Windows FE による X-Ways Forensics 起動メディアの作成

株式会社ディアイティ
セキュリティサービス事業部

1. はじめに

本手順書は、Windows FE を使用して USB メモリより OS を起動し、X-Ways Forensics を利用するためのメディアを作成するための手順書です。

(1)Windows FE について

Windows FE は、Troy Larson と Microsoft 社の Sr Forensic Examiner and Research によって開発された Windows PE をベースにしたフォレンジック用 Live CD です。

Windows FE は以下の特徴があります。

- USB デバイスからのブートも可能
- ブート時にローカルメディアをマウントしないように設計されている
- 様々なフォレンジックソフトウェアを含めることが可能

(2)免責事項

- 本手順書に記載事項は、当社の知識・経験に基づき、当社内の環境を前提としたものであり、すべての環境に対して有効であるとは限りません。
- 本手順書を利用される場合は、利用者自身の判断および責任の下で実施されるものとし、弊社は、本資料を利用したことにより被ったいかなる損害についても一切の責任を負いません。
- 本手順書内に記載されているフリーツールに関するお問い合わせは、弊社ではお受けすることはできません。
- X-Ways Forensics の利用には、ライセンスが必要です。
- 本手順書の著作権、その他知的財産権は、株式会社ディアイティに帰属します。利用者は、許可なく複製、転載、翻案、翻訳、販売等、その他一切の行為を行うことはできません。

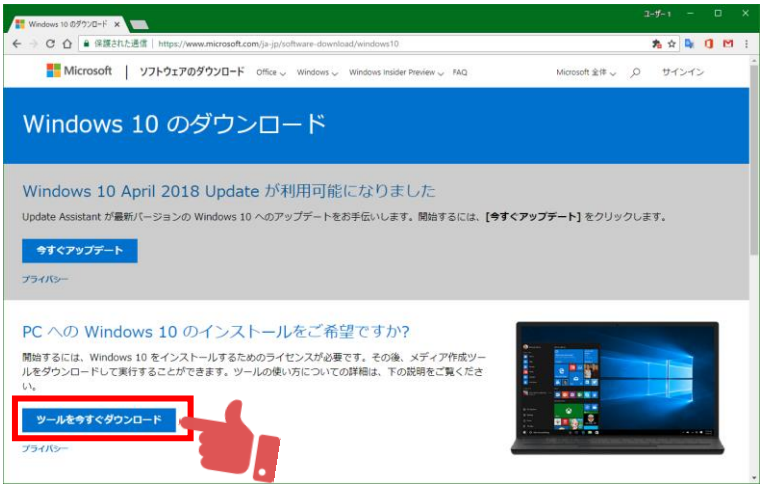
2. 事前準備

- 本書
- Windows 10 インストール ISO
  ※ ない場合は、「Windows 10 インストールメディアの入手」に従い入手。
- 4GB 以上の USB メモリ
- X-Ways Forensics
- X-Ways Forensics ドングル

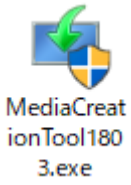
3. Windows 10 インストールメディアの入手

① 以下の URL にアクセスします。
https://www.microsoft.com/ja-jp/software-download/windows10

② 「ツールを今すぐダウンロード」をクリックし、ファイルをダウンロードします。

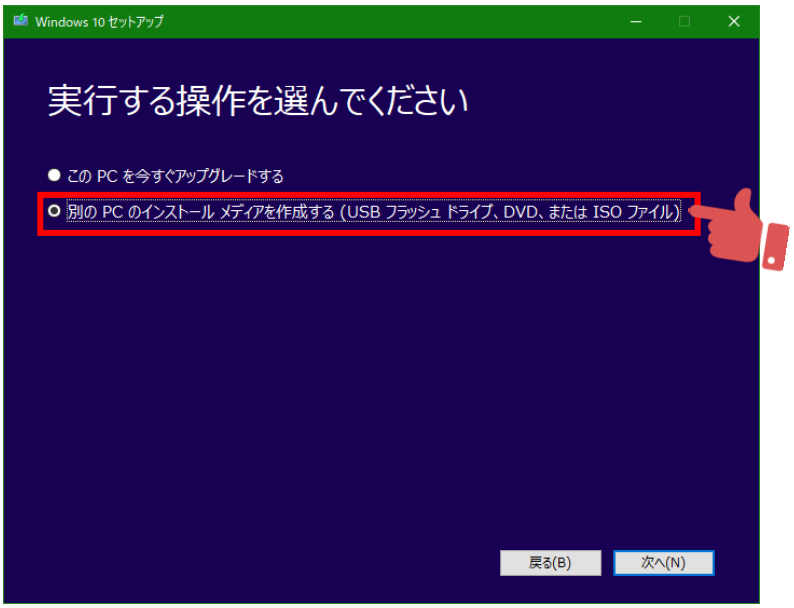


③ ダウンロードしたファイルをダブルクリックします。



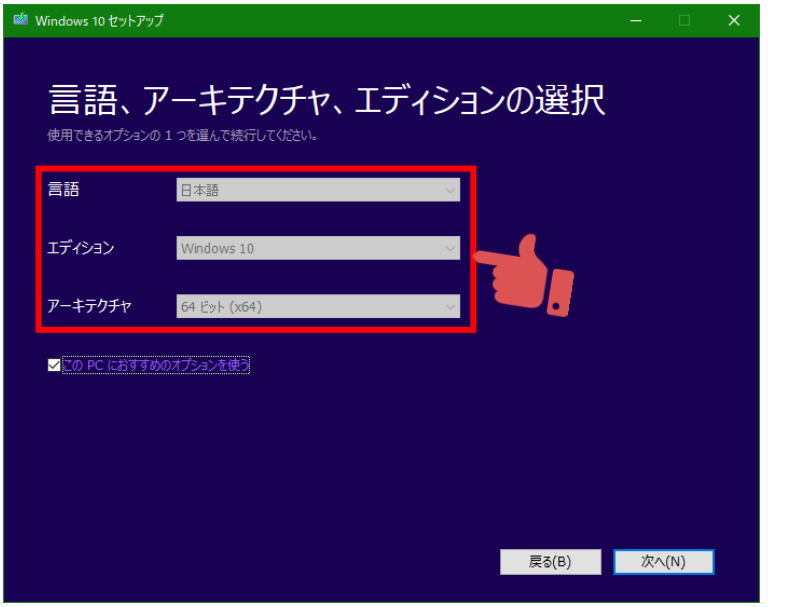
④ ライセンス条項の画面で、「同意する」をクリックします。

⑤ 「別の PC のインストールメディアを作成する(USB フラッシュドライブ、DVD、または ISO ファイル)」を選択し、「次へ」をクリックします。

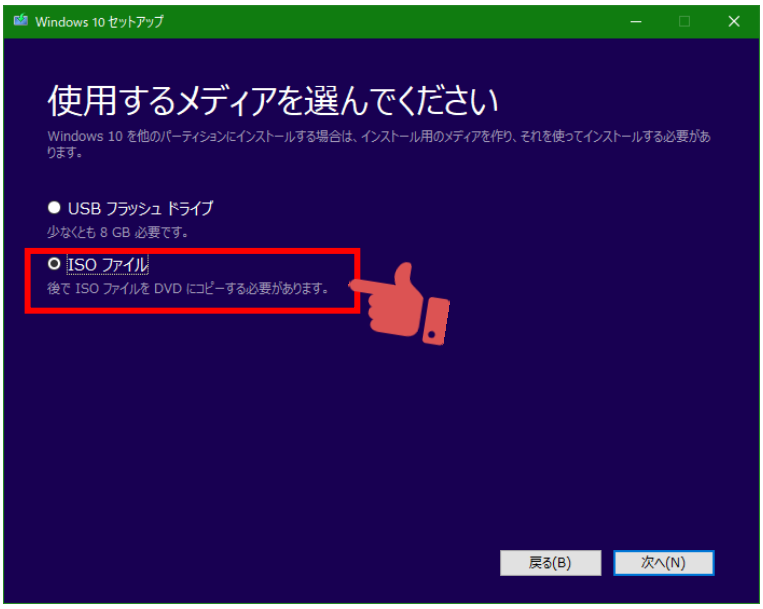


⑥ 以下の選択になっていることを確認し、「次へ」をクリックします。
異なる設定となっている場合は、「この PC におすすめのオプションを使う」のチェックを外し、各項目を選択してください。

