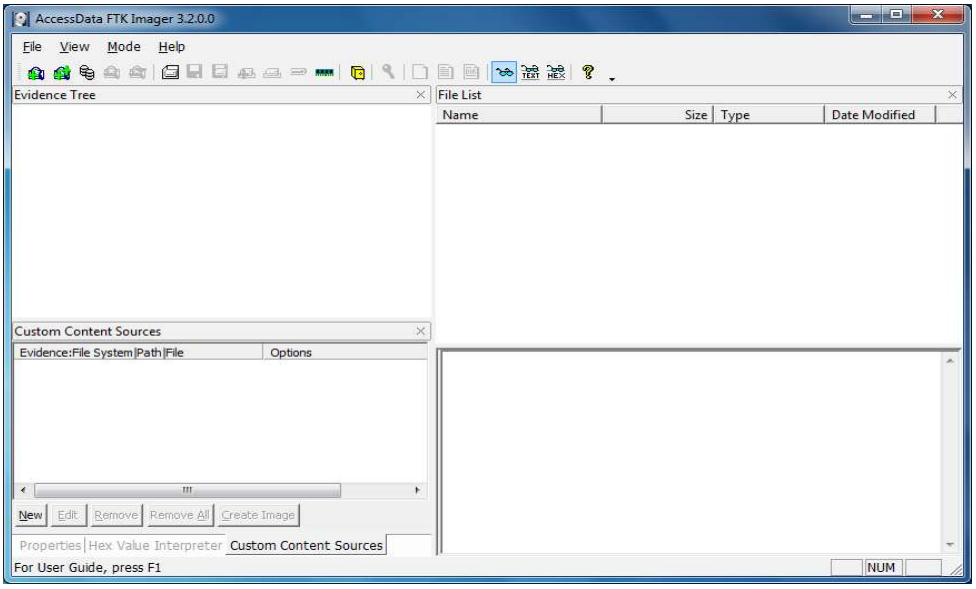
PRACTICAL NO. 04

Using File Recovery Tools [FTK Imager] Creating Image

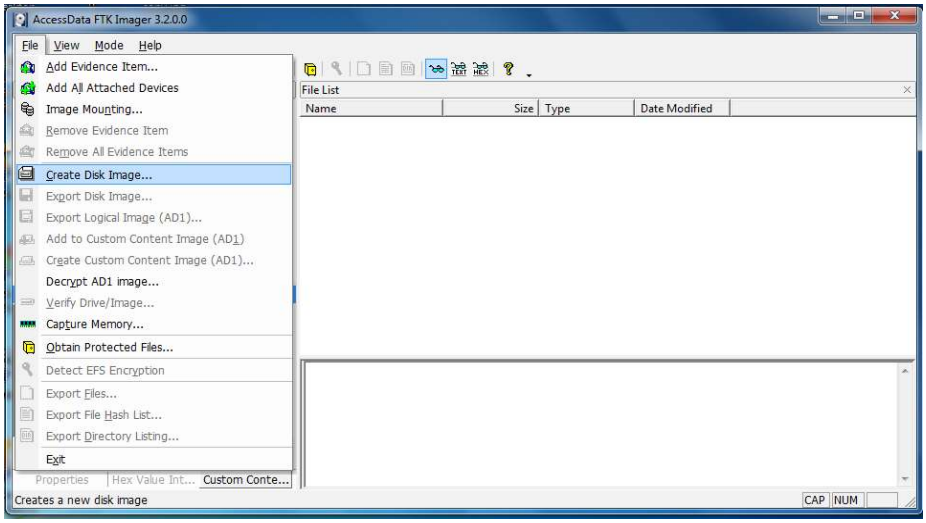
Aim: Understanding & working with the process of the process of taking a drive image using AccessData's FTK Imager tool.

Step 1) Run **FTK Imager.exe** to start the tool.



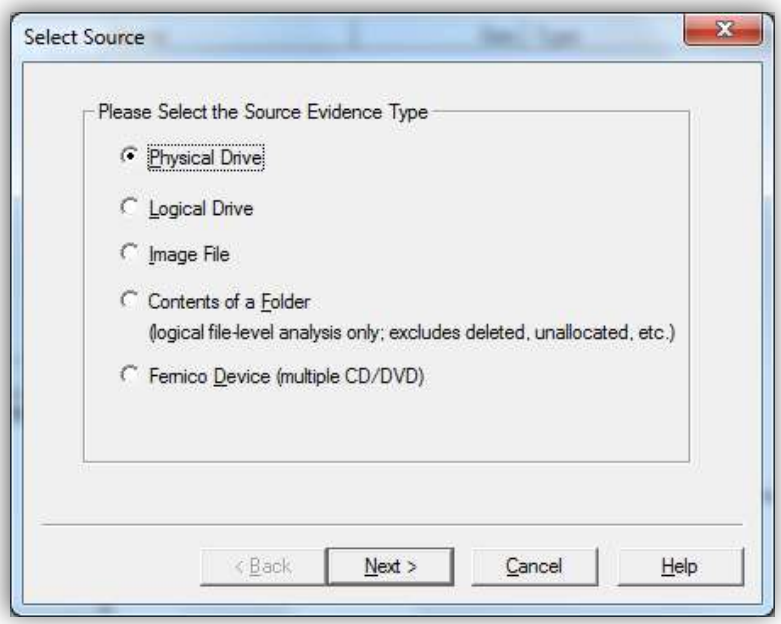
Step 2) To create a forensic image:

Click File > Create Disk Image

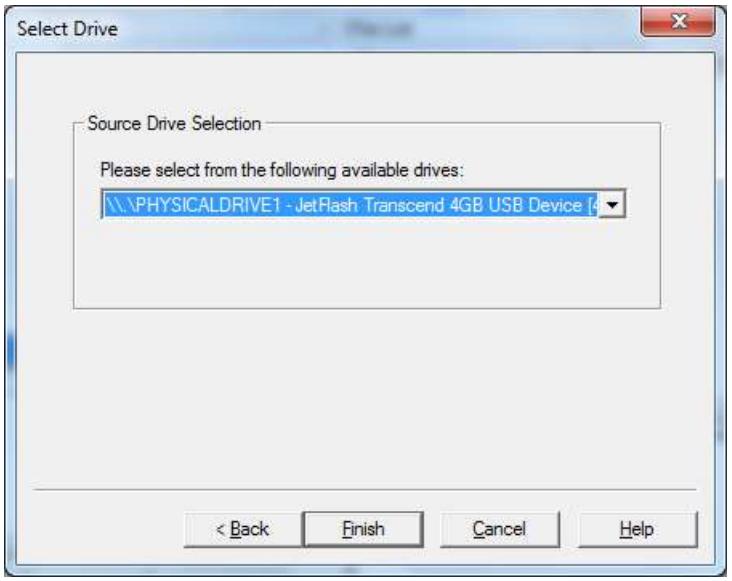


Step 3) In the Select Source dialog box, select the source you want to make an image of. Click Next.

If you select Logical Drive and need to select a floppy or CD as a source, you can check the Automate multiple removable media box to create groups of images. Imager will automatically increment the case numbers with each image, and if something interrupts the process, you may assign case number manually.



