exterro®
Data Risk Management

FTK IMAGER PRO

FEATURE GUIDE

Table of Contents

FTK Imager Pro - Features

Introducing FTK Imager Pro

FTK Imager is a powerful data preview and imaging tool used to acquire electronic evidence in a forensically sound manner. It allows users to create bit-for-bit copies of data without altering the original evidence.

FTK Imager Pro enhances this capability by supporting the decryption of various file systems and encrypted volumes. When an encrypted volume is detected, FTK Imager Pro prompts the user to provide the necessary password or recovery key to decrypt it. If the credentials are not available, it still allows the creation of a forensically sound copy of the encrypted data, but the data remains inaccessible.

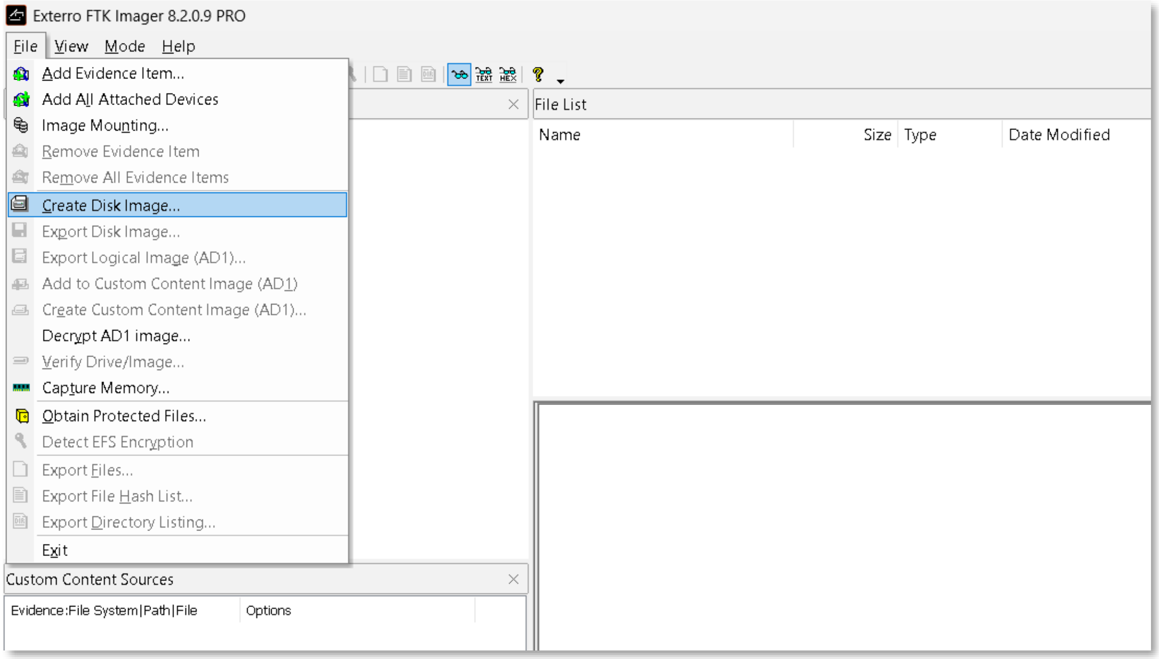
The supported iOS versions are from 13 to 26.

Prerequisites for FTK Imager Pro

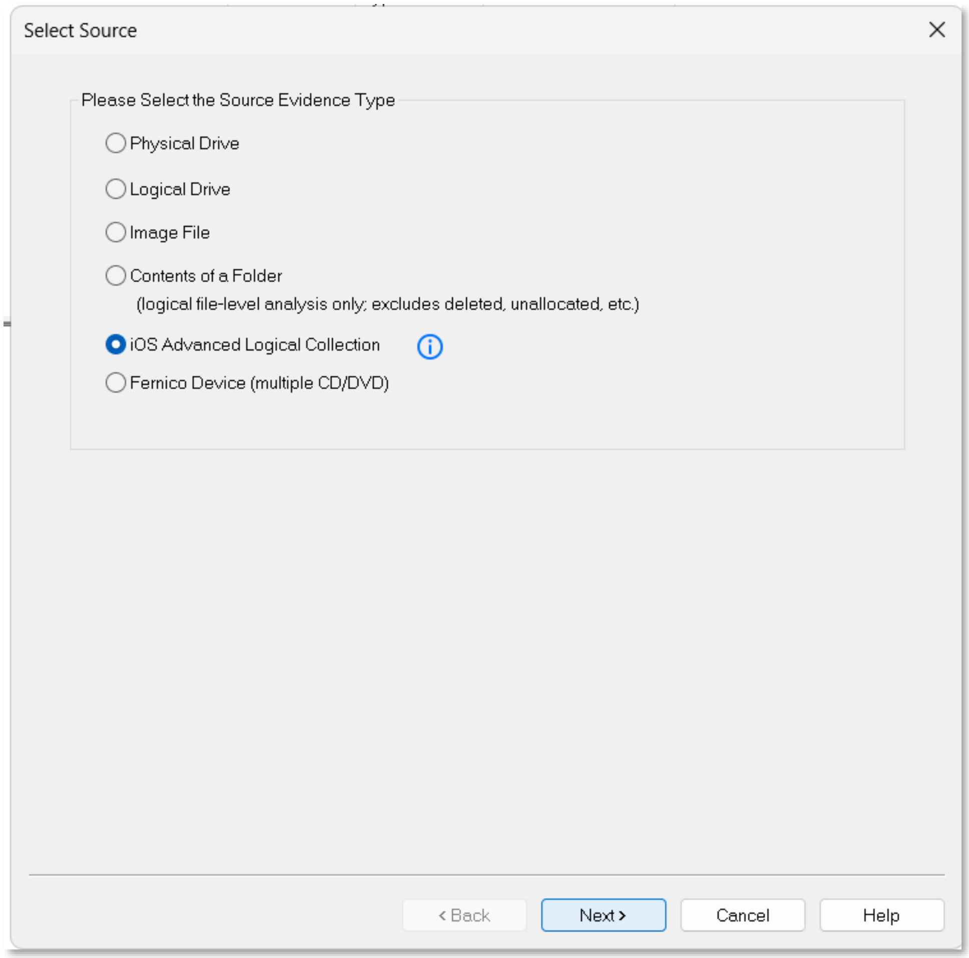
- **iTunes dependencies**: FTK Imager Pro installs iTunes dependencies automatically. It is recommended not to remove them.
- **Passcode**: A passcode for the iPhone is required to perform Collection.
- **Passcode attempts**: FTK Imager Pro may ask for the passcode up to 3 times to:
    - Remove the preset iTunes password
    - Set the iTunes password to "1234"
    - Initiate data collection
- **Cable**: Required to connect the iPhone to the FTK Imager Pro machine.

Steps to Extract Data from iPhone Using FTK Imager Pro

1. Open the **FTK Imager Pro** application.
2. Click on the **Create Disk Image Icon** or navigate to **File** > **Create Disk Image**.



- The **Select Source** pop-up is displayed.



Select Source

Please Select the Source Evidence Type

○ Physical Drive

○ Logical Drive

○ Image File

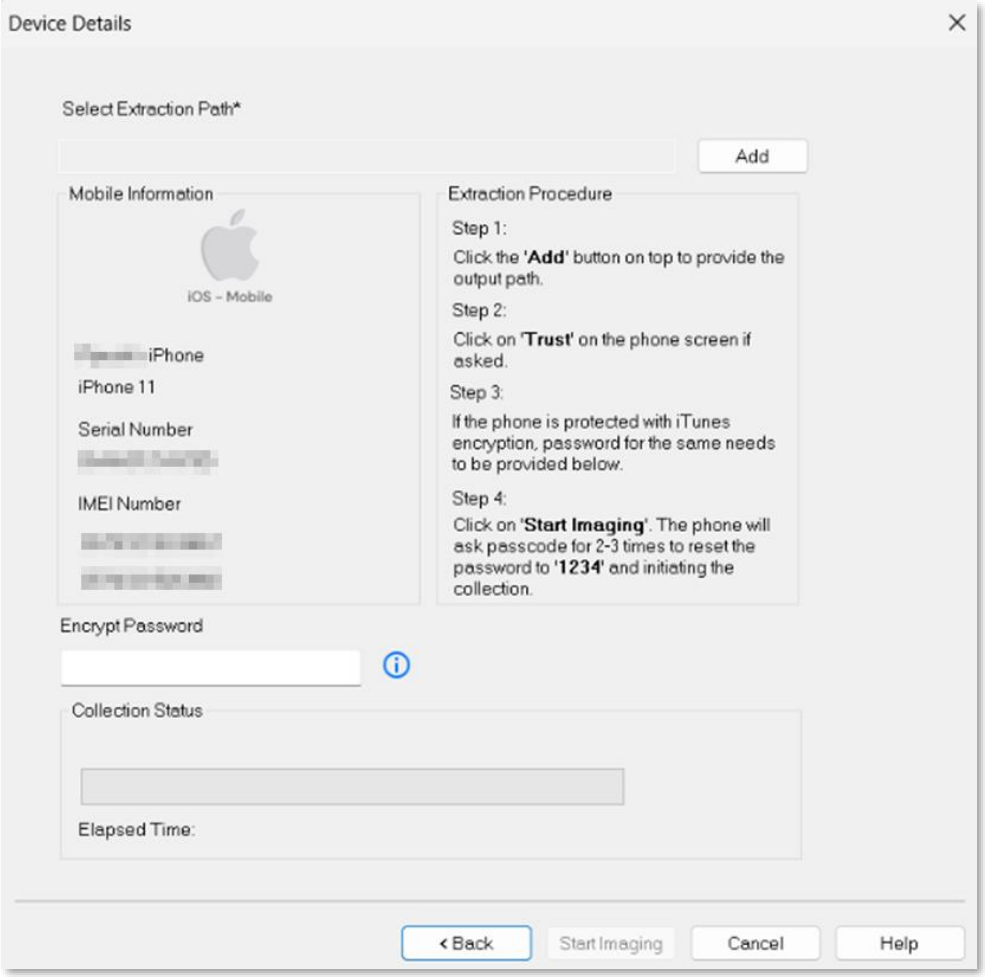
○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

● iOS Advanced Logical Collection

○ Fernico Device (multiple CD/DVD)

3. Connect the iPhone using a cable and unlock it.
4. Select **iOS Advanced Logical Collection** (requires FTK Imager Pro license).
5. Once the device is connected, the following details will be displayed:
   - Device Name
   - Serial Number
   - IMEI Number
6. Click on **Add** to choose the destination folder for saving the extracted data.