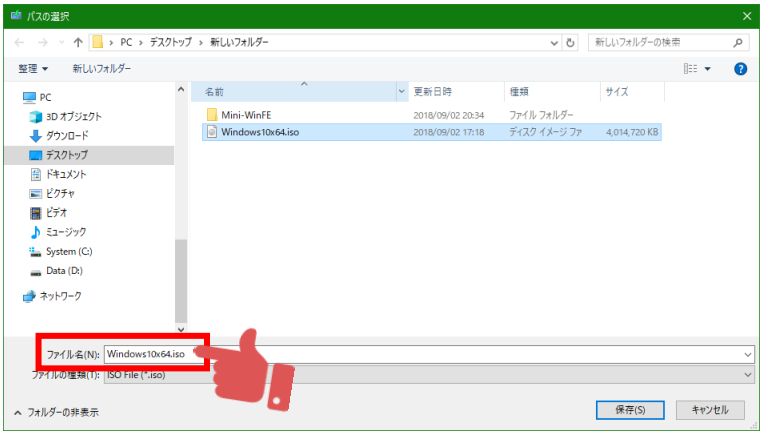
- 言語　：日本語
- エディション　：Windows 10
- アーキテクチャ　：64 ビット（x64）



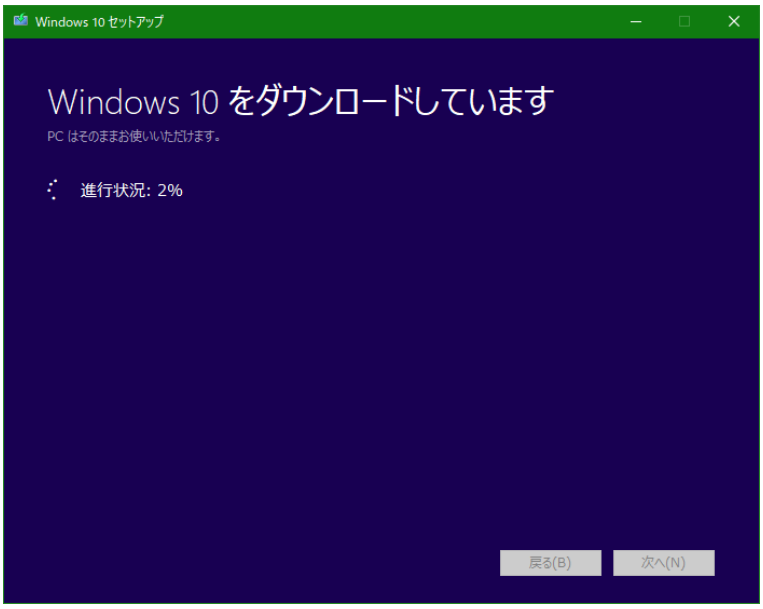
⑦ 使用するメディアで「ISO ファイル」を選択し、「次へ」をクリックします。



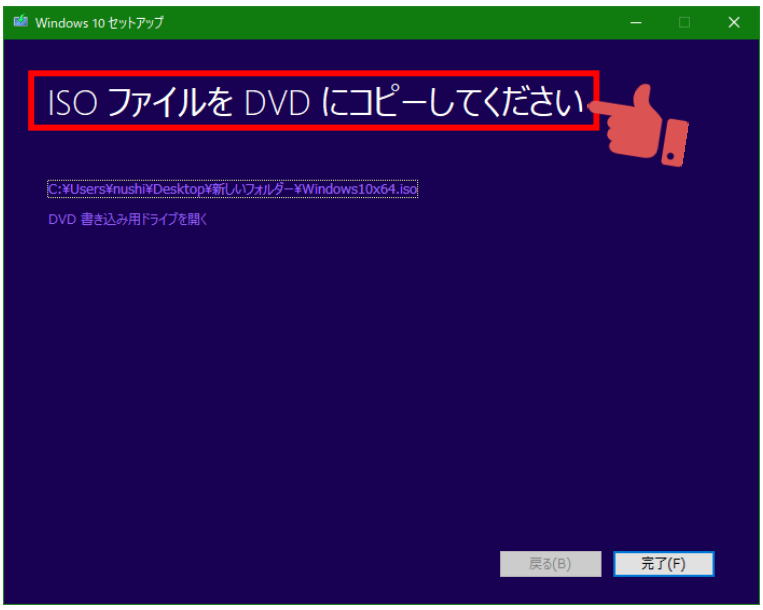
⑧ 任意の保存先を指定し、ファイル名に「Windows 10x64.iso」と入力して「保存」をクリックします。



⑨　Windows 10 のダウンロードが開始されます。



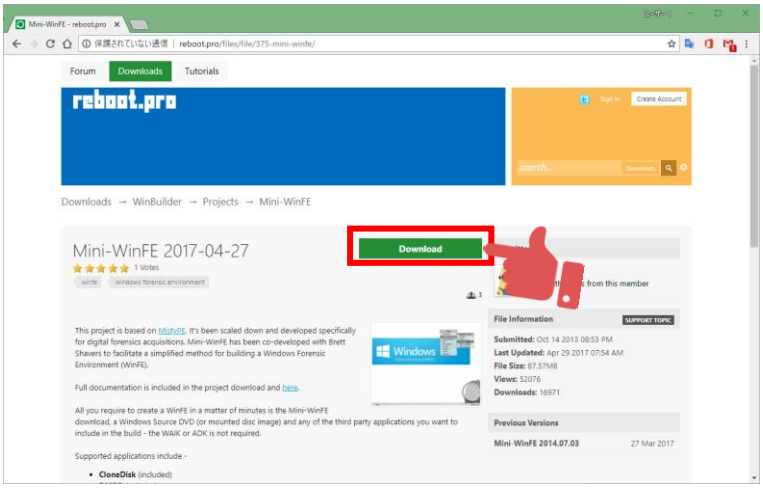
⑩　「ISO ファイルを DVD にコピーしてください」の画面が表示されましたら、作成の完了です。「完了」をクリックし終了します。



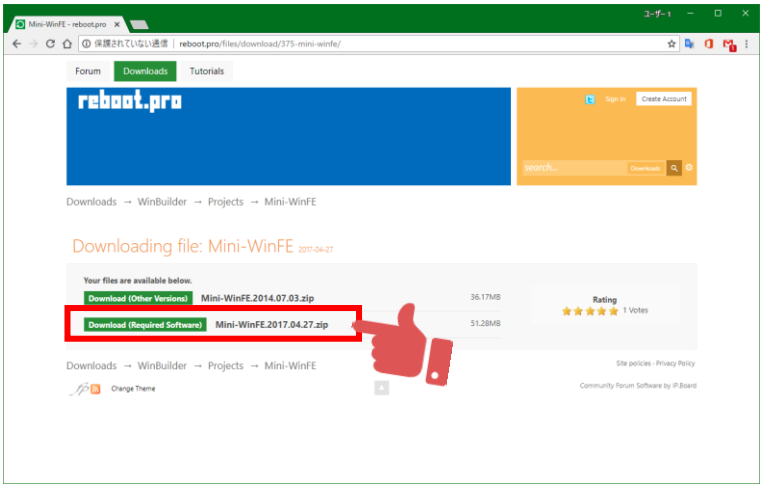
4. Mini-WinFE の入手

① 以下の URL にアクセスします。
http://reboot.pro/files/file/375-mini-winfe/

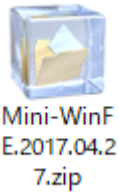
② 「Download」をクリックします。



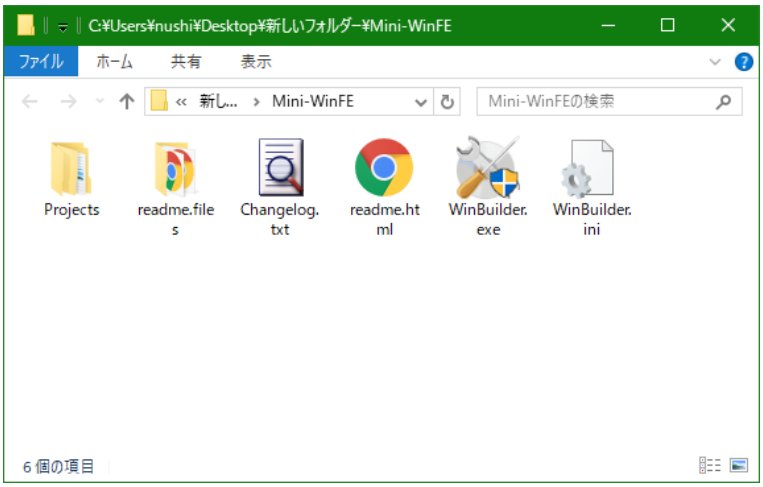
③ 最新の Mini-WinFE をダウンロードし、任意の場所に保存します。
※ 本書作成時点での最新版は、「Mini-WinFE.2017.04.27.zip」