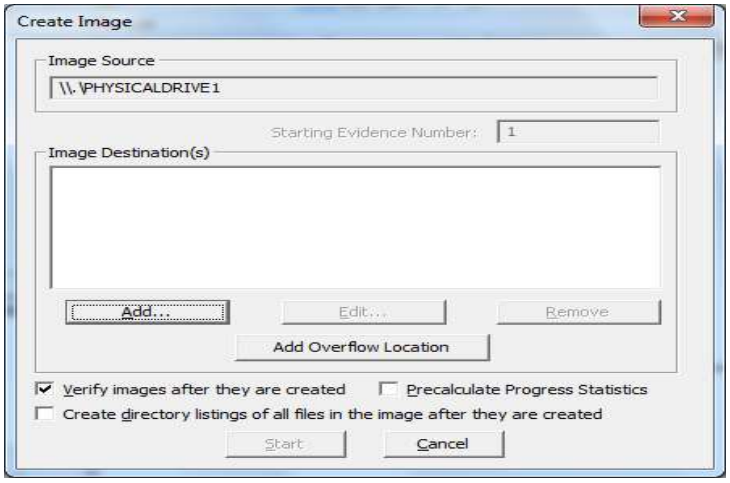
Step 4) Select the drive or browse to the source of the image you want, and then click Finish.



Step 5) In the Create Image dialog, click Add**...** to add the image destination.

- Compare the stored hashes of your image content by checking the Verify images after they are created box. If a file doesn't have a hash, this option will generate one.

List the entire contents of your images with path, creation dates, whether files were deleted, and other metadata. The list is saved in tab-separated value (.TSV) format.

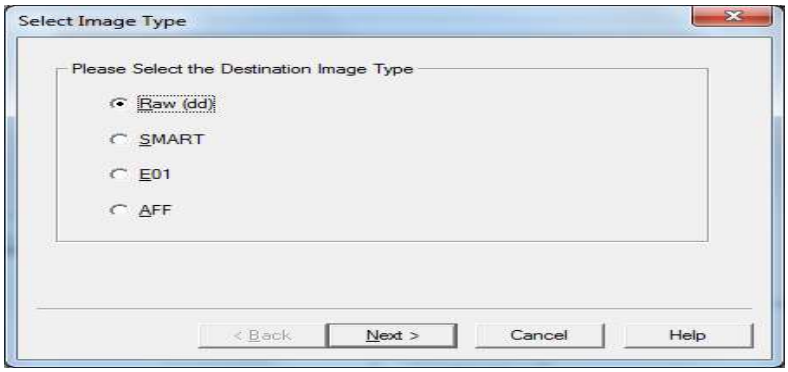


Step 6) Select the type of image you want to create.

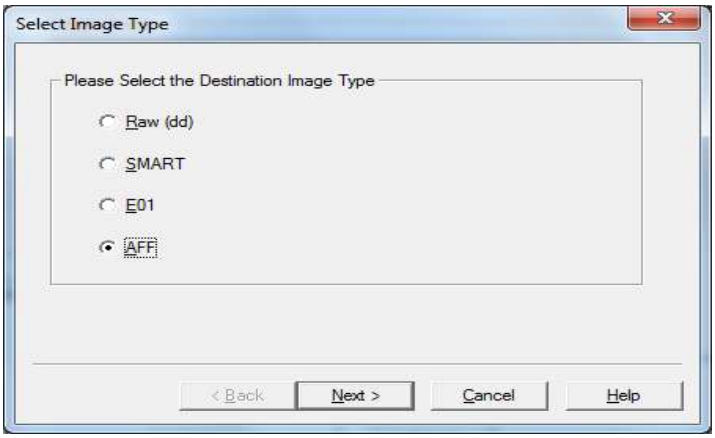
The type you choose will usually depend on what tools you plan to use on the image. The dd format will work with more open-source tools, but you might want SMART or E01 if you will primarily be working with ASR Expert Witness or EnCase, respectively.

Note: If you are creating an image of a CD or DVD, this step is skipped because all CD/DVD images are created in the IsoBuster CUE format. Hashes are not generated for CD and DVD images so they will not be verified, as well.

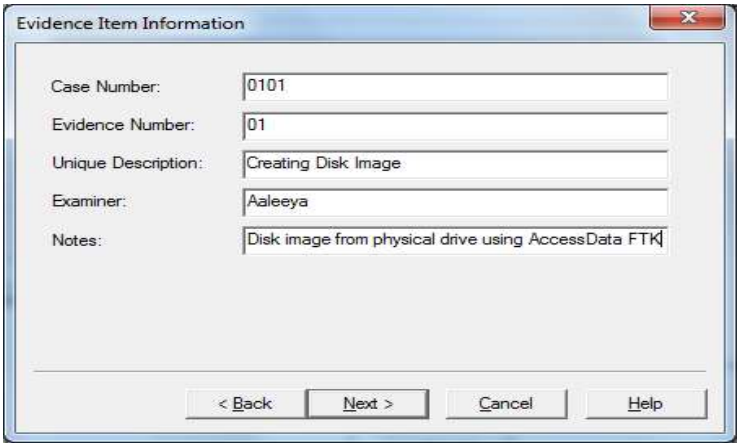
Important: The raw image type is not compressed. If you select the Raw (dd) type, be sure to have adequate available drive space for the resulting image.



Step 7) If you are creating an AFF image type, choose AFF. Click Next.
The Image Destination Folder dialog box you see will be different than that seen when selecting any other image type



Step 8) If your version of FTK requests evidence information, you can provide it. Specify Evidence Item Information. All Evidence Item Information is optional, but it is helpful to have the information easily accessible in case it is called into question at any time after creation



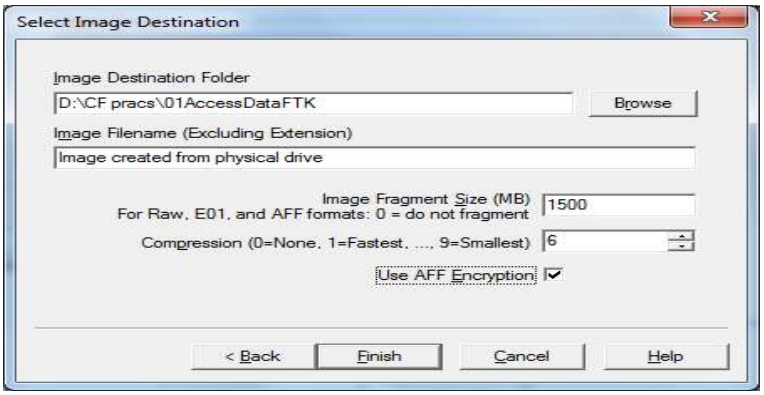
Complete the fields in the Evidence Item Information dialog. Click Next.

Step 9) Select the Image Destination folder and file name. You can also set the maximum fragment size of image split files. Click Finish to complete the wizard.

In the Image Destination Folder field, do one of the following:

- Type the location path where you want to save the image file.
- Click Browse to find and select the desired location.

In the Image Filename field, specify a name for the image file but do not specify a file extension.



Step 10) Specify the Image fragment Size:

- Default Image Fragment Size = 1500 MB
- To save images segments that can be burned to a CD, specify 650 MB.
- To save image segments that can be burned to a DVD, specify 4000 MB.
- The .S01 format is limited by design to sizes between 1 MB and 2047 MB (2 GB). Compressed block pointers are 31-bit numbers (the high bit is a compressed flag), which limits the size of any one segment to two gigabytes.

