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





#### 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)

<b>1</b>	Windows 10 セットアップ				
	言語、ア	ーキテクチャ、エディションの選択 1 วを選んで続行してください。			
	言語	日本語			
	エデイション	Windows 10			
	アーキテクチャ	64 Ёуһ (х64) 🗸			
	<mark>√</mark> ೭೦ PC におすすめの	オプションを使う			
		戻る(B)	次へ	(N)	

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。

🃫 パスの選択						×
← → × ↑	' > 新しいフォルダー		ٽ ~	新しいフォルダーの特	東索	δ
整理 ▼ 新しいフォルダー						?
PC ^	名前 ^	∨ 更新日時	種類	サイズ		
	Mini-WinFE	2018/09/02 20:34	ファイル フォルダー			
↓ ダウンロード	Windows10x64.iso	2018/09/02 17:18	ディスク イメージ ファ	4,014,720 KB		
三. デスクトップ						
F#1X7F						
■ ピクチャ						
📰 ಲೆಸ್ಸ						
🎝 ミュージック						
System (C:)						
👝 Data (D:)						
💣 ネットワーク						
-						
v						
ファイル名(N): Windows10x64.iso	4					~
ファイルの檀類(T): ISO File (*.iso)						~
▲ フォルダーの非表示	-			保存(S)	キャンセ	٧.

⑨ Windows 10 のダウンロードが開始されます。



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。

🛍 Windows 10 セットアップ	- 0	×
ISO ファイルを DVD にコピーしてください		
C:¥Users¥nushi¥Desktop¥新しいフォルター¥Windows10x64.iso		
DVD 書き込み用ドライブを開く		
戻る(B)	完了(F)	

## dit

## 4. Mini-WinFE の入手

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

Mini-WinFE - reboot.pro X				
← → C 合 ① 保護されていない通信	reboot.pro/files/download/375-mini-winfe/		x 🗣 🤇	) 📲 i
Forum Downloads	Tutorials			
reboot.pro			Sign In Create Account	
			search Downloads Q Q	
Downloads → WinBuild	er → Projects → Mini-WinFE			
Downloading	file: Mini-WinFE 2017-04-27			
Your files are available be	low.			
Download (Other Versio	ns) Mini-WinFE.2014.07.03.zip	36.17MB	Rating	
Download (Required Sol	tware) Mini-WinFE.2017.04.27.zip	51.28MB	Image: Single Contribution       Image: Single Contribution	
Downloads → WinBuild	er → Projects → Mini-WinFF		Site policies - Privacy Policy	
Jp 🛐 Change Theme			Community Forum Software by IP.Board	

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

- 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。

🔜 X-Ways Forensics - no dongle!						
ファイル(F) 編集(E) 検索(S) ナビゲーション(N) 表示(V) ツ ケーステータ ファイル(L) 編集(D)	-JL(T) Specialis	オブション(O) ウィンドウ(W) ヘルブ(H) 会般的な設定(G ボリュームスナップショット ビューア設定(P)	F5 Ctrl+1+F5 1+F5	-	19.5 SI	R-8 x64
		データインターブリタの設定(D) 操作取り消しの設定(U) セキュリティの設定(S)	Alt+F5			
		編集モードの設定(M)	F6			

- 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
    - ▶ 一時ファイル用フォルダ
    - ▶ イメージ/バックアップ用フォルダ : <u>.</u>¥WORK¥backup
    - ▶ ケース/プロジェクト用フォルダ : <u>.¥WORK¥cases</u>
- : チェックを入れる
- : .¥WORK¥temp