④ 保存した Mini-WinFE の zip ファイルを展開します。



⑤ 展開された Mini-WinFE フォルダを開き、下図のファイルが作成されていることを確認します。

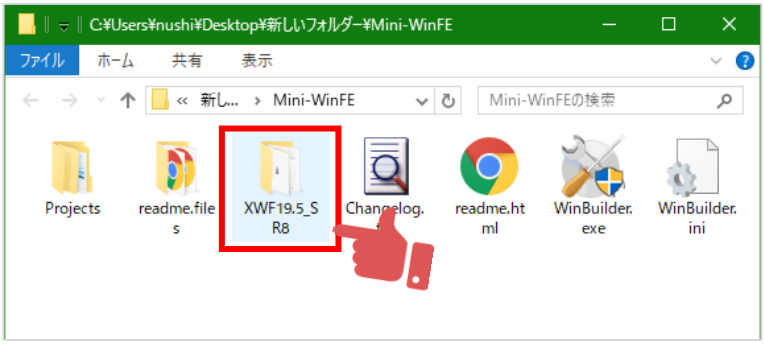


5. X-Ways Forensics 起動メディアの作成

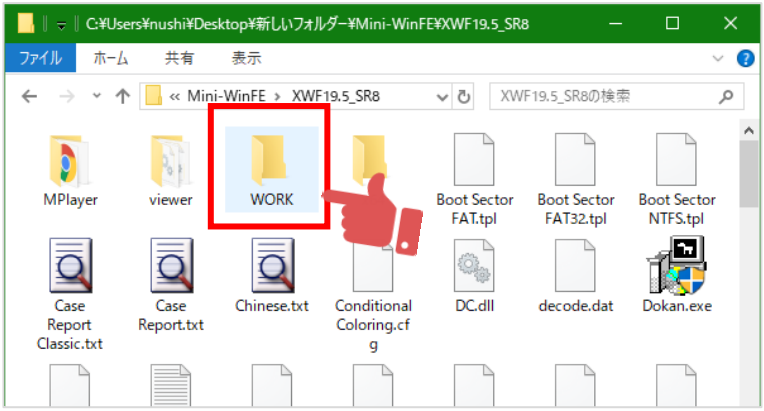
(1) X-Ways Forensics の設定

① 現在使用している X-Ways Forensics のフォルダを「Mini-WinFE」フォルダにコピーします。

※ 下図の例では、XWF19.5_SR8 をコピーしています。

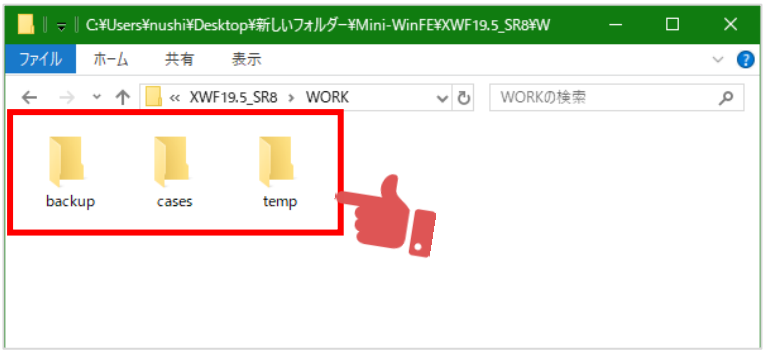


② X-Ways Forensics のフォルダを開き、配下に「WORK」フォルダを作成します。



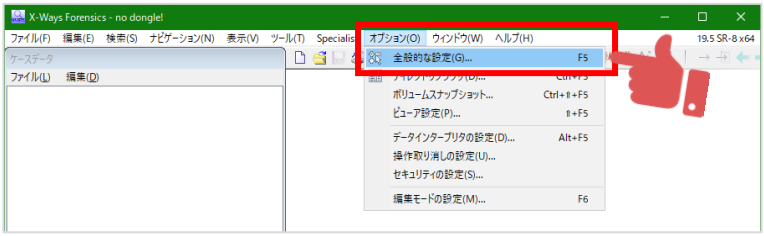
③ 「WORK」フォルダを開き、以下のフォルダを作成します。

- temp
- backup
- cases



④ PC に X-Ways Forensics ドングルを接続し、X-Ways Forensics を起動します。

⑤ [オプション]－[全般的な設定]を選択します。

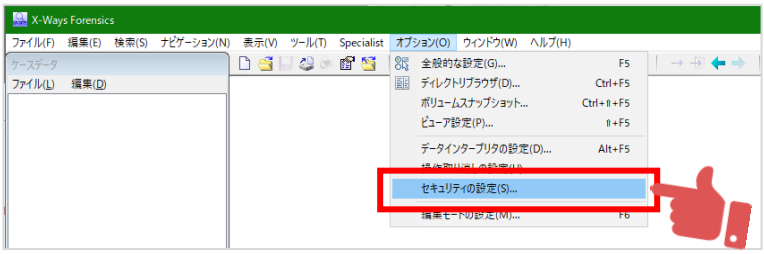


⑥ 「常に管理者として実行」にチェックを入れ、X-Ways Forensics の作業用フォルダを以下のように設定し、「OK」をクリックします。

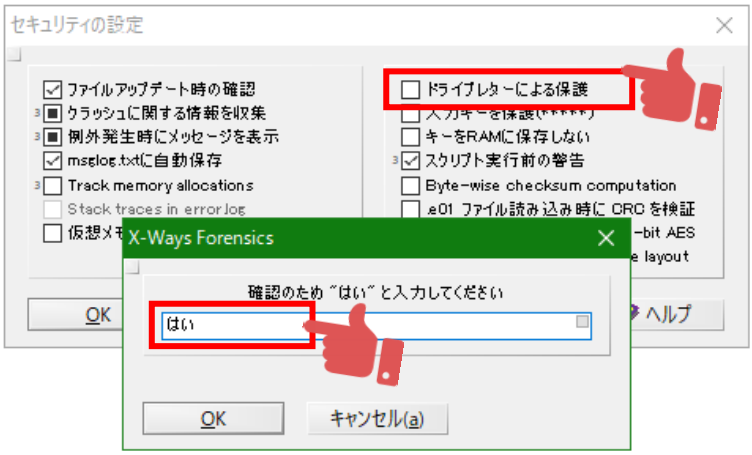
※ 相対パスで設定します。

- 常に管理者として実行 ： チェックを入れる
- 一時ファイル用フォルダ ： .¥WORK¥temp
- イメージ/バックアップ用フォルダ ： .¥WORK¥backup
- ケース/プロジェクト用フォルダ ： .¥WORK¥cases

⑦ [オプション]－[セキュリティの設定]を選択します。



⑧ 「ドライブレターによる保護」のチェックを外します。
確認の画面が表示されますので、日本語で「はい」と入力し、「OK」をクリックします。
チェックが外れていることを確認し、「OK」をクリックして「セキュリティの設定」を閉じます。