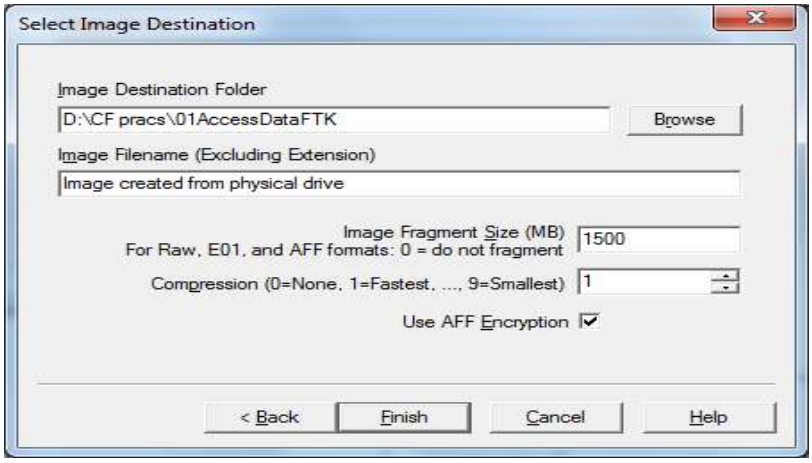
Step 10 a) Select the compression level to use.

- 0=No Compression
- 1=Fastest, Least Compression (faster, and also slightly smaller than a 0-compression file)
- 9=Slowest, Most Compression (smallest file, slowest to create).

Numbers between 1 and 9 produce an image with varying levels of compression to speed ratio.

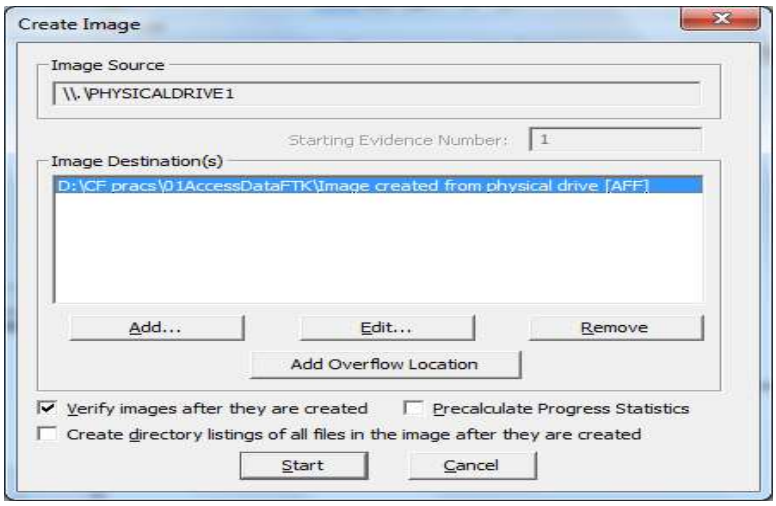
Step 11) To encrypt the image, choose the correct encryption box as explained below:
a. To encrypt the new image with AD Encryption, mark the Use AD Encryption box.
b. To encrypt the new image with AFF Encryption, mark the Use AFF Encryption box.

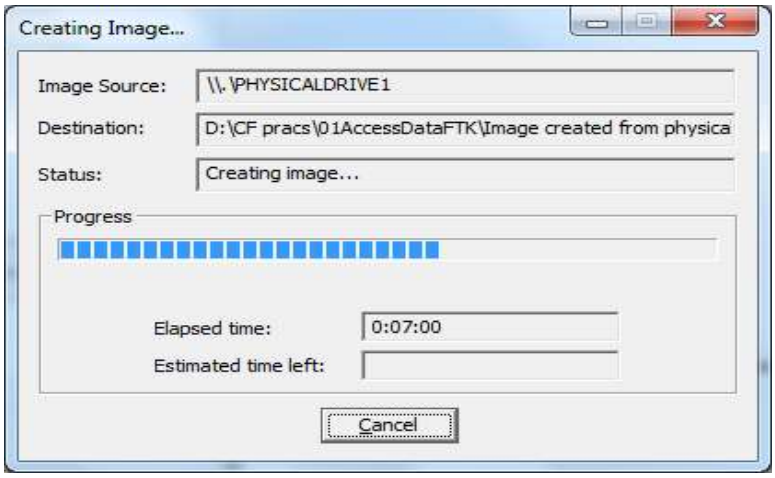
Step 12) Click Finish.



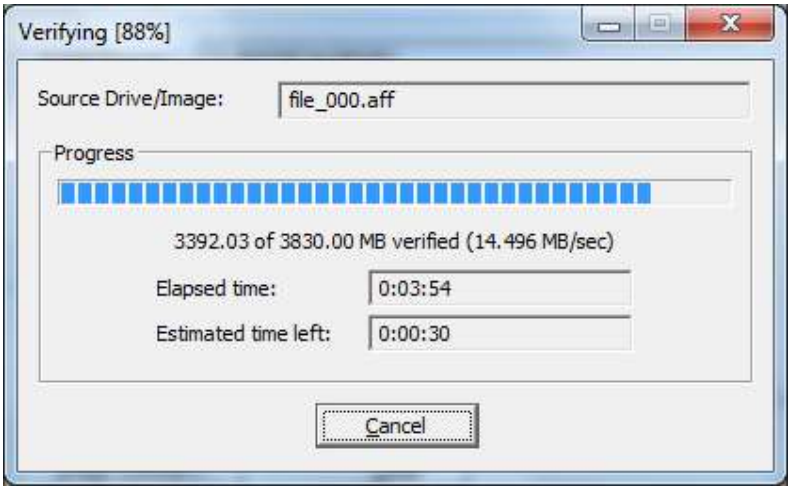
Step 13) When AFF Encryption is selected, type the password, and retype the password to confirm. Click Show Password to see that you have typed it correctly the first time.

Step 14) When encryption selections are made, click **OK** to save selections and return to the **Create Image dialog.** Click **Start** to begin the imaging process.

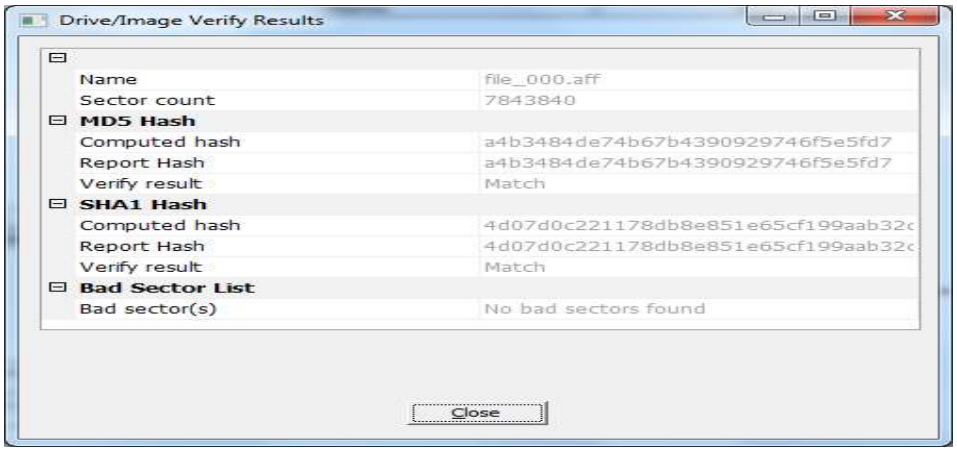


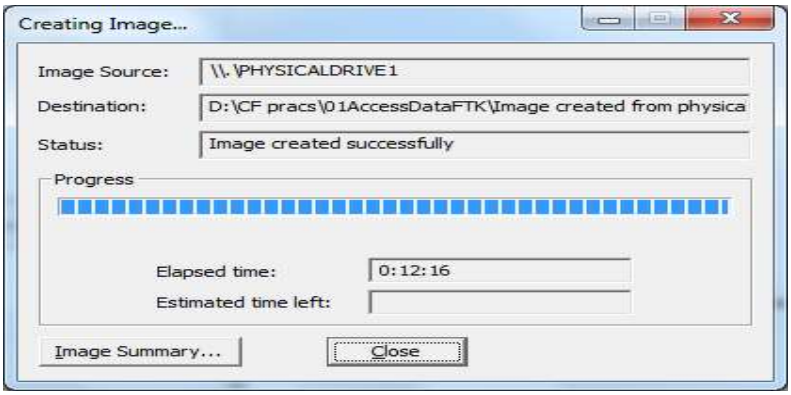


After the images are successfully created, the Drive/Image Verify Results box shows detailed image information, including MD5 and SHA1 check sums, and bad sectors.