7. (Optional), Click on **Next** and provide evidence information and specify the output path (Image destination) and the desired image name.



[redacted] iPhone

iPhone 11

Serial Number

[redacted]

IMEI Number

[redacted]

Step 1:

Click the '**Add**' button on top to provide the output path.

Step 2:

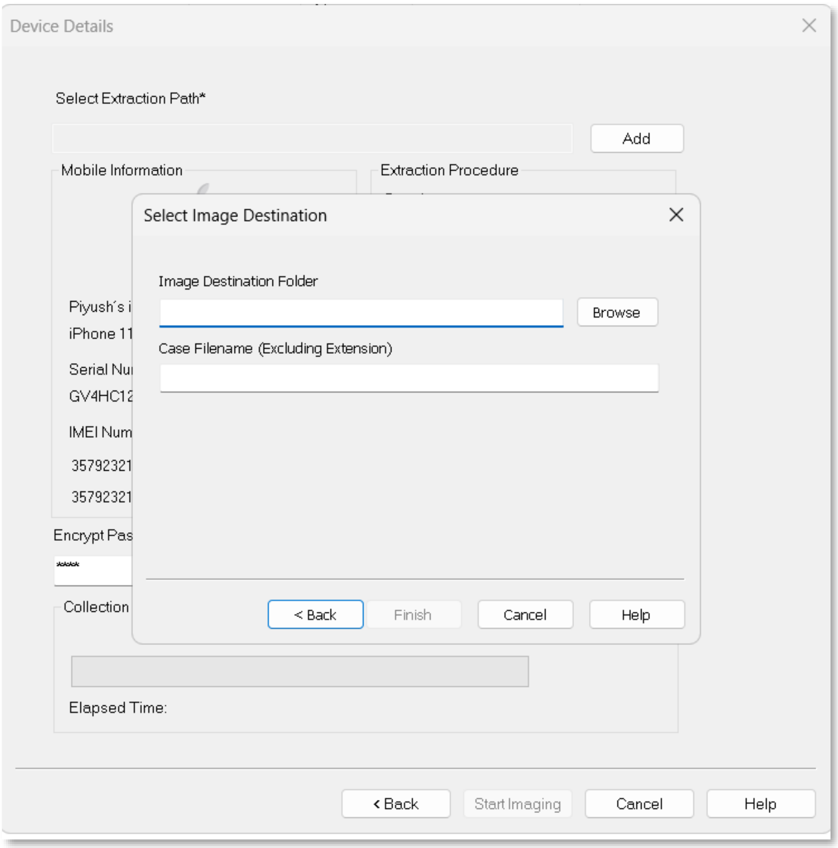
Click on '**Trust**' on the phone screen if asked.

Step 3:

If the phone is protected with iTunes encryption, password for the same needs to be provided below.

Step 4:

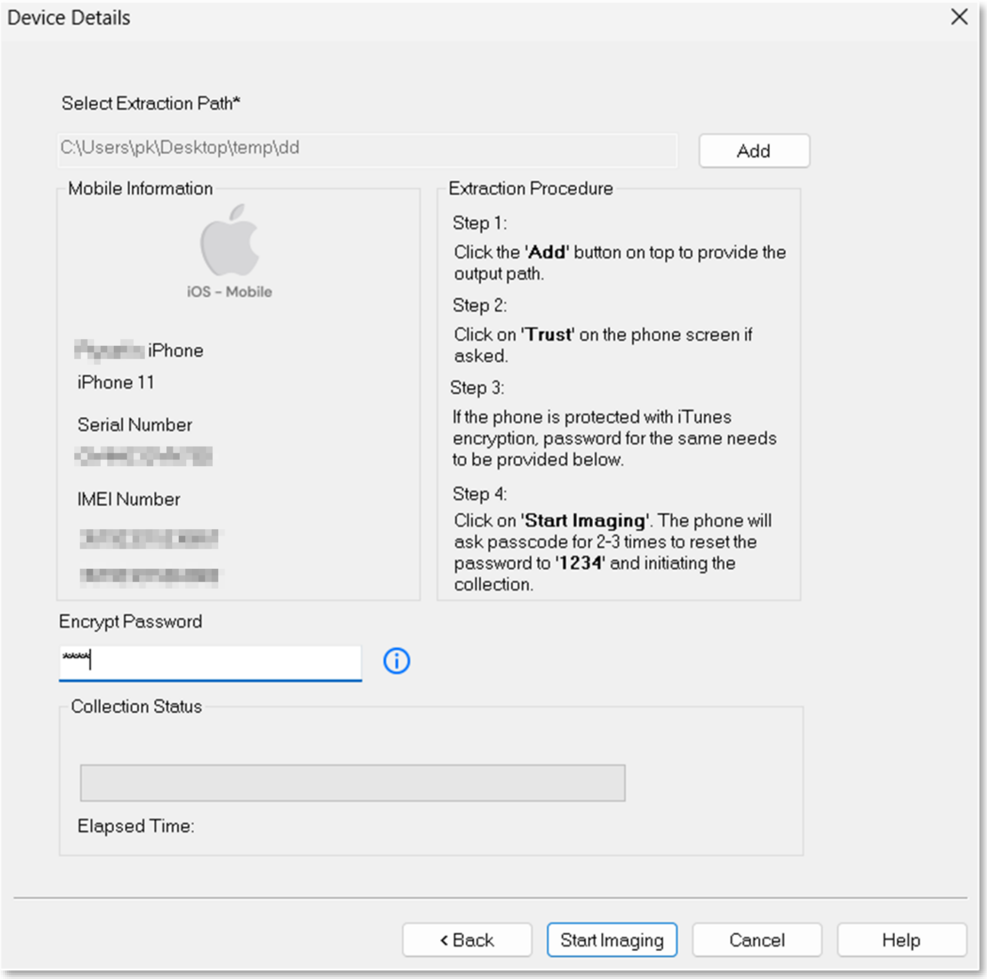
Click on '**Start Imaging**'. The phone will ask passcode for 2-3 times to reset the password to '**1234**' and initiating the collection.


Device Details
Select Extraction Path*
Add
Mobile Information
Extraction Procedure
Piyush's i
iPhone 11
Serial Nu
GV4HC12
IMEI Num
35792321
35792321
Encrypt Pas
Collection
Elapsed Time:
< Back
Start Imaging
Cancel
Help
Select Image Destination
Image Destination Folder
Browse
Case Filename (Excluding Extension)
< Back
Finish
Cancel
Help

8. If the iPhone is set up with an iTunes passcode, provide the passcode:

***Note**: Imager will ask for the passcode 3 times in order to:*

- Remove the preset iTunes password.
- Set the new iTunes password to “1234”.
- Start the collection.



Device Details

Select Extraction Path*

C:\Users\pk\Desktop\temp\dd

Mobile Information

iOS – Mobile

[redacted] iPhone

iPhone 11

Serial Number

[redacted]

IMEI Number

[redacted]

[redacted]

Extraction Procedure

Step 1:

Click the '**Add**' button on top to provide the output path.

Step 2:

Click on '**Trust**' on the phone screen if asked.

Step 3:

If the phone is protected with iTunes encryption, password for the same needs to be provided below.

Step 4:

Click on '**Start Imaging**'. The phone will ask passcode for 2-3 times to reset the password to '**1234**' and initiating the collection.

Encrypt Password

****

Collection Status

Elapsed Time:

9. After specifying the destination details, click **Start Extraction**. The extraction process will begin.

   Note*: It is advised to wait for the process to complete and avoid closing the window or shutting down the machine.*

