初めての「FTK Imager」

2015年2月8日

セクタンラボ

FTK Imagerについて

- FTK Imagerは，Windows上で動作する簡易フォレンジックツールです。
- ディスクイメージ作成，メモリ取得，ファイル取得など，ライブレスポンスにおけるエビデンス取得機能を有しています。
  - ディスクを直接解析しているため，アクセス権やファイルロックの影響を受けることなく，全てのフォルダ・ファイルにアクセスできます。
  - 調査対象ディスクの内容を書き換える機能を有していないため，ライブレスポンスで利用した場合に，証拠の改変を最小限に抑えることができます。

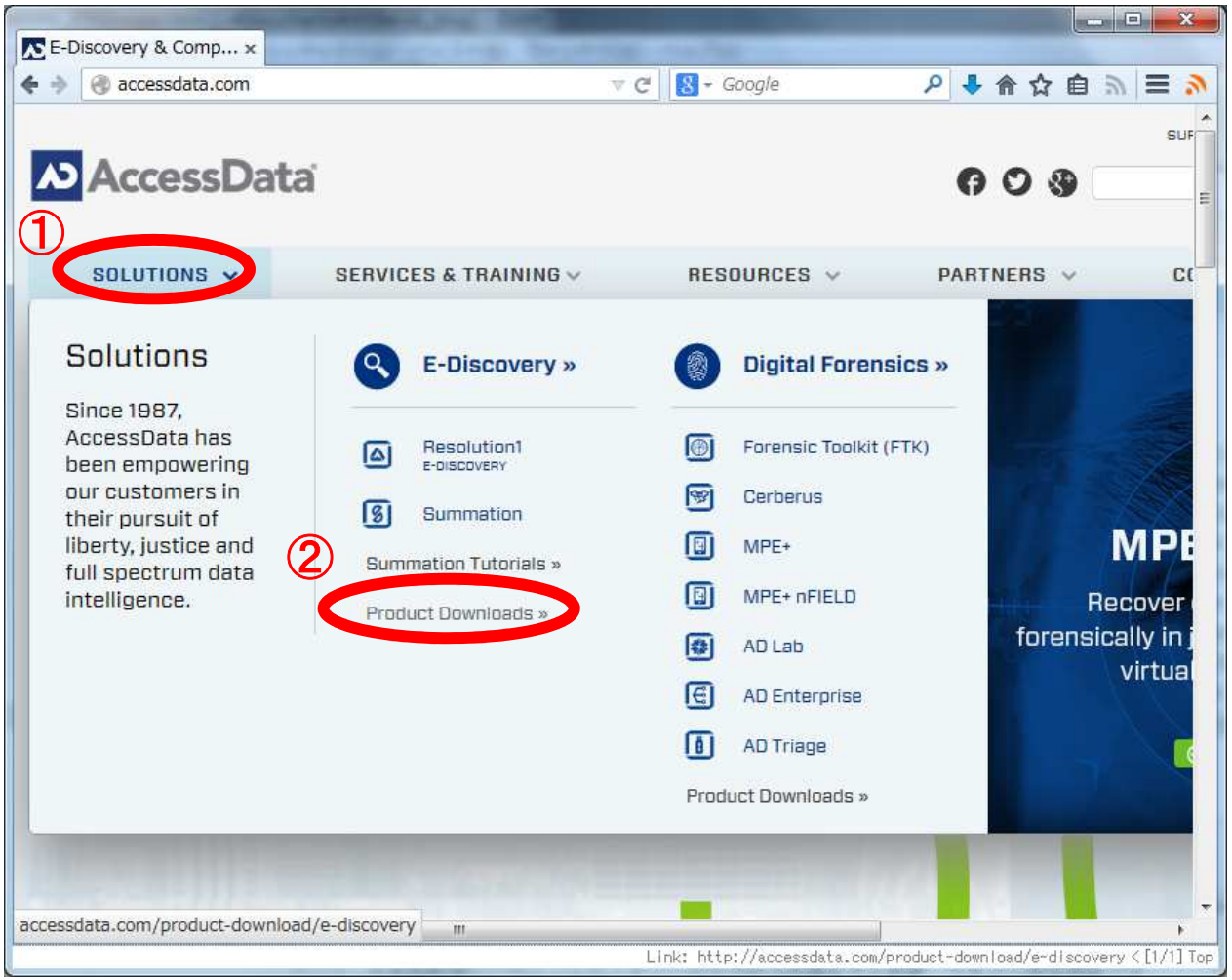
- また，取得したディスクイメージなどを簡易閲覧することもできます。

- 本資料では，FTK Imager Lite版を利用してエビデンスを取得するための操作方法を記載します。

ダウンロードとインストール

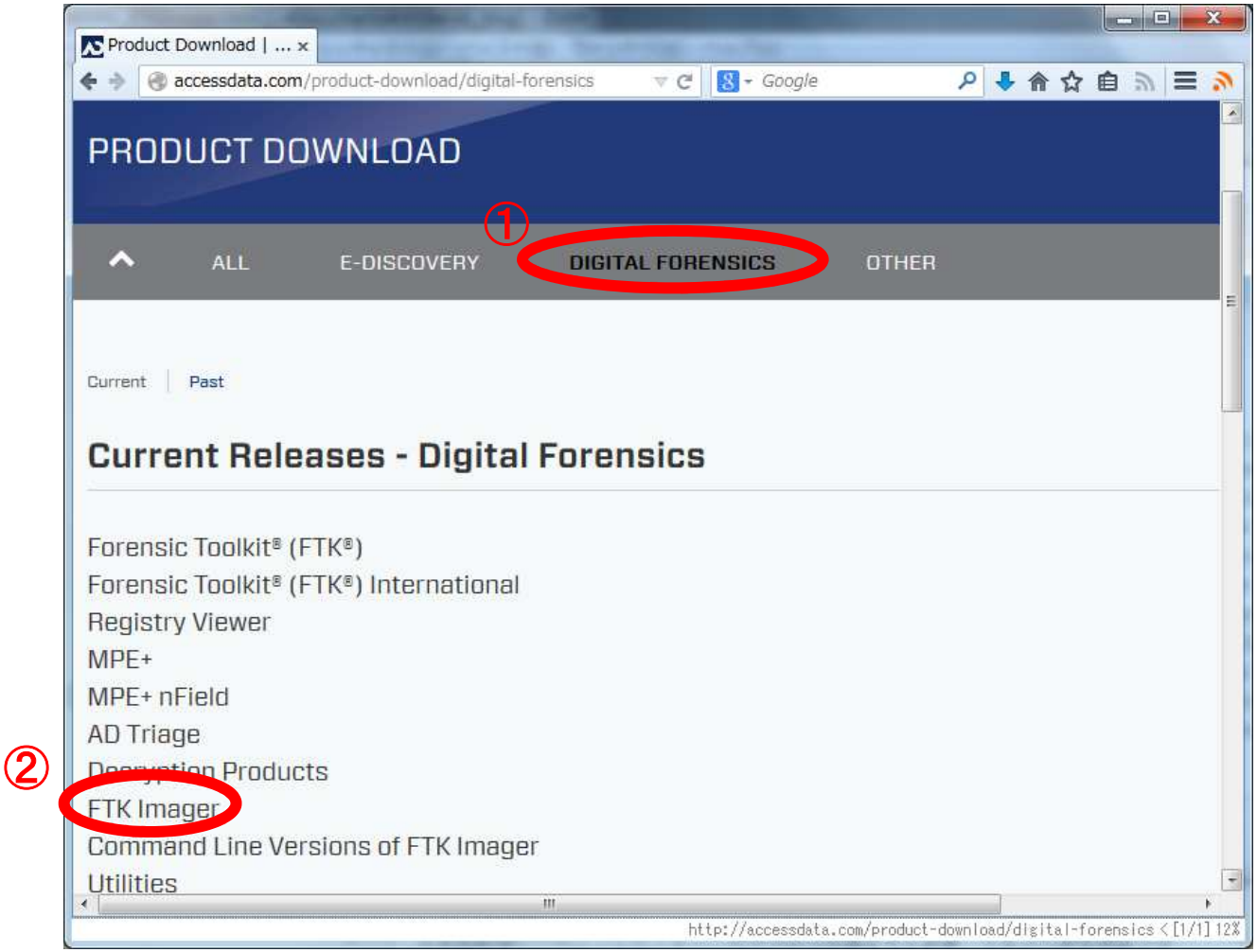
ダウンロード（1）

- **AccessData社のWEBサイト（http://accessdata.com/）にアクセスし，上部メニュー「SOLUTIONS」-「Product Downloads」をクリック**