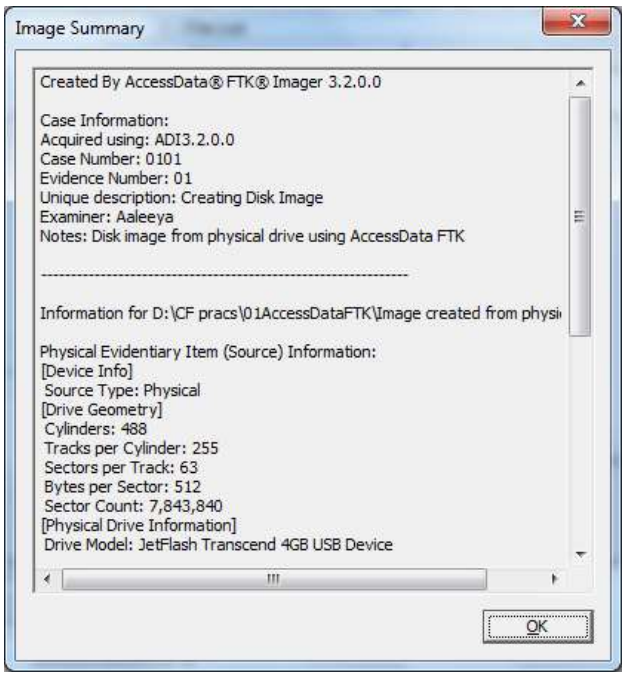
Now is a good time to refill that coffee cup! Once the acquisition is complete, you can view an image summary and the drive will appear in the evidence list in the left-hand side of the main FTK Imager window. You can right-click on the drive name to Verify the Image:

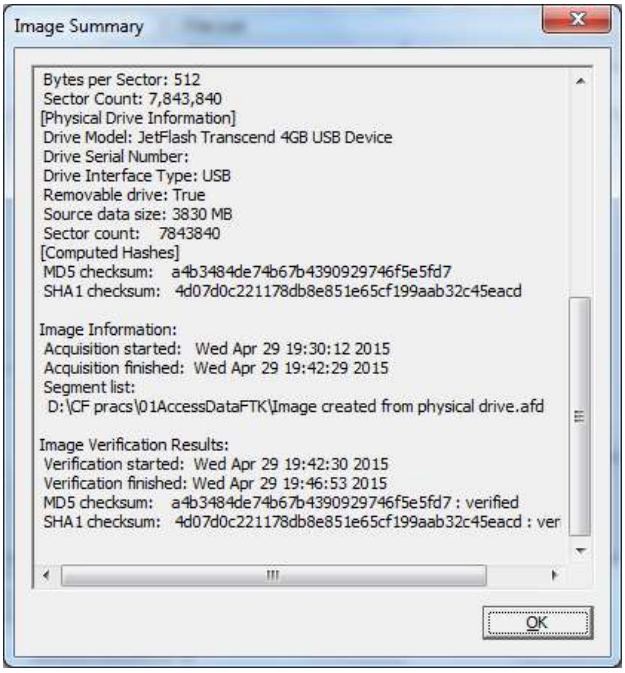




A progress dialog appears that shows the following:

- The source that is being imaged
- The location where the image is being saved
- The status of the imaging process
- A graphical progress bar
- The amount of data in MB that has been copied and the total amount to be copied
- Elapsed time since the imaging process began
- Estimated time remaining until the process is complete
- Image Summary button. Click it to open the Image Summary window as shown below:

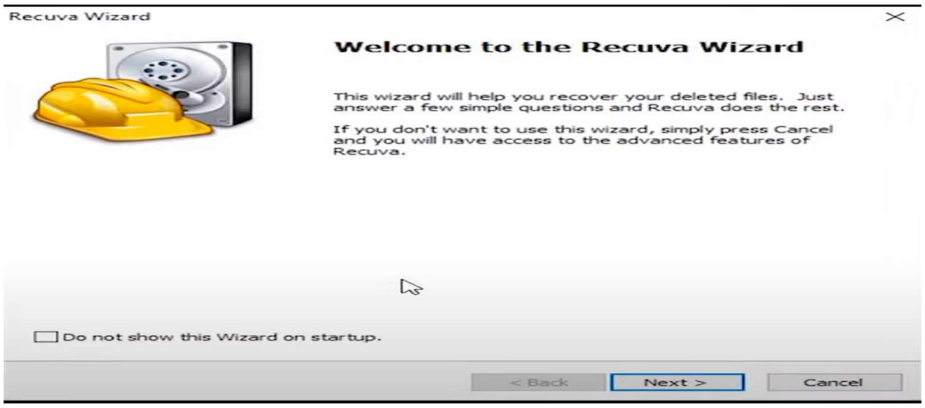




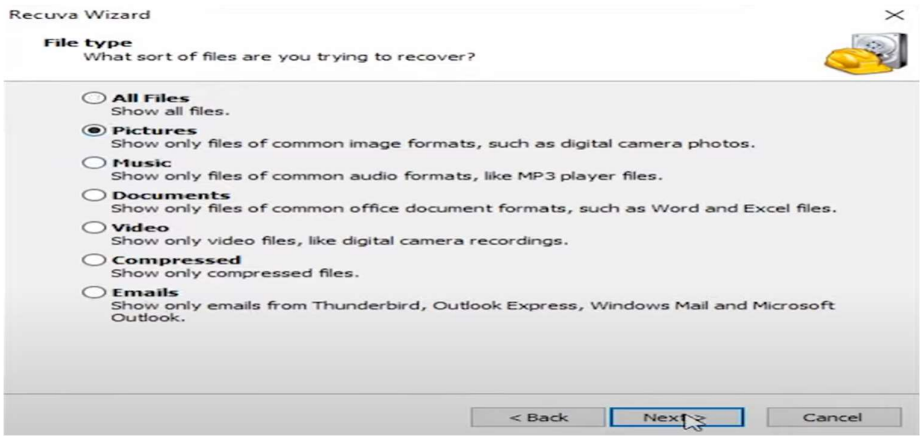
b. Recover Deleted files using Recuva, PC Inspector File Recovery, Recover My Files