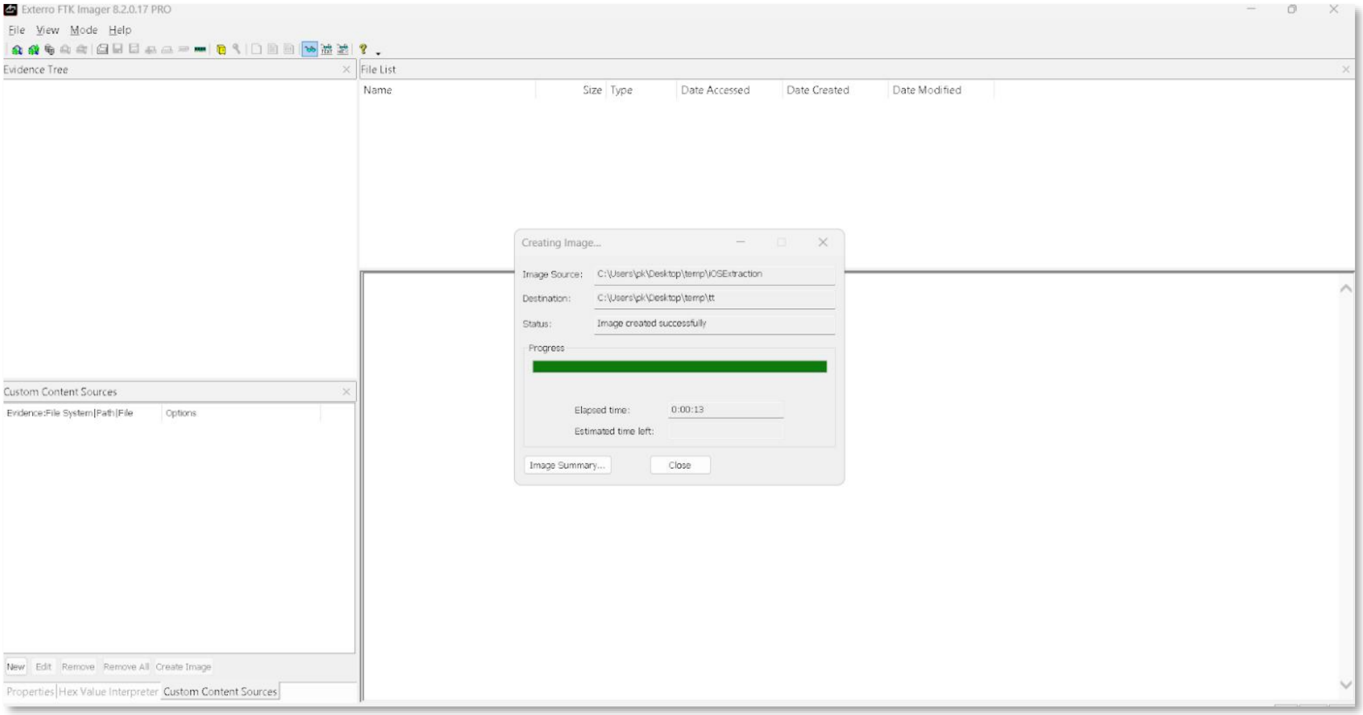


Image Source: C:\Users\pk\Desktop\temp\iOSExtraction

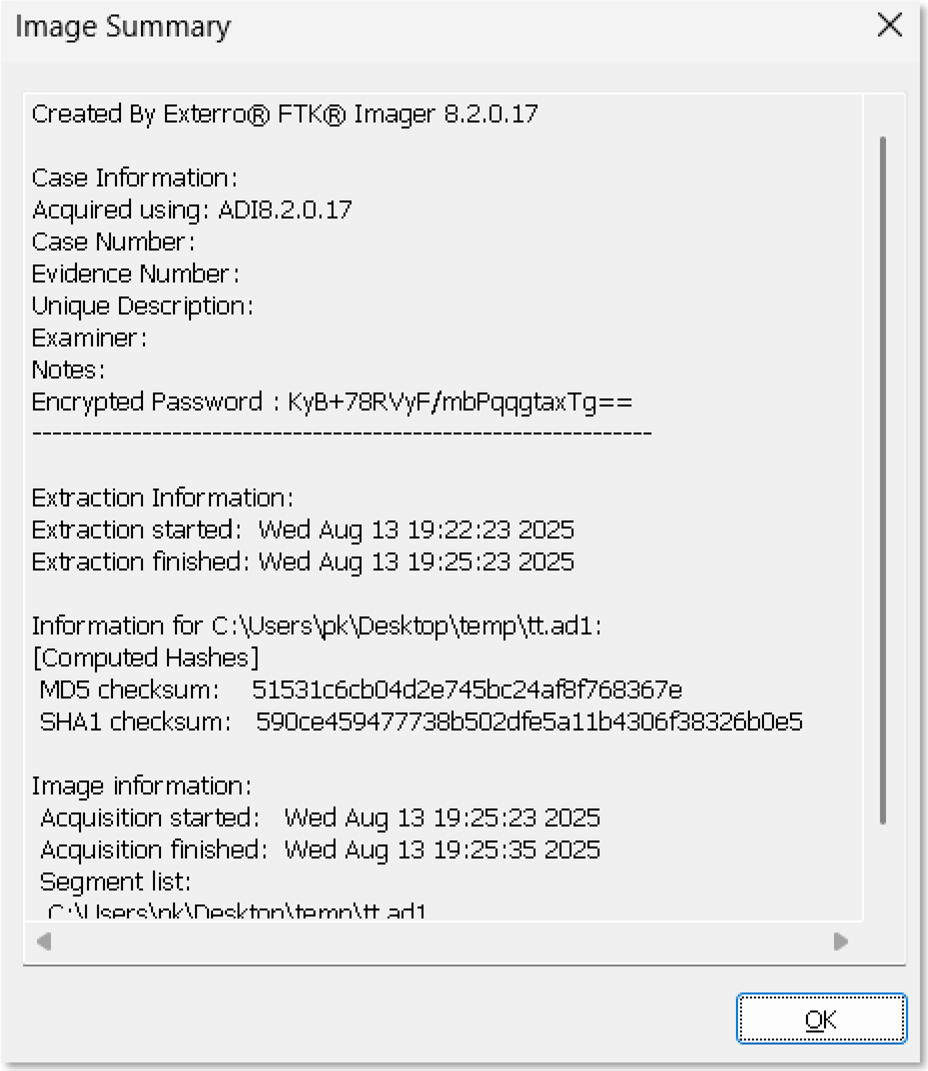
Destination: C:\Users\pk\Desktop\temp\tt

Status: Image created successfully

Elapsed time: 0:00:13

Estimated time left:

10. Once extraction is **complete**, you can click on **Image Summary** and note down the hash values generated and close the window.



```
Created By Exterro® FTK® Imager 8.2.0.17

Case Information:
Acquired using: ADI8.2.0.17
Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:
Encrypted Password : KyB+78RVyF/mbPqqgtaxTg==
--------------------------------------------------------------


Extraction Information:
Extraction started:  Wed Aug 13 19:22:23 2025
Extraction finished: Wed Aug 13 19:25:23 2025

Information for C:\Users\pk\Desktop\temp\tt.ad1:
[Computed Hashes]
 MD5 checksum:    51531c6cb04d2e745bc24af8f768367e
 SHA1 checksum:   590ce459477738b502dfe5a11b4306f38326b0e5

Image information:
 Acquisition started:   Wed Aug 13 19:25:23 2025
 Acquisition finished:  Wed Aug 13 19:25:35 2025
 Segment list:
  C:\Users\pk\Desktop\temp\tt.ad1
```

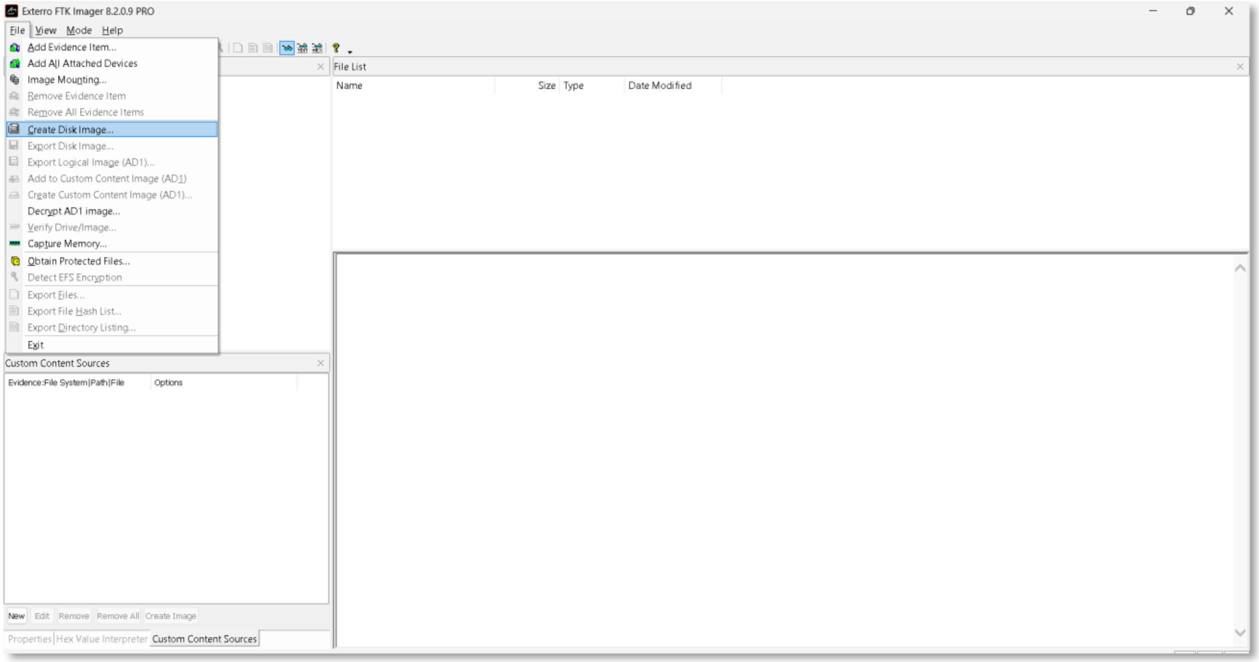
Decryption of Live Data

FTK Imager Pro provides the ability to create a decrypted copy of BitLocker-encrypted drives, allowing access to the decrypted data without altering the original.

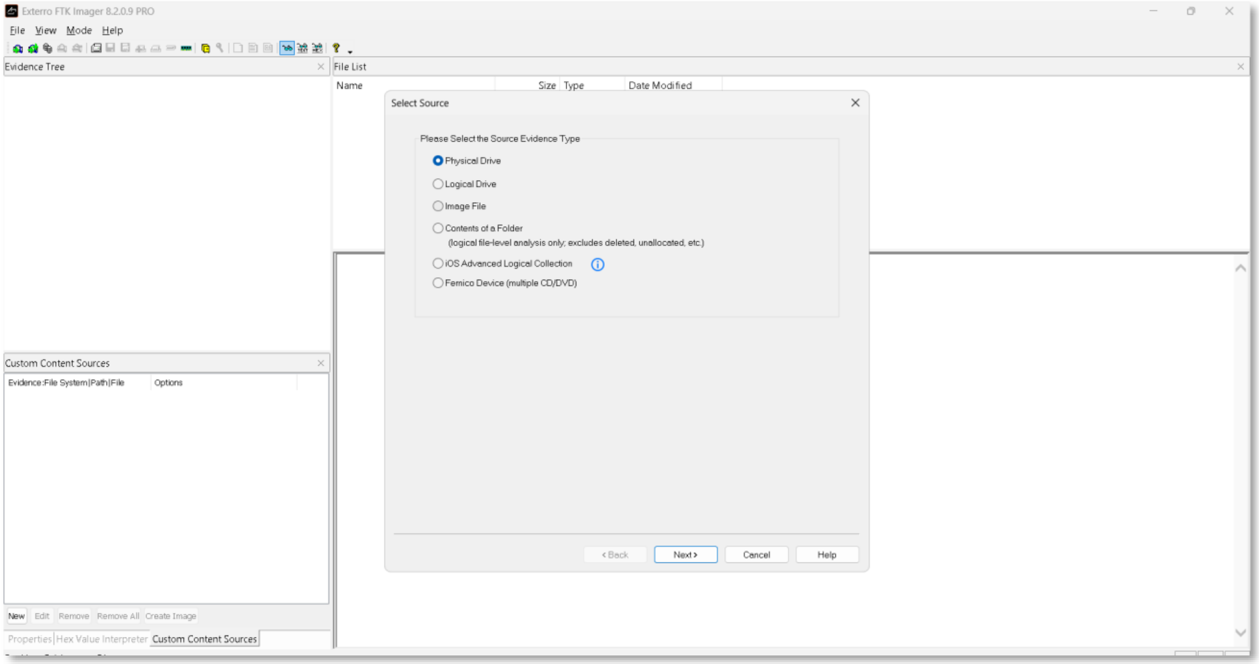
Prerequisite: A password or recovery key is required for decryption.

