 13.1 - 15.4.1
iPad 6th gen	iOS 13.0 - 15.4.1
iPad 5th gen	iOS 12.4 - 15.4.1
iPad Mini 4	iOS 12.4 - 14.8

- Make sure the latest [version of iTunes](#) is installed.
- The device must be fully charged.

**!** To successfully exploit the checkm8 vulnerability on iPhone 8, iPhone 8 Plus, iPhone X running iOS 14.0-15.4.1 and other supported devices running iOS 15.0-15.4.1, please turn off the device screen lock passcode.

**!** SEP vulnerability that does not require turning off screen lock passcode could be exploited on iPhone 7 and 7 Plus operated on iOS 14.0-14.8. Please do not change the screen lock passcode after exploiting the SEP vulnerability as it could lead to disabling the device. If this occurs the device can only be restored by reflashing it and the user data will be deleted. You can change the screen lock passcode as soon as the extraction is over and the device has been rebooted.

Path to the extraction:  
C:\User\... Oxygen Forensic

Available space: 48.6 Gb

**Checkm8 acquisition**  
Extract data exploiting checkm8 vulnerability

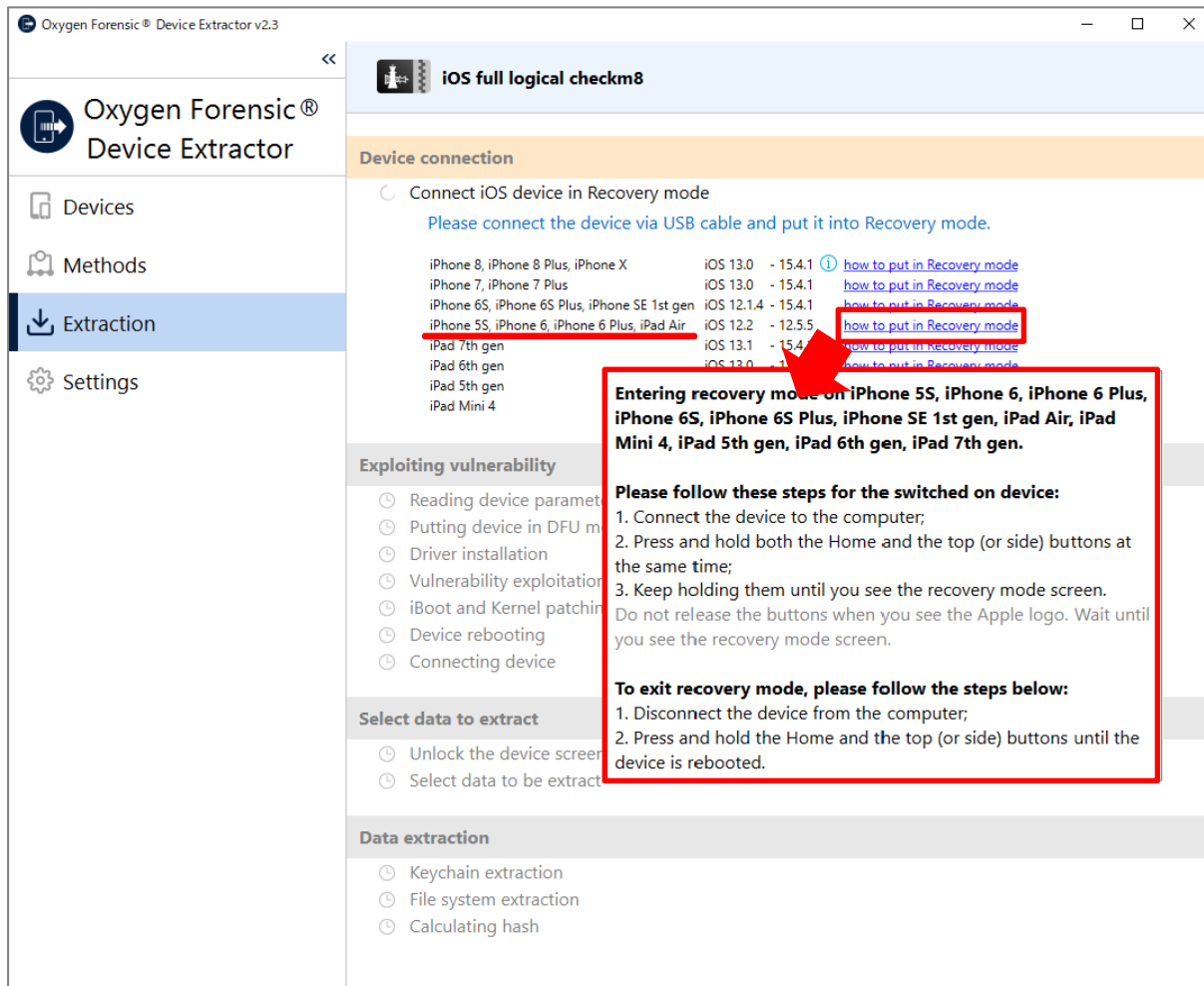
④ 対象デバイスをリカバリモードにします。

※リカバリモードへの入り方は、デバイスによって一部異なります

📌 **リカバリモードへの入り方が分からない場合：**

対象デバイスの右側の「how to put in Recovery mode」をクリックすると、リカバリモードへの入り方の手順が表示されます。

この図では、iPhone5S、iPhone6、iPhone6 Plus、iPad Airのリカバリモードの入り方を表示させています。



Oxygen Forensic® Device Extractor v2.3

iOS full logical checkm8

Device connection

Connect iOS device in Recovery mode  
Please connect the device via USB cable and put it into Recovery mode.

iPhone 8, iPhone 8 Plus, iPhone X	iOS 13.0 - 15.4.1	<a href="#">how to put in Recovery mode</a>
iPhone 7, iPhone 7 Plus	iOS 13.0 - 15.4.1	<a href="#">how to put in Recovery mode</a>
iPhone 6S, iPhone 6S Plus, iPhone SE 1st gen	iOS 12.1.4 - 15.4.1	<a href="#">how to put in Recovery mode</a>
<b>iPhone 5S, iPhone 6, iPhone 6 Plus, iPad Air</b>	iOS 12.2 - 12.5.5	<a href="#">how to put in Recovery mode</a>
iPad 7th gen	iOS 13.1 - 15.4.1	<a href="#">how to put in Recovery mode</a>
iPad 6th gen	iOS 13.0 - 15.4.1	<a href="#">how to put in Recovery mode</a>
iPad 5th gen	iOS 13.0 - 15.4.1	<a href="#">how to put in Recovery mode</a>
iPad Mini 4	iOS 13.0 - 15.4.1	<a href="#">how to put in Recovery mode</a>

**Entering recovery mode on iPhone 5S, iPhone 6, iPhone 6 Plus, iPhone 6S, iPhone 6S Plus, iPhone SE 1st gen, iPad Air, iPad Mini 4, iPad 5th gen, iPad 6th gen, iPad 7th gen.**

**Please follow these steps for the switched on device:**

1. Connect the device to the computer;
2. Press and hold both the Home and the top (or side) buttons at the same time;
3. Keep holding them until you see the recovery mode screen. Do not release the buttons when you see the Apple logo. Wait until you see the recovery mode screen.

**To exit recovery mode, please follow the steps below:**

1. Disconnect the device from the computer;
2. Press and hold the Home and the top (or side) buttons until the device is rebooted.

Exploiting vulnerability

- Reading device parameters
- Putting device in DFU mode
- Driver installation
- Vulnerability exploitation
- iBoot and Kernel patching
- Device rebooting
- Connecting device

Select data to extract

- Unlock the device screen
- Select data to be extracted

Data extraction

- Keychain extraction
- File system extraction
- Calculating hash

## リカバリモードへの入り方具体例 (iPhone5s、iPhone6、iPhone6 Plus、iPad Air の場合)



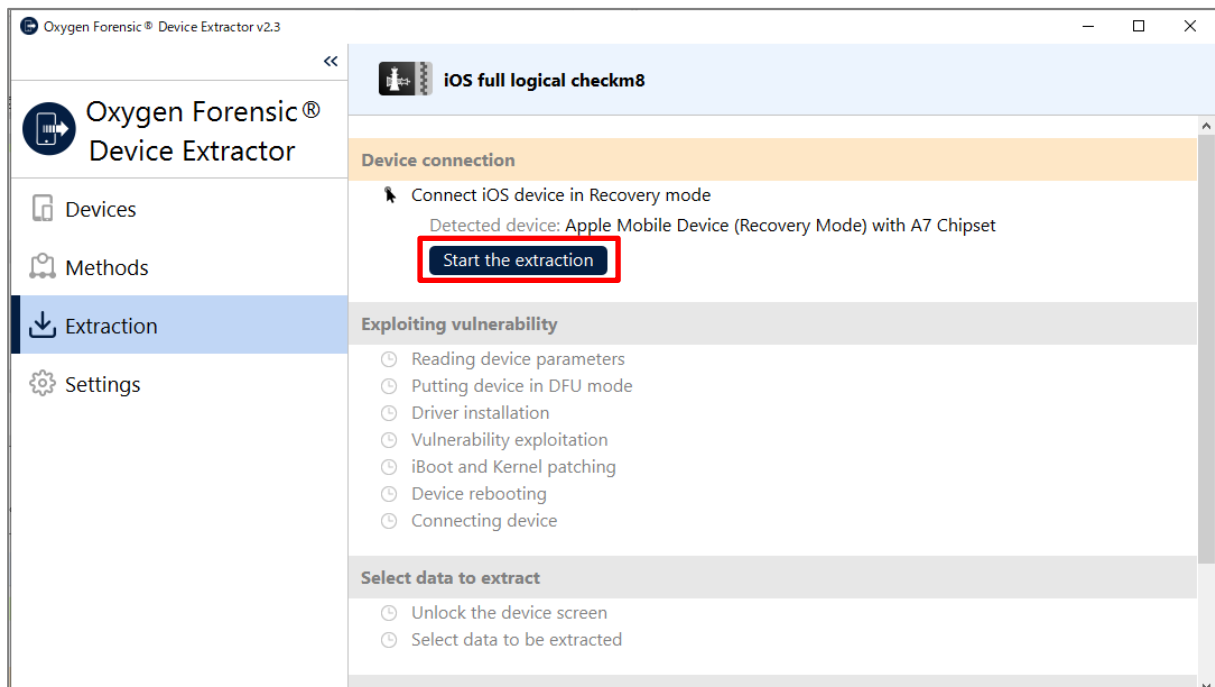
1. デバイスを PC と接続します (デバイスは起動した状態)
2. 電源ボタンとホームボタン両方を長押ししたままにします。
3. 画面がリカバリーモードになるまで長押しし続けます。

Apple のロゴがデバイス画面に表示されても手を離さずに、画面がリカバリーモードに切り替わるまでそのまま長押しし続けてください。

リカバリモードを解除する場合、以下のステップを実施します：

1. デバイスと PC の接続を解除します
2. 電源ボタンとホームボタン両方をデバイスがリブートするまで長押しします。

⑤ デバイスが認識されたことを確認し、「Start the extraction」をクリックします。

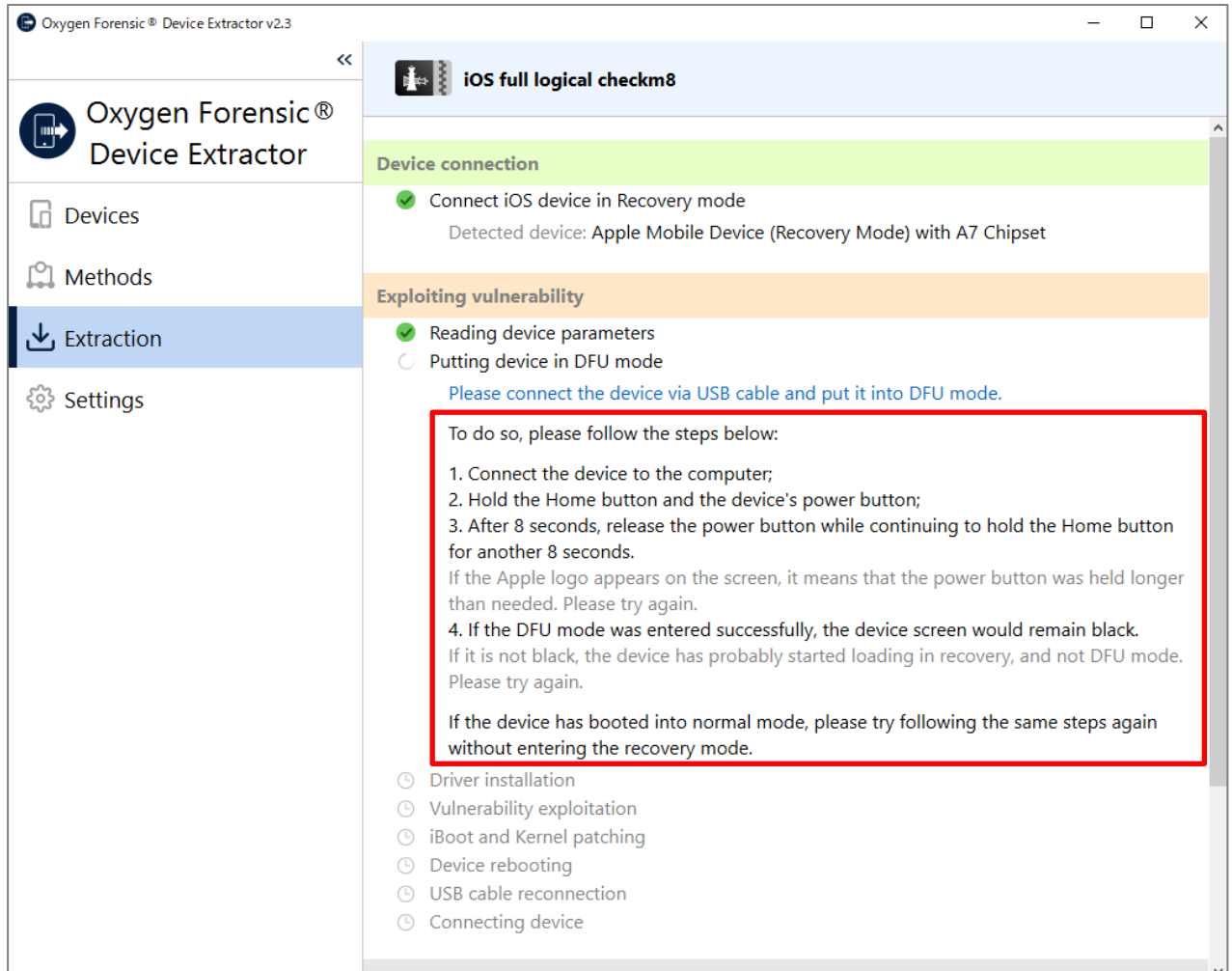




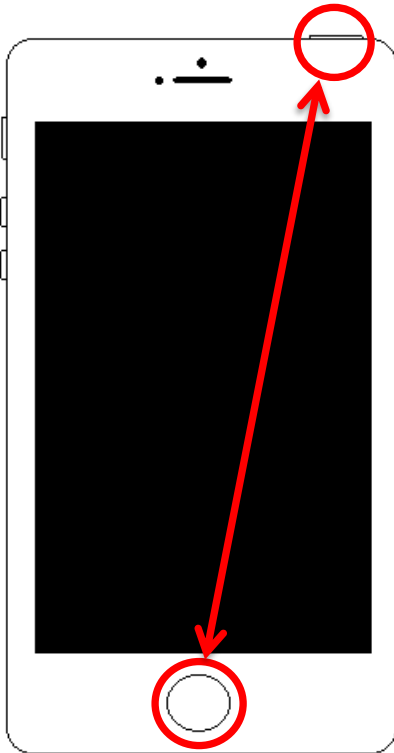
⑥ しばらくすると、以下の図の様な DFU モードへの切り替えの指示が表示されます。

画像の赤枠部分の手順にそって DFU モードに切り替えます。

※DFU モードへの入り方は、デバイスによって異なるので実際の画面の手順を都度ご確認ください。

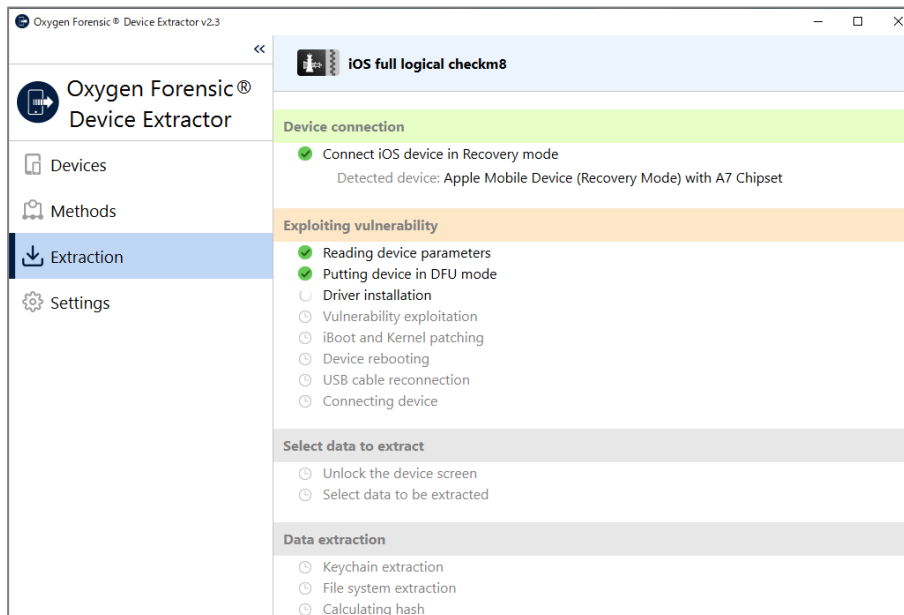


### DFUモードへの入り方具体例 (iPhone5s、iPhone6、iPhone6 Plusの場合)

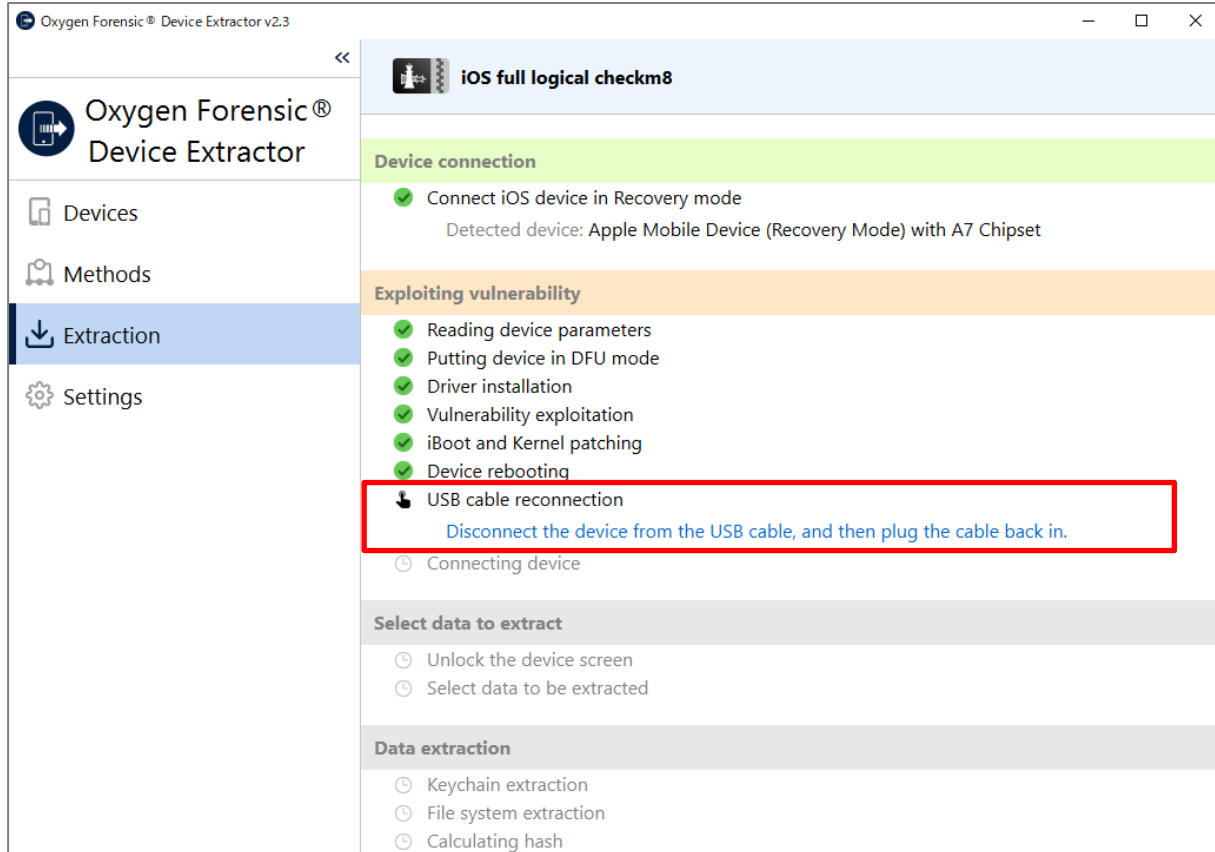


1. デバイスとPCは接続したまま
2. 電源ボタンとホームボタン両方を長押ししたままにします。
3. 長押ししたまま 8 秒経過後、電源ボタンを外し、ホームボタンは押したまま更に 8 秒経過させます。  
  
Apple のロゴがデバイス画面に表示された場合、電源ボタンが指定秒より長く押された事を意味します。再度やり直してください。
4. DFU モードに正常に入れた場合、デバイスの画面は黒のままになります。

DFU モードが認識されると、以下の画面の様に次の処理に進みます。



- ⑦ 「USB cable reconnection」が表示されたら、一度デバイスを外し、再度接続し直します。  
また、DFU モードから復帰したデバイスは、画面がロックされるため手動で解除します。

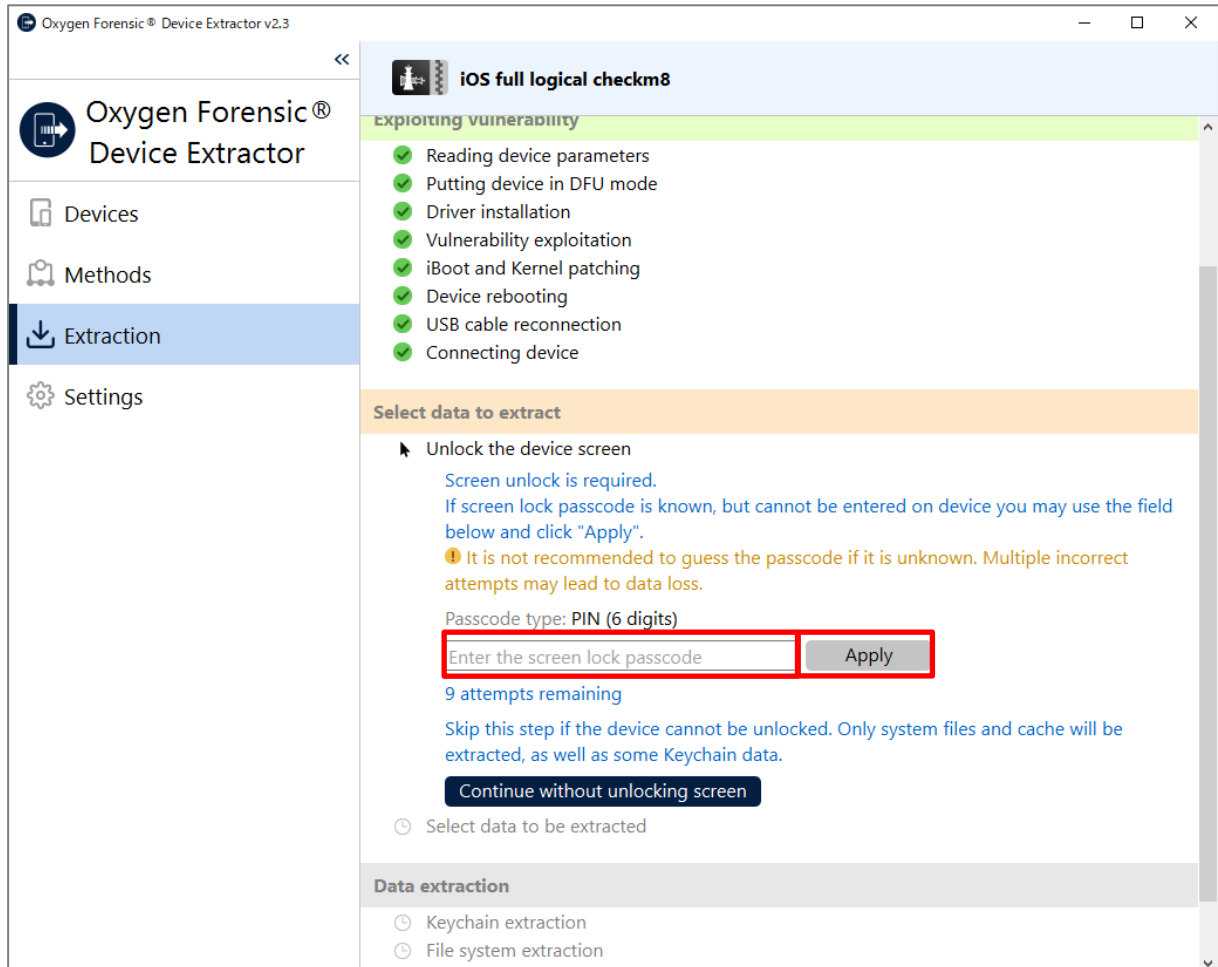


画面ロックの解除をしなかった場合：

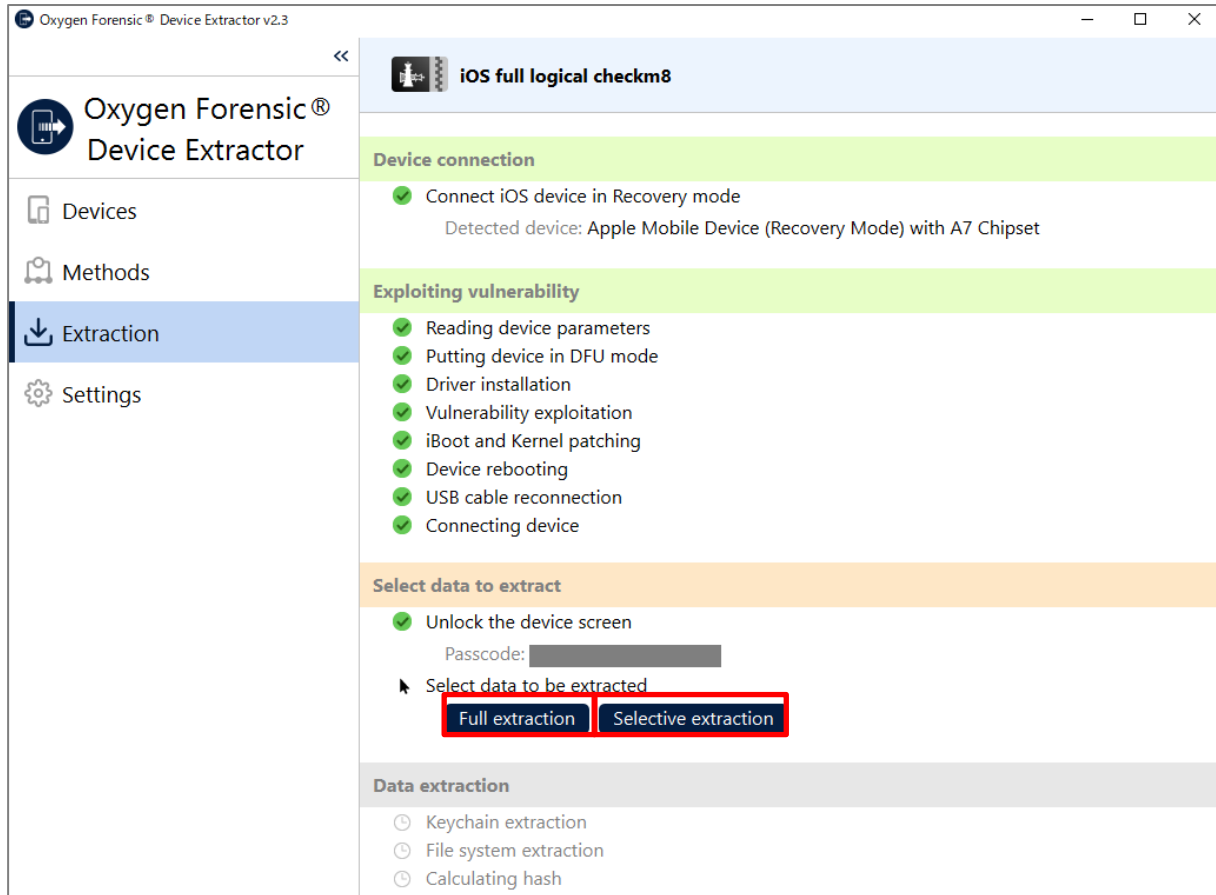
以下の様な画面が表示されて、画面ロックのパスコードの入力を求められます。

※パスコードが不明な場合、推測して入力することはお勧めしません。誤ったパスコードを複数回入力するとデータが失われる可能性があります。

※画面のロックを解除できない場合は、この手順はスキップしてください(Continue without unlocking screenをクリックします)。その場合システムファイルとキャッシュ、および一部のキーチェーンデータのみが抽出されます。(セクション「3. データの違い」の「Continue without unlocking screen」をクリックした場合を参照)



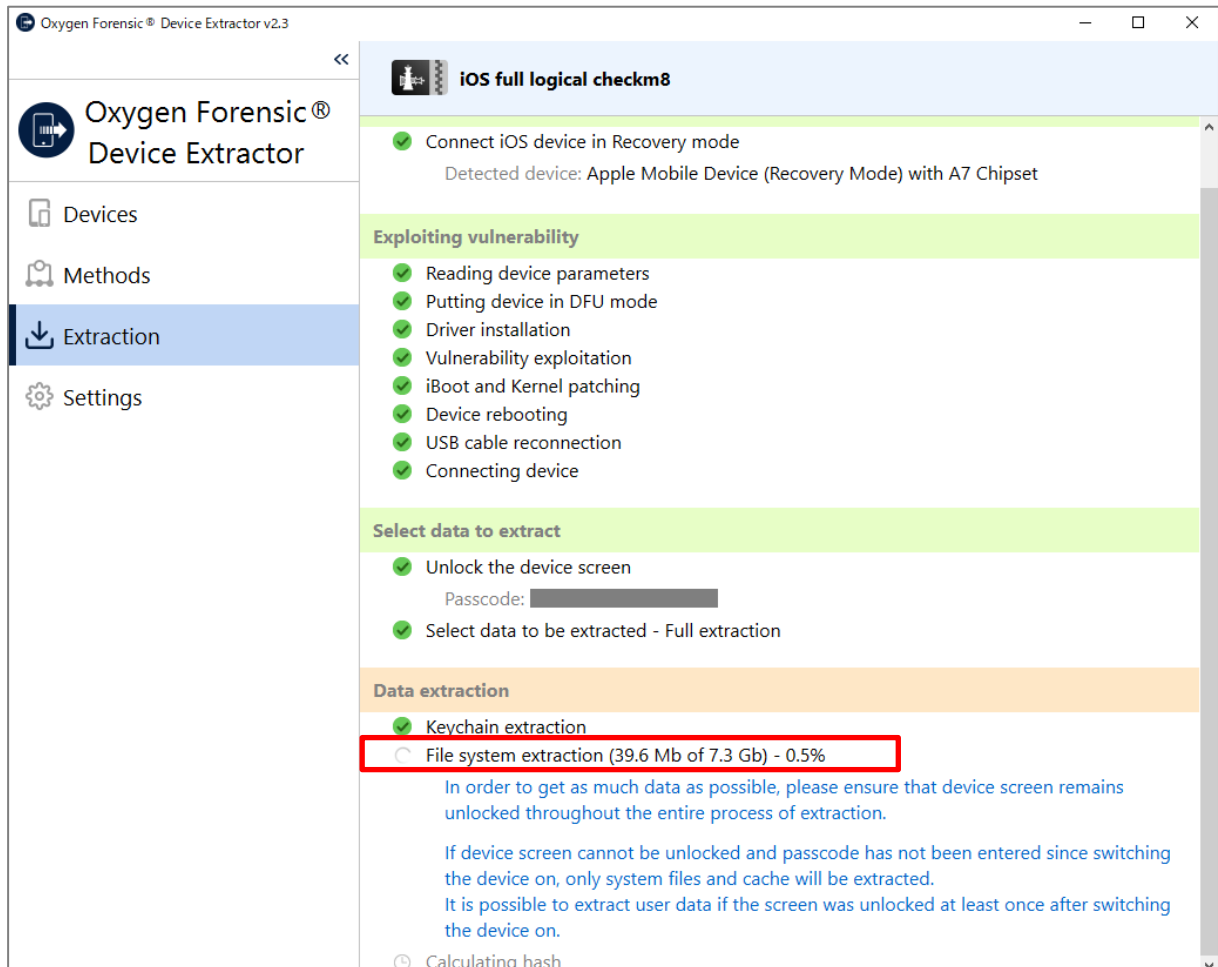
⑧ 抽出の準備が完了すると「Full extraction」と「Selective extraction」の抽出実施メニューが表示されます。



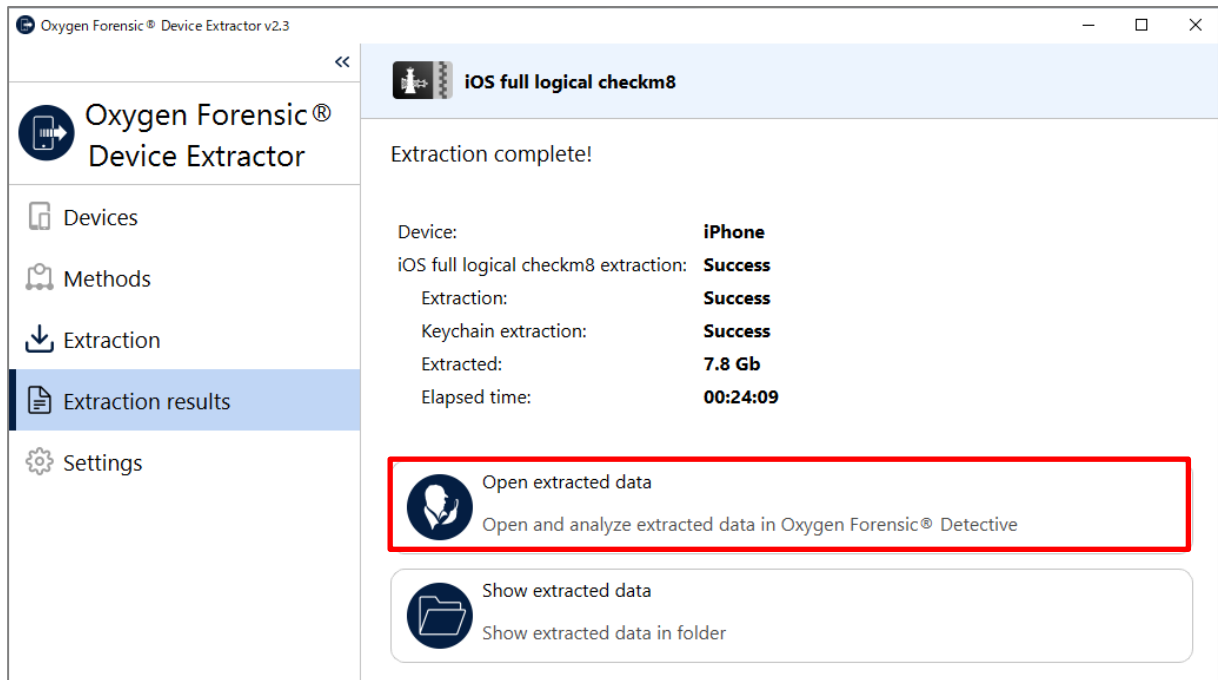
## 2.3 抽出実施

▼ 手順⑧の画面で「Full extraction」をクリックした場合：

⑨ 抽出が開始されるとパーセントが表示されますので、処理が完了するまでしばらくお待ちください

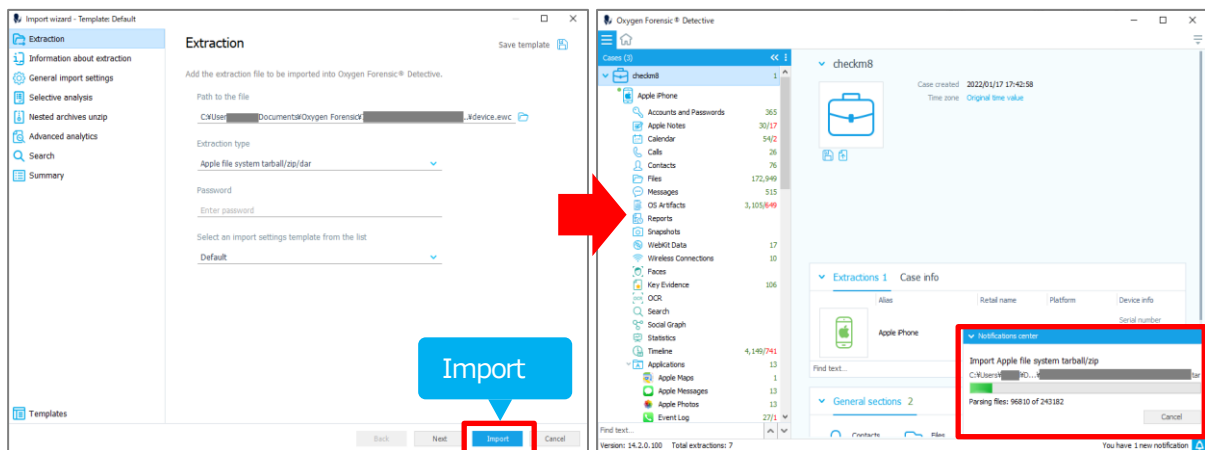


⑩ 抽出が完了すると以下の様な画面が表示されます。「Open extracted data」をクリックします。



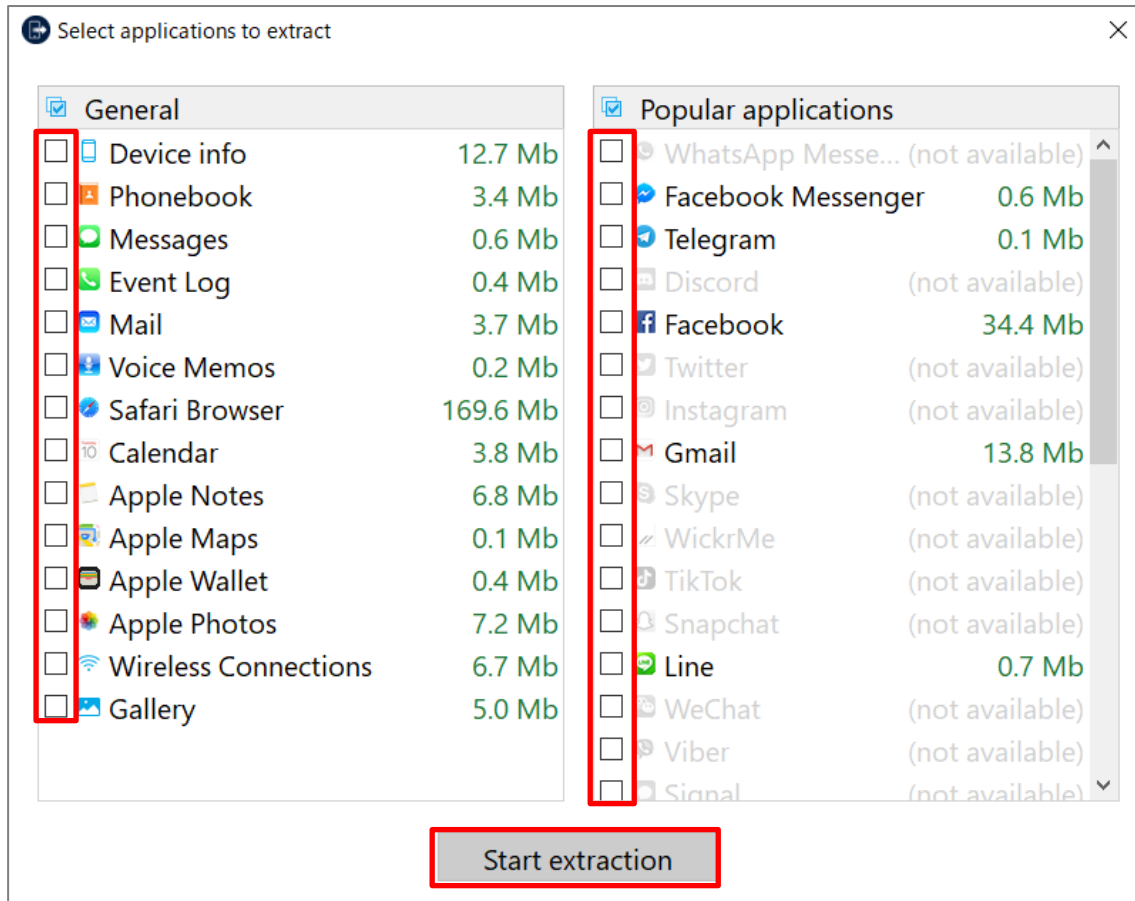
「Import」をクリックすると、緑の進捗バーが表示されます：通常の OFD へのデータの取り込み（インポート）

と同じ手順です。



▼ 手順⑧の画面で「Selective extraction」をクリックした場合：

アプリケーション一覧が表示されます。抽出したいアプリケーションにチェックを入れて「Start extraction」をクリックします。



以降は、「Full extraction」を選択した場合と同様の手順で抽出が開始します。



## 2.4 日本語訳

手順③に表示される注意事項、およびインフォメーションマークの内容の日本語訳を『』内に載せています。

! To successfully exploit the checkm8 vulnerability on iPhone 8, iPhone 8 Plus, iPhone X running iOS 14.0-15.4.1 and other supported devices running iOS 15.0-15.4.1, please turn off the device screen lock passcode ⓘ

! SEP vulnerability that does not require turning off screen lock passcode could be exploited on iPhone 7 and 7 Plus operated on iOS 14.0-14.8.  
Please do not change the screen lock passcode after exploiting the SEP vulnerability as it could lead to disabling the device.  
If this occurs the device can only be restored by reflashing it and the user data will be deleted. You can change the screen lock passcode as soon as the extraction is over and the device has been rebooted.



To successfully exploit the checkm8 vulnerability on iPhone 8, iPhone 8 Plus, iPhone X running iOS 14.0-15.4.1 and other supported devices running iOS 15.0-15.4.1, please turn off the device screen lock passcode.

If you disable the screen lock by entering the password,  
- Apple Pay cards will be deleted.  
- it will not be possible to reset the Apple ID password by entering the screen-lock password.

Details at [oxygen-forensic.com](https://oxygen-forensic.com)

『iOS14.0-15.4.1が搭載されている iPhone 8、8 Plus、iPhone X および iOS15.0-15.4.1が搭載されている他のデバイスについて、checkm8の脆弱性を利用するには、パスコードを入力して画面ロックを無効にしてください。』

SEPの脆弱性は画面ロックの無効化が不要で、iOS14.0-14.8が搭載されている iPhone7、7 Plus で利用できる可能性があります。

SEPの脆弱性を利用後、デバイスが無効化されてしまう可能性があるため、画面ロックのパスコードを変更しないでください。変更してしまった場合、デバイスの初期化が必要になりユーザデータは削除されます。抽出が完了し、デバイスが再起動されると画面ロックのパスコードは変更可能になります。』

『iOS14.0-15.4.1が搭載されている iPhone 8、8 Plus、iPhone X および iOS15.0-15.4.1が搭載されている他のデバイスについて、checkm8の脆弱性を利用するには、パスコードを入力して画面ロックを無効にします。』

パスワードを入力して画面ロックを無効にした場合、

- ApplePay カードは削除されます
- 画面ロックのパスコードを入力することで AppleID のパスワードはリセットされません 』

### 3 抽出データの違い

同一のデバイス(iPhone5s)を使用して、checkm8 で抽出したデータと iTunes backup で抽出したデータの違いを一覧表示します。

<iTunesBackup を暗号化オプション有で抽出した例>

Category	Count
Accounts and Passwords	148
Apple Notes	13
Calendar	54/2
Calls	26
Contacts	6
Files	1,935
Messages	13
OS Artifacts	37
Reports	
Snapshots	
WebKit Data	2
Wireless Connections	10
Faces	
Key Evidence	18
OCR	
Search	
Social Graph	
Statistics	
Timeline	490/75
Applications	12
Apple Maps	1
Apple Messages	13
Apple Photos	13
Event Log	26
Facebook	7
Facebook Messenger	31
Health	245
HouseParty	2
iBooks	1
Line	1
Phonebook	3
Safari Browser	166/75

















<checkm8 で抽出した例>

Category	Count
Accounts and Passwords	365
Apple Notes	30/17
Calendar	54/2
Calls	26
Contacts	76/5
Files	172,949
Messages	515
OS Artifacts	3,105/649
Reports	
Snapshots	
WebKit Data	17
Wireless Connections	10
Faces	
Key Evidence	106
OCR	
Search	
Social Graph	
Statistics	
Timeline	4,149/741
Applications	13
Apple Maps	1
Apple Messages	13
Apple Photos	13
Event Log	27/1
Facebook	68/2
Facebook Messenger	33
Health	248
HouseParty	37
iBooks	1
Line	4
Mail	502
Phonebook	3
Safari Browser	2,903/77

☛ 「Continue without unlocking screen」をクリックした場合：

同一のデバイス(iPhone5s)を使用して、画面ロック設定が有効化のまま、且つ DFU モードから復帰後に手動で画面ロックの解除も行わなかった場合の抽出結果を載せています。この様に得られるデータが少なくなります。

<画面ロックされたまま checkm8 で抽出した例>

Apple iPhone_withLockandON		
	Accounts and Passwords	127
	Contacts	
	Files	164,188
	OS Artifacts	37
	Reports	
	Snapshots	
	Wireless Connections	2/1
	Faces	
	Key Evidence	36
	OCR	
	Search	
	Social Graph	
	Statistics	
	Timeline	191
	Applications	1
	Facebook	10

### 改訂履歴

版数	発行日	改訂履歴
Ver. 1.0	2021年3月17日	初版発行
Ver. 1.1	2021年3月18日	タイトルの変更、本文の加筆修正
Ver. 1.2	2022年1月25日	UI 変更に伴う全体的な加筆修正
Ver. 1.3	2022年2月04日	ロックされている場合を加筆修正
Ver. 1.4	2022年5月13日	ツールの手順変更に伴い修正