Recuva

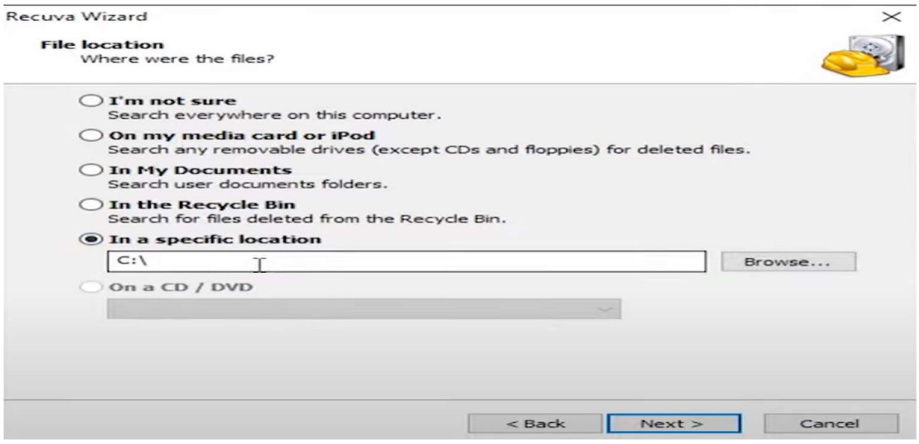
Download and install **Recuva**



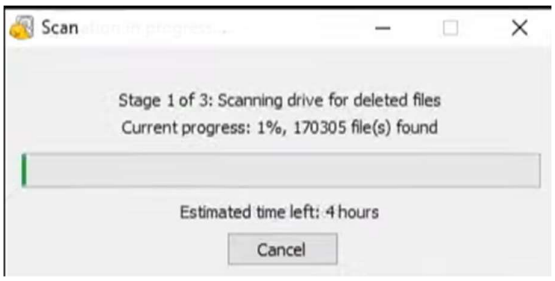
Select File Type you need to recover

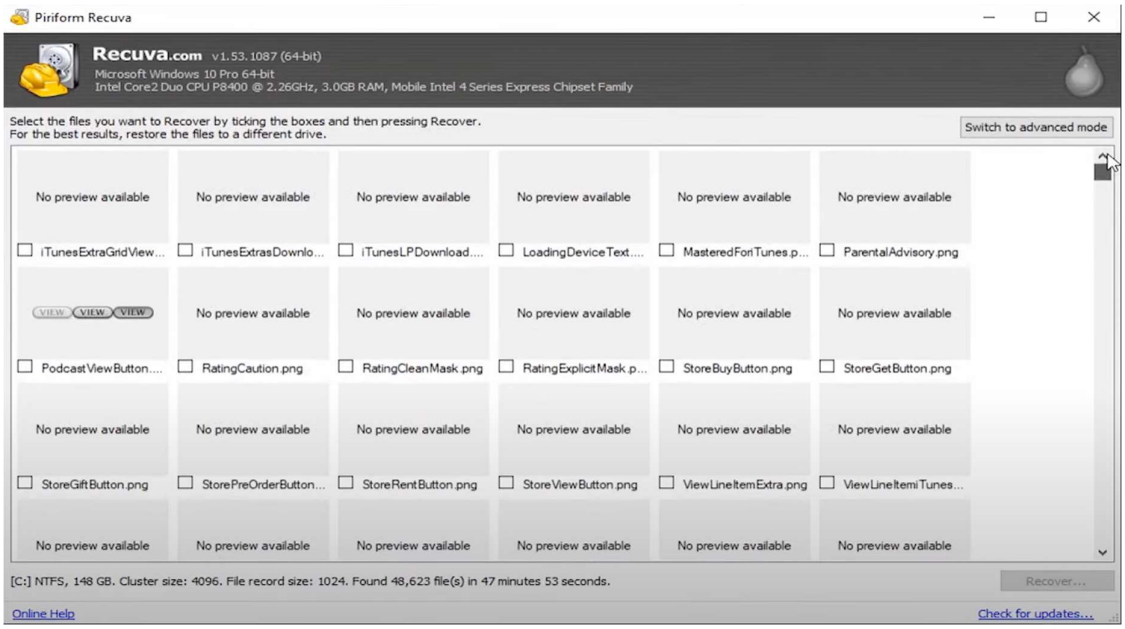


Select File location, which you want to recover files

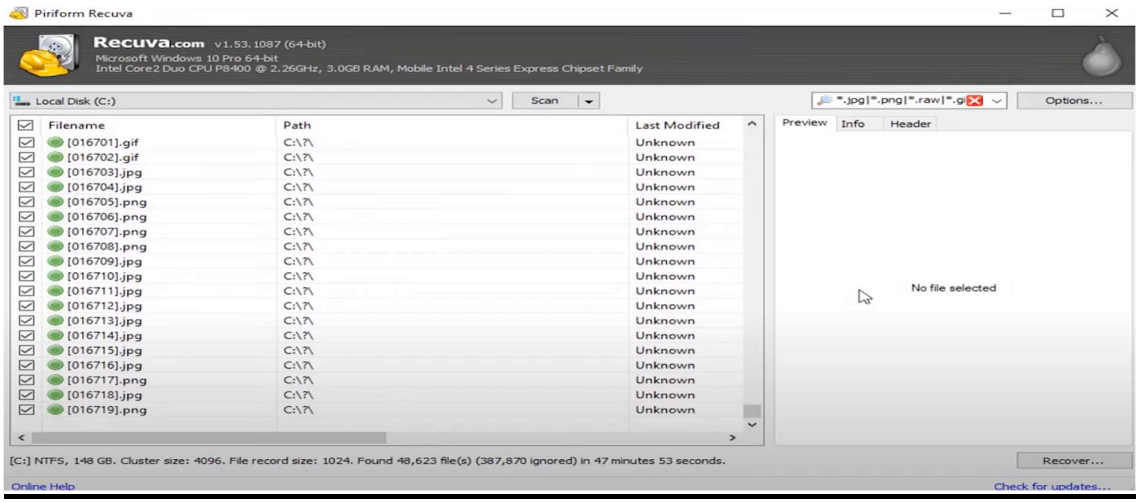


Click next (If want enable Deep Scan)

