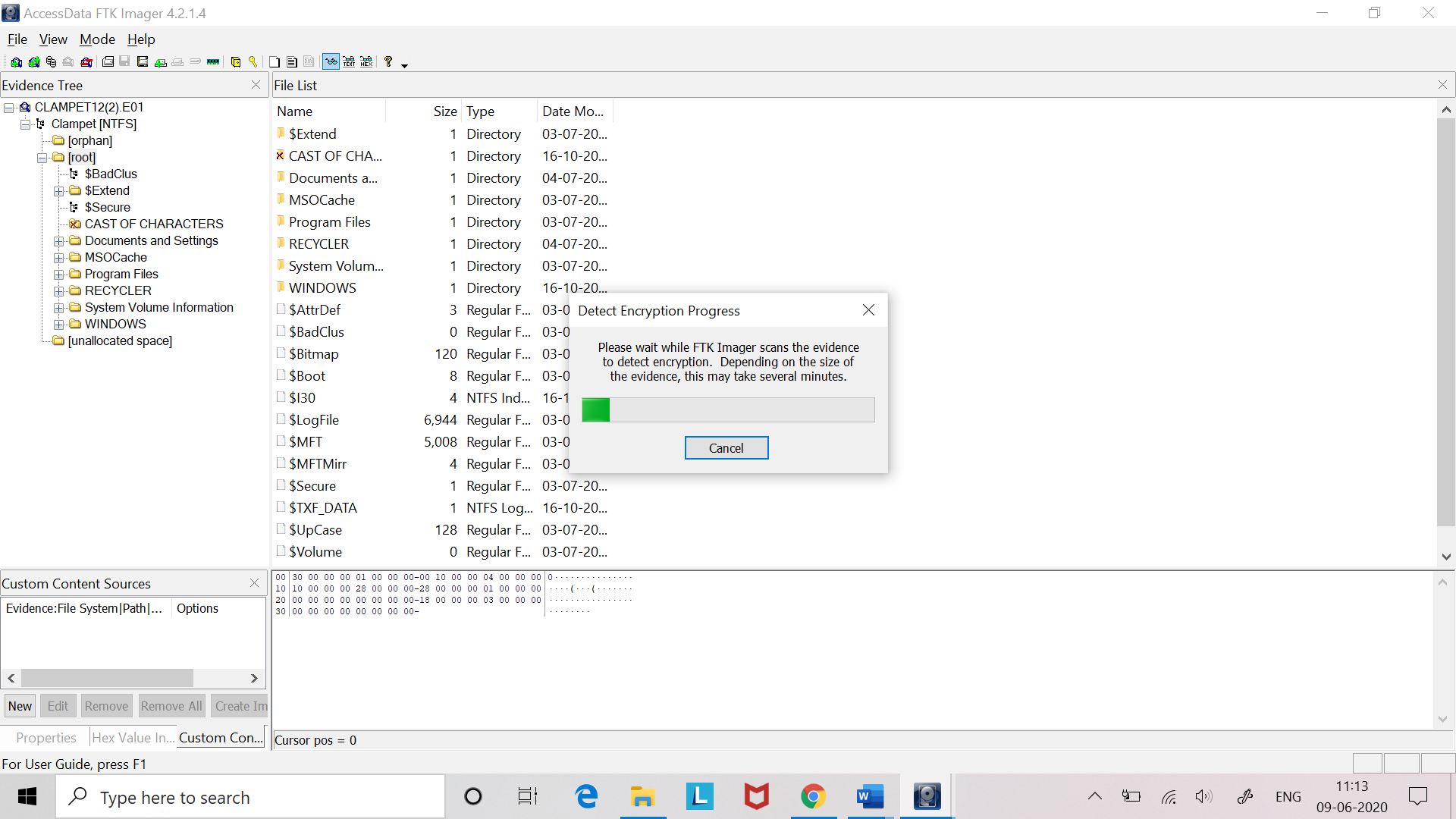
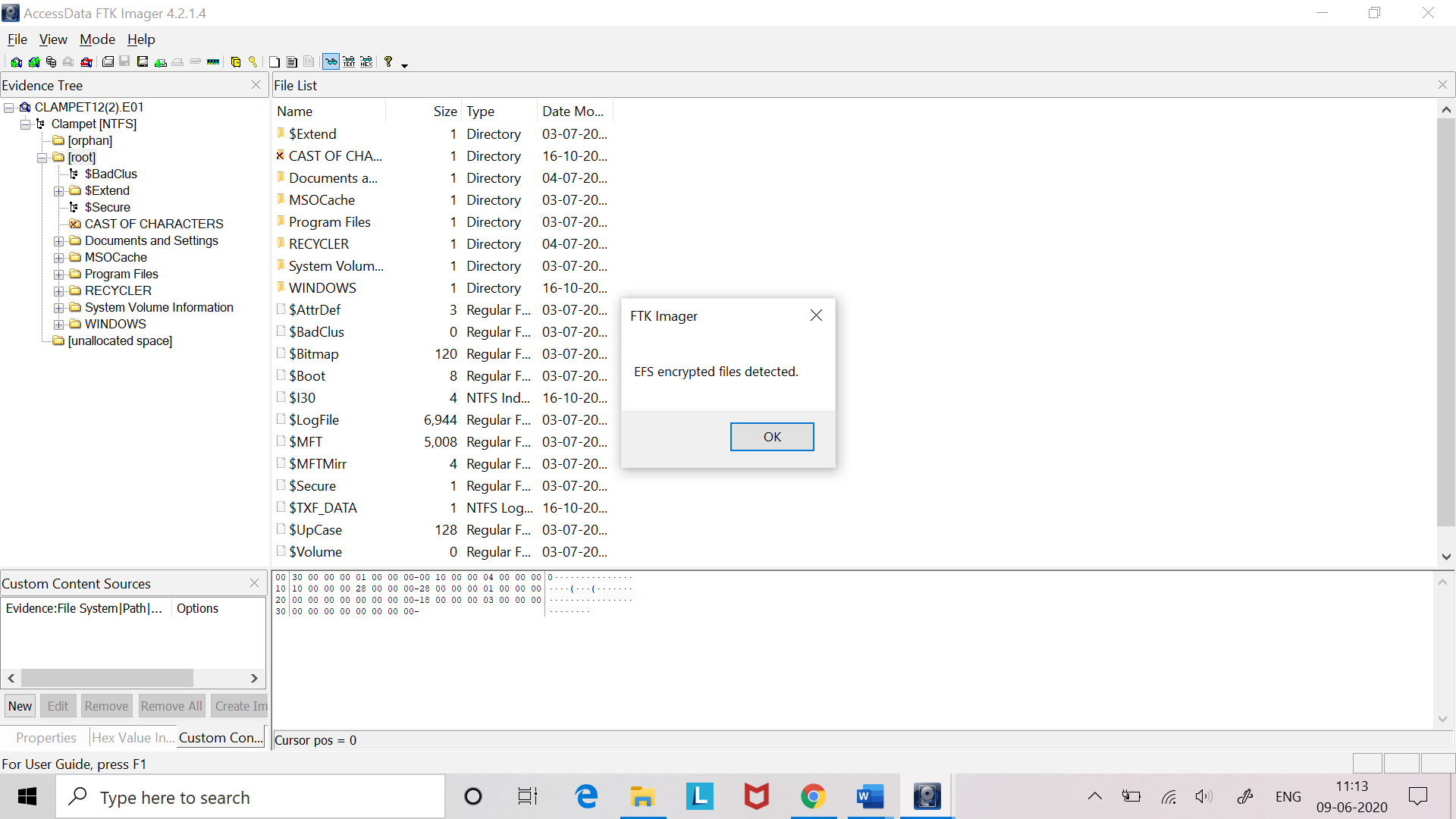
Using Encrypted Images

FTK Imager can work with images that are encrypted with either EFS or AD Encryption.

**Detecting EFs (Encrypting file system) Encryption**

We can check for encrypted data on a physical drive or an image with FTK Imager. To check whether EFS encrypted files are present do one of the following:

* + Click **File > Detect EFS Encryption**.
  + Click the **Detect EFS Encryption** button  on the *Toolbar*.

The program scans the evidence and notifies us if encrypted files are located. EFS Encrypted files are indicated by a key icon, , in the Evidence Tree.

**Note:** This feature does not work with .L01 files.

**AD Encryption**

FTK Imager 3.0 and later has the ability to encrypt data during export to an image. This feature is known as AD Encryption.

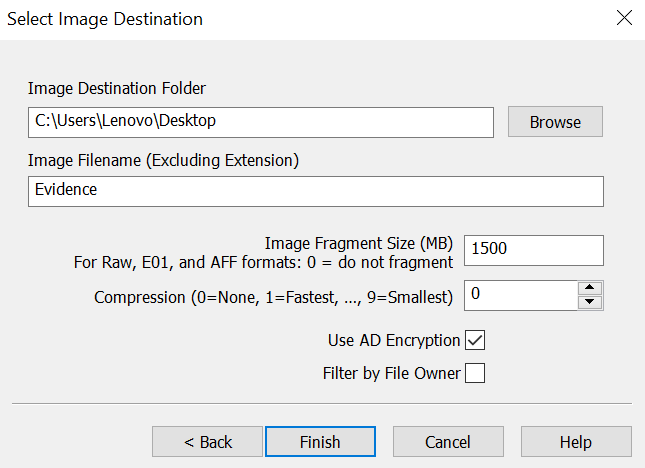
Supported image types are:

* AD1 (AD Custom Content)
* E01 (EnCase Compatible)
* S01 (Smart)
* AFF (Advanced Forensic Format)
* 001 (RAW/DD)

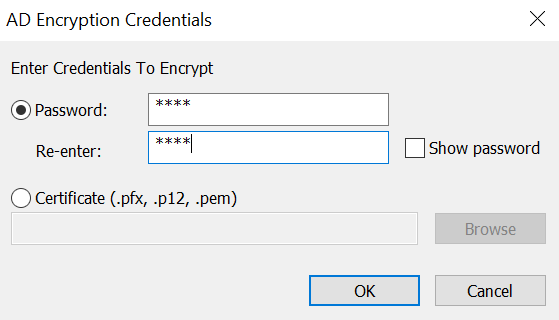
Suppose we want to create a different image of a particular file or folder present in some drive image that is of our interest and needs further investigation. We can encrypt that newly created image file using AD Encryption.

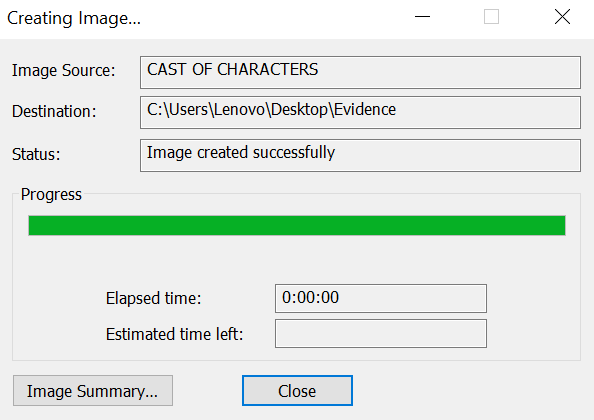
Follow the steps:

1. Go to File> Export Logical image (AD1)
2. Add Image destination folder where to store image file and tick the **Use AD Encryption** check box.
3. Click on **Finish**.



1. Choose whether to encrypt file using a password or a Certificate. And click **OK**.





1. Now, if we add that image as an evidence to FTK Imager. Before adding it, Imager will ask for the AD Encryption credentials. After verifying the credentials, the file will open and we can access that.