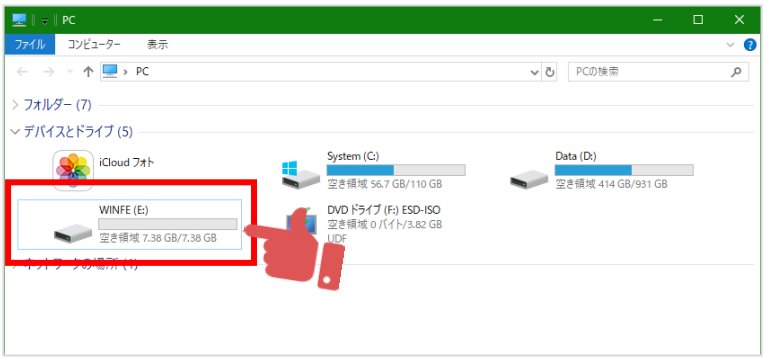


⑨ X-Ways Forensics を終了します。

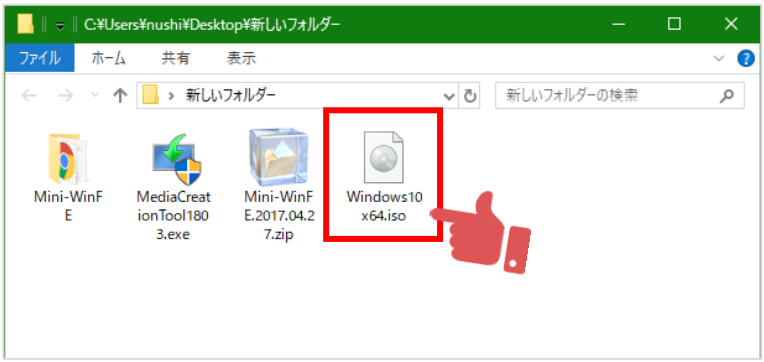
(2)ブートメディアの作成

① USB メモリを接続し、割り当てられたドライブレターを確認します。

※ 下図では、E ドライブ(E:)に割り当てられています。

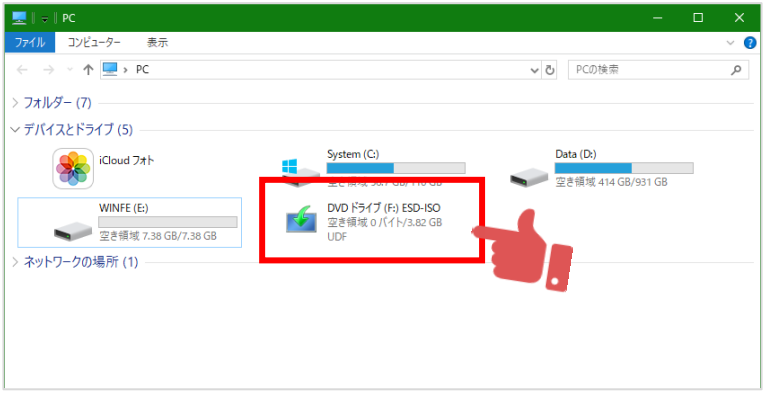


② ダウンロードした Windows 10 のインストール ISO をダブルクリックし、マウントします。

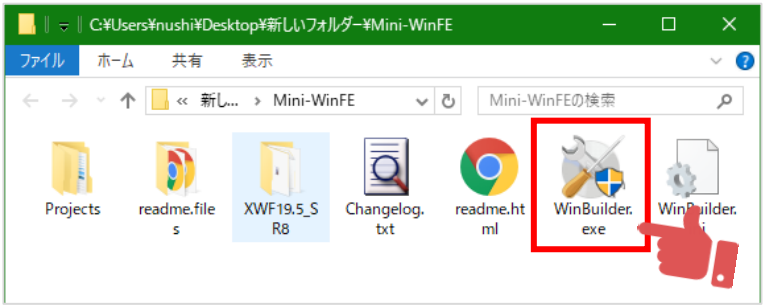


③ エクスプローラを開き、インストール ISO に割り当てられたドライブレターを確認します。

※ 下図では、F ドライブ(F:)に割り当てられています。

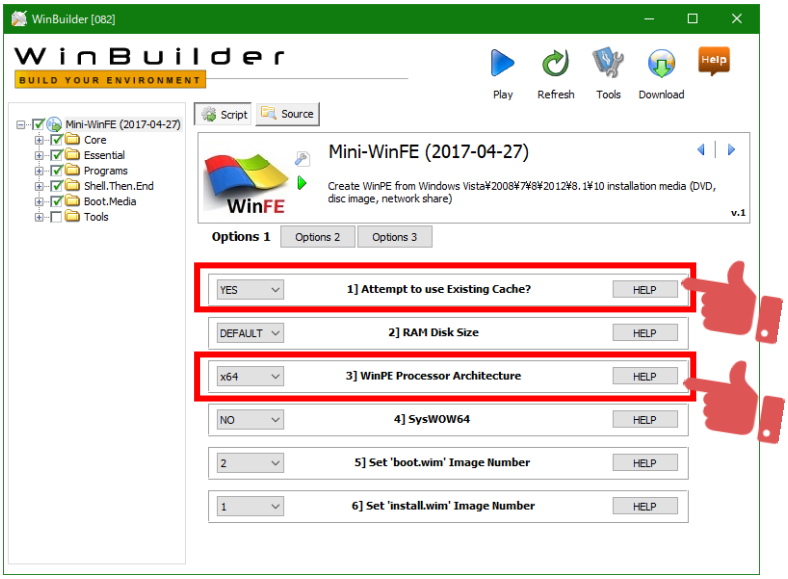


④　「Mini-WinFE」フォルダを開き、「WinBuilder.exe」をダブルクリックして起動します。



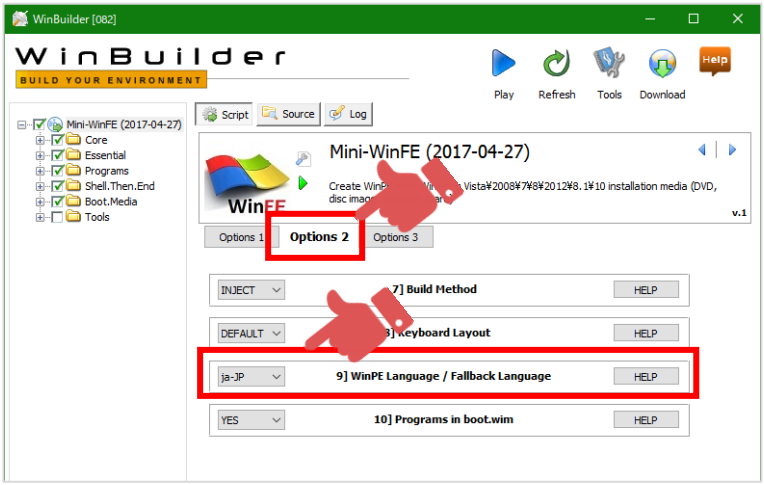
⑤　最初の画面で以下の項目を設定します。

- 1] Attempt to use Existing Cache?　：　NO
  - ※　初めて実施するときは「NO」、2 回目以降は「YES」にしてください。
- 3] WinPE Processor Architecture　：　x64