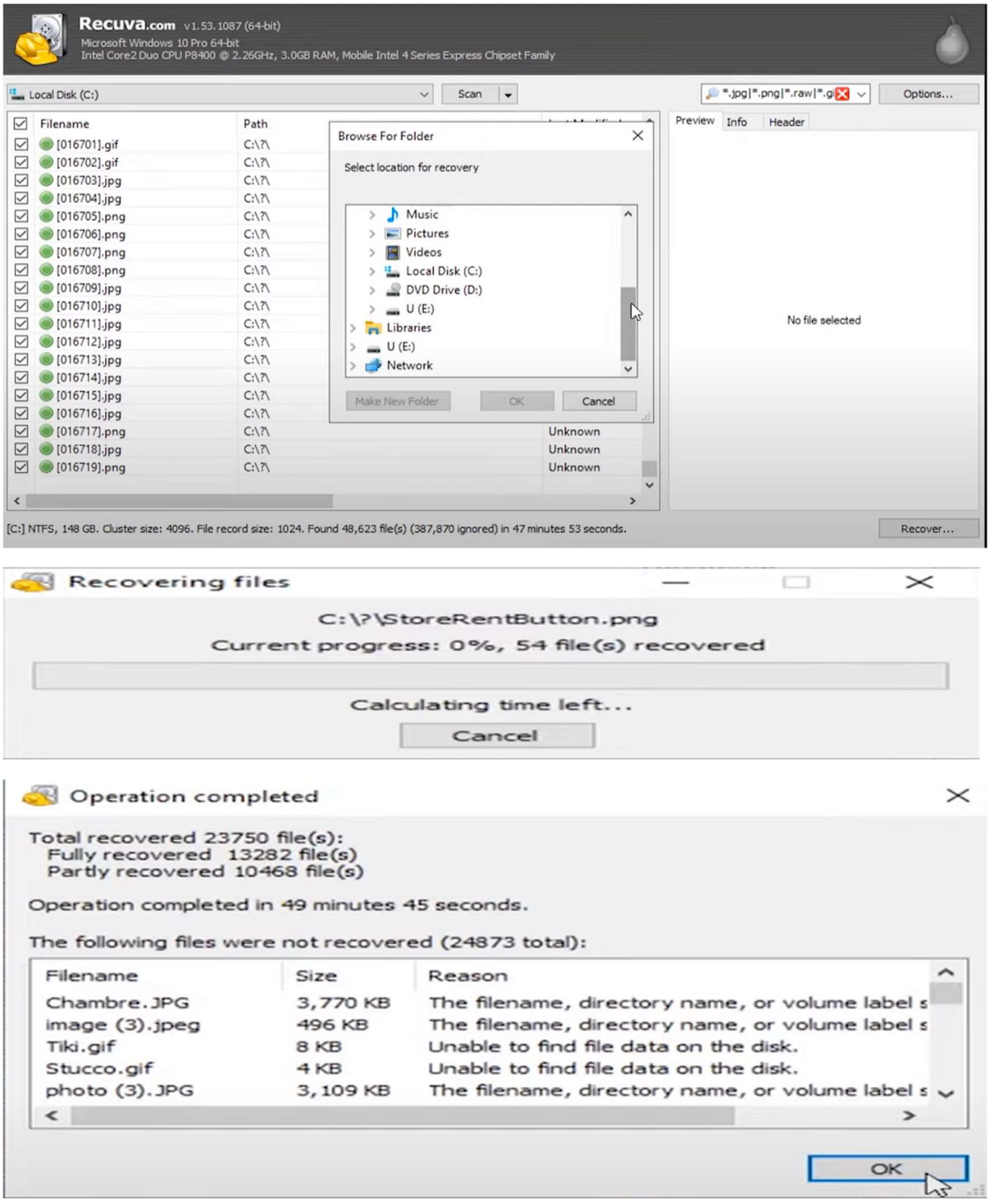




Switch to advanced mode and select all recover file



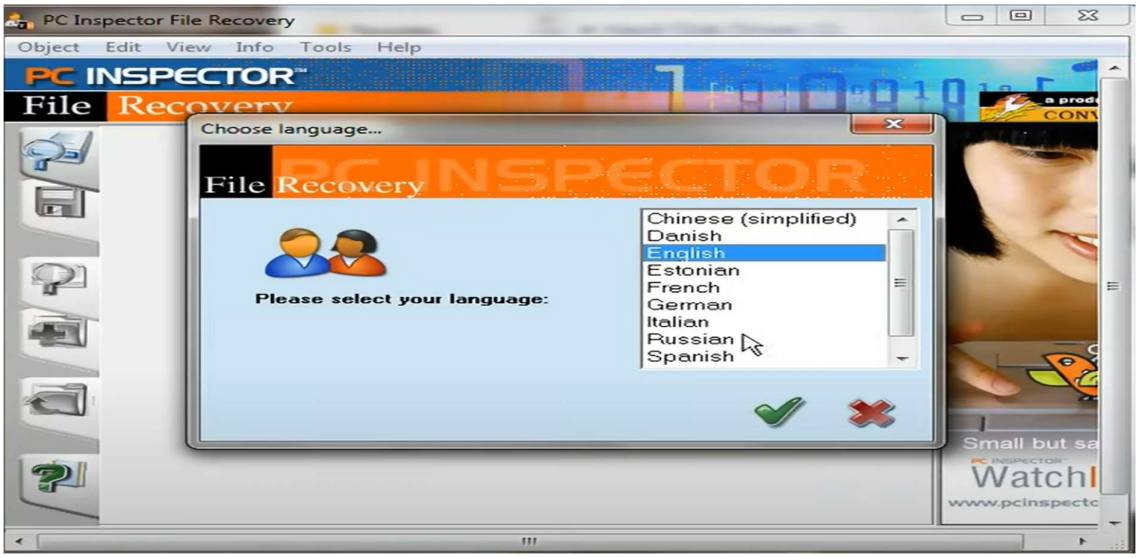
Select the location were to recover the file



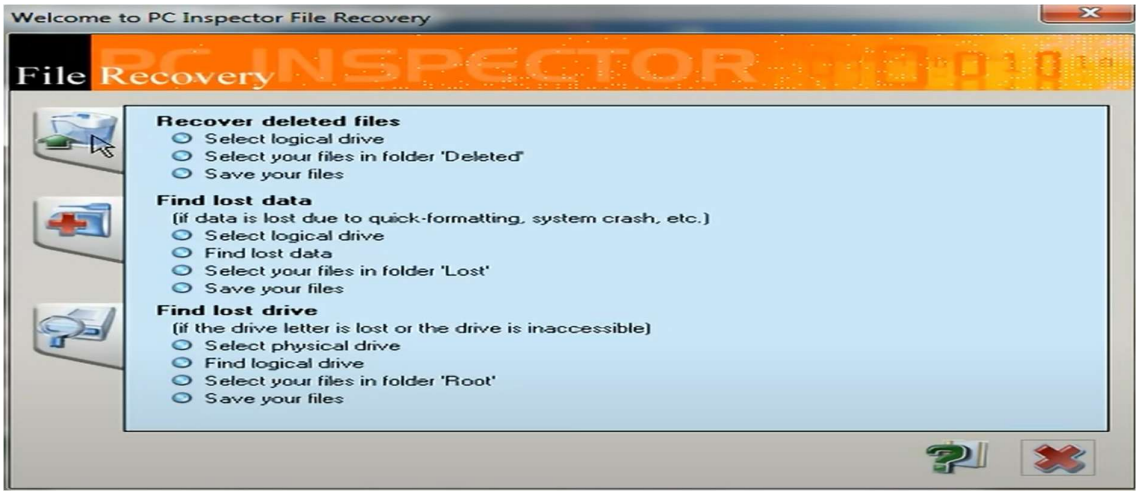
All deleted Files are recovered at specified location