全般的な設定	×
○ 常に管理者として実行           ● 時間がで時のウベンドや設定を           ● 前面球で時のウベンドや設定を           ● 前面球で時のウベンドや設定を           ● 「方へンドウを最大化してテータを!           ● 「百 原型のある大阪(*)           ● 「百 房屋のある大阪(*)           ● 「方ク・レドウを最大化してテータを!           ● 「百 房屋のある大阪(*)           ● 「百 房屋のある大阪(*)           ● 「西谷のある大阪(*)           ● 「西谷のかのコンテキストメニューに表示(d)           ● 「五クリーンセーバーの起動を阻止           ● 「 コクシム教定を ork ファイルに保存           ● ディスク配置によるパーティション毎号           ● 削除パーティションの自動検出	<ul> <li>自動生成(G) 0× 000A with ENTER</li> <li>Tabキー入力による5 J - ド入力(T)</li> <li>C0/200文字表現</li> <li>11 (トレ文字としてテキストを表示)</li> <li>たらびきアドレス使用(N)</li> <li>たびきアドレス使用(N)</li> <li>たびきアドレス使用(N)</li> <li>ためのパイカ数</li> <li>ヴルーフあたりのパイト数</li> <li>ヴルーフあたりのパイト数</li> <li>ヴルーフもたりのパイト数</li> <li>ヴルースをためパイト数</li> <li>ヴルースをためパイト数</li> <li>ヴレースをためパイト数</li> <li>ビクセルの追加(F間スペース)</li> <li>マティルモードで快速結果を強調表示)</li> <li>の自動方・リング:</li> <li>ア</li> </ul>

⑦ [オプション]-[セキュリティの設定]を選択します。

🔒 X-Way	s Forensic											
ファイル(F)	編集(E)	検索(S)	ナビゲーション(N)	表示(V)	ツール(T)	Specialist	オプ	ション(0)	ウィンドウ(W)	ヘルプ(H)		
ケースデータ				🗋 🍯 I	] 🤩 🗞	🗊 🛅	85	全般的;	な設定(G)		F5	$\rightarrow - $
ファイル(上)	編集( <u>D</u> )							ディレクト	ヽリブラウザ(D)		Ctrl+F5	
								ボリューノ	ムナップショット		Ctrl+1+F5	
								ビューア	受定(P)		1+F5	
								データイン	ソタープリタの設:	定(D)	Alt+F5	
								セキュリ	ティの設定(S)			
								福果t-	・トの設定(M)		F6	



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。

セキュリティの設定	×
<ul> <li>✓ ファイルアップデート時の確認</li> <li>■ クラッシュに関する情報を収集</li> <li>■ 例外発生時にメッセージを表示</li> <li>✓ msslog.txtに自動保存</li> <li>■ Track memory allocations</li> <li>Stack traces in error log</li> </ul>	<ul> <li>ドライブレターによる保護</li> <li>人 ハキーを保護(*****)</li> <li>キーをRAMに保存しない</li> <li>マカリブト実行前の警告</li> <li>Byte-wise checksum computation</li> <li>e01 ファイル読み込み時に CBC を検証</li> </ul>
□ 仮想Xモ X-Ways Forensics	-bit AES e layout
<u>QK</u> <u> 健認のため</u> ~はい	**と入力してください * ヘルプ
<u>Q</u> K +v:	ノセル( <u>a)</u>

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。

🔜    🗢    PC		- 0	×
ファイル コンピューター 表示			~ <b>(</b> )
$\leftrightarrow \rightarrow \checkmark \uparrow \blacksquare PC$		✓ 己 PCの検索	Q
> フォルダー (7)			
~ デバイスとドライブ (5)			
iCloud 7#1	System (C:)	Data (D:)	
	空き領域 56.7 GB/110 GB	空き領域 414 GB/931 GB	
WINFE (E:)	DVD ドライブ (F:) ESD-ISO		
空き領域 7.38 GB/7.38 GB	UDF		
<del>&gt; +&gt;+ &gt; &gt; &gt; &gt; &gt; &gt; &gt; &gt; = = =</del>			
	4		

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。

∥ ≂ ∥ C:¥Use	rs¥nushi¥Deskt	op¥新しいフォルタ	1-			—	×
ファイル ホーム	共有	表示					~ 🕐
$\leftarrow \rightarrow \cdot \uparrow$	> 新しい	フォルダー		~ Ō	新しいフォルダ-	の検索	Q
Mini-WinF E	MediaCreat ionTool180 3.exe	Mini-WinF E.2017.04.2 7.zip	Windows10 x64.iso				