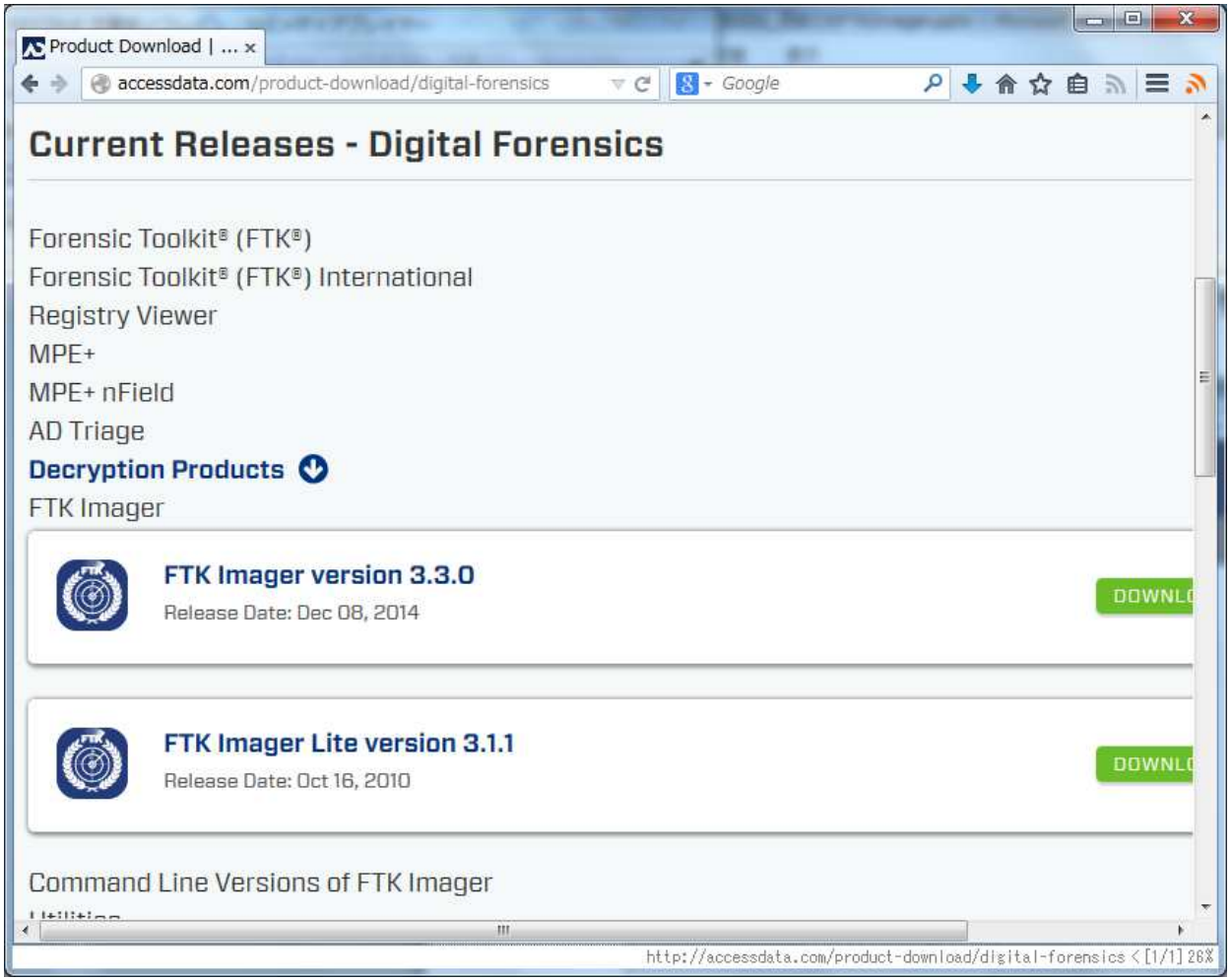
ダウンロード（2）

- [DIGITAL FORENSICS]をクリックし，フォレンジック製品一覧の中から「FTK Imager」をクリック



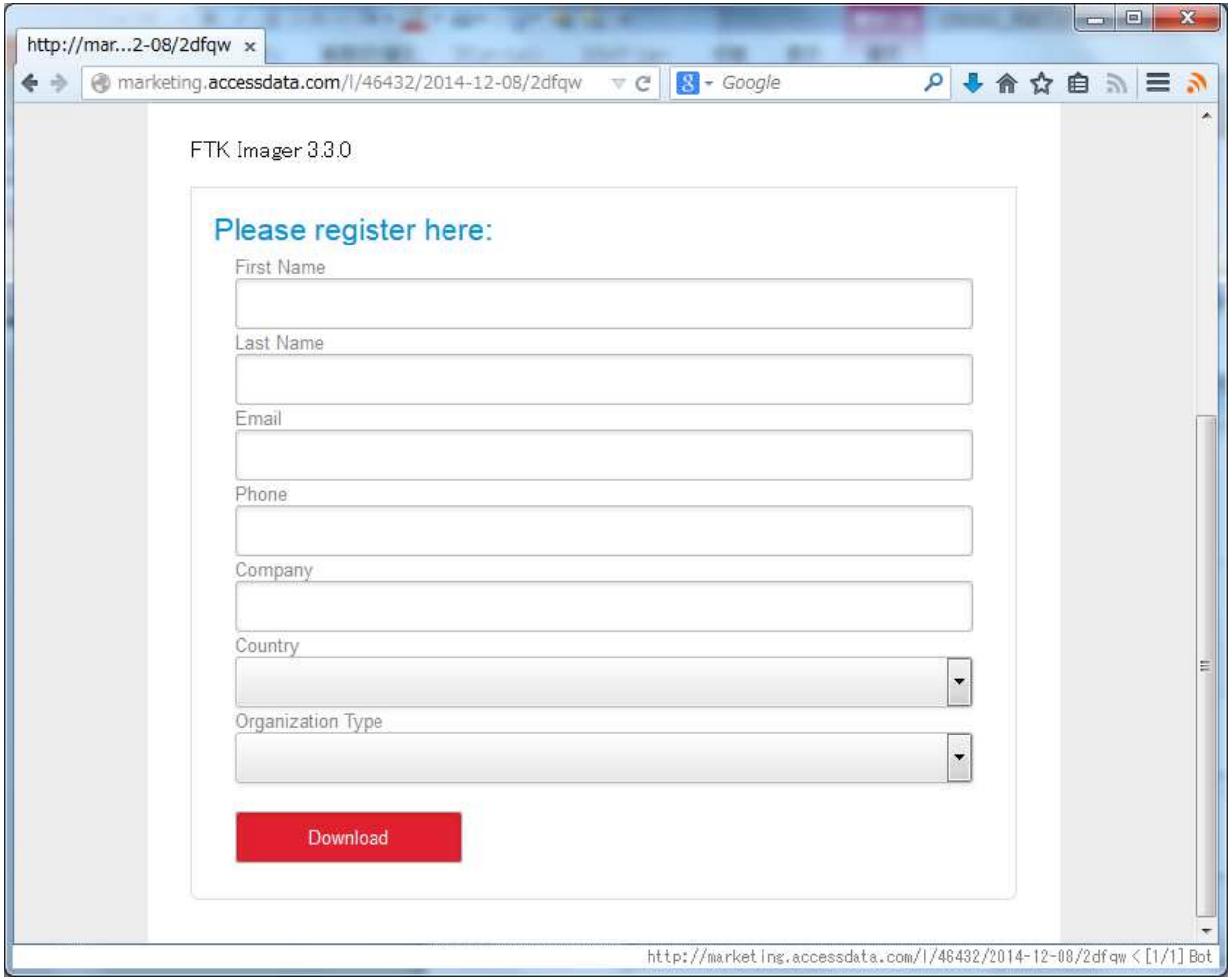
ダウンロード（3）

- 2種類あるので，好きなほうをダウンロードします。Lite版はインストール不要でUSBメモリなどから利用できます。（機能は通常版とほぼ同じ）



ダウンロード（4）

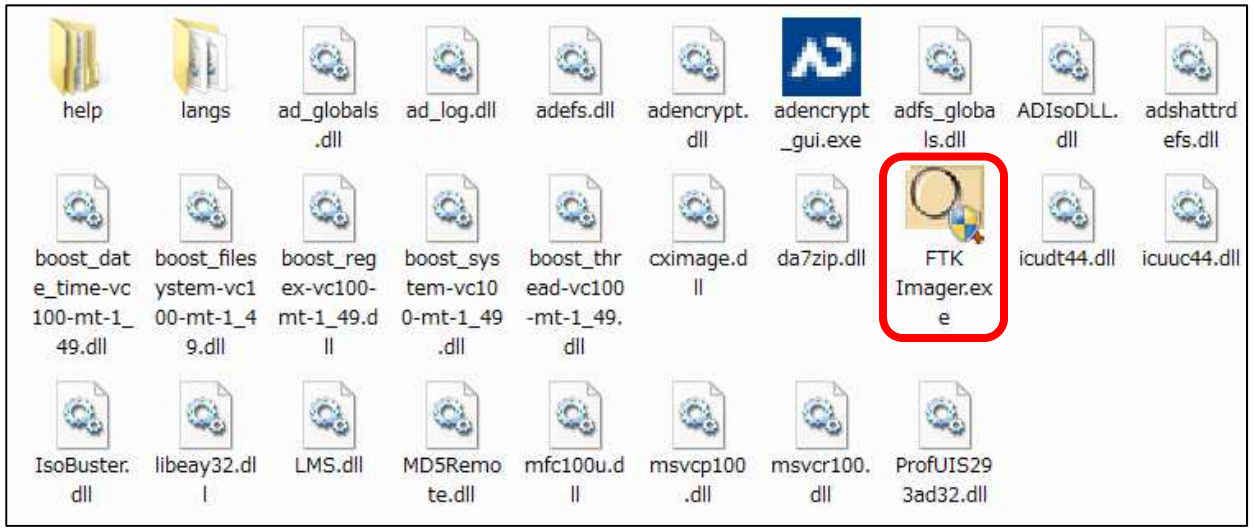
- ダウンロードするために，氏名，メールアドレス，電話番号などを入力します。
- 登録したメールアドレスには，AccessData社からたまにDMが届きます。