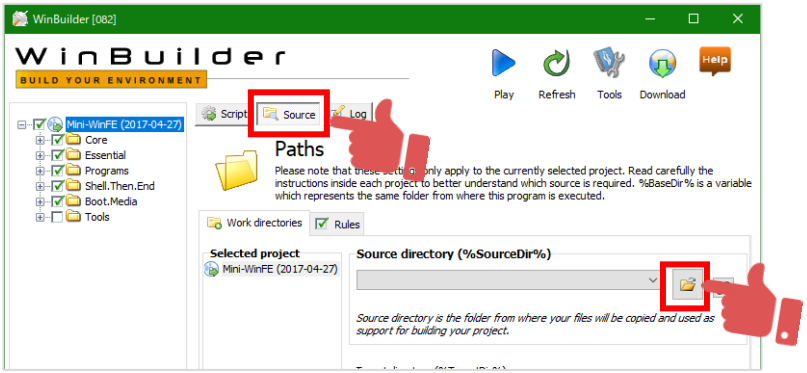


⑥　「Options 2」をクリックし、以下の項目を設定します。

- 9] WinPE Language / Fallback Language　：　ja-JP

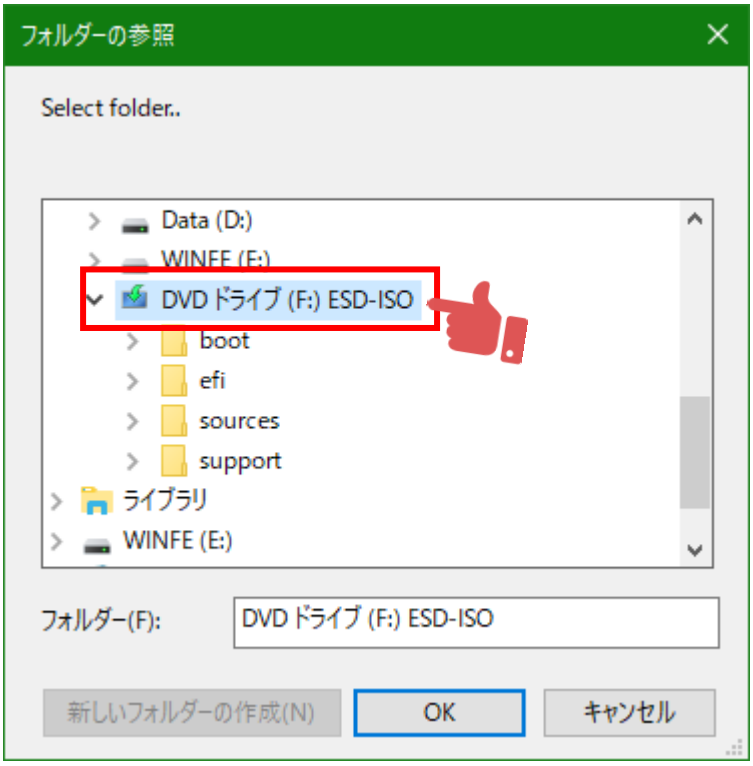


⑦　「Source」ボタンをクリックして画面を切り替え、「Source Directory (%SourceDir%)」の項目にあるフォルダアイコンのボタンをクリックします。

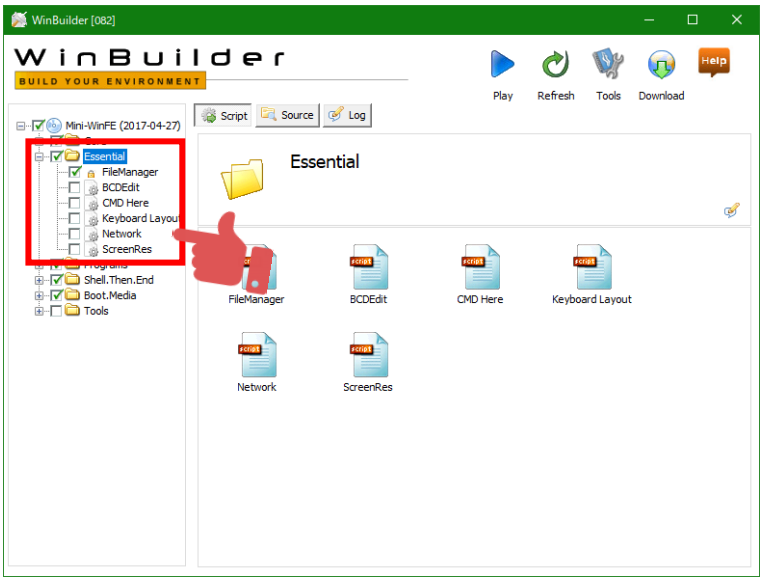


⑧　Windows 10 インストール ISO に割り当てられたドライブを選択し、「OK」をクリックします。

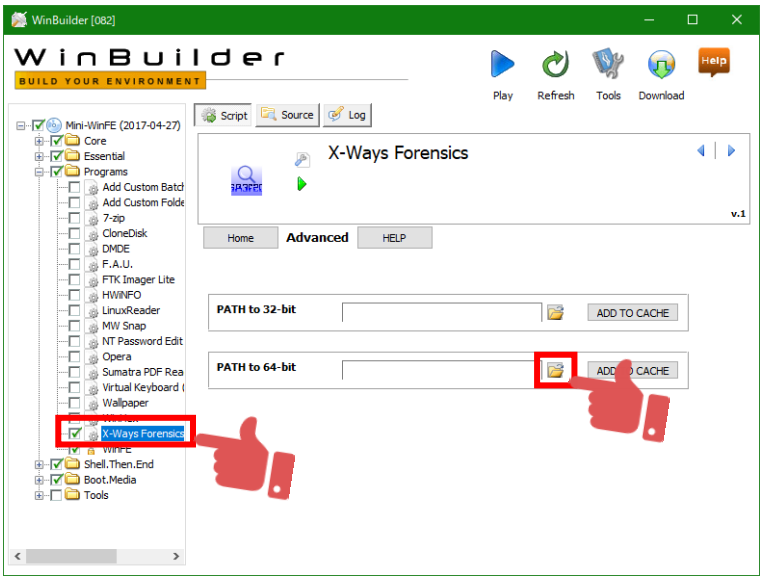
※　②の手順で確認したドライブレターを選択



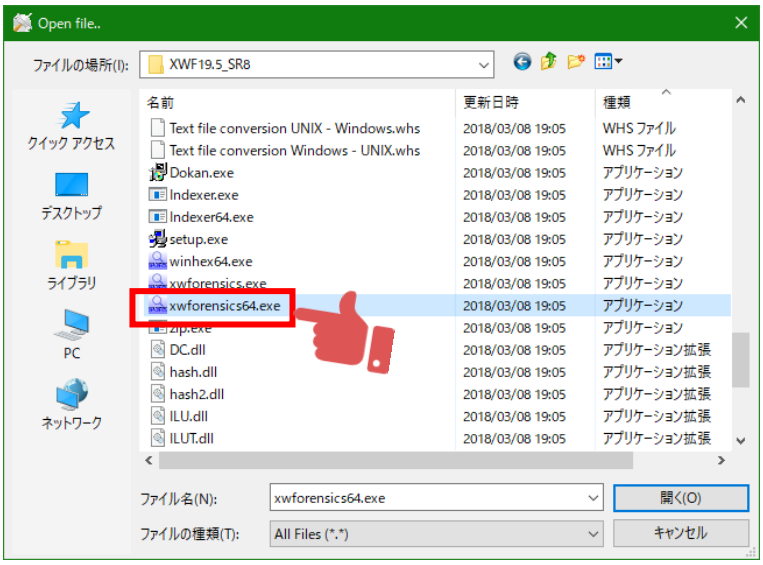
⑨ 左のツリーより、「Essential」を展開し、「FileManager」以外の項目のチェックを外します。



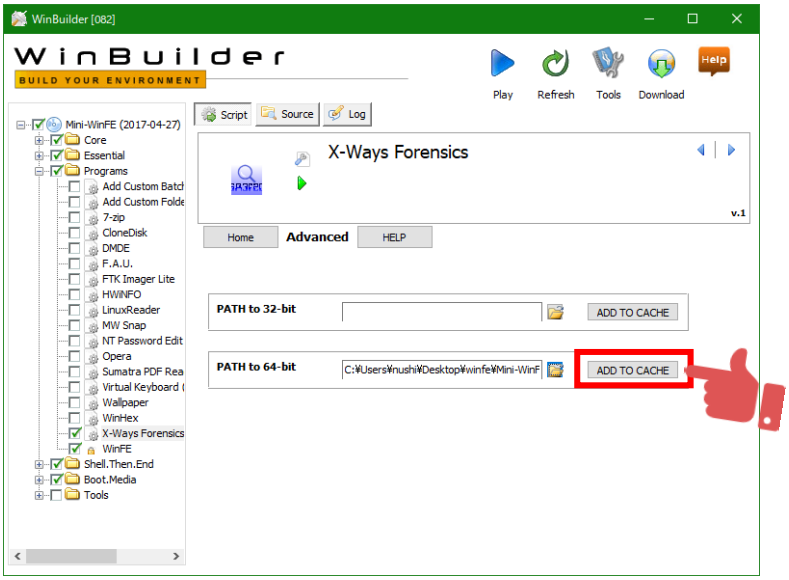
⑩ 「Programs」を展開し、「X-Ways Forensics」にチェックを入れます。
右の画面で、「PATH to 64-bit」の欄のフォルダアイコンのボタンをクリックします。



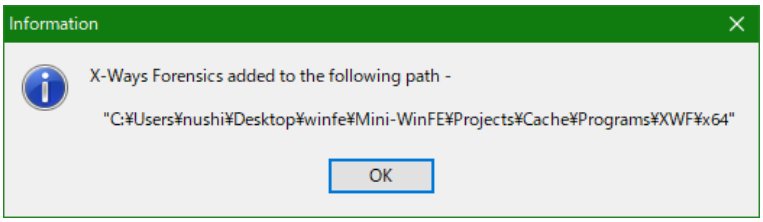
⑪ 「Mini-WinFE」フォルダにコピーした X-Ways Forensics のフォルダ（下図では「XWF19.5SR8」）を開き、「xwforensics64.exe」を選択して「開く」をクリックします。



