UFED Touch2 Ver7.28 でサポートされた Full File System Extractions について

（原文：https://www.cellebrite.com/en/blog/a-practical-guide-to-checkm8/　2020/1/14）

checkra1n 脆弱性による checkm8 エクスプロイトを利用した新しいジェイルブレイクが、iOS デバイスからファイルシステムを抽出するために採用されました。

checkra1n を使用するには、Cydia や AFC2（Apple File Conduit 2）などの追加サービスのインストールが必要なデバイスもあれば、SSH プロトコルを使用して直接機能するデバイスもありました。

UFED 7.28 では、checkm8 によるファイルシステムの完全な抽出を実行できます。

このソリューションは、Cellebrite の UFED 4PC および Touch 2 プラットフォームで利用可能です。

UFED は、ロックされていない iOS デバイス（既知のパスコードまたは未設定）からのキーチェーン抽出、および未知のパスコードを持つロックされたデバイスからの部分的なファイルシステム（Before-First-Unlock）を含む完全なファイルシステム抽出をサポートするようになりました。

次の表は、サポートされているデバイスと iOS バージョンを示しています。

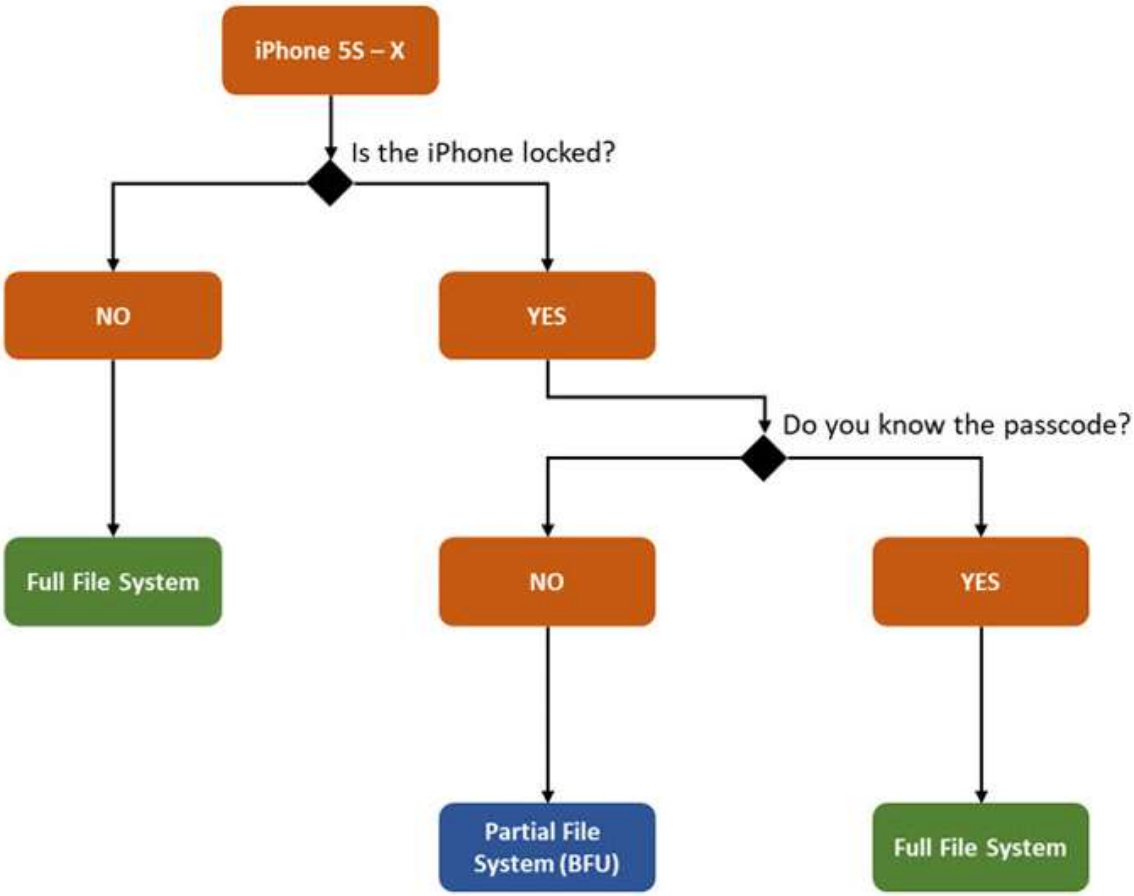
Supported devices and iOS versions – UFED 7.28