- 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。

🔜    🗢    PC		-	×
ファイル コンピューター 表示 ← → ✓ ↑ ↓ PC		✓ O PCの検索	> ?
> フォルダー (7)			
デバイスとドライブ (5) iCloud フォト	System (C:)	Data (D:)	
WINFE (E:)	<u> </u>	空き領域 414 GB/931 GB	
空き領域 7.38 GB/7.38 GB       > ネットワークの場所 (1)	UDF		



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? : <u>NO</u>
     ※ 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

鯅 WinBuilder [082]					— C	x c
WinBui	lder		Ø	Wy.	<b></b>	Help
BUILD YOUR ENVIRONMEN	Script Source	Play	Refresh	Tools	Download	4
B C Descrive B C Description B C Description B C Description B	WinFE Create V disc imag	WinPE from Windows Vista¥2008¥3 ge, network share)	7¥8¥2012¥8.	1¥10 installa	ition media (	DVD, v.1
	Options 1 Options 2	Options 3	<b>-</b> 7	н	IFI P	
	DEFAULT ~	2] RAM Disk Size		н	ELP	
	x64 ~ 3] W	VinPE Processor Architecture		Н	ELP	
	NO V	4] SysW0W64		Н	IELP	
	2 ~ 5]	Set 'boot.wim' Image Numbe	er	Н	IELP	
	1 ~ 6]	Set 'install.wim' Image Numb	er	Н	IELP	

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

鯅 WinBuilder [082]					-		×
WinBui	lder		Ø	Wy.	•	Hel	Р
BUILD YOUR ENVIRONME	Script Surce Surce Log Mini-Winf WinFF Options 1 Options 2 Option	Play E (2017-04-27 V Vista¥2008¥2 5 3	Refresh	Tools	Download	4   a (DVD,	> v.1
	IDEFALLT     IDEFALLT       IDEFALLT     IDEFALLT       Iga-3P     9] WinPE Land       IVES     10] Provide	Build Method eyboard Layout guage / Fallback Lang rograms in boot.wim	uage		HELP HELP HELP		



「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。

💓 WinBuilder [082]						-		×
WinBui	lder			Ø	<b>B</b>	•	Help	
	Script Source Please note to instructions is which represent	Log hat these settle to only apply uside each project to better u units the same folder from who Rules	Play to the curre nderstand v ere this prog	Refresh ently selecte which source gram is exec	Tools d project. is required uted.	Download Read carefu 1. %BaseDir	lly the % is a va	riable
	Selected project	Source directory (% Source directory is the fo support for building your	SourceD	<b>ir%)</b> here your fi	es will be c	copied and u	sed as	

- 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

フォルダーの参照	×
Select folder.	
> 👝 Data (D:)	^
> WINFE (E:)	
✓ M DVD ドライブ (F:) ESD-ISO	
> boot	
> efi	
> sources	
> support	
> 🀂 ライブラリ	
> WINFE (E:)	~
フォルダー(F): DVD ドライブ (F:) ESD-ISO	
新しいフォルダーの作成(N) OK キャンセル	, 



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。



① 「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。

鯅 WinBuilder [082]					-		×
	der		٢	<b>W</b>	<b></b>	Hei	P
	🐞 Script 🔄 Source 🧭 Log	Play	Reffesh	TOOIS	Download		
Core Core Core Core Core Core Core Core	X-Ways Forensics					<b>∢</b>	
7-zip CloneDisk DMDE F.A.U.	Home Advanced HELP						v.1
HWINFO	PATH to 32-bit			ADD TO	CACHE		
	PATH to 64-bit			ADD	CACHE		
- ✔ 🗋 X-Ways Forensics - ✔ Shell Then.End ⊕ - ✔ 🖨 Boot.Media							
⊕-□ Cools							



 「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。



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

💢 WinBuilder [082]					-		×
WinBui	lder		Ø	<b>W</b>	<b></b>	Help	
	📸 Script 🔄 Source 🧭 Log	Play	Refresh	Tools	Download		
Core     Core     Sesential     Original Add Custom Batch     Add Custom Folde	X-Ways Forensi	cs				<b>∢</b>	
7-zip CloneDisk DMDE F.A.U. FTK Imager Lite	Home Advanced HELP						v.1
	PATH to 32-bit		1	ADD TO	CACHE		
Opera     Sumatra PDF Rea     Virtual Keyboard (     Walpaper     WinHex	PATH to 64-bit C:\Users\	op¥winfe¥Mini-V	/inF	ADD TO	O CACHE	1	5
X-Ways Forensics							
٢ >							

③ 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。

Informati	on X
1	X-Ways Forensics added to the following path - "C:¥Users¥nushi¥Desktop¥winfe¥Mini-WinFE¥Projects¥Cache¥Programs¥XWF¥x64"
	ОК



- ④ 「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。

泛 WinBuilder [082]						□ ×
	der		<b>O</b> Pafrath	Tools	Download	нер
Mini-WinFE (2017-04-27)     Ore     Gree     Gree     Sesntial     Gree     Sel. Then.End     Greet 500	Script Source	USB stable USB Drive. DO NOT USE 2003	IF YOUR HC	ST OS IS	WINDOWS	•   •
Greate LSG - Greate USB Greate USB Create USB Create USB Create USB Tools	E v	1] Select Drive			HELP	
	FAT32 V	2] File System			HELP	
	RAM V	3] Boot Type?			HELP	
	NO ~ 4] C	Copy Disk Contents?			HELP	
	5] Backup Drive contents to - %	Cache%¥UFD.contents				
< >>						

「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。

鯅 WinBuilder [082]		- 0	ı x
	I der Script 🔍 Source	Download	Help
	Create USB     Create USB Drive. DO NOT USE IF YOUR HOST OS     NT/2000/XP/2003	IS WINDOWS	•   •
	E v 1] Select Drive	HELP	
	FAT32 V 2] File System	HELP	
	RAM V 3] Boot Type?	HELP	
	NO V 4] Copy Disk Contents?	HELP	
	5] Backup Drive contents to -{%Cache%%UFD.contents		
< >			

<sup>16</sup> 以下の画面が表示された場合は、「Yes」をクリックします。

Confirm	×
?	Detected the following settings from the source files Architecture=x64 - Language = ja-JP - Build = 10.0.17134 The following settings are user defined boot.wim Image# = 2 - install.wim Image# = 1 - Fallback Language = ja-JP - Method = INJECT Select YES to CONTINUE - or NO to ABORT Yes No

① 以下の画面が表示された場合は、「OK」をクリックします。



1 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。

onfirm	x
$\bigcirc$	FINAL CHECKI You are running the create bootable USB drive option.
$\bullet$	WARNING - ALL PARTITIONS ON THE TARGET DRIVE (DRIVE E:) WILL BE DELETED AND THE DEVICE WILL BE FORMATTED. THIS COULD RESULT IN DATA LOSSI
	Are you sure you want to proceed? Select YES to CONTINUE - or NO to ABORT
	Ver
	165 140



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。

鯅 WinBuilder [082]					-		×
WinBui	lder		Ø	<b>W</b>	•	Hel	P
	Script Register Source Contractions of Log Log Window you In this window you wou save the log and	Play W find messages from the processee working as supposed. In case yo d post the log.html file on the supp	Refresh d files. Logs u run into pr port forums.	Tools are the be- oblems, ot	Downloa st way of s hers may h	d cripts lett elp you b	ting you vetter i
Create USB → Create USB → Create USB (GPT ⊕ → Tools	⊕ Scripts (7) ⊕ Sections (37) ⊕ Processed (613) ⊕ V Processed (215) ⊕ Info (80)	<ul> <li>※ IF - [ram] is not equa</li> <li>◆ [If,ExisFile, *%USB.D.</li> <li>◆ [FileCopy, *%Program:</li> <li>※ [End]</li> <li>※ IF - [ram] is not equa</li> <li>◆ IF.ExisFile, *%USB.D.</li> </ul>	l to: [flat] ev rive%:¥EFI¥ s%¥misc¥UE l to: [both] e rive%:¥EFI¥	valuated st microsoft¥ FI-FLATBo evaluated s microsoft¥	ring: [If,% boot¥BCD" ot-BCD","% tring: [If,% boot¥BCD"	Boot.Met ,FileDele 6USB.Dri 6Boot.Me ,FileDele	te, ve ett
		<ul> <li>● [FieCopy, "94Programs</li> <li>※ [End]</li> <li>✓ [End]</li> <li>■ Run - Processed sectit</li> <li>© Script time: 1 minute,</li> <li>♀ Finished processing sc</li> </ul>	s%¥misc¥UE on [Copy.Ba 54 seconds ; ript: Create	FI-FLATan ck.To.USB] and 173 mi USB	dRAM-BCD in file: [% liseconds	","%USB BaseDir%	.D
		😟 Project time: 2 minute	s, 49 secono	ds and 426	milisecond	s	*
< >		Save as log.html	6	View la	st log		



### 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。

۵.	Disk Mg	ır 0.9 - erwan22	212@gmail.o	com 🗖 🗖 🔀	4
#	Туре	Name	Size (MB)	Attributes	
0	DISK	VMware Virtu	61440	Offline Read-Only	
	Offline	Online	Read-On	br Read-Write	
	O Mille		itead on	iy need inte	

④ Windows FE が起動し、以下のような画面が表示されます。

<b>Windows</b> Forensic Environment (WinFE)	
l≹	10011101 010011001111 11101001100100 0011001100100
alpha •••	010100110011 0111010010010 100110011010100 101010011001100 1111010011001100 10011001110 10011001110 100110011110 100110011110 100110011011

- 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。

Disk Mgr 0.9 - erwan2212@gmail.com _ X					
#	Туре	Name	Size (MB)	Attributes	
0	DICK	Addition Adults	61440	Office Read-Oaly	
1	DISK	Silicon-Powe	59104	Offline Read-Only	-
				N	€.
	Offline	Online	Read-On	ly Read-Write	

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。

Disk Mgr 0.9 - erwan2212@gmail.com 🗕 🗙					
#	Туре	Name	Size (MB)	Attributes	7
0	DISK	Williamo Virtu	61440	Offling Road-Oply	
1	DISK	Silicon-Powe	59104	Offline Read-Write	
					-
Offline Online Fad-Only Read-Write					
IOCTL_DISK_SET_DISK_ATTRIBUTES WRITE OK					

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。

DiskMgr	×
WARNING - You are about to mount every volume on disk 1. If the disk is NOT Read-Only, it will NOT be write protected. Continue?	
(‡6)(Y) (13 (N)	

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。

Disk Mgr 0.9 - erwan2212@gmail.com 🗕 🗙					
#	Туре	Name	Size (MB)	Attributes	]
0	DISK	VAdmoro Virtu	61440	Offling Rood-Oply	
1	DISK	Silicon-Powe	59104	Online Read-Write	
Offline Online Read-Only Read-Write				1	
2018/09/23 12:23:38 : device inserted C:					

#### (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。

- In 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。

•		Q-Dir 6.49.7		- 0	×
File Edit View Favorites	Extras Info 🛛 🖽 🕇			🗆 🛛 📩 PC 💦 🔫 🛃 📌 🕅 🥨 (	_
🔀 🖪 🔯 🔜 🗙	G O 🤌 🖻 🖽 💋	💻 PC		✓	Ŧ
☆ お気に入り からし、からし、 からし、 からし、<	名前 フォルダー (1)	種類	合計サイズ	空き領域	•
SYSTEM	3D Objects デバイスとドライブ (3)	システム フォルダー		·	•
●	<ul> <li>64GBUSB (C:)</li> <li>Boot (X:)</li> </ul>	USB ドライブ ローカル ディスク	57.7 GB 512 MB	56.8 GB 510 MB	
	∑ 4 Objects ▼			🧉 ኛ 📼 🗙   👗 🛅   🔏 🛽	
4 Objects	🕔 SYSTEM (Po	ortable/x64) 📃 PC		1181	



## 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。

Menu	]
File Manager	
LaunchBar	FORENSIC TOOLS
FORENSIC TOOLS .	XWays Forensics
Command Prompt	README 😽 🥄
Run	DiskMgr
System 🕨	
Shutdown +	

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