⑫ 「PATH to 64-bit」の欄の「ADD TO CACHE」ボタンをクリックします。



⑬ キャッシュに成功すると、以下のような画面が表示されますので、「OK」をクリックします。

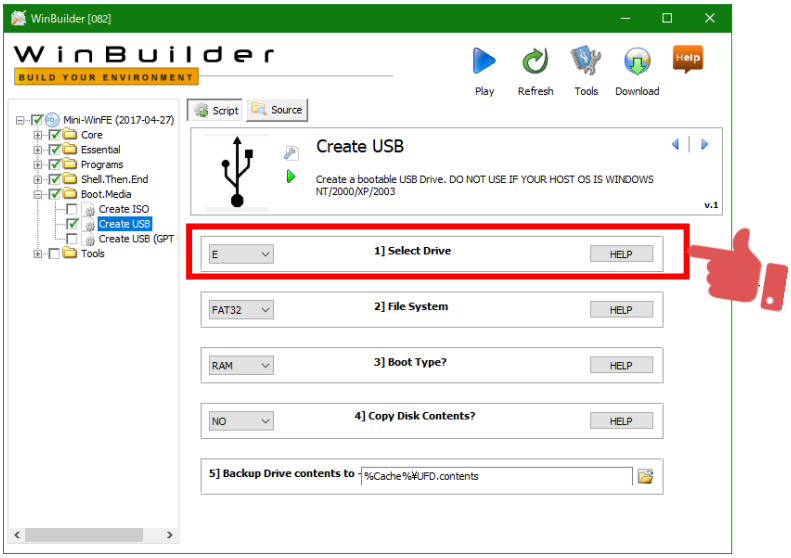


⑭ 「Boot.Media」を展開し、「Create USB」にのみチェックを入れ、右側の画面で以下の項目を設定します。

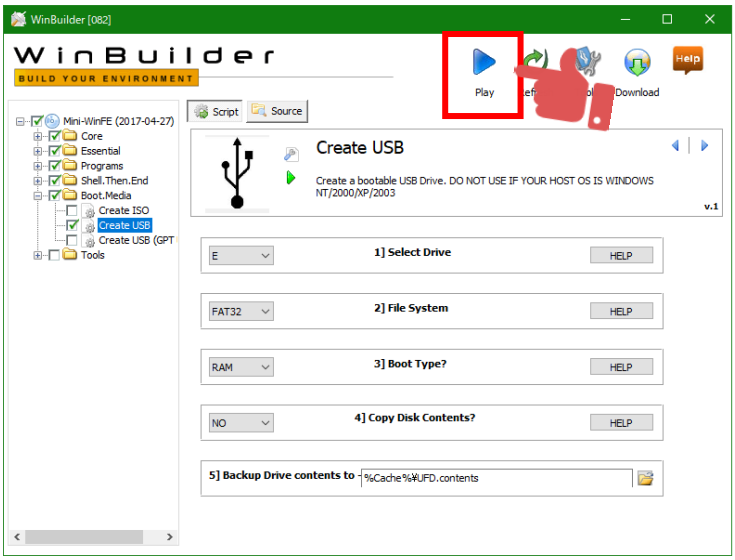
- 1] Select Drive ： ①の手順で確認した USB メモリのドライブレター

※ 下図では、E ドライブを選択しています。

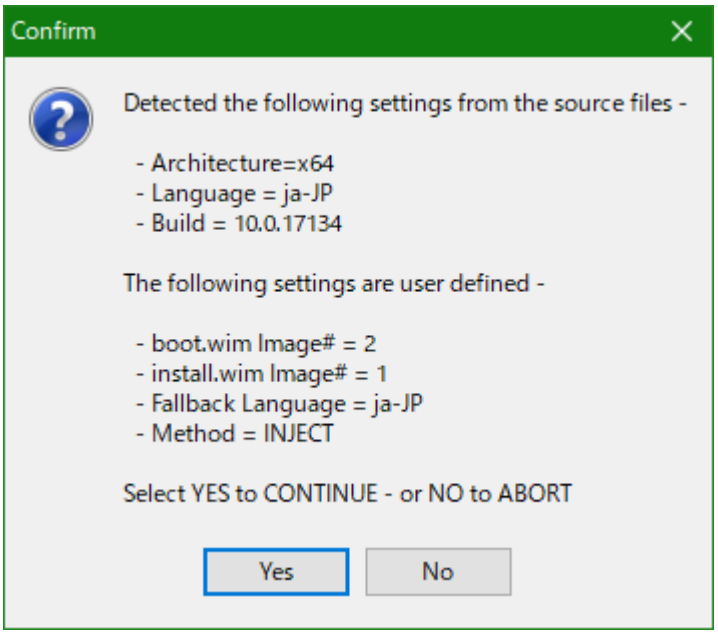
※ **メディア作成時に選択したドライブレターのディスクはフォーマットされます。必ず USB メモリのドライブレターが選択されていることを確認してください。**



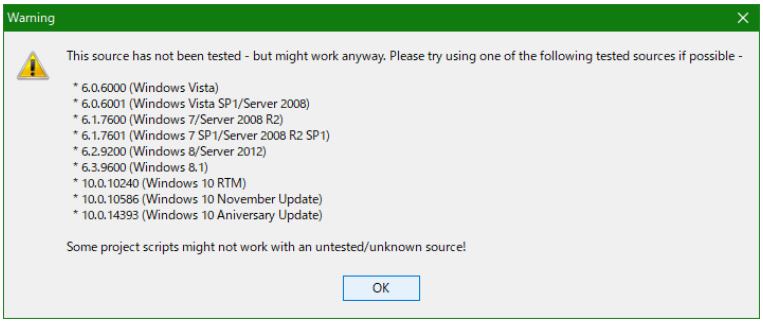
⑮ 「Play」ボタンをクリックします。
メディアの作成が開始されます。



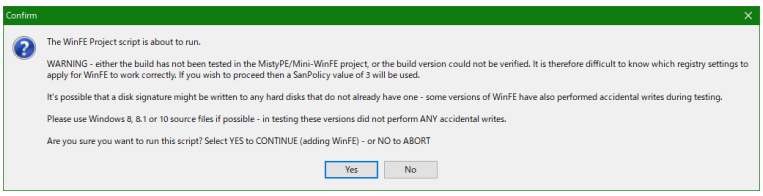
⑯　以下の画面が表示された場合は、「Yes」をクリックします。



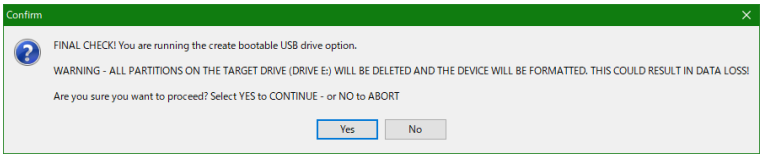
⑰　以下の画面が表示された場合は、「OK」をクリックします。



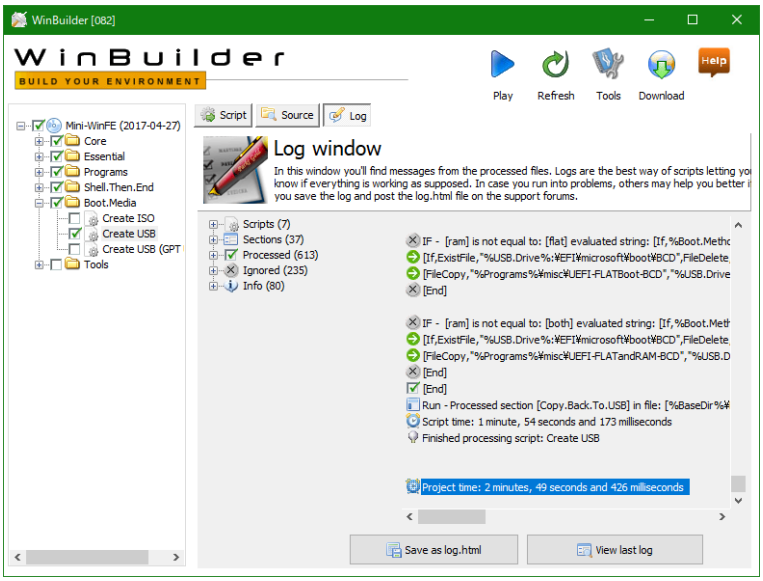
⑱　以下の画面が表示された場合は、「Yes」をクリックします。



⑲　以下の画面が表示された場合は、「Yes」をクリックします。



⑳　エラー表示なく、WinBuilder の画面に戻りましたら作成は完了です。
画面右上の「×」をクリックし終了します。



6. Windows FE による起動

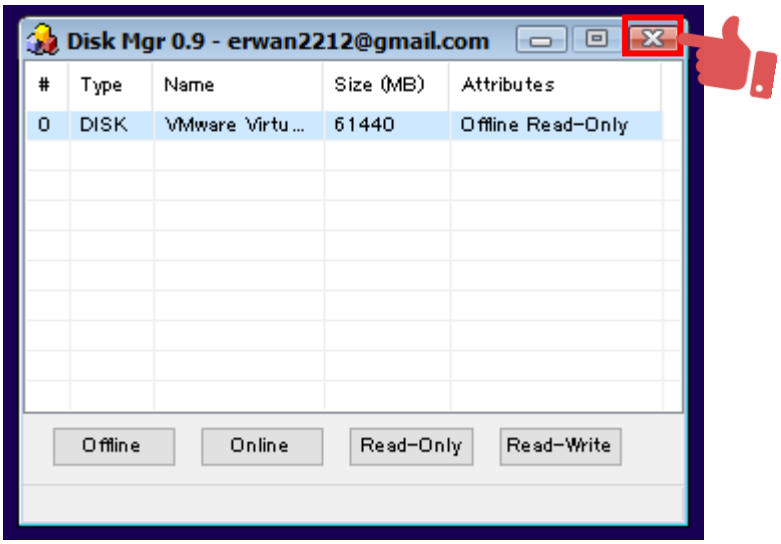
(1)Windows FE の起動

① 端末に Windows FE をインストールした USB メモリを接続し、電源を投入します。

② ファンクションキー（[F2]など)を押下し、ブートメニューを表示します。

※ ブートメニューを表示するファンクションキーは、メーカーにより異なります。必ずメーカーホームページ等で確認の上実施してください。

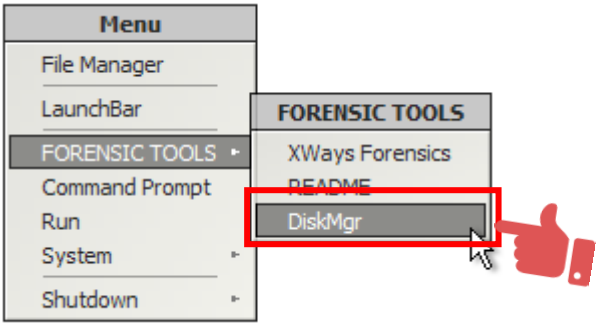
③ 以下のような画面（Disk Mgr)が表示されます。画面右上の「×」ボタンをクリックし、画面を閉じます。



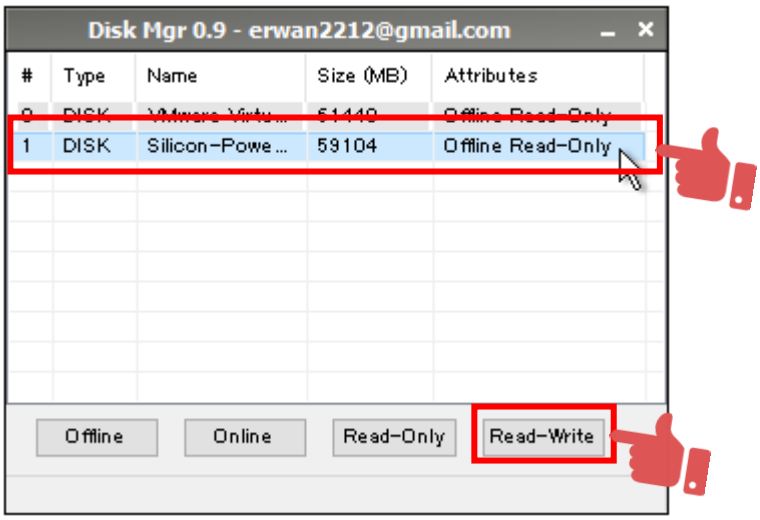
④ Windows FE が起動し、以下のような画面が表示されます。

⑤ 端末にイメージ保存用の USB-HDD を接続します。

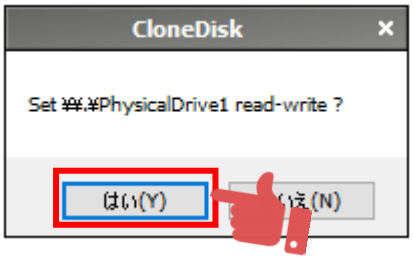
⑥ 画面上で右クリックすると、メニューが表示されます。
[FORENSIC TOOLS]－[DiskMgr]を選択します。



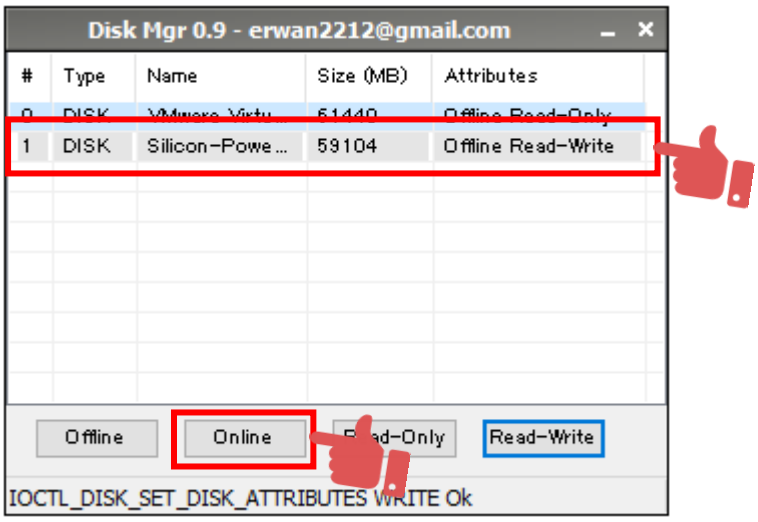
⑦ 接続した USB-HDD が表示されていることを確認します。
USB-HDD を選択し、「Read-Write」をクリックします。



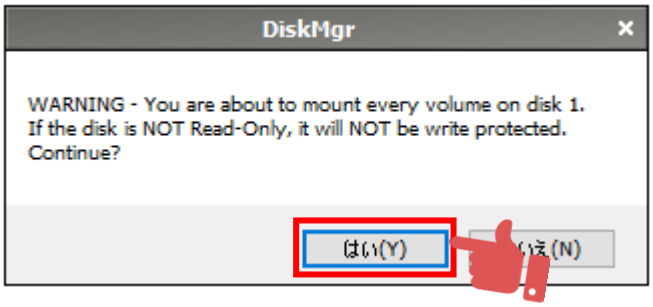
⑧ 確認の画面が表示されますので、「はい」をクリックします。



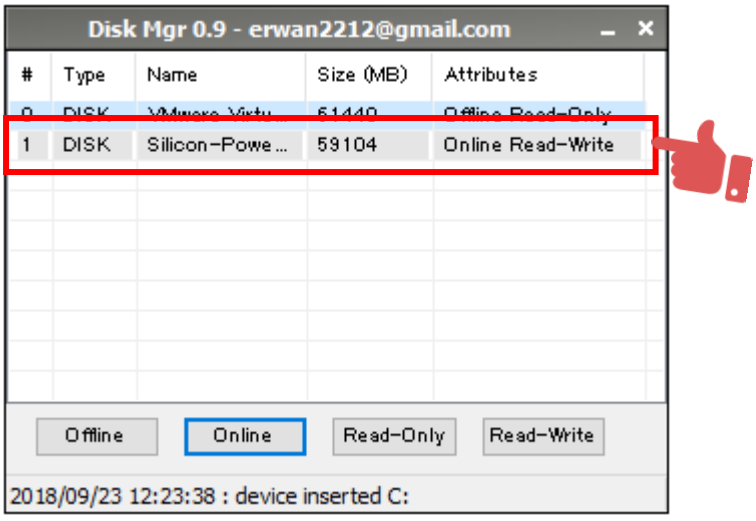
⑨ USB-HDD が「Offline Read-Write」と表示されていることを確認します。
USB-HDD を選択し、「Online」をクリックします。