インストール

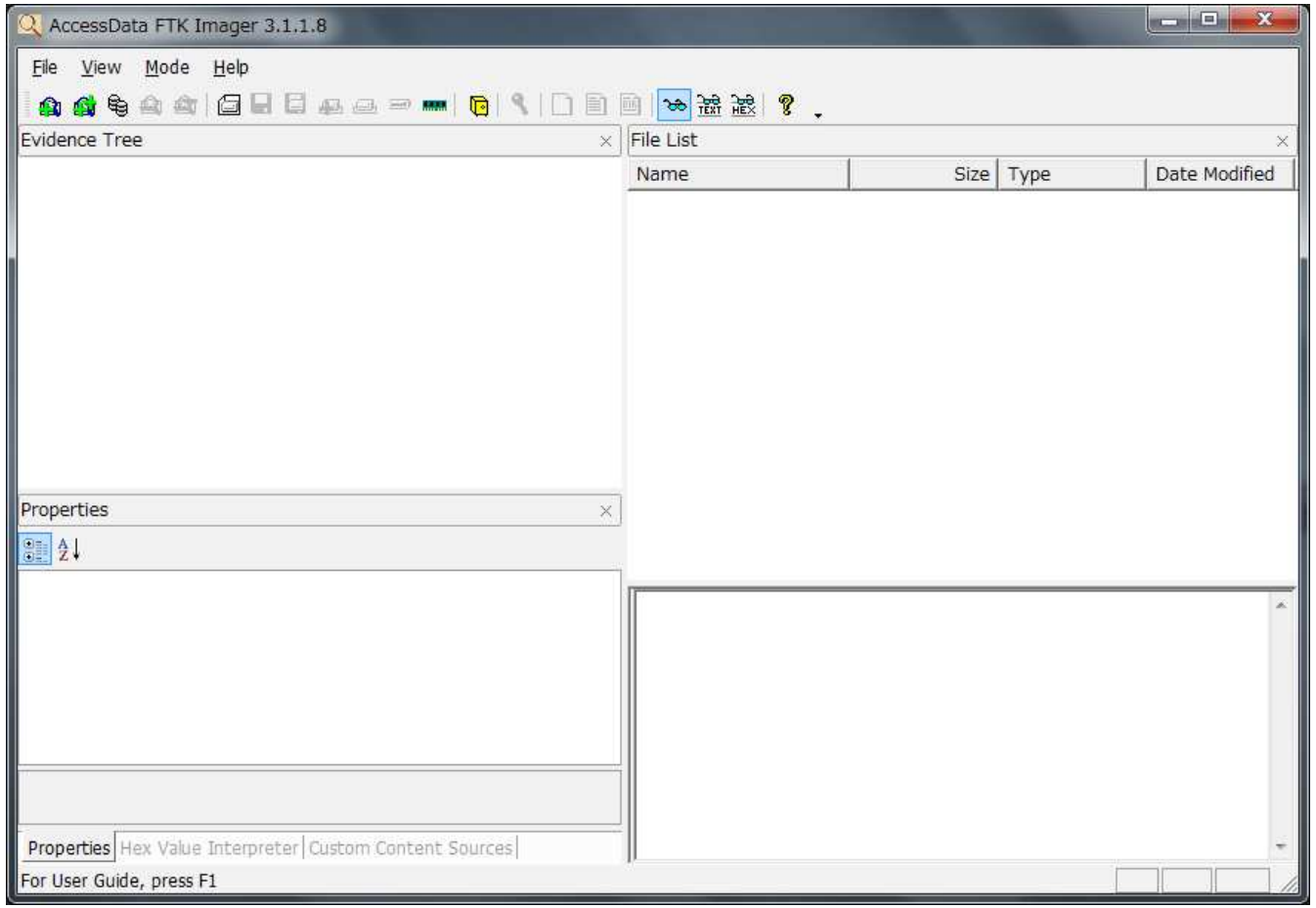
- 通常版は，インストーラーの指示どおりにクリックするだけで，難しいことは何もないので割愛します。
- Lite版は，ZIPファイルを任意の場所に展開するだけです。
  - この資料では，Lite版の利用を前提として操作方法を説明します。

Lite版のZIPファイルに格納されているファイル



起動

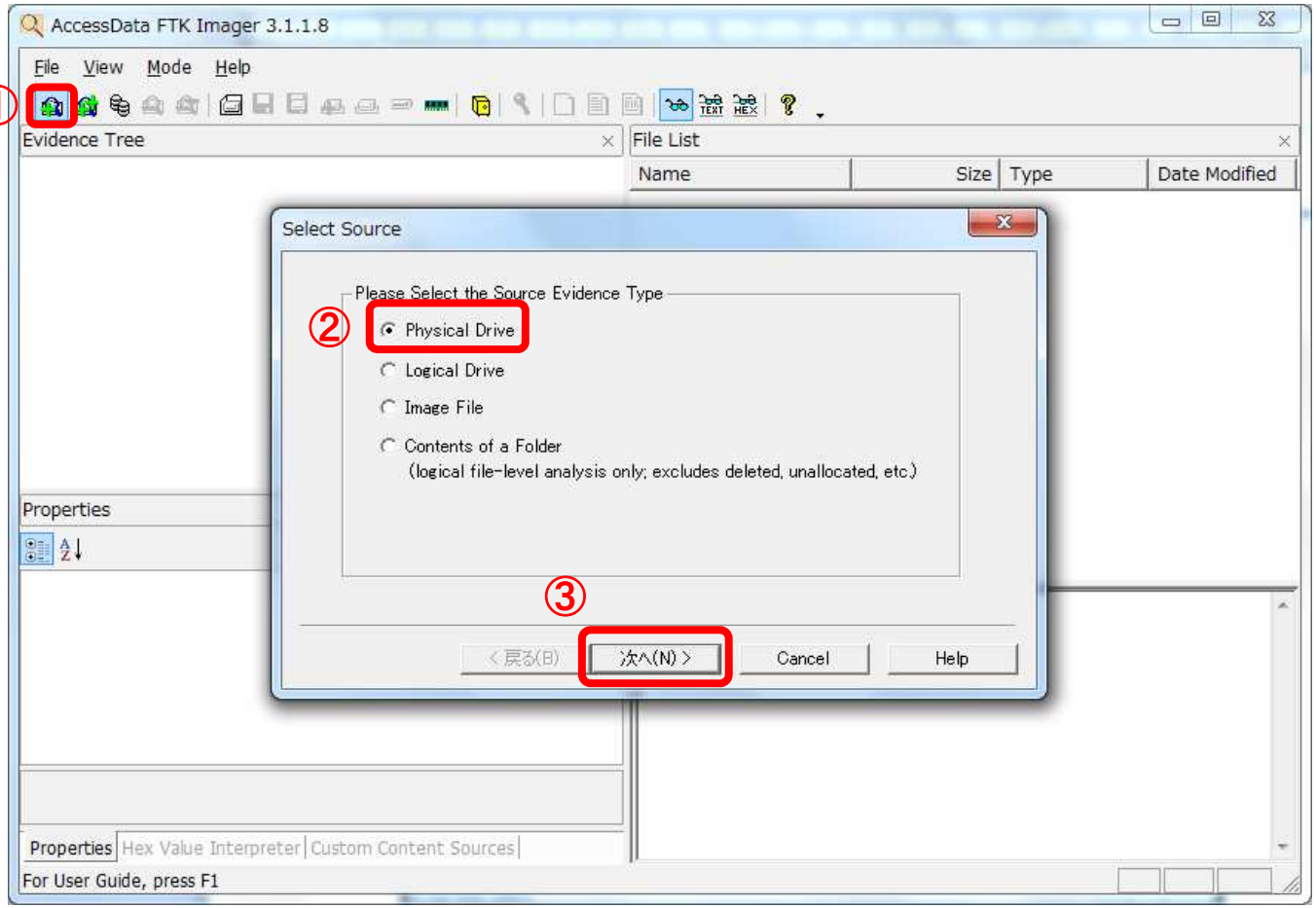
- 「FTK Imager.exe」を実行します。
- なお，起動には管理者権限が必要となります。



エビデンスの追加

調査対象ハードディスクの閲覧

- ツールバーから「Add Evidence Item」をクリック
- 「Select Source」ダイアログで「Physical Drive」を選択した状態で「次へ」をクリック

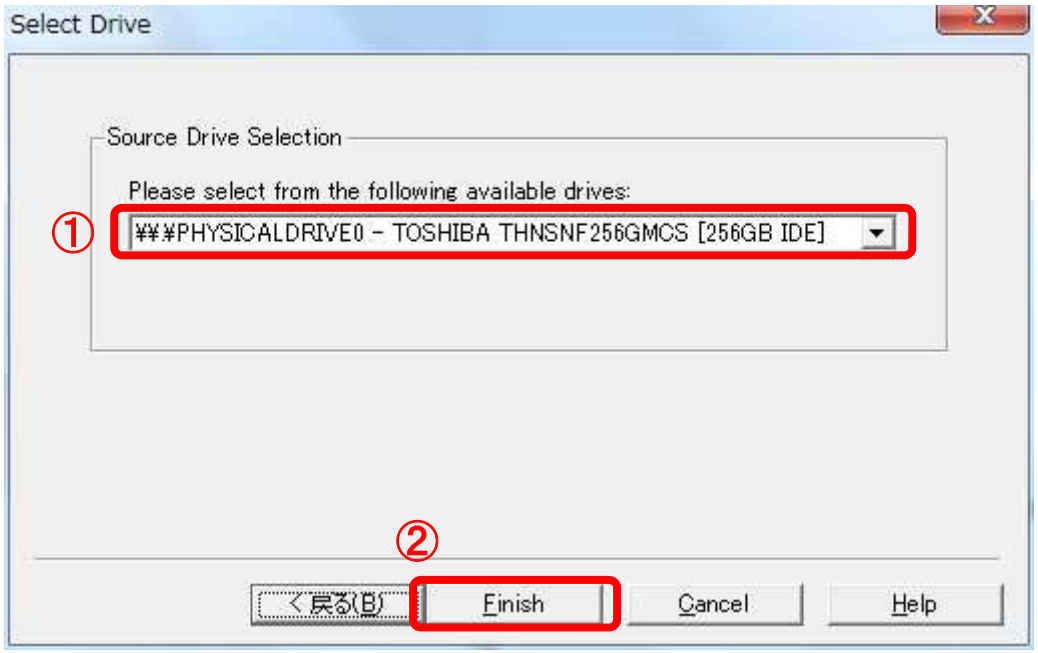


（補足）「Select Source」ダイアログ

選択肢	説明
Physical Drive	• 物理的なディスクを選択します。 • 未割当領域，削除済領域も含めて，ディスクの全領域を調査できます。
Logical Drive	• 論理ドライブ（例：Cドライブ）を選択します。 • 選択したパーティションのみ調査できます。
Image File	• イメージファイルを選択します。
Contents of a Folder	• 特定のフォルダを選択します。 • 未割当領域，削除済領域などは調査できません。