Steps to Image Decrypted Data

1. Go to **Create Disk Image** from the menu.



2. Select **Physical Disk** and choose the **BitLocker-encrypted disk**.



Select Source

Please Select the Source Evidence Type

● Physical Drive

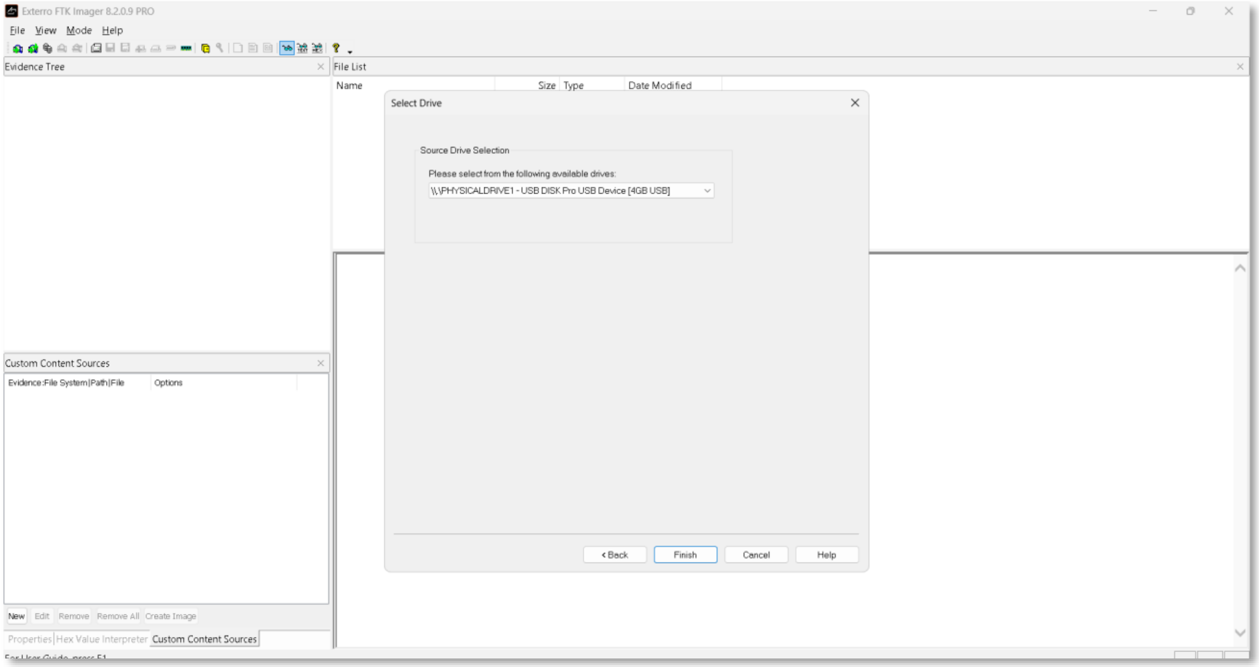
○ Logical Drive

○ Image File

○ Contents of a Folder
(logical file-level analysis only; excludes deleted, unallocated, etc.)

○ iOS Advanced Logical Collection

○ Femico Device (multiple CD/DVD)



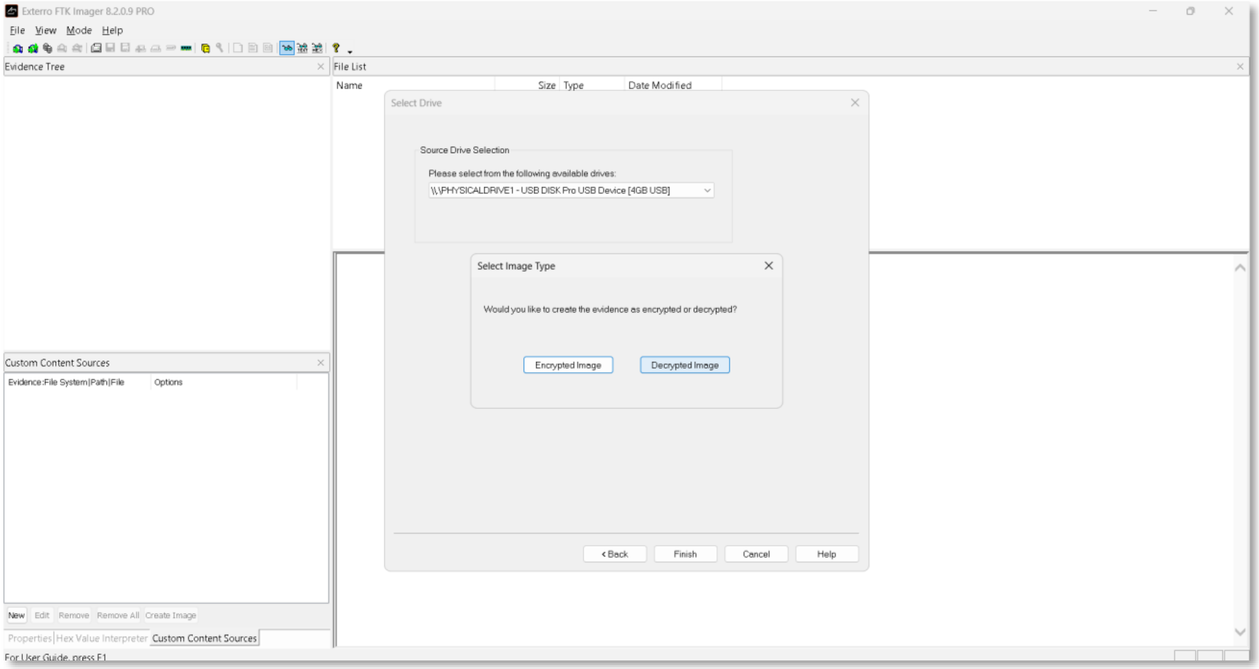
Select Drive

Source Drive Selection

Please select from the following available drives:
\\.\PHYSICALDRIVE1 - USB DISK Pro USB Device [4GB USB]

3. FTK Imager Pro will prompt whether to create a **Decrypted Copy** of the BitLocker-protected drive.

__Note__: This feature is only available in the licensed version of Imager Pro.



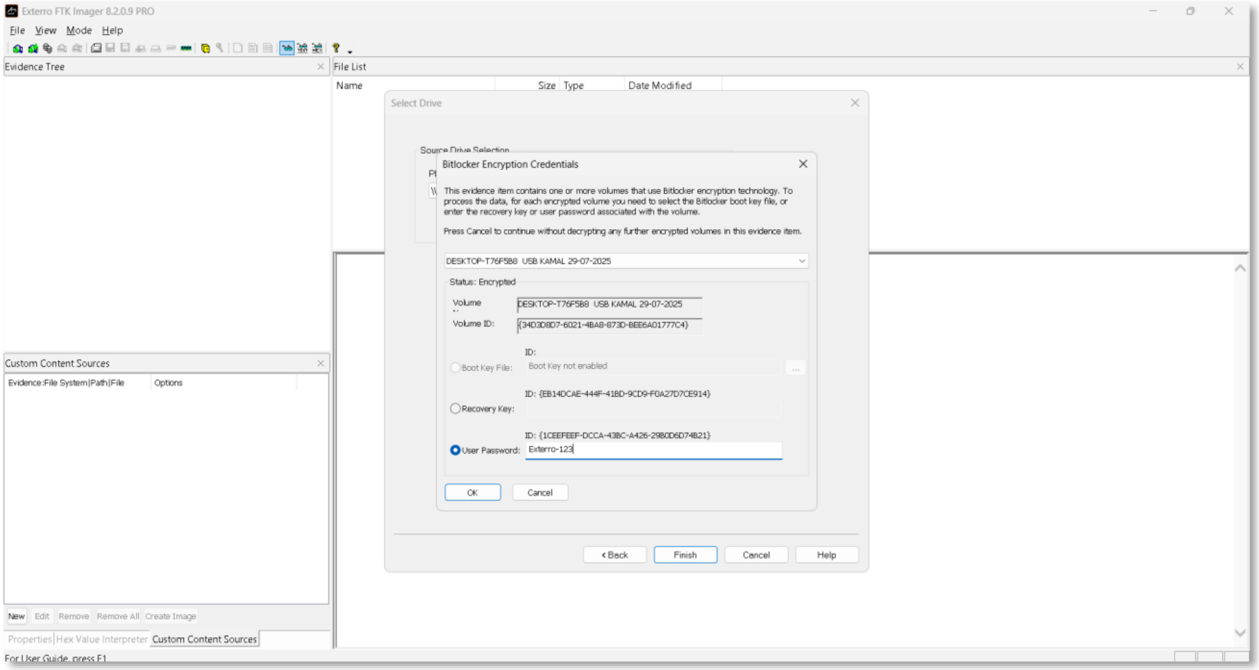
Source Drive Selection

Please select from the following available drives:

\\.\PHYSICALDRIVE1 - USB DISK Pro USB Device [4GB USB]

Would you like to create the evidence as encrypted or decrypted?

4. Enter the **password/recovery key** for the encrypted disk.



Bitlocker Encryption Credentials

This evidence item contains one or more volumes that use Bitlocker encryption technology. To process the data, for each encrypted volume you need to select the Bitlocker boot key file, or enter the recovery key or user password associated with the volume.

Press Cancel to continue without decrypting any further encrypted volumes in this evidence item.