⑩ 確認の画面が表示されますので、「はい」をクリックします。



⑪ USB-HDD が「Online Read-Write」と表示されていることを確認します。
右上の「×」をクリックし、画面を閉じます。



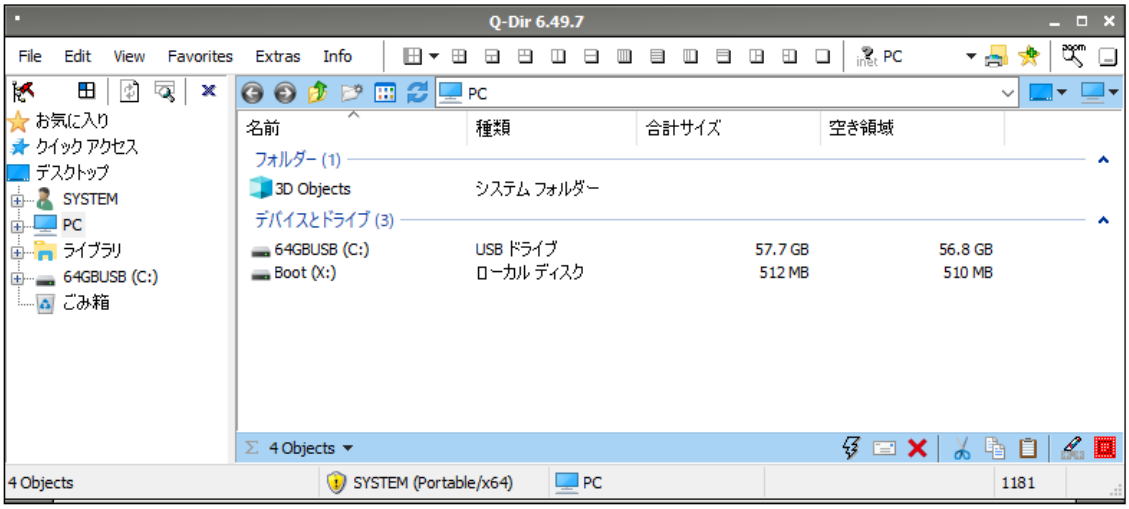
(2)Windows FE のドライブ構成

Windows FE で起動したときのドライブ構成は、以下のようになります。

※　構成は環境により異なる場合があります。

- C:　　：オンラインにした USB 外部接続デバイス（データ保存用）
  ※　Disk Mgr で外部接続デバイスを Online すると表示されます。
- X:　　：Windows FE のシステムドライブ

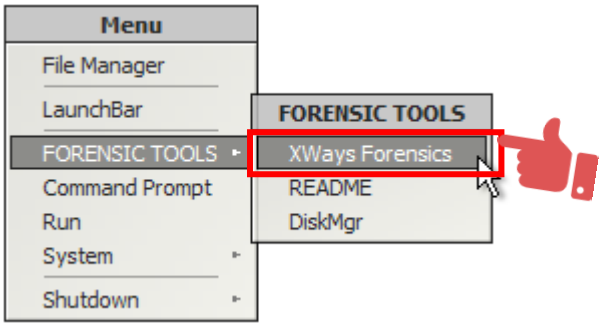
- X-Ways Forensics のプログラム、および WORK フォルダは以下のパスに格納されています。
  - X-Ways Forensics　：　X:¥Programs¥XWF
  - WORK フォルダ　　：　X:¥Programs¥XWF¥WORK
- Windows FE では、システムドライブ(X:)にデータを一時的に書き込むことはできますが、シャットダウン（または再起動)後、データは保持されません。
  データを保存する場合は、必ずデータ保存用として USB-HDD を接続してください。
- Windows FE 上でフォレンジックを実施する場合は、WORK フォルダを USB-HDD 上に再作成し、X-Ways Forensics の「全般的な設定」で temp、backup、cases フォルダの設定を変更してください。
- フォレンジックに十分なリソースが確保できない恐れがありますので、Windows FE での X-Ways Forensics の利用は、ディスクイメージの作成のみでご利用頂くことを推奨します。



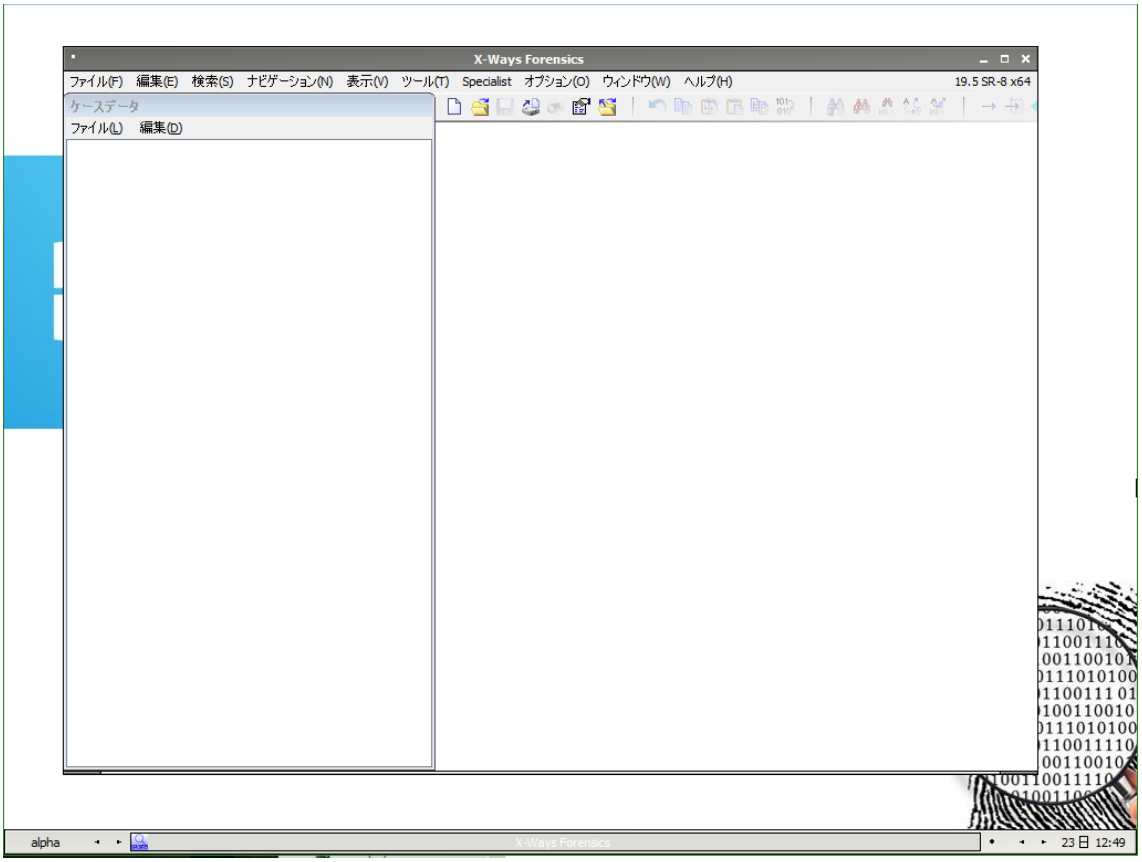
7. X-Ways Forensics の起動

① 端末に X-Ways Forensics のドングルを接続します。

② 画面を右クリックし、[FORENSIC TOOLS]－[XWays Forensics]を選択します。

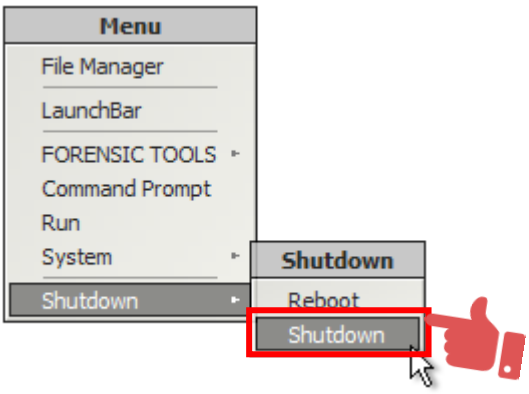


③ X-Ways Forensics が起動します。



8. Windows FE の終了

① 画面を右クリックし、[Shutdown]－[Shutdown]を選択します。



以 上