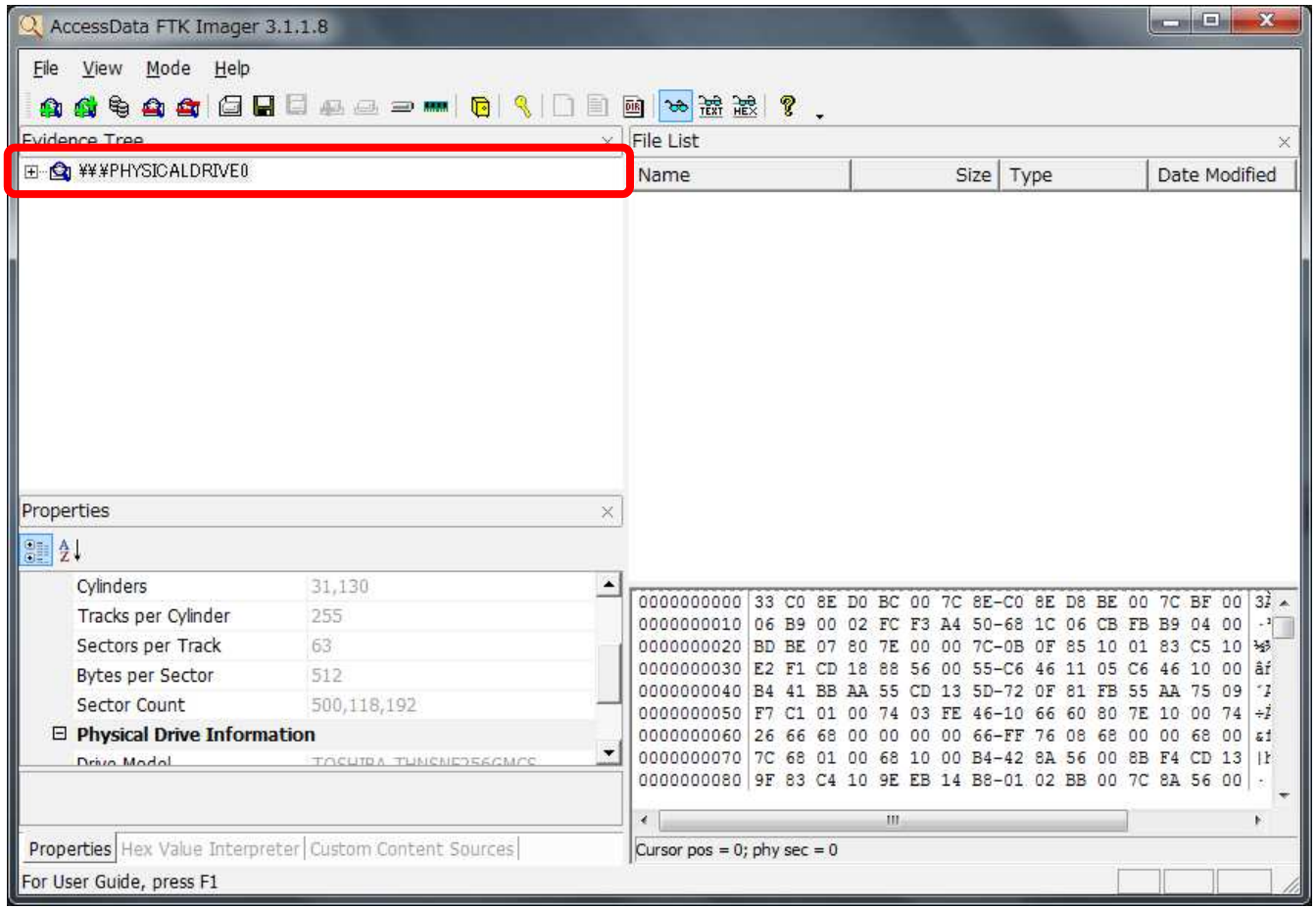
ドライブの選択

- 「Select Drive」ダイアログで，調査対象ディスクを選択し，「Finish」をクリック
  - ドロップダウンリストには，パソコンに接続されている全てのストレージが表示されます。（USBメモリも表示されます）
  - メーカー名，型番，容量などを参考に，調査したいディスクを選択します。



エビデンスツリー

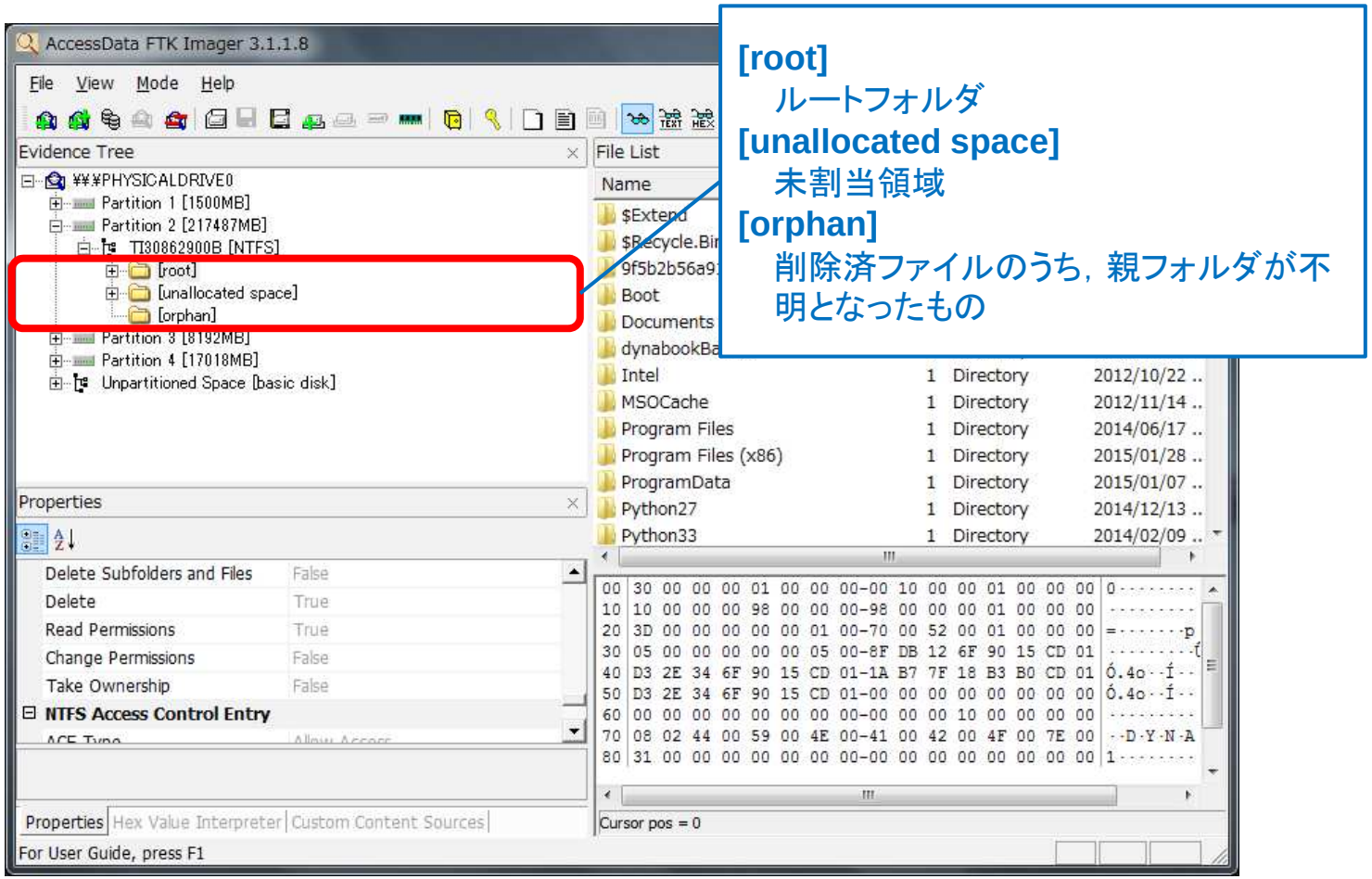
- 「Evidence Tree」に，ディスクが追加されました。
- 同様の操作で，複数のディスクやディスクイメージをエビデンスツリーに追加できます。



