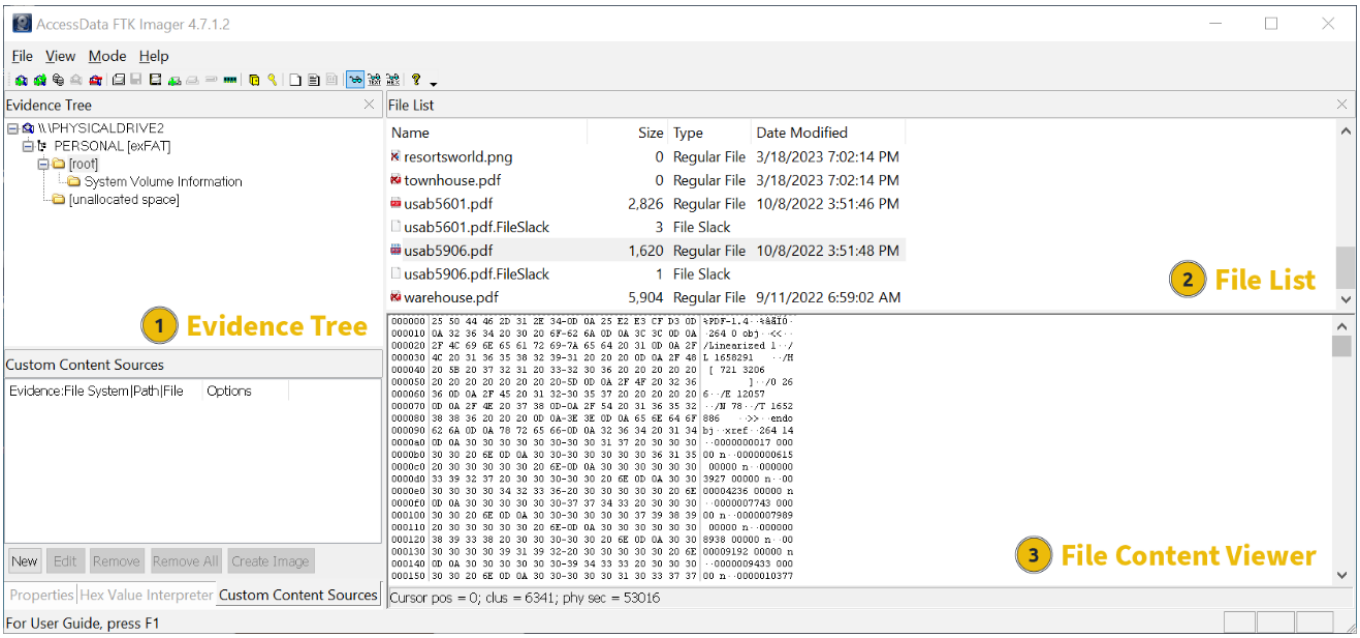
ANANDU R DAS (CB.SC.P2CYS23014)

Description of the tool

FTK Imager, or Forensic Toolkit Imager, is a forensic imaging software . It is commonly used in the field of digital forensics to create forensic images of storage devices such as hard drives, USB drives, and other media. Forensic imaging involves creating a bit-by-bit copy of the entire content of a storage device, ensuring that the original data is preserved for analysis while minimizing any potential changes or damage.

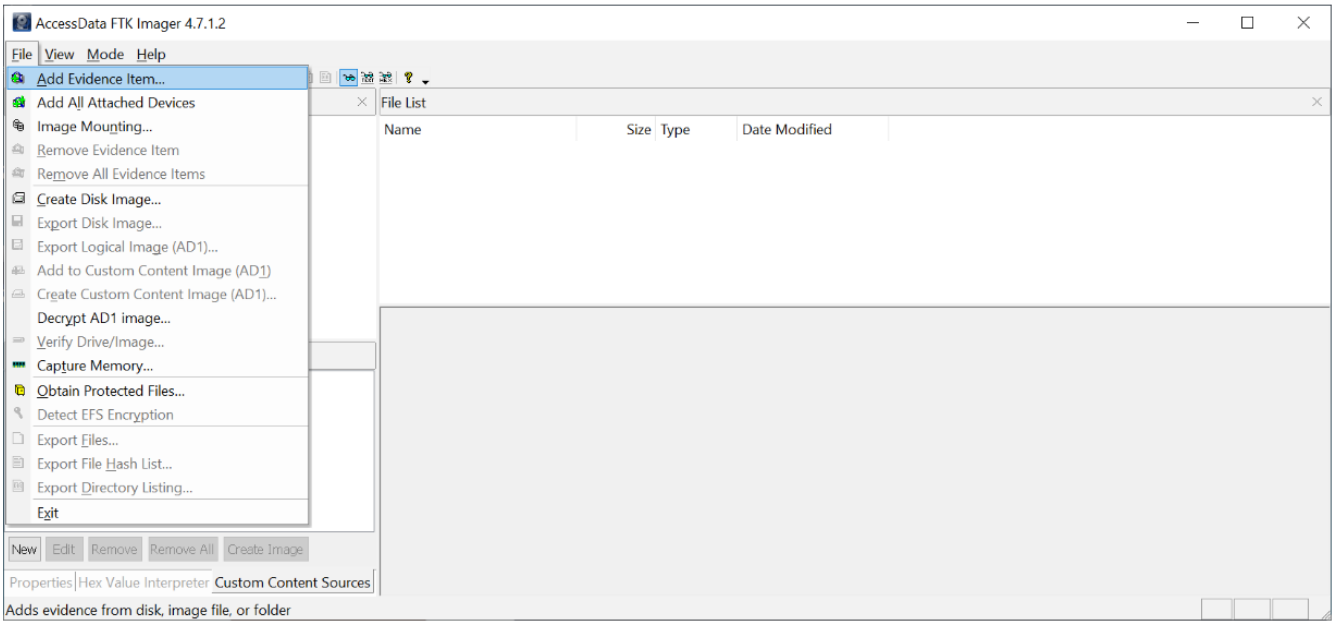
FTK Imager includes vital UI components that are crucial to its functionality. These components are:

- **Evidence Tree Pane**: Displays a hierarchical view of the added evidence sources such as hard drives, flash drives, and forensic image files.
- **File List Pane:** Displays a list of files and folders contained in the selected directory from the Evidence Tree Pane.
- **Viewer Pane:** Displays the content of selected files in either the Evidence Tree Pane or the File List Pane.

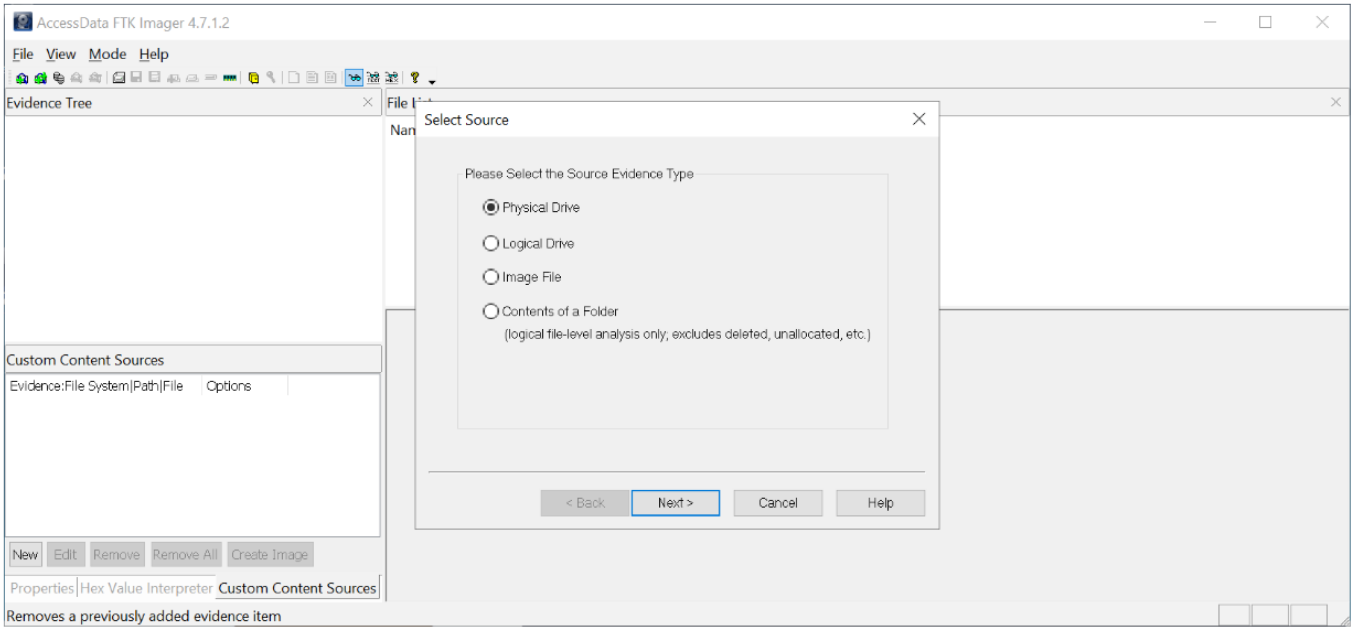


Adding the evidence item

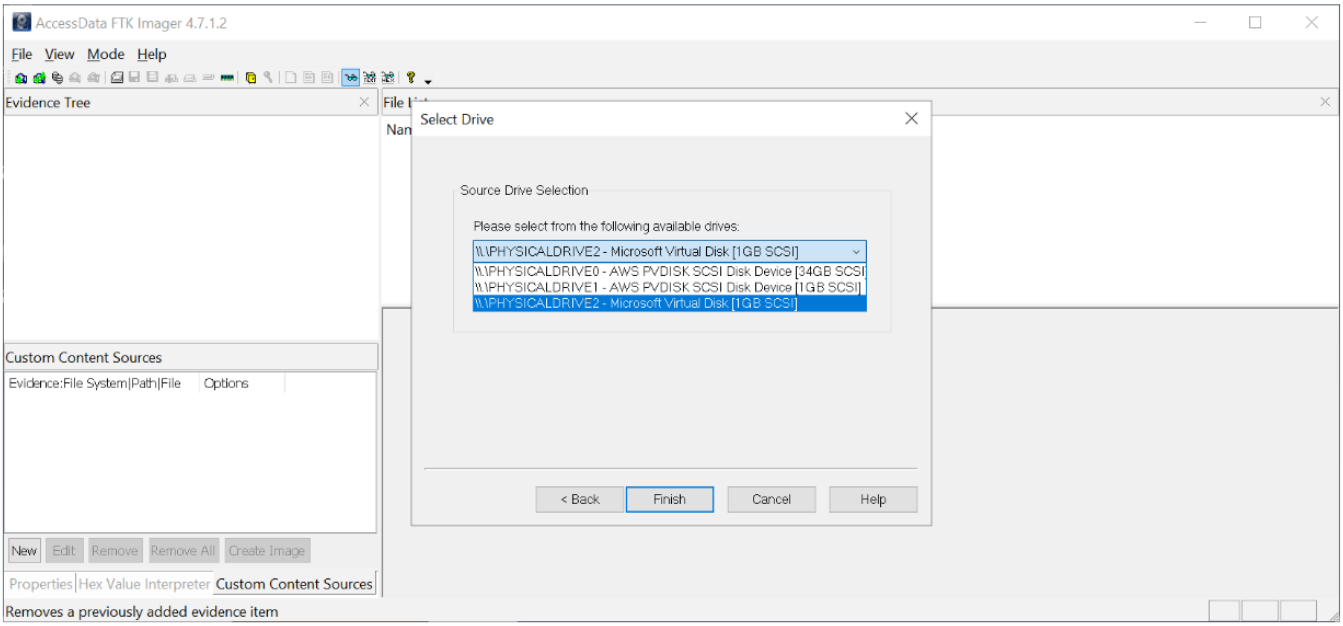
Open **FTK Imager** and navigate to `File > Add Evidence Item`



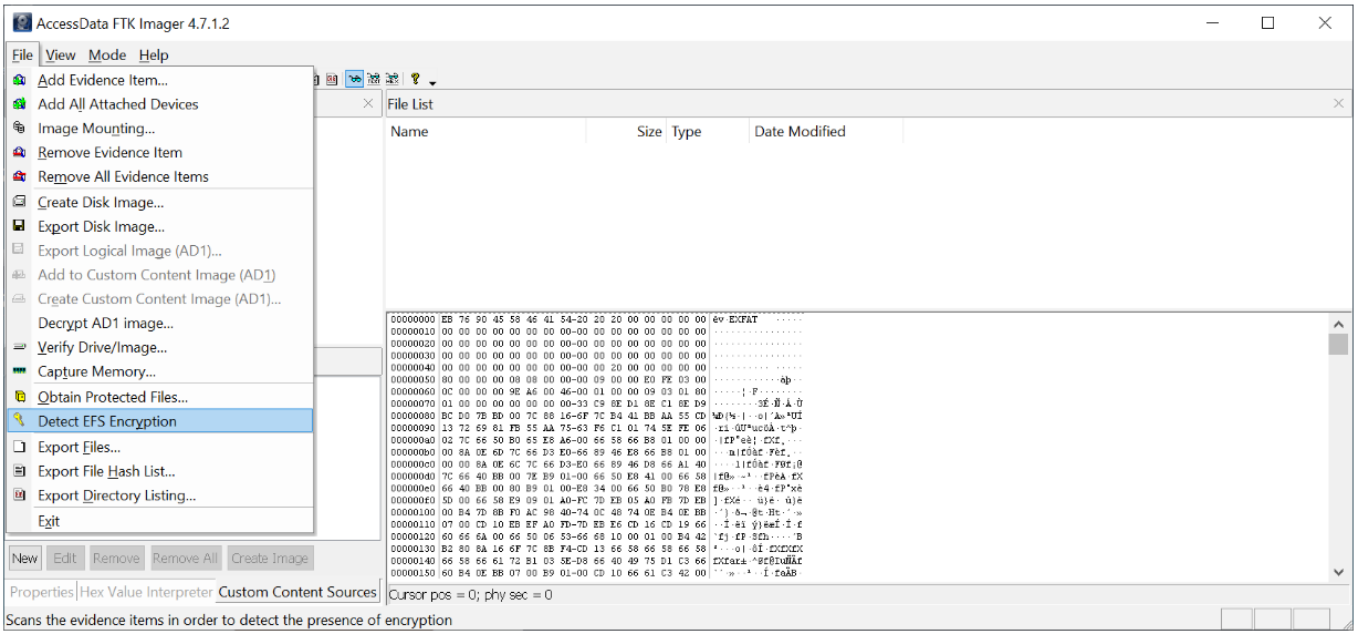
Choose **Physical Drive** on the **Select Source** window, then click **Next**.



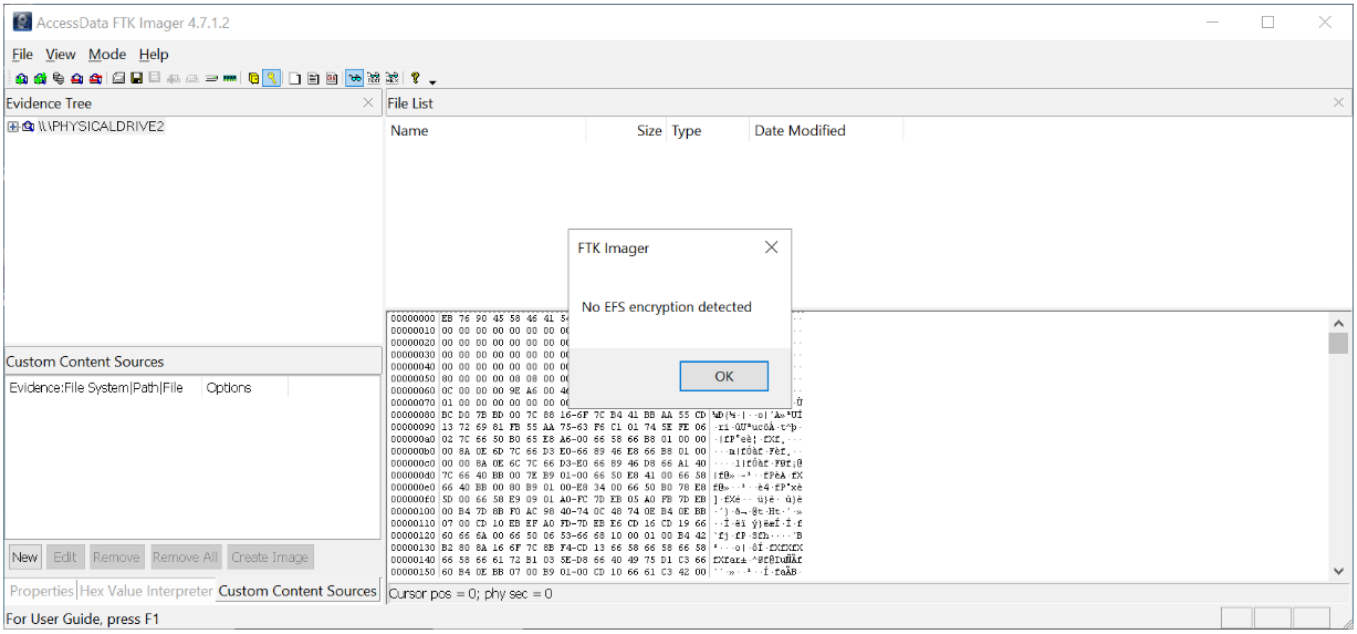
Choose **Microsoft Virtual Disk** (our virtual flash drive) on the **Select Drive** window, then click **Finish**.



Navigate and click `File > Detect EFS Encryption` to scan the drive and detect the presence of encryption.

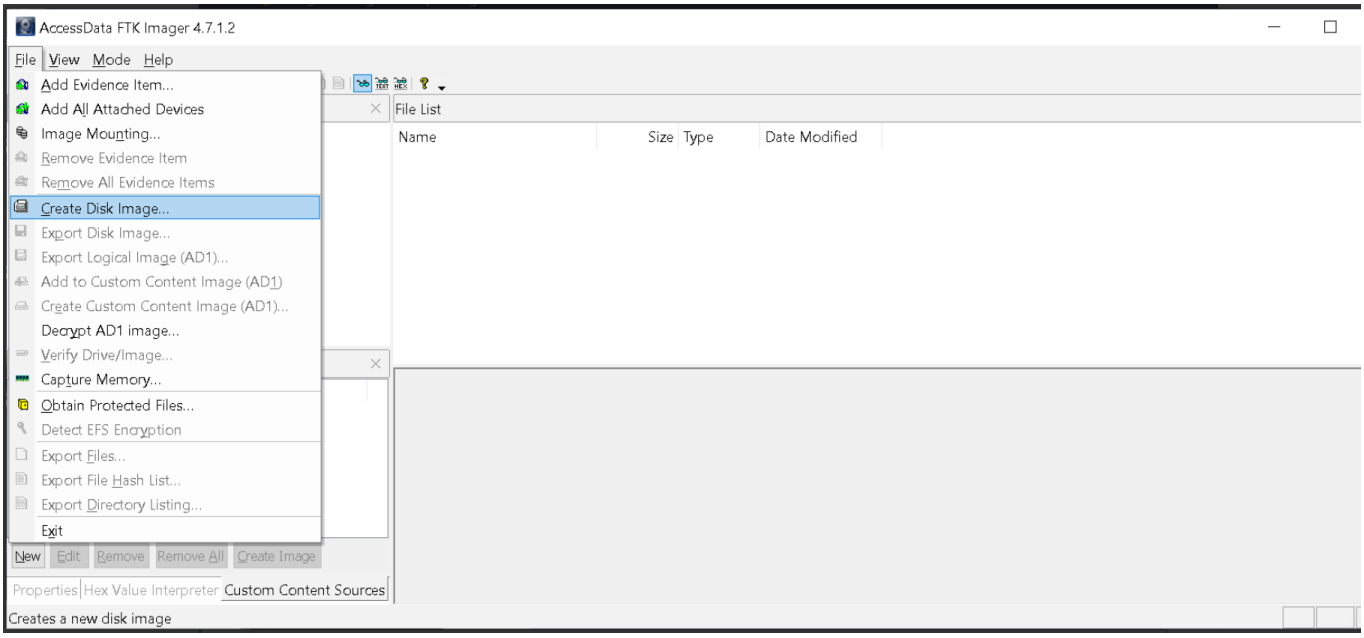


A message box will indicate whether or not EFS encryption is on the attached drive.

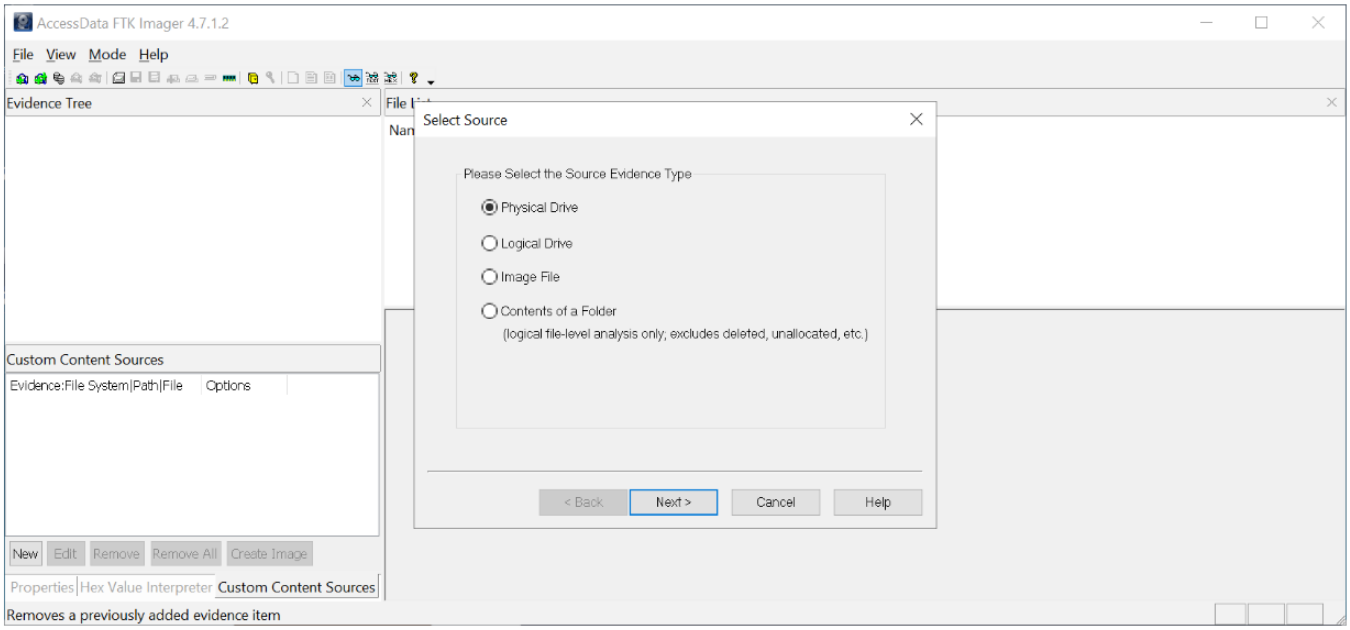


Creating a Forensic Disk Image with FTK Imager

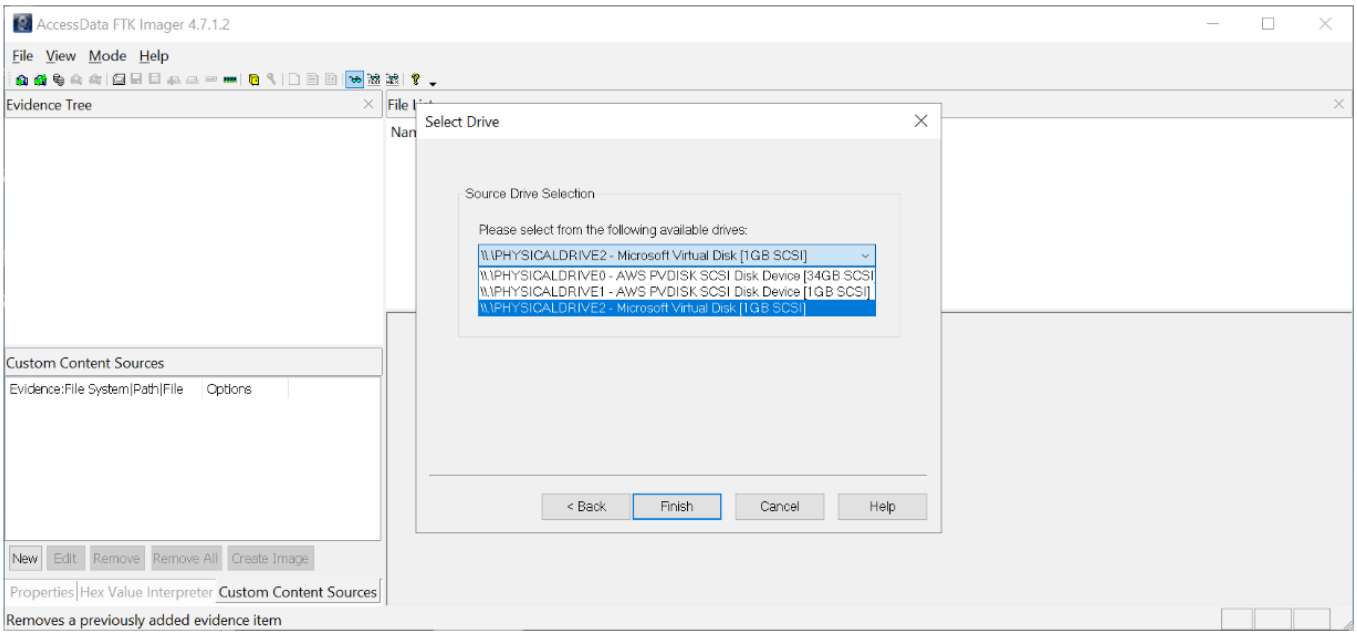
Open **FTK Imager** and navigate to `File > Create Disk Image`



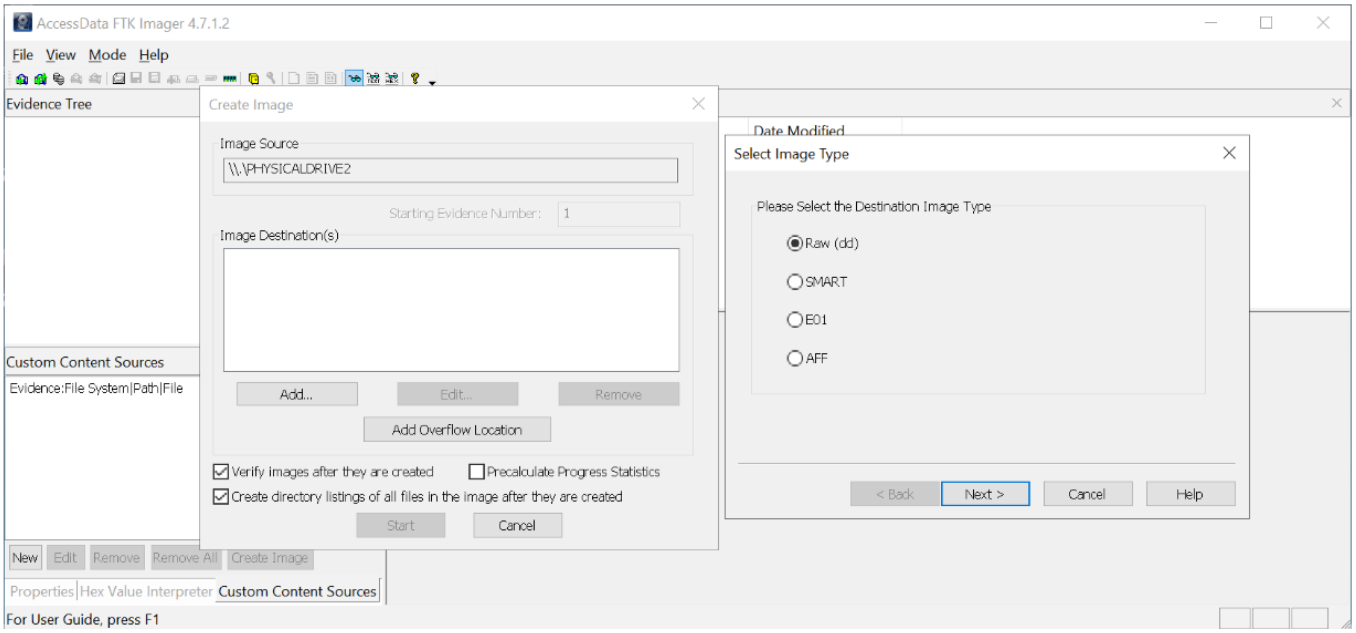
Choose **Physical Drive** on the **Select Source** window, then click **Next**.



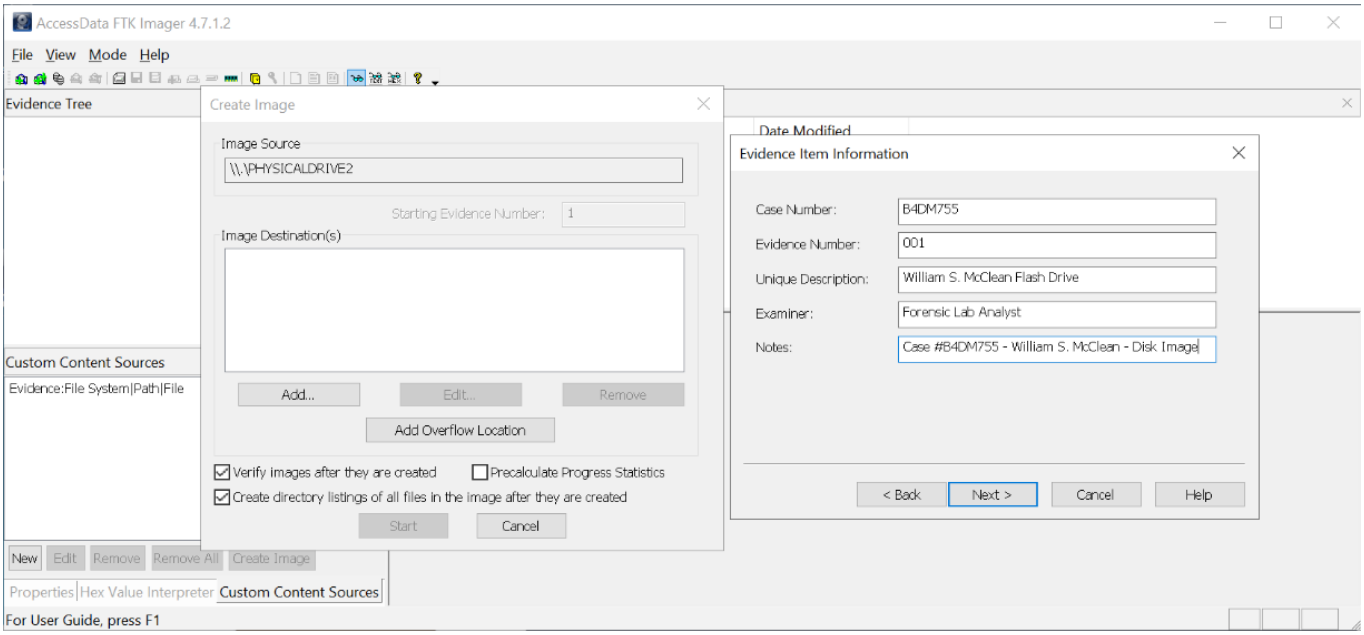
Select the disk to make the image.



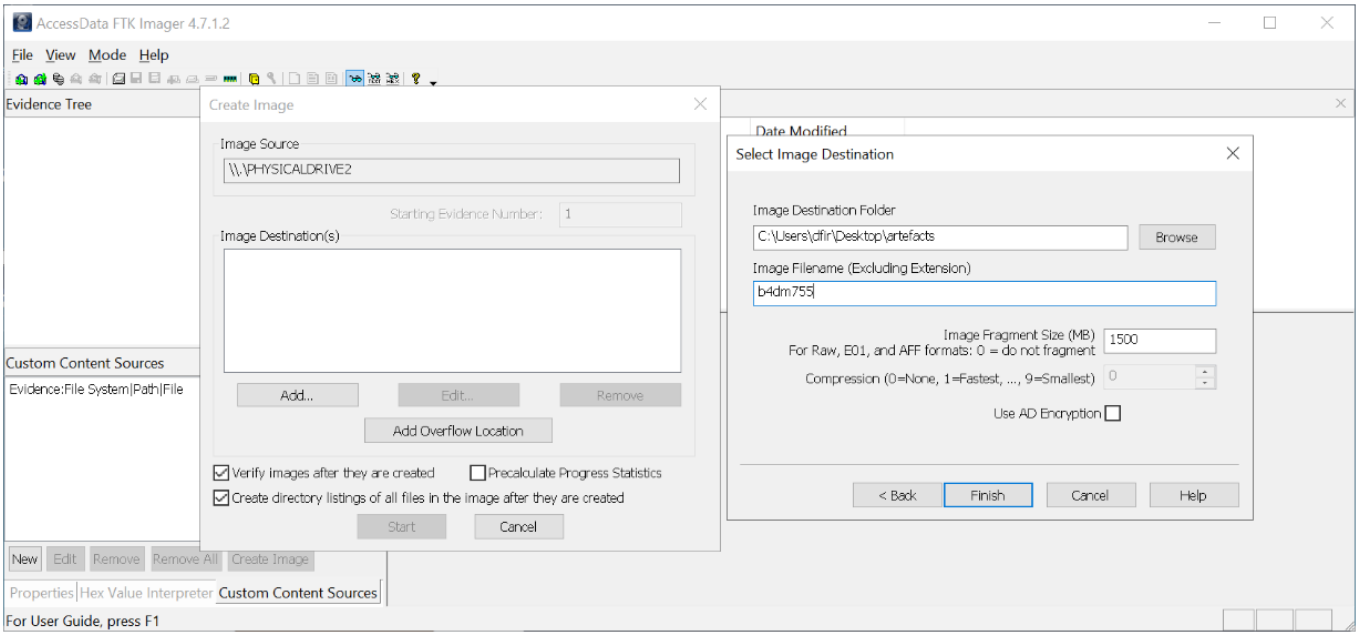
Ensure you check **"Verify images after they are created"** and **"Create directory listings of all files in the image after they are created"** on the **Create Image** window. Press **Add** to open the **Select Image Type** window, choose **Raw (dd)**, then click **Next**.



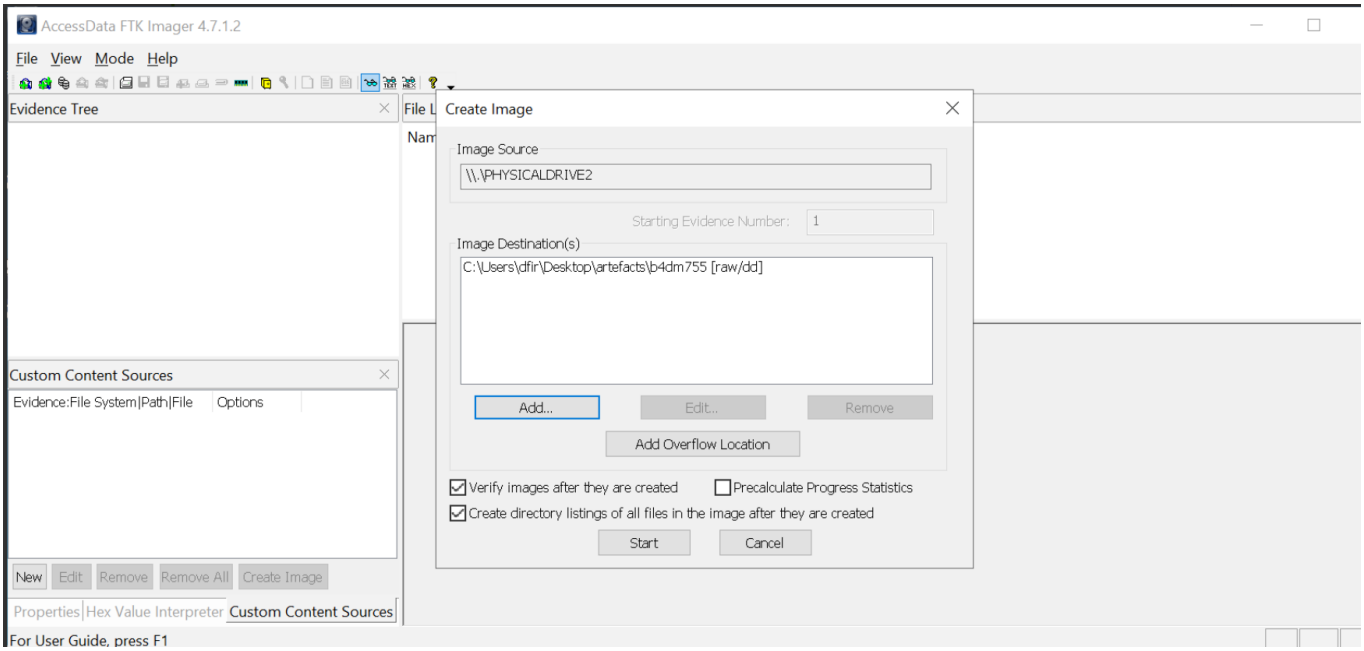
Enter case details in the **Evidence Item Information** window, then click **Next**.

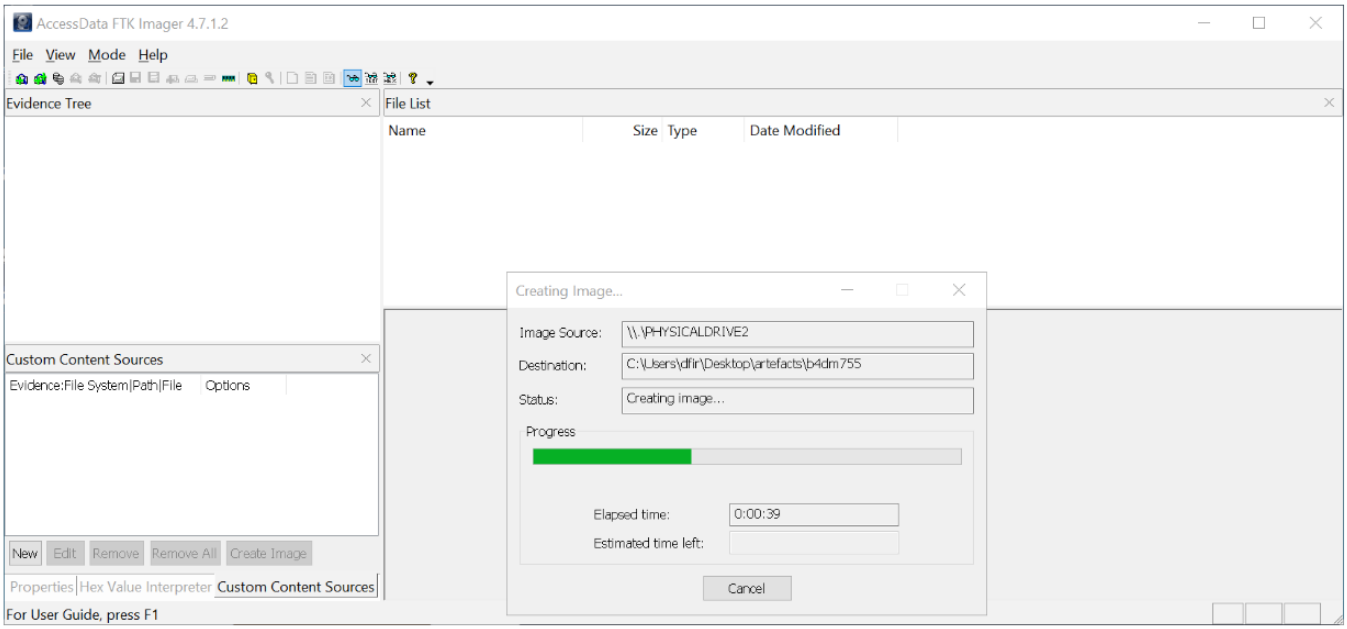


Enter the **Image Destination Folder** and **Image Filename**, then click **Finish**.



Press **Start** to begin creating the *forensic disk image*.





It will start building the disk image after that we can analyze the content of the disk.