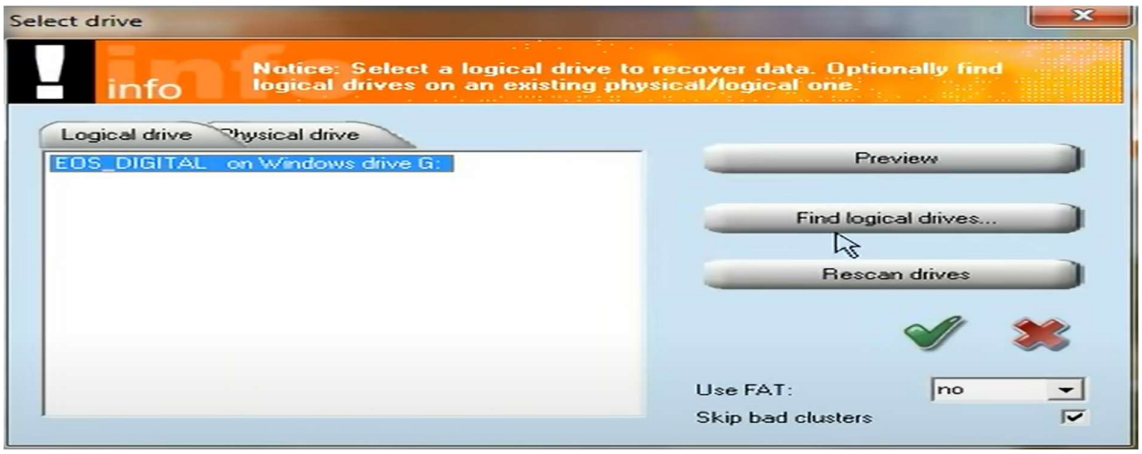
PC Inspector File Recovery

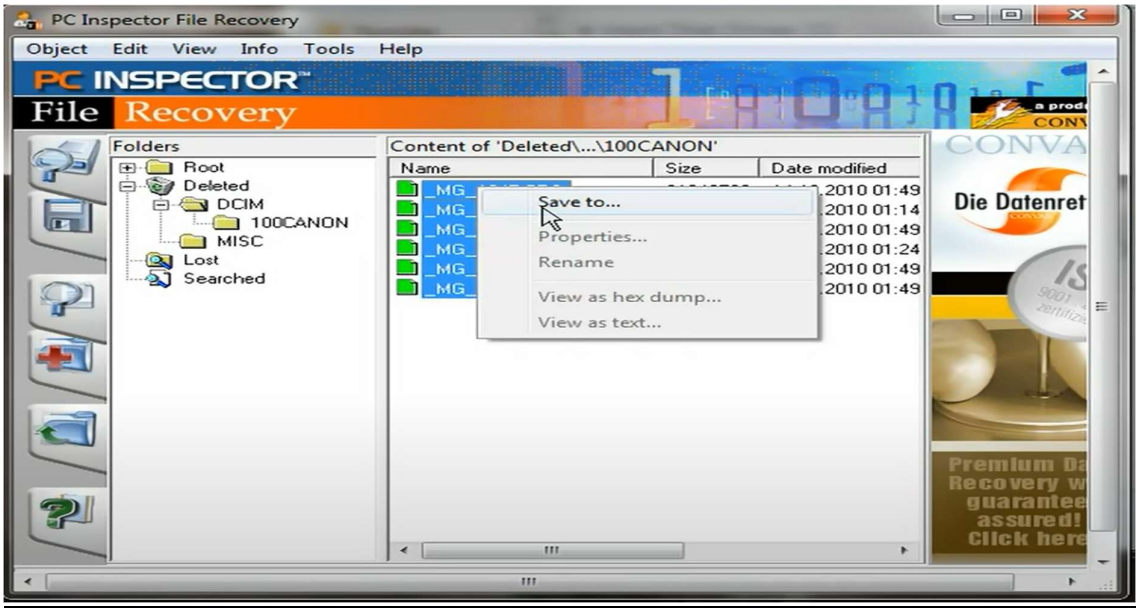
Download and install **PC Inspector File Recovery**