エビデンスの閲覧

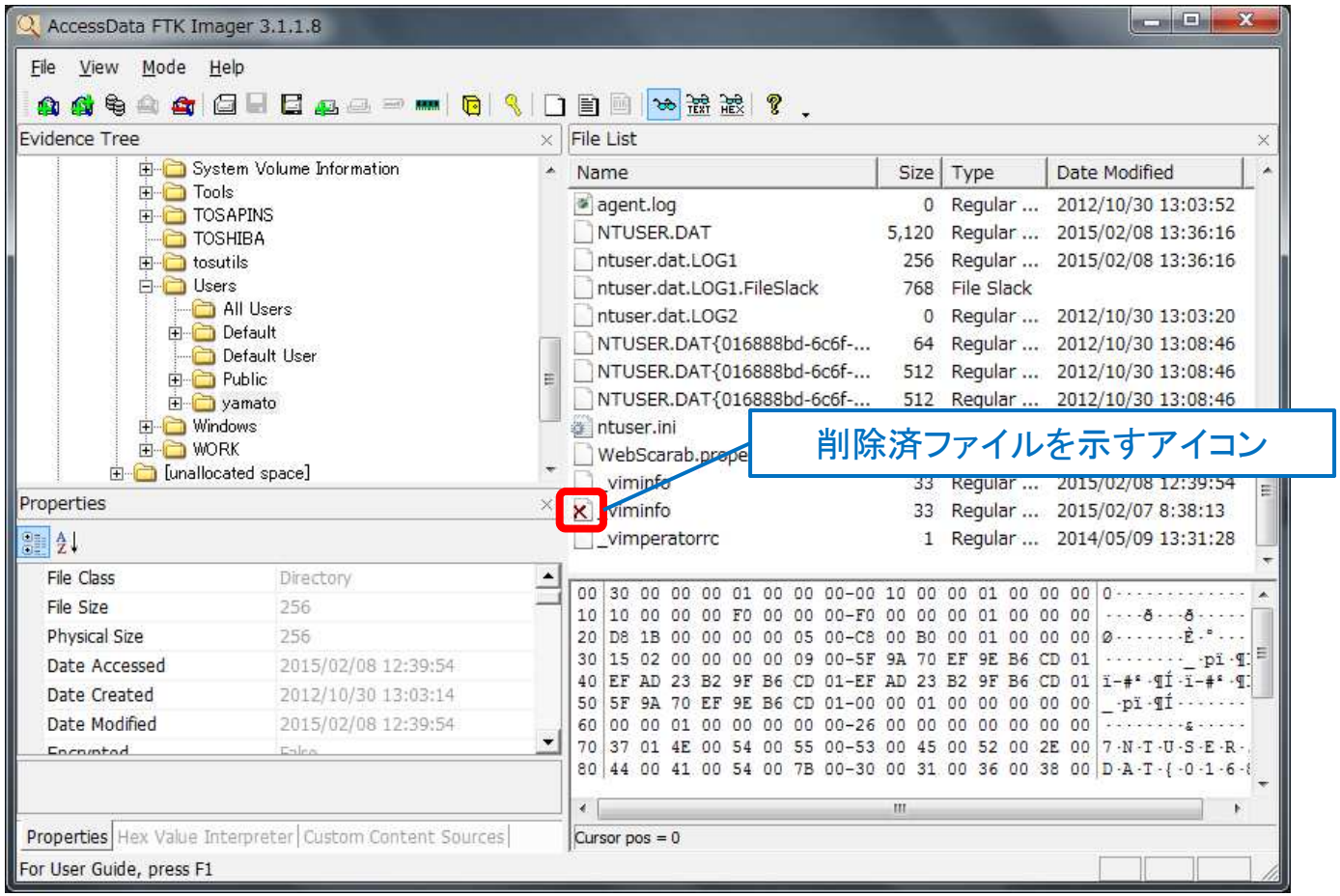
エビデンスツリーの展開

- 「Evidence Tree」のディスクを展開していくと，各パーティションに格納されているフォルダなどが表示されます。



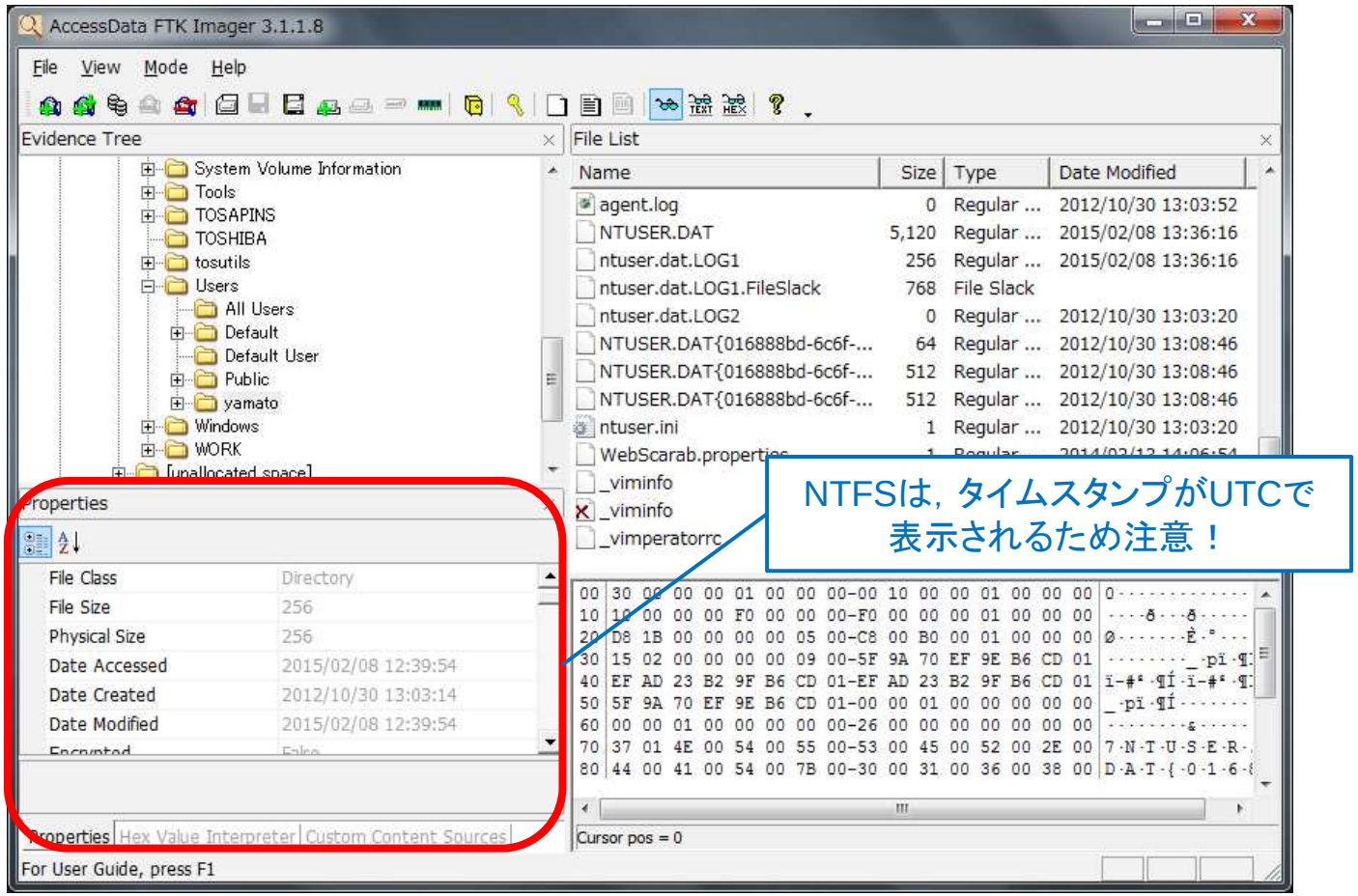
フォルダ・ファイルの閲覧

- FTK Imagerは，OSを介さずにファイルシステムを直接解析するため，Windowsのアクセス権などの影響を受けずに，全てのフォルダ・ファイルにアクセスできます。
- また，削除済フォルダ・ファイルも表示できます。