Device (SoC)	Minimum iOS version	Latest iOS version*
iPhone 5S (A7)	12.3	12.4.4
iPhone 6	iPhone 6 +(A8)	12.3	12.4.4
iPhone 6S	iPhone 6S + (A9)	12.3	13.3
iPhone SE (A9)	12.3	13.3
iPhone 7	iPhone 7+ (A10)	12.3	13.3
iPhone 8	iPhone 8+ (A11)	12.3	13.3
iPhone X (A11)	12.3	13.3

* UFED で検証された最新の iOS バージョン

将来的には、iOS がサポートする最新バージョンが継続的に更新されます。

“full file system”と“partial file system”（BFU）という用語との混同を避け、UFED を使用して各デバイスで何ができるかを明確にするために、下の決定フロー図を使用することをお勧めします。パスコードが不明なロックされたデバイスについては、追加のサポートについて Cellebrite にお問い合わせください。



1. To verify the iPhone’s model please look at the back of the device or use the IMEI in the SIM tray or Settings\General\About (if the device is unlocked)
2. If you don’t know the passcode it’s recommended to preform BFU

上の表の各デバイスについて、「Full-File System」（checkm8）と呼ばれる新しいメソッド（ボタン）を Advanced Logical の下に追加しました。ボタンを押すと、デバイスを「デバイスファームウェアアップデート」（DFU）モードにする方法の概要を示す一般的な指示画面が表示されます。

DFU にデバイスを配置するのは少し難しい場合があるため、リストされている iPhone バージョンについて以下の手順に従ってください。[続行]ボタンは、デバイスが DFU にある場合にのみ有効になります。iPhone の画面を見て、iOS の Cellebrite クライアントが表示されるかどうかを確認することで、攻撃が成功したかどうかを確認できます。

DFU ガイド

iPhone 5S | iPhone 6 | iPhone 6 以降| iPhone 6S | iPhone 6S + | iPhone SE

1　デバイスを回復モードにします。　（Apple iTunes ロゴが表示されます。）
2　「電源」ボタンを 3 秒間押します。
3　3 秒後、電源ボタンと「ホーム」ボタンの両方をさらに 10 秒間押し続けます。
4　ホームボタンをさらに 5 秒間押したまま、電源ボタンを放します。
5　UFED「Continue」が有効になります。

iPhone 7 | iPhone 7 以降

1　デバイスを回復モードにします。　（Apple iTunes ロゴが表示されます。）
2　「電源」ボタンと「音量を下げる」ボタンの両方を同時に 10 秒間押し続けます。
3　音量小ボタンをさらに 10 秒間押したまま、電源ボタンを放します。
4　UFED「Continue」が有効になります。

iPhone 8 | iPhone 8 以降| iPhone X

1　デバイスを回復モードにします。　（Apple iTunes ロゴが表示されます。）
2　リカバリ画面で、「ボリュームアップ」ボタンを短押しします。
3　「音量を下げる」ボタンを短押しします。
4　画面が完全にオフになるまで「サイド」ボタンを押し続けます。
5　サイドボタンと音量ダウンボタンの両方を同時に 5 秒間押し続けます。
6　音量を下げるボタンをさらに 10 秒間押したまま、サイドボタンを放します。
7　UFED「Continue」が有効になります。

checkm8 の未来

UFED の checkm8 パスはまだ始まったばかりです。新しい OS バージョンでは、それらをサポートするために追加の研究開発が必要になる場合があります。時間が必要な労力を教えてくれます。将来のバージョンでは、checkm8 により、審査官は特定のアプリケーションまたはファイルを直接抽出するために、詳細な「選択的」抽出を実行できるようになり、調査中の貴重な時間を節約できます。