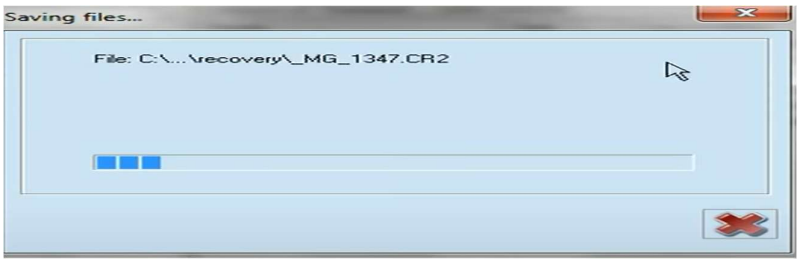


Choose what to recover delete files, lost data or lost drive

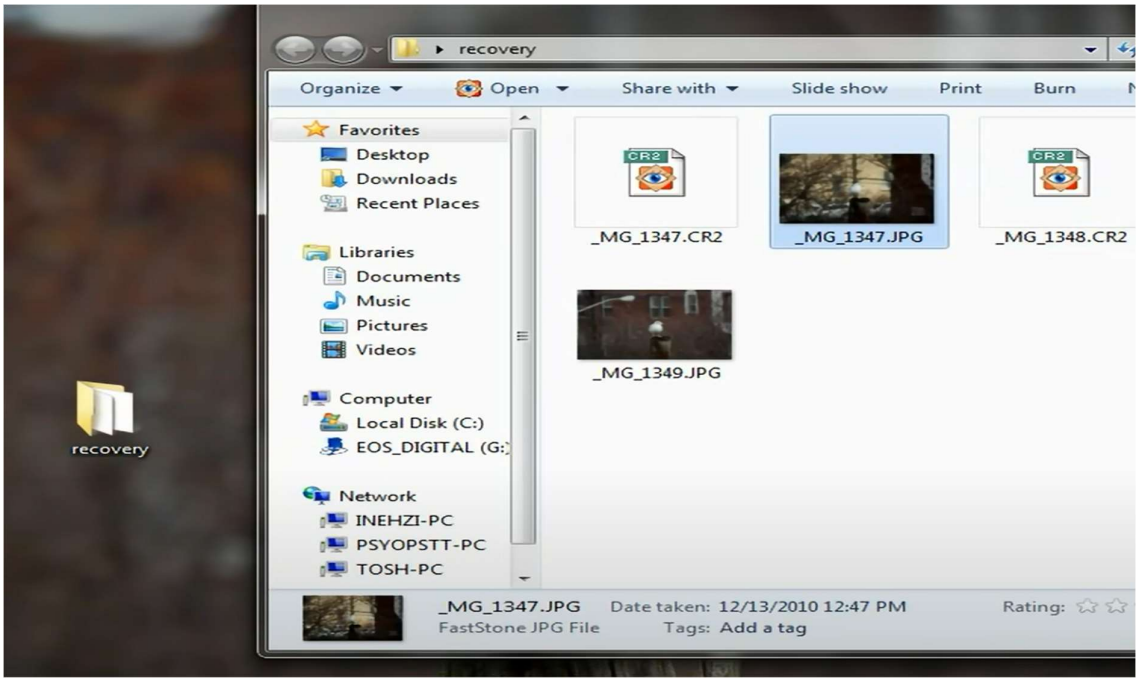






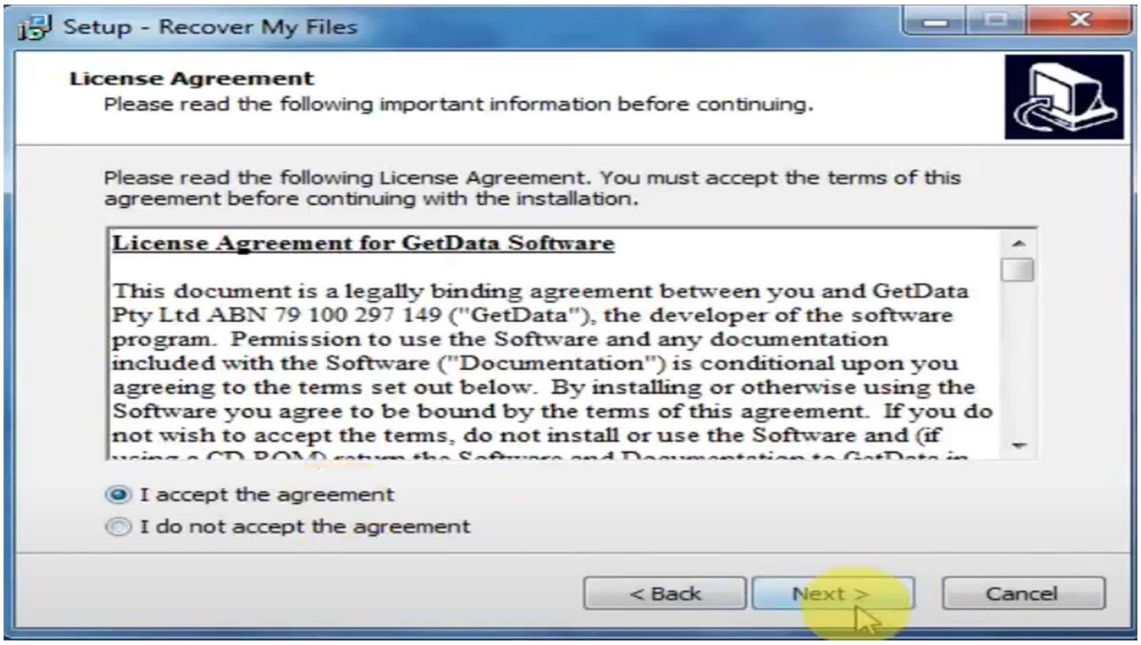


Recover data is saved to specified location



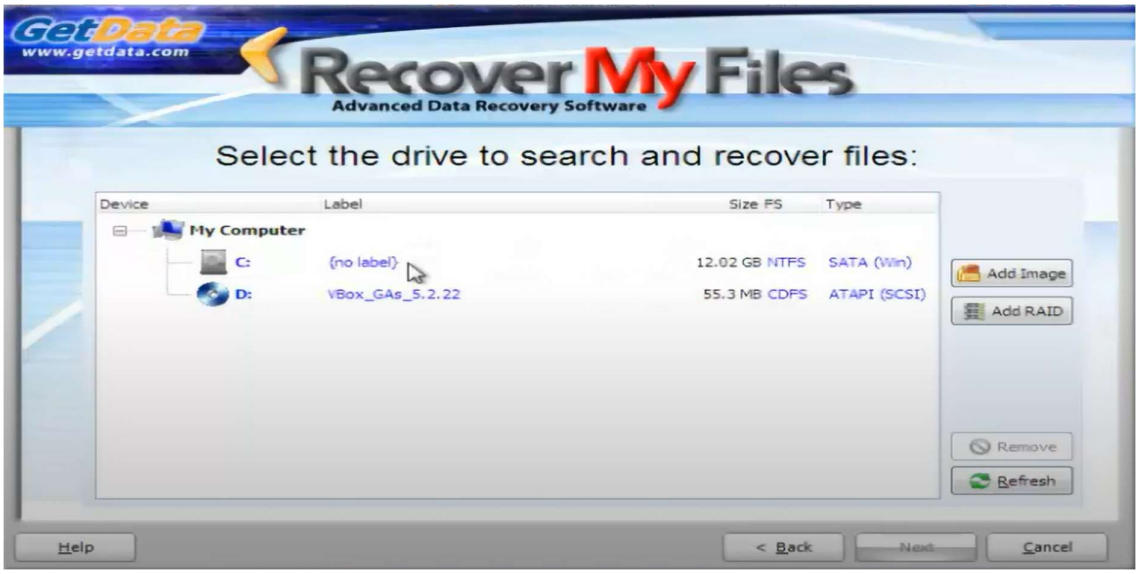
Recover My Files

Download and install Recover My Files

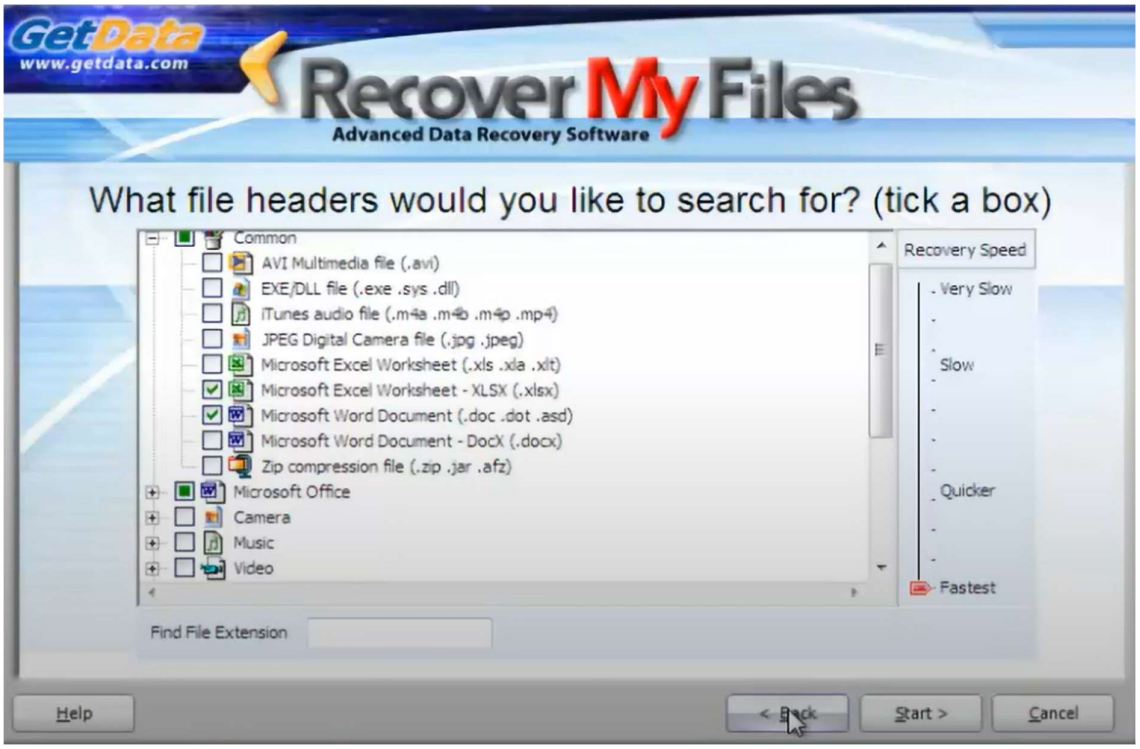


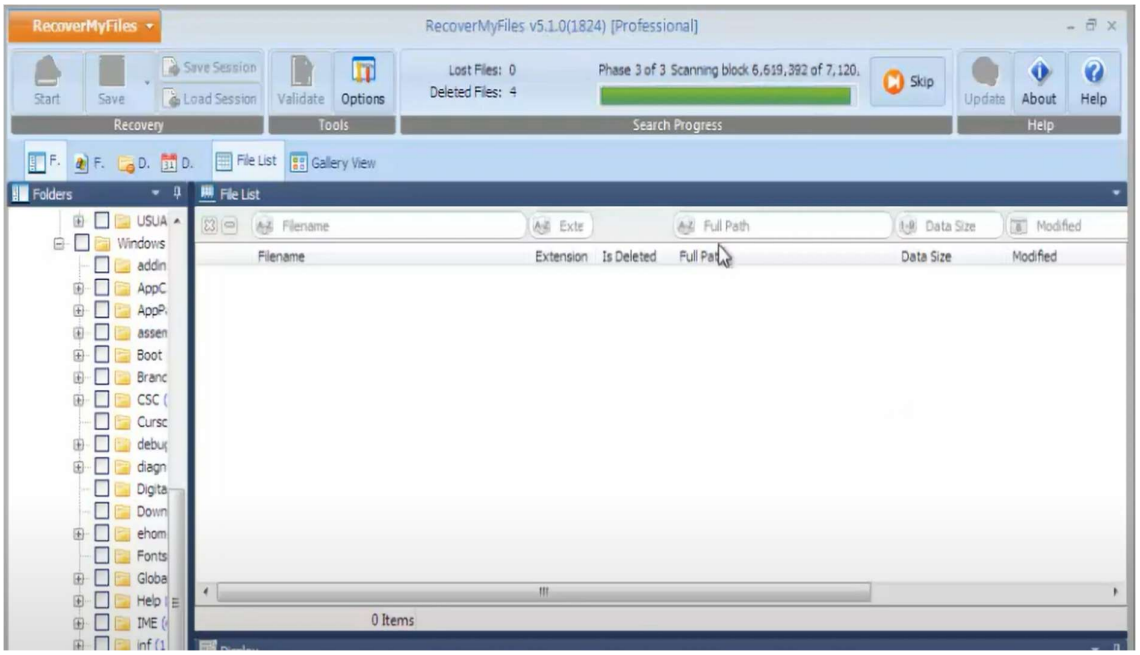
Select the option you wish to of Recover Files and Recover a Drive

Select the drive to search and recover files & select one of the File Recovery options



What file headers would like to search from recover files





Scan and save the recovered file to desired location