DESKTOP-T76F5B8 USB KAMAL 29-07-2025

Status: Encrypted

Volume: DESKTOP-T76F5B8 USB KAMAL 29-07-2025

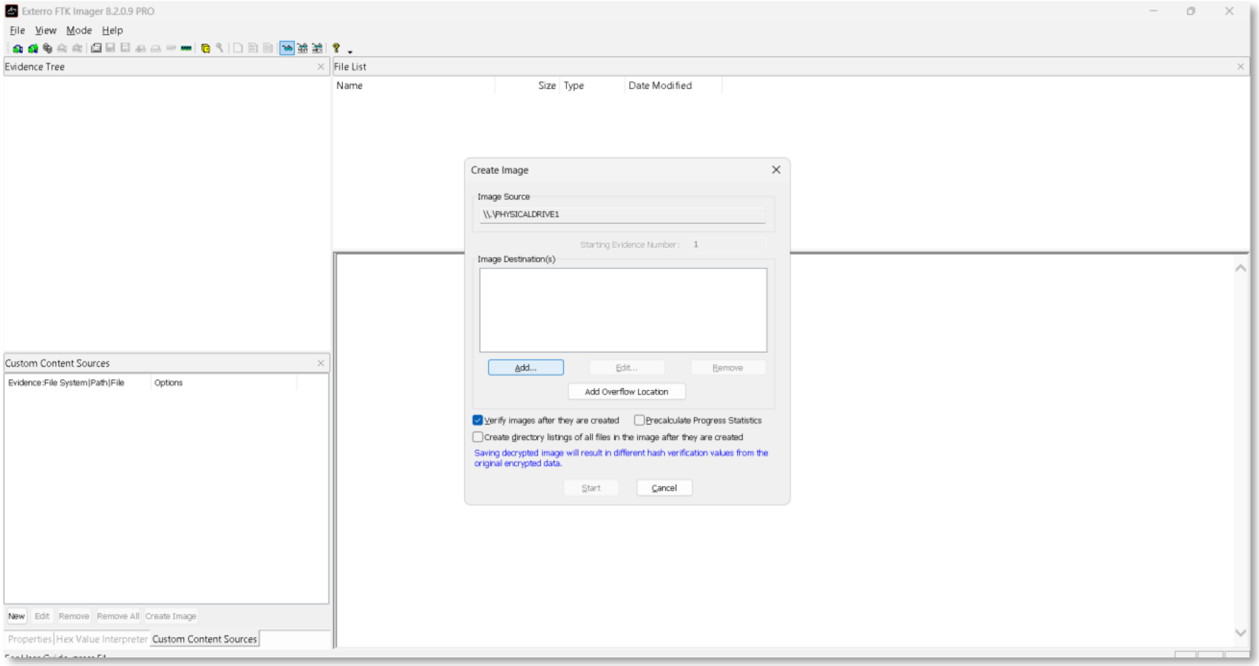
Volume ID: {34D3D8D7-6021-4BA8-873D-BEE6A01777C4}

○ Boot Key File: ID: Boot Key not enabled

○ Recovery Key: ID: {EB14DCAE-444F-41BD-9CD9-F0A27D7CE914}

● User Password: ID: {1CEEFEEF-DCCA-43BC-A426-29B0D6D74B21} Exterro-123

5. Click **Add** to select the format and other details.



Create Image

Image Source: \\.\PHYSICALDRIVE1

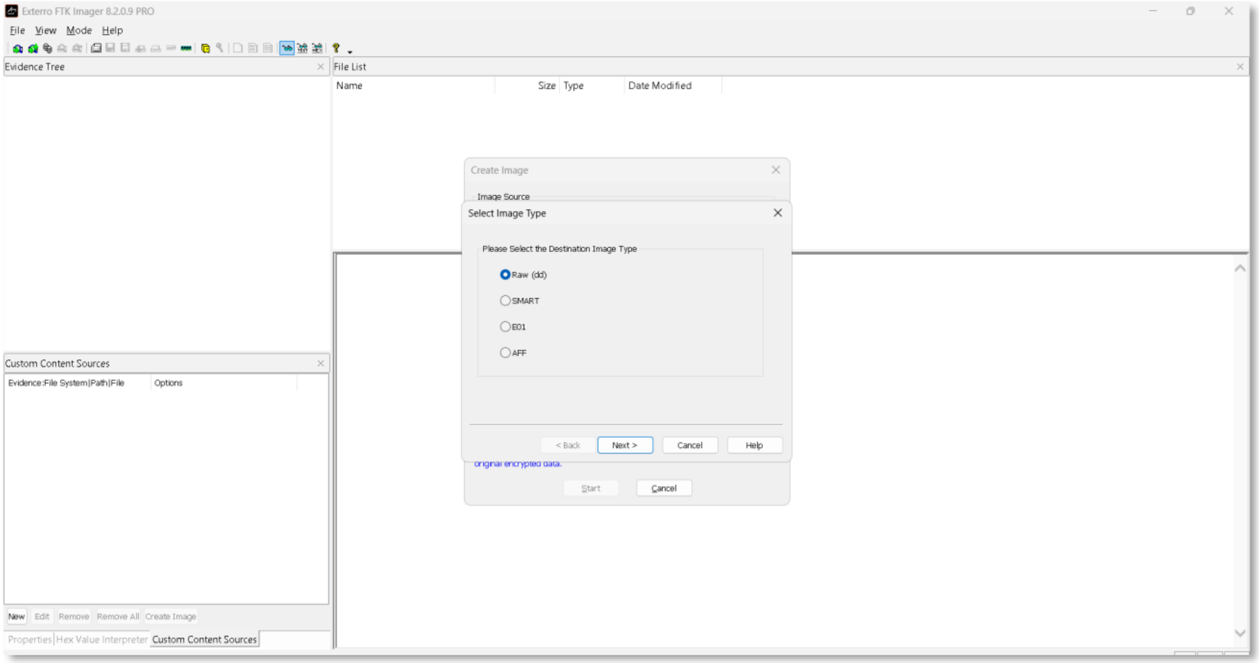
Starting Evidence Number: 1

Image Destination(s)

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

Saving decrypted image will result in different hash verification values from the original encrypted data.

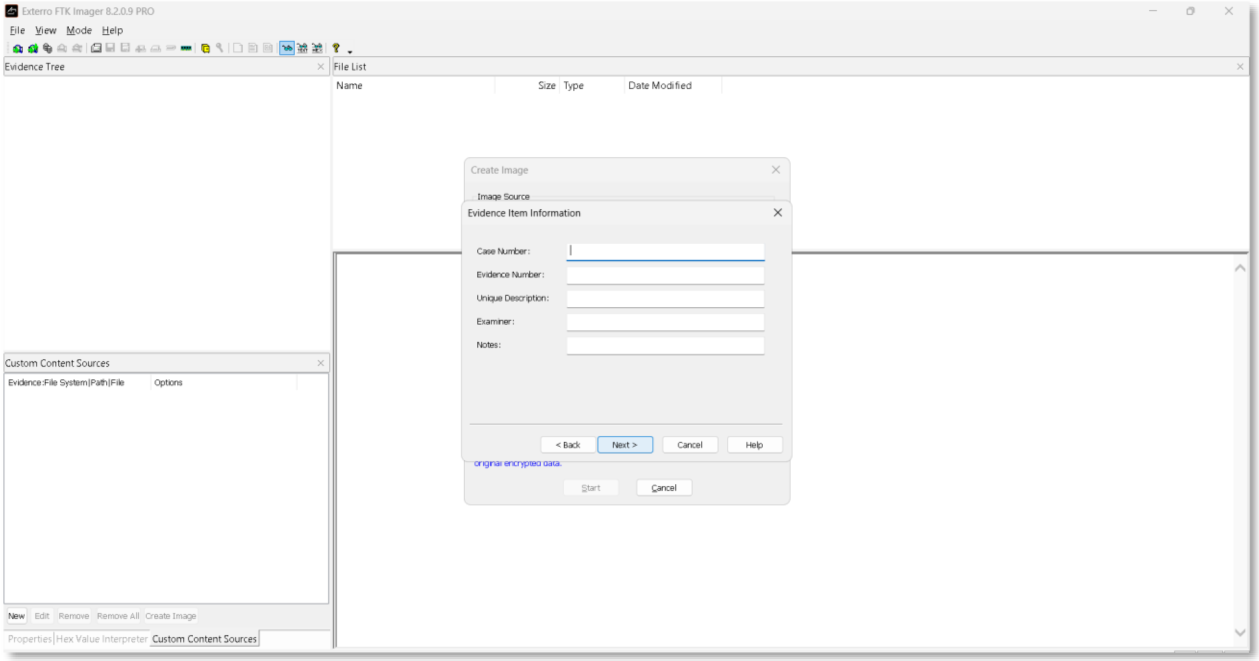

Exterro FTK Imager 8.2.0.9 PRO
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Image Source
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Interpreter Custom Content Sources
original encrypted data.
Start Cancel

Select Image Type

Please Select the Destination Image Type

● Raw (dd)
○ SMART
○ E01
○ AFF

< Back | Next > | Cancel | Help


Exterro FTK Imager 8.2.0.9 PRO
File View Mode Help
Evidence Tree
File List
Name Size Type Date Modified
Create Image
Image Source
Custom Content Sources
Evidence:File System|Path|File Options
New Edit Remove Remove All Create Image
Properties Hex Value Interpreter Custom Content Sources
original encrypted data.
Start Cancel

Evidence Item Information

Case Number:
Evidence Number:
Unique Description:
Examiner:
Notes:

< Back | Next > | Cancel | Help

6. Provide the output path and image name, then click **Finish**.

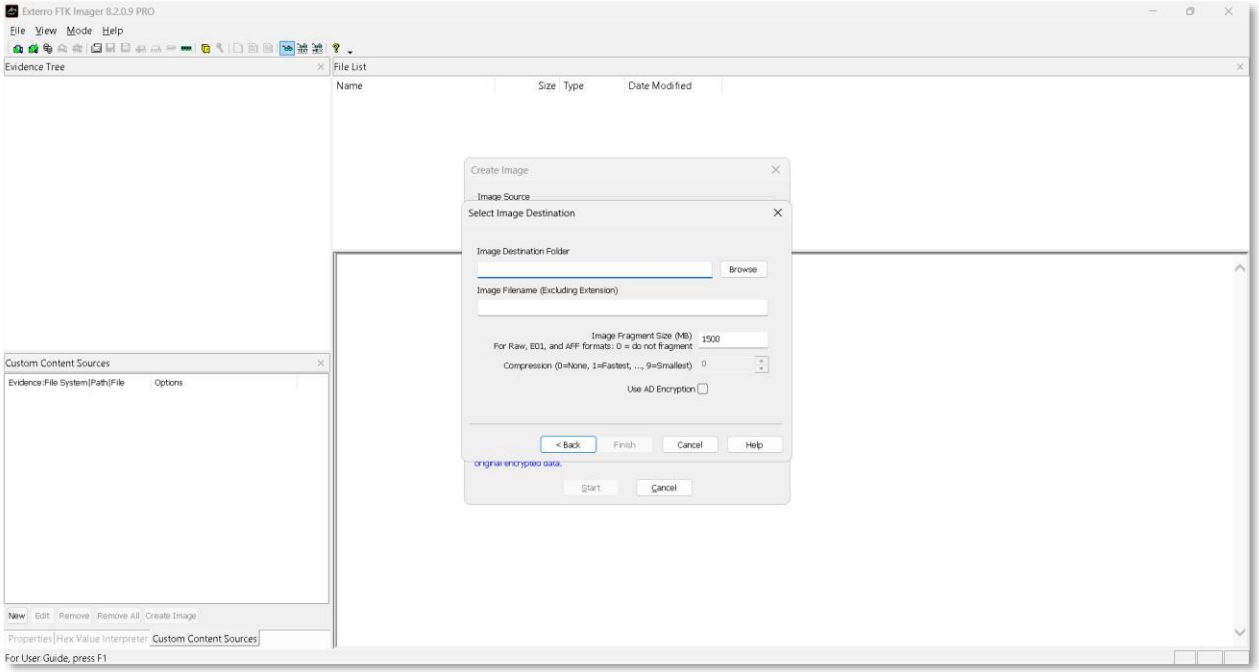


Image Destination Folder

Image Filename (Excluding Extension)

Image Fragment Size (MB) For Raw, E01, and AFF formats: 0 = do not fragment: 1500

Compression (0=None, 1=Fastest, ..., 9=Smallest): 0

Use AD Encryption ☐

7. Click **Start** to begin the decryption and imaging process.

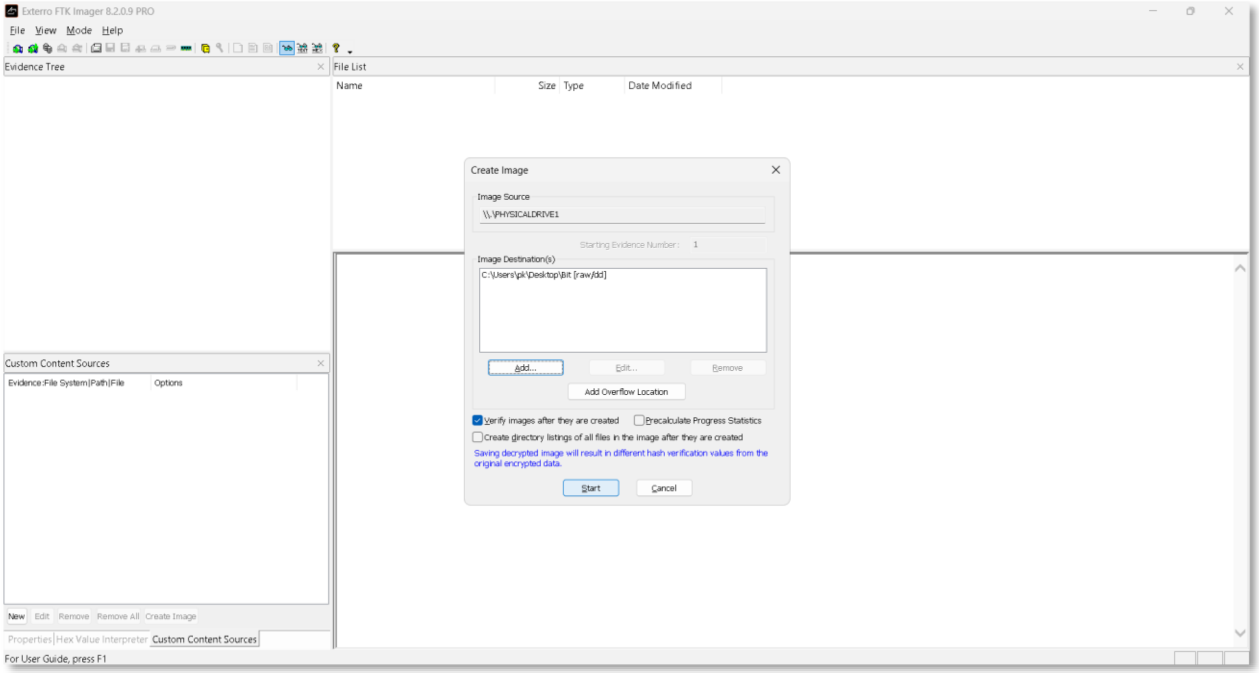


Image Source: \\.\PHYSICALDRIVE1

Starting Evidence Number: 1

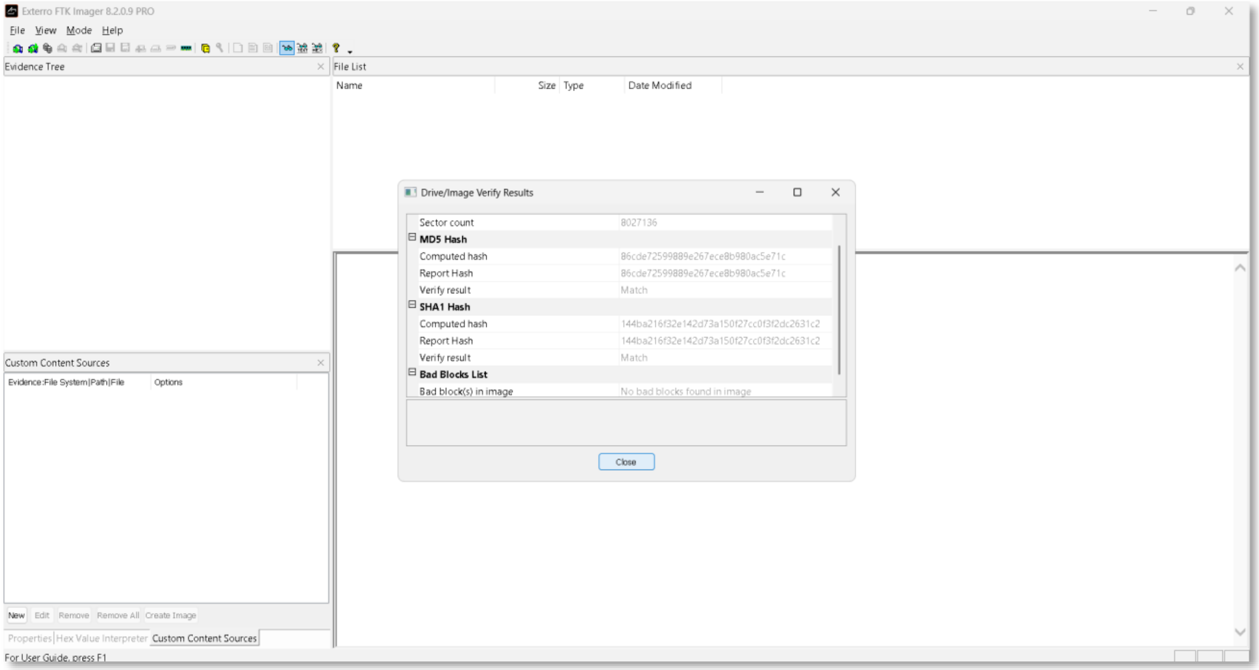
Image Destination(s): C:\Users\pk\Desktop\Bit [raw/dd]

☑ Verify images after they are created ☐ Precalculate Progress Statistics

☐ Create directory listings of all files in the image after they are created

Saving decrypted image will result in different hash verification values from the original encrypted data.

8. Once the process is complete, review the final results.



Drive/Image Verify Results

Sector count	8027136
⊟ **MD5 Hash**	
Computed hash	86cde72599889e267ece8b980ac5e71c
Report Hash	86cde72599889e267ece8b980ac5e71c
Verify result	Match
⊟ **SHA1 Hash**	
Computed hash	144ba216f32e142d73a150f27cc0f3f2dc2631c2
Report Hash	144ba216f32e142d73a150f27cc0f3f2dc2631c2
Verify result	Match
⊟ **Bad Blocks List**	
Bad block(s) in image	No bad blocks found in image

Supported Encryption Technologies for Forensic Images

FTK Imager Pro supports decryption for a wide range of encrypted file systems and partitions. When adding encrypted forensic images to a case, FTK Imager Pro will detect the encryption type and prompt the user for the necessary credentials.

Supported Encryption Types:

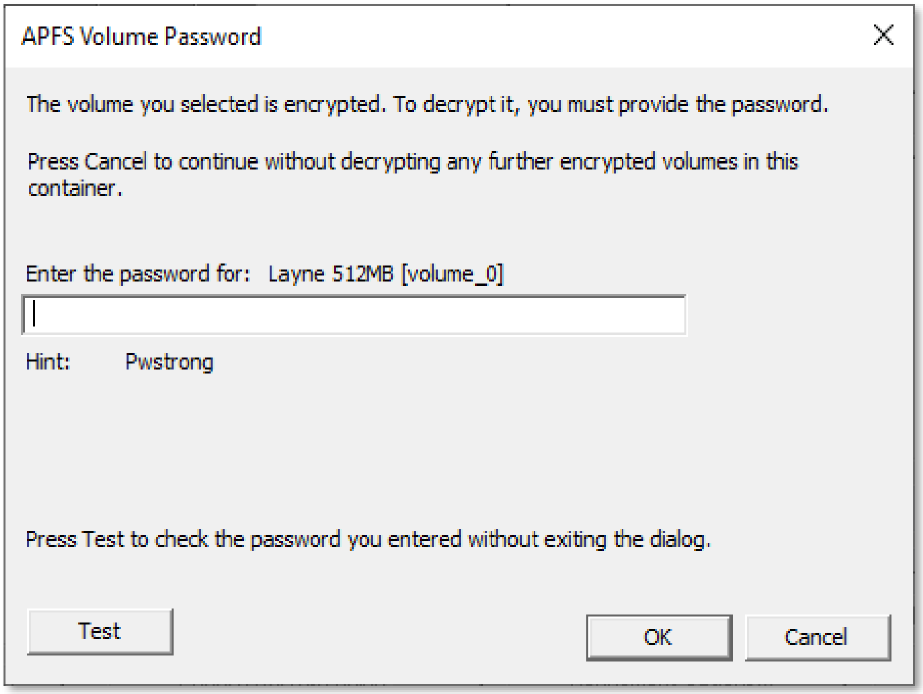
Encryption Type
▪ Apple APFS Encryption
▪ BitLocker (Windows Vista, 7, 8, 10)
▪ Checkpoint/PointSec R73 7.4.5
▪ Decrypting McAfee Drive Encryption
▪ Decrypting SafeBoot Files
▪ Decrypting Guardian Edge Files
▪ Checkpoint 7.6.150 with token challenge
▪ McAfee Endpoint Encryption (formerly Safeboot) 5.x and 6.0
▪ McAfee Drive Encryption 7.2.x
▪ Safeguard Easy 4.40.9 and Enterprise 5.40 and 5.50
▪ SecureDoc WinMagic o SecureDoc Enterprise Server (SES) Version 8.2 o Standalone Installer Version 7.5
▪ Symantec Endpoint Encryption (formerly Guardian Edge) 8.1.1, 9.1.6, 9.3.0, 9.4.1, 9.5.3.
▪ Symantec Drive Encryption (PGP WDE) 10.0 (only)
▪ Advanced Forensic Format (AFF)
▪ FileVault
▪ VeraCrypt

Decrypting Process for Each Encryption Type

Decrypting Apple APFS

Encrypted Apple File System (APFS) volumes (other than volumes encrypted by the "T2 security chip" internal to Mac systems 2017 and newer) can be decrypted. When adding an image file as evidence to your case, you will be prompted to enter the user-created password used to encrypt the volume.

For APFS volumes encrypted by the Apple T2 security chip, the best practice would be to acquire the hard drive data while still internal to the system that encrypted it.



APFS Volume Password

The volume you selected is encrypted. To decrypt it, you must provide the password.

Press Cancel to continue without decrypting any further encrypted volumes in this container.

Enter the password for: Layne 512MB [volume_0]

Hint: Pwstrong

Press Test to check the password you entered without exiting the dialog.

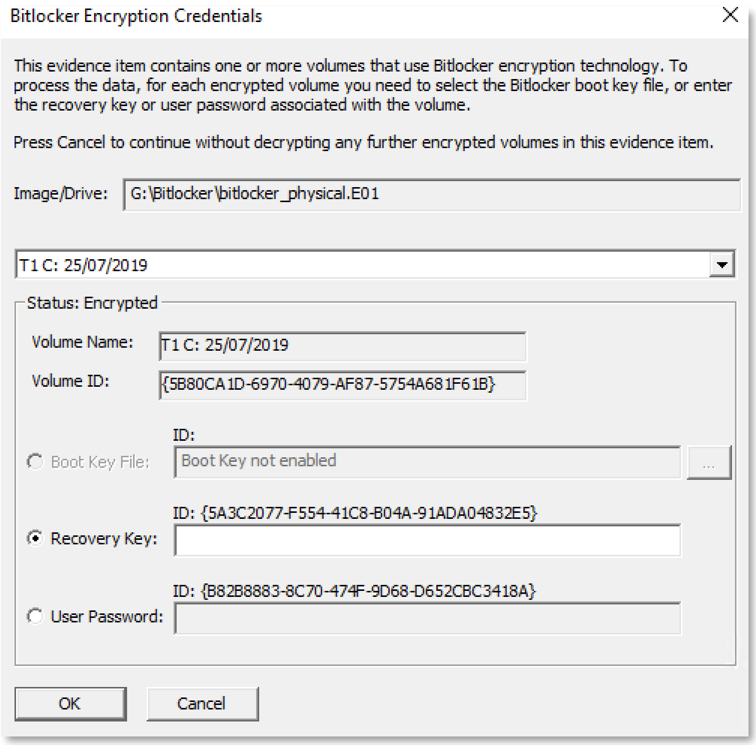
Decrypting Bitlocker Partitions

If you have the proper credentials, you can decrypt BitLocker-encrypted partitions. You can decrypt the BitLocker partitions from Windows Vista, 7, 8, and 10 workstations. You can either provide the unique credentials for multiple encrypted partitions or the Boot Key File that corresponds to the BitLocker installation on that system. After you provide the correct information, the files in the BitLocker-encrypted partitions are decrypted while the evidence is processed.

To decrypt BitLocker partitions

1. Add evidence that has BitLocker encryption to a case.

   If BitLocker encryption is detected, you are prompted to enter credentials in the following dialog:



Bitlocker Encryption Credentials

This evidence item contains one or more volumes that use Bitlocker encryption technology. To process the data, for each encrypted volume you need to select the Bitlocker boot key file, or enter the recovery key or user password associated with the volume.

Press Cancel to continue without decrypting any further encrypted volumes in this evidence item.

Image/Drive: G:\Bitlocker\bitlocker_physical.E01

T1 C: 25/07/2019

Status: Encrypted

Volume Name: T1 C: 25/07/2019

Volume ID: {5B80CA1D-6970-4079-AF87-5754A681F61B}

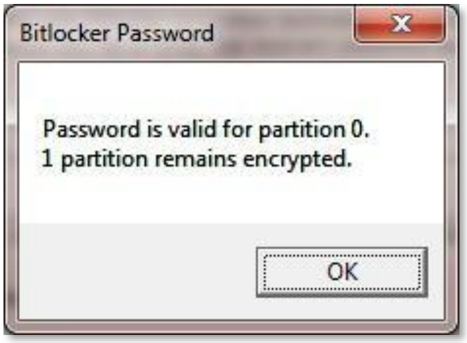
ID:
○ Boot Key File: Boot Key not enabled

ID: {5A3C2077-F554-41C8-B04A-91ADA04832E5}
● Recovery Key:

ID: {B82B8883-8C70-474F-9D68-D652CBC3418A}
○ User Password:

2. Enter one of the following credentials:
   - Boot Key File
   - Recovery Password.

3. If there are multiple partitions, a dialog will be displayed saying that the password for the first partition is valid, and that additional partitions remain encrypted.



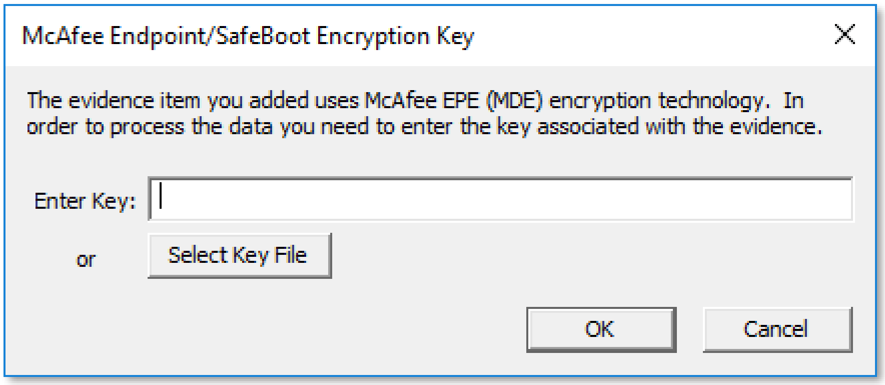
Password is valid for partition 0.
1 partition remains encrypted.

4. Click **OK** and the credential dialog is again displayed for the next partition.

   This sequence continues until you have entered the credentials for all encrypted partitions.

Decrypting McAfee Drive Encryption

When adding a disk image of a drive encrypted with McAfee Drive Encryption (MDE), you will be prompted to enter the decryption key or XML (which contains the decryption key in plain text). Enter either the key or the XML in order to proceed with the decryption.



McAfee Endpoint/SafeBoot Encryption Key

The evidence item you added uses McAfee EPE (MDE) encryption technology. In order to process the data you need to enter the key associated with the evidence.

Decrypting Safeguard Utimaco Files

You can use either Imager or the *Examiner* interface to decrypt boot drives that were encrypted with SafeGuard by Utimaco.

Safeguard Easy

Safeguard Easy works only with an image of a complete drive or a live drive. Imaged partitions cannot be decrypted because the information needed to decrypt the partition exists in the boot record of the drive.

When a live drive or drive image is added as evidence, it is checked to determine if SafeGuard Easy encryption is used on the drive. If it is used, a dialog will appear asking for the user name and password required to access the drive. If the correct user name and password are entered, the drive will be decrypted transparently during processing and the user can access information on the drive as though the drive were not encrypted. Incorrect passwords will result in long waits between attempts -- waits that grow exponentially for each failure. Hitting the cancel button on the dialog will allow the drive to be added as evidence, but the encrypted portions will not be processed.

Secondary hard drives and removable media that has been encrypted with SafeGuard Easy are not currently supported. The problem with secondary drives and removable media is that they contain NO information that indicates how they are encrypted. The encryption information for secondary drives and removable media is contained on the boot drive of the computer that encrypted them.

Versions 2.x and later, and all Imager versions since then support SafeGuard Easy drives encrypted with the following algorithms: AES128, AES256 (the default), DES, 3DES, and IDEA.

The Safeguard dialog box appears only when a valid Utimaco-encrypted image is read.

The username and password used to create the encrypted image are required for decryption. Once the credentials have been added, click **OK** to return to the *Manage Evidence* dialog. Select a time zone from the Time Zone drop-down, then click **OK** to begin processing.

Important: The following important information applies when using SafeGuard Decryption:

- Enter the User Name and Password carefully and verify both before clicking *OK*. If this information is entered incorrectly, the entire image is checked for matching information before returning with an error message. Each wrong entry results in a longer wait.
- If you click *Cancel* to process the evidence without decrypting, you will *not* be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.

SafeGuard Enterprise

SafeGuard Enterprise (SGN) is supported. Utimaco supplied libraries to access the decryption keys for SGN via their recovery mechanism. This involves a somewhat cumbersome challenge/response system with the server to access the decryption keys. Each partition may be decrypted with a different key. The challenge/response process needs to be done for each encrypted partition. In order to enable the challenge/response system, a file called recoverytoken.tok needs to be retrieved from the server and selected in the decryption dialog. A recoverytoken.tok file is automatically selected if it is in the same directory as the evidence file.