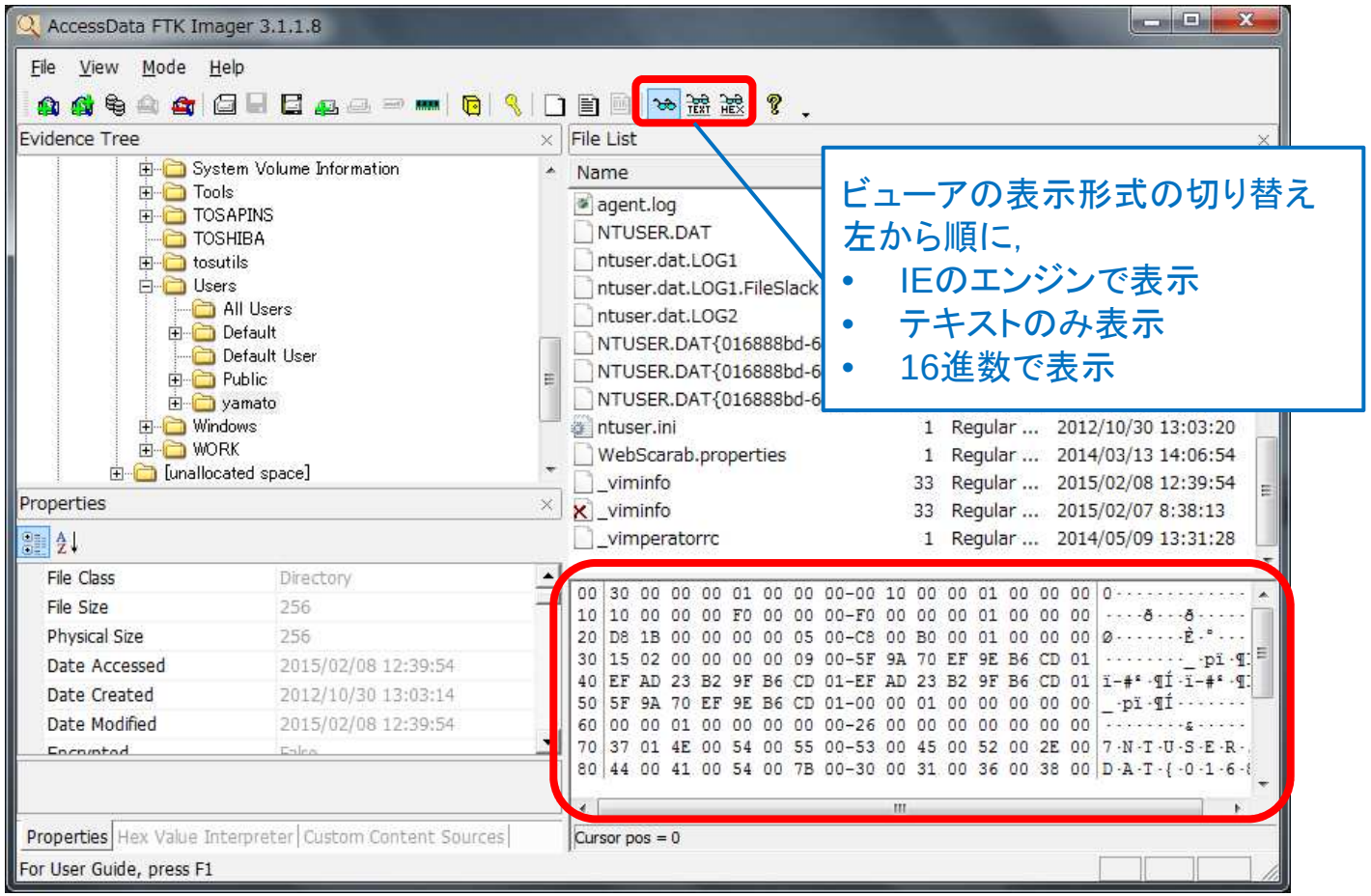
プロパティペイン

- プロパティペインには，選択したファイルのタイムスタンプなどの詳細情報が表示されます。なお，NTFSのタイムスタンプは，UTC（協定世界時）で表示されます。日本時間に換算するには，+9時間して読み取ってください。（FATは日本時間で表示されます。）



ビューアーペイン

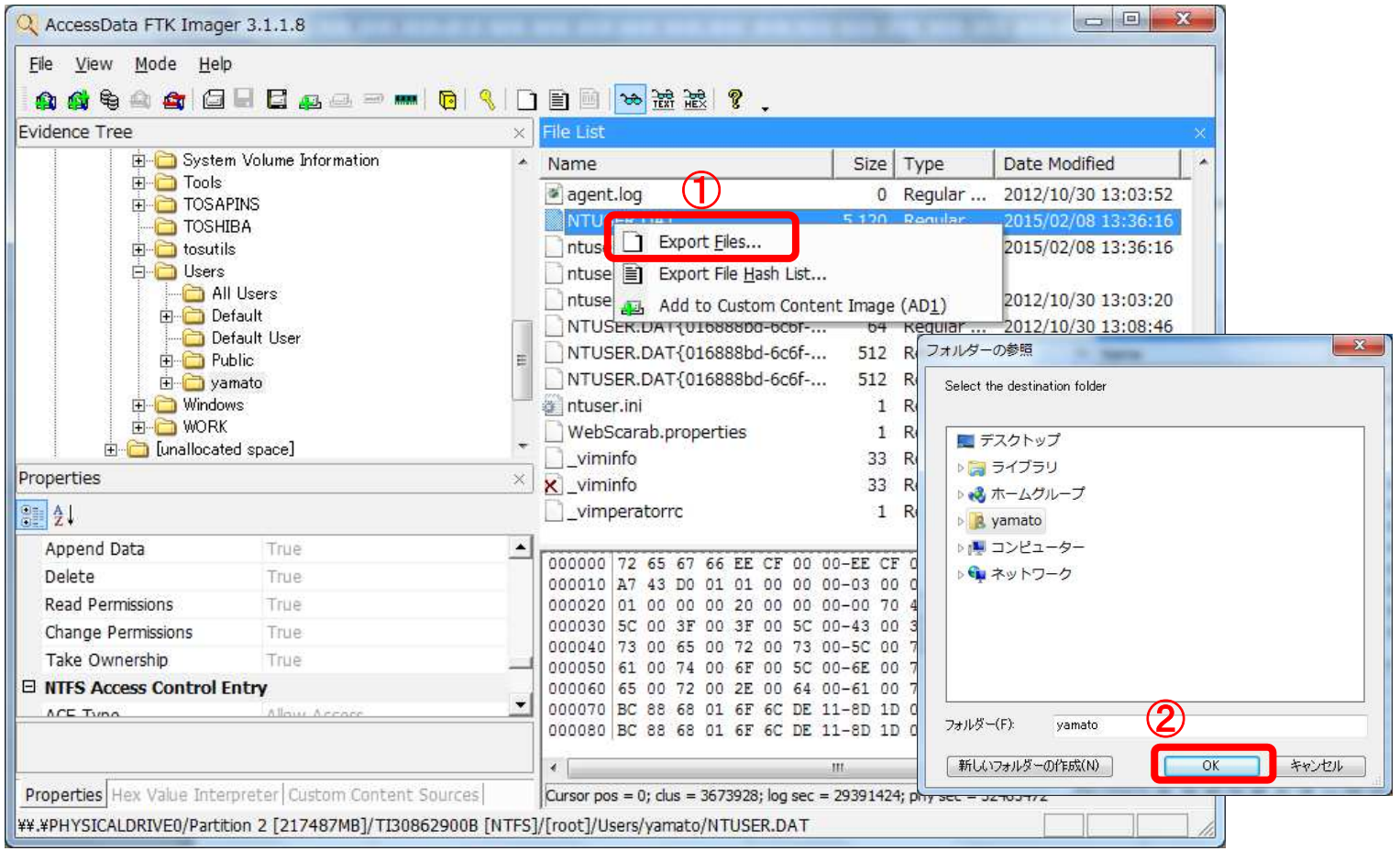
- 選択したファイルの内容を閲覧できます。



フォルダ・ファイルの抽出

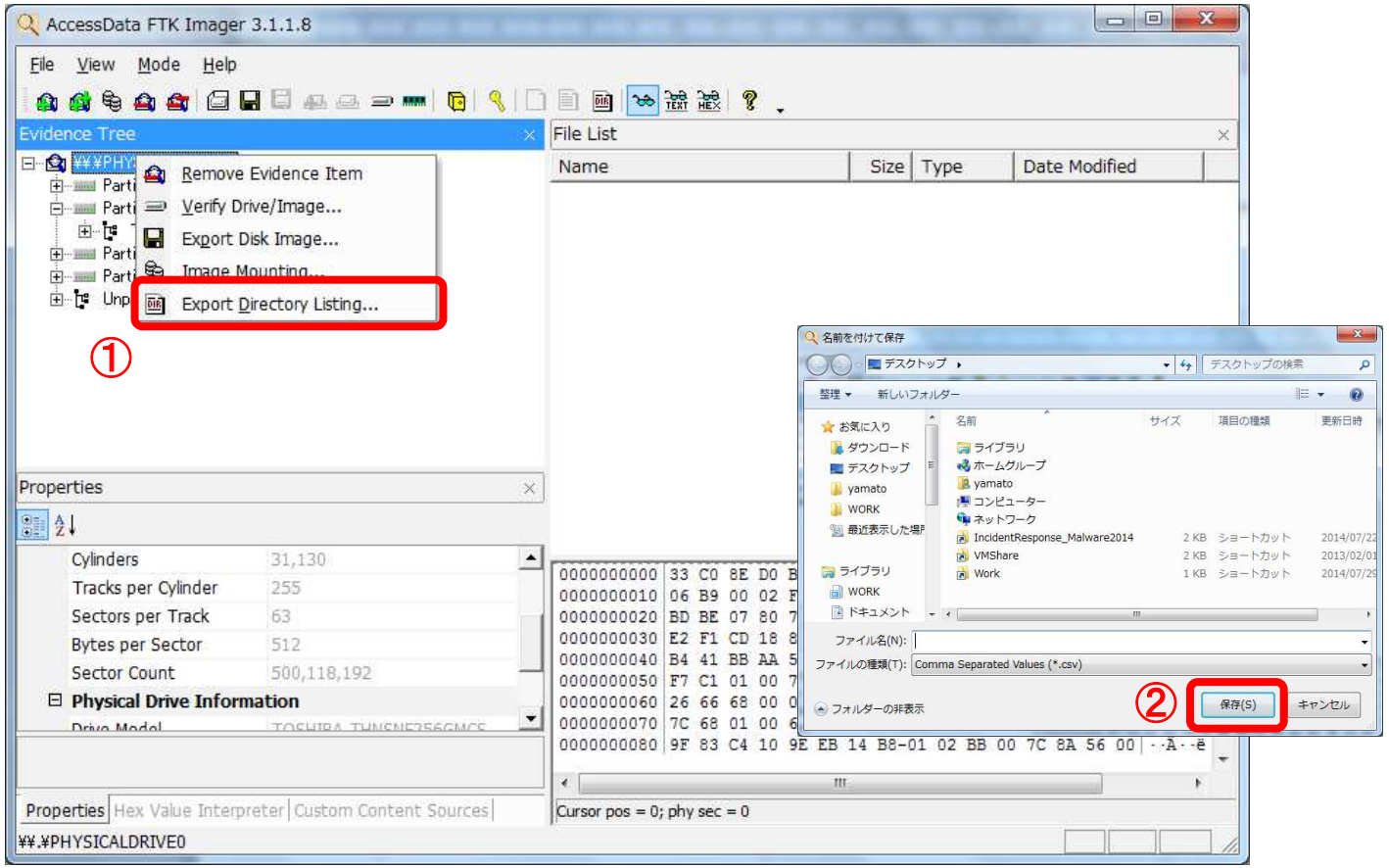
フォルダ・ファイルのエクスポート

- 次の操作により，任意のフォルダ・ファイルを抽出して保存できます。
  - 取得したいフォルダ・ファイルを右クリックし，「Export Files…」をクリック
  - 保存するフォルダを指定して「OK」をクリック



ファイルリストの作成

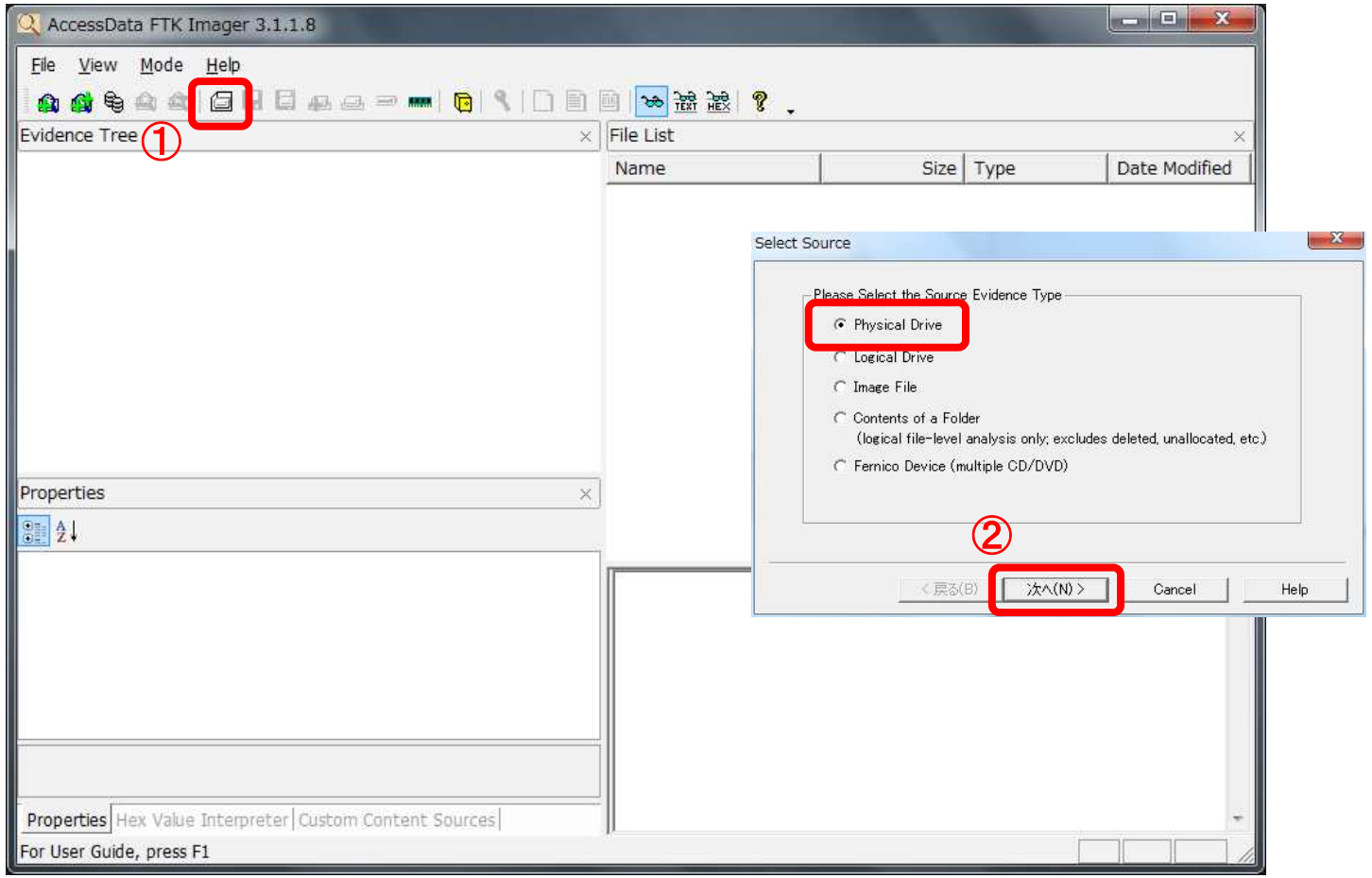
- 次の操作により，ファイルリストをCSV形式で作成できます。
  - 「Evidence Tree」のディスク，またはパーティションを右クリックし，「Export Directory Listing…」をクリック
  - ファイルリストの保存先を選択し「保存」をクリック



ディスクイメージの作成

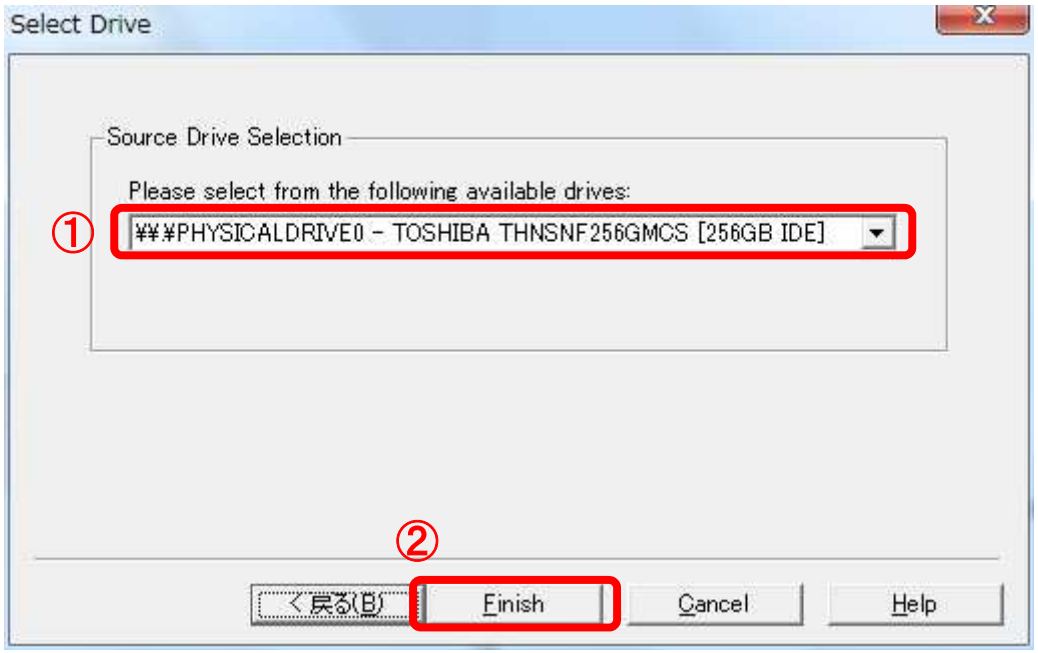
ディスクイメージの作成

- ツールバーから「Create Disk Image」をクリック
- 「Select Source」ダイアログで「Physical Drive」を選択し，「次へ」をクリック



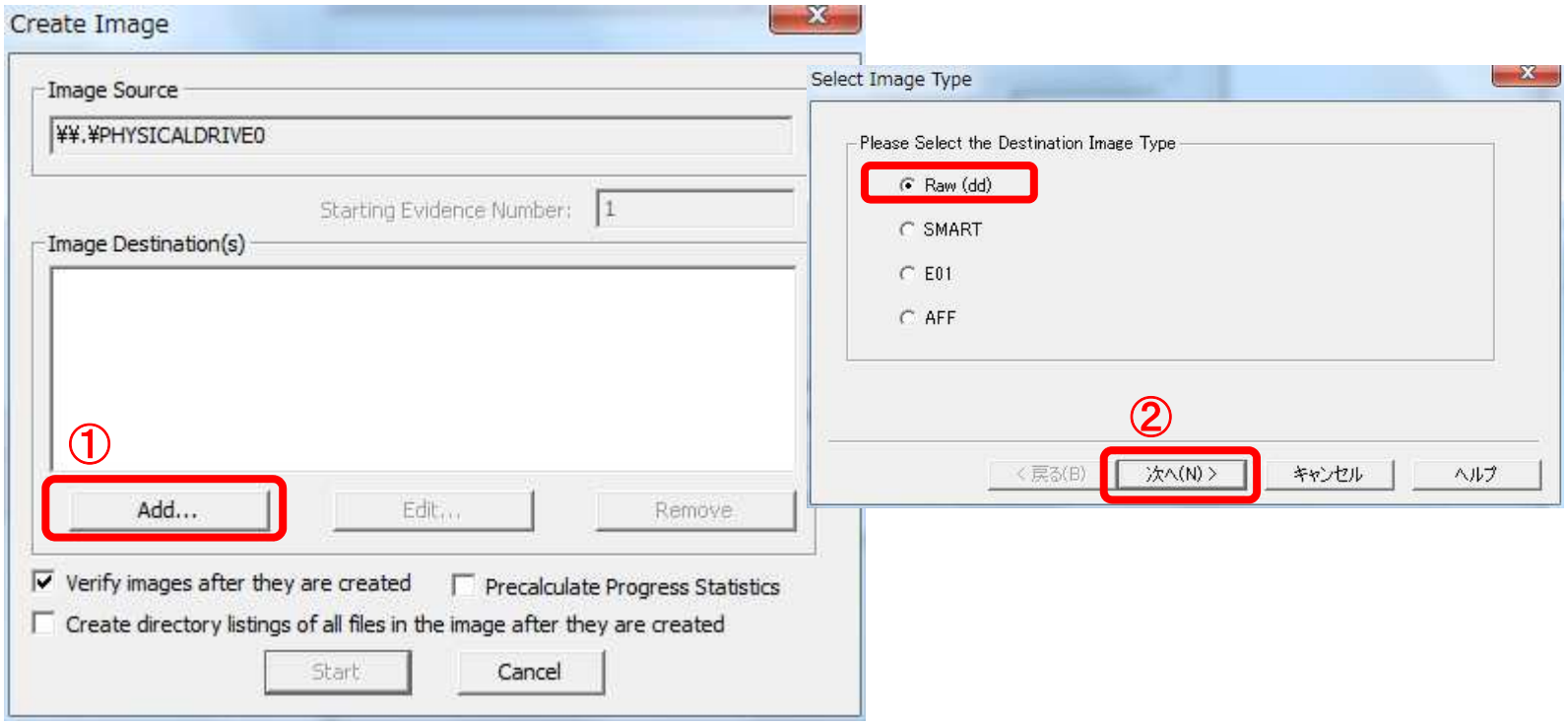
ドライブの選択

- 「Select Drive」ダイアログで，調査対象ディスクを選択し，「Finish」をクリック
  - ドロップダウンリストには，パソコンに接続されている全てのストレージが表示されます。（USBメモリも表示されます）
  - メーカー名，型番，容量などを参考に，ディスクを選択します。



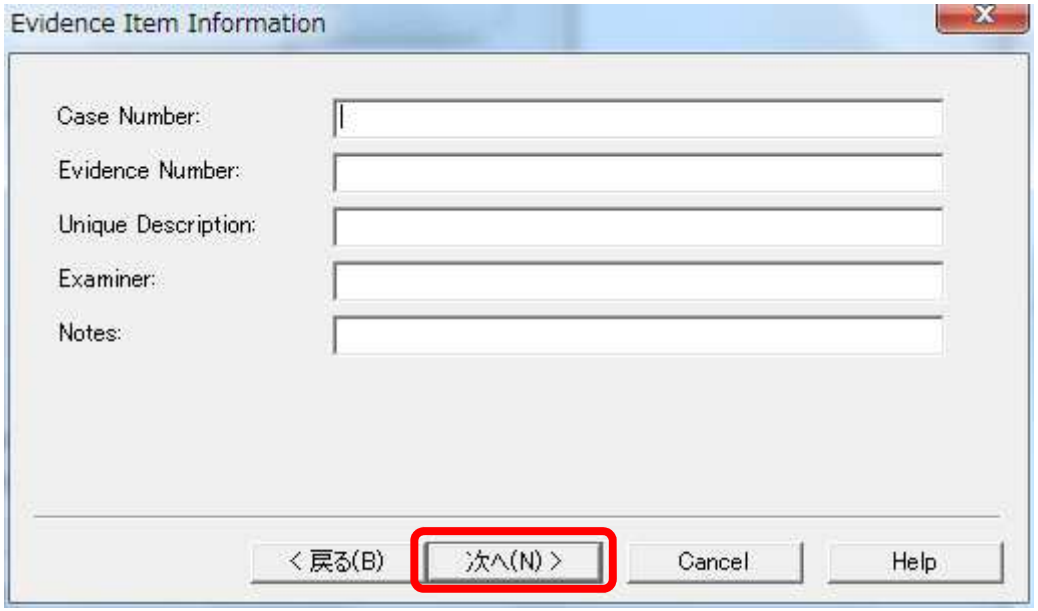
ディスクイメージ形式の指定

- 「Create Image」ダイアログで「Add…」をクリック
- 「Select Image Type」ダイアログで「Raw(dd)」を選択し「次へ」をクリック



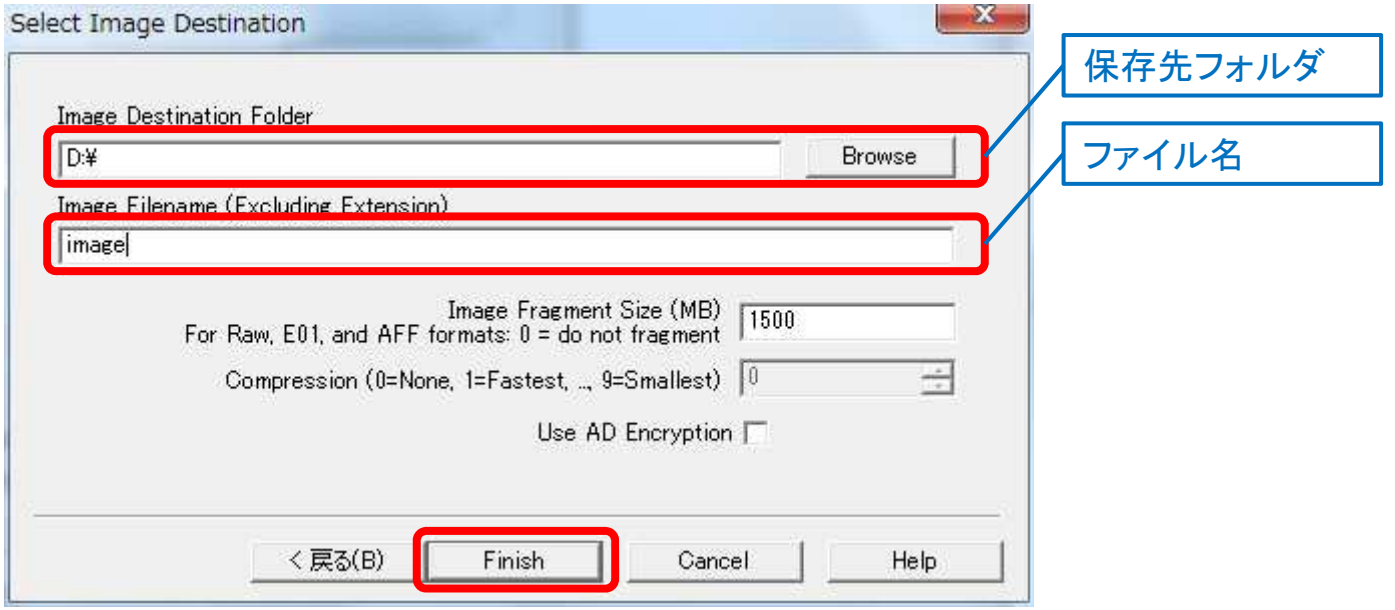
事案情報の入力

- 「Evidence Item Information」ダイアログに，任意の情報を入力して，「次へ」をクリック
  - ここで入力した情報が，ディスクイメージのログファイルに記録されます。
  - 何も入力しなくとも問題ありません。



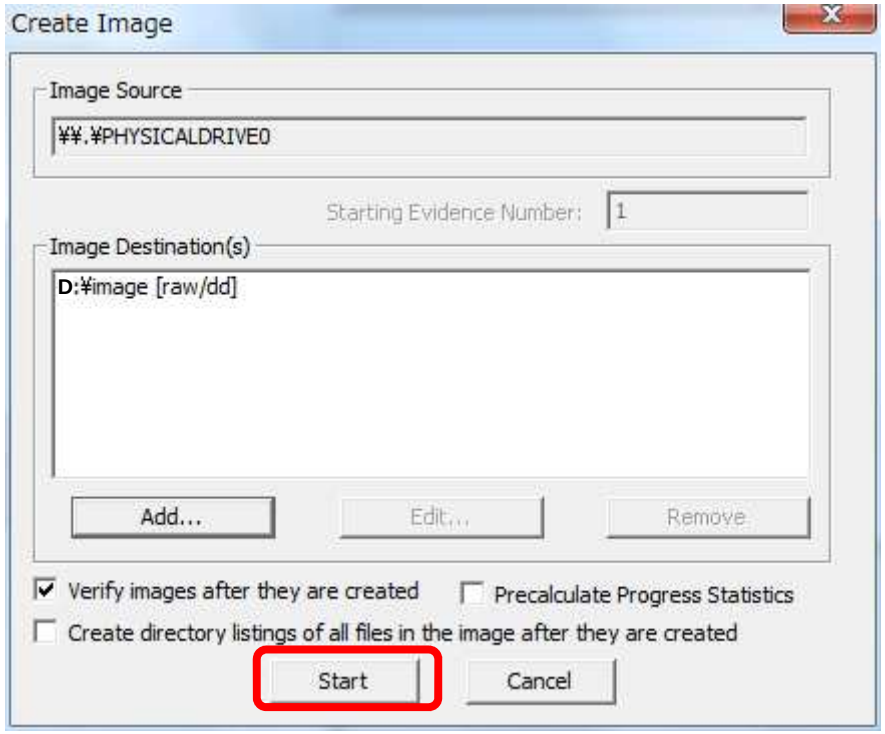
保存先の指定

- 保存先フォルダ，ファイル名，およびファイル分割サイズを指定し，「Finish」をクリック
  - デフォルトでは，1.5GBごとにファイルが分割されます。
  - 分割されたファイルは，拡張子として数字の連番が付定されます。



ディスクイメージ作成の開始

- 「Start」ボタンをクリック
- 容量の大きなディスクイメージの作成は，かなり時間がかかるので気長に待ちます。
- 作成したディスクイメージは，前述「エビデンスの追加」手順で閲覧できます。



メモリイメージの作成

メモリイメージの作成

- ツールバーから「Capture Memory」をクリック
- 「Memory Capture」ダイアログで保存先フォルダ，ファイル名を入力して「Capture Memory」をクリック