SafeGuard Enterprise decryption was developed using version 5.x.

Exterro uses SafeGuard-provided BE_Sgn_Api.DLL and BE_KBRDLLn.DLL. These libraries are 32-bit libraries. The 32-bit process is used to retrieve keys in 64-bit. The actual decryption of the drive is done in the Examiner, but the SafeGuard libraries are needed to generate the key from the username/password.

To recognize that a drive is encrypted with SafeGuard Enterprise, “UTICRYPT” is searched for at the beginning of the first sector of each partition.

Retrieving the Recovery Token

Before the decryption process can occur, the recoverytoken.tok file must be retrieved from the server.

To retrieve the Recovery Token

1. From the server, you must create a virtual client.
2. Then you must export the virtual client. This is where the recoverytoken.tok file is created.
3. This file must be copied to a place where the *Examiner* can access the file.
4. Click the **Recovery** button next to each partition to retrieve that partition's key. A dialog will open, telling you which key to retrieve:

    4a. On the server, select **Tools > Recovery** from the menu.

    4b. Select the virtual client you exported (the recoverytoken.tok file)

5. Select **Key requested.**
6. Find the requested key (in this case 0x1C3A799F48FB4B199903FB5730314ABF). You can use **Find > Key IDs** from the drop-down, and enter a partial key into **Search Name** to help find the correct key.
7. A challenge code of 6 segments of 5 characters each is offered.
8. Enter the characters from the challenge portion of the dialog into the server's dialog.
9. Click **Next**.
10. The server then offers a response code consisting of 12 segments of 5 characters each.
11. Enter these into the corresponding dialog that provides the decryption key.
12. Click **OK**. The drive is decrypted and added as evidence to the case.

Decrypting SafeBoot Files

SafeBoot is a program that encrypts drives and/or partitions. The encryption key must be available to enter into the **Key** field. All recognized partitions are selected by default, up to a maximum of eight. You can unselect any partition that you do not want to add to the case.

Important: *The following important information applies when using SafeBoot Decryption:*

- *If you click **Cancel** to process the evidence without decrypting, you will not be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.*
- *You must add all partitions and decrypt the encrypted partitions when first adding the evidence to the case or you will be unable to see them. Encrypted partitions do not display in the Evidence list.*

Once the key has been added and the appropriate partitions selected, click **OK** to return to the *Manage Evidence* dialog. Select a time zone from the Time Zone drop-down, then click **OK** to begin processing.

Decrypting SecureDoc WinMagic AES Files

When a SecureDoc WinMagic AES-encrypted image is added to a case, it is automatically detected as a SecureDoc image and a dialog will appear asking for credentials. You will need to enter the following information:

- Key File (a browse button is available)
- Password
- Emergency Disk Folder (a browse button is available) Click **OK** to proceed with the decryption process.

Decrypting Guardian Edge Files

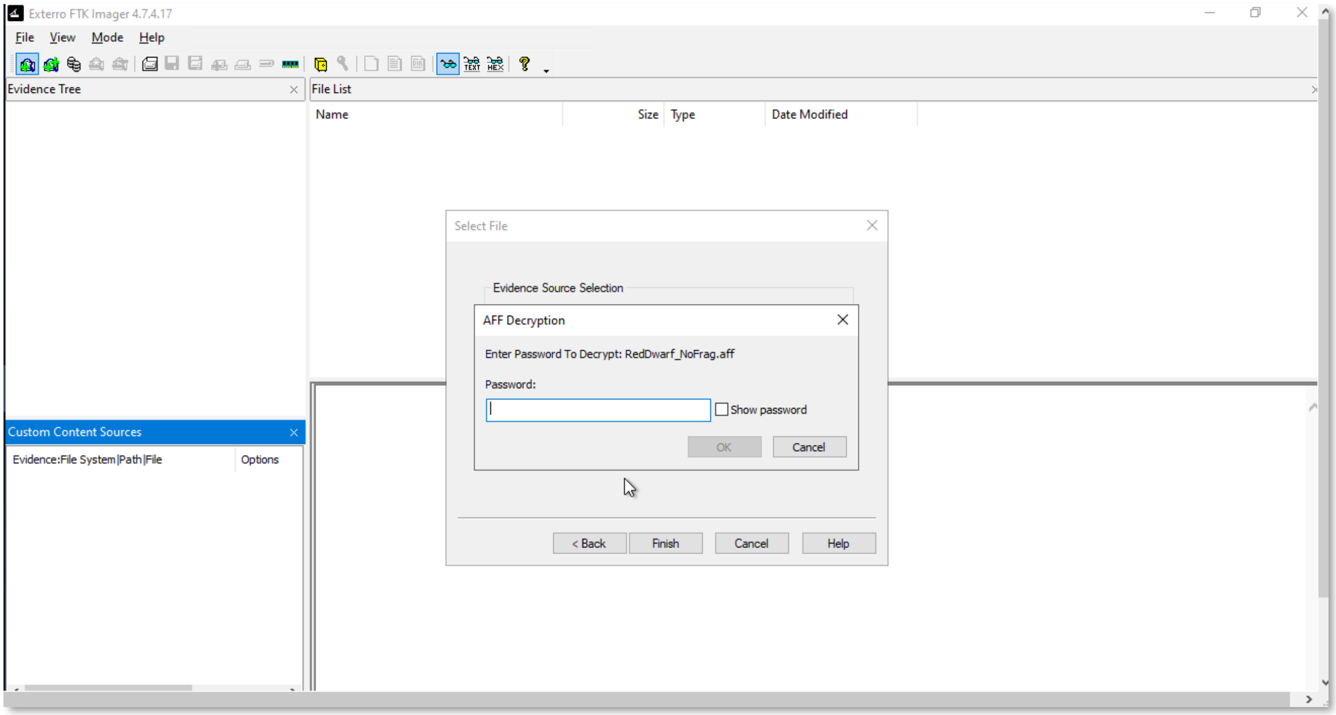
When a Guardian Edge-encrypted image is added to a case, it is automatically detected as a Guardian Edge image and a dialog will appear asking for credentials. The dialog has a drop-down list box with the user names that have been found to be associated with the image. Select the user name for which you have a password and enter that password. Enter the password in one of two ways:

- Enter it twice with dots appearing for each character (to keep it hidden from on-lookers).
- Check the **Show in plain text** box and enter it once. Click **OK** to proceed with the decryption process.

Important: *If you click* ***Cancel*** *to process the evidence without decrypting, you will not be able to decrypt at a later time. Also, the evidence cannot be added to the same case a second time. You will have to create a new case to decrypt and process this evidence.*

Decrypting AFF

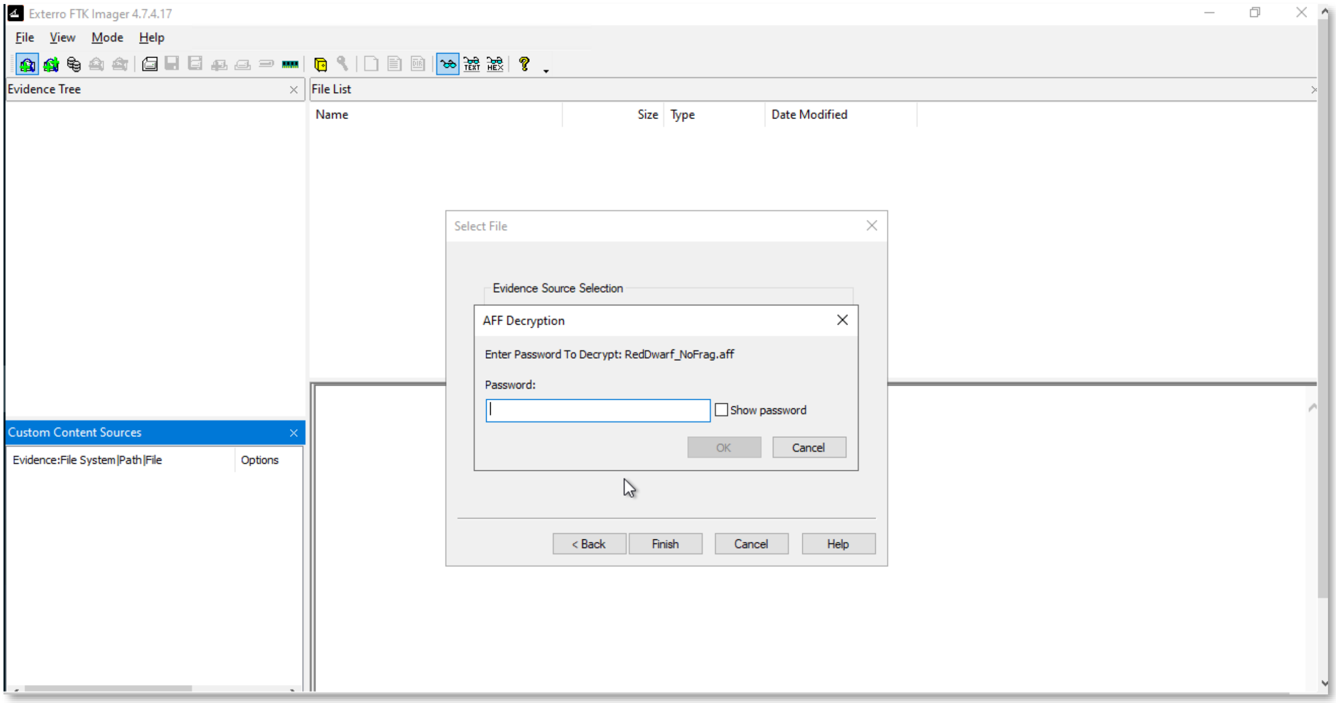
When an AFF Encrypted image is added to a case, the encryption will be automatically detected, and a dialog will prompt you to enter the password for the image.



Enter Password To Decrypt: RedDwarf_NoFrag.aff

Decrypting FileVault

When a FileVault-protected image is added, the encryption will be automatically detected, and a prompt will appear requesting the correct password or recovery key to decrypt the FileVault encryption. After entering the password or recovery key, click "Finish" to decrypt the image.



Enter Password To Decrypt: RedDwarf_NoFrag